ISSN 0002-9920

Notices

of the American Mathematical Society

March 2010

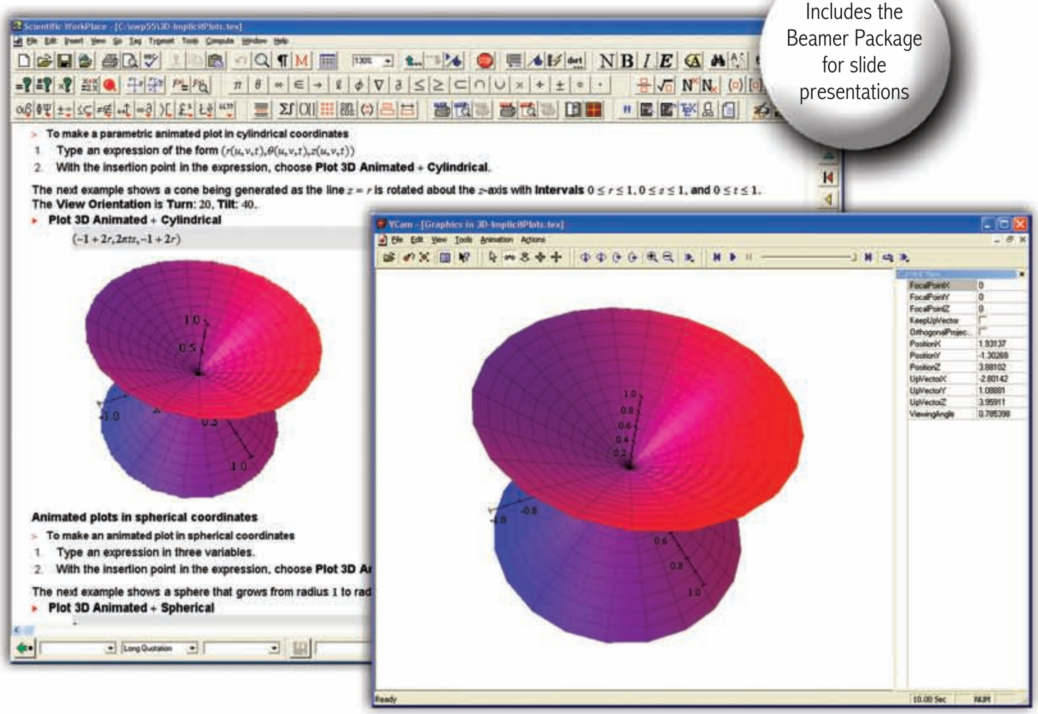
Volume 57, Number 3

Cryptography Issue
(see page 419)

Scientific WorkPlace®
Scientific Word®

- Mathematical Word Processing
- LATEX Typesetting
- Computer Algebra

Includes the Beamer Package for slide presentations



Scientific WorkPlace - [C:\swp55\3D-ImplicitPlots.tex]

File Edit Insert View Go Tag Typeset Tools Compute Window Help
130%

> To make a parametric animated plot in cylindrical coordinates

1. Type an expression of the form $(r(u,v,t),\theta(u,v,t),z(u,v,t))$
2. With the insertion point in the expression, choose **Plot 3D Animated + Cylindrical**.

The next example shows a cone being generated as the line $z = r$ is rotated about the z-axis with **Intervals** $0 \le r \le 1$, $0 \le z \le 1$, and $0 \le t \le 1$. The **View Orientation** is **Turn**: 20, **Tilt**: 40.

▸ **Plot 3D Animated + Cylindrical**

$(-1+2r, 2\pi tz, -1+2r)$

Animated plots in spherical coordinates

> To make an animated plot in spherical coordinates

1. Type an expression in three variables.
2. With the insertion point in the expression, choose **Plot 3D Ar**

The next example shows a sphere that grows from radius 1 to rad

▸ **Plot 3D Animated + Spherical**

VCam - [Graphics in 3D-ImplicitPlots.tex]

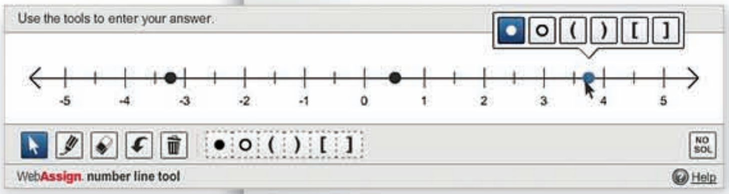
FocalPointX	0
FocalPointY	0
FocalPointZ	0
KeepUpVector	□
OrthogonalProjec	□
PositionX	1.93137
PositionY	-1.30269
PositionZ	3.88102
UpVectorX	-2.80142
UpVectorY	1.08881
UpVectorZ	3.95911
ViewingAngle	0.785398

The Gold Standard for Mathematical Publishing

Scientific WorkPlace and ***Scientific Word Version 5.5*** make writing, sharing, and doing mathematics easier. You compose and edit your documents directly on the screen, without having to think in a programming language. A click of a button allows you to typeset your documents in LATEX. You choose to print with or without LATEX typesetting, or publish on the web. ***Scientific WorkPlace*** and ***Scientific Word*** enable both professionals and support staff to produce stunning books and articles. Also, the integrated computer algebra system in ***Scientific WorkPlace*** enables you to solve and plot equations, animate 2D and 3D plots, rotate, move, and fly through 3D plots, create 3D implicit plots, and more.

MacKichan SOFTWARE, INC.

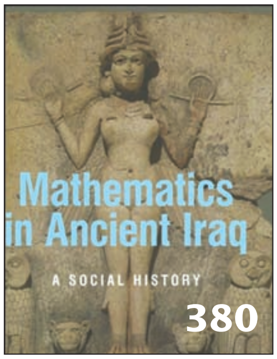
Visit our website for free trial versions of all our products.
www.mackichan.com/notices • Email: info@mackichan.com • Toll free: 877-724-9673

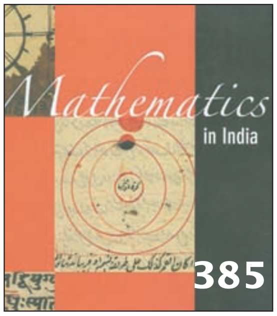

Use the tools to enter your answer.

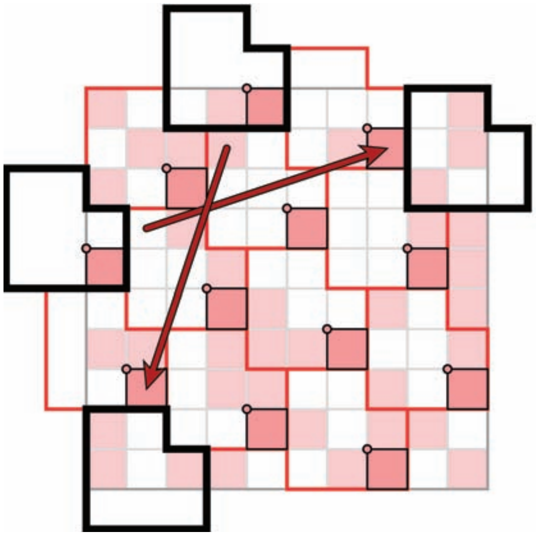
Notices
of the American Mathematical Society
March 2010

Communications

Commentary







378

Cryptography is a strong and vital influence in modern life. Security issues permeate all aspects of what we do. It is surprising and delightful that mathematics plays such a powerful role in the subject. This issue of the *Notices* considers many new developments, together with related topics in the field.

—*Steven G. Krantz*
Editor

Features

Notices
of the American Mathematical Society

SUBSCRIPTION INFORMATION: Subscription prices for Volume 57 (2010) are US$488 list; US$390 institutional member; US$293 individual member. (The subscription price for members is included in the annual dues.) A late charge of 10% of the subscription price will be imposed upon orders received from nonmembers after January 1 of the subscription year. Add for postage: Surface delivery outside the United States and India—US$27; in India—US$40; expedited delivery to destinations in North America—US$35; elsewhere—US$120. Subscriptions and orders for AMS publications should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904 USA. All orders must be prepaid.

ADVERTISING: *Notices* publishes situations wanted and classified advertising, and display advertising for publishers and academic or scientific organizations. Advertising material or questions may be sent to `classads@ams.org` (classified ads) or `notices-ads@ams.org` (display ads).

SUBMISSIONS: Articles and letters may be sent to the editor by email at `notices@math.wustl.edu`, by fax at 314-935-6839, or by postal mail at Department of Mathematics, Washington University in St. Louis, Campus Box 1146, One Brookings Drive, St. Louis, MO 63130. Email is preferred. Correspondence with the managing editor may be sent to `notices@ams.org`. For more information, see the section "Reference and Book List".

NOTICES ON THE AMS WEBSITE: Supported by the AMS membership, most of this publication is freely available electronically through the AMS website, the Society's resource for delivering electronic products and services. Use the URL `http://www.ams.org/notices/` to access the *Notices* on the website.

[*Notices of the American Mathematical Society* (ISSN 0002-9920) is published monthly except bimonthly in June/July by the American Mathematical Society at 201 Charles Street, Providence, RI 02904-2294 USA, GST No. 12189 2046 RT****. Periodicals postage paid at Providence, RI, and additional mailing offices. POSTMASTER: Send address change notices to *Notices of the American Mathematical Society,* P.O. Box 6248, Providence, RI 02940-6248 USA.] Publication here of the Society's street address and the other information in brackets above is a technical requirement of the U.S. Postal Service. Tel: 401-455-4000, email: `notices@ams.org`.

Printed in the United States of America. The paper used in this journal is acid-free and falls within the guidelines established to ensure permanence and durability.

Opinions expressed in signed *Notices* articles are those of the authors and do not necessarily reflect opinions of the editors or policies of the American Mathematical Society.

Departments

From the AMS Secretary

I thank Randi D. Ruden for her splendid editorial work, and for helping to assemble this issue. She is essential to everything that I do.

—*Steven G. Krantz*
Editor

Math Blogs

Should you blog about mathematics? Before I answer this, I should explain what “blogging” is, since there are probably three or four people who still don’t know.

A blog lets you write whatever you want and have it appear online. Your entries are displayed in reverse chronological order. People reading them can post comments, and you can reply to those comments. I could describe how to set up a blog, but that would make it seem harder than it is. Any idiot can do it, and many do. Websites like Wordpress and Blogger will lead you through the process step by step—and they’re free.

For a while math blogging was held back by the difficulty of including equations. Now Wordpress allows for TEX. So, we are now seeing a flowering of math blogs—and for some mathematicians, blogging has become an important part of their research activity.

My introduction to blogging came in 1993 when I started an online column called “This Week’s Finds in Mathematical Physics”. The idea was to write summaries of papers I’d read and explain interesting ideas. I soon discovered that, when I made mistakes, readers would kindly correct them—and when I admitted I didn’t understand things, experts would appear from nowhere and help me out. Other math bloggers report similar results.

In 2006 I joined forces with David Corfield and Urs Schreiber to start “The *n*-Category Café”, a group blog on math, physics, and philosophy. My column is now just a small part of lively discussion of topics ranging from elliptic cohomology, tensor categories, and type theory to “mathematics as a vocation”—and all these examples were taken from comments that appeared on one randomly chosen day!

By now there are over fifty math blogs in English. At least four are by Fields medalists; Timothy Gowers and Terry Tao have famously popular ones. Some math blogs are focused on specific topics: for example, “Low-Dimensional Topology” or “Motivic Stuff”. Some roam all over the map. Some start with great enthusiasm but sink into inactivity. To keep the conversation going, it helps to team up with a group of friends. A great example is the “Secret Blogging Seminar”, run by eight recent Berkeley math Ph.D.s.

Should you blog about mathematics? Judging from what I’ve seen, you should do it if you like explaining things, enjoy public discussions, and can deal calmly but firmly with arguments that get out of hand, or the occasional troublemaker. Some mathematicians are too worried about making a fool of themselves in public to enjoy blogging. Others are too afraid of offending people. And if my joke about “idiots” bothered you, blogging may be too hard-knuckled for you.

Even for those with the right personality, running a really good blog takes some skill. So, if you haven’t done so already, spend awhile reading blogs before trying to start your own. The same problems keep coming up, and you’ll see better and worse ways to deal with them.

But there’s no need to start your own blog to enjoy some of the benefits. You can get a lot out of just reading them, and more if you join the conversations. Math blogs are also a great way for students and amateurs to get a sense of what research is like. Academic math bloggers spend a lot of time talking about topics that don’t appear in the published literature. Discussions once confined to the math department lounge are now conducted worldwide. While not without problems, this is a truly wonderful thing.

Here are a few examples of what math blogs can do, all taken from the “The *n*-Category Café”. Blog entries by Urs Schreiber (a postdoc in Germany) led to online discussions which blossomed into collaborative papers with Dave Roberts (a grad student in Australia) and James Stasheff (the American topologist)—neither of whom he had ever met, except online. A discussion on *n*-categories and stratified spaces evolved into Jonathan Woolf’s new paper “Transversal homotopy theory”. Perhaps most importantly, an online community has formed that has geometers, topologists, and category theorists regularly talking to physicists, computer scientists, and philosophers of mathematics.

The Internet has been around for a while, but we are far from figuring out everything we can do with it. Blogs are not the last word: wikis, where people can jointly write and edit texts, are also catching on. “The *n*-Category Café” now has an associated wiki, the “*n*-Lab”, which is a place for collaborative research and expository writing. Timothy Gowers and Terry Tao are using blogs and a wiki to run a series of “Polymath” projects, where large numbers of people cooperate to prove theorems. Recently, the website “Math Overflow” has become a universal clearinghouse for math questions. One can imagine many more experiments with the technology we have, and still more with the technology yet to come. Some will work, some will not. It’s an adventure.

For a list of math blogs, and further discussions on math blogging, see: `http://www.ncatlab.org/nlab/show/Online+Resources`.

—John C. Baez
baez@math.ucr.edu

Numbers at Work and Play

Igor E. Shparlinski

Background

Number theory targets the most fundamental object of a human's mind: integer numbers. Its questions can be explained to high school students, while getting answers requires very deep and convoluted arguments. Its internal beauty has always been an irresistible attraction for mathematicians, computer scientists, engineers, and enthusiastic amateurs. Furthermore, its primal motivation has always been our natural intellectual curiosity rather than everyday practical needs.

Cryptography is a key technology widely deployed by private, commercial, and governmental users to ensure privacy and authenticity in secure electronic data communication. Its research directions are often driven by practical demands. For example, recently, various issues of privacy and electronic voting entered the world of cryptography. While most of us would agree that these activities are not the most pure and beautiful in our lives, cryptography has its own irresistible attraction and intrinsic motivation for further developments.

The goal of this article is twofold. We hope to convince cryptographers that number theory still has much to offer in terms of concrete results and that they can also extend their toolbox with a variety of little-used, yet powerful, methods. We also hope that number theorists will gain new interest in such an exciting area as cryptography, which guarantees to keep them supplied with new challenges. The dull, politically correct cliché that different cultures are to be explored and enjoyed rather than treated as hostile may actually be correct.

Cryptography is the best-known area of applications of number theory, but it is not the only one. The others include computer science, dynamical systems, physics, and even molecular chemistry. There are also recently emerging applications of number theory to quantum computing and financial mathematics. Nevertheless, here we concentrate only on the interplay between number theory and cryptography and on what they have given and can give to each other.

Honeymoon

Prior to pioneering works of Whitfield Diffie and Martin Hellman, Ralph Merkle and Martin Hellman, and Ron Rivest, Adi Shamir, and Leonard Adleman, which essentially invented public key cryptography (see [30]), number theory had always been considered as the most conservative and closed part of mathematics with only occasional and short-lasting affairs outside.

We briefly remind readers how the Diffie-Hellman and RSA schemes work.

In the *Diffie–Hellman scheme*, two communicating parties, say C (for a Cryptographer) and $\mathcal{M}$ (for a Mathematician) agree on a cyclic group $\mathcal{G}$, generated by $g \in \mathcal{G}$. Then C and $\mathcal{M}$ choose secret numbers x and y and compute g^x and g^y, respectively. The values of g^x and g^y are now made publicly available. It is easy to see that both C and $\mathcal{M}$ can compute

$$(g^y)^x = g^{xy} = (g^x)^y .$$

Note that g^{xy} does not carry any meaningful information. However, it can be used to derive (via a publicly known algorithm) a common key for

Igor E. Shparlinski is professor of mathematics at Macquarie University, Australia. His email address is igor@comp.mq.edu.au*;* http://www.comp.mq.edu.au/~igor/.

some pre-agreed private key cryptosystem, which C and $\mathcal{M}$ can now use for their communication. It is believed that the problem of finding g^{xy} from given values of g^x and g^y is hard, and solving the corresponding *discrete logarithm problem* is the only feasible line of attack. That is, the attacker simply tries to recover x from the given value of g^x (or does the same for y). We also recall that the order of $\mathcal{G}$ needs to be prime (to prevent the so-called Pohlig-Hellman attack of reducing the problem to prime order subgroups).

In *RSA*, C chooses two primes p and q and computes $N = pq$; note that the Euler function $\varphi(N) = (p-1)(q-1)$ can easily be evaluated. Then, C also chooses an *encryption exponent* e with $\gcd(e, \varphi(N)) = 1$ and computes the *decryption exponent* d such that

$$de \equiv 1 \pmod{\varphi(N)}.$$

Now the values of N and e are made public, while d is kept private. To encrypt a message m (represented by an integer in the reduced residue system modulo N), $\mathcal{M}$ simply computes and transmits

$$c \equiv m^e \pmod{N}.$$

The decryption is as easy:

$$c^d \equiv (m^e)^d \equiv m^{de} \equiv m \pmod{N},$$

since by the *Euler Theorem*

$$a^{\varphi(N)} \equiv 1 \pmod{N}$$

for any integer a with $\gcd(a, N) = 1$. It is also believed that, in order to attack this cryptosystem, one must find d, which in turn requires $\varphi(N)$, which is equivalent to finding the factors p and q of N.

As we have just seen, both the Diffie-Hellman key exchange protocol and RSA cryptosystem are based on very simple number-theoretic facts, which date back centuries. But certainly it was not the mathematics behind these constructions that made number theorists so excited. It was the realization that attacking these schemes required very deep insight into some fundamental properties of integers.

The sudden discovery of the great potential of number theory for very practical applications immediately got the attention of many leading researchers in number theory. Such distinguished number theorists as Neal Koblitz, Jeffrey Lagarias, Hendrik Lenstra, Andrew Odlyzko, Carl Pomerance, Hugh Williams, and many others started to actively work in this area and achieved a series of fundamental results and also established new directions.

Midlife Crisis

Unfortunately, over the years the tight links and mutual interest have somewhat diminished. Much of the cryptographic research became occupied with protocol designs. Although this is undeniably highly important and interesting, it is, typically, a not so mathematically rich part of cryptography. Certainly this must not be held against protocol design; using mathematics is not a goal, it is a way to achieve a goal. There is nothing wrong if some areas do not need much of it. Furthermore, there have been many really delightful exceptions, such as zero-knowledge proofs and the identity-based cryptosystem of Boneh and Franklin; short signatures of Boneh, Lynn, and Shacham; and the tripartite key exchange protocol of Joux. See [1] for a detailed description of these schemes.

However, due to increased applied orientation, researchers with more advanced knowledge of engineering and of actual demands of practical cryptography, but lesser fundamental mathematical background, moved into the area. In turn, this led to relying on a somewhat lightweight approach to proofs, led to creating oxymorons such as "*heuristic proof*", and developing a frequently used argument that "if we do not understand some object well enough, it behaves as a uniformly distributed random variable." Unfortunately, one of the effects of this was that mathematicians, both several individual researchers and the whole community, have somewhat distanced themselves from cryptography. The creation of NTRU [18] in the mid-1990s by number theorists Jeffrey Hoffstein and Joseph Silverman and harmonic analyst Jill Pipher was one of the few very welcome exceptions, but it did not change the trend of somewhat abstained position among most of the mathematicians. On the bright side, theoretical computer scientists have moved in, bringing with them new paradigms such as zero-knowledge proofs, secure computation, privacy protection, pseudorandomness, and many other insights which greatly expanded the scope of cryptographic research.

So, by all means, the word "crisis" in the title of this section refers only to the relations between cryptography and mathematics, but not to the progress in each individual area, which has been truly remarkable.

Surprisingly enough, in many cases it was exactly the practical aspect of cryptography which suffered first from that lack of broad mathematical background.

For example, since Neal Koblitz and Victor Miller independently invented elliptic curve cryptography (see [1]), its well-known Achilles heel was the encryption/decryption speed. The idea is based on the fact that the set of rational points on an elliptic curve over a finite field form an Abelian group under an appropriate composition law.

Traditionally, the group of points on an elliptic curve is written additively, so we talk about addition rather than multiplication, doubling rather than squaring, and multiplication by a scalar rather than exponentiation. Furthermore, typically it is easy to choose a curve for which this group contains a large cyclic subgroup of prime order. So many standard constructions such as the Diffie–Hellman key exchange scheme can be implemented over an elliptic curve, too. So far, no efficient general attack has been found on this scheme; however, this security advantage is somewhat offset by higher computational costs. Another potential weakness (which is elliptic-curve-specific) is that typically doubling a point and adding two points on an elliptic curve follow different formulas and thus take different amounts of time. This can be efficiently exploited by the so-called timing or power attacks. There is an extensive literature, where a number of very clever tricks have been suggested to remedy the situation (see [1, Chapter 29]). Unfortunately, being carried away by the race to reduce the number of arithmetic operations in computational formulas (and also balancing them between doubling and additions), the cryptographic community missed the fact that a readily available solution already existed in literature. The insight came from a number theorist. Namely, it was the paper of Edwards [16] that changed the whole game here. Since then, *Edwards curves* have become a hot topic in elliptic curve cryptography. Let us hope that history will not repeat itself and the new spiral of incremental adjustments on the original idea of Edwards curves will not distract from searching for (and finding!) new fundamental improvements.

There are also strong trends within cryptography, motivated by both inner dynamics and practical demands, to make it more rigorous. Overall, this is a very positive development; the idea goes in the right direction. Research in this area has led to such remarkable achievements as the Cramer-Shoup cryptosystem [12]. This and many other papers follow the same standards of rigor as a typical mathematical paper.

However, the quest for provable security occasionally takes too extreme forms. Nowadays, it is very hard for a newly proposed cryptographic scheme to get accepted for publication if the authors do not say something about "provable security". In turn it sometimes leads to hastily composed proofs which have gaps or simply do not address the statement they are supposed to prove. As a result, there have been quite a few completely broken "provably secure" cryptosystems. Recently, similar concerns have been expressed by Koblitz [23], albeit in maybe a too radical form; see also [25] for the follow-up discussion.

Even linguistically, the word "provable" is slightly overemphasized, as all known proofs are nothing but reductions between various problems. No one in complexity theory calls an NP-complete problem "provably hard". Nowadays, we may only dream of such a proof (and probably these dreams will last for a long time…). In any case, the author personally would put much more trust into a protocol which remains unscathed after it has been carefully examined by several well-known "code-breakers" rather than in any "provably secure" scheme.

Living Happily Ever After?

There is no reason not to! Actually there are strong indications that this may really happen. Over the last several years one could see a large group of researchers, of different academic ages, who started their careers in classical or computational number theory and moved toward cryptography. In turn the modern cryptographic community seems to be ready to embrace mathematicians.

Although this is still mostly limited to elliptic curve cryptography, this is a really delightful development. These mathematicians represent different generations and areas of number theory and hopefully will also diversify the area of applications to cryptography.

Furthermore, most mathematicians probably limit the involvement of mathematics in cryptography to only *public key cryptography*. There is, however, much more out there. For example, secret sharing, which we describe below, gives an example of such unjustly lesser-known applications. Quantum cryptography is yet another direction which is rapidly becoming very practical, too.

In fact, the main point of this article is to exhibit great opportunities for both disciplines and give several concrete examples where such joint work may start. Number theory still has a lot to offer, while cryptography provides a constant stream of new beautiful problems and points of view. Both sides just need to take a step toward each other and become more accepting:

$$\boxed{\text{Number Theory} + \text{Cryptography} - \text{Prejudice} = \text{Love}}$$

Although typically number theory plays a service role, simply responding to challenges and requests coming from cryptography, there are also examples when cryptographic techniques have directly led to very interesting number-theoretic results. Below we try to give a brief outline of several recent activities and achievements which have been cross-fertilized by, and belong to, both number theory and cryptography. Our intention has been to give a diverse scope of possible directions for further collaboration, as well as to formulate some specific problems. Unfortunately the space limitations forced us to leave out many exciting topics, such as, for example, constructions of expanders from isogeny maps on elliptic curves and their applications to constructing hash functions and investigating of the security of discrete logarithm problems on elliptic curves (see [8, 20]).

It is important to remember that number theory is not the only branch of mathematics which is related to cryptography. For instance, recently we have witnessed very exciting developments in the group-theory-based cryptography as well as recently emerged links between cryptography and polynomial algebra.

The author is indebted to Joachim von zur Gathen for the observation that three out of seven Clay Millennium problems—P vs. NP, Birch and Swinnerton-Dyer Conjecture, and Riemann Hypothesis—deal with objects of cryptographic relevance: hard computational problems, elliptic curves, and prime numbers; see http://www.claymath.org/millennium/.

Current Developments and Perspectives

In RSA We Trust!

RSA cryptosystem is based on the *Euler Theorem*, which is one of the most well-known and fundamental number-theoretic facts. However, it has always excited number theorists, not because of the way it works, but because we think that despite (or maybe because of) the simplicity of the underlying mathematics, it is very hard to break. Designing attacks on RSA and evaluating their strength is exactly where most of the interplay between number theory and cryptography has happened.

Certainly the modulus factorization attack is the most general way of breaking RSA. All factorization algorithms, heuristic and rigorous, are based on our knowledge and understanding of the behavior and distribution of smooth numbers and thus have very strong number theory contents (see [13, 30]). We recall that an integer n is called y-smooth if n has no prime divisor $p > y$. Furthermore, the elliptic curve factoring algorithm of Lenstra [24] is based on some deep facts on the distribution of elliptic curves over finite fields and class numbers.

Yet, despite very significant and concentrated efforts, integer factorization remains a very hard computational problem, which is poorly understood theoretically and practically. One of the possible ways to gain more understanding of this problem is to ask how much "help" one should request from an all-powerful oracle in order to be able to factor a given integer N. Two most impressive achievements in this direction are due to Maurer [27] and Coppersmith [10]. Maurer [27] has proved, conditionally on some natural conjecture on the density of very smooth numbers in a short interval, that for any $\varepsilon > 0$ one can request (adaptively) at most $\varepsilon \log n$ bits of information and then factor n in polynomial time. In the approach of Coppersmith [10] more information is requested, but it is limited to specific bits of prime factors of n. For example, if $n = pq$, where $p < q < 2p$ are primes, then about $0.25 \log n / \log 2$ of the most significant bits of p are enough to factor n; see also [28] for an exhaustive survey of follow-up developments. Both approaches contain a number of open problems of rich number-theoretic contents and certainly deserve more attention from number theorists.

Finally, there are also attacks on RSA that are based on an unlucky or careless choice of the modulus. For example, such is the *cyclic attack* on RSA analyzed by Friedlander, Pomerance, and Shparlinski on the basis of the results on the distribution of the Carmichael function of shifted prime numbers; see [33, Chapter 15].

Similarly, the problem of the distribution and frequency of so-called *strong primes* (see [30, Section 4.4.2]), has been resolved in [2]. In both cases, it is shown that the overwhelming majority of the moduli is perfectly safe against both threats. And also in both cases there are several exciting directions for further research and collaboration between number theorists and cryptographers.

Geometry of Numbers and Lattice-Based Cryptography

In 1978 Merkle and Hellman suggested a cryptosystem based on a very elegant idea of using a *superincreasing knapsack*, that is, a sequence of integers $a_1, \dots, a_n$ with $a_i > a_{i-1} + \dots + a_1$, $i = 2, \dots, n$ (see [30, Section 8.6]). Although in general the Knapsack Problem is NP-complete, a superincreasing knapsack is easy: Given the sum

$$A = \sum_{i=1}^{n} a_i x_i,$$

with a binary vector $(x_1, \dots, x_n) \in \{0,1\}^n$, one can recover $x_n, \dots, x_1$ consecutively by using a simple "greedy" algorithm. One, however, may try to hide the superincreasing structure by choosing a prime $p > a_n$, a random $\lambda \not\equiv 0 \pmod p$, an element π of the symmetric group S_n, and then publishing a permutation

$$c_1 = b_{\pi(1)}, \dots, c_n = b_{\pi(n)}$$

of the residues

$$b_i \equiv \lambda a_i \pmod p, \qquad i = 1, \dots, n.$$

Then a binary vector $(y_1, \dots, y_n) \in \{0,1\}^n$ is encrypted by

$$C = \sum_{i=1}^{n} c_i y_i,$$

which can be decrypted by anyone who knows p, λ, and the permutation π by computing $A \equiv \lambda^{-1} C \pmod p$, recovering $(x_1, \dots, x_n)$ for the corresponding superincreasing knapsack, and then computing $y_i = x_{\pi^{-1}(i)}$, $i = 1, \dots, n$. This idea is very attractive and encryption/decryption are both very fast. However, unfortunately, this scheme and its various extensions have all been broken by an appropriate application of the famous LLL algorithm of Lenstra, Lenstra, and Lovász; see [32]. This series of unsuccessful attempts to build a reliable cryptosystem based on hard lattice problems was quite frustrating, and for quite some time this direction was put on the back burner.

The first theoretical breakthrough, which reignited interest in lattice-based cryptosystems, happened in 1997 when Ajtai and Dwork and Goldreich, Goldwasser, and Halevi reinstated this direction. Although these cryptosystems and their variations are either impractical or under attack (or both) (see [31, 32]), they proved the vitality of the idea of using hard problems of the geometry of numbers for cryptographic purposes. Furthermore, at around the same time, the highly practical NTRU was invented by Hoffstein, Pipher, and Silverman [18]. A decade of attacks on NTRU has led to a series of modifications and adjustments of the original scheme, but it seems that it has survived the storm and provides a very secure and efficient cryptosystem.

Nowadays there is a strong and active group of cryptographers who are combining practical aspects of lattice-based cryptography with a deep and original mathematical insight; see the surveys [28, 31, 32].

There are, however, many unexplored directions. For example, is it possible to salvage the original Merkle-Hellman idea by mixing a superincreasing knapsack with some other types of easily recoverable knapsacks? It is known that iterating the modular multiplication hiding trick does not help here, but what about a more general affine transformation

$$b_i \equiv \lambda a_i + \mu \pmod{p}, \qquad i = 1, \dots, n,$$

and then insisting that the encoded message is always of the same weight $w \sim n/2$ (so the total additive shift is $w\mu$)?

There are many other possibilities to investigate and certainly an unlimited field of action for number theory.

Anatomy of Integers and Cryptographic Attacks[1]

As we have mentioned, our insight on the behavior of prime divisors of a "typical" integer underlies all modern integer factorization algorithms. There are, however, several more important, albeit not so well-known, cryptographic constructions which rely on some delicate properties of prime and integer divisors of integers.

However, these algorithms are not the only applications of number-theoretic results on the fine structure of integers. Here we recall a few more cryptographic constructions and algorithms with a rich and nontrivial number theoretic content. In particular, many cryptographic attacks target "atypical" integers, and it is important to know how rare they are.

The traditional Discrete Logarithm Problem (DLP) is the problem of finding x from a given value of g^x where g is a generator of a cyclic group $\mathcal{G}$. There are, however, several cryptographic protocols which rely on the presumed hardness of finding x from given values of $g^x, \dots, g^{x^n}$ (or, sometimes, just of two values g^x and g^{x^n}). Intuitively it may seem that this extra information cannot help much and the problem is not easier than the original DLP (corresponding to $n = 1$).

Quite surprisingly, this intuition has turned out to be wrong. In particular, Cheon [9] has shown that, ignoring some logarithmic factors:

- given g^x and g^{x^d} for some $d \mid p-1$, one can find x in time about $\mathcal{O}\left(\sqrt{p/d} + \sqrt{d}\right)$ (which is $\mathcal{O}\left(p^{1/4}\right)$ for $d \sim \sqrt{p}$);
- given $g^x, \dots, g^{x^d}$ for some $d \mid p+1$, one can find x in time about $\mathcal{O}\left(\sqrt{p/d} + d\right)$ (which is $\mathcal{O}\left(p^{1/3}\right)$ for $d \sim p^{1/3}$).

This gives rise to the question of estimating the probability with which a random prime p is such that $p \pm 1$ has a divisor d of a given size.

Fortunately, readily available results and methods, such as the classical Brun sieve as well as some more recent results, give almost perfect answers to this and related questions and imply that the above attacks apply to a rather dense set of primes. We refer to [9] for more details.

In [29], Menezes introduces the *Large Subgroup Attack* on some cryptographic protocols over a prime field $\mathbb{F}_p$. The attack can be applied, if for some $q \mid p-1$, the ratio $n = (p-1)/(2q)$ has a smooth divisor $s > q$. Banks and Shparlinski [3] have used their asymptotic formula on the probability $\eta(k, \ell, m)$ that a k-bit integer n has a divisor $s > 2^m$ which is 2^ℓ-smooth to give some insight on the frequency with which this attack succeeds on "random" primes, assuming that shifted primes $p-1$ behave like "random" integers.

One of the most interesting choices of parameters is:

$$k = 863, \qquad m = 160, \qquad \ell = 80$$

(which produces a 1024-bit prime p), in which case it has been shown in [3] that (heuristically) the attack succeeds with probability $\eta(863, 80, 160) \approx 0.09576 > 9.5\%$.

[1] *The author admits that the title of this section is greatly influenced by [14].*

Pell Equations and Pairing-Based Cryptography

Elliptic curve cryptography is yet another confirmation of the great practicality of deep mathematical theories. Recently, the area enjoyed a second wave of activity in which elliptic curves are not merely used as just an example of a finite group but in a much more subtle way, which has no analogue in other groups such as $\mathbb{F}_q^*$. Namely, following the pioneering works of Boneh and Franklin, Boneh, Lynn and Shacham, Joux, Joux and Nguyen, Menezes, Okamoto and Vanstone, a diverse scope of cryptographic applications of the Tate, Weil, and other pairings on elliptic curves has been discovered (see [1, Chapters 22 and 24] for an exhaustive survey).

A background on elliptic curves can be found in [1, 36]; however, for our purposes it is quite enough just to recall that an elliptic curve in the affine model is essentially the set of solutions (x, y) in the algebraic closure of a finite field $\mathbb{F}_q$ of q elements to the Weierstrass equation

$$Y^2 = X^3 + aX + b$$

, where the coefficients $a, b \in \mathbb{F}_q$ avoid a certain surface in $\mathbb{F}_q^2$ (and also $\gcd(q, 6) = 1$; otherwise, the Weierstrass equation takes a slightly more complicated form).

In modern applications of elliptic curves in cryptography, the notion of *embedding degree* plays one of the central roles. Recall that an elliptic curve $\mathbf{E}$ over the finite field $\mathbb{F}_q$ of q elements has embedding degree k with respect to the subgroup $\mathcal{G}$ of the group $\mathbf{E}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on $\mathbf{E}$, if $\#\mathcal{G} \mid q^k - 1$, and k is the smallest positive integer with this property. Typically, only subgroups $\mathcal{G}$ of prime order ℓ of $\mathbf{E}(\mathbb{F}_q)$ are of interest.

The above applications have naturally led to two mutually complementary directions:

- Estimating the probability that a "random" elliptic curve (in some natural sense) has a small embedding degree with respect to a subgroup $\mathcal{G}$ of $\mathbf{E}(\mathbb{F}_q)$ of large prime order ℓ.
- Finding explicit constructions of elliptic curves $\mathbf{E}$ having a small embedding degree with respect to some subgroup $\mathcal{G}$ of $\mathbf{E}(\mathbb{F}_q)$ of large prime order ℓ.

There are results of various flavors which show that a "random" curve (for different types of randomization) tends to have a large embedding degree with respect to large prime order subgroups of $\mathbf{E}(\mathbb{F}_q)$ (see [21, 26]). In particular, this means that the so-called *MOV attack* of Menezes, Okamoto and Vanstone (see [1, Section 22.2]) is not likely to succeed on a "random" curve. On the other hand, this also means that "random" curves are useless for the purposes of pairing-based cryptography, thus making the second problem even more important.

Both directions still have many open questions with a strong number theory context, even if in many cases only conditional results, under the Generalized Riemann Hypothesis and/or the Bateman-Horn Conjecture on primes in polynomial values. For example, in [26], an approach is given to getting a heuristic upper bound on the number of the pairing-friendly MNT curves, named after Miyaji, Nakabayashi and Takano; see [1, Section 24.2.3.a], (who surprisingly enough, invented this very elegant construction even before applications of pairing-friendly curves had been found). However, to get precise results one needs to estimate the order of magnitude (as the function of the parameter $z > 1$) of the series

$$S(z) = \sum_{\substack{s \le z \\ s \text{ squarefree}}} \sum_{\substack{n^2+8=3sm^2 \\ n\equiv 1 \pmod 6 \\ n \ge 2}} \frac{1}{(\log n)^2},$$

where the inner sum is taken over positive solutions $n \equiv 1 \pmod 6$, $n \ge 2$ to the *Pell* equation $n^2 + 8 = 3sm^2$ (see [19] for a background on the Pell equation). It is believed that, typically such solutions grow exponentially and the jth solution is of order of magnitude $\exp(c\sqrt{s}j)$ for some absolute constant $c > 0$ (in particular, the first solution is exponential in $\sqrt{s}$). This may lead to a suggestion that $S(z) = z^{o(1)}$. However, Karabina and Teske [22] noticed that there is a thin set of exceptional values of $s = 12k^2 + 4k + 3$, satisfying $3s = (6k + 1)^2 + 8$, for which there is a very small solution of order $\sqrt{s}$. This implies that

$$S(z) \ge C \frac{\sqrt{z}}{(\log z)^2}$$

for some absolute constant $C > 0$. In [21] this bound has been slightly improved, but the question about the precise behavior of $S(z)$ is still wide open and is of great interest for both number theory (because of the new methods it is likely to require to develop) and cryptography (because of the application to such a "hot" topic as pairing-based cryptography). Let us reiterate that so far even heuristically the situation is poorly understood.

Similar questions can be asked for other constructions (see [17] for a survey), giving unlimited opportunities for collaboration between both communities.

Secret Sharing and Algebraic Number Theory

Since Shamir introduced the first secret sharing scheme (SSS) (see [30, Section 12.7.2]), this area has enjoyed a tremendous amount of attention and work. We recall that, in the simplest settings, a "t-out-of-n" SSS is a way of distributing some information, derived from a secret key X, between n participants so that any $t + 1$ of them can recover X, but no coalition of t participants can gain any knowledge about X. The initial scheme of Shamir already used a very elegant idea of polynomial interpolation over finite fields. Later, much deeper tools of polynomial algebra and algebraic number theory were applied to improve the existing schemes. These schemes also cover many more access scenarios of threshold secret sharing over an arbitrary abelian group when given only blackbox access to the group operations and to blackbox randomness (while the original scheme of Shamir is essentially limited to secret sharing over finite fields). In turn this generality required use of much deeper number-theoretic tools. For example, Desmedt and Frankel [15] constructed a scheme based on cyclotomic fields and discussed the relations between their construction and the *Lenstra constant*. We recall for an algebraic number field $\mathbb{K}$ the Lenstra constant $L(\mathbb{K})$, introduced as a tool to study Euclidean number fields, is defined as the largest number m of algebraic integers $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{\mathbb{K}}$ such that the differences $\alpha_i - \alpha_j$, $1 \le i < j \le m$, belong to the unit group of $\mathbb{K}$. Unfortunately, $L(\mathbb{K})$ tends to be rather small.

In fact, the construction of [11], which builds upon some previous ideas of Cramer and Fehr, is still based on using algebraic numbers, but its effectiveness is not limited by the size of the Lenstra constant.

We also note that algebraic geometry, in particular constructions of curves with many rational points over finite fields, has also been used for the same purpose [7]. There is very little doubt that experts in algebraic number theory may find (and solve!) a wealth of challenging problems in this area and thus greatly contribute to its further development.

Exponential Sums and Pseudorandomness

Exponential sums, and more generally character sums, form a well-developed number-theoretic tool to show that certain objects behave similarly to uniformly distributed random variables. So there is no surprise they can be of invaluable help for analyzing cryptographic primitives; see [33] for some examples.

For example, let $g \in \mathbb{F}_q^*$ be an element of order t. The Diffie–Hellman problem (that is, recovering g^{xy} from g^x and g^y) is nowadays usually called the *Computational Diffie–Hellman Problem*, CDH. One can also consider a variant of this problem that is known as the *Decisional Diffie–Hellman Problem*, DDH, which is about distinguishing a stream of Diffie–Hellman triples (g^x, g^y, g^{xy}) from a stream of triples (g^x, g^y, g^z) where x, y, z are chosen uniformly at random from the interval $[0, t-1]$. The complexity status and interrelations between the CDH and DDH are mostly unknown, but both are presumed to be hard. One, however, may try to get some indirect evidence in support of their hardness. Motivated by this point of view, the uniformity of distribution of (g^x, g^y, g^{xy}) has been established by Canetti, Friedlander and Shparlinski and then improved by Canetti, Friedlander, Konyagin, Larsen, Lieman and Shparlinski (see [33, Chapter 3]). Finally, Bourgain [5], using very powerful methods of additive combinatorics, has greatly extended the range of t for which such a result holds. Yet one can still find here many open questions and unexplored directions.

There are also more direct applications of exponential sums. For instance, Boneh and Venkatesan [4] introduced the following problem, known as the *Hidden Number Problem*, HNP:

> *For a prime p, recover $\alpha \in \mathbb{F}_p$, given the ℓ most significant bits of $\alpha t_i \pmod p$ for k elements $t_1, \ldots, t_k \in \mathbb{F}_p$, chosen independently and uniformly at random.*

Certainly when ℓ is large (say, larger than the bit length of p), the problem is trivial. Boneh and Venkatesan [4] have given a probabilistic polynomial time algorithm which works for much smaller values of ℓ, namely $\ell \approx \sqrt{\log p}$. They have also shown that the HNP has close links with the bit security property of the Diffie-Hellman key. The latter means that recovering even a small portion of the bits of g^{xy} is as hard as recovering the whole key. This property is crucial to guarantee that when only some bits of g^{xy} are used to establish a common key for a private key cryptosystem, this does not introduce any additional weakness in the protocol. Recall that the bit length of such keys (80-120 bits) is significantly shorter than the bit length of the Diffie-Hellman key (500-1,000 bits). One of the facts used in the proof was the observation that if $t \in \mathbb{F}_p$ is chosen uniformly at random, then the probability that $\alpha t \pmod p$ belongs to a prescribed interval of length h inside of $[0, p-1]$ is about h/p.

However, it has turned out that for the above application the multiplier t is chosen from a multiplicative subgroup of $\mathbb{F}_p$, and thus the above uniformity of distribution property had to be reestablished, and this is exactly where exponential sums came into the picture (see [34]).

The HNP algorithm of Boneh and Venkatesan [4], reinforced with bounds of exponential sums, has also been used for a very "destructive" purpose, namely to attack the Digital Signature Scheme (see [33, Chapter 20]). The exponential sums which appear here are of a type which does not appear in any "pure" number theory applications, and their estimating required a combination of various techniques.

Even more surprisingly, the modification suggested in [35] to the HNP algorithm of [4] has tight links with the Waring problem in finite fields and allows the study of very general sequences of multipliers; see [34] for a survey of algorithms for several other variants of the HNP.

Finally, just to give a brief taste of the diversity of application of exponential sums to cryptography, we also mention:

- The construction of Bourgain [6] of so-called randomness extractors, a very important object in theoretic cryptography and computer science. Obtaining explicit forms of the estimates of [6] is a natural, interesting, but not easy, question.
- Results of Jao, Miller and Venkatesan [20] on the reducibility between the discrete logarithm problem on different elliptic curves with the help of bounds of character sums (implied by the Generalized Riemann Hypothesis). A natural direction of research would be to apply the large sieve technique in order to establish a similar result for almost all primes (instead of all primes as in [20]) but unconditionally.

Conclusion

By no means is this paper intended to be a survey of all links, both existing and potential, between cryptography and number theory. Many important topics and directions are left out. We still hope it says enough to exhibit the richness and potential of the two interacting galaxies of cryptography and number theory. In particular, we have tried to show to mathematicians there is much more in cryptography than RSA and other classical schemes of public key cryptography, where they can apply their knowledge and experience. On the other hand, the intent was to show to cryptographers that there is much more in mathematics than congruences and prime numbers, which can be of great value for cryptography

The author does hope that the title of this section refers only to the paper, and not to the story. In fact, we have strong reasons to expect that we are just at the beginning of a new chapter with many more exciting twists and an elaborate plot. We anticipate this will bring a lot of success and enjoyment to all its participants and interested viewers.

Acknowledgments

The author is very grateful to many cryptographers and mathematicians for providing various specific and general comments on the preliminary draft and also for supplying additional references. Unfortunately, not all of them could be included due to size limitations; on the other hand, some passages in the text are almost direct quotations of their comments. This especially applies to Jung Hee Cheon, Ronald Cramer, Joachim von zur Gathen, Jorge Jimenez Urroz, Carl Pomerance, Joseph Silverman, and Edlyn Teske.

Very special thanks go to Steven Galbraith who, besides making many critical remarks and useful suggestions, also helped with language editing.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Elliptic and Hyperelliptic Curve Cryptography: Theory and Practice*, CRC Press, 2005.

[2] W. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, Multiplicative structure of values of the Euler function, *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, vol. 41, Amer. Math. Soc., 2004, 29–48.

[3] W. D. Banks and I. E. Shparlinski, Integers with a large smooth divisor, *Integers* **7** (2007), # A17, 1–11.

[4] D. Boneh and R. Venkatesan, Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 129–142.

[5] J. Bourgain, Estimates on exponential sums related to Diffie–Hellman distributions, *Geom. and Func. Anal.* **15** (2005), 1–34.

[6] J. Bourgain, On the construction of affine extractors, *Geom. and Func. Anal.* **17** (2007), 33–57.

[7] I. Cascudo, H. Chen, R. Cramer, and C. Xing, Asymptotically good ideal linear secret sharing schemes with strong multiplication over any fixed finite field, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin (to appear).

[8] D. X. Charles, E. Z. Goren, and K. E. Lauter, Cryptographic hash functions from expander graphs, *J. Cryptology* (to appear).

[9] J. Cheon, Discrete logarithm problems with auxiliary inputs, *J. Cryptology* (to appear).

[10] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *J. Cryptology* **10** (1997), 233–260.

[11] R. Cramer, S. Fehr, and M. Stam, Primitive sets over number fields and absolutely optimal black-box secret sharing, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **3621** (2005), 344–360.

[12] R. Cramer and V. Shoup, Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, *SIAM J. Comp.* **33** (2003), 167–226.

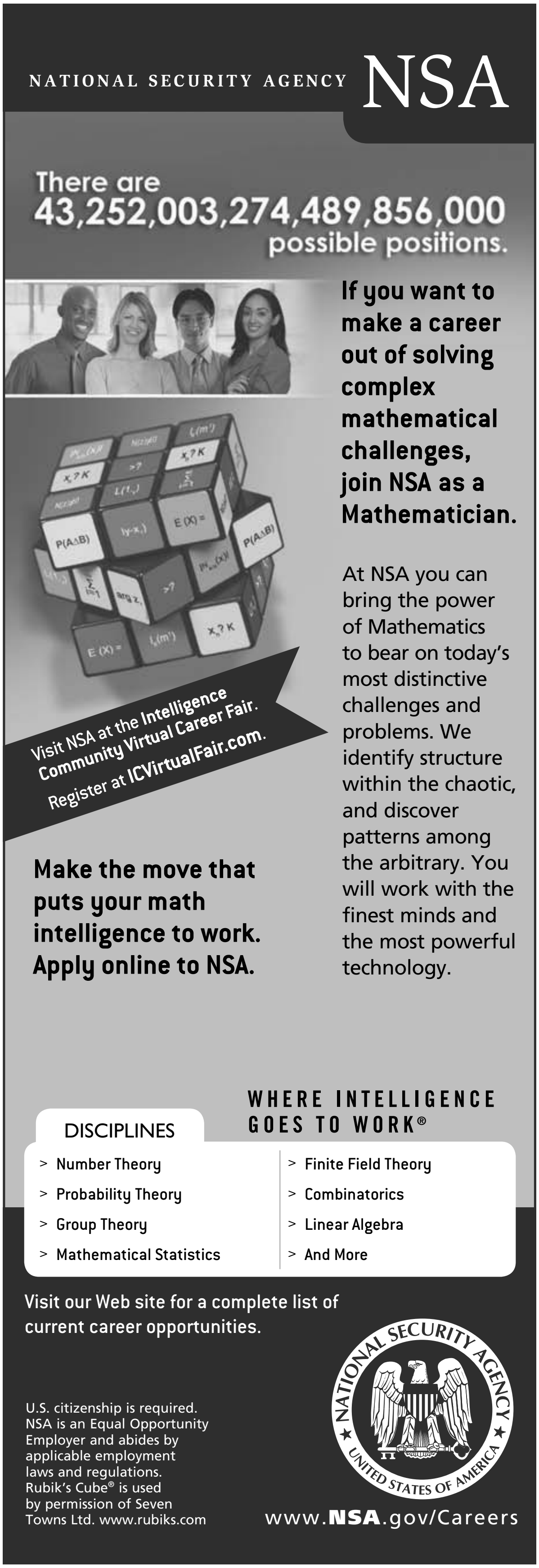
[13] R. Crandall and C. Pomerance, *Prime numbers: A Computational Perspective*, Springer-Verlag, New York, 2005.

[14] J.-M. De Koninck, A. Granville, and F. Luca (eds.), *Anatomy of integers*, CRM Proc. and Lect. Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008.

[15] Y. Desmedt and Y. Frankel, Homomorphic zero-knowledge threshold schemes over any finite Abelian group, *SIAM J. Discr. Mathem.* **7** (1994), 667–679.

[16] H. M. Edwards, A normal form for elliptic curves, *Bull. Amer. Math. Soc.* **44** (2007), 393–422.

[17] D. Freeman, M. Scott, and E. Teske, A taxonomy of pairing-friendly elliptic curves, *J. Cryptology* (to appear).



[18] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU: A ring based public key cryptosystem, *Lect. Notes in Comp. Sci.*, vol. 1433, Springer-Verlag, Berlin, 1998, 267–288.

[19] M. J. Jacobson and H. C. Williams, *Solving the Pell Equation*, Springer-Verlag, Berlin, 2009.

[20] D. Jao, S. D. Miller, and R. Venkatesan, Expander graphs based on GRH with an application to elliptic curve cryptography, *J. Number Theory* **129** (2009), 1491–1504.

[21] J. Jiménez Urroz, F. Luca, and I. E. Shparlinski, On the number of isogeny classes of pairing-friendly elliptic curves and statistics of MNT curves, *Preprint*, 2008

[22] K. Karabina and E. Teske, On prime-order elliptic curves with embedding degrees $k = 3, 4$ and 6, *Lect. Notes in Comp. Sci.*, vol. 5011, Springer-Verlag, Berlin, 2008, 102–117.

[23] N. Koblitz, The uneasy relationship between mathematics and cryptography, *Notices of the Amer. Math. Soc.* **54** (2007), 972–979.

[24] H. W. Lenstra, Factoring integers with elliptic curves, *Ann. Math.* **126** (1987), 649–673.

[25] Letters to the Editor, *Notices of the Amer. Math. Soc.* **54** (2007), 1454–1456.

[26] F. Luca and I. E. Shparlinski, Elliptic curves with low embedding degree, *J. Cryptology* **19** (2006), 553–562.

[27] U. M. Maurer, On the oracle complexity of factoring integers, *Computational Complexity* **5** (1996), 237–247.

[28] A. May, Using LLL-reduction for solving RSA and factorization problems, *Proc. Conf. in Honour of the 25th Birthday of the LLL algorithm, LLL+25* Caen, France, 2007 (to appear).

[29] A. J. Menezes, Another look at HMQV, *J. Math. Cryptology* **1** (2007), 47–64

[30] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.

[31] D. Micciancio and O. Regev, Lattice-based cryptography, *Post-Quantum Cryptography*, Springer-Verlag, 2009, 147–191.

[32] P. Q. Nguyen, Public-key cryptanalysis, *Recent Trends in Cryptography*, Contemp. Math., vol. 477, Amer. Math. Soc., 2009 (to appear).

[33] I. E. Shparlinski, *Cryptographic Applications of Analytic Number Theory*, Birkhäuser, 2003.

[34] I. E. Shparlinski, Playing "Hide-and-Seek" with numbers: The hidden number problem, lattices and exponential sums, *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **62** (2005), 153–177.

[35] I. E. Shparlinski and A. Winterhof, A hidden number problem in small subgroups, *Math. Comp.* **74** (2005), 2073–2080.

[36] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, 1995.

Can’t Decide? Undecide!

Chaim Goodman-Strauss

In my mathematical youth, when I first learned of Gödel’s Theorem and computational undecidability, I was at once fascinated and strangely reassured of our limited place in the grand universe: incredibly, mathematics itself establishes limits on mathematical knowledge. At the same time, as one digs into the formalisms, this area can seem remote from most areas of mathematics and irrelevant to the efforts of most workaday mathematicians. But that’s just not so! Undecidable problems surround us, everywhere, even in recreational mathematics!

Three Mysterious Examples

Somehow these simple questions seem difficult to resolve:

Mysterious Example #1

Tilings are a rich source of combinatorial puzzles. We can ask, for a given tile, whether or not it *admits a tiling*: that is, does there exist a tiling of the plane by copies of this tile?

For many examples, this is utterly trivial: clearly the tile at left in Figure 1 above does admit a tiling, and the tile at middle left does not. One might discover a simple proof that the tile at middle right does not admit a tiling either,[1] though it is more difficult to work out just how large a region you can cover before getting stuck. But it’s a reasonable bet that you will not be able to discover whether or not the tile at right, discovered by J. Myers in 2003, admits a tiling, at least not without resorting to some sort of brute-force calculation on a computer! Try this for yourself! A downloadable file with tiles to cut out and play with has been placed at `http://http://mathfactor.uark.edu/downloads/myers_tile.pdf`.

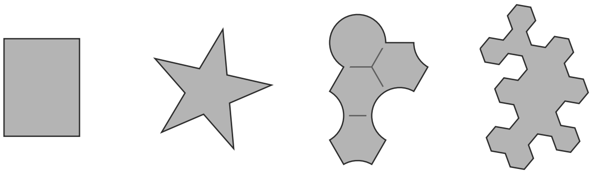


Figure 1

In general, then, we have

> `Input:` *A tile.*

and a

> `Decision Problem:` *Does the given tile admit a tiling of the plane?*

With enough brute-force effort, in some circumstances, we can answer this problem:

We might simply enumerate all possible configurations admitted by the tile, covering larger and larger disks. If the tile *does not* admit a tiling, eventually there will be some sized disk we can no longer cover, we run out of configurations to enumerate, and we then know the answer to our problem: `No`, the tile fails to admit a tiling. If a tile does not admit a tiling, the “Heesch number” is a measure of the complexity of such a tile, as the largest possible combinatorial radius of disks it can cover (in other words, the maximum number of concentric rings that copies of the tile

Chaim Goodman-Strauss is professor of mathematics at the University of Arkansas. His email address is `strauss@uark.edu`.

[1] *Hint: the tile, discovered by C. Mann, can be viewed as a cluster of hexagons, with some edges bulging inwards and some bulging out—but there are more bulging inwards than outwards. Etc.…*

can form); C. Mann discovered the current world record examples, with Heesch number 5 [22, 23]. But how can we determine whether an arbitrary given tile *does* admit a tiling?

We can modify our procedure just a bit to discover if a tile admits a *periodic* tiling:[2] As we enumerate larger and larger configurations, we check to see if we have yet come across one that can serve as a fundamental domain in a periodic tiling. If we find such a configuration we have the answer: Yes, the tile admits a tiling. The "isohedral number" is a measure of the complexity of this, as the minimum number of tiles required to form a fundamental domain (that is, the minimum number of orbits in a tiling by such a tile). J. Myers has found many bizarre examples, including the world record example, with isohedral number 10, shown in Figure 1 at right [30].

If it were true that every tile either admits a periodic tiling or does not admit a tiling at all, then we would have a procedure to settle our decision problem for any given tile—enumerate larger and larger configurations until we run out or find a fundamental domain. But could there exist an "aperiodic" tile, one admitting only nonperiodic tilings?

Almost unimaginably, could it be that there is no possible systematic method to answer our decision problem? Honestly—how hard do you suspect this could be?

If that problem were in fact *undecidable*, then we would have immediate, difficult-to-believe corollaries: There must exist an aperiodic tile—a tile which somehow wrecks translational symmetry at all scales. There cannot be a bound on Heesch number—for any N there must be a tile that can form at least N concentric rings but then somehow get stuck and never be continued to form a tiling.

Experimenting with some of the stranger examples discovered by Mann and Myers might give one pause—it seems utterly baffling to discern how and why these examples behave as they do, and others don't.

Mysterious Example #2

A large literature on the Collatz function (cf. [20, 21, 25]) has not settled this seemingly simple problem:

> Input: *A counting number n.*

Repeatedly we apply the following function to our current n, obtaining a new number n at each step: if n is odd, take $3n + 1$; if our n is even, take $n/2$; we halt if we ever obtain $n = 1$.

For example, if we begin with, say, $n = 7$, we obtain 22, then 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2 and finally 1.[3]

> Decision Problem: *On a given input, do we obtain 1 and halt, or do we enter into a loop, or do we run forever, obtaining larger and larger numbers in the long run?*

For a taste of how vexing the behavior of this process can be, work out by hand what occurs beginning with $n = 27$. Again we see our numbers grow and shrink, seemingly without rhyme or reason, until, finally, thankfully!, the process terminates after 111 steps, at one point reaching $n = 9232$.

As in the previous example, we can eventually determine, with enough patience, whether the process halts or loops on a particular given input. As of this writing, this process is known to halt on every input less than $5 \cdot 2^{60}$ [32]! Yet there is no obvious means to determine whether the process runs forever.

If we could prove, once and for all, that this process always halts, the decision problem is instantly solved for all input. But could it be that there is no theorem possible that declares, definitively, that this process always halts? Paul Erdős is said to have remarked "Mathematics is not yet ready for such confusing, troubling, and hard problems."

Mysterious Example #3

The logician Emil Post explored this system as a student in the early 1920s [33]:

> Input: *A string of* 0*'s and* 1*'s.*

We will repeatedly cross off three digits from the front of our string and tack on digits at the end by the following rule: If the first crossed-off digit is 0, we tack on 00; if the first crossed-off digit is 1, we tack on 1101.

There are three possibilities: either our string at some point will have too few letters to cross off, and we *halt*; or we might enter into a *loop*, in which the same strings recur again and again *ad infinitum*; or we might run forever, without looping, the strings eventually growing without bound.

For example, if we begin with the string 10101, we cross off 101 from the left and tack on 1101 on the right, obtaining ~~101~~01 1101 = 011101. Repeating this process we obtain ~~011~~101 00 = 10100, then 001101, and then once again 10100. So on our third string we enter into a loop of length 2.

[2] *That is, a tiling invariant under some translation. In the Euclidean plane—though not in higher dimensions nor in the hyperbolic plane—if a tile admits such a tiling, it must in fact admit a tiling with a compact fundamental domain* [16].

[3] *Of course if we allowed the process to run forever we would then have* 4, 2, *and again* 1, *ad infinitum.*

> Decision Problem: *For a given input, does this process loop, halt, or run forever?*

Running through a few examples, we quickly see how vexing this question is! As a nice exercise, consider 1··1· (where each · can be either 0 or 1—since those will be crossed off without rising to the front of the string, it cannot matter either way).

Rummaging through other small examples by hand, one is hard-pressed to find a pattern, and soon one reaches the limits of one's patience:

On input 1··1··1··0··, we run for a whopping 419 steps, before finally reaching 00 and halting.

On input 1··1··1··0··1··0··, we run for 2137 steps before entering into a loop of length 28. Along the way, the strings grow and shrink in a most confounding manner.

Worse yet, seemingly similar inputs, such as 1··1··0··1··0··1·· (which halts after just 32 steps) give rise to much simpler behavior. Can you explain *why*?[4]

Certainly, with enough patience, we can determine whether the process will halt or loop on a given input string—simply run the process until one of these two events occurs. But there is no obvious way to determine if we do *not* halt or loop! Is there a procedure that can settle this question for any given input, in a finite number of steps? Post dryly remarks that the problem has "proven intractable" [33].

Undecidability

No one knows how to answer the decision problems above. In each case, we can answer the problem for some inputs and seem to be stuck on others. In each case, the behavior of the problem on each given input can be rather unexpected, and small changes to the input can cause our process to play out in radically different ways.

In each case, we might throw up our hands and ask whether a general technique for answering the decision problem is even possible, whether one might find a theorem that could classify, in some effective manner, for which inputs the problem is answered one way, and for which, another. No one even knows, though, whether the mysterious examples above are in fact *undecidable*.

Quite remarkably, as many readers will of course know, there are in fact decision problems for which one can *prove* that no mechanical process—or procedure or algorithm—can provide an answer on any given input; problems one can *prove* are undecidable.[5]

I'll go out on a limb and state my belief that one of our mysterious examples is almost certainly undecidable, one seems not likely to be, and for one I have no idea. But of course it would be rash to say which is which.

Our main point here—which seems to be less widely appreciated—is that *undecidable problems are in a sense ubiquitous*, arising even in elementary, recreational settings.

There are hundreds of interesting and useful treatments of this subject: an excellent beginning is Sipser's *Introduction to the Theory of Computation* [39]. Minsky's classic *Computation: Finite and Infinite Machines* [29] provides valuable context and constructions. Together with its encyclopedic endnotes, Wolfram's *A New Kind of Science* [45] is a definitive sourcebook of specific, simple examples. The Wikipedia entries in this area are comprehensive and generally well written and accurate. Margenstern's helpful survey reviews the recent state of the art of our knowledge of the frontier between decidability and undecidability [24]. Smullyan's many puzzle books, particularly *The Lady or the Tiger?* [40], pose these issues in fun ways that can excite very young mathematicians. Finally, Hofstader's Pulitzer Prize-winning, delightful *Gödel, Escher, Bach* [18] continues to earn a wider audience for this subject.

The three mysterious examples each generalize to problems known to be undecidable:

Undecidable Tiling Problems

Undecidability has a long pedigree in recreational mathematics. In 1961, as an aside within his work on one of the then remaining open cases of Hilbert's *Entscheidungsproblem* ("Is a given first order logical formula satisfiable?") [4, 44], Hao Wang noted the undecidability of a particular elementary tiling problem. This began a course of development that led straight to the discovery of various "aperiodic" sets of tiles, most famously Penrose's, popularized by Martin Gardner [14].

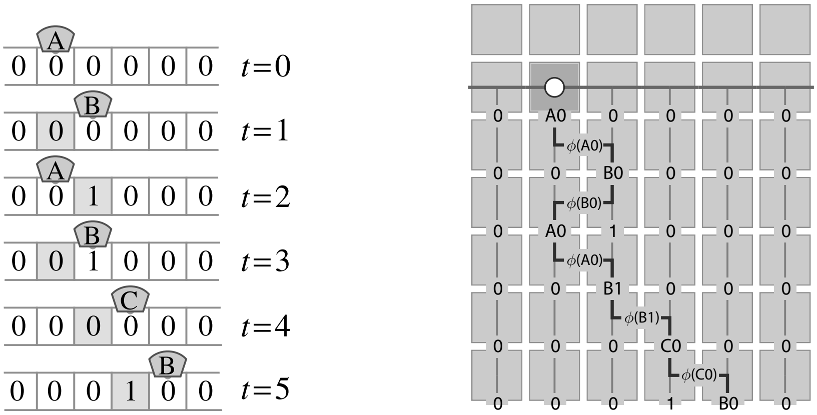
> Input: *A finite collection of tiles, and a particular "seed" configuration.*
>
> Decision Problem: *Do the given tiles admit a tiling of the plane which contains the given configuration?*

That is, can we "complete" the seed configuration to form a tiling of the entire plane,[6] using copies of some or all of the given tiles?

[4] *For that matter, why is* this *system so inscrutable but not other similar-looking systems?*

[5] *This should not be confused with the use of the word "undecidable" to mean that a given statement is independent of a specific formal deductive system, as for example the Continuum Hypothesis is independent of Zermelo-Fraenkel set theory.*

[6] *It's easy enough to decide whether we can complete a tiling of a specific-sized finite region—there are only finitely many possibilities to check.*



Figures 2a (left) and 2b (right)

Wang accomplished this by reducing the "Halting Problem" for Turing machines to his Completion Problem: For any given Turing machine, he produced a set of tiles and seed configuration, in such a way that the seed configuration could be extended to a tiling by copies of the tiles if and only if the machine never halts.

Of course the Halting Problem is a touchstone of undecidability: in 1935, through a simple and elegant construction, Turing proved there can be no procedure to decide whether a given Turing machine will halt or not [43]; consequently, there can be no procedure to tell whether one of Wang's corresponding sets of tiles, with its seed configuration, can complete a tiling of the plane.

Wang's construction is easy enough to illustrate by an example: Consider the Turing machine specified by

ϕ	A	B	C
0	0RB	1LA	1RB
1	1RB	0RC	0LH

This machine will work on an infinite tape; at each step, each cell is marked 0 or 1, and the machine will be in a particular state A, B, or C, reading one particular cell. The transition function ϕ determines the action of the machine, depending on its state and the marking it is reading; for example, if the machine is in state A reading 0, as in the upper left of the table, the machine will leave a 0 in that spot on the tape, move right one cell, and go into state B. If it is in state B reading a 0, it leaves 1 on the tape, moves one cell to the left, and goes into state A. There is one special "halt" state H—if the machine enters this state, it can do no more, and the process halts.

Beginning in state A, on a tape marked with all 0's, we can illustrate the first few steps of the run of the machine, Figure 2a. The essential point is that this illustration itself satisfies completely local rules: it is composed of pieces that must fit together in a certain manner. We can encode this as a tiling, shown in Figure 2b.

With only a little care, we then have a set of tiles, shown in Figure 3, that *can* emulate the machine. It is possible to cover the plane with copies of these tiles, so that labels on adjacent edges match,[7] as shown above.

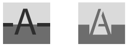
Must they emulate this machine? In any tiling containing the initial "seed tile", at upper left in Figure 3, there must be, inductively row by row, a faithful representation of the run of the machine; this can be completed into a tiling of the entire plane if and only if the machine never halts—note that the tile at bottom right in Figure 3 corresponds to the machine entering the halt state, and no tile can fit beneath it. As the Halting Problem is undecidable, so too is the Completion Problem.

(On the other hand, note that it's easy enough to tile in other ways, if we *don't* place the seed tile. For example, we could just cover the plane with copies of the filler tile at upper right in Figure 3.)

This example highlights the deep connection between *undecidability* and *computational universality*: The celebrated Church-Turing thesis in effect asserts that anything we might mean by computation can be realized by a Turing machine and thus by anything that can emulate a Turing machine. Wang's Completion Problem is undecidable precisely because it has this property, precisely because completing a tiling from a seed tile is "computationally universal" and can emulate *any* computation (albeit wildly inefficiently!).

As an aside, Wang posed the "Domino Problem" (or "Tiling Problem"): *Does a given set of tiles admit*

[7] *It is easy enough, if one prefers, to use unmarked tiles that simply are required to fit together: we may convert the labels into geometric jigsaw-like bumps and notches:*



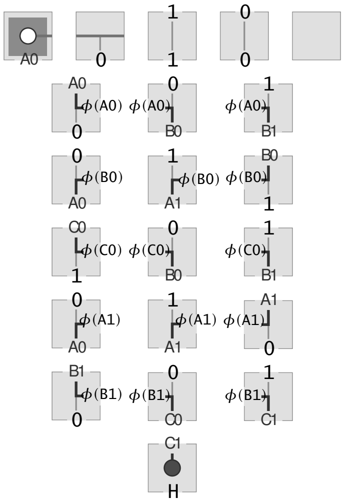


Figure 3

a tiling of the plane? This is trivial for the sets constructed above since we may cover the plane with just copies of the blank filler tile. He noted that if the Domino Problem were in fact undecidable, there must exist sets of tiles that *do* admit tilings, but *none of which* are periodic—because just as we discussed in the section Mysterious Example #1, if every set of tiles either does not admit a tiling or admits a tiling with a compact fundamental domain, then we have an algorithm for answering the Domino Problem: enumerate configurations, covering larger and larger disks, until we run out of possibilities (No, the tiles do not admit a tiling), or until we discover a fundamental domain (Yes, the tiles admit a tiling).

Wang reasonably conjectured that no such *aperiodic* set of tiles could exist—after all, somehow, just by local rules, symmetry would have to be broken at all scales—but within a few years R. Berger and then R. Robinson gave subtle proofs that the Domino Problem is undecidable, along the way producing aperiodic sets of tiles [2, 36]. Today, the Penrose tiles remain the most famous aperiodic set, but still, remarkably little is known about this phenomenon.

Fractran

John H. Conway's Fractran [7] is an amusing generalization of the Collatz function described above. A Fractran program consists of a list of fractions, say these, discovered by D. Kilminster:

$$\frac{3}{11} \quad \frac{847}{45} \quad \frac{143}{6} \quad \frac{7}{3} \quad \frac{10}{91} \quad \frac{3}{7} \quad \frac{36}{325} \quad \frac{1}{2} \quad \frac{36}{5}$$

At each step, we will have some integer n; we then multiply by the first fraction p/q in our list so that np/q is an integer, which we take as our integer at the next step. If no such fraction can be found, then the program halts, with output n.

So, for example, beginning with 10, we would first multiply by $1/2$, obtaining 5; we then multiply by $36/5$, obtaining 36; in this manner, we see 858, then 234; then 5577; 1521; 3549; 8281; 910 and then 100; after another 36 steps, we have 1000; some 150 steps later, 10^5, and 304 steps after that, 10^7. In fact, this procedure generates the primes—every power of ten that appears is a prime power, and every prime power appears, in order! Astonishing!

Most generally, a Collatz-like function is of the form

$$f(n) = \begin{cases} a_0 n + b_0 & \text{for } n \equiv 0 \bmod N \\ a_1 n + b_1 & \text{for } n \equiv 1 \bmod N \\ \dots & \\ a_{(N-1)} n + b_{(N-1)} & \text{for } n \equiv N-1 \bmod N, \end{cases}$$

where N is some fixed counting number and all the a's and b's are rational, chosen in such a way that for integers n, $f(n)$ is an integer as well. The function f is completely specified by the list of values $N, a_0, b_0, \dots a_{(N-1)}, b_{(N-1)}$, and our input is thus

> Input: *f and some integer n_0.*

Iterating f, obtaining, $n_0, f(n_0), f(f(n_0)), \dots$ we ask

> Decision Problem: *Does iterating f on n_0 ever lead to a repeating loop of values?*

A Fractran program can be described as a Collatz-like function with all $b_i = 0$ (taking N to be the least common multiple of all the denominators in the program). Though the Fractran program above seems to work by magic, it is easy, just as with Wang's Completion Problem, to see that this decision problem is undecidable, and that in fact, *any* computation can be encoded in Fractran!

Conway pulled off this trick by encoding Minsky register machines, which themselves are computationally universal [28, 29]. A Minsky register machine can be thought of as having "registers" $a_1, a_2, \dots a_k$, each of which can take on a value in $0, 1, 2, \dots$, and a list of instructions of the form:

> Instruction I_n: Increment a_n and go on to instruction I_{n_1}

or

> Instruction I_n: If register $a_n > 0$, decrement a_n and go to instruction I_{n_1}; otherwise go to instruction I_{n_2}.

It is not hard to see how we can build these up into subroutines, and we do not gain any power by allowing more complex instructions such as

> Instruction I: If $a > k$, decrement a by j, increment b by 2, and go to instruction A, otherwise increment a and go to instruction B.

Nor is it difficult to believe that anything we might be able to calculate using, say, assembly language could be calculated by a Minsky register machine. (It is substantially more remarkable, as Minsky showed [28], that already just two registers are sufficient to carry this out!)

Given such a list of instructions, it's not hard at all to construct a Fractran program that faithfully emulates the machine:

To each register a_n and each instruction I_n, we associate a unique prime number. For example, if our machine has three registers a, b, c and three instructions A, B, C, we associate these with $2, 3, 5$ and $7, 11, 13$, respectively. Then at each step of the run, our integer will be of the form $2^a 3^b 5^c I$, where I is one of $7, 11, 13$, depending on which instruction we are to read next.

An instruction of the form "Instruction A: Increment a and go to instruction B" is encoded quite simply as the fraction $22/7$: All of the other fractions in the program will have a factor of 11 or 13 in the denominator, but not 7, and so if at a given time our integer is $2^a 3^b 5^c 7$, we must faithfully execute instruction A, obtaining $2^{a+1} 3^b 5^c 11$. Similarly, an instruction of the form "Instruction A: If register $a > 0$, decrement a and go to instruction B; otherwise go to instruction C" is encoded simply as the pair of fractions $11/14$ and $13/7$, in that order.

There is only one small caveat: in a Fractran program, no instruction can jump to itself; for example, within an instruction A, we cannot go directly to A—the corresponding primes would cancel in the fraction encoding this instruction! But this is easy to work around, by introducing intermediate dummy instructions—we go to some instruction A' and then on to A. On the other hand, Fractran allows many shortcuts! It is quite pleasurable to work out just how Kilminster's program carries out its task; Conway has given other elegant examples in [7].

Precisely because arbitrary computations can be encoded as Fractran programs, problems such as these must be undecidable:

> Input: *A finite sequence of rational numbers and a starting integer.*

We iteratively multiply by the first rational number in the sequence for which the result is an integer; unless no such rational is available and we halt and ask:

> Decision Problem: *Will we ever halt?*

Both this and the problem earlier in this section are just disguised forms of the Halting Problem.

Post Tag Productions

The example in section Mysterious Example #3 generalizes readily: specify an arbitrary alphabet $\mathcal{A}$; for each letter $a \in \mathcal{A}$ a word σ_a which it produces; a starting word ω_0; and some fixed constant k.

At each step, we have a word ω_n; if the length of this word is less than k, then we halt; otherwise, we produce ω_{n+1} by striking off the first k letters of ω_n and appending σ_a where a is the first letter of ω_n. We can indicate this production rule by writing $ab\omega \to \omega\sigma_a$, where the variable b stands for any word of length $k-1$, and ω for any word at all.

For example, we might take $k = 2$, and $\mathcal{A} = \{a, b, c\}$, and specify $\sigma_a = cb, \sigma_b = aaa$, and $\sigma_c = a$. Taking $\omega_0 = aaa$, we produce in turn $aaa \to \cancel{aa}a\,cb = acb \to \cancel{ac}b\,cb \to baaa \to aaaaa$, which we abbreviate as a^5. Focusing on just the words of the form a^n, we soon produce a^8, a^4, a^2, and finally $a^1 = a$, at which point we have too few letters to cross out, we cannot apply our rules, and the process halts.

In fact, this system precisely encodes the Collatz function [10]! Beginning with a^n, with n even, it is not difficult to see that after n iterations, we obtain $a^{n/2}$. If $n > 1$ is odd, then $n+1$ iterations produce $a^{(3n+1)/2}$. Our process eventually halts if and only if iterating the Collatz function eventually reaches 1.

> Input: *A set of "tag" productions and a start word.*
>
> Decision Problem: *Does the process eventually stop, beginning with the given start word?*

Tag production systems are a simple and useful undecidable system, with a beautiful mathematical history, initiated by Post while a student in the early 1920s, reaching fruition with his lovely Normal Form Theorem in 1943 [33] and then the constructions of universal tag systems in the 1960s [6, 28]. Yu. Rogozhin [37] and others have used tag production systems to construct remarkably small "universal Turing machines", and M. Cook's proof of the computational universality of Wolfram's cellular automaton "Rule 110" relies on the device of "cyclic tag systems" [8].

Most generally, we may consider production systems of the following "canonical" form: Beginning with a finite list of words ("axioms"), we repeatedly produce new words ("assertions") on the basis of old ones, by production rules of the form

$$\begin{gathered}
g_{11}\omega_{11}g_{12}\omega_{12}\dots\omega_{1n_1}g_{1(n_1+1)},\\
g_{12}\omega_{12}g_{22}\omega_{22}\dots\omega_{2n_2}g_{2(n_2+1)},\\
\vdots\\
g_{m1}\omega_{m1}g_{m2}\omega_{m2}\dots\omega_{mn_m}g_{m(n_m+1)}\\
\longrightarrow\\
g_1\omega'_1 g_2\omega'_2\dots\omega'_n g_{n+1}
\end{gathered}$$

where all the g's are specified, fixed, possibly empty words, and the ω's are variables, each ω'_i being some one of the ω_{jk}'s. That is, each production is a rule for generating a new assertion on the basis of one or more earlier assertions.

As a specific example, on the alphabet $1, +, =$, take as a single axiom $1 + 1 = 11$ and production rules $\omega_1 + \omega_2 = \omega_3 \to 1\omega_1 + \omega_2 = 1\omega_3$ and $\omega_1 + \omega_2 = \omega_3 \to \omega_1 + 1\omega_2 = 1\omega_3$, producing such arresting assertions as $1111 + 11 = 111111$ and $1 + 11111 = 1111111$.

As a more interesting example, take alphabet $1, A, B, C, D$, axioms $A111$, 11 and productions

$$\begin{array}{rcl} A\omega & \to & A\omega 1 \\ A\omega 1 & \to & B\omega C D\omega 1 \\ \omega_1 1 C\omega_2 1 & \to & 1\omega_1 C 1\omega_2 \\ \omega_1 BC\omega_2 1 & \to & B\omega_1 C\omega_2 1 \\ \omega_1 B\omega_2 1 C\omega_3 D & \to & B\omega_1\omega_2 CD\omega_3 \\ 11BC\omega D1 & \to & \omega 1 \end{array}$$

which generate the prime numbers! (That is, the assertions of the form $1\dots1$ are precisely the prime numbers in unary form [29].) The active reader should be able to work out the mechanism behind this by tracing out what is produced beginning from each $A1\dots1$, with either a prime or composite string of 1's.

Post makes the point that essentially any formal, mechanizable system can be described as the applications of such rules: the local application of mechanical rules on strings of symbols. It is in fact not too difficult to design rules that can, say, emulate a Turing machine or produce all the theorems under some first-order formal system. But how simple can our systems be and still be powerful?

A production is in "normal form" if all of its production rules are of the very simple form $g\omega \to \omega g'$, with one variable and two fixed words; given the apparent simplicity of such systems, it is remarkable that:

Normal Form Theorem (Post, [33]). *Given any system in canonical form, on alphabet $\mathcal{A}$ there exists a system in normal form on alphabet $\mathcal{A}' \supset \mathcal{A}$ so that the words produced by the first system are exactly those produced by the second, that contain only letters in $\mathcal{A}$.*

In other words, in effect, *every* formal system can be captured by some system in normal form! But we can go further: Post's "tag"[8] productions are a special kind of system in normal form: in a tag system we require that for any pair of rules $g_1\omega \to \omega g'_1$, $g_2\omega \to \omega g'_2$ where both g_1 and g_2 begin with the same letter, then $g'_1 = g'_2$, and that all of the fixed words g on the left of the production rules have the same length. Such a system then can be thought of as in our initial example: at each step, cross off some k letters, tacking on a string on the end as determined by the first letter crossed out.

So in our initial example, as a normal form system, we have nine rules:

$$ax\omega \to \omega cb \qquad bx\omega \to \omega aaa \qquad cx\omega \to \omega a$$

where x is each of a, b, c.

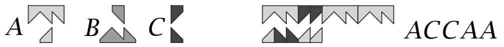
These systems are truly restricted and seem so simple! It seems incredible that they could have much power, yet by 1961, Minsky showed tag systems to be computationally universal [28], as Post suspected: given any Turing machine, there exists a tag system that completely encodes the machine's behavior. In particular, then, it is undecidable whether a given word is an assertion by a particular tag system, and it is undecidable whether a given tag system halts; Cocke and Minsky soon showed that $k = 2$ would suffice [6].

A Few More Examples

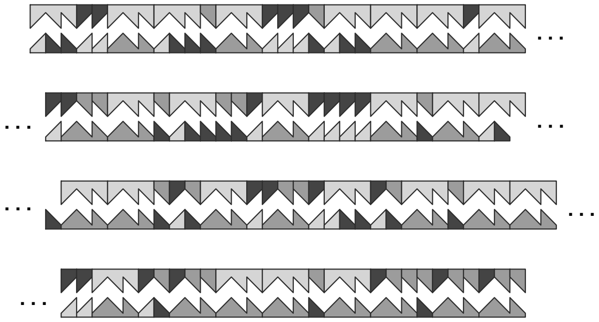
Fun, simple examples abound! Here are several more:

The Post Correspondence Problem

Can you solve the following puzzle? Pairs A, B, C of puzzle pieces are shown; select some sequence of pairs of pieces, forming a top row and a bottom row of pieces that must fit together.



It's not hard to see that any such sequence must begin with pair A and continue $CCAA\dots$. It may be surprising that the shortest possible sequence requires 75 pairs:



There is actually a second solution of 75 pairs; can you find it?

More generally, an instance of the Post Correspondence Problem has

> `Input:` *A finite collection of ordered pairs of words (A_i, B_i) in some fixed alphabet,*

and we ask:

[8] *So called because Post envisioned a finite-state machine reading one portion of a tape and writing on another; as the length of the tape between them grows and shrinks, the read and write heads appear to be playing a game of tag.*

size	width	record instance known	# min sols	sol length	author
3	3	((0,1),(1,011),(011,0))	2	75	Lorentz & Waldmann
3	4	((001,0),(1,1001),(0,01))	1	452 (?) (> 340)	Rahn & Stamer
3	5	((0,001),(00100,0),(10,0100))	1	288	Rahn
4	3	((0,011),(001,1),(1,00),(11,110))	?	595	Rahn
4	4	((0,00),(0000,0101),(0001,10),(101,1))	1	781	Rahn

> `Decision Problem:` *Does the instance have a solution? That is, is there some nonempty sequence of indices $i_1, i_2, \ldots i_n$ with $A_{i_1} A_{i_2} \ldots A_{i_n} = B_{i_1} B_{i_2} \ldots B_{i_n}$?*

Post's original point was that it is quite easy to encode a given set of productions in normal form as an instance of the Correspondence Problem—certainly easy enough for the active reader to rediscover how!

In the example above, discovered by R. J. Lorentz and J. Waldmann [41], we could regard our alphabet as $\{0, 1\}$ (drawn as zags slanting up to the right and down to the right respectively), with pairs $(011, 0)$, $(1, 011)$, $(0, 1)$. This example is known to be the longest possible minimal solution known among instances with alphabets of two letters, in three pairs of words, each of length at most three. Heiko Stamer's website PCP@HOME [41] features an evolving list of other record examples, all on an alphabet of two letters (see chart above).

M. Rahn [34] has identified many exotic instances, some of which may themselves beat these known records by substantial margins: Consider ((0,01),(1,10)), which has no finite solution but does admit the Thue-Morse sequence as an infinite solution. But adding one more pair of words gives an instance that has so far resisted analysis: ((0,01),(1,10),(0010,0)).

It is impossible to explain any of these in any satisfying manner: *why* are they as they are—and why are others *not*? Apart from the Lorentz and Waldmann example, which is known to be a true record, it is highly likely that the actual records are far worse—and perhaps will never be known. In particular, as we soon shall see in the section How Bad Can These Examples Be?, as the size and width increase, the largest possible minimum solution length must grow *faster than any function that can be explicitly described!*

This chart illustrates several hallmarks of undecidability: The interesting instances seem to have an arbitrary, *ad hoc* feel. The known record examples may or may not have much structure, though such structure may be needed in order to prove that the example actually has a solution. There are examples that seem beyond analysis, that will beat known records, if they do have a solution. The size of the true record solutions will grow rapidly with the size of the instances. Each of these phenomena is explainable by studying the "proof-complexity" of an undecidable decision problem, as we will discuss soon in the section How Hard Are These Examples to Understand?.

On the other hand, it is not hard to prove that the Post Correspondence Problem is undecidable: The essential idea is that any given Turing machine can be encoded as a collection of pairs of finite words so that any finite run of the machine corresponds to a finite sequence of pairs. The key is that the top row runs just one step ahead in time of the bottom row; the bottom row can "catch up" and there is a solution if and only if the machine eventually halts. Nicely written accounts of this proof appear in [29, 39]. More subtle constructions allow the encoding of an arbitrary Turing machine with as few as seven rules [31] or with only very short rules of width two [17]. It is not known whether instances with fewer than seven rules already have this power, but already the Collatz function can be encoded with just five—suggesting that this case is at a minimum very difficult to understand [34]. Up-to-date summaries can be found in [34, 41] and in the bibliographic references found therein.

NP-Hard Problems

Thousands upon thousands of problems are now known to be NP-hard, and the threshold for this distinction does not seem particularly high: In essence, a problem is NP-hard if it is as difficult as any NP problem, that is, a problem with a solution that can be checked in a reasonably effective manner—below we touch cursorily on the elegant formalisms that make this rigorous, but among hundreds of excellent references, Garey and Johnson's classic *Computers and Intractability* [15] and Sipser's more recent textbook [39] will serve most beginning needs.

Yet undecidability lurks within every setting complicated enough to have NP-hard problems! Admittedly, the construction here will be somewhat artificial—to my knowledge, the following idea has not been exploited to produce simple, reasonable undecidable problems from NP-hard ones—but it is amusing to know that undecidability lurks in the Traveling Salesman Problem, the computer game Minesweeper, Sudoku puzzles, or any of the myriad NP-hard settings. And again, our main point is that undecidability resides in every combinatorially interesting corner: here we give a large and robust collection of (OK, seemingly contrived) examples.

We begin with S. Cook's original NP-hard problem, SAT, the satisfiability problem [9]:

> `Input:` *A collection of boolean variables $\{q_1, \ldots q_k\}$, and a collection of clauses, each of the form $p_1 \vee \ldots \vee p_l$ with each $p_i \in \{q_1, \ldots q_k, \overline{q_1}, \ldots \overline{q_k}\}$.*
>
> `Decision Problem:` *Is there an assignment of values to the variables so that all of the clauses are true—that is, is the instance* satisfiable*?*

Cook's insight was that one can show a problem is NP-hard by showing it can encode finite runs of nondeterministic[9] Turing machines. In particular, he showed SAT is NP-hard by giving a simple procedure for encoding each assertion that a given machine M can halt, accepting its input word ω, in less than n steps. The construction is strikingly elementary, with some similarity to the tiling example in the section Undecidable Tiling Problems:

The variables encode such individual assertions as *"the kth cell contains letter a at time t"*, or *"the machine is reading the kth cell, in state s, at time t"*. The clauses build these up, averring *"the machine is in exactly one state at time t"*, *"the kth cell contains exactly one letter at time t"*, as well as statements that depend on the machine itself: *"if at time t, the machine is in state s reading a in cell k, then at time $t+1$ the machine is in state s', one cell to the left* (say) *and cell k now contains letter b, or* (as these encode nondeterministic machines) *the machine is in state s etc."* Finally all the clauses assemble into one grand assertion: *"The machine can halt and rest in the accept state by the end of the run, at time n."* This instance of SAT perfectly encodes the run of the machine—it is satisfiable if and only if the machine can indeed halt by time n.

It's not too difficult to work out a process to carry out this encoding, and there will be a certain boring uniformity to all of the instances of SAT that arise from whatever encoding process we choose. Having a specific method in mind, then, consider the individual instances SAT(M,n) of SAT encoding runs, of length n, of each (deterministic) Turing machine M, on empty input, the instance being satisfiable if and only if the machine halts by time n. Fixing M, the instances SAT(M,n) all appear roughly the same, the same building blocks repeated in a regular way, each instance in a sense contained within the next as n increases.

But then we have the following:

> `Input:` *A machine M.*
>
> `Decision Problem:` *Is there an N such that for all $n \geq N$, the instances SAT(M,n) are all satisfiable?*

This is, of course, merely a disguised form of the Halting Problem and so is undecidable.

Now we leverage this out into the wider class of NP-hard problems. SAT itself is transparently in NP: any purported solution of an instance can be rapidly checked. Consequently, *any* NP-hard problem itself encodes SAT, and in turn encodes finite runs of arbitrary Turing machines. In particular, any such encoding must be comparatively simple and tractable (through the formalism of polynomial time reducibility), and just as with SAT(M,n), the instances that arise will have a certain rather tedious regularity and can be quite explicitly described.

So, for example, HAM asks whether a given graph contains a Hamiltonian cycle; as HAM is NP-hard, we thus obtain an explicit means for constructing graphs HAM(M, n) for each given machine M and counting number n, so that HAM(M, n) contains a Hamiltonian circuit if and only if M halts by time n. Consequently it is undecidable, for a given M, whether infinitely many of the graphs HAM(M, n) do in fact have a Hamiltonian circuit.

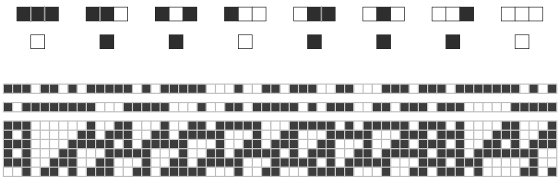
Or ... the list goes on: any of the thousands of problems known to be NP-hard may be converted into such an undecidable problem. Given an NP-hard decision problem P, we can construct for each given machine M and counting number n an instance $P(M, n)$ so that $P(M, n)$ is decided `Yes` if and only if the machine M halts by time n; it is thus undecidable for each given M whether infinitely many of the $P(M, n)$ are decided `Yes`. And, again, as contrived as this construction appears, typically the specific instances of $P(M, n)$ will have a somewhat regular feel, having been built out of basic building blocks in a mechanical way—the collection is not *entirely* artificial.[10]

Some Very Simple Universal Systems

We close this section with some very simple, absolutely remarkable universal systems. Each of these is a single instance—a single Turing machine, for example—that by itself can emulate any computation by reading and executing a program as input. Of course, the computer I am typing on now is exactly such a system (ignoring the limitations of time and memory!), but these are vastly simpler, though vastly less efficient!

[9] *That is, a broader class of machines for which there might be more than one valid transition from a given state, reading a given symbol. Cook does not construct clauses asserting that the machine* does *halt in the accept state by time n, but that it* can, *that there is some sequence of valid transitions that leads to halting. For our discussion of decidability, we need only use deterministic machines, but the construction is indifferent and works either way.*

[10] *And what of the converse? Does every undecidable problem give rise to an NP-hard one? We prove a problem is undecidable by showing it can encode unending runs of deterministic Turing machines; to obtain an NP-hard problem, we need only modify our problem to encode finite runs of nondeterministic machines.*



Such very simple universal systems can be very useful in proofs that other problems are undecidable: one need only show that such a system can be encoded in the problem we are trying to analyze.

Word ladders were invented by Lewis Carroll: Can you, for example, convert the word `sleep` into the word `dream`, at each step changing one letter, always maintaining a legitimate English word?

Word ladders are themselves decidable, simply because there are only finitely many legitimate words to comb through. But the formal productions discussed in the section Post Tag Productions are a kind of generalization, and there are many specific undecidable examples. G. S. Tseitin and Dana Scott found simple universal, undecidable examples in 1956 [38, 42]:

> `Input:` *Two words α and ω written in the letters* `a`, `b`, `c`, `d`, `e`

We are allowed to make the following seven substitutions:

```
ac ↔ ca     ad ↔ da     bc ↔ cb     bd ↔ db
  ce ↔ eca     de ↔ edb     cdca ↔ cdcae
```

> `Decision Problem:` *Is there a sequence of substitutions taking α to ω?*

In 1966 Y. Matiyasevich [26] found a means of encoding any such system into one with just two letters and three substitutions! One of the substitutions, however, uses quite long words; encoding the example above requires a substitution between one word of length 304 and another of length 621.

Conway's Game of Life is well known to almost every first-semester programming student as a fun and diverting homework assignment. It is less widely remembered that Conway specifically sought this as a simple, universal model of computation; one can "program" by specially setting the start state, and then recording how the playing field evolves through time [13].

Wolfram's Rule 110 was conjectured to be universal, and though litigation delayed publication for many years, M. Cook finally produced a proof [8] by showing that this 1-dimensional cellular automaton can emulate "cyclic" tag systems and that these themselves are computationally universal. This automaton has, at every time, an infinite row of cells each colored white or black. At the next step the color of each cell is determined by its current color and those of its neighbors, by the simple rule shown in the top two rows of the figure at left.

A short run of the machine can appear as in the bottom part of the figure at left.

However, in order to emulate a given Turing machine, the automaton must begin on a specially prepared infinite but repeating pattern.

The (2,3) universal Turing machine was conjectured universal by S. Wolfram, who in 2007 offered a US$25,000 prize for a proof, awarded to A. Smith within just a few months:

ϕ	A	B
0	1RB	2LA
1	2LA	2RB
2	1LA	0RA

A vigorous discussion followed, as Smith's proof requires encoding the emulated machine as a particular infinite pattern on the tape. These patterns are not periodic, as with Rule 110, but they are highly ordered—that is, they are generated by simple machines that are not themselves computationally universal. As even a casual reader can guess, this result can be interpreted in a variety of ways: there is a widespread sense that, though elegant and interesting, Smith's proof enlarges the notion of "universal Turing machine". The interested reader can ask for no better starting point than the talk page of the relevant Wikipedia article [46], following the many outward links from there.

Many small universal machines working off of a finite input have been found by several authors, notably Yu. V. Rogozhin [37], C. Baiocchi [3], and D. Woods and T. Neary [47].

What Does This Mean to the Workaday Mathematician?

By this time, this article has made its case as best it will: undecidable, computationally universal problems are ubiquitous, occurring everywhere in mathematics, even in the simplest settings. Why, indeed, even elementary arithmetic already has enough power to fully encode arbitrary computation, as Gödel, Turing, and Kleene each point out [5, 19].

In essence all that is required is some sort of collection of simple elements interacting in a relatively constrained manner; whether symbols on a page, mathematical objects in some structure, or a soup of chemicals, one expects the full power of computational universality to kick in readily. Computational universality can be found in devices made of Tinkertoys or stone-age ropes and pulleys [11] or powered by billiard balls [12].

Of course there are many famous, natural examples in more classical mathematical realms. It is undecidable whether a diophantine equation has a solution; whether a given presentation describes the trivial group; whether two 4-manifolds are homeomorphic. Even in elementary analysis we have such trouble as [35]:

Let E be a set of expressions representing real, single-valued, partially defined functions of one real variable, containing rational-valued constant functions, the identity function x, the functions $\sin x$, $\ln x$, $|x|$ *and* e^x, *and closed under at least* $+, -, \times$ *and composition* (of course we restrict ourselves to just such a set in our algebra and calculus courses). *Presume too that there is at least one expression in E that has no antiderivative in E* (for example, e^{-x^2}).

`Input:` *An expression A in E*

Each of the following is undecidable!

`Decision Problem:` *(a) Is* $A(x) = 0$ *for all x?*
(b) Is $A(x) \geq 0$ *for all x?*
(c) Does A have an antiderivative in E, a B in E with $B'(x) = A(x)$*?*

Would it relieve or upset our calculus students if they knew there were no way to decide whether a given elementary function has an elementary antiderivative?! In considering how much trouble a given setting might provide, we rely on

Conway's Presumption: *If a lot is going on, everything can.*[11]

Meaning that if a system has enough complexity, the betting man should assume there are enough building blocks to encode arbitrary computation. At the very least, the betting man is not likely to be contradicted! Examples abound, and it does not take much to lift off into computational universality—in some sense we might argue that this is the generic condition!

How Bad Can These Examples Be?

Over and over again, we see very specific hallmarks of undecidability in the above examples: Suppose we have a collection of input instances $I_0, I_1, \ldots$ and a decision problem P. We ask: is there a mechanical procedure to decide P on input I_n?

Let us suppose further that—just as with every example in this article—our problem is *semi-decidable*; that is, there's a procedure that can decide in finite time at least if the answer is `Yes`, but no procedure can answer in every instance that the answer is `No` (or, depending on which way round our problem is phrased, *vice versa*).

But even if we can decide in some instances, how long does this take? Fix some model of computation—Turing machines, Minsky register machines, a Java or Fractran program, or any of the universal examples in this article—and some method of counting how many steps a given calculation takes. Then for any procedure for deciding P when we can, let us define $f(n)$ to be the minimum possible time it takes to find an answer, if we can find an answer, and set $f(n) = 0$ if we cannot.

It doesn't matter, really, how you do this. We have the remarkable:

Lemma: *The function f cannot be bounded by any computable function!*

Computable functions are simply those with some explicit description of how to calculate their values on the counting numbers: n, 2^n, n^n are all computable, and it is amusing to invent outrageous computable functions that defy imagination.[12] Yet f beats all!

It's not hard to see how. Suppose f were bounded by some function g whose values we could compute. Then given n, compute $g(n)$, and then try to decide our problem P on input I_n; if we try for $g(n)$ steps and have not yet succeeded, we know we never will, and the answer must be `No`. But we know there can be no procedure that can always decide P and so no g can exist!

We snuck in an important point: this holds for *any* model of computation, and this article gives several. We can reinterpret this lemma in many, somewhat startling ways, such as:

- *Let* $H(n)$ *be the maximum Heesch number attained by any set of n tiles; then* $H(n)$ *cannot be bounded by any computable function.*
- *Among Fractran programs with n fractions that eventually halt, let* $F(n)$ *be the maximum number of steps required to do so; then* $F(n)$ *cannot be bounded by any computable function.*
- *Let* $P(n, m)$ *be the maximum length minimal solution of an instance of the Post Correspondence Problem of width m and n rules; then* $P(n, m)$ *cannot be bounded by any computable function.*

For Turing machines, let $S(m, n)$ be the maximum number of steps an m-state machine on an alphabet of n letters can run, starting on a blank tape, before halting; this, too, of course, cannot be bounded by any computable function,

[11] *Many people presume the same; Wolfram, for example, states something similar as his* Principle of Computational Equivalence.

[12] *For example, on the natural numbers, define* $u(a, b, n) = a$, *for* $b = 1$; $u(a, b, n) = a^b$ *for* $n = 1$; *and* $u(a, b, n) = u(a, u(a, b-1, n), n-1)$ *otherwise (thus* $u(a, b, n) = a \uparrow \ldots \uparrow b$ *with n* $\uparrow$*'s in the Knuth arrow notation). Then set* $v(1) = u(3, 3, 4)$ *and take* $v(n) = u(3, 3, v(n-1))$ *for* $n > 1$. *The value* $v(64)$ *is the famous Graham's Number! But we can consider such marvels as* $V(n)$ *equal to v composed with itself* $V(n-1)$ *times and other gems, playing this game all day, producing utterly incomprehensible but computable functions.*

and staggering lower bounds on S are actively being discovered: A few notable examples are shown in the next table [27].

In a span of just a few months in the winter of 2007–2008, T. and S. Ligocki produced a flurry of examples bounding $S(3,3) \geq 119,112,334,170,342,540$; $S(2,5) > 1.9 \times 10^{704}$; $S(2,6) > 2.4 \times 10^{9866}$; and $S(3,4) > 5.2 \times 10^{13036}$. There is no reason to believe that the true values of S are not much, much higher.

ϕ	A	B	C	D	E
0	1RB	1RC	1RD	1LA	1RH
1	1LC	1RB	0LE	1LD	0LA

Halts in 47,176,870 steps!
(Marxen, Buntrock, 1990)

ϕ	A	B	C	D	E	F
0	1RB	1LC	1LD	1LE	1LA	1LE
1	0LE	0RA	0RC	0LF	1LC	1RH

Halts after more than 2.584×10^{2869} steps!!
(T. and S. Ligocki, 2007)

How Hard Are These Examples to Understand?

Examining specific instances of a specific undecidable problem, we see more and more outrageous behavior, leaping upward with no computable bound. But that is hardly the worst of it. How difficult will it be to *prove* that these instances are as bad as we claim they are?

Again, fix some model of computation; we've seen plenty in this article and any model will do, but for the sake of familiarity, imagine programming in some structured computer language such as C or Java.

Fix any consistent "reasonable" formal system, one that has a "reasonable" language and a "reasonable" concept of theorem and is "reasonably" powerful. An elementary, very broad discussion of these terms can be found in a lovely paper by A. Charlesworth [5], but in essence all we mean is that we can mechanically check that a given string of symbols is a statement in the system, that any statement or its negation (but not both) is to be true, that we can mechanically enumerate all possible proofs and check the soundness of any proof in the system, and that the system is powerful enough to prove such statements as *Program P halts after 100 steps* and *Program P halts eventually*. (Such statements are really just statements about basic arithmetic: for example, at each step of the run of a program on an electronic computer, we are just manipulating a gigantic binary number by simple rules of arithmetic, and we're only asking for a demonstration that we can make such a manipulation a finite number of times and then reach some desired result.)

But we can ask: What is the *shortest possible* proof of such an assertion, that is, what is the *proof complexity* $\pi(T)$ of each given theorem T in our system? Defining $\pi(n)$ to be the maximum proof complexity among all theorems of length n, we have the disturbing:

Lemma: *The function π cannot be bounded by any computable function!*

That is, in any reasonable formal system, we expect short theorems with incredibly long proofs! This is really just a restatement of the lemma in the previous section, which in turn is a disguised form of the Halting Problem:

For any given specific program P, one of the two statements *Program P eventually halts* or *Program P does not ever halt* must be true. Let n be the length in our formal system of the first statement, and suppose $\pi(n)$ is bounded by some computable function $g(n)$. Then we can decide which of the two statements is true: Calculate $g(n)$ and then enumerate all proofs up to this length, checking to see if we've ever managed to prove the first statement. If at some point we have, we know the first statement is true. If we haven't, we never will, and so the second statement is true. In either case we will have decided which statement holds, but then as the Halting Problem is undecidable, there can be no such g.[13]

But as before, this can be reinterpreted within any of the various models of computation we've discussed in this article. For example:

- *Mechanically enumerate all sets of tiles; let H_n be the nth set that does not admit a tiling; there is a proof that it doesn't, as discussed at the end of the section Undecidable Tiling Problems. Let $h(n)$ be the length of the* shortest *proof of this in our formal system. Then $h(n)$ cannot be bounded by any computable function!*
- *Mechanically enumerate Fractran programs; let F_n be the nth set that eventually halts. We can prove this by simply running the program; let $f(n)$ be the length of the shortest proof of this in our formal system. Then $f(n)$ cannot be bounded by any computable function!*
- *Mechanically enumerate instances of the Post Correspondence Problem; let P_n be the nth set that has a solution and let $p(n)$ be the length of the shortest proof that it does. Then $p(n)$ cannot be bounded by any computable function!*

That's just fun and games, but remember: these examples are stand-ins for a huge range of similarly computationally universal problems—this sort of

[13] *Kleene* [5, 19] *uses this approach to prove Gödel's Theorem: If, in our consistent, reasonable formal system, every* true *statement had a proof, then we can decide the Halting Problem: given a procedure P, just start enumerating proofs until we reach a proof of one of our two statements!*

trouble is everywhere. This raises an essential issue:

To What Extent Are the Ideas in This Essay Mathematical?

Don't misunderstand me—beyond a doubt, it is all mathematics: Everything here can be proven to the usual acceptable standards. The theory of computation, with its foundational ties to the underpinnings of logic itself, is as mathematical a subject as can be, with an abundance of beautiful and elegant proofs and constructions. And it's lovely that such simple ideas are sufficient to pin down some of the metamathematics, such as the asymptotic complexity of proofs. In this essay, we've only scratched the surface of this deep and beautiful topic, and we hope we have encouraged some readers to learn much more.

What of proofs that specific settings are computationally universal, or that specific problems are undecidable? Often these can be quite clever and appealing. It is certainly useful to know that certain problems—at least the especially important or natural ones—will forever be beyond full mathematical analysis (the word problem for groups comes to mind).

But what of studying individual instances within a universal setting, looking at the specific growth of the functions discussed a moment ago, finding more and more outrageous examples of Busy Beaver Turing machine candidates or high Heesch number sets of tiles? To what extent are *these* examples mathematical?

I confess delight in each of these examples—it's absolutely mesmerizing to see them in action. But not only do they leave one unsatisfied, with little means of penetrating just *why* these particular examples—but not others!—behave as they do, but also we can *prove* that we can *never* expect to understand why these, particularly, are just so.[14] That is, though there is some "reason" they are as they are, in the form of an astoundingly long proof, there cannot be any "good reason" or understandable short proof.

In a human sense, mathematics—just as is science—is fundamentally reductionist. Good mathematics synthesizes the disparate behavior seen in a wide range of examples into sweeping understanding. Mathematics, even difficult, highly technical mathematics, simplifies and unifies: It is no accident that we speak of "elegance" or of "proofs in The Book". Studying individual instances within undecidable problems, at least asymptotically, cannot be mathematical in this sense: no unified understanding will be available, whatever "proofs" there are giving no insight.

And yet we are surrounded! Such problems arise everywhere there is suitable combinatorial structure—and the bar is really quite low. These issues are likely to be increasingly hard to avoid as complexity and algorithms become more common tools within certain mathematical disciplines. And as many mathematicians begin to use computational experiments in their work, it is a natural temptation to explore increasingly intractable cases. In the sciences, too, "emergent" phenomena are increasingly studied, phenomena of precisely this sort in which small agents interact by combinatorial rules producing complex, large-scale structure. Mathematical or not, these systems are relevant, abundant, and worth studying: It certainly seems wise to have some sense of where lies the edge of the abyss!

[14] *Theology has not had a respectable place in the mathematics literature for many centuries; however, we cannot resist pointing out a fundamental blasphemy inherent in the doctrine of "Intelligent Design" so fashionable in certain quarters: The word "design", in a common sense, implies having some guiding principles, a simplified means of understanding the implications of choosing one set of conditions versus another. Within these computationally universal systems, by the arguments in this section,* no general design principles can exist. *That is, there is no simpler way to understand these implications than, well, just following them out. Now of course it would be foolish to presume just how an omnipotent deity would go about setting up a universe, life, etc. But to insist, as proponents of Intelligent Design do, that a deity* must *go about things in the most difficult, least powerful manner seems like a very limiting theology, to say the least.*

References

[1] S. I. Adian and V. G. Durnev, Decision problems for groups and semigroups, *Russian Math. Surveys* **55** (2000), 207–296.

[2] R. Berger, The undecidability of the Domino Problem, *Memoirs Amer. Math. Soc.* **66** (1966).

[3] C. Baiocchi, Three small universal Turing machines, *Machines, Computations, and Universality*, (M. Margenstern and Yu. Rogozhin, eds.), Springer-Verlag, 2001, pp. 1–10.

[4] E. Börger, E. Grädel, and Yu. Gurevich, *The Classical Decision Problem*, Springer, 2001.

[5] A. Charlesworth, A proof of Gödel's Theorem in terms of computer programs, *Math. Mag.* **54** (1981), 109–121.

[6] J. Cocke and M. L. Minsky, Universality of tag systems with $P = 2$, *J. Assoc. Comput. Mach.* **11** (1964), 15–20.

[7] J. H. Conway, Fractran: A Simple Universal Programming Language for Arithmetic, Ch. 2 in *Open Problems in Communication and Computation* (T. M. Cover and B. Gopinath, eds.), Springer-Verlag, 1987, pp. 4–26.

[8] M. Cook, Universality in elementary cellular automata, *Complex Systems* **15** (2004), 1–40.

[9] S. Cook, The complexity of theorem proving procedures, *Proc. of the Third Annual ACM Symp. on Thy. of Computing*, 1971, 151–158.

[10] L. De Mol, Tag systems and Collatz-like functions, *Theor. Comp. Sci.* **390** (2008), 92–101.

[11] A. K. Dewdney, *The Tinkertoy Computer and Other Machinations: Computer Recreations from the Pages of* Scientific American *and* Algorithm, W. H. Freeman & Company, New York, 1993.

[12] E. Fredkin and T. Toffoli, Conservative Logic, *Int. J. Theor. Phys.* **21** (1982), 219–253.

[13] M. Gardner, The fantastic combinations of John Conway's new solitaire game "Life", *Scientific American* **223** (1971), 120–123.

[14] ______, Extraordinary nonperiodic tiling that enriches the theory of tilings, *Scientific American* **236** (1977), 110–121.

[15] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, W. H. Freeman and Co., New York, 1979.

[16] B. Grünbaum and G. C. Shepherd, *Tilings and Patterns*, W. H. Freeman and Co., 1987.

[17] V. Halava, T. Harjua, M. Hirvensaloa, and J. Karhumäki, Post Correspondence Problem for short words, *Info. Proc. Let.* **108**, 115–118.

[18] D. Hofstader, *Gödel, Escher, Bach: An Eternal Golden Braid*, Vintage, 1980.

[19] S. C. Kleene, Recursive predicates and quantifiers, *Trans. Amer. Math. Soc.* **53** (1943), 41–73.

[20] J. Lagarius, *The* $3x + 1$ *Problem: An Annotated Bibliography (1963–1999)*, arXiv:math 0309224v11.

[21] ______, *The* $3x + 1$ *Problem: An Annotated Bibliography, II (2000–)*, arXiv:math/0608208v4.

[22] C. Mann, Heesch's tiling problem, *Amer. Math. Monthly* **111** (2004), 509–517.

[23] ______, *The Edge-Marked Polyform Database.* `http://www.math.uttyler.edu/polyformDB/`

[24] M. Margenstern, Frontier between decidability and undecidability: A survey, *Theor. Comp. Sci.* **231** (2000), 217–251.

[25] P. Michel and M. Margenstern, *Generalized* $3x+1$ *functions and the theory of computation*, preprint.

[26] Yu. V. Matiyasevich, Simple examples of undecidable associative calculi, *Dokl. Akad. Nauk SSSR* **173** (1967), 1264–1266; English transl., *Soviet Math. Dokl.* **8** (1967), 555–557.

[27] P. Michel, *Historical Survey of Busy Beavers*, `http://www.logique.jussieu.fr/~michel/ha.html`

[28] M. L. Minsky, Recursive unsolvability of Post's Problem of 'tag' and other topics in the theory of Turing machines, *Ann. of Math.* **74** (1961), 437–455.

[29] ______, *Computation: Finite and Infinite Machines*, Prentice Hall, Englewood Cliffs, 1967.

[30] J. Myers, *Polyomino, polyhex and polyiamond tiling*, `http://www.srcf.ucam.org/~jsm28/tiling/`

[31] F. Nicolas, *Post Correspondence Problem and semi-Thue systems*, lecture notes, arXiv:0802.0726v5.

[32] T. Oliveira e Silva, *Computational verification of the* $3x + 1$ *conjecture*, `http://www.ieeta.pt/~tos/3x+1.html`

[33] E. Post, Formal reductions of the combinatorial decision problem, *Amer. J. Math.* **65** (1943), 197–215.

[34] M. Rahn, *Entsheidbare Fälle des Postschen Korrenspondenzproblems*, doctoral thesis, Universität Fridericiana zu Karlsruhe (2008).

[35] D. Richardson, Some undecidable problems involving elementary functions of a real variable, *J. of Symb. Logic* **33** (1968), 514–520.

[36] R. M. Robinson, Undecidability and nonperiodicity of tilings in the plane, *Inv. Math.* **12** (1971), 177–209.

[37] Yu. V. Rogozhin, Small universal Turing machines, *Theor. Comp. Sci.* **168** (1996), 215–240.

[38] D. Scott, A short recursively unsolvable problem (abstract), *J. Symbolic Logic* **21** (1956), 111–112.

[39] M. Sipser, *Introduction to the Theory of Computation, 2nd ed.*, Course Technology, 2005.

[40] R. Smullyan, *The Lady or the Tiger?: And Other Logic Puzzles Including a Mathematical Novel that Features Gödel's Great Discovery*, Random House, 1992.

[41] H. Stamer, `PCP@HOME`, `http://www.theory.informatik.uni-kassel.de/~stamer/pcp/pcpcontest_en.html`

[42] G. S. Tseitin, Associative calculus with insoluble equivalence problem, *Dokl. Akad. Nauk SSSR* **107** (1956), 370–371. (Russian)

[43] A. Turing, On computable numbers, with an application to the Entscheidungsproblem, *Proc. London Math. Soc. Ser. 2* **42** (1936), 230–265.

[44] H. Wang, Proving theorems by pattern recognition. II, *Bell System Technical Journal* **40** (1961), 1–42.

[45] S. Wolfram, *New Kind of Science*, Wolfram Media, 2002.

[46] *Wolfram's 2-state 3-symbol Turing machine*, talk page, Wikipedia.

[47] D. Woods and T. Neary, On the time complexity of 2-tag systems and small universal Turing machines, *Proc. of the 46th Symp. on Found. Comp. Sci.*, 2006, 439–446.

The Brave New World of Bodacious Assumptions in Cryptography

Neal Koblitz and Alfred Menezes

There is a lot at stake in public-key cryptography. It is, after all, a crucial component in efforts to reduce identity theft, online fraud, and other forms of cybercrime. Traditionally, the security of a public-key system rests upon the assumed difficulty of a certain mathematical problem. Hence, newcomers to the field would logically expect that the problems that are used in security proofs come from a small set of extensively studied, natural problems. But they are in for an unpleasant surprise. What they encounter instead is a menagerie of ornate and bizarre mathematical problems whose presumed intractability is a basic assumption in the theorems about the security of many of the cryptographic protocols that have been proposed in the literature.

What Does Security Mean?

Suppose that someone is using public-key cryptography to encrypt credit card numbers during online purchases, sign a message digitally, or verify the route that a set of data followed in going from the source to her computer. How can she be sure that the system is secure? What type of evidence would convince her that a malicious adversary could not somehow compromise the security of the system?

At first glance it seems that this question has a straightforward answer. At the heart of any public-key cryptosystem is a *one-way function*—a function $y = f(x)$ that is easy to evaluate but for which it is computationally infeasible (one hopes) to find the inverse $x = f^{-1}(y)$. The two most important examples of such functions are the following:

- The Rivest-Shamir-Adleman (RSA) type of cryptography [28] is based on the assumed intractability of inverting the function $(p, q) \mapsto N = pq$, where (p, q) is a pair of randomly generated primes of roughly the same magnitude. The task of inverting this function is the famous integer factorization problem (the most difficult cases of which are believed to have the form $N = pq$ of an RSA modulus).
- Elliptic curve cryptography (ECC) is based on the assumed difficulty of inverting the function $x \mapsto xP$, where P is a point of large prime order p on an elliptic curve E defined over the field $\mathbb{F}_q$ of q elements and x is an integer mod p. The task of inverting this function is the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Indeed, a large proportion of all of the mathematical research in public-key cryptography is concerned with algorithms for inverting the most important one-way functions. Hundreds of papers in mathematics as well as cryptography journals have been devoted to index calculus methods for factoring integers, to improved Pollard-ρ algorithms [33] and Weil descent methods [18] for finding discrete logarithms on elliptic curves, and to searches for weak parameters, i.e., RSA moduli N that are a little easier to factor than most, finite fields over which the ECDLP is slightly easier to solve, and so on. Traditionally, many mathematicians working in cryptography have tended to regard the question of security of a type of public-key system as equivalent to hardness of inverting the underlying one-way function.

Neal Koblitz is professor of mathematics at the University of Washington, Seattle. His email address is koblitz@math.washington.edu.

Alfred Menezes is professor of combinatorics and optimization at the University of Waterloo. His email address is ajmeneze@uwaterloo.ca.

However, this answer to the security question is woefully inadequate. In the first place, the implication goes only one way: if the underlying problem is efficiently solvable, then the system is insecure; but if it is intractable, the system is not necessarily secure. In other words, intractability is a necessary but not sufficient condition.

In the case of RSA, for example, the encryption function is exponentiation modulo N: $C = P^e \bmod N$, where e is a fixed integer prime to $\phi(N) = (p-1)(q-1)$, P is a block of plaintext (regarded as an integer less than N), and C is the scrambled text, called *ciphertext*. The decryption function $P = C^d \bmod N$ (where d is an inverse of the exponent e modulo $\phi(N)$) can be computed if one knows the factorization of N. But it has never been proved that knowledge of that factorization is *necessary* in order to decrypt. In fact, in a paper titled "Breaking RSA may not be equivalent to factoring" [12], Boneh and Venkatesan gave evidence that the above e-th root problem modulo N might be strictly easier than factoring N.

Moreover, there might be indirect ways to exploit the particular implementation of RSA that in certain cases would allow someone (Cynthia) other than the intended recipient (Alice) to learn the secret plaintext. For example,

- Suppose that Alice is receiving messages that have been encrypted using RSA; her public key is (N, e). Cynthia, after intercepting the ciphertext C that her competitor Bob sent to Alice, wants to know the plaintext P (let's say it was his bid on a job). If Cynthia asks Alice for P directly, Alice won't tell her Bob's bid, because it's against Alice's interests for Cynthia to know that. But suppose that awhile back, before Bob muscled in on her territory, Cynthia had extensive correspondence with Alice, and she now sends a message to Alice saying (falsely) that she lost one of her messages to Alice, she needs it for her records, and all she has is the ciphertext C'. Alice's computer willingly decrypts C' for Cynthia and sends her $P' = C'^d \bmod N$. But in reality Cynthia formed C' by choosing a random R and setting $C' = CR^e \bmod N$. After Alice is tricked into sending her P', all Cynthia has to do is divide it by R modulo N in order to learn P. This is called a *chosen-ciphertext attack.*

More precisely, in such an attack the adversary is assumed to be able to get Alice to decipher any ciphertext C' she wants other than the target ciphertext C. The system is said to have *chosen-ciphertext security* if knowledge of all those other plaintexts P' will not enable Cynthia to decrypt C.

In RSA the simplest way to prevent a chosen-ciphertext attack is to "pad" a message with a block of random bits before encryption (see, for example, [3]); then when Alice reveals only the subset of bits of P' that are in the message part of C'^d, Cynthia is stymied.

- Again suppose that Alice is receiving messages that have been encrypted using RSA. The plaintext messages have to adhere to a certain format, and if a decrypted message is not in that form, Alice's computer transmits an error message to the sender. This seems innocuous enough. However, Bleichenbacher [5] showed that the error messages sometimes might compromise security.

Bleichenbacher's idea can be illustrated if we consider a simplified version of the form of RSA that he attacked in [5]. Suppose that we are using RSA with a 1024-bit modulus N to send a 128-bit secret key m (for use in symmetric encryption). We decide to pad m by putting a random number r in front of it, but since this doesn't take up the full 1024 bits, we just fill in zero-bits to the left of r and m. When Alice receives our ciphertext, she decrypts it, checks that it has the right form with zero-bits at the left end—if not, she informs us that there was an error and asks us to resend—and then deletes the zero-bits and r to obtain m. In that case Bleichenbacher can break the system—in the sense of finding the plaintext message—by sending a series of carefully chosen ciphertexts (certain "perturbations" of the ciphertext he wants to decipher) and keeping a record of which ones are rejected because their e-th root modulo N is not of the proper form; that is, does not have the prescribed number of zero-bits.

Notice that the particular way that RSA is being used plays a crucial role. Thus, when discussing security, one must specify not only the type of cryptography and choice of parameters but also the instructions that will be followed. The sequence of steps the users of the system go through is called a *protocol.* A protocol description might take the form, "First Alice sends Bob the elements…; then Bob responds with…; then Alice answers with…; and so on."

Also notice that both of the above types of attacks can be avoided if a protocol is used that has chosen-ciphertext security, that is, if it can withstand a chosen-ciphertext attack. Ideally, what this means is that there is an efficient reduction from $\mathcal{P}$ to $\mathcal{Q}$, where $\mathcal{Q}$ is the problem of making a successful chosen-ciphertext attack and $\mathcal{P}$ is a mathematical problem (such as integer factorization) that is widely believed to be very difficult (provided that one chooses the parameters suitably). Such a reduction implies that $\mathcal{Q}$ is at least as hard as $\mathcal{P}$. What a "security proof"—or, as we prefer to say, a *reductionist security argument* [23]—does is show that an adversary cannot succeed in mounting a certain category of attack unless a certain underlying mathematical problem is tractable.

Rabin-Williams

In 1979 Rabin [27] proposed an encryption function that could be *proved* to be invertible only by someone who could factor N. His system is similar to RSA, except that the exponent is 2 rather than an integer e prime to $\varphi(N)$. For N a product of two primes the squaring map is 4-to-1 rather than 1-to-1 on the residues modulo N, so Rabin finds all four square roots of a ciphertext C (and in practice chooses the plaintext that makes sense to the message recipient).

Reductionist Security Claim. Someone who can find messages P from the ciphertext C must also be able to factor N.

Argument. Informally, the reason is that finding P means being able to find all four square roots of C, because any one of them could be the true plaintext P. Those square roots are $\pm P$ and $\pm\epsilon P$, where ϵ is a residue mod N that is $\equiv 1 \pmod{p}$ and $\equiv -1 \pmod{q}$. That means that someone who can find messages must know the value of ϵ, in which case N can be factored quickly using the Euclidean algorithm, since $\gcd(N, \epsilon - 1) = p$.

A more formal reduction would go as follows. We suppose that there exists an adversary that takes N and C as input and produces one of the square roots of C modulo N. We think of the adversary as a computer program, and we show how someone (Cynthia) who has that program could use it to quickly factor N.

What Cynthia does is the following. She chooses a random residue x, sets $C = x^2 \bmod N$, and inputs that value of C to the adversary. The adversary outputs a square root P of C mod N. With probability 1/2 the root P is $\pm\epsilon x$, and in that case Cynthia can immediately compute $\epsilon = \pm x/P$ and then factor N. If, on the other hand, $P = \pm x$, then the value of P won't help her factor N, and she tries again, starting with a new value of x. There is only a $1/2^k$ chance that she will fail to factor N in k or fewer tries. We say that this argument reduces factoring N to breaking Rabin encryption mod N (where "breaking" means recovering plaintext messages). Rabin's scheme was the first public-key system to be proposed that was accompanied with a reductionist security argument. Users of Rabin encryption could be certain that no one could recover plaintexts unless they knew the factorization of N.

Soon after Rabin proposed his encryption scheme, Rivest pointed out that, ironically, the very feature that gives it an extra measure of security would also lead to total collapse if it were confronted with a chosen-ciphertext attacker. Namely, suppose that the adversary could somehow fool Alice into decrypting a ciphertext of its own choosing. The adversary could then follow the same procedure that Cynthia used in the previous paragraph to factor N. An adversary who could trick Alice into deciphering k chosen ciphertexts would have a $1 - 2^{-k}$ probability of factoring N.

However, at about the same time that Rivest made this observation, Williams [34] developed a variant in which the mapping is 1-to-1 that is especially useful for digital signatures. The resulting Rabin-Williams signature scheme appears to have significant efficiency and security advantages over traditional RSA. Recently, Bernstein [4] was able to show that even without random padding of messages, Rabin-Williams signatures are safe from chosen-message attack unless the adversary can factor N.[1] Unlike many proofs of security in the literature, Bernstein's paper is well written, logical, and lucid. In fact, after reading it, the obvious reaction is to ask: Why doesn't everyone switch to Rabin-Williams signatures?

In the real world, however, it is too late for that. Because of progress in factoring, for the highest security it is now recommended that 15360-bit N be used for any factorization-based cryptosystem. Meanwhile, the very highest security level with ECC requires q of 571 bits. Thus, users of RSA who are willing to change their software to accommodate a different system are going to switch to ECC, not to Rabin-Williams. If [4] had been published twenty years earlier, the history of digital signatures might have been very different.

The neglect of exponent 2 in RSA is a typical example of how historical happenstance and sociological factors, rather than intrinsic technical merit, can often determine what technology is widely used (see [22] for more discussion of this phenomenon).

The One-More-Discrete-Log Problem

Just as integer factorization is not exactly the problem one has to solve to invert the RSA encryption function, similarly, in systems using elliptic curves and other algebraic groups, the discrete log problem (DLP) is not the problem that is most immediately related to the task of the adversary Cynthia. Take, for example, the simplest ECC protocol, namely, the basic Diffie-Hellman key exchange [17] between two users, Alice and Bob. Let $\mathbb{G}$ be the group that is generated by a point $P \in E(\mathbb{F}_q)$ of prime order p. Suppose that Alice's public key is $Q_A = xP$ and her secret key is the integer x mod p; and Bob's public key is $Q_B = yP$ and his secret key is y. Then the shared key is simply xyP, which Alice computes as xQ_B and Bob as yQ_A.

[1] *Resistance to chosen-message attacks, in which the adversary can obtain signatures of messages of her choice and then has to sign a different message, is the commonly accepted standard of security of digital signatures; it is closely analogous to chosen-ciphertext security for encryption.*

The task of Cynthia, who knows P, xP, and yP, but neither of the secret keys, is to determine xyP from that triple of points. This is called the Diffie-Hellman Problem (DHP) in the group $\mathbb{G}$. Someone who can find discrete logs in $\mathbb{G}$ can obviously solve the DHP. The converse is a much more difficult question. However, in contrast to the situation with RSA, where there is doubt about the equivalence of the e-th root problem mod N and integer factorization, in ECC there is considerable evidence that the DHP and the DLP are of equivalent difficulty. The results showing this equivalence in many cases are surveyed in [25].

Because of the nature of chosen-ciphertext (or chosen-message) security and because many cryptographers want to have formal reduction arguments, they have had to greatly enlarge the types of mathematical problems that are used in their security analyses. Often the problems whose intractability is linked to the security of the protocols have lengthy, elaborate input or are interactive. In an interactive problem the solver is permitted to request additional information by making a bounded number of queries to an *oracle,* that is, a black box whose only function is to give correct answers to a certain type of question. On occasion, an interactive problem or one with input and output that appear unnatural might be used carefully and to good effect (see, for example, [15]). But in other cases the use of this type of problem raises more questions than it answers about the true security of the protocol.

Here are some examples of such problems that arose in connection with protocols that use elliptic curves or other algebraic groups:

- *The One-More-Discrete-Log Problem (1MDLP)* as first formulated in [1] and [2]. The solver is supplied with a challenge oracle that produces a random group element $Y_i \in \mathbb{G}$ when queried and a discrete log oracle. After ℓ queries to the challenge oracle (where ℓ is chosen by the solver) and at most $\ell - 1$ queries to the discrete log oracle, the solver must find the discrete logs of all ℓ elements Y_i.
- *The One-More-Diffie-Hellman Problem (1MDHP)* as first formulated (in a slightly different version) in [6]. The solver is given an element $X \in \mathbb{G}$, an oracle that can solve the Diffie-Hellman problem for the given X and arbitrary $Y \in \mathbb{G}$, and a challenge oracle that produces random group elements Y_i. After ℓ queries to the challenge oracle (where ℓ is chosen by the solver) and at most $\ell - 1$ queries to the Diffie-Hellman oracle, the solver must find all ℓ solutions $Z_i = xy_iP$ (where $X = xP$ and $Y_i = y_iP$).

At first it might seem that these problems should be equivalent in difficulty to the problem of finding the discrete log of a single random element or finding the Diffie-Hellman element Z for fixed X and a single random Y. However, it turns out that this depends very much on what groups are used. In [24] we studied these problems and several others in the setting of the jacobian group of a genus-g curve. Assuming that one uses current state-of-the-art algorithms, we found that 1MDLP is harder than 1MDHP for $g = 1, 2$, whereas it is strictly easier than 1MDHP for $g \geq 4$; the two problems are of roughly equal difficulty for $g = 3$; and it is only for nonhyperelliptic curves of genus 3 that the two problems are no easier than the DLP and DHP. Our conclusion is that it is often unclear how to gauge the true level of difficulty of an interactive problem or one with complicated input.

Reduction Theorems That Do Not Say Much

Suppose that the designers of a cryptographic protocol claim to have proved its security by constructing a reduction from $\mathcal{P}$ to $\mathcal{Q}$, where $\mathcal{Q}$ is the problem of mounting a successful attack (of a prescribed type) on the protocol and $\mathcal{P}$ is a mathematical problem that they believe to be intractable. Often a close examination of the two problems $\mathcal{P}$ and $\mathcal{Q}$ will show that they are trivially equivalent, in which case the theorem that supposedly establishes security is really assuming what one wants to prove. In that case the problem $\mathcal{P}$ has been tailored to make the proof work, and, in fact, the main difference between $\mathcal{P}$ and $\mathcal{Q}$ is simply that in the former the extraneous elements and cryptographic terminology have been removed.

For example, in most signature schemes the actual messages being signed are extraneous to an analysis of the scheme, because the first thing one does to a message is to compute its hash-function value (fingerprint), which is used instead of the message itself in all subsequent steps. If the security theorem is assuming that the hash-values are indistinguishable from random numbers—in which case one says that the proof is in the random-oracle model—then the set of messages can be replaced by a set of random numbers. If $\mathcal{P}$ has been constructed by removing this sort of irrelevant feature from $\mathcal{Q}$, then the equivalence of the two problems will be a tautology, and the reduction theorem does not provide any meaningful assurance that the protocol is secure.

Even if the reduction from $\mathcal{P}$ to $\mathcal{Q}$ is not trivial, one has to wonder about the value of the theorem whenever $\mathcal{P}$ is complicated and contrived. One should be especially skeptical if the protocol designers refer to $\mathcal{P}$ as a "standard" problem, because there is a long history of misleading uses of the word "standard" in cryptography. For example, a proof of security that uses weaker assumptions about the hash function than the random-oracle assumption (see above) is commonly said to be a proof in the standard model. The reader might not notice that, in order to work in the standard rather than the random-oracle model, the authors had to invent a new nonstandard problem.

There is another questionable use of the word "standard" that is frequently encountered in the literature. After a complicated interactive problem $\mathcal{P}$ has been used in a couple of papers, subsequent papers refer to it as a standard problem. The casual reader is likely to think that something that is standard has withstood the test of time and that there's a consensus among researchers that the assumption or problem is a reasonable one to rely upon—although neither conclusion is warranted in such cases. The terminology obfuscates the fact that the new problem is highly nonstandard.

Pairing-Based Cryptography

Starting in 2001, pairing-based cryptosystems were proposed by Dan Boneh, Matt Franklin, and others. Although some of the ideas had been around for a couple of years (see, for example, [21, 29]), their tremendous potential had not been realized before.

The basic idea is that the Weil or Tate pairing on elliptic curves allows certain cryptographic goals to be achieved that no one knows how to achieve with conventional techniques. In some other cases, pairings give more efficient or conceptually simpler solutions.

Let

$$e: \mathbb{G} \times \mathbb{G} \longrightarrow \mu_p \subset \mathbb{F}_{q^k}$$

be a nondegenerate bilinear pairing on the group $\mathbb{G} \subset E(\mathbb{F}_q)$ generated by a point P of prime order p with values in the p-th roots of unity of the degree-k extension of $\mathbb{F}_q$, where k (called the *embedding degree*) is the smallest positive integer such that $p|q^k - 1$. The feasibility of computing pairings depends on how big k is. For example, if $\mathbb{F}_q$ is a prime field and E has $q + 1$ points (such a curve is called *supersingular*), then since $p|q + 1$ and $q + 1|q^2 - 1$, the embedding degree is $k = 2$, and pairings can be computed quickly.

One of the first uses of pairing-based cryptography was the elegant solution by Boneh and Franklin [10] to an old question of Shamir [30], who had asked whether an efficient encryption scheme could be devised in which a user's public key would be just her identity (e.g., her email address). Such a system is called *identity-based encryption*. Another early application (see [11]) was to obtain short signatures.

By the time pairing-based cryptography arose, it had become *de rigueur* when proposing a cryptographic protocol always to give a "proof of security", that is, a reduction from a supposedly intractable mathematical problem $\mathcal{P}$ to a successful attack (of a specified type) on the protocol. A peculiar feature of many pairing-based cryptosystems is that $\mathcal{P}$ has often been very contrived—the sort of problem that hardly any mathematician would recognize as natural, let alone want to study. Nevertheless, it has become customary to regard a conditional result of the form "if $\mathcal{P}$ is hard, then my protocol is safe from chosen-ciphertext attacks" as a type of guarantee of security.

The Strong Diffie-Hellman Problem

In [8, 9], Boneh and Boyen proposed a new digital signature that works as follows. As before, let $\mathbb{G}$ be the group generated by a point $P \in E(\mathbb{F}_q)$ of prime order p, and let $e: \mathbb{G} \times \mathbb{G} \longrightarrow \mu_p$ be a nondegenerate bilinear pairing with values in the p-th roots of unity in a (not too big) field extension of $\mathbb{F}_q$.

In the Boneh-Boyen protocol, to sign a message m, which is regarded as an integer mod p, Alice uses her secret key (x, y), which is a pair of integers mod p. Her public key, which the recipient (Bob) will use to verify her signature, consists of the two points $X = xP$ and $Y = yP$. Alice picks a random r mod p and sets $Q = (x + yr + m)^{-1}P$ (where the reciprocal of $x + yr + m$ is computed mod p). Her signature consists of the pair (Q, r).

After receiving m and (Q, r), Bob verifies her signature by checking that

$$e(Q, X + rY + mP) = e(P, P);$$

if equality holds, as it should because of the bilinearity of e, he is confident that Alice was truly the signer — that is, only someone who knows the discrete logs of X and Y could have computed the point Q that makes the above equality hold.

Boneh and Boyen give a reductionist security argument that basically shows that a chosen-message attacker cannot forge a signature provided that the following Strong Diffie-Hellman (SDH) problem is hard. This problem is parameterized by an integer ℓ (which is a bound on the number of signature queries the attacker is allowed to make) and is denoted ℓ-SDH:

- The ℓ-SDH problem in the group $\mathbb{G} \subset E(\mathbb{F}_q)$ generated by a point P of prime order p is the problem, given points $P, xP, x^2P, \ldots, x^\ell P$ (where x is an unknown integer mod p), of constructing a pair (c, H) such that $(x + c)H = P$ (where c is an integer mod p and $H \in \mathbb{G}$).

The difficulty of this problem can be shown to be less than or equal to that of the classical Diffie-Hellman problem (which requires the construction of xyP given P, xP, and yP). But the problem is an odd one—the "S" in SDH should really have stood for "strange"—that had never been studied before. It was because of nervousness about the ℓ-SDH assumption that the authors of [8] felt the need to give evidence that it really is hard. What they did was derive an exponential-time lower bound for the amount of time it takes to solve ℓ-SDH in the *generic group model*.

The notion of a generic group in cryptography was first formalized by Nechaev [26] and Shoup [31]. The generic group assumption essentially means that the group has no special properties that could be exploited to help solve the problem. Rather, the only things that a solver can do with group elements are performing the group operation, checking whether two elements are equal, and (in the case of pairing-based cryptography) computing the pairing value for two elements. A lower bound on solving $\mathcal{P}$ in the generic group model means that, in order to solve $\mathcal{P}$ in a specific group such as $E(\mathbb{F}_q)$ in time less than that bound, one would have to somehow exploit special features of the elliptic curve. In [31] Shoup proved that neither the discrete log problem (DLP) nor the Diffie-Hellman problem (DHP) can be solved in fewer than $\sqrt{p}$ steps in a generic group of prime order p.

In §5 of [8] Boneh and Boyen proved that ℓ-SDH in a generic group with a pairing cannot be solved in fewer than (roughly) $\sqrt{p/\ell}$ operations.

Note that this lower bound $\sqrt{p/\ell}$ for the difficulty of ℓ-SDH is weaker by a factor of $\sqrt{\ell}$ than the lower bound $\sqrt{p}$ for the difficulty of the DLP or the DHP in the generic group model. At first it seemed that the factor $\sqrt{\ell}$ was an artifact of the proof and not a cause for concern and that the true difficulty of the ℓ-SDH problem was probably $\sqrt{p}$ as in the case of the DLP and DHP. However, at Eurocrypt 2006 Cheon [16], using the same attack that had been described earlier in a different setting by Brown and Gallant [14], showed that ℓ-SDH can be solved—and in fact the discrete logarithm x can be found—in $\sqrt{p/\ell_0}$ operations if $\ell_0 \le \ell$ divides $p-1$ and $\ell_0 < p^{1/3}$. Thus in some cases ℓ-SDH can be solved in $p^{1/3}$ operations. This means that, to get the same security guarantee (if one can call it that) that signatures based on the DHP have with group order of a certain bitlength, Boneh-Boyen signatures should use a group whose order has 50% greater bitlength. It should also be noted that, even though solving ℓ-SDH does not immediately imply the ability to forge Boneh-Boyen signatures, recently Jao and Yoshida [20] showed how, using the solution to ℓ-SDH in [16], one can forge signatures in roughly $p^{2/5}$ operations (with roughly $p^{1/5}$ signature queries) under certain conditions.

Some of the other supposedly intractable problems that arise in security reductions for pairing-based protocols are even more ornate and contrived than the ℓ-SDH. Several such problems, such as the following Hidden Strong Diffie-Hellman (HSDH), are listed in [13]:

- In ℓ-HSDH one is given $P, xP, yP \in \mathbb{G}$ and $\ell - 1$ triples

$$(w_jP, (x+w_j)^{-1}P, yw_jP), \qquad j = 1, \dots, \ell - 1,$$

and is required to find one more triple of the form $(wP, (x+w)^{-1}P, ywP)$ that is distinct from any of the $\ell - 1$ triples in the problem's input.

When readers encounter the bewildering array of problems whose presumed difficulty is linked to the security of important cryptographic protocols, a common reaction is dismay. However, some people who work in pairing-based cryptography prefer to put a positive spin on the unusual assortment of intractability assumptions. In a paper presented at the Pairing 2008 conference [13], Boyen said:

> The newcomer to this particular branch of cryptography will therefore most likely be astonished by the sheer number, and sometimes creativity, of those assumptions. The contrast with the more traditional branches of algebraic cryptography is quite stark indeed… the much younger "Pairing" branch…is already teeming with dozens of plausible assumptions, whose distinctive features make them uniquely and narrowly suited to specific types of constructions and security reductions.
>
> Far from being a collective whim, this haphazard state of affair [sic] stems from the very power of the bilinear pairing…in comparison to the admittedly quite simpler algebraic structures of twentieth-century public-key cryptography…[T]he new "bilinear" groups offer a much richer palette of cryptographically useful trapdoors than their "unidimensional" counterparts.

Boyen eloquently expresses a youthful optimism about the advantages of twenty-first-century cryptography—with its "rich palette" of exotic intractability assumptions—over the "unidimensional" RSA and ECC that were invented in the 1970s and 1980s. However, some recent experiences with these "plausible assumptions" suggest a need to temper this exuberance.

In the next section we describe a particularly dramatic example of how things can go wrong.

Sequential Aggregate Signatures

In 2007, Boldyreva, Gentry, O'Neill, and Yum [7] constructed a new type of digital signature called an Ordered Multi-Signature (OMS). This means a single compact signature produced by several people acting in sequence. It has fixed length independent of the number of signers—even though the different signers may be attesting to different messages. The main application discussed in [7] is to secure routing of messages through a network.

The authors of [7] describe the advantages of their OMS. In the first place, it is identity-based, i.e., there are no public keys other than the signers' email addresses; this "permits savings on bandwidth and storage…Our OMS construction substantially improves computational efficiency and scalability over any existing scheme with suitable functionality." Moreover, the authors write,

> In contrast to the only prior scheme to provide this functionality, ours offers improved security that does not rely on synchronized clocks or a trusted first signer. We provide formal security definitions and support the proposed scheme with security proofs under appropriate computational assumptions.

That is, the OMS in [7] is not only more efficient but also has "improved security".

The construction in [7] used groups $\mathbb{G}$ with bilinear pairings, and the proof of security assumed that the following Modified Lysyanskaya-Rivest-Sahai-Wolf (M-LRSW) problem is intractable:

- Given a group $\mathbb{G}$ of prime order p, a nondegenerate bilinear pairing $e: \mathbb{G} \times \mathbb{G} \longrightarrow \mu_p$, fixed nonidentity elements $P, U, V \in \mathbb{G}$ that are known to the solver, and fixed exponents a, b mod p with aP and bP but not a or b known to the solver, the M-LRSW problem assumes that the solver is given an oracle that, when queried with an integer m mod p, chooses a random r mod p and gives the solver the triple (X, Y, Z) of elements of $\mathbb{G}$ such that

$$X = mrU + abP, \qquad Y = rV + abP, \qquad Z = rP.$$

The solver must then produce some m' not equal to any of the m that were queried and one more triple (X', Y', Z') such that for some integer x

$$X' = m'xU + abP, \qquad Y' = xV + abP, \qquad Z' = xP.$$

Just as Boneh and Boyen did in [8], the authors of [7] argue that this problem is truly hard by giving an exponential lower bound for the time needed to solve M-LRSW in a generic group. They emphasize that:

> This has become a standard way of building confidence in the hardness of computational problems in groups equipped with bilinear maps.

Just about a year after [7] appeared, Hwang, Lee, and Yung [19] made a startling discovery: the "provably secure" protocol in [7] can very easily be broken, and the supposedly intractable M-LRSW problem can very easily be solved! Here is the fast and simple solution to M-LRSW that they found. Choose any m_1, m_2, and m' that are distinct and nonzero modulo p. Choose β_1, β_2 to be solutions in $\mathbb{F}_p$ to the two relations $\beta_2 = 1 - \beta_1$ and

$$\frac{\beta_1}{m_1} + \frac{\beta_2}{m_2} = \frac{1}{m'}.$$

(The solutions are $\beta_i = \frac{m_i(m_{3-i} - m')}{m'(m_{3-i} - m_i)}$, $i = 1, 2$.) Then make two queries to the oracle with inputs m_1 and m_2; let (X_i, Y_i, Z_i), $i = 1, 2$, denote the oracle's responses, and let r_i, $i = 1, 2$, denote the random r used by the oracle to produce (X_i, Y_i, Z_i). One then easily checks that, for m' the triple

$$X' = m'((\beta_1/m_1)X_1 + (\beta_2/m_2)X_2),$$
$$Y' = \beta_1 Y_1 + \beta_2 Y_2, \; Z' = \beta_1 Z_1 + \beta_2 Z_2$$

(where the coefficients of the X_i are computed in $\mathbb{F}_p$) is a solution of M-LRSW (with $x = \beta_1 r_1 + \beta_2 r_2$). Notice that this algorithm is generic, i.e., it works in any group of order p.

But Theorem 5.1 of [7], which is proved in Appendix D of the full version of the paper, gives an exponential lower bound (essentially of order $\sqrt{p}$) for the time needed to solve M-LRSW. The above Huang-Lee-Yung algorithm shows that Theorem 5.1 is dramatically false.

Oops!

What went wrong? The 4-page single-spaced argument purporting to prove Theorem 5.1 is presented in a style that is distressingly common in the provable security literature, with cumbersome notation and turgid formalism that make it unreadable to nonspecialists (and even to some specialists). To a mathematician reader, Appendix D of [7] does not resemble what we would normally recognize as a proof of a theorem. If one tries to wade through it, one sees that the authors are essentially assuming that all an attacker can do is make queries of the oracle and some rudimentary hit-or-miss computations and wait for two group elements to coincide. They are forgetting that the exponent space is a publicly known prime field and that the attacker is free to do arithmetic in that field and even solve an equation or two.

Conclusion

What are the implications of all this confusion? Should we be worried about the true security of the protocols that are deployed in the real world? Should we cut up our credit cards and stop making online purchases?

No, that's not the conclusion to draw from these examples. In the first place, fallacies found in proofs of security do not necessarily lead to an actual breach. Rather, the flaw in the proof simply means that the advertised guarantee disappears. Similarly, even if we are bewildered and unimpressed by the mathematical problem whose intractability is being assumed in a security proof, we might still have confidence—based on other criteria besides the reductionist proof—that the protocol is secure.

In the second place, cryptographic protocols are not developed and marketed in the real world unless they have been approved by certain industrial-standards bodies. Most cryptosystems proposed in academic papers never get used commercially, and the ones that do have a long lag—sometimes decades—between the initial proposal and actual deployment. Protocols that are based on dubious assumptions or fallacious proofs are not likely to survive this process.

In reality the mathematical sciences have only a limited role to play in evaluating the true security of a cryptographic protocol. Admittedly it is tempting to hype up the centrality of mathematics in cryptography and use cryptographic applications as a marketing tool for mathematics, saying things like: "Number theory can provide the foundation for information security in an electronic world." The first author pleads guilty to having made this statement to an audience of several thousand security specialists at the 2009 RSA Conference. In so doing he violated his own belief that scientists should show self-restraint and refrain from BS-ing[2] the public.

Perhaps the main lesson to learn from the unreliability of so many "proofs of security" of cryptosystems is that mathematicians (and computer scientists) should be a bit more modest about our role in determining whether or not a system can be relied upon. Such an evaluation needs to incorporate many other disciplines and involve people with hands-on experience and not just theoretical knowledge. A discussion of the nonmathematical side of this problem would be out of place in the *AMS Notices*. For the interested reader a good place to start would be the short article [32] by Brian Snow, the Technical Director of Research (now retired) at the U.S. National Security Agency.

References

[1] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko, The one-more-RSA inversion problems and the security of Chaum's blind signature scheme, *J. Cryptology* **16** (2003), pp. 185–215.

[2] M. Bellare and A. Palacio, GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks, *Advances in Cryptology—Crypto 2002*, LNCS 2442, Springer-Verlag, 2002, pp. 149–162.

[3] M. Bellare and P. Rogaway, Optimal asymmetric encryption—how to encrypt with RSA, *Advances in Cryptology—Eurocrypt '94*, LNCS 950, Springer-Verlag, 1994, pp. 92–111.

[4] D. Bernstein, Proving tight security for Rabin-Williams signatures, *Advances in Cryptology—Eurocrypt 2008*, LNCS 4965, Springer-Verlag, 2008, pp. 70–87.

[5] D. Bleichenbacher, A chosen ciphertext attack against protocols based on the RSA encryption standard PKCS #1, *Advances in Cryptology—Crypto '98*, LNCS 1462, Springer-Verlag, 1998, pp. 1–12.

[6] A. Boldyreva, Efficient threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme, *Proc. Public Key Cryptography 2003*, LNCS 2567, Springer-Verlag, 2003, pp. 31–46.

[7] A. Boldyreva, C. Gentry, A. O'Neill, and D. H. Yum, Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing, *Proc. 14th ACM Conference on Computer and Communications Security, CCS 2007*, ACM Press, 2007, pp. 276–285; full version available at `http://eprint.iacr.org/2007/438`.

[8] D. Boneh and X. Boyen, Short signatures without random oracles, *Advances in Cryptology—Eurocrypt 2004*, LNCS 3027, Springer-Verlag, 2004, pp. 56–73.

[9] ———, Short signatures without random oracles and the SDH assumption in bilinear groups, *J. Cryptology* **21** (2008), pp. 149–177.

[10] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *Advances in Cryptology—Crypto 2001*, LNCS 2139, Springer-Verlag, 2001, pp. 213–229; *SIAM J. Computing* **32** (4) (2003), pp. 586–615.

[11] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, *J. Cryptology* **17** (2004), pp. 297–319.

[12] D. Boneh and R. Venkatesan, Breaking RSA may not be equivalent to factoring, *Advances in Cryptology—Eurocrypt '98*, LNCS 1233, Springer-Verlag, 1998, pp. 59–71.

[13] X. Boyen, The uber-assumption family: A unified complexity framework for bilinear groups, *Pairing-Based Cryptography—Pairing 2008*, LNCS 5209, Springer-Verlag, 2008, pp. 39–56.

[14] D. Brown and R. Gallant, The static Diffie-Hellman problem, available at `http://eprint.iacr.org/2004/306`.

[15] D. Cash, E. Kiltz, and V. Shoup, The twin Diffie-Hellman problem and applications, *Advances in Cryptology—Eurocrypt 2008*, LNCS 4965, Springer-Verlag, 2008, pp. 127–145.

[16] J. Cheon, Security analysis of the Strong Diffie-Hellman problem, *Advances in Cryptology—Eurocrypt 2006*, LNCS 4004, Springer-Verlag, 2006, pp. 1–11.

[17] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inf. Theory, IT-22*, 1976, pp. 644–654.

[18] F. Hess, Weil descent attacks, in *Advances in Elliptic Curve Cryptography*, ed. by I. Blake, G. Seroussi, and N. Smart, Cambridge University Press, 2005, pp. 151–182.

[19] J. Y. Hwang, D. H. Lee, and M. Yung, Universal forgery of the Identity-Based Sequential Aggregate Signature Scheme, *ACM Symposium on Information, Computer & Communication Security, ASIACCS 2009*.

[20] D. Jao and K. Yoshida, Boneh-Boyen signatures and the Strong Diffie-Hellman problem, *Pairing-Based Cryptography—Pairing 2009*, LNCS 5671, Springer-Verlag, 2009, pp. 1–16.

[21] A. Joux, A one round protocol for tripartite Diffie-Hellman, *Algorithmic Number Theory: Fourth International Symposium*, LNCS 1838, Springer-Verlag, 2000, pp. 385-393.

[22] A. H. Koblitz, N. Koblitz, and A. Menezes, Elliptic curve cryptography: The serpentine course of a paradigm shift, to appear in

[2] *With apologies to the* Notices *editor, who asked us to be sure to write out all acronyms.*

J. Number Theory, available at `http://eprint.iacr.org/2008/390`.

[23] N. Koblitz and A. Menezes, Another look at "provable security", *J. Cryptology* **20** (2007), pp. 3–37.

[24] N. Koblitz and A. Menezes, Another look at non-standard discrete log and Diffie-Hellman problems, *J. Math. Cryptology* **2** (2008), pp. 311–326.

[25] U. Maurer and S. Wolf, The Diffie-Hellman protocol, *Designs, Codes and Cryptography* **19** (2000), pp. 147–171.

[26] V. I. Nechaev, Complexity of a deterministic algorithm for the discrete logarithm, *Mathematical Notes* **55** (2) (1994), pp. 165–172.

[27] M. Rabin, Digitalized signatures and public-key functions as intractable as factorization, MIT Lab. for Computer Science Technical Report LCS/TR-212, 1979.

[28] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM* **21** (2) (1978), pp. 120–126.

[29] R. Sakai, K. Ohgishi, and M. Kasahara, Cryptosystems based on pairings, *Proc. 2000 Symposium on Cryptography and Information Security*, Okinawa, 2000.

[30] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology—Crypto '84*, LNCS 196, Springer-Verlag, 1985, pp. 277–296.

[31] V. Shoup, Lower bounds for discrete logarithms and related problems, *Advances in Cryptology—Eurocrypt '97*, LNCS 1233, Springer-Verlag, 1997, pp. 256–266.

[32] B. Snow, We need assurance!, *Proc. 21st Annual Computer Security Applications Conference*, IEEE Computer Society, 2005, pp. 3–10.

[33] E. Teske, Square-root algorithms for the discrete log problem (a survey), in *Public-Key Cryptography and Computational Number Theory*, Walter de Gruyter, 2001, pp. 283–301.

[34] H. Williams, A modification of the RSA public-key encryption procedure, *IEEE Trans. Inf. Theory, IT-26*, 1980, pp. 726–729.

The Arithmetic Behind Cryptography

Gerhard Frey

The security of very efficient and widely used public key crypto systems is based on the hardness of mathematical problems. Typically such problems come from arithmetic. Here are three important examples: Find shortest or closest vectors in lattices, factor large numbers, and **compute logarithms in finite groups**.

In this article we shall concentrate on the last example and so cover crypto systems for which the crypto primitive behind them is the discrete logarithm (DL) in cyclic groups of prime order (see the subsection on Diffie-Hellman Problems).

The first proposal for such systems was given by Diffie and Hellman in their groundbreaking article [DH]. As groups they suggested taking roots of unity in the multiplicative group of finite fields.

The generality of the methods provided by algorithmic arithmetic geometry opens immediately a wide range of possibilities. One can replace torsion points in the multiplicative group by torsion points of Jacobian varieties of curves over finite fields. But, on the other side, the strength of the methods allows us to develop very efficient attacks. So most of the suggested candidates for public key systems did not fulfill the expectations, and only DL-systems based on carefully chosen elliptic curves and curves of genus 2 survived without any blame.

This does not mean that the study of curves of arbitrary genus is not important for applications in data security. In many cases we understand partial weaknesses of elliptic curves by making more general objects accessible to computation. The continuous study of consequences of advances in algorithmic arithmetic geometry for the security of used crypto system and failures of attacks give mathematicians a better conscience and users more trust. So even people only involved in designing systems without being interested in the theoretical background can choose (very special) cases, for example, one elliptic curve over a fixed field with explicit addition formulas given in a list of standardized curves, for instance listed in [NIST] or in [BRAIN]. But apart from applications to elliptic curves the higher genus curves have various applications in cryptography which we cannot describe in this short survey.

But it is not only the status quo which is supported. New points of view from the theoretical side lead to advances in the design of hardware as well as in protocols. One of the striking examples is the development of pairing-based cryptography. From its background, namely duality theory in arithmetic geometry, there goes a direct path to very efficient implementations of pairings which allow, for instance, new ways to sign, and here curves of higher genus may play an important role.

Acknowledgment. The author would like to thank the referees for careful reading of the manuscript and for their helpful comments.

Some Aspects of Arithmetic Geometry

In the section "Construction of DL-Systems" we shall formulate tasks for mathematicians motivated by needs of data security. It turns out that it is surprisingly difficult to find families of groups which are candidates for DL-systems, and that the search for bilinear structures is even more involved.

The only known examples are constructed with the help of advanced methods of arithmetic geometry mostly developed during the last sixty years. We emphasize the remarkable fact that they both enable us to solve old problems like FLT (see the subsection "Digression: FLT") and lead to efficient and secure families of public key crypto systems.

What Is Arithmetic Geometry?

Arithmetic geometry is one of the most powerful ingredients in mathematics. It combines classical algebraic number theory with algebraic geometry. It uses the theory of functions over ℂ, and so analytic geometry, and it transfers this theory to its p-adic counterpart, the p-adic rigid geometry.

The important feature is that objects from number theory, like the ring of integers, and

Gerhard Frey is professor of mathematics at the University of Duisburg-Essen. His email address is `gerhard.frey@gmail.com`.

objects from algebraic geometry, like varieties over finite fields, can be treated in a unified way (as schemes consisting of the set of points with topology and sheaves of functions). For instance, the arithmetic of rings of integers in number fields is very similar to the arithmetic of rings of holomorphic functions on affine curves over finite fields. The analogy is neither only formal nor in all aspects obtained by using a dictionary, and the interplay between the arithmetic world and the geometric world is extremely fruitful for both sides.

The situation becomes very interesting and extremely difficult if both points of view are mixed together, for instance, if we look at the arithmetic of curves C defined over number fields or p-adic fields K. Geometrically these are varieties of dimension 1, but since we can look at them as being defined over the ring of integers O_K of K, they carry a 2-dimensional structure: from C we get an arithmetical surface C. This surface contains for each prime ideal $\mathfrak{p}$ of O_K a closed fiber $C^{\mathfrak{p}}$ (special fiber at $\mathfrak{p}$) which is the reduction of C modulo $\mathfrak{p}$, that is, roughly speaking, the curve obtained by looking at the equations defining C (in a suitable normalization with respect to $\mathfrak{p}$) modulo $\mathfrak{p}$. The arithmetical surface C contains much more information than its generic fiber C. It is not uniquely determined by C. There is an optimal model, the so-called minimal model, and using this model one can try to get the arithmetical data of C from studying the analogous data of the special fibers. In the case that K is a number field one tries to exploit the local information one gets over the completions at all places of K simultaneously in order to get global information, for example, about rational points on C. (If $K = \mathbb{Q}$ these completions are the reals $\mathbb{R}$ and, for all prime numbers p, the p-adic numbers $\mathbb{Q}_p$.) If this strategy is successful then one has established a local-global principle. One famous example of such a principle is the theorem of Hasse-Minkowski which states that one quadratic polynomial in arbitrarily many variables with coefficients in a number field K has a K-rational solution if and only if it has solutions in all fields obtained as completions with respect to valuations of K.

We cannot expect to get such a principle for general varieties. In fact we already find counterexamples if we look at the set of solutions of two quadratic equations or of polynomials in two variables of degree 3. But there is a Galois theoretical variant which relates local with global information: the density theorem of Čebotarev (Theorem 2.5).

Algorithmic Arithmetic Geometry

Classically algorithmic aspects of number theory mostly deal with lattices and derived objects. A fundamental tool is Minkowski's theorem on points with small norms in lattices and related results, for instance reduction of quadratic forms following Lagrange and Gauss. The enormous growth of computational power made it possible to construct interesting examples in a wide range, and very often one meets the LLL algorithm as a major tool.

The theoretical insights obtained by the approach described in the preceding subsection made rapid and exciting progress possible in the area of algorithmic arithmetic geometry, generalizing considerably both range and techniques of computational number theory. Prominent examples are computation of tables of modular forms including congruences, algorithmic study of modular curves (see, for instance, the Cremona tables [C] listing elliptic curves) and related Galois representations.

Translating arithmetical problems into the geometric language has the immediate consequence that one can apply the methods from arithmetic to the geometric case, too. And so we have now a very advanced theoretical and algorithmic toolkit to deal with the **explicit theory** of varieties over finite fields as a counterpart to the explicit theory of algebraic number fields. We devote the subsection "Arithmetic in Divisor Classes" to an important example.

Complexity Hierarchy. A crucial part of every algorithmic theory is the determination of the complexity of the available algorithms.

Here we can only scratch the surface of this fascinating mathematical subject. We introduce Landau's notation:

For

$$f, g : \mathbb{N} \to \mathbb{R}$$

with g positive define

$$f = \mathcal{O}(g)$$

if there exists $d \in \mathbb{R}_{>0}$ with

$$| f(N) | \leq dg(N)$$

for all N.

Take $\alpha \in [0,1], c \in \mathbb{R}_{>0}$.

Define

$$L_N(\alpha, c) := \exp(c \cdot \log(N)^{\alpha} \cdot \log(N)^{1-\alpha}).$$

For (almost all) $N \in \mathbb{N}$, let

$$f_N : A_N \to B_N$$

be maps from sets A_N to sets B_N. Assume that there is an algorithm which evaluates f_N with (probabilistic) complexity (e.g., number of bit operations needed) $F(N)$.

Then the (probabilistic) asymptotic complexity of the family f_N is called

- *polynomial* if $F = \mathcal{O}(L_N(0, c))$ ("*fast algorithm*")

- *exponential* if $F = \mathcal{O}(L_N(1, c))$ ("*hard algorithm*") and
- *subexponential* if there is $0 < \alpha < 1$ with $F = \mathcal{O}(L_N(\alpha, c))$

in $\log(N)$.

Subexponential complexity is a very interesting case between the two extremes.

Caution: This notion of complexity is an asymptotic estimate of a specific algorithm for the evaluation of f_N. In particular, it is only an upper bound for the hardness of the evaluation of f_N.

Nevertheless it gives a good impression of what one can expect for given instances with concrete N large enough.

Examples for algorithms with polynomial complexity are

- the (extended) Euclidean algorithm and
- exponentiation in groups (expressed in costs for group operation).

The first example implies that the computation of the greatest common divisor of numbers and polynomials as well as the computation of the inverse in finite groups with known group order is of polynomial complexity.

From the second example it follows that exponentiation in finite fields $\mathbb{F}_q$ is, as a function in $\log(q)$, polynomial. The same is true for scalar multiplication in elliptic curves (see the subsection "Curves of Genus 1: Elliptic Curves"). But a highly nontrivial and much more general result is explained in the next subsection.

Arithmetic in Divisor Classes. We take a (projective absolutely irreducible nonsingular) curve C of genus g defined over a field K which has no inseparable algebraic extensions. This means that irreducible polynomials over K have no multiple zeros. Examples are all fields of characteristic 0 and all finite fields.

We assume that we have a K-rational point P_∞ on C and denote by O_C the ring of functions on C which have only poles in P_∞.

As an example take C as projective line. Then O_C is isomorphic to the ring of polynomials in one variable.

The ring O_C is a Dedekind domain and so every ideal $\neq \{0\}$ is, in a unique way, the product of powers of prime ideals.

The quotient field $F_C = Quot(O_C)$ is the function field of C and is independent of the choice of P_∞.

We generalize the notion of ideals of O_C to ideals of F_C by defining: $A \subset F_C$ is an ideal if there is an element $f \in F_C^*$ such that $f \cdot A \subset O_C$ is an ideal of O_C in the usual sense.

The set of ideals of F_C is a commutative group $I(O_C)$ which is freely generated by the set of prime ideals of O_C.

Inside of $I(O_C)$ we have the subgroup $\mathrm{Princ}(O_C)$ of principal ideals $f \cdot O_C, f \in F_C^*$. The quotient group

$$\mathrm{Pic}(O_C) := I(O_C)/\mathrm{Princ}(O_C)$$

is the ideal class group of O_C. It is in a natural way isomorphic to $\mathrm{Pic}^0(C)$, the divisor class group of degree 0 of C, and a fundamental theorem of the theory of curves states that $\mathrm{Pic}^0(C)$ is in a functorial way isomorphic to the group of K-rational points of the Jacobian variety J_C of C. This is an abelian variety (i.e., a geometrically connected projective commutative group scheme) of dimension g over K.

The crucial point is that we can add in an explicit way in $J_C(K) = \mathrm{Pic}^0(C) = \mathrm{Pic}(O_C)$! To see this one recalls that the algebraic structure of O_C is similar to the structure of the rings of integers of number fields and that $Pic(O_C)$ is analogous to the ideal class groups of number fields. Computing in these groups is one of the major tasks of computational number theory, and it is done effectively because of Minkowski's theorem on points with small norm in lattices. An immediate consequence is that class groups of number fields are finite.

In the geometric frame Minkowski's theorem is replaced by the even more fundamental theorem of Riemann-Roch. The size of the discriminant of K is replaced by the genus g of C. Again we get as an immediate consequence that for finite fields $K = \mathbb{F}_q$ (the field with q elements) the group $\mathrm{Pic}^0(C)$ is a finite group. In fact, we get a rather sharp estimate from below and above for this size depending on q and g in the subsection "The Local Information".

We state an important and amazing recent result concerning the computation of the sum of two elements in $\mathrm{Pic}^0(C)$.

Theorem 2.1 (Hess, Diem)**.** *Let C be a curve of genus g over the field $\mathbb{F}_q$. The addition and inversion in the divisor class group of degree 0 of C can be performed by an explicitly given algorithm in an expected number of bit operations which is polynomially bounded in g and $log(q)$, i.e., group operations and scalar multiplication in divisor class groups are of polynomial complexity both in g (with fixed q) and* $\log(q)$ *(with fixed g).*

Curves of Genus 1: Elliptic Curves. We apply the Riemann-Roch theorem to the special case that C has genus 1 and a rational point P_∞ and come to a well-known object: elliptic curves. We get:

- $E(K)$ is in a natural way an abelian group with neutral element P_∞.
- E is as a variety isomorphic to its Jacobian variety, and so elliptic curves with chosen point P_∞ are abelian varieties of dimension 1.

- The addition in $E(K)$ is given by the following rule: $R = P \oplus Q$ is the unique point on $E(K)$ for which there exists a function in F_E with zeroes of order 1 in P and Q (respectively a zero of order 2 if $P = Q$) and poles of order 1 in P_∞ and R (and of order 2 in P_∞ if $R = P_\infty$).
- We find projective coordinates such that E is given by a cubic homogenous equation

  $$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

  (called the Weierstrass equation) without singular points. The only point with Z-coordinate equal 0 is $P_\infty = (0, 1, 0)$. All other points can be given by affine coordinates as $P = (x, y)$ with $y^2 + a_1xy + a_3y = x^3 + a_2x + a_4x + a_6$.
- If char(K) is prime to 6 we find a short Weierstrass equation

  $$E : \ Y^2Z \ = \ X^3 \ + AXZ^2 \ + BZ^3$$

  with $A, B \in K$ and discriminant $\Delta_E := 4A^3 + 27B^2 \neq 0$.

Using the short Weierstrass equation we can describe addition geometrically by the following rule: Take the line through P and Q (take the tangent line if $P = Q$) and compute the third intersection point $-R$ with E. Then R is the point obtained from $-R$ by reflection at the x-axis.

From this description one easily deduces formulas for the addition on $E(K)$: For

$$P_1 = (x_1, y_1, 1), \qquad P_2 = (x_2, y_2, 1)$$

we get "in general"

$$P_3 \ = (x_3, y_3, 1) \ := \ P_1 \ \oplus \ P_2$$

with

$$x_3 \ = \ -(x_1 + x_2) + \ ((y_1 - y_2)/(x_1 - x_2))^2.$$

For doubling points there is another explicit formula.

This is a short and simple formula. But, because of its importance, a lot of work has been done to make addition even faster, by using appropriate coordinates, appropriate coefficients, and appropriate normal forms for equations. This is described in full detail in [ACF], Chapter 13.

Remark 2.2. It is obvious that we do not need deep theory to get Theorem 2.1 for elliptic curves. But in many cases one can transfer the group structure of elliptic curves to the addition in divisor class groups of more general curves. By the theorem we know that the complexity hierarchy of the group operations is not changed. This is important for the analysis of attacks to crypto systems (the subsection "Attacks").

Galois Representations Attached to Abelian Varieties

In arithmetic geometry we want to find properties of objects over arithmetically interesting fields K such as number fields, p-adic fields, finite fields. The methods used from algebraic geometry and analysis work better over separably closed fields. The bridge between the two concepts is built by the action of the absolute Galois group $G_K = Aut(K_s/K)$ (K_s the separable closure of K), always assumed to be continuous with respect to the profinite topology on G_K.

Very often this action is studied on free modules over appropriate rings R like $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_\ell$, the ℓ-adic numbers, and leads to *Galois representations.*

Elements of finite order in abelian varieties A of dimension d are a main source for such representations. A basic result is that, for natural numbers n prime to char(K), the group of torsion points of order n

$$A[n] := \{P \in A(K_s); \ n \cdot P = 0\}$$

is an abelian group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2d}$. Hence, after choosing a $\mathbb{Z}/n\mathbb{Z}$-base of $A[n]$, the action of $\sigma \in G_K$ is given by a matrix, and we get a continuous homomorphism

$$\rho_{A,n} : G_K \to M_{2d}(\mathbb{Z}/n) \text{ with } M_{2d} = \text{set of } 2d \times 2d\text{-matrices.}$$

In particular, one can attach to curves C of genus g Galois representations of dimension $2g$ induced by the action of G_K on $J_C[n]$ or, nearer to computation, on the elements of order dividing n in the divisor class group of degree 0 of C regarded as a curve over K_s.

Example 2.3. Let E/K be an elliptic curve and $n \in \mathbb{N}$ prime to the characteristic of K. The action of G_K on $E[n]$ induces a 2-dimensional Galois representation $\rho_{E,n}$ over $\mathbb{Z}/n\mathbb{Z}$.

For $\sigma \in G_K$ the characteristic polynomial is defined by

$$\chi_{\rho_{E,n}(\sigma)}(T) = T^2 - Tr(\rho_{E,n}(\sigma))T + \det(\rho_{E,n}(\sigma)).$$

In many important cases $\rho_{E,n}$ is semisimple and hence it is determined by its characteristic polynomials.

ℓ-adic version. Take a prime ℓ different from char(K) and define the ℓ =adic Tate module of an abelian variety A (e.g., $A = J_C$) by

$$T_\ell(A) :=\overset{lim}{\leftarrow} A[\ell^k].$$

G_K acts continuously (with respect to the ℓ-adic topology) on $T_\ell(A)$ and induces a representation $\tilde{\rho}_{A,\ell}$ over $\mathbb{Z}_\ell$ or, by tensoring with $\mathbb{Q}$, over the field of ℓ-adic numbers.

In particular, we can attach ℓ-adic representations to the divisor class groups of curves.

Galois Representations in Arithmetical Geometry

In this subsection K is a number field, that is, a finite algebraic extension of $\mathbb{Q}$. In number theory we have a hierarchy of fields: The number field K carries various topologies induced by valuations v which extend the p-adic valuations and the absolute value on $\mathbb{Q}$.

The completion of K with respect to the topology induced by one v is the local field K_v which is an algebraic extension field of p-adic numbers $\mathbb{Q}_p$ or an extension field of $\mathbb{R}$. It contains K as a dense subfield.

If v is an extension of a p-adic valuation then the ring of integers O_K of K is contained in the valuation ring of v and dense in the ring O_v of v-adic integers of K_v. The residue field of v is the finite field $\mathbb{F}_v$ obtained as quotient of O_K or, equivalently, of O_v modulo the maximal ideal m_v of v. It is a finite algebraic extension of $\mathbb{F}_p$ and so isomorphic to $\mathbb{F}_q$ with $q = p^d$.

Remark 2.4. In *number theory* one tries to solve problems over global fields by looking at them over (all) local fields and then reducing them modulo v to problems over finite fields. One hopes that one does not lose too much information (local-global-principle), see "What Is Arithmetic Geometry?"

In *cryptography* one is mainly interested in objects over *finite fields* but by studying them one is often led to problems over local fields ("lifting") and even over global fields.

The hierarchy of fields is reflected by the hierarchy of Galois groups.

The global Galois group G_K is big and complicated. It is studied by restriction to subgroups G_v which consist of elements of G_K acting continuously with respect to the v-topology. G_v can be identified with the Galois group G_{K_v} whose structure is much simpler. In particular, it has a canonical quotient group which is the Galois group of the maximal unramified extension of K_v in its separable closure. This quotient is canonically isomorphic to $G_{\mathbb{F}_q}$ and so topologically generated by the Frobenius automorphism ϕ_q mapping elements of $\mathbb{F}_{q,s}$ to their qth power.

Via these identifications one can define (conjugacy classes of) Frobenius elements $\sigma_v \in G_K$ attached to each v.

We come back to the Galois representations attached to torsion points, respectively, Tate modules of abelian varieties A.

A consequence of the arithmetic of abelian varieties is that the fixed field $K_s^{ker(\tilde{\rho}_{A,\ell})}$ of the kernel of $\tilde{\rho}_{A,\ell}$ is ramified only in places v of K dividing either ℓ or at which A has bad reduction. Hence almost all places of K are unramified. Representations satisfying this condition are called geometric. It has turned out that the study of these representations is the key to the great results in number theory achieved during the last thirty years, and, at the same time, it is crucial for finding DL-systems.

Having a geometric representation ρ, we define S_ρ as the finite set of places of K which consist of all extensions of the absolute value and of all places which ramify in $K_s^{ker(\rho)}/K$. For every place $v \notin S_\rho$ we can choose a Frobenius element σ_v. The image of ρ at σ_v determines the restriction of ρ to G_{K_v}. It gives the local information about ρ at v.

Looking at all $v \notin S_\rho$ we can bundle this local information. The next big result tells us that we have a local-global principle for semisimple geometric representations.

Theorem 2.5 (Čebotarev's Density Theorem)**.** *Let ρ be a geometric Galois representation of G_K.*

If ρ is semisimple, then ρ is determined by

$\{\chi_{\rho(\sigma_v)}(T); v$

runs over places of K not contained in S_ρ $\}$.

It is even allowed to omit finitely many additional places of K.

Remark 2.6. To demonstrate the power of this statement we remark that the proof of Mordell's conjecture by Faltings follows from his result that for prime numbers ℓ and all abelian varieties A defined over K the representation $\tilde{\rho}_{A,\ell}$ is semisimple.

The Local Information

We fix a finite field $\mathbb{F}_q$ and take a curve C of genus g defined over $\mathbb{F}_q$. The following result is a landmark (established ~ 1930–40) in arithmetical geometry.

Theorem 2.7 (Weil)**.** *There is a monic polynomial $\chi_C(T) \in \mathbb{Z}[T]$ such that:*

- *All zeroes of $\chi_C(T)$ have (complex) value $\sqrt{q}$.*[1]
- *For all n, the characteristic polynomial of the Frobenius automorphism ϕ_q under the representation $\rho_{J_C,n}$ is congruent to $\chi_C(T)$ modulo n.*
- *For all $\ell \neq p$, the characteristic polynomial of the Frobenius automorphism ϕ_q under the representation $\tilde{\rho}_{J_C,\ell}$ is equal to $\chi_C(T)$.*

By linear algebra we see that $|J_C(\mathbb{F}_q)| = |Pic^0(C)| = \chi_C(1)$.

As consequence we get that $|Pic^0(C) - q^g| = \mathcal{O}(q^{g-1/2})$.

Corollary 2.8. *Let E be an elliptic curve over $\mathbb{F}_q$.*

Then $a_q :=| \ E(\mathbb{F}_q) \ |= q + 1 - Tr(\tilde{\rho}_{E,\ell})$ and $|\ | \ E(\mathbb{F}_q) \ | - q - 1| \le 2\sqrt{q}$ (Hasse bound).

[1] *This is an analogue of the Riemann hypothesis in number theory and so it is sometimes called the "Riemann hypothesis" for curves though it is a proven result.*

The Global Information

We are very short on space here and consider only a special case: $K = \mathbb{Q}$ and $C = E$ an elliptic curve. In the preceding subsection we have computed the characteristic polynomial of the Frobenius endomorphism ϕ_p at least when p is not dividing Δ_E.

We bundle the local information and form the **global L-series** of E:

$$L_E(s) := f^*(s) \cdot \prod_{p \text{ prime to } \Delta_E} (1-(p+1-a_p)p^{-s}+p^{1-s})^{-1}$$

where $f^*(s)$ is a rational function which takes care of bad primes and a_p is, as above, the order of $E(\mathbb{F}_p)$.

This is a Dirichlet series, and the conjecture of Hasse-Taniyama was that it could be extended to an analytic function in the complex plane.

This was known since about the 1950s from results of M. Deuring in the case that E has complex multiplication (CM) and yields an important tool for cryptography.

Digression: FLT. Though it has nothing to do with cryptography, we cannot resist hinting at how to prove FLT.

The conjecture of Hasse-Taniyama has been proved by A. Wiles ([W]) in a relevant special case; in fact he proved the conjecture of Shimura-Taniyama-Weil for semistable elliptic curves:[2] $L_E(s)$ is the Euler product attached to a **modular form of weight** 2!

Proof of FLT in Eight Lines

Assume that $A^p - B^p = C^p$ for $p \geq 5$.

I suggested to look at the elliptic curve $E : Y^2 = X(X - A^p)(X - B^p)$.

By global information (Wiles) $\rho_{E,p}$ is attached to a modular form. By local information about E and the theorem of Ribet (Serre's conjecture) $\rho_{E,p}$ is attached to a modular form $\neq 0$ of level 2 and weight 2. Such a form does not exist!

Construction of DL-Systems

We want to explain how the methods sketched in the preceding section can be used for cryptography.

We introduce very shortly the requirements coming from the needs of public key cryptography based on discrete logarithms.

Diffie-Hellman Problems

Let G be a group of known order n.

We can formulate a *computational problem*:

DHCP: For randomly chosen $a, b \in \{1, \dots, n\}$, $g \in G$ and given $g_1 = g^a, g_2 = g^b$, compute $g^{a \cdot b}$.

DHCP is called the Diffie-Hellman computational problem.

It is obvious that we can solve DHCP if we can solve the following task:

For randomly chosen $g_1, g_2 \in G$ decide whether g_2 lies in the cyclic group generated by g_1, and if so, compute $k \in \mathbb{N}$ with

$$g_2 = g_1^k.$$

The residue class of such a k modulo n is the discrete logarithm (DL) $log_{g_1}(g_2)$. Highly nontrivial is a kind of converse: there is a subexponential algorithm due to Maurer-Wolf that can compute the (DL) in G if one knows how to solve DHCP. Thus, the complexity of (DL) is an upper bound for the complexity of DHCP and, up to subexponential algorithms, the crypto primitive determining security of the Diffie-Hellman key exchange and encryption, as well as of the El Gamal signature ([ACF]), is the discrete logarithm.

By elementary number theory (Chinese remainder theorem and p-adic expansion of numbers) one sees immediately that without loss of generality we can and shall assume that n is a prime number ℓ. So G is a cyclic group generated by an element g_0, and (DL) is equivalent to the computation of $log_{g_0}(g)$ for random $g \in G$.

There are "derived" cryptographic schemes for which the hardness of the *Diffie-Hellman decision problem* **DHDP** determines security. The DHDP asks—for randomly given elements g_0, g_1, g_2, g_3—for a decision whether

$$\log_{g_0}(g_1) \cdot \log_{g_0}(g_1) = \log_{g_0}(g_3).$$

DL-Systems

To use (family of) groups G for public key systems we have to solve three crucial tasks:

(1) Store the elements in G in a computer in a compact way (ideally $\mathcal{O}(\log(\mid G \mid))$ bits should be enough).

(2) The group composition is given by an algorithm which is easily implemented and very fast (at most polynomially bounded time and space is allowed). So exponentiation is of polynomial complexity, too.

(3) The computation of the DL in G (for random elements) is (to the best of our knowledge) very hard and so unfeasible in practice (ideally exponential in $\mid G \mid$).

Groups G with generator g_0 satisfying these conditions are called DL-systems.

[2] *The general proof was given by Breuil, Conrad, and Diamond. The conjecture is a special case of* Serre's conjecture, *which is now proved, too.*

Remark 3.1. We use the structure "group" to define the crypto primitive. This already implies that the complexity of the DHCP is at most $\sim \sqrt{\ell}$ since there are (deterministic and probabilistic) algorithms for the computation of discrete logarithms applicable to *all* groups (e.g., Shank's Baby-Step-Giant-Step or Pollard's ρ-algorithm) of this complexity. A deep fact is that in generic groups no faster algorithm is available. Hence $\sqrt{\ell}$ is the benchmark for the hardness of DL and DHCP.

Bilinear Structures

Discrete logarithms concern the $\mathbb{Z}/\ell$-linear structure of cyclic groups. In every elementary course on linear algebra one learns that there are multilinear aspects coming in a natural way from the theory of linear maps. The principle behind this is duality.

During the last ten years this aspect has become more and more important in public key cryptography, and there is much ongoing research in this area.

Definition 3.2. Let G be a cyclic group of prime order ℓ. Assume that there are $\mathbb{Z}/\ell$-modules B and C and a bilinear map $Q : G \times B \to C$ with

i): the group composition laws in G, B, and C, as well as the map Q, are fast (e.g., polynomial time).

ii): For random $b \in B$ we have $Q(g_1, b) = Q(g_2, b)$ iff $g_1 = g_2$.

We call (G, Q) a *DL-system with bilinear structure.*

Since we can transfer the computation of discrete logarithms from G to C via Q, the existence of bilinear structures may weaken DL-systems. Moreover, if $G = B$, then DHDP becomes trivial.

But there are very interesting constructive features, too. In the center of interest are short signatures and identity-based protocols.

Candidates for DL-Systems

We want to find groups G satisfying the conditions of subsection "DL-Systems" and analyze bilinear structures.

As mentioned earlier, Diffie and Hellman suggested taking a prime ℓ dividing $q-1$ and G as the group of ℓth roots of unity in $\mathbb{F}_q^*$. It is not difficult to find instances where ℓ is of the same magnitude as q, and conditions i and ii of Definition 3.2 are satisfied. But the hardness of the DL (which is the classical one already studied by Jacobi) is disappointing. It is only of subexponential complexity; the reason is that points on the projective line over $\mathbb{F}_q$ are easily lifted to points on the line over $\mathbb{Z}$, and then a powerful method, index calculus (cf. [ACF]), can be applied.

Structural theorems about abelian varieties over number fields imply that such a lifting is very difficult if we take Jacobians of curves of genus larger than 0.

This was the motivation for V. Miller [M1] to suggest in 1985 using elliptic curves over finite fields for DL-systems. Independently N. Koblitz [K1] suggested this at the same time, and in 1989 [K2] he went further to propose class groups of hyperelliptic curves, too.

With the results obtained in Theorem 2.1, we can go even further and try to use divisor class groups of curves of any genus $g > 0$ over $\mathbb{F}_q$. Fixing a size of magnitude M for ℓ (e.g., 10^{80}) we can use Weil's theorem and take q and g such that $M \approx q^g$ (e.g., $g \cdot \log_{10}(q) \approx 80$). Then the diophantine task is to find a field $\mathbb{F}_q$ and a curve C of genus g defined over $\mathbb{F}_q$ such that $|\mathrm{Pic}^0(C)|$ is (maybe up to a small cofactor) a prime number ℓ.

There are theorems from analytic number theory which predict that the chances to find such pairs are rather good; and so the strategy is to choose random curves and test whether they satisfy the condition.

To do this we need a fast algorithm to determine $|\mathrm{Pic}^0(C)|$.

Point Counting

This cannot be done naively. One has to use the action of Frobenius automorphisms ϕ_q and compute its characteristic polynomial. For this one uses all the techniques sketched in the section "Some Aspects of Arithmetic Geometry" in very advanced forms:

(1) Class field theory of CM-fields leads to the so-called CM method worked out for genus 1,2,3 by Atkin, Enge, Morain, Spallek, Weng, and many others. Hence we use global Galois theory. We remark that for $g = 1$ this leads to the explicit class field theory of imaginary quadratic fields.

(2) Etale cohomology groups, i.e., ℓ-adic representations attached to Tate modules of J_C (Schoof, Atkin, Elkies, Pila, …).

(3) p-adic cohomology (Satoh, Kedlaya, Mestre,…) for moderate sizes of p (lifting to p-adic fields).

For details we refer to [ACF]. As state of the art, we get

Result 1. In cryptographically relevant areas

- we can count points on random elliptic curves,
- we can count points on Jacobians of random curves over fields of small (and even medium) characteristic,
- we still have problems with random curves of genus 2 over prime fields (but see the work of Gaudry and Schost [GS]); we can

use class field theory of CM-fields to find an abundance of curves of genus 2 suitable for DL-systems,

- and, of course, we have many *special* families of curves whose members are accessible for point counting.

So for every $g \in \mathbb{N}$ we find divisor class groups of curves of genus g which satisfy conditions 1 and 2 of the subsection "DL-Systems".

Attacks

Curves of Genus > 2. The main motivation to take divisor class groups was to avoid index-calculus attacks enabled by lifting points on curves from finite fields to number fields.

But it was soon discovered that the internal structure of divisor class groups of curves of large genus yields another type of index-calculus attack.

Even worse: variants of this attack are applicable to curves of moderate genus. The sharpest result nowadays is

Theorem 3.3 (Diem, Gaudry, Thomé, Thériault)**.** *There exists an algorithm which computes, up to* $\log(q)$*-factors, the DL in the divisor class group of curves of genus* g *in expected time of* $\mathcal{O}(q^{(2-2/g)})$.

If C *is given by a plane curve of degree* d *(singularities allowed), then the DL in the group of divisor classes of degree* 0 *is of complexity* $\mathcal{O}(q^{2-\frac{2}{d-2}})$.

Recall that the generic algorithms have complexity $\mathcal{O}(q^{g/2})$. Hence curves of genus larger than 4 are not advisable.

The results of the theorem do not imply that systems using hyperelliptic curves of genus 4 are insecure, but the parameters of the systems have to be larger than for generic groups.

Particularly interesting is the situation for curves of genus 3. Surprisingly, nonhyperelliptic curves are less secure since they have a plane model of degree 4. So one has to exclude hyperelliptic curves of genus 3 which have computable isogenies to nonhyperelliptic curves. Unfortunately there are many such curves, and at the moment it is not clear how to find criteria for the nonexistence of such isogenies.

So it may be wise to use only curves of genus 1 and 2 if there are no very good reasons for deciding otherwise.

Elliptic Curves. There is no direct index-calculus attack known which is effective on elliptic curves. But if the ground field is not a prime field, we can apply Weil descent (a well-known method in algebraic geometry [Fr1]) and transfer the DL in $E(\mathbb{F}_q)$ to the DL in an abelian variety of higher dimension and defined over a smaller ground field. Again, one can try to apply index-calculus in these abelian varieties, and there are many cases where one succeeds (e.g., the field $\mathbb{F}_{2^{155}}$ is not good for cryptographical use). To avoid this it is suggested that one use as ground field either $\mathbb{F}_p$ or $\mathbb{F}_{2^n}$, where n is a prime which is not a Mersenne prime.

Bilinear Structures

In the last section we saw that divisor classes of carefully enough chosen curves of genus 1 (elliptic curves) and genus 2 cannot be attacked nowadays by index-calculus methods. Now we want to discuss transfers by duality theorems coming from class field theory of local and global fields [Fr3].

The Lichtenbaum-Tate Pairing on Elliptic Curves

Divisor class groups carry a natural duality induced by class field theory of local fields. For Jacobian varieties this is made explicit by the Lichtenbaum-Tate pairing.

We state a version of this pairing for elliptic curves E over $\mathbb{F}_q$. (For the general background see [Fr3], for the general version see [FR].)

Theorem 4.1. *Let* ℓ *be a prime dividing* $|E(\mathbb{F}_q)|$. *Let* k *be the smallest natural number such that* $\ell|(q^k-1)$. *Let* ζ_ℓ *be an* ℓ*th root of unity in* $\mathbb{F}_{q^k}$.

Define $G := E[\ell] \cap E(\mathbb{F}_q)$ *and* $G^\perp := \{Q \in E(\mathbb{F}_q^k) \cap E[\ell];\ \phi_q(Q) = q \cdot Q\}$.

There is a nondegenerate pairing

$$Q : G \times G^\perp \to < \zeta_\ell >$$

which can be computed with complexity polynomial in $k \cdot \log q$.

This pairing is given very explicitly. For an algorithm see [M2] and [ACF], Chapter 16. Because of its importance there are many versions trying to accelerate the computation of pairings related to Q.

Corollary 4.2. *The DL in elliptic curves over* $\mathbb{F}_q$ *is transferred to the discrete logarithm in* $\mathbb{F}_{q^k}^*$ *and hence has complexity which is subexponential in* $k \cdot \log q$.

Pairing-Friendly Curves

Theorem 4.1 has computational relevance only if k is not large.

It is a dangerous result if k is small (say ≤ 6), and it can be used constructively if $k \approx 12$.

If we take random elliptic curves we shall expect that k is of the same size as ℓ. An elliptic curve E is called pairing-friendly if k is small.

There are curves which are too friendly: if E is supersingular (i.e., there are no algebraic points of order p on E), then $k \leq 6$ and even $k \leq 2$ if $p > 3$. Hence the DL on supersingular curves is not harder than the classical DL. For this reason supersingular curves play only a minor role in DL-systems based on elliptic curves. The nice thing is that they deliver easy examples for groups with gaps between DHCP and DHDP.

To use the constructive aspects of pairings described in the subsection "Bilinear Structures", for example, short signatures, one has to solve interesting diophantine problems in order to find elliptic curves with small, but not too small, k. In [BN] one finds (conjecturally infinitely) many elliptic curves with $k = 12$.

Remark 4.3. It would be interesting to be able to construct nonsupersingular pairing-friendly curves of genus 2.

Conclusion

We end by giving the equation of an elliptic curve which passed all security checks and travels on passports. Its equation is

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

with

$A = 7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9$,

$B = 26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6$

defined over $\mathbb{F}_{A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377}$.

$|E(\mathbb{F}_p)|$ is a prime ℓ

with $\ell = A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7$.

The name of the curve is **brainpoolP256r1**.

References

[ACF] H. Cohen and G. Frey (eds.), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC, 2005.

[BN] P. S. L. M. Barreto and M. Nähriq, *Pairing-Friendly Elliptic Curves of Prime Order*, SAC'2005, LNCS 3897, Springer, 319–331, 2006.

[BRAIN] `http://www.ecc-brainpool.org/ecc-standard.htm`.

[C] J. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd edition, Cambridge University Press, 1997.

[DH] W. Diffie and M. E. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory*, **22**(6) (1976), 644–654.

[Di] C. Diem, *On arithmetic and the discrete logarithm problem in class groups of curves*, Habil. Thesis, Leipzig 2009.

[Fr1] G. Frey, *How to disguise an elliptic curve*, slides, `http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html`.

[Fr3] ______, Discrete Logarithms, Duality, and Arithmetic in Brauer groups, in: *Algebraic Geometry and its Applications*, J. Chaumine, J. Hirschfeld, R. Rolland eds., 241–272, World Scientific, 2008.

[FR] G. Frey and H. G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, preprint IEM, Essen, 7, 1991, appeared in: *Math. Comp.* **62** (1994), 865–874.

[GS] P. Gaudry and E. Schost, Construction of secure random curves of genus 2 over prime fields, in: *Advances in Cryptology*, Eurocrypt 2004, LNCS 3027, 239–256, 2004.

[He] F. Hess, Computing Riemann-Roch spaces in algebraic function fields and related topics, *J. Symbolic Comp.* **33**(4) (2002), 425–445.

[K1] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.* **48** (1987), 203–209.

[K2] ______, Hyperelliptic cryptosystems, *J. Cryptology* **1** (1989), 139–150.

[M1] V. Miller, *Use of elliptic curves in cryptography*, Advances in cryptology—CRYPTO 85, Springer Lecture Notes in Computer Science, vol. 218, 1985.

[M2] V. S. Miller, Short programs for functions on curves, IBM, Thomas J. Watson Research Center, 1986; `http://crypto.sanford.edu/miller/`.

[NIST] National Institute of Standard and Technology, Recommended elliptic curves for federal use, 1999, `http://www.csrc.nist.gov/encryption/`.

[W] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. Math.* **141**(3) (1995), 443–551.

WHAT IS... a Gaussian Entire Function?

Fedor Nazarov and Mikhail Sodin

Random analytic functions have been attracting the attention of mathematicians since the 1930s, though the focus of interest has been changing with time. Just as the distribution of eigenvalues is the essence of the random matrix theory, central to the study of random analytic functions are their zero sets. Our random functions are Gaussian and live on the complex plane. The instance when the random zero set is invariant in distribution with regard to (w.r.t., for short) isometries of the plane is the most interesting one. Here we will introduce the reader to a remarkable model of Gaussian entire functions with invariant distribution of zeros.

A Gaussian entire function $f(z)$ is the sum $\sum_k \zeta_k f_k(z)$ of entire functions f_k with independent standard complex Gaussian random coefficients ζ_k (whose density w.r.t. the area measure in $\mathbb{C}$ is $\frac{1}{\pi}e^{-|\zeta|^2}$). We assume that

$$\sum_k |f_k(z)|^2 < \infty \text{ locally uniformly in } \mathbb{C},$$

and also that the functions f_k are linearly independent over ℓ^2, i.e., $\sum_k a_k f_k$ with $\{a_k\} \in \ell^2$ does not vanish identically unless all $a_k = 0$. The first condition implies that almost surely (a.s., for short) the random function f is entire.

Each Gaussian entire function can be uniquely identified with some Hilbert space $\mathcal{H}$ of entire functions (the image of the mapping

$$\ell^2 \ni \{a_k\} \mapsto \sum_k a_k f_k$$

with the scalar product borrowed from ℓ^2) so that the covariance function

$$C_f(z,w) = \mathcal{E}\left\{f(z)\overline{f(w)}\right\} = \sum_k f_k(z)\overline{f_k(w)}$$

is the reproducing kernel in $\mathcal{H}$; i.e.,

$$g(w) = \langle g, C(\cdot, w)\rangle_{\mathcal{H}} \text{ for every } g \in \mathcal{H}, w \in \mathbb{C}.$$

The functions f_k form an orthonormal basis in $\mathcal{H}$. Reversing the order, one can start with a Hilbert space $\mathcal{H}$ of entire functions with the reproducing kernel $C_{\mathcal{H}}$, take an orthonormal basis $\{f_k\}$ in $\mathcal{H}$, and build a Gaussian entire function $f_{\mathcal{H}} = \sum_k \zeta_k f_k$ with covariance $C_{\mathcal{H}}$. Since the Gaussian process is determined by its covariance function, this construction does not depend on the choice of the basis in $\mathcal{H}$.

The properties of the (random) zero set $\mathcal{Z}_f = f^{-1}\{0\}$ are encoded in its (random) counting measure n_f defined by $n_f(A) = \#\,(\mathcal{Z}_f \cap A)$ for any Borel set A. Recall that for every analytic function f, we have

$$n_f = \frac{1}{2\pi}\Delta \log|f|$$

with the Laplacian taken in the sense of distributions. This makes it possible to use complex analysis tools for the study of the distribution of zeroes of Gaussian analytic functions. Using this formula, and taking the expectation of both sides, we get $\mathcal{E}n_f = \frac{1}{2\pi}\Delta\mathcal{E}\log|f|$. Note that $\frac{f(z)}{\sqrt{C_f(z,z)}}$ is the standard complex Gaussian random variable, so

$$\mathcal{E}\log|f| = \tfrac{1}{2}\log C_f(z,z) + \text{const}\,.$$

This way, we arrive at the elegant Edelman-Kostlan formula

$$\mathcal{E}n_f(z) = \tfrac{1}{4\pi}\Delta\log C_f(z,z)\,.$$

The surprising Calabi rigidity tells us that the mean $\mathcal{E}n_f$ determines the distribution of $\mathcal{Z}_f$. Alas, this uniqueness gives us no hint as to how to find the distribution of n_f from its mean $\mathcal{E}n_f$.

All the aforementioned results are valid for Gaussian analytic functions in other plane domains. It is the gaussianity that is crucial, not the domain of f.

Fedor Nazarov is professor of mathematics at the University of Wisconsin, Madison. His email address is nazarov@math.wisc.edu.

Mikhail Sodin is professor of mathematics at Tel Aviv University. His email address is sodin@post.tau.ac.il.

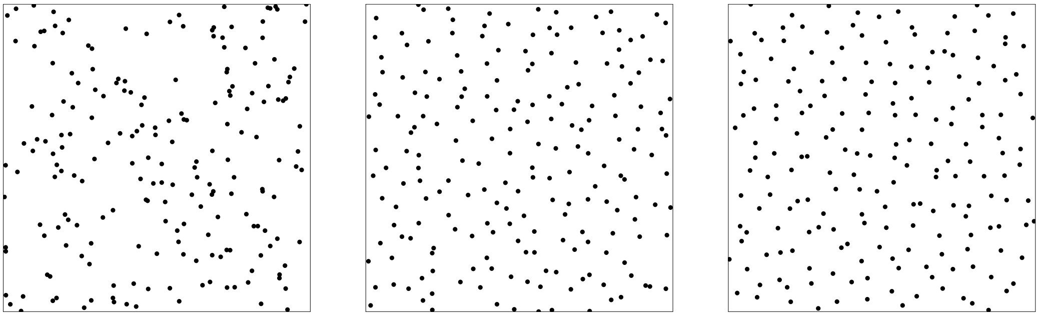


Figure 1. Samples of the Poisson process (figure by B. Virág), limiting Ginibre process, and zeroes of a GEF (figure by M. Krishnapur). The last two processes are quite different, though the eye does not easily distinguish them.

It is not at all obvious that there exist Gaussian entire functions with zeros having a translation-invariant distribution. It is not difficult to see that Gaussian entire functions cannot be translation invariant themselves.[1] Fortunately, a weaker property called projective invariance is sufficient for the translation invariance of zeros. Namely, if there is a family of nonrandom functions ϕ_λ $(\lambda \in \mathbb{C})$ without zeros such that the random functions $\phi_\lambda(z)f(z+\lambda)$ and $f(z)$ have the same distribution, then the distribution of $\mathcal{Z}_f$ is translation invariant.

Letting $f_k(z) = z^k/\sqrt{k!}$, we get $C_f(z,w) = e^{z\overline{w}}$, which is the kernel for the classical Fock-Bargmann space of entire functions, that is, the closure of polynomials in $L^2(\mathbb{C}, \frac{1}{\pi}e^{-|z|^2})$. The Gaussian entire function associated with this Hilbert space is projective invariant w.r.t. isometries of $\mathbb{C}$. The rotation and reflection invariance are obvious. To show the translation invariance, note that the Gaussian entire function

$$f(z+\lambda)e^{-z\overline{\lambda}-\frac{1}{2}|\lambda|^2}, \quad \lambda \in \mathbb{C},$$

has the same covariance function as f.

By the Edelman-Kostlan formula,

$$\mathcal{E}n_f = \tfrac{1}{4\pi}\Delta|z|^2 = \tfrac{1}{\pi}m,$$

where m is the area measure (we treat the average $\mathcal{E}n_f$ as a measure). Replacing f by $f_L(z) = f(\sqrt{\frac{L}{\pi}}\,z)$, this average can be changed to Lm with any $L > 0$. On the other hand, if zeros of a Gaussian entire function F have a translation-invariant distribution, then the mean $\mathcal{E}n_F$ is a translation-invariant measure on $\mathbb{C}$. Hence, it is proportional to the area measure m; i.e., $\mathcal{E}n_F = Lm$ with a constant $L > 0$. Then by the Calabi rigidity, the zero sets $\mathcal{Z}_F$ and $\mathcal{Z}_{f_L}$ have the same distribution. In other words, the only freedom in this construction is the scaling $z \mapsto tz$ with $t > 0$, and the Gaussian Entire Function (GEF, for short) with translation-invariant zeros is essentially unique. Geometers know this in a different wording: $z \mapsto \{z^k/\sqrt{k!}\}_{k\geq 0}$ is an isometric embedding of the Euclidean plane into the projective Hilbert space $P(\ell_2)$ equipped with the Fubini-Study metric, and this embedding is essentially unique.

The construction leading to projective invariance has been known since the 1930s, though the corresponding Gaussian functions were introduced only in the 1990s by Kostlan, Bogomolny-Bohigas-Lebouef, Shub-Smale, and Hannay. It is worth mentioning that there are similar constructions for other domains with transitive groups of isometries (hyperbolic plane, Riemann sphere, cylinder, and torus).

Few natural translation-invariant random point processes on the plane are known. The most widely studied one is the Poisson process, where for any collection of disjoint subsets of the plane, the numbers of points in these subsets are independent, and the mean number of points in a set is proportional to its area. This process is invariant w.r.t. all measure-preserving transformations of the plane, which is far more than we asked for. Another example is a one-component plasma of charged particles of one sign confined by a uniform background of the opposite sign. It contains as a special case the large N limit of Ginibre ensemble of eigenvalues of $N \times N$ matrices with independent standard complex Gaussian entries.[2] One more example is the random zero set $\mathcal{Z}_f$ of GEF f.

The Poisson process can be easily recognized since its points can clump together while, in contrast, the Ginibre eigenvalue process and the GEF zero process have local repulsion between points: it is unlikely that one would see two points very close to each other. The latter two look rather alike, although some of their characteristics are quite different. For instance, as Forrester and Honner observed, if h is a smooth function with

[1] *B. Weiss showed that, unexpectedly, there are translation-invariant random entire functions, not Gaussian, of course.*

[2] *Though one-component plasma has been studied by physicists for a long time, it seems that almost all rigorous mathematical results still pertain only to the special case of Ginibre ensemble.*

compact support, then the variance of the linear statistics of zeros $n_f(r;h) = \sum_{\mathcal{Z}_f} h(\frac{a}{r})$ decays as $\|\Delta h\|^2_{L^2} r^{-2}$ for $r \to \infty$, while in the Ginibre case the corresponding variance tends to the limit proportional to $\|\nabla h\|^2_{L^2}$ (for the Poisson process the variance grows with r as $\|h\|^2_{L^2}\, r^2$).

The decay of the variance of smooth linear statistics for zeros of GEF yields another surprising rigidity. We fix a bounded plane domain G and suppose that we know the configuration of zeros of f outside of G. Then taking any smooth compactly supported test-function h that equals 1 in some neighborhood of the origin, we recover the number of zeros of f inside G:

$$n_f(G) = \lim_{r\to\infty}\left\{\frac{r^2}{\pi}\iint_{\mathbb{C}} h\,\mathrm{d}m - \sum_{a\in\mathcal{Z}_f\setminus G} h\left(\frac{a}{r}\right)\right\} \quad \text{a.s.}$$

At the end of this introductory tour, we will take a brief look at the random potential

$$U_f(z) = \log|f(z)| - \tfrac{1}{2}|z|^2$$

and at its gradient field ∇U_f. Their distributions are invariant w.r.t. isometries of $\mathbb{C}$, and

$$\tfrac{1}{2\pi}\Delta U_f = \operatorname{div}(\nabla U_f) = n_f - \tfrac{1}{\pi}m.$$

The potential U_f equals $-\infty$ on $\mathcal{Z}_f$ and has no other local minima since its Laplacian is negative on $\mathbb{C}\setminus\mathcal{Z}_f$. The gradient curves oriented in the direction of decay of U_f and terminating at $a \in \mathcal{Z}_f$ form a basin B_a. Different basins are separated by the gradient curves joining local maxima with saddle points. Remarkably, all bounded basins have the same area π:

$$1 - \frac{1}{\pi}m(B_a) = \frac{1}{2\pi}\iint_{B_a}\Delta U_f = \frac{1}{2\pi}\int_{\partial B_a}\frac{\partial U_f}{\partial n} = 0\,.$$

One can prove that the probability of a long gradient curve decays exponentially with its diameter, so, a.s., all basins are bounded. Thus, one obtains a random partition of $\mathbb{C}$ into nice bounded domains of equal area with many intriguing properties.

We hope that we have aroused the reader's curiosity by now. Note that we have presented only a tiny portion of results and questions concerning Gaussian analytic functions and their zeros.

Further Reading

For those new to this subject, we recommend the book *Zeros of Gaussian Analytic Functions and Determinantal Point Processes*, J. B. Hough, M. Krishnapur, Y. Peres, B. Virág, Amer. Math. Soc., 2009. The electronic version is available at `stat-www.berkeley.edu/~peres/GAF_book.pdf`.

The lecture by M. Sodin at the 4th ECM, Stockholm, 2004 (`arXiv:math/0410343`), surveys results obtained by that time. Further developments can be found in recent papers written by the authors with A. Volberg, by B. Tsirelson, and by A. Nishry, and posted in the `arXiv`.

Complex-geometry-oriented readers might be interested in reading the papers by P. Bleher, M. Douglas, B. Shiffman, and S. Zelditch, which are also posted in the `arXiv`.

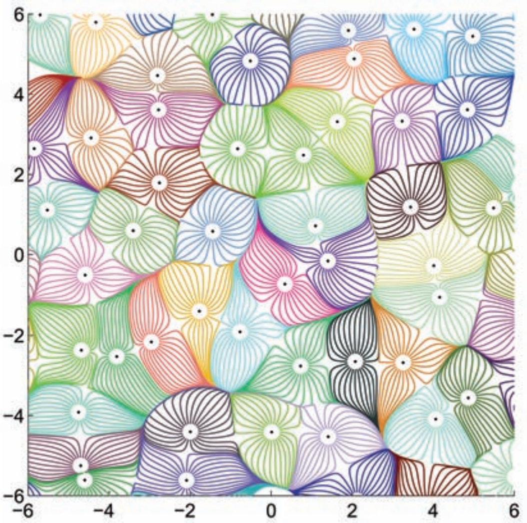
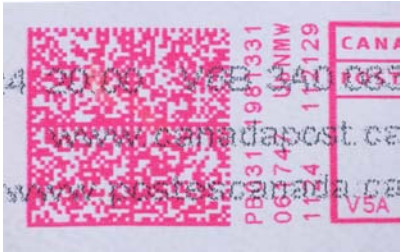


Figure 2. Random partition of the plane into domains of equal area generated by the gradient flow of the random potential U_f (figure by M. Krishnapur). The lines are gradient curves of U_f, the black dots are random zeros. Many basins meet at the same local maximum, so that two of them meet tangentially, while the others approach it cuspidally, forming long, thin tentacles.

Visible Cryptography

Bill Casselman

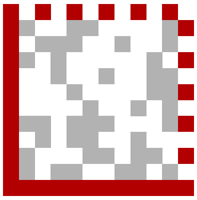
Cryptography literally permeates the air we breathe, since it is part of nearly all transmissions through cellular phones as well as many on the Internet, but there is one form of encryption that is visibly ubiquitous—those little matrices of pixels that occur on the mail of many countries of Europe and North America, inside letters from the Internal Revenue Service, on packaging of many commercial products in the U.S., and (at least in the future) on all pharmaceutical products in Europe. They are classified as bar codes, but in fact they are extremely sophisticated 2D arrays.



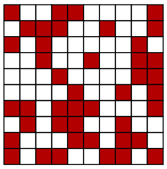
Their main advantage over older bar codes is that they allow a great deal of information to be packed into a very small space. All of them require several layers to be unpeeled before they can be interpreted, and in most applications the final layer involves elliptic curve cryptography (ECC). In postal use this provides a certificate of fee payment, among other things, and in pharmaceutical packaging it is intended to prevent counterfeits.

Data matrices come in a wide but fixed range of sizes, from 10 × 10 to 144 × 144. What a matrix displays is essentially an array of zeroes and ones. These are assembled into an array of bytes, each one 8 bits in size. These are unpacked according to one of several different modes of interpretation. The last several bytes of each matrix are added to the original message to allow error correction. After possible correction, one might have at hand a readable message, but more likely what one sees at this point is an array to be deciphered only by a secret key. Even if the message is not encrypted for security, it is likely to be somewhat condensed and meant to be interpreted according to some coding scheme particular to the application.

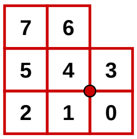
What I'll explain here is how the pixels are to be assembled into bytes, at least in one simple example. Let's look at the symbol on the right above, which was found on a carton of ice cream for sale in a supermarket in western Michigan. Every data matrix symbol is divided up into one or more smaller regions. The Canada postage symbol is divided up into 2 × 2 regions, while the one at hand is made up of just one. These regions are demarcated by special *peripheral pixels*, which are solid at left and bottom, alternating at right and top. These are used for alignment of bar code readers.



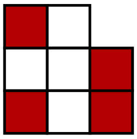
The core matrix is what you get by stripping away the peripheral pixels. Conventionally, its points are given coordinates (r, c) in matrix fashion, so r is row, c is column. Thus $(0, 0)$ is the upper left corner. A pixel is assigned the coordinate of its upper left corner.



There are 8 pixels in each byte, and the region occupied by a byte (at least for this symbol) is a 3 × 3 square with a corner taken out. These pixels are ordered right to left, bottom to top.

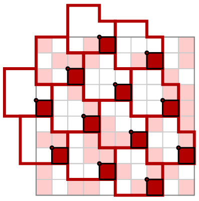


Thus the byte just below is 10001101 = 141.

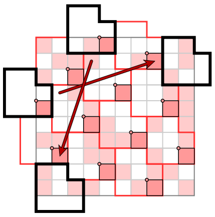


Bill Casselman is professor of mathematics at the University of British Columbia and graphics editor of the Notices. *His email address is* `cass@math.ubc.ca`.

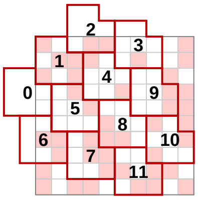
What I call the **origin pixel** is at lower right of the byte. Bytes are arranged so that one byte is packed in tightly at upper left, and then the rest spread out from there on the lattice spanned by vectors $[2, -2]$ and $[3, 1]$.



For this particular size of data matrix, bytes are in bijection with their origin pixels inside the symbol. Since $100 = 10 \cdot 10$ is not divisible by 8, 4 pixels are ignored.



Bytes that do not fit inside the symbol wrap around on the other side, with a shift as indicated by arrows in the diagram below.



Bytes are numbered up and down along diagonals, starting at upper left.

What do we do with the bytes we can now read? There are 12 altogether, and the data matrix specification tells us that 7 of them are added at the end according to the ECC200 coding scheme, which is based on a Reed-Solomon code using the Galois field $\mathbb{F}_{256}$. This leaves 5 in the actual message: 84, 157, 171, 130, 129. There are several modes of interpretation of bytes, but this one is in the simplest ASCII mode.

The last byte 129 marks the end of the message (and would begin a padding sequence if the message didn't take up all available space). Bytes in the range $[1, 128]$ are ordinary ASCII characters shifted up by 1, so 84 represents **S**. Bytes in the range $[130, 229]$ represent integers in the range 0-99, so the sequence 157, 171, 130 represents 27, 41, 0. But now I have to say I have no idea what "S 27 41 0" means. Presumably it is expressed in some code known to packagers and distributors and provides an example of coding for compression rather than security. By contrast, in the Canadian postage stamp roughly 3/4 of the 174 message bytes are devoted to digital keys.

References

The only comprehensive reference in print that I know of is the book

Electronic Postage Systems: Technology, Security, Economics, Gerrit Bleumer, Springer, 2007.

It is mostly concerned with how cryptography is employed in postal systems. As far as low-level reading of data matrix symbols goes, one thing that is presumably essential for professional work is the ISO specification, which you can find by searching for ISO/IEC 16022-2006 at

`http://www.iso.org/iso/`

but it costs real money (224 Swiss francs!), and I have not seen it. The Wikipedia entry for **data matrix** at

`http://en.wikipedia.org/wiki/`
`Data_ matrix`

is helpful, but doesn't have much detail. The webpage

`http://www.bcgen.com/`
`datamatrix-barcode-creator.html`

has an interactive application that will allow you to create data matrix symbols from text you type in. As far as technical details are concerned, links to pages on data matrices can be found on

`http://grandzebu.net/`.

Follow links to the English version of bar codes, then to "data matrix". Another good source of information is

`http://www.libdmtx.org/`

which will allow you to obtain C++ code for reading and writing data matrices. This combined with the `grandzebu` site makes a fairly practical source for programming.

The 12 × 12 symbol on the ice cream carton has analogues on other groceries, as you can see at

`http://www.flickr.com/photos/nickj365/`

Is there a single company ultimately responsible for this phenomenon?

The Feature Column of the AMS (`http://www.ams.org/featurecolumn`) for February 2010 covered this topic in more detail.

Book Review

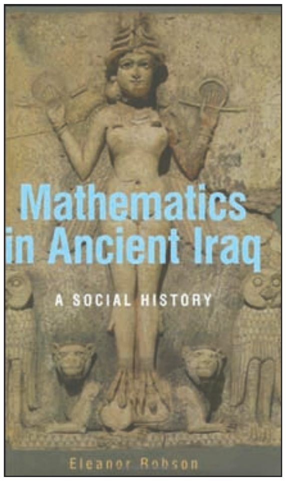
From Numerate Apprenticeship to Divine Quantification

Reviewed by Peter Damerow

Mathematics in Ancient Iraq: A Social History
Eleanor Robson
Princeton University Press, 2008,
US$49.50, 472 pages
ISBN-13: 978-0691091822

To make it clear from the very beginning, Eleanor Robson's book *Mathematics in Ancient Iraq* is presently unique and will surely become a classic in the history of early mathematics. Despite the meticulous and detailed presentation of a representative selection of available sources, the book is very readable and captures the attention of the interested reader from the first to the last page. I recommend it to anyone who would like to learn something about the fascinating story of the development of mathematical activities in Mesopotamia, from its roots in bookkeeping practices at the beginning of the third millennium BCE to the divine quantification practiced by the educated scholarly priests of the declining Babylonian culture about 3,000 years later in the Hellenistic period founded by Alexander the Great.

This story deserves closer attention, not only because it sheds light on the origins of the long tradition of scholarly activities concerned with arithmetical problems, but also because it challenges the familiar understanding of mathematics in general. It is commonly assumed that mathematics deals with provable and therefore absolutely true knowledge, in contrast to empirical sciences, which provide knowledge that can always be disproved by new discoveries. The book makes evident that this understanding of mathematics is heavily biased by our access to the historical sources that contribute to our knowledge about its early history. The term "mathematics" is a Greek term, usually confounded with the notion of mathematical proof as introduced by Greek mathematicians. Up to the 1920s, any mathematical activity predating classical Antiquity was conceived as more or less based on empirically discovered patterns that were transformed into rules without justification by proof. When, around seventy years after the basic decipherment of cuneiform writing, it turned out that some of the thousands of cuneiform tablets unearthed at that time contained problems and their correct solutions, which could be interpreted as solutions of second-degree equations, the pioneers of the decipherment of these tablets coined the term "mathematical cuneiform texts". They maintained that such tablets represent a kind of "Babylonian algebra" from which Greek mathematics adopted a range of content and methods and transformed them into a geometrical conceptual framework.



While it is true that none of the mathematical cuneiform tablets discovered contained anything comparable with or similar to the Greek way of representing mathematical material by "theorem" and "proof", these tablets made evident that it was no longer reasonable to restrict the term "mathematics" to the specific Greek form of representation. For several decades, conflicting opinions of classicists and orientalists about the relation of Babylonian and Greek mathematics were vehemently expressed without any substantial progress. One of the reasons for the

Peter Damerow is a research scholar at the Max Planck Institute for the History of Science, Berlin. His email address is damerow@mpiwg-berlin.mpg.de

many fruitless debates was that what was indiscriminately designated by the term "Babylonian mathematics" incorporated neither deductive theories nor algebraic transformations in the modern sense. It is only due to recently pursued, careful philological studies and investigations of specific cultural contexts represented by archaeological evidence that we are able to achieve a better understanding of the intellectual background of the challenging mathematical cuneiform sources. This intellectual background is based partly on mental representations of geometrical relationships and partly on reflections about ingeniously designed arithmetical procedures.

This situation is the starting point of Eleanor Robson's eminent study. It is the first to combine the analysis of mathematical content with the results of recent philological and archaeological investigations in order to gain an extended reinterpretation of the conflicting traditional interpretation of available sources. Her profound knowledge of these investigations in combination with her mathematical competence make her statements truly reliable. Nearly all of her claims are justified by references to the publications on which they are based. The extensive bibliography documents this diligent attempt to produce a verifiable integration of what can be derived from the sources into a coherent picture of the origins and nature of mathematics in the ancient Near East. If the available evidence does not allow for a definite answer to a question, the alternative interpretations of the sources are usually made explicit, sometimes indicating an inclination to accept one or the other alternative.

In spite of the accuracy in presenting details of the development of early mathematics, the presentation is never boring. It always follows a clear line of argument, frequently interrupted only by a close reading of some challenging mathematical cuneiform tablets to reveal their genuine mathematical content. This way of discussing sources in order to substantiate general claims is applied in the introduction (called "Scopes, Methods, Sources"), which specifies the scope of the study, the methods applied, and the range of sources on which the study is built. In this way the author's program is made understandable, even to readers who never have heard about mathematics documented by cuneiform tablets. A simple mathematical exercise concerning the squaring of a number is used to explain basic characteristics of the writing system, the system of numerical notations, the method of interpreting the written text as well as the use of archaeological information that may contribute to the reconstruction of the function of mathematical cuneiform tablets in the ancient social context of learning and applying mathematical techniques. Even this introduction can be considered to be a masterpiece of presenting complex information in an understandable and concise manner without losing its full meaning.

The succeeding chapters follow the course of historical development. The presentation begins with the earliest sources documenting enumeration and abstraction, dating back to the period before the mid-third millennium, and ends with mathematical and astronomical texts written in the later first millennium BCE, which represent the last blossoming of cuneiform culture before the end of local rule in Mesopotamia. This long history of approximately 3,000 years is divided roughly by the chapters of the book into periods of about 500 years each.

The second chapter, "Before the Mid-Third Millennium", starts with the incipient forms of any explicit mathematical activity beginning with the emergence of sedentary settlements around 10,000 BCE and ending around the middle of the third millennium, when early forms of writing and calculating were fully developed. The author identifies the origins of these administrative tools in techniques that were developed as an outcome of the emergence of sedentary settlements. The early settlers constructed dwellings and storerooms, indicating a long-term administration of domesticated plants and animals. It is likely that this social change from hunting and gathering to farming and animal husbandry was the condition for the invention of counters in the form of clay tokens with different shapes and incisions used as administrative tools. Beginning around the fifth millennium BCE, influenced by population growth and the emergence of increasingly large cities, the use of counters became complemented by further administrative tools such as cylinder seals, sealed tablets with impressions of styluses representing quantities, and sealed envelopes containing counters. Around 3000 BCE, the arsenal of tools at the disposal of the administrators of cities and city states was further enlarged by the invention of signs incised on clay tablets. These signs complemented the documentation of quantities by stylus impressions with means to indicate objects, agents, and institutions. Thus they initiated the development of a writing system representing the Sumerian language leading finally to the abstraction of arithmetical and geometrical notions.

In order to adequately conceptualize this development from incipient forms of mathematical activities and record-keeping to a numerate and literate urban culture, the author redefines the traditional concept of mathematics, which was based on the study of classical Greek mathematics. For her, scholarly mathematics is "an intellectual, supra-utilitarian end in itself, written for the purpose of communicating or recording a mathematical technique or aiding a mathematical procedure to be carried out in the course of scribal training" to be distinguished from "numeracy as the routine application of mathematical skills by professional scribes" (pp. 28f.). This definition implies that numerical activities performed in the context of scribal training, which do not directly serve administrative purposes but instead relate to the study and elaboration of their inherent potential in administrative contexts, have to be considered as mathematics. Accordingly, a specific focus of the chapter is the identification and analysis of "pedagogical exercises", in contrast to sources documenting actual accounting practices.

The third chapter, "The Later Third Millennium", focuses on the origins of what was probably the most influential innovation in southern Mesopotamia to foster the development of Babylonian mathematics, i.e., the invention of the sexagesimal place value system. Before this invention, all mathematical activities in Mesopotamia were based on commodity-specific metrological notations and context-dependent symbolic operations. Robson documents in this chapter how the administrative needs of developing empires led to the expansion, standardization, and integration of metrological systems and the development of ever more sophisticated methods of predicting and managing the storage and distribution of commodities, the allocation of labor, and the distribution of arable land. This development eventually resulted in the invention of an abstract numerical notation system, the sexagesimal place value system, which brought about a radical unification and simplification of all kinds of calculation as applied by the scribes of the state bureaucracy. Almost nothing is known about the training of the enormous number of scribes, who are known from the tens of thousands of preserved administrative documents dating to the period of the third dynasty of Ur when, during the last one hundred years of the third millennium, the rulers of this dynasty temporarily integrated all city states of Mesopotamia into one huge empire. Robson suggests that this missing evidence indicates that scribal education in this period was still realized by a kind of apprenticeship, a kind of learning through participation in administrative activities, as is attested for the earlier Sargonic period.

Chapter Four, "The Early Second Millennium", deals with the outstanding product of the Old Babylonian scribal culture that followed, conventionally designated as Babylonian mathematics. This kind of mathematics is represented by some 700 cuneiform tablets containing—besides lists, tables, diagrams, and calculations—some 150 tablets containing hundreds of mathematical problems and their numerical solutions, which differ from all earlier cuneiform tablets documenting mathematical activities. Among them are tablets with sophisticated mathematical exercises, for example finding a number that exceeds its reciprocal by 7 (pp. 113–115), which implicitly require the resolution of second-degree equations. The way such mathematical knowledge was represented and how the solutions to such problems were achieved differs from the kind of mathematics for which Euclidean geometry became a prominent paradigm, as well as from the methods of modern symbolic algebra. In the present case, for instance, the number 5 is calculated as the solution. This shows that the product of a number and its reciprocal is assumed not to be 1 but 60—i.e., the base of the sexagesimal positional system. This example indicates that sexagesimal notation represents entities that were not considered to be absolute numbers in the modern sense.

Following the work of Jens Høyrup, the author argues that the terminology used in the calculation of the result suggests that the solution is based on the mental image of a field with the area 60, and that the calculation procedure reflects some mentally performed cut-and-paste operations for which the calculation was a generic outcome.

While such problems were obviously somehow derived from the mathematical methods developed in the context of administrative practices of the state bureaucracies, it goes without saying that problems such as the given example no longer had any practical value within this context. Robson focuses in Chapter Four on the question of what might explain the development from the mathematical activities of practitioners to mathematics as a kind of esoteric art. She writes:

"While the invention of the sexagesimal place value system was a necessary condition for the creation of mathematics as an intellectual activity, divorced from the mundane necessities of central administration, the sexagesimal place value system alone is not sufficient to explain that extraordinary development." (p. 123)

In order to figure out what might explain this development, the author goes beyond the mathematical analysis of the texts. She also pays close attention to their linguistic, material, and social context in an educational environment that brought about specific numeracy and literacy in the Old Babylonian period. She investigates the archaeological context of the findings, the social context of learning that then took place in schools, the social function of the competence achieved in these schools, the material that defined the curriculum of the education system, the way in which the contents of the curriculum were perceived, and the consequences of an education establishing a "royal ideology" (p. 124) among the administrators of the first empires in the region of ancient Iraq. In her conclusion she writes:

"Thus, while modern scholars have chosen to portray Old Babylonian literature and mathematics as amongst the world's first truly creative and non-utilitarian writings (…) for their producers and consumers they represented above all idealised abstractions of the ordered urban state, with god, king, and scribe at its centre." (p. 124)

The short Chapter Five, "Assyria", sidesteps to a certain extent the chronological sequence of the main chapters. In this chapter Robson discusses the often neglected development of mathematical activities in the region commonly designated as Assyria in the northern parts of the rivers Euphrates and Tigris. Highly influenced by cultural traditions of the south, this development is an example of the diffusion of knowledge in the wake of the spreading of writing. In a spirit of "fascination with Babylonian intellectual culture" (pp. 149f), Assyria adopted techniques of administrative control together with related mathematical activities, as well as ideological notions such as the ideal of metrological justice. However, the transmission of knowledge from the south to the north involved adaptations to local conditions that in particular resulted in "a rather different flavour" as she puts it (p. 125). These differences resulted, for instance, from the fact that in the northern region merchants played a more important role than administrators of a centralized bureaucracy. As a consequence, no institutions comparable to the Old Babylonian scribal schools developed at this time in this region. Moreover, in addition to the imported sexagesimal notations, a decimal numerical notation system was used in this region, reflecting the decimal counting system of Semitic languages. Therefore, calculations had to be performed taking into account a hybridization of both systems.

The sixth chapter, "The Later Second Millennium", returns from the geographical digression of the preceding chapter to the chronological presentation of the development of mathematical activities. Archaeological evidence of the survival of the scribal culture of the Old Babylonian kingdom after its decline is scarce. On the other hand, the spreading of cuneiform writing and its adaptation to other languages such as Hittite, accompanied by the diffusion of knowledge transmitted by means of writing such as sexagesimal numeracy, reached a climax, especially in this period. The expansion of the influence of knowledge based on Babylonian origins can be traced by archaeological findings to places as far as the eastern Mediterranean coast, Anatolia, Syria, the southwest of Iran, and Egypt.

This chapter assembles the poor evidence of the scribal culture and in particular of mathematical activities in the heartland of Babylonia, showing that there was a continuity of reproducing, transmitting, and disseminating mathematical techniques, even in the so-called dark age of Babylonian culture and the ensuing occupation of the southern plain by people of Kassite ethnicity invading from an Iranian region east of the Zagros mountains. It turns out that substantial parts of Old Babylonian numeracy survived, although the political ideology that supported it was tending to disappear. The author discusses in particular the extensive innovations developed by scribes of southern Babylonia in the preceding Old Babylonian period based probably on some poorly attested earlier attempts—that is to say, the use of a tabular accounting technique. She furthermore discusses the work of northern Babylonian land surveyors who adopted the surveying methods of the south. This work is known as well from cuneiform tablets documenting the results of the surveying practice as also from a considerable number of extant so-called Kudurrus—i.e., stelae that contain monumental copies of legal documents concerning royal grants of land to courtiers or other high-ranking officials.

The seventh chapter, "The Early First Millennium", deals with a period in which Babylonia came under Assyrian control, followed by a period of Babylonian control over Assyria, and ending with the conquest by the Achaemenid Persians. Again, for this period documents related to mathematical activities are rare. Robson, however, assumes that the available evidence may at least partly be enriched in the future when the numerous excavated but still unpublished cuneiform tablets from the first millennium, now located in museums and archives, are made accessible. But even the scanty evidence available so far shows that scribal education was gradually revived, ending with a formalized curriculum in spite of the political turmoil at this time. Basic metrology and numerical knowledge related to its use in practical contexts were part of this education, which otherwise lacked the sophisticated characteristic of Babylonian mathematics as created in the Old Babylonian period. This is demonstrated in the chapter using two examples that are documented by documents from this period. The first example is the use of numeracy in urban household archives; the second is the calculation methods of land surveyors. Moreover, a few surviving examples of school exercises documenting the revival of a formalized education system are presented, and their relation to administrative practices is extensively discussed.

Chapter Eight deals with the final time period covered by the book, that is "The Later First Millennium", which according to Robson can be characterized by a growing erosion of the indigenous Babylonian culture due to Greek and Iranian influences on the one hand, and on the other by a last blossoming of cuneiform culture, in which scholarly mathematics and a newly created mathematical astronomy were central components. The surviving tablets from this period show the same intellectual complexity as their Old Babylonian ancestors but are complemented with an unprecedented application of arithmetical knowledge to systematically collected empirical data about astronomical events. This Babylonian astronomy constitutes probably the oldest empirical science based on systematic observation and measurement, integrated with inductively achieved rules. By contrast, the available sources seem to indicate that at the same time numeracy as a professional skill of scribes lost its importance. As a hypothesis, the author suggests that Babylonian mathematics underwent a major conceptual shift in the period between the fifth century BCE and the mature Hellenistic period, indicated by a "dramatic rethinking of the status of number". According to this assumption numeracy lost its close ties to administrative practices and became considered "as an entity in its own right (to) be accounted for" (p. 261). Correspondingly, the locus of intellectual mathematical activities moved from the practitioners in institutions of a central economical administration to the age-old temples, which became widely independent of royal patronage. Babylonian mathematics, according to this assumption, no longer served predominantly practical purposes but religious ones instead and diminished with the decline of this intellectual tradition in the Hellenistic period.

The book ends with an extensive "Epilogue", drawing a "big picture" (p. 263) of three millennia of the development of Babylonian mathematics. Robson derives as a conclusion from her meticulous investigation of this development that three phases can be distinguished, characterized by numerate apprenticeship, metrological justice, and divine quantification. The actors practising Babylonian mathematics, the problems they were dealing with, and the methods they applied changed accordingly.

In the first phase of numerate apprenticeship "a small cadre of bureaucrats managed the domestic economics of big institutions" (p. 263). They developed for this purpose complex standardized metrologies and used them to control the flow of commodities by symbolic means. For all we know, the professional knowledge of these bureaucrats was transmitted from one generation to the next by apprenticeship and participation in administrative practices.

The situation changed with the occurrence of the first empires, in particular with the rise of the empire of the Third Dynasty of Ur at the end of the third millennium BCE. The standardization and unification of metrology supported the development of an ideology of metrological justice as the divine goal of bureaucracy. The author writes: "It is probably at this time that pedagogical curricula began to be formalised […]. Increased numbers of bureaucrats were needed, who had to be trained in consistent transterritorial accounting methods and in writing Sumerian, the language of bureaucracy and state" (p. 265). Thus, systematic training in school-like institutions replaced the small-scale education by apprenticeship of the earlier period of bookkeeping.

The situation changed again with the Assyrian, Neo-Babylonian, Persian, and Seleucid empires of the first millennium BCE. Empirically based astronomy was created in accordance with a growing need by the rulers to foresee the future by determining the will of the gods and acting in accordance with their wishes. Mathematics was conceived of in terms of divine quantification. Astronomical observations played an increasing role in omens foretelling the future, and arithmetical techniques became a major instrument for predicting astronomical events from observed data. Accordingly, in this last phase of cuneiform literacy, mathematics developed into a matter of priestly concern. Robson writes: "The secret knowledge of mathematics, astronomy, and ritual was communicated through apprenticeship within a tightly restricted social circle, either down the bloodline or between male members of a tiny number of families […]. These men resisted the allure of newfangled Persian and Hellenistic culture, clinging to the old ways of belief while constantly renewing and improving their mathematical methodologies" (p. 268).

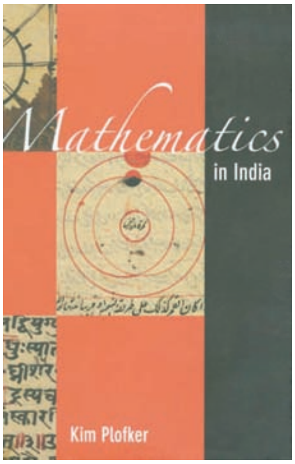
This "big picture" of three millennia of the development of Babylonian mathematics is not the only content of the epilogue. It is followed by an outline of the rediscovery and reappraisal of ancient mathematics in the modern world. Robson maintains that misinterpretations of Babylonian mathematics in the standard literature on the history of mathematics result from the chronology of decipherment: Babylonian mathematics similar to mathematical activities of other ancient non-Greek cultures was studied only when ancient Greek mathematics had long achieved the status of representing the origins of mathematics per se. Therefore, mathematical activities of other ancient cultures were widely neglected or interpreted as being deficient if compared with the Greek style. For readers who are unaware of the dramatic changes of our understanding of non-Greek ancient mathematics in recent decades, Robson ends the epilogue with a glimpse of the fascinating story of the development of our modern understanding of Babylonian mathematics, from the enthusiasm of the pioneers of its decipherment to the integration of our current knowledge, leading to the composition of her book.

Admittedly, the book does not provide "a definitive history of mathematics and numeracy in and around ancient Iraq" (p. 263). It should rather be considered as a first attempt to meet "the need to break down the monolithic twentieth-century construction of Babylonian (or Mesopotamian or cuneiform) mathematics into more historically manageable pieces" (p. 288). Numerous tables listing specific groups of sources and providing tools to study them invite scholars to join the program she has sketched with her publication.

Book Review

Mathematics in India

Reviewed by David Mumford



Mathematics in India
Kim Plofker
Princeton University Press, 2008
US$39.50, 384 pages
ISBN-13: 978-0691120676

Did you know that Vedic priests were using the so-called Pythagorean theorem to construct their fire altars in 800 BCE?; that the differential equation for the sine function, in finite difference form, was described by Indian mathematician-astronomers in the fifth century CE?; and that "Gregory's" series $\pi/4 = 1 - \frac{1}{3} + \frac{1}{5} - \cdots$ was proven using the power series for arctangent and, with ingenious summation methods, used to accurately compute π in southwest India in the fourteenth century? If any of this surprises you, Plofker's book is for you.

Her book fills a huge gap: a detailed, eminently readable, scholarly survey of the full scope of Indian[1] mathematics and astronomy (the two were inseparable in India) from their Vedic beginnings to roughly 1800. There is only one other survey, Datta and Singh's 1938 *History of Hindu Mathematics*, recently reprinted but very hard to obtain in the West (I found a copy in a small specialized bookstore in Chennai). They describe in some detail the Indian work in arithmetic and algebra and, supplemented by the equally hard to find *Geometry in Ancient and Medieval India* by Sarasvati Amma (1979), one can get an overview of most topics.[2] But the drawback for Westerners is that neither gives much historical context or explains the importance of astronomy as a driving force for mathematical research in India. While Western scholars have been studying traditional Indian mathematics since the late eighteenth century and Indian scholars have been working hard to assemble and republish surviving Sanskrit manuscripts, a widespread appreciation of the greatest achievements and the unique characteristics of the Indian approach to mathematics has been lacking in the West. Standard surveys of the history of mathematics hardly scratch the surface in telling this story.[3] Today, there is a resurgence of activity in this area both in India and the West. The prosperity and success of India has created support for a new generation of Sanskrit scholars to dig deeper into the huge literature still hidden in Indian libraries. Meanwhile the shift in the West toward a multicultural perspective has allowed us Westerners to shake off old biases and look more clearly at other traditions. This book will go a long way to opening the eyes of all mathematicians and historians of mathematics to the rich legacy of mathematics to which India gave birth.

The first episode in the story of Indian mathematics is that of the *Śulba-sūtras*, "The rules of the cord", described in section 2.2 of Plofker's book.[4]

David Mumford is professor of applied mathematics at Brown University. His email address is `david_mumford@brown.edu`.

[1] *The word "India" is used in Plofker's book and in my review to indicate the whole of the Indian subcontinent, including especially Pakistan, where many famous centers of scholarship, e.g., Takshila, were located.*

[2] *For those who might be in India and want to find copies, Datta and Singh's book is published by Bharatiya Kala Prakashan, Delhi, and Amma's book by Motilal Banarsidass, Delhi. An excellent way to trace the literature is through Hayashi's article "Indian mathematics" in the AMS's CD* History of Mathematics from Antiquity to the Present: A Selective Annotated Bibliography *(2000).*

[3] *The only survey that comes close is Victor Katz's* A History of Mathematics.

[4] *There are multiple ways to transcribe Sanskrit (and Hindi) characters into Roman letters. We follow the precise scholarly system, as does Plofker (cf. her Appendix A) which uses diacritical marks: (i) long vowels have a bar over them; (ii) there are "retroflex" versions of t, d, and n where the tongue curls back, indicated by a dot beneath the letter; (iii) h, as in th, indicates aspiration, a breathy sound, not the English "th"; and (iv) the "sh" sound is written either as ś or as ṣ (the two are distinguishable to Indians but not native English speakers).*

These are part of the "limbs of the Vedas", secular compositions[5] that were orally transmitted, like the sacred verses of the Vedas themselves. The earliest, composed by Baudhāyana, is thought to date from roughly 800 BCE. On the one hand, this work describes rules for laying out with cords the sacrificial fire altars of the Vedas. On the other hand, it is a primer on plane geometry, with many of the same constructions and assertions as those found in the first two books of Euclid. In particular, as I mentioned above, one finds here the earliest explicit statement of "Pythagorean" theorem (so it might arguably be called Baudhāyana's theorem). It is completely clear that this result was known to the Babylonians circa 1800 BCE, but they did not state it as such—like all their mathematical results, it is only recorded in examples and in problems using it. And, to be sure, there are no justifications for it in the *Śulba-sūtras* either—these sutras are just lists of rules. But Pythagorean theorem was very important because an altar often had to have a specific area, e.g., two or three times that of another. There is much more in these sutras: for example, Euclidean style "geometric algebra", very good approximations to $\sqrt{2}$, and reasonable approximations to π.

Another major root of Indian mathematics is the work of Pāṇini and Piṅgala (perhaps in the fifth century BCE and the third century BCE respectively), described in section 3.3 of Plofker's book. Though Pāṇini is usually described as the great grammarian of Sanskrit, codifying the rules of the language that was then being written down for the first time, his ideas have a much wider significance than that. Amazingly, he introduced abstract symbols to denote various subsets of letters and words that would be treated in some common way in some rules; and he produced rewrite rules that were to be applied recursively in a precise order.[6] One could say without exaggeration that he anticipated the basic ideas of modern computer science. One wishes Plofker had described Pāṇini's ideas at more length. As far as I know, there is no exposition of his grammar that would make it accessible to the non-linguist/Sanskrit scholar. P. P. Divakaran has traced the continuing influence of the idea of recursion on Indian mathematics,[7] leading to the thesis that this is one of the major distinctive features of Indian mathematics.

Piṅgala, who came a few centuries later, analyzed the prosody of Sanskrit verses. To do so, he introduced what is essentially binary notation for numbers, along with Pascal's triangle (the binomial coefficients). His work started a long line of research on counting patterns, including many of the fundamental ideas of combinatorics (e.g., the "Fibonacci" sequence appears sometime in 500-800 CE in the work of Virahānka). There is an interesting treatment of this early period of Indian mathematics in Frits Staal's excellent recent book *Discovering the Vedas*,[8] ch.14. For example, Staal traces recursion back to the elaborate and precise structure of Vedic rituals.

After this period, unfortunately, one encounters a gap, and very little survives to show what mathematicians were thinking about for more than 500 years. This was the period of Alexander's invasion, the Indo-Greek Empire that existed side by side with the Mauryan dynasty including Aśoka's reign, and the Indo-Scythian and Kushan empires that followed. It was a period of extensive trade between India and the West, India and China. Was there an exchange of mathematical ideas too? No one knows, and this has become a rather political point. Plofker, I believe, does a really good job discussing the contentious issues, stating in section 4.6 the "consensus" view but also the other points of view. She states carefully the arguments on both sides and lets the reader take away what he or she will. She deals similarly with the early influences from the Middle East in section 2.5 and of the exchanges with the Islamic world in Chapter 8.

For my part, I follow my late colleague David Pingree, who trained a whole generation of scholars in ancient mathematics and astronomy. He argues that the early version of Greek astronomy, due to Hipparchus, reached India along with Greek astrology. The early Indian division of the ecliptic into twenty-eight *Nakṣatras*, (the moon slept with a different wife every night in each trip around the ecliptic) was replaced by the Greek zodiac of twelve solar constellations and—more to the point—an analysis of solar, lunar, and planetary motion based on epicycles appears full-blown in the great treatise, the *Āryabhaṭīya* of Āryabhaṭa, written in 499 CE. But also many things in the Indian treatment are totally different from the Greek version. Their treatment of spherical trigonometry is based on three-dimensional projections, using right triangles *inside* the sphere,[9] an approach

[5] *Technically, they are called* smṛti *("remembered text") as opposed to* śruti *("heard", i.e., from divine sources).*

[6] *To get a glimpse of this, see Plofker, p. 54; F. Staal, "Artificial languages across sciences and civilization",* J. Indian Philosophy*, pp. 89–141 (esp. sections 11–12), 2006; or B. Gillon, "Aṣṭādhyāyī and linguistic theory",* J. Indian Philosophy*, pp. 445–468, 2007.*

[7] *"Notes on Yukti-Bhāṣā: Recursive methods in Indian mathematics", forthcoming in a book entitled* Studies in the History of Mathematics in India.

[8] *Penguin Books, 2008.*

[9] *A basic formula in the Gola section of the* Āryabhaṭīya *is that if P is a point on the ecliptic with longitude λ, then the declination δ of P is given by* $\sin(\delta) = \sin(\lambda).\sin(i)$, *$i$ the inclination of the ecliptic. If I understand it right, later writings suggest this was proven by considering the planar right triangle given by P, P_1, P_2, where P_1 is the orthogonal projection of P onto the plane of the equator (inside the sphere!) and P_2 is its projection onto the line*

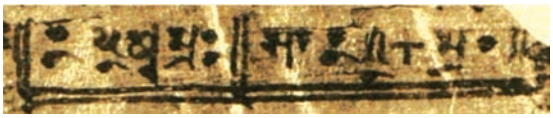
which I find much simpler and more natural than Ptolemy's use of Menelaus's theorem. Above all, as mentioned above, they found the finite difference equation satisfied by samples $\sin(n.\Delta\theta)$ of sine (see Plofker, section 4.3.3). This seems to have set the future development of mathematics and astronomy in India on a path totally distinct from anything in the West (or in China).

It is important to recognize two essential differences here between the Indian approach and that of the Greeks. First of all, whereas Eudoxus, Euclid, and many other Greek mathematicians created pure mathematics, devoid of any actual numbers and based especially on their invention of indirect *reductio ad absurdum* arguments, the Indians were primarily applied mathematicians focused on finding algorithms for astronomical predictions and philosophically predisposed to reject indirect arguments. In fact, Buddhists and Jains created what is now called Belnap's four-valued logic claiming that assertions can be true, false, neither, or both. The Indian mathematics tradition consistently looked for *constructive arguments and justifications and numerical algorithms.* So whereas Euclid's *Elements* was embraced by Islamic mathematicians and by the Chinese when Matteo Ricci translated it in 1607, it simply didn't fit with the Indian way of viewing math. In fact, there is no evidence that it reached India before the eighteenth century.

Secondly, this scholarly work was mostly carried out by Brahmins who had been trained since a very early age to memorize both sacred and secular Sanskrit verses. Thus they put their mathematics not in extended treatises on parchment as was done in Alexandria but in very compact (and cryptic) Sanskrit verses meant to be memorized by their students. What happened when they needed to pass on their sine tables to future generations? *They composed verses of sine differences*, arguably because these were much more compact than the sines themselves, hence easier to set to verse and memorize.[10] Because their tables listed sines every 3.75 degrees, these first order differences did not closely match the sine table read backward; but the second differences were almost exactly a small negative multiple of the sines themselves, and this they noticed.

There are several excellent recent books that give more background on these early developments. The mathematical sections of the *Āryabhaṭīya* with the seventh century commentary on it by Bhāskara (I) and an extensive modern commentary, all entitled *Expounding the Mathematical Seed*, has been published[11] in English by Agathe Keller. One hopes she will follow this with an edition of the astronomical chapters. And Glen van Brummelen has written a cross-cultural study of the use of trigonometry, entitled *The Mathematics of the Heavens and the Earth*,[12] which compares in some detail Greek and Indian work.

Chapters 5 and 6 of Plofker's book, entitled *The Genre of Medieval Mathematics* and *The Development of "Canonical" Mathematics*, are devoted to the sixth through twelfth centuries of Indian mathematical work, starting with Āryabhaṭa and ending with Bhāskara (also called Bhāskara II or Bhāskaracharya, distinguishing him from the earlier Bhāskara). This was a period of intense mathematical-astronomical activity from which many works have survived, and I want to touch on some of its high points. We find already in the seventh century the full arithmetic of negative numbers in Brahmagupta's *Brāhmasphuṭa-siddhānta* (see Plofker, p. 151). This may sound mundane but, surprisingly, nothing similar appears in the West until Wallis's *Algebra* published in 1685.[13] And in the *Bakhshālī* manuscript, an incredibly rare birch bark manuscript unearthed by a farmer's plow in 1881, we find algebraic equations more or less in the style of Viète, Fermat, and Descartes. It is incomplete and neither title nor author survives, but paleographical evidence suggests that it was written between the eighth and twelfth centuries, and Hayashi argues that its rules and examples date from the seventh century.[14] The manuscript puts equations in boxes, like our displayed formulas. On p. 159 of Plofker's book, she gives the example from bark fragment 59. The full display in the original is below.



0	5	yu	mū	0	sā	0	7	+	mū	0
1	1			1		1	1			

Here the 0's (given by solid dots in the manuscript) stand for unknowns, the 1's (given by the sigma-like subscripted symbols in the manuscript)

through ♈, the intersection of the equator and the ecliptic. It is immediate to derive the formula using this triangle.

[10] Using $R = 3438$, the number of minutes in a radian to the nearest integer, and $\Delta\theta = 3.75$ degrees, they calculated $R \cdot \sin(n\Delta\theta)$ to the nearest integer.

[11] Springer-Verlag, 2008, for an obscene price of $238!!

[12] Princeton University Press, 2009.

[13] For example, both Cardano and Harriot were unsure whether to make $(-1) \cdot (-1)$ equal to -1 or $+1$.

[14] See the fully edited and commented edition by Takao Hayashi, The Bakhshali Manuscript: An Ancient Indian Mathematical Treatise, *John Benjamin Pub. Co., 1995.*

are just denominators, the *yu* means 5 is added to the unknown on its left, + sign signifies that 7 is subtracted, *mū* means square root, and *sā* is a pronoun indicating that the 1st and 3rd unknowns are equal. The whole thing has the modern equivalent:

$$\sqrt{x+5} = w, \quad \sqrt{x-7} = z.$$

This is to be solved in integers, giving $x = 11$. Note, however, that the Bakhshālī manuscript does not solve its problems using manipulations of its equations. In Brahmagupta's treatment of algebra in the *Brāhma-Sphuṭa-Siddhānta*, distinct colors are used to represent distinct unknowns (see Plofker's discussion of his Chapter 18, pp. 149–157).

The use of negative numbers to represent points on a line to the left of a base point appears in Bhāskara's *Līlāvatī*. This twelfth-century book, described in section 6.2.1 of Plofker's book, is arguably the most famous of all Indian texts on mathematics. Given the fact that *Līlāvatī* literally means "beautiful" or "playful" and that many verses are addressed to "the fawn-eyed one", the conjecture made by a Persian translator that the book was written to explain mathematics to Bhāskara's daughter seems quite reasonable.

Another basic tool which appears in all Indian manuscripts is what they called the pulverizer. This is an extension of the Euclidean algorithm, the idea of starting with two positive integers and repeatedly subtracting the lesser from the greater. They go further than Euclid in using this to systematically write down all solutions of first-order integer equations $ax + by = c$. It seems unlikely that the Greek algorithm, embedded in the *Elements* in highly abstract form, was transmitted to India, hence more likely that the idea was discovered independently in India. In fact, Indian astronomers had a very pressing application for this algorithm. Although they had, in fact, abandoned almost all of the ancient Vedic astronomy, they were not happy doing this and they retained one startling idea from that tradition: the vast epochs into which the past was divided, the yugas, all had to begin with one spectacular conjunction of the sun, the moon, and all the planets. To ascertain when the present yuga began and thus put future predictions on a sound basis, they had to solve such integer equations involving the periods of the heavenly bodies.

There are other high points of the work of this period. One of them is Brahmagupta's formula for the area of a quadrilateral inscribed in a circle. How he discovered this is a fascinating question. No justification has been found in any manuscripts earlier than the Kerala work (see below). It can be derived from Pythagorean theorem and simple geometry but only with substantial algebraic computation. Did Brahmagupta use algebra, manipulations of algebraic equations, to find it or not? That he gives many quite complex auxiliary results on cyclic quadrilaterals suggests he played with such quadrilaterals extensively.[15]

Indian work on Pell's equation in the general form $x^2 - Ny^2 = c$ also goes back to Brahmagupta. He discovered its multiplicative property—solutions for c_1 and c_2 can be "multiplied" to give one for c_1c_2 (Plofker, pp. 154-156). A complete algorithm, known as the "cyclic method", for constructing a solution to the basic equation $x^2 - Ny^2 = 1$ was discovered by Jayadeva, whose work is dated indirectly to the eleventh century (Plofker, pp. 194-195). Note again the emphasis on construction instead of indirect proofs of existence, which are the staple of our treatment of the subject.[16] Why such a focus on this equation? One idea is that if x, y is a solution, then x/y is a good approximation to $\sqrt{N}$.

The discovery of the finite difference equation for sine led Indian mathematicians eventually to the full theory of calculus for polynomials and for sine, cosine, arcsine, and arctangent functions, that is, for everything connected to the circle and sphere that might be motivated by the applications to astronomy. This work matured over the thousand-year period in which the West slumbered, reaching its climax in the work of the Kerala school in the fourteenth to sixteenth centuries. I won't describe the full evolution but cannot omit a mention of the discovery of the formula for the area and volume of the sphere by Bhāskara II. Essentially, he rediscovered the derivation found in Archimedes' *On the Sphere and the Cylinder I*. That is, he sliced the surface of the sphere by equally spaced lines of latitude and, using this, reduced the calculation of the area to the integral of sine. Now, he knew that cosine differences were sines but, startlingly, he integrates sine by summing his tables! He seems well aware that this is approximate and that a limiting argument is needed but this is implicit in his work. My belief is that, given his applied orientation, this was the more convincing argument. In any case, the argument using the discrete fundamental theorem of calculus is given a few centuries later by the Kerala school, where one also finds explicit statements on the need for a limiting process, like: "The greater the number [of subdivisions of an arc], the more accurate the circumference [given by the length of the inscribed polygon]" and "Here the arc segment has to be imagined to be as small as one wants... [but] since one has to explain [it] in a certain [definite] way, [I] have said [so far] that a quadrant has twenty-four chords."

[15] *Added in proof: I just received a copy of S. Kichenassamy's article "Brahmagupta's derivation of the area of a cyclic quadrilateral",* Historia Mathematica, *2009.*

[16] *See, e.g., Artin's* Algebra, *Prentice-Hall, 1991, pp. 434-437.*

Chapter 7 of Plofker's book is devoted to the crown jewel of Indian mathematics, the work of the Kerala school. Kerala is a narrow fertile strip between the mountains and the Arabian Sea along the southwest coast of India. Here, in a number of small villages, supported by the Maharaja of Calicut, an amazing dynasty[17] of mathematicians and astronomers lived and thrived. A large proportion of their results were attributed by later writers to the founder of this school, Madhava of Sangamagramma, who lived from approximately 1350 to 1425. It seems fair to me to compare him with Newton and Leibniz. The high points of their mathematical work were the discoveries of the power series expansions of arctangent, sine, and cosine. By a marvelous and unique happenstance, there survives an informal exposition of these results with full derivations, written in Malayalam, the vernacular of Kerala, by Jyeṣṭhedeva perhaps about 1540. This book, the *Gaṇita-Yukti-Bhāṣā*, has only very recently been translated into English with an extensive commentary.[18] As a result, this book gives a unique insight into Indian methods. Simply put, these are recursion, induction, and careful passage to the limit.

I want to give one example in more detail, the derivation of the power series expansion for sine. It seems most transparent to explain the idea of the proof in modern form and then to indicate how Jyeṣṭhadeva's actual derivation differed from this. The derivation is based on the integral equation for sine:

$$\begin{aligned}\theta - \sin(\theta) &= \int_0^\theta (1-\cos(\beta))d\beta \\ &= \int_0^\theta \left(\int_0^\beta \sin(\alpha)d\alpha \right) d\beta = (K * \sin)(\theta) \\ &\qquad \text{where } K(x,y) = \max(0, x-y).\end{aligned}$$

Jyeṣṭhadeva uses a finite difference form of this equation using discrete samples of sine: he subdivides the arc $[0,\theta]$ into n "arc-bits" of size $\Delta\theta = \theta/n$ and, choosing a big radius R (like 3438, see above), he works with sampled "Rsines" $B_k = R \cdot \sin(k\Delta\theta)$ and also the "full chord" of the arc-bit: $2R\sin(\Delta\theta/2)$. Then, based on the formula for the second difference of sines which goes back to Aryabhata, he derives:

$$\begin{aligned}\theta - \sin(\theta) \approx bB_1 - B_n &= (2\sin(\Delta\theta/2))^2 \\ &\cdot ((B_1 + \cdots + B_{n-1}) + (B_1 + \cdots + B_{n-2}) \\ &\qquad + \cdots + (B_2 + B_1) + B_1).\end{aligned}$$

Note that the right-hand side is exactly the finite difference version of the double integral in the calculus version. Here is how Jyeṣṭhadeva expressed this formula (p. 97 of Sarma's translation; here "repeated summation" stands for the sum of sums on the right):

> Here, multiply the repeated summation of the Rsines by the square of the full chord and divide by the square of the radius. ... In this manner we get the result that when the repeated summation of the Rsines up to the tip of a particular arc-bit is done, the result will be the difference between the next higher Rsine and the corresponding arc. Here the arc-bit has to be conceived as being as minute as possible. Then the first Rsine difference will be the same as the first arc-bit. Hence, if multiplied by the desired number, the result will certainly be the desired arc.

He is always clear about which formulas are exact and which formulas are approximations. In the modern approach, one has the usual iterative solution to the integral equation $\theta - K*\theta + K*K*\theta - \cdots$, and you can work out each term here using the indefinite integrals $\int_0^y x^n dx = \frac{y^{n+1}}{n+1}$ resulting in the power series for sine. Jyeṣṭhadeva does the same thing in finite difference form, starting with $\sin(\theta) \approx \theta$, and recursively improving the estimate for sine by resubstitution into the left-hand side of the above identity. Instead of the integral of powers, he needs the approximate sum of powers, i.e., $\sum_{k=1}^n k^p = \frac{k^{p+1}}{p+1} + O(k^p)$, and he has evaluated these earlier (in fact, results like this go way back in Indian mathematics). Then repeated resubstitution gives the usual power series $\theta - \frac{\theta^3}{6} + \frac{\theta^5}{120} - \cdots$ for sine. I consider this argument to be completely correct, but I am aware that it is *not* a rigorous proof by modern standards. It can, however, be converted into such a proof by anyone with basic familiarity with ϵ,δ-techniques. I hope I have whetted your appetite enough so you will want to feast on the riches laid out in Plofker's book and the *Gaṇita-Yukti- Bhāṣā* itself.

It is very tempting to read the history of mathematics as a long evolution toward the present state of deep knowledge. I see nothing wrong with understanding the older discoveries in the light of what we know now—like a contemporary metallurgist analyzing ancient swords. Needham, the great scholar of Chinese science, wrote "To write the History of Science we have to take modern science as the yardstick—that is the only thing we can do—but modern science will change and the end is not yet." Nevertheless, it is much more satisfying, when reading ancient works, to know as

[17] *The names we know form an essentially linear sequence of teacher and student (sometimes son).*

[18] *Translated and edited by the late K. V. Sarma, with notes by K. Ramasubramanian, M. D. Srinivas, and M. S. Sriram, and published in India in 2008 by the Hindustan Book Agency at a price of $31 and distributed in the West by Springer for $199, a 640% markup.*

much as possible about the society in which these mathematicians worked, to know what mathematics was used for in their society, and how they themselves lived.

Chapter 1 in Plofker's book is an extensive introduction that gives vital background on the history and traditions from which all the Indian work sprang. A series of extremely helpful appendices provide basic facts about Sanskrit, a glossary of Sanskrit terms, and a list of the most significant Indian mathematicians with whatever basic facts about them are known (often distressingly little). In places she gives some literal translations such as those of numbers in the colorful concrete number system that uses a standard list of sets with well-known cardinalities, e.g., "In a *kalpa*, the revolutions of the moon are equal to five skies [0], qualities [3], qualities, five, sages [7], arrows [5]", which means 5,753,300,000 lunar months with the digits described backwards starting from the one's place. It is becoming more and more recognized that, for a good understanding of ancient writings, one needs *both* an extremely literal translation and one paraphrased so as to be clear in modern terms. In Sanskrit a literal translation of the complex compound words sometimes gives additional insight into the author's understanding (as well as the ambiguities of the text), so one wishes there were more places in this book where Plofker gave such literal translations without using modern expressions.

I have not touched on the astronomical side of the story. Suffice it to say that almost all treatises from the sixth century on deal with both astronomy and mathematics. To follow these, one needs a bit of a primer in geocentric astronomy, a vanishing specialty these days, and Plofker provides a very handy introduction in section 4.1. Just as in Indian mathematics, there is a steady increase in sophistication over the centuries, culminating in dramatic advances in Kerala. Most strikingly, Nīlakaṇṭha in the fifteenth century proposed a model in which the planets were moving in eccentric and inclined circles with respect to the mean sun moving in its ecliptic orbit—a "virtually" heliocentric model remarkably better than Ptolemy's.

It is high time that the full story of Indian mathematics from Vedic times through 1600 became generally known. I am not minimizing the genius of the Greeks and their wonderful invention of pure mathematics, but other peoples have been doing math in different ways, and they have often attained the same goals independently. Rigorous mathematics in the Greek style should not be seen as the only way to gain mathematical knowledge. In India, where concrete applications were never far from theory, justifications were more informal and mostly verbal rather than written. One should also recall that the European Enlightenment was an orgy of correct and important but semirigorous math in which Greek ideals were forgotten. The recent episodes with deep mathematics flowing from quantum field and string theory teach us the same lesson: that the muse of mathematics can be wooed in many different ways and her secrets teased out of her. And so they were in India: read this book to learn more of this wonderful story!

Interview with Mikhail Gromov

Martin Raussen and Christian Skau

Mikhail Gromov is the recipient of the 2009 Abel Prize of the Norwegian Academy of Science and Letters. On May 18, 2009, prior to the Abel Prize celebration in Oslo, Gromov was interviewed by Martin Raussen and Christian Skau. This interview originally appeared in the September 2009 issue of the *Newsletter of the European Mathematical Society* and is reprinted here with permission.

A Russian Education

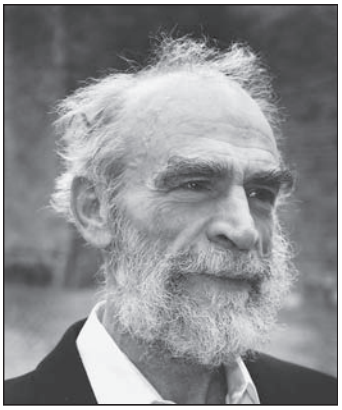
Raussen and Skau: *First of all, we would like to congratulate you warmly for having been selected as the 2009 Abel Prize winner. We would like to start with some questions about your early years and your early career. You were born towards the end of World War II in a small town called Boksitogorsk, 245 km east of St. Petersburg (at that time Leningrad).*

Gromov: My mother was a medical doctor in the fighting army—and to give birth at that time, she had to move a little away from the frontline.

Raussen and Skau: *Could you tell us about your background, your early education, and who or what made you interested in mathematics?*

Gromov: My first encounter with mathematics besides school was a book my mother bought me called *Numbers and Figures* by Rademacher and Toeplitz, which had a big influence on me. I could not understand most of what I was reading but I was excited all the same. I still retain that excitement by all the mysteries that you cannot understand but that make you curious.

Raussen and Skau: *Did you know you would go into mathematics while at high school?*



Mikhail Gromov

Photo by Knut Falch/Scanpix, for the Abel Prize, the Norwegian Academy of Science and Letters.

Gromov: In my middle and later years at high school I was more interested in chemistry than in mathematics. But then I was hooked. There were some very good books in Russia on mathematical problems for youngsters. I was going through them and I immersed myself in all this for a year. In my last year of high school I was attending a so-called mathematics circle, something for youngsters at the university, run by two people, Vasia Malozemov and Serezha Maslov (Maslov became a logician; coincidentally, he was the one who suggested Hilbert's tenth problem to Matiasevic). They were running an extremely good group for young children that I attended. This was in St. Petersburg in 1959, the year before I started at university, and it was the major reason for my decision to study mathematics.

Raussen and Skau: *You started studying mathematics at Leningrad University. Please tell us about the environment there, how you were brought up mathematically and about the teachers who were important for you.*

Gromov: I think it was a pleasant environment despite the political surroundings, which were rather unpleasant. There was an extremely high spirit in the mathematical community and among professors. I remember my first teachers, including Professor Isidor Pavlovich Natanson, and also I attended a class run by Boris Mikhailovich

Martin Raussen is associate professor of mathematics at Aalborg University. His email address is `raussen@math.aau.dk`.

Christian Skau is professor of mathematics at the Norwegian University of Science and Technology, Trondheim, Norway. His email address is `csk@math.ntnu.no`.

Makarov. You could see the high intensity of these people and their devotion to science. That had a very strong impact on me, as well as the interactions with the senior students. Let me mention one, the young algebraist Tolia Yakovlev, who projected this image of absolute dedication to mathematics. On the other hand, there was a general trend in Leningrad of relating mathematics to science. This was influenced, I think, by Kolmogorov and Gelfand from Moscow. Kolmogorov made fundamental contributions to hydrodynamics, and Gelfand was working in biology and also in physics. Basically, there was an idea of the universality of knowledge, with mathematics being kind of the focus of intellectual ideas and developments. And that, of course, shaped everybody who was there, myself included. And I learned very much of the Moscow style of mathematics from Dima Kazhdan, with whom we were meeting from time to time.

Raussen and Skau: *Can you remember when and how you became aware of your exceptional mathematical talent?*

Gromov: I do not think I am exceptional. Accidentally, things happened, and I have qualities that you can appreciate. I guess I never thought in those terms.

Raussen and Skau: *At least towards the end of your studies, your academic teacher was Vladimir Rokhlin. Do you still sense his influence in the way you do mathematics today?*

Gromov: You see, Rokhlin himself was educated in Moscow, and the Moscow mathematical way of thinking was very different from that in Leningrad. They had a different kind of school that was much more oriented towards Western mathematics. Leningrad was more closed and focused on classical problems; Moscow was more open to new developments. And that is what he brought to Leningrad. Another person with the same attitude was Boris Venkov, an algebraic geometer. From him and from Rokhlin, I got a much broader view and perception of mathematics than what I could have got from the traditional school in Leningrad. On the other hand, the traditional school was also very strong; for instance, the geometry school of Aleksandr Danilovich Alexandrov. There were people like Zalgaller and Burago from whom I learned most of my geometry. Burago was my first teacher in geometry.

Raussen and Skau: *You were very successful at Leningrad University at the beginning of the 1970s. Still, you left Leningrad and the Soviet Union shortly after in 1974. What was the background for your desire to leave?*

Gromov: This is very simple. I always say, if someone tells you you should not do something, you try to do exactly that. You know what happened when God prohibited Eve eating the apple. This is human nature. It was said that you cannot leave the country; it is just impossible, it is wrong, it is horrible. It is like in scientific work: if it is impossible, you try to do it anyway.

Raussen and Skau: *It was probably not that easy to get out of the Soviet Union at that time?*

Gromov: For me it was relatively easy. I was very lucky. But in general it was difficult and risky. I had to apply, I waited for several months, and then I got permission.

Russian Mathematics

Raussen and Skau: *Jacques Tits, one of the Abel prize winners last year, praised Russian mathematical education and Russian schools for the strong personalities and the strong ties between motivations, applications, and the mathematical apparatus, as well as the lively seminars and discussions sometimes lasting for many hours. What is your perception: what is special about the Russian mathematical style and school?*

Gromov: Like I said, it was somewhat different in Leningrad compared to Moscow. What Tits was probably referring to was Gelfand's seminars in Moscow. I attended this seminar in Moscow only once, when I was invited to give a talk, so my recollection might not be typical. But when I came, it took about two hours before the seminar could start because Gelfand was discussing various matters with the audience. Another seminar was run by Piatetsky-Shapiro and that was very rigorous. When something was presented on the blackboard and the audience asked questions, then Shapiro would express his attitude, which was very strong and a bit aggressive: on what students should know and should not know, the idea that they should learn this and this and that… Extremely powerful indications of his personality!

Raussen and Skau: *Do you still feel that there is a specific Russian mathematical background that you build your work upon?*

Gromov: Yes, definitely. There was a very strong romantic attitude towards science and mathematics: the idea that the subject is remarkable and that it is worth dedicating your life to. I do not know whether that is also true in other countries because I was not elsewhere at that time of my education. But that is an attitude that I and many other mathematicians coming from Russia have inherited.

Raussen and Skau: *Is there still a big difference between Russian mathematics and, say, Western mathematics in our days? Or is this difference about to disappear, due to the fact that so many Russians are working in the West?*

Gromov: This I cannot tell, given there are so many Russians working in the West. I do not know much about mathematical life in Russia nowadays; certainly, things have changed tremendously. In my time in Russia, this intensity was partly a reaction to the outside world. Academic life was a peaceful garden of beauty where you could leave a rather ugly political world outside. When this all changed, this sharp concentration went down. It might be so. I don't know. This is only a conjecture.

Raussen and Skau: *Do you still have a lot of contact with Russian mathematicians? Do you go there once in a while?*

Gromov: I have been there twice since I left the country. You still feel the intensity of life there but things go down, partially because so many gifted people are leaving. They are drawn to larger centers where they can learn more.

Raussen and Skau: *Can you tell us about other Russian mathematicians that have influenced you, like Linnik?*

Gromov: Yes. Yuri Linnik was a great scientist, professor, and academician in Leningrad. He was running educational seminars in algebraic geometry one year. A remarkable thing was that he always admitted his complete ignorance. He never pretended to know more than he did, rather the contrary. And secondly, there was always a complete equality between him and his students. I remember one time I was supposed to give a talk there but I overslept and arrived one hour late. But he was just laughing at it—not annoyed at all. And that, I think, exhibits some of his spirit in mathematics—the atmosphere of how we were all in the same boat, regardless of who you were.

Raussen and Skau: *How would you compare him with Rokhlin as a person?*

Gromov: Rokhlin was a more closed person as he had gone through a very complicated life. He was a prisoner in the Second World War. He was Jewish but he somehow managed to conceal it. He had an extremely strong personality. After he was liberated, he was sent to a prison in Russia, a labor camp, because it was considered that he hadn't finished his military service. Being a prisoner of war didn't count as military service! After some work he came to Moscow. It was difficult to say what he thought. He was very closed and tried to keep high standards on everything, but he was not so relaxed and open as Linnik was. It was at first unclear what it was, but then you realized that he was shaped by those horrible experiences.

Raussen and Skau: *Was Linnik also Jewish?*

Gromov: I think Linnik was half Jewish, but he did not participate in the war. He had a different kind of life. He was better positioned in his career as a member of the Academy and so on. Rokhlin was always discriminated against by the authorities, for reasons I don't know. I heard some rumors that he was getting into conflict with some officials in Moscow.

For some time he was a secretary for Pontryagin because Pontryagin was blind and, as an academician, needed a secretary. Rokhlin had this position until he had defended his second thesis. Then he was kicked out of Moscow because he was overqualified. A. D. Alexandrov, then the rector at Leningrad University, made a great effort to bring him to Leningrad in 1960. That had a very strong influence on the development of mathematics in Leningrad. The whole school of topology grew out of his ideas. Rokhlin was a very good teacher and organizer.

Raussen and Skau: *Is it true that Pontryagin was anti-Semitic?*

Gromov: I believe he became anti-Semitic after his second marriage. He was blind, and it is unclear how independent his perception of the world was. In his later years he became anti-Semitic, and he also wrote pamphlets that sounded absolutely silly. It is unclear what or who influenced him to get those ideas.

History of Geometry

Raussen and Skau: *You are the first Abel laureate to receive the prize explicitly for your "revolutionary contribution to geometry". From Euclid's time geometry was, so to say, the "face" of mathematics and a paradigm of how to write and to teach mathematics. Since the work of Gauss, Bolyai, and Lobachevsky from the beginning of the nineteenth century, geometry has expanded enormously. Can you give us your thoughts on some of the highlights since then within geometry?*

Gromov: I can only give a partial answer and my personal point of view. It is very difficult to find out about how people thought about the subject in ancient times. Seen from today, geometry as a mathematical subject was triggered from observations you make in the world; Euclid gave a certain shape of how to organize observations and made an axiomatic approach to mathematics and what followed from those. It happened that it worked very badly beyond the point that it was designed for. In particular, there was a problem with the parallel postulate, and people tried to prove it.

There was a mixture: on one hand they believed that the way you see the world was the only way for you to see it, and they tried to justify that axiomatically. But it did not work. Eventually, mathematicians realized that they had to break out of the naïve way of thinking about axioms. The axioms happened to be very useful but only useful in a limited way. Eventually, you had to deny them. This is how they served. From this point on, mathematics started to move in different directions. In particular, Abel was one of the people who turned mathematics from just observing and formalizing what you see to formalizing what you cannot see directly—what you can only see in a very opaque way. Modern mathematics was shaped in the beginning of the nineteenth century. Then it became more and more structural. Mathematics not only deals with what you see with your eye but what you see in the structure of things, at a more fundamental level, I would say. If you formulate the problem in modern language, the mathematicians at the

Photo by Heiko Junge/Scanpix, for the Abel Prize, the Norwegian Academy of Science and Letters.

Interview in Oslo in May 2009. Left to right, Christian Skau, Martin Raussen, and Mikhail Gromov.

time faced trying to understand the limitations of Euclidean geometry; it is completely obvious. But it took centuries to develop this language. This work was started by Lobachevsky, Bolyai, and Gauss, and in a different domain by Abel and Galois.

The Laureate's Research in Geometry

Raussen and Skau: *It is said that you revolutionized Riemannian geometry in the late 1970s. Could you explain to us what your novel and original idea consisted of, the idea that turned out to be so groundbreaking?*

Gromov: I cannot explain that since I never thought of them as groundbreaking or original. This happens to any mathematician. When you do something new, you don't realize it is something new. You believe everybody knows it, that it is kind of immediate and that other people just have not expressed it. This happens in fact with many mathematical proofs; the ideas are almost never spoken out. Some believe they are obvious and others are not aware of them. People come from different backgrounds and perceive different things…

Raussen and Skau: *A hallmark of your work has been described as the softening of geometry, whereby equations are replaced by inequalities or approximate or asymptotic equations. Examples include the "coarse viewpoint" on Riemannian geometry, which considers all Riemannian structures at once. This is very original. Nobody had thought about that before. Isn't that true?*

Gromov: That is probably true. But again, I am not certain whether somebody else had had this idea before. For me it was clear from the very beginning, and I actually never articulated it for a long time, believing everybody knew it. I believe that some people knew about it but they never had an occasion to say it aloud. In the end, I formulated it because I gave a course in France.

Raussen and Skau: *First of all, you had this new perspective. The basic ideas are perhaps very simple but you were the first to get any deep results in that direction.*

Gromov: Well, there were predecessors. This trend in Riemannian geometry started with the work of Jeff Cheeger. Earlier, up to some point, people were thinking about manifolds in very abstract terms. There were many indices and you could not take the subject into your hand. I think that one of the first works in which Riemannian geometry was turned into something simple was by John Nash. Actually, he had a tremendous influence on me. He was just taking manifolds in his hands and putting them in space, just playing with them. From this I first learned about this very concrete geometry. Simple things, but you had to project it to very high dimensions. And then there was the work by Jeff Cheeger, formally a very different subject but with the same attitude, realizing that things got quite simple when formalized, if that was done properly. So I was just following in the steps of these people.

Raussen and Skau: *This means that you read Nash's work and were impressed by it very early?*

Gromov: Yes, I read it very carefully. And I still believe I am the only person who read his papers from the beginning to the end. By judging what people have written about it afterwards, I do not think they have read it.

Raussen and Skau: *Why not?*

Gromov: At first, I looked at one of Nash's papers and thought it was just nonsense. But Professor Rokhlin said: "No, no. You must read it." I still thought it was nonsense; it could not be true. But then I read it, and it was incredible. It could not be true but it was true. There were three papers; the two more difficult ones, on embeddings, they looked nonsensical. Then you look at the way it is done, and you also think that it looks nonsensical. After understanding the idea you try to do it better; many people tried to do it in a better way. But when you look at how they were doing it, and also what I tried, and then come back to Nash, you have to admit that he had done it in a better way. He had a tremendous analytic power combined with geometric intuition. This was a fantastic discovery for me: how the world may be different from what you think!

Raussen and Skau: *John Nash received the Nobel Prize in economics and he was also the person behind the* Beautiful Mind *movie. Many people think he should have gotten the Fields Medal for his efforts. Do you subscribe to this idea?*

Gromov: Yes. When you think about this guy and his achievements in science, forgetting about medals, the discoveries he made were fantastic. He was a person thinking in a most unusual way. At least, his work in geometry was contrary to what everybody would expect, concerning the results, the techniques, and the ideas he used. He did various matters in an extremely simple way, so that everybody could see it but nobody would believe it could work. He also had a tremendous power of implementing it, with a dramatic analytic power. What he has done in geometry is, from my point of view, incomparably greater than what he has done in economics, by many orders of magnitude. It was an incredible change in attitude of how you think about manifolds. You can take them in your bare hands, and what you do may be much more powerful than what you can do by traditional means.

Raussen and Skau: *So you admit that he had an important influence upon you and your work.*

Gromov: Yes, absolutely. All over, his work and the work of Smale, which was explained to me by Sergei Novikov at a summer school in the early 1960s, have had the most important influence on me.

Raussen and Skau: *You introduced the h-principle, where "h" stands for homotopy, in order to study a class of partial differential equations that arises in differential geometry rather than in physical science; it has proved to be a very powerful tool. Could you explain the h-principle and your ideas behind introducing the concept?*

Gromov: This was exactly motivated by the work of Smale and Nash. And I realized then that they dealt more or less with the same topic—which had not been clear at all. In particular, if you use Nash's techniques you immediately get all the results of immersion theory. You do not have to go deep. The first lemma in Nash proves all immersion theorems in topology! I was thinking about this for several years, trying to understand the mechanism behind it. I realized there was a simple general mechanism, which was rather formal but incorporated the ideas of Nash and Smale by combining them. This applies to a wide class of equations because you interpolate between rather remote topics and then you cover a very large ground.

Raussen and Skau: *You proved a celebrated theorem, precursors of which were theorems by Milnor-Wolf and Tits. It tells us that if a finitely generated group has polynomial growth, then it contains a nilpotent subgroup of finite index. A particularly remarkable aspect of your proof is that you actually use Hilbert's Fifth Problem, which was proved by Gleason, Montgomery, and Zippin. And this is the first time, apparently, that this result has been used in a significant way. Can you explain and expand on this?*

Gromov: I thought previously about applying this theorem in Riemannian geometry, though in a different context, inspired by Margulis' 1967 paper on 3-dimensional Anosov flows and by his 1970 rendition of Mostow's rigidity theorem, where Margulis introduced and exploited quasi-isometries. I wanted to prove something that happened to be wrong. I tried to apply a version of the Shub-Franks construction in topological dynamics. It didn't work either. Also, there was a paper by Hirsch concerning exactly this question about polynomial growth—a special case of this problem—where he tried to apply the classification of topological groups; and again it didn't work. So I believed it couldn't be applied. It was kind of clear to us that it was close but it didn't seem to work. But when I was formalizing the idea of limits of manifolds, I tried to think in those terms and then I saw that it might work. This was kind of a surprise to me.

Raussen and Skau: *It must have been a very nice experience when you realized that this would work out?*

Gromov: Well, it was not really a sudden insight. I realized what was needed was just a slight change in conceptions. Then it is not difficult to do it. The proof is extremely simple in a way. You take an obvious concept of a limit, and then, by the power of analysis, you can go to the limit many times, which creates structures that you have not seen before. You think you have not done anything but, amazingly, you have achieved something. That was a surprise to me.

Raussen and Skau: *You introduced the idea of looking at a group from infinity, which is an apt description of looking at the limit of a sequence of metric spaces associated to the group in the so-called Gromov-Hausdorff metric. You have used this technique with impressive effect. Please give us some comments.*

Gromov: After proving the theorem about polynomial growth using the limit and looking from infinity, there was a paper by Van den Dries and Wilkie giving a much better presentation of this using ultrafilters. Then I took it up again and I realized it applied to a much wider class of situations where the limits do not exist but you still have the ultralimits, and it gives you a very good view on many mathematical objects, including groups. But it is still not tremendously powerful.

In the context of groups, I was influenced by a survey of the small cancellation theory by Paul Schupp in the book *Word Problems* (1973) where he said—and I think this was a very honest and very useful remark—that "people don't understand what small cancellation groups are." And I felt very comfortable because I didn't understand it either. I started thinking about what they could be, and then I came up with this concept of hyperbolicity. This was rather pleasing to me, but there were some technical points I could not handle for some time, such as the rough version of the Cartan-Hadamard theorem, before I could write an article about it.

Raussen and Skau: *When did you introduce the concept of a hyperbolic group?*

Gromov: My first input on the geometry of groups came from Dima Kazhdan, who explained to me in the middle of the 1960s the topological proof of the Kurosh subgroup theorem. Later on I read, in the same 1971 issue of *Inventiones*, the paper by Griffiths on complex hyperbolicity and the paper by Klingenberg on manifolds of hyperbolic type. The latter contained the idea of rough hyperbolicity, albeit the main theorem in this paper was incorrect. And, as I said, I had read the paper by Schupp.

I presented the first definition of hyperbolicity during the 1978 meeting at Stony Brook under the name of Is(2)-groups as they satisfy the linear isoperimetric inequality in dimension two. The article appeared three years later. Also, I recall, I spoke about it at the Arbeitstagung in 1977. I tried for about ten years to prove that every hyperbolic group is realizable by a space of negative curvature, which I couldn't do, and this is still unknown. Then Steve Gersten convinced me to write what I already knew about it, and I wrote that but I was very dissatisfied because I couldn't decide if you needed the theory of such groups. If they were "geometric", the way I said, we would not need hyperbolicity theory, and we would have much better theorems.

Raussen and Skau: *You said that almost all groups are hyperbolic?*

Gromov: Right. That was actually the point. When I realized that we could see hyperbolicity in certain generic constructions better without an appeal to curvature, then I accepted it as a worthwhile notion. In my first article I suggested a rather technical definition and terminology. I believed it was a preliminary concept. But then I realized eventually that it probably was the right concept, regardless of whether the geometrization theorem I was trying to prove was true or not. Also, I was encouraged by talking to Ilia Rips in the early 1980s, who, by that time, had developed hyperbolic group theory in a combinatorial framework, well beyond what I knew at the time, by the ongoing development of Thurston's 3-D theory and by Cannon's solution of Thurston's rationality conjecture.

Raussen and Skau: *We move to a different area, symplectic geometry, that you have also made a revolutionary contribution to. You introduced methods from complex analysis, notably pseudoholomorphic curves. Could you expand on this and explain how you got the idea for this novel approach? And also on the Gromov-Witten invariant, which is relevant for string theory and which came up in this connection.*

Gromov: Yes, I remember very vividly this amazing discovery I made there. I was reading a book by Pogorelov about rigidity of convex surfaces. He was using the so-called quasi-analytic functions developed by Bers and Vekua. He talked about some differential equations and said that the solutions were quasi-analytic functions. I couldn't understand what the two had in common. I was looking in his books and in articles of these people but I couldn't understand a single word; and I still don't. I was extremely unhappy about this, but then I thought about it in geometric terms. And then you immediately see there is an almost complex structure there, and the solutions are just holomorphic curves for this almost complex structure. It is nothing special because any elliptic system in two variables has this property. It has the same principal symbol as the Cauchy-Riemann equation. The theorem he was using is obvious once you say it this way. You didn't have to use any theory; it is obvious because complex numbers have a forced orientation. That's all you use!

Raussen and Skau: *You say obvious but not many mathematicians were aware of this?*

Gromov: Yes, exactly. They were proving theorems but they never looked at this. If you look at this in certain terms, it becomes obvious because you have experience with algebraic geometry. Once you know algebraic geometry you observe it as the same. We have this big science of complex analysis and algebraic geometry with a well-established theory; you know what these things are, and you see there is no difference. You use only some part of this but in higher generality. Then, I must admit that for some time I was trying to use it to recapture Donaldson theory, but I couldn't do it because there were some technical points that did not work. Actually, it was similar to the obstruction of being Kähler in dimension four. I spoke with Pierre Deligne and asked him whether there was an example of a complex surface that was not Kählerian and that would have certain unpleasant properties. He said, yes, and showed me such examples. I turned then to the symplectic case, and I realized that it worked very well. And once again, things were very simple, once you knew where to go. It was so simple that I had difficulty believing it could work because there was only one precedent, due to Donaldson. It was Donaldson's theory that said that such mathematics can give you that kind of conclusion. It had never happened before Donaldson, and that was very encouraging. Otherwise I probably wouldn't have believed it would work if not for Donaldson's discovery. Besides, I was prepared by Arnold's conjectures, which I learned from Dima Fuks in the late 1960s, by the symplectic rigidity ideas of Yasha Eliashberg developed by him in the 1970s, and by the Conley-Zehnder theorem.

Raussen and Skau: *Could you say something about the proof by Perelman and Hamilton of the Poincaré conjecture? Did they use some of your results?*

Gromov: No. If at all, then just some very simple things. That is a completely different mathematics. There are interactions with the geometry, I know, but they are minor. It is essentially a quite different sort of mathematics, which I understand only superficially, I must admit. But I must say that it is a domain that is basically unexplored compared to what we know about Cauchy-Riemann equations in a generalized sense, or Yang-Mills, Donaldson, or Seiberg-Witten equations. Here, it is one theorem and it is still somewhat isolated. There is no broader knowledge around it, and we have to wait and see what comes. We certainly expect great developments from this yet to come.

Raussen and Skau: *Do you have any interaction with Alain Connes?*

Gromov: Oh yes, certainly. We have interacted quite a bit, though we think in very different ways. He understands one half and I understand the other half, with only a tiny intersection of the two parts; amazingly, the outcome turns out to be valid sometimes. I have had two joint papers with him and Moscovici, proving particular cases of the Novikov conjecture.

Raussen and Skau: *You came up with an example of some expanders on some groups and thus produced a counterexample to the Baum-Connes conjecture.*

Gromov: This counterexample is due to Higson, [Vincent] Lafforgue, and Skandalis, where they used the construction of random groups.

Raussen and Skau: *Is there one particular theorem or result you are the most proud of?*

Gromov: Yes. It is my introduction of pseudoholomorphic curves, unquestionably. Everything else was just understanding what was already known and to make it look like a new kind of discovery.

Raussen and Skau*: You are very modest!*

Mathematical Biology

Raussen and Skau: *We have been told that you have been interested in questions and problems in mathematical biology recently. Can you describe your involvement and how your mathematical and geometric insights can be useful for problems in biology?*

Gromov: I can explain how I got involved in that. Back in Russia, everybody was excited by ideas of René Thom on applying mathematics to biology. My later motivation started from a mathematical angle, from hyperbolic groups. I realized that hyperbolic Markov partitions were vaguely similar to what happens in the process of cell division. So I looked in the literature and spoke to people, and I learned that there were so-called Lindenmayer systems. Many biologists think that they represent a very good way of describing the growth of plants by patterns of substitution and cell division. Then, at the base of that, we had a meeting at the IHES [Institut des Hautes Etudes Scientifiques] in Bures on pattern formation, in particular in biology. I got interested and I wanted to learn more about biology. Soon, I realized that there had been a huge development in molecular biology in the 1980s, after the discoveries of genetic engineering and of PCR (polymerase chain reaction). It was really mathematical procedures applied to living cells. Mathematicians could invent PCR. It didn't happen, but mathematicians could have invented PCR. It was one of the major discoveries of the century. It changed molecular biology completely. I started to learn about these mathematical procedures and to realize that it led to fantastic mathematical questions. But it was hard to say exactly what it is; I just cannot formulate it. Of course there are very particular domains like sequencing, and there are specific algorithms used there. But this is not new mathematics; it is old mathematics applied to this domain. I believe there is mathematics out there still unknown to us that is yet to be discovered. It will serve as a general framework, just like differential equations give a framework for classical mechanics. It will be rather abstract and formal, but it should embed our basic knowledge of biology and maybe accumulate results that we still do not know. I still think about this but I do not know the answer.

Mikhail Gromov on left, being greeted by the king and queen of Norway.

Photo by Erlend Aas/Scanpix, for the Abel Prize, the Norwegian Academy of Science and Letters.

Raussen and Skau: *Would you please explain the term PCR?*

Gromov: It means polymerase chain reaction, and you can see it as follows. You come to a planet that is populated by rats, and they all look the same. In your lab, you also have rats that are very similar. They look absolutely identical, but they are of a different species. Now, one of the female rats escapes. One year later you want to decide whether it has survived or not. There are billions of those rats, so you cannot check all of them, so what do you do? Here is the idea. You throw in several billion male rats, and if the escaped rat is still there, then you will find a certain population of your rats. Then you wait a little bit, and the number of them will grow into billions. You take a sample and check if it contains your rat. This is how a polymerase chain reaction works, but instead of rats you use DNA. There are billions of different DNAs of various kinds, and if you want to know if a particular one of them is out there, then there is a way to do that with a given molecule that amplifies exponentially. If one had been out there, you would have billions of them after several cycles. This incredible idea is very simple and powerful. One fundamental thing happening in biology is amplification; it is specific for biology. Mathematics should be useful for biologists. We cannot make it yet, but I believe it can be done. It will have impact on problems in genetic engineering and identifying gene functions, but it has not been developed yet. It will be very different from other kinds of mathematics.

Mediation Between Mathematics and Science

Raussen and Skau: *Is it your impression that biologists recognize and appreciate your work and the work of other mathematicians?*

Gromov: I have not done anything. I just communicated with biologists. But I think many of them were quite satisfied talking to me, as well as to other mathematicians. Not because we know something but because we ask many questions. Sometimes they cannot answer but that makes them think. That is about it, but this is not so little in my opinion. In this way, mathematicians can be useful by being very good listeners.

It happens very rarely that something is done by mathematicians in science. One of the most remarkable examples happened here in Norway in the middle of the nineteenth century. In collaboration, the mathematician Guldberg and the chemist Waage invented chemical kinetics. I do not know of any other situation since then where mathematicians have contributed to experimental science at this level. This shows that it is possible, but it happened through a very close collaboration and in a special situation. I think something like that may happen in biology sometime but it cannot come so easily.

Raussen and Skau: *You came across Guldberg and Waage in connection with your interest in chemistry?*

Gromov: Yes. This is kind of the fundamental equation in chemistry and also in molecular biology, always in the background of things. Mathematicians can have their word, but it is not so easy. You cannot program it. You have to be involved. Sometimes, very rarely, something unexpected happens, with a very strong impact!

Raussen and Skau: *To our amazement, we realized that one of the Abel lectures in connection with the prize, the science lecture, was given on computer graphics. It is said that computer graphics or computer vision, and shape analysis in particular, benefits from your invention: the Gromov-Hausdorff distance. Can you explain where this notion comes in and how it is used?*

Gromov: When you have to compare images, the question is how you compare them. Amazingly—for a geometer it looks unbelievable—the early work on computer vision was based on matching images with another, taking differences in intensity—which is certainly completely contrary to what your eyes do! Actually, the idea of how eyes operate with images goes back to Poincaré. In his famous book called *Science and Hypothesis* he thinks, in particular, about how the human mind can construct Euclidean geometry from the experience we have. He gives an almost mathematical proof that it would be impossible if your eyes could not move. So, what you actually reconstruct, the way your brain records visual information, is based on the movement of your eyes and not so much on what you see. Roughly, the eye does this. It does not add images. It moves images. And it has to move them in the right category, which is roughly the category that appears in Riemannian geometry, with Hausdorff convergence or whatever, using small distortions and matchings of that.

For a mathematician who has read Poincaré, this is obvious. But for the people in computer science, following different traditions from linear analysis, it was not obvious at all. And then, apparently, they brought these ideas from geometry to their domain… Actually, several times I attended lectures by Sapiro since I became interested in vision. He is someone who has thought for a long time about how you analyze images.

Raussen and Skau: *It seems that there is not enough mediation between science and mathematics.*

Gromov: Absolutely, I completely agree. To say "not enough" is an understatement. It is close to zero. The communities have become very segregated due to technical reasons and far too little communication. A happy exception is the Courant Institute. We still have many people interacting, and it happens that mathematicians fall in love with science. To see these young people at Courant is extremely encouraging because you don't see this kind of applied mathematicians anywhere else. But they are well aware of the body of pure mathematics where they can borrow ideas and then apply them. Typically, applied mathematicians are separated from the pure ones. They, kind of, don't quite like each other. That's absurd. This has to be changed because we have the same goals. We just understand the world from different sides.

Raussen and Skau: *Do you have any ideas of how to improve this situation?*

Gromov: No. But I think in any subject where you have this kind of problem, the only suggestion is that you have to start by studying the problem. I don't know enough about this; I just have isolated examples. We have to look at where it works, where it doesn't work and just try to organize things in a new way. But it has to be done very gently because you cannot force mathematicians to do what they don't like. The obvious way to do it is to design good combined educations in mathematics and science. Actually, there is a very good initiative by François Taddei in Paris who organizes classes with lectures on biology for nonbiologists—for young people in mathematics and physics. He is extremely influential and full of enthusiasm. I attended some of those classes, and it was fantastic. He was teaching biology at Ecole Normale for mathematicians and physicists, and he manages to make those ideas accessible for everybody. That is what I think should be done at the first stage. We have to have this special kind of education that is not in any curriculum; you cannot formalize it. Only people who have enough enthusiasm and knowledge can project this knowledge to young people. An institutionalized system is much harder to design, and it is very dangerous to make it in any way canonical, because it may just misfire. Forcing mathematics on nonmathematicians only makes them unhappy.

Raussen and Skau: *We have already talked about your affiliation with the Courant Institute in New York, but for a much longer time you have been affiliated with the Institut des Hautes Etudes Scientifiques (IHES) at Bures-sur-Yvette, close to Paris. Can you explain the role of this institution for your research—and for your daily life, as well?*

Gromov: It is a remarkable place. I knew about it before I came there; it was a legendary place because of Grothendieck. He was kind of a god in mathematics. I had met Dennis Sullivan already at Stony Brook but then met him again at IHES, where I learned a lot of mathematics talking to him. I think he was instrumental bringing me there because he liked what I was doing and we interacted a lot. Dennis interacted with many people. He had a fantastic ability of getting involved in any idea—absorbing and helping to develop an idea. Another great man there was René Thom but he was already into philosophy apart from doing mathematics. Pierre Deligne was also there. From Pierre I learned some stuff rather punctually; on several occasions, I got fantastic answers when I asked him questions. He would take an idea from your mind and turn it in another direction.

Basically, the whole atmosphere created at this institution was very particular. You are almost completely free of anything except for doing research and talking to people—a remarkable place. I think my best memories go back to when I was there as a first-year visitor. Then I was really free. When I became a part of it there were some obligations. Not much, but still. It is ideal for visitors to come for half a year and just relax, but being there permanently was also not so bad.

Raussen and Skau: *Did you get your best results when you were at Bures?*

Gromov: Yes. When I was between 35 and 39, I would say. That's when I was the most productive.

Computers for Mathematicians and for Mathematics

Raussen and Skau: *It is clear that the use of computers has changed the everyday life of mathematicians a lot. Everybody uses computers to communicate and editing is done with computer tools by almost everybody. But other people use computers also as essential research equipment. What are your own experiences? Do you use computers?*

Gromov: No, unfortunately not. I am not adept with computers. I can only write my articles on a computer, and even that I learned rather recently. I do believe that some mathematics, particularly related to biology, will be inseparable from computers. It will be different mathematics when you, indeed, have to combine your thinking with computer experiments. We have to learn how to manipulate large amounts of data without truly understanding everything about it, only having general guidelines. This is, of course, what is happening but it is not happening fast enough. In biology, time is the major factor because we want to discover cures or at least learn about human diseases. And the faster we do it, the better it is. Mathematicians are usually timeless. You are never in a hurry. But here you are in a hurry and mathematicians can accelerate the process. And there, computers are absolutely a part of that. In this way, I believe computers are playing and will play a crucial role.

Raussen and Skau: *And that will change the way mathematics is done in the long run, say within the next fifty years?*

Gromov: I think that within fifty years there will be a radical change in computers. Programming develops very fast, and I also believe mathematicians may contribute to the development in a tremendous way. If this happens, we will have very different computers in fifty years. Actually, nobody has been able to predict the development of computers. Just look at how Isaac Asimov imagined robots and computers thirty years ago when he was projecting into the twenty-first century how they looked like in the 1970s. We probably cannot imagine what will happen within fifty years. The only thing one can say is that they will be very different from now; technology moves at a very fast speed.

Raussen and Skau: *What do you think about quantum computing?*

Gromov: Well, I am not an expert to say anything about that. You have to ask physicists, but they have very different opinions about it. My impression is that the experimental physicists believe we can do it and theorists say: "No, no, we cannot do it." That is the overall impression I have, but I cannot say for myself because I don't understand either of the aspects of it.

Mathematical Work Style

Raussen and Skau: *You have been described as a mathematician who introduces a profoundly original viewpoint to any subject you work on. Do you have an underlying philosophy of how one should do mathematics and, specifically, how one should go about attacking problems?*

Gromov: The only thing I can say is that you have to work hard and that's what we do. You work and work, and think and think. There is no other recipe for that. The only general thing I can say is that when you have a problem then—as mathematicians in the past have known—one has to keep the balance between how much you think yourself and how much you learn from others. Everybody has to find the right balance according to his or her abilities. That is different for different people so you cannot give any general advice.

Raussen and Skau: *Are you a problem solver more than a theory builder? Would you describe yourself in any of those terms?*

Gromov: It depends upon the mood you are in. Sometimes you only want to solve one problem. Of course, with age, you become more and more theoretical. Partly because you get wiser but you can also say it is because you get weaker. I suppose it depends on how you look at it.

Raussen and Skau: *Concerning your mathematical work style, do you think about mathematics all the time?*

Gromov: Yes, except when I have some problems of a personal nature; if there is something else that disturbs me then I cannot think. But if everything is okay and, at least, if there is nothing else to do at the moment, I immerse myself in mathematics, or other subjects, like biology, but in a mathematical way, so to say.

Raussen and Skau: *How many hours per day do you work with mathematics?*

Gromov: Not as much as I used to. When I was young I could go on all day, sometimes from nine in the morning to eleven at night. Nothing could distract me. Of course, now I cannot do that any longer. I can only do five, six hours a day without getting tired.

Raussen and Skau: *When you were younger, you had more energy, but now you are a lot wiser, right?*

Gromov: You can say you become more experienced and wiser when you get older. But you also lose your mental powers and you become weaker. You certainly just have to accept that. Whether you become wiser is questionable. But it is obvious that you become weaker.

Raussen and Skau: *John von Neumann once said that you do the most important things in mathematics before you are thirty. When he himself turned thirty he added that you get wiser as you get older. Do you think that the best mathematics is done before you are thirty?*

Gromov: I can say about myself that I think my best work was done when I was between thirty and forty years old. When I started, I didn't have any perspective and was just doing whatever was coming first. As I was learning more, I kept changing my attitude all the time. Now, if I had to start anew, I would do something completely different, wrongly or rightly, I cannot judge. On the other hand, I must say that everything I think about now, I had already thought of forty years ago. Ideas were germinating in me for a long time. Well, some people probably create radically new work late in life, but basically you develop certain feelings very early. Like your abilities to talk, right? You learn to talk when you are three years old but it doesn't mean you say the same things when you are thirty as when you are three. That's how it works.

Raussen and Skau: *We are surprised that you are so modest by playing down your own achievements. Maybe your ideas are naíve, as you yourself say; but to get results from these ideas, that requires some ingenuity, doesn't it?*

Gromov: It is not that I am terribly modest. I don't think I am a complete idiot. Typically when you do mathematics you don't think about yourself. A friend of mine was complaining that anytime he had a good idea he became so excited about how smart he was that he could not work afterwards. So naturally, I try not to think about it.

Raussen and Skau: *Having worked so hard as you say, have you ever suffered from depression because you have overexerted yourself?*

Gromov: No. Sometimes some outside unhappy things have distracted my work. Of course, sometimes you get very tired and you are glad that someone interrupts your work but other times you cannot stop. You work and work, like an alcoholic, so then it is good to get some rest.

Abel and the Abel Prize

Raussen and Skau: *You once complained that the mathematical community only has digested a minor part of your work, rather the technical details than the underlying big ideas and vistas. Do you think that being awarded the Abel Prize may change that situation?*

Gromov: First about this complaint: it was kind of a half-joke. There were some pieces of work where there happened to be ideas that could not be developed, unlike more successful ones, and I was unhappy about that. It depends on how you look at it; either the ideas were no good or people were not paying attention. You just never know. I wished something I was saying could be developed further but this was not happening. And that was my complaint, or rather the motivation for my complaint. It has nothing to do with the Abel Prize.

Raussen and Skau: *What do you think about prizes in general and, in particular, about the Abel Prize?*

Gromov: Objectively, I don't think we need these prizes for mathematicians who have already achieved much. We need more to encourage young people at all levels, and we must put more effort into that. On the other hand, it is very pleasant to receive this prize. I enjoy it, and it may have some overall positive effect on the perception of the mathematical community in the eyes of the general public. That may be just self-justification because I like it, of course, for appreciation of my work by my friends and by receiving this prize. But as the general scientific concern, the far more serious issue is projecting a much greater effort in getting funds for educating and motivating young people to embrace mathematics. What I have seen here in Oslo, at the high school I visited earlier today—with these young people—I was tremendously impressed. I want to see this kind of event everywhere in the world. Of course, mathematicians are not so ascetic that they don't like prizes, but in the long run it is not prizes that shape our future.

Raussen and Skau: *Coming back to Abel, do you admire him as a mathematician?*

Gromov: Yes, absolutely. As I said, he was one of the major figures, if not the major figure, in changing the course of mathematics from what could be visualized and immediately experienced to the next level, a level of deeper and more fundamental structures.

Raussen and Skau: *There is a posthumous paper by Abel where he writes about the theory of equations, which later became Galois theory, and in the introduction he says something very interesting. He says something like: "A problem that seems insurmountable is just seemingly so because we have not asked the right question. You should always ask the right question and then you can solve the problem".*

Gromov: Absolutely. He changed the perspective on how we ask questions. I do not know enough about the history of mathematics but it is obvious that the work of Abel and his way of thinking about spaces and functions has changed mathematics. I do not know enough history to say exactly when this happened, but the concept of underlying symmetries of structures comes very much from his work. We still follow that development. It is not exhausted yet. This continued with Galois theory and in the development of Lie group theory, due to Lie, and, in modern times, it was done at a higher level, in particular by Grothendieck. This will continue, and we have to go through all that to see where it brings us before we go on to the next stage. It is the basis of all we do now in mathematics.

Future of Mathematics

Raussen and Skau: *After this excursion into the history of mathematics, may we speculate a little about the future of mathematics? You once compared the whole building of mathematics with a tree, Hilbert's tree, with a metric structure expressing closeness or nearness between different areas and results. We know from Kurt Gödel that there are parts of that tree we will never reach. On the other hand, we have a grasp of a certain part of the tree, but we don't know how big this part is. Do you think we know a reasonable part of Hilbert's tree? Is the human mind built for grasping bigger parts of it or will there stay areas left uncharted forever?*

Gromov: Actually, I am thinking about that now. I don't know the answer, but I have a program of how we can approach it. It is a rather long discussion. There are certain basic operations by which we can perceive the structure. We can list some of them, and apparently they bring you to certain parts of this tree. They are not axioms. They are quite different from axioms. But eventually you cannot study the outcome with your hands and you have to use computers. With computers you come to some conclusions without knowing the intermediate steps. The computational size will be too huge for you. You have to formalize this approach to arrive at certain schemes of computations. This is what I think about now but I don't know the answer. There are indirect indications that it is possible but those are of a nonmathematical nature, rather biological.

Raussen and Skau: *If you try to look into the future, fifty or one hundred years from now…*

Gromov: Fifty and one hundred is very different. We know more or less about the next fifty years. We shall continue in the way we go. But in fifty years from now, the Earth will run out of the basic resources, and we cannot predict what will happen after that. We will run out of water, air, soil, rare metals, not to mention oil. Everything will essentially come to an end within fifty years. What will happen after that? I am scared. It may be okay if we find solutions, but if we don't then everything may come to an end very quickly!

Mathematics may help to solve the problem, but if we are not successful, there will not be any mathematics left, I am afraid!

Raussen and Skau: *Are you pessimistic?*

Gromov: I don't know. It depends on what we do. If we continue to move blindly into the future, there will be a disaster within one hundred years, and it will start to be very critical in fifty years already. Well, fifty is just an estimate. It may be forty or it may be seventy, but the problem will definitely come. If we are ready for the problems and manage to solve them, it will be fantastic. I think there is potential to solve them, but this potential should be used, and this potential is education. It will not be solved by God. People must have ideas and they must prepare now. In two generations people must be educated. Teachers must be educated now, and then the teachers will educate a new generation. Then there will be sufficiently many people who will be able to face the difficulties. I am sure this will give a result. If not, it will be a disaster. It is an exponential process. If we run along an exponential process, it will explode. That is a very simple computation. For example, there will be no soil. The soil is being exhausted everywhere in the world. It is not being said often enough. Not to mention water. It is not an insurmountable problem, but it requires solutions on a scale we have never faced before, both socially and intellectually.

Education Systems for the Future

Raussen and Skau: *Education is apparently a key factor. You have earlier expressed your distress about realizing that the minds of gifted youths are not developed effectively enough. Any ideas about how education should change to get better adapted to very different minds?*

Gromov: Again I think you have to study it. There are no absolutes. Look at the number of people like Abel who were born two hundred years ago. Now there are no more Abels. On the other hand, the number of educated people has grown tremendously. It means that they have not been educated properly because where are those people like Abel? It means that they have been destroyed. The education destroys these potential geniuses—we do not have them! This means that education does not serve this particular function. The crucial point is that you have to treat everybody in a different way. That is not happening today. We don't have more great people now than we had one hundred, two hundred, or five hundred years ago, starting from the Renaissance, in spite of a much larger population. This is probably due to education. This is maybe not the most serious problem with education. Many people believe in very strange things and accordingly make very strange decisions. As you know, in the UK, in some of the universities, there are faculties of homeopathy that are supported by the government. They are tremendously successful in terms of numbers of students. And anybody can learn that nonsense. It is very unfortunate.

Raussen and Skau: *You point out that we don't have anybody of Abel's stature today, or at least very few of them. Is that because we, in our educational system, are not clever enough to take care of those who are exceptionally gifted because they may have strange ideas, remote from mainstream?*

Gromov: The question of education is not obvious. There are some experiments on animals that indicate that the way you teach an animal is not the way you think it happens. The learning mechanism of the brain is very different from how we think it works: like in physics, there are hidden mechanisms. We superimpose our view from everyday experience, which may be completely distorted. Because of that, we can distort the potentially exceptional abilities of some children.

There are two opposite goals education is supposed to achieve: firstly, to teach people to conform to the society they live in; on the other hand, to give them freedom to develop in the best possible way. These are opposite purposes, and they are always in collision with each other. This creates the result that some people get suppressed in the process of adapting them to society. You cannot avoid this kind of collision of goals, but we have to find a balance between the two, and that is not easy, on all levels of education.

There are very interesting experiments performed with chimpanzee and bonobo apes and under which conditions they learn, or even how you teach a parrot to talk. How do you do that? The major factor is that it should not see the teacher. You put a mirror between you and the parrot and then you speak behind the mirror. The parrot then sees a bird—it talks to a bird. But if it sees you, it will learn very badly.

That is not an obvious thing. The very presence of a teacher, an authority, moves students in a particular direction and not at all the direction the teacher wants them to move. With all this accumulated evidence, you cannot make any simple decision. If you say "do this and this," you are wrong for sure. Solutions are not obvious; they can only come after analyzing deeply what is actually known and by studying the possibilities. I think the answers will be unexpected. What children can learn and what they cannot learn, we don't know because we don't know how to conduct experiments to be ethical and instructive at the same time. It is a very nontrivial issue, which has not been studied much. With animals we have results but not very much with people.

Raussen and Skau: *Let us come back to mathematics and to mathematics education. It seems that many people stop dealing with mathematics as soon as they have left high school. But as mathematicians we know that mathematics is everywhere, though often hidden: as the workhorse in science and technology, but also as a pillar in human culture, emphasizing rigor and organized thinking. Do you have any ideas on how we can make this double role perceived and appreciated by society and how to make decision makers realize that mathematics needs support?*

Gromov: It is a very difficult question because we have to project mathematical ideas to people who work very far from mathematics—to people who make decisions in society. The way we think is very different from the way they operate.

I don't know but I think that within our mathematical society we can make some steps towards education, like creating good mathematical sources for children. Today we have the Internet so we should try to make Internet presentations. Actually, in France there are some people trying to organize extracurricular activities for younger children on a small scale. We should try to do something like that on a big scale: big centers of stimulating creativity in all directions. I would not only focus on mathematics but on science and art and whatever can promote creative activity in young people. When this develops, we may have some influence but not before that. Being inside our ivory tower, what can we say? We are inside this ivory tower, and we are very comfortable there. But we cannot really say much because we don't see the world well enough either. We have to go out, but that is not so easy.

Raussen and Skau: *You mentioned that you first got interested in mathematics after reading the book* Numbers and Figures *by Rademacher and Toeplitz. We could also mention the book* What Is Mathematics? *by Courant and Robbins. Should we encourage pupils in high school who show an interest in mathematics to read books like that?*

Gromov: Yes. We have to produce more such books. Already there are some well-written books, by Martin Gardner, by Yakov Perelman (*Mathematics Can Be Fun*), by Yaglom and co-authors—very remarkable books. Other mathematicians can contribute by writing such books and combine this with the possibilities of the Internet, in particular visualization.

It is relatively simple to write just one page of interesting mathematics. This should be done so that many different subjects in mathematics become easily available. As a community we should go out and create such structures on the Internet. That is relatively easy. The next level is more complicated; writing a book is not easy. Within the community we should try to encourage people to do that. It is a very honorable kind of activity. All too often mathematicians say: "Just vulgarization, not serious". But that is not true; it is very difficult to write books with a wide appeal, and very few mathematicians are actually able to do that. You have to know things very well and understand them very deeply to present them in the most evident way.

Raussen and Skau: *This could be a way to get more young people to take up mathematics?*

Gromov: You will attract more young people. Moreover, the political figures will sense it on a much larger scale because it will have a much wider appeal than what we do internally.

Poetry

Raussen and Skau: *You have mentioned that you like poetry. What kind of poetry do you like?*

Gromov: Of course, most of what I know is Russian poetry—the so-called Silver Age of Russian Poetry at the turn of the twentieth century. There were some poets but you, probably, do not know them. They are untranslatable, I guess. People in the West know Akhmatova, but she was not the greatest poet. The three great poets were Tsvetaeva (also a woman), Blok, and Mandelstam.

Raussen and Skau: *What about Pushkin?*

Gromov: You see, with Pushkin, the problem is as follows. He was taught at school, and that has a tremendously negative impact. But forty years later I rediscovered Pushkin and found him fantastic—when I had forgotten what I had learned in school.

Raussen and Skau: *What about modern poetry and English poetry?*

Gromov: I have read some English poetry. I know some pieces but I don't know it on a larger scale. It is difficult. Even with modern Russian poetry, e.g., Brodsky, I find it difficult to absorb a new style. To absorb a poet is nontrivial. For English poetry, there are a few particular pieces that I learned and appreciate. Some of them are easy to deal with; some have Russian translations. A remarkable one is Edgar Allan Poe. He is kind of simple in a way. But many other English poets are more remote from Russian style. I know a little bit of French poetry, like François Villon; I can appreciate him in French. But modern poetry is very difficult for me.

Raussen and Skau: *To finish the interview, we would like to thank you very much on behalf of the Norwegian, the Danish, and the European Mathematical Societies.*

Popa Receives Ostrowski Prize

Sorin Popa of the University of California Los Angeles has received the 2009 Ostrowski Prize recognizing outstanding mathematical achievement. The prize carries a monetary award of 75,000 Swiss francs (approximately US$75,000). The prize ceremony will be held on March 12, 2010, at the University of Basel.

Popa received his Ph.D. degree in 1983 from the University of Bucharest. He has been a professor at UCLA since 1988. He also held a professorship at the University of Geneva from 1996 to 1998. He has been an invited speaker at the 1990 International Congress of Mathematicians (ICM) in Kyoto and a plenary speaker at the 2006 ICM in Madrid. He was a Guggenheim Fellow from 1995 to 1996 and has been awarded the E. H. Moore Research Article Prize for 2010. He is an editor of the *Pacific Journal of Mathematics* and an associate editor of the *Journal of the American Mathematical Society* and the *Journal of Operator Theory.*

Sorin Popa works in operator algebras (von Neumann and C^*-algebras) and orbit equivalence ergodic theory (also called measurable group theory). During the thirty years of his mathematical career, he settled several difficult, fundamental problems in these areas. Thus, in the early 1980s, he answered three of the twenty problems posed by R. V. Kadison in his famous 1967 "List of Problems", notably an important characterization of the trivial relative commutant condition for II_1 subfactors involving maximal abelian subalgebras. In 1984 Popa gave a positive answer to the long-standing factor-state Stone-Weierstrass conjecture, and in 1985 he solved the B. E. Johnson–S. K. Parrott problem, showing that all derivations of a II_1 factor into the ideal of compact operators are implemented by a compact operator. During the period 1985–2000 Popa proved several deep, fundamental results in Jones theory of subfactors with finite index. For instance, in a series of papers dealing with increasing levels of generality, he proved that hyperfinite subfactors with principal graph satisfying a certain amenability condition are completely classified by their standard invariant. Together with results of A. Ocneanu, M. Izumi, Y. Kawahigashi, and P. Loi, this led to a complete listing of subfactors of Jones index less than or equal to 4, in both type II and III cases. In 1994 he gave an abstract characterization of the standard invariants of subfactors based on an important reconstruction theorem involving amalgamated free products of von Neumann algebras. Also, he introduced a "quantum double" construction for subfactors and used it to prove a surprising hereditary property for hyperfinite subfactors with amenable graph, an analogue to Connes's celebrated heredity of hyperfiniteness in II_1 factors.

During the period 2001–2004 Popa developed deformation-rigidity theory, a series of powerful techniques for studying rigidity phenomena in II_1 factors and orbit equivalence relations arising from measure-preserving actions of groups on probability spaces. He used these techniques and results of D. Gaboriau on "cost" of group actions to prove that the natural action of SL(2, Z) on the 2-torus gives rise to a II_1 factor which is not isomorphic to the n by n matrices over itself, for any integer n, and more generally for any positive real n (in the sense of Murray–von Neumann continuous dimension). This result solved another problem from Kadison's list. Also, he used deformation rigidity to prove a striking version for group actions of Connes's rigidity conjecture, showing that any isomorphism between II_1 factors arising from Bernoulli actions of groups with the property (T) of Kazhdan comes from a conjugacy of the actions.

In particular, two such factors can be isomorphic only if the corresponding groups are isomorphic. Moreover, Popa showed that a Bernoulli action of a property (T) group G is orbit equivalence superrigid; that is, if it has the same orbits as an arbitrary free measure preserving action of some group H, then $G = H$, and the two actions are conjugate. In an important subsequent development, he showed in 2006 that similar results hold true for nonamenable product groups as well. These breakthroughs had considerable impact, leading to many more surprising results in von Neumann algebras and ergodic theory. They also led to fruitful interactions with geometric group theory and found interesting applications to logic (countable Borel equivalence relations). According to the prize citation, Popa's new research direction "completely revolutionized the part of von Neumann algebra theory that is closely related to ergodic theory. His outstanding recent contributions undoubtedly deserve a major prize."

About the Prize

The Ostrowski Foundation was created by Alexander Ostrowski, for many years a professor at the University of Basel. He left his entire estate to the foundation and stipulated that the income should provide a prize for outstanding recent achievements in pure mathematics and the foundations of numerical mathematics. The prize is awarded every other year. The prize jury consists of representatives from the universities of Basel, Jerusalem, and Waterloo and from the academies of Denmark and the Netherlands. For the 2009 prize, the jury members were: Christian Berg, Joram Lindenstrauss, David Masser, Lex Schrijver, and Cameron Stewart. Previous recipients of the Ostrowski Prize are Louis de Branges (1990), Jean Bourgain (1991), Miklos Laczkovich (1993), Marina Ratner (1993), Andrew Wiles (1995), Yuri Nesterenko (1997), Gilles Pisier (1997), Alexander Beilinson (1999), Helmut Hofer (1999), Henryk Iwaniec (2001), Peter Sarnak (2001), Richard L. Taylor (2001), Paul D. Seymour (2003), Ben Green (2005), Terence Tao (2005), and Oded Schramm (2007).

—Elaine Kehoe

American Mathematical Society

AMS Sectional Meetings – Spring 2010

MAR 27-28

University of Kentucky
Lexington, KY

March 27–28

University of Kentucky
Lexington, KY

Invited Addresses by **Percy A. Deift**, Courant Institute–New York University; **Irina Mitrea**, Worcester Polytechnic Institute; **Bruce Reznick**, University of Illinois at Urbana-Champaign; **Bernd Ulrich**, Purdue University; and **Doron Zeilberger**, Rutgers University (Erdős Memorial Lecture)

APR 10-11

Macalester College,
St. Paul, MN

April 10–11

Macalester College,
St. Paul, MN

Invited Addresses by **Charles Doering**, University of Michigan; **Matthew James Emerton**, Northwestern University; **Vladimir Touraev**, Indiana University; and **Peter Webb**, University of Minnesota

APR 17-18

University of New
Mexico
Albuquerque, NM

April 17–18

University of New Mexico
Albuquerque, NM

Invited Addresses by **Kenneth Bromberg**, University of Utah; **Danny Calegari**, California Institute of Technology; **Ioana Dumitriu**, University of Washington; and **Steffen Rhode**, University of Washington

MAY 22-23

New Jersey Institute
of Technology
Newark, NJ

May 22–23

New Jersey Institute of
Technology
Newark, NJ

Invited Addresses by **Simon Brendle**, Stanford University; **Konstantin M. Mischaikow**, Rutgers University; **Ricardo H. Nochetto**, University of Maryland; and **Richard E. Schwartz**, Brown University

See the AMS website for the most up-to-date lists of Invited Addresses and Special Sessions.

www.ams.org/amsmtgs/sectional.html

Come to hear presentations, connect with researchers in your field, and meet colleagues, mentors, and students.
While at the meetings visit the AMS exhibit to see the book sale and receive information on AMS membership and programs.

AMS
American Mathematical Society

National Academies Evaluation of the VIGRE Program Is Released

William E. Kirwan, Mark L. Green, and Neal D. Glassman

In the 1980s and 1990s, there was concern within the mathematical sciences community that post-secondary education in the mathematical sciences was in trouble. A series of challenges was identified in important national reports, including in particular the following:

- *Renewing U.S. Mathematics: Critical Resource for the Future* (1984), also known as the David Report after the chair of the committee, former Presidential Science Advisor Edward David;
- *Educating Mathematical Scientists: Doctoral Study and the Postdoctoral Experience in the United States* (1992), also known as the Douglas Report after committee chair Ronald Douglas; and
- The report of an international panel convened by the National Science Foundation (NSF), *Report of the Senior Assessment Panel for the International Assessment of the U.S. Mathematical Sciences* (1998), also known as the Odom Report after panel chair General William Odom.

Together, these reports painted a picture of the mathematical sciences that focused on three major challenges: inadequate funding, insufficient numbers of students interested in mathematics, and shortcomings in the shape and direction of postsecondary mathematics education. These reports raised four issues concerning students: (1) the number of students receiving degrees, (2) the lack of racial and gender diversity among the mathematics graduate student body, (3) the declining fraction of U.S. citizens receiving advanced degrees in mathematics, and (4) the lack of sufficient postdoctoral fellowships for new doctorates. Four issues were identified with respect to the structure of training in the mathematical sciences: (1) the need for increased breadth, (2) providing a better balance of education and research, (3) decreasing the time to degree, and (4) creating a more positive learning experience.

In response to all of these concerns, Donald J. Lewis, then director of the Division of Mathematical Sciences (DMS) at NSF wrote a "Dear Colleague" letter to the mathematical sciences community, based on recommendations of a DMS Special Emphasis Panel, which introduced and justified the Grants for Vertical Integration of Research and Education in the Mathematical Sciences (VIGRE) Program. The panel recommended that the VIGRE program enable departments to carry out innovative educational programs at all levels not possible through (then) current departmental resources, and it saw the program achieving a change of culture in departments resulting in broadening opportunities through new curriculum development and research experiences. Although the goals of the VIGRE program have changed from year to year, they have consistently included

- Integration of research and education;
- Enhanced interaction across undergraduates, graduates, postdoctoral fellows, and faculty;
- Broadened educational experiences of students to include workforce and early research opportunities; and
- More students motivated to study mathematics and statistics.

VIGRE has been a continuing program of DMS since 1999, but it had not been externally evaluated until NSF requested the appointment of a committee of the National Research Council's (NRC) Board on Mathematical Sciences and Their Applications in 2007 (see sidebar). The charge to this committee included the evaluation of past and current prac-

Neal D. Glassman is senior program officer at the National Research Council. His email address is nglassman@nas.edu. *Mark L. Green is director emeritus of the Institute for Pure and Applied Mathematics at UCLA. His email address is* mlg@ipam.ucla.edu. *William E. Kirwan is chancellor of the University System of Maryland. His email address is* bkirwan@usmd.edu.

Committee to Evaluate the NSF's Vertically Integrated Grants for Research and Education (VIGRE) Program

William E. Kirwan (chair)
Efraim Armendariz
John A. Burns
C. Herbert Clemens
Dona L. Crawford
Cristine M. Cumming
Lawrence Craig Evans
Charles L. Fefferman
Martin Golubitsky
Mark L. Green
Leo P. Kadanoff
Daniel L. Solomon
Lynn Arthur Steen
Karen L. Vogtmann
Eric W. Welch
Shmuel Winograd

tices for steering and assessing the VIGRE program and recommendations on how to improve the program. At about the same time, NSF also commissioned a report, *Increasing the Quantity and Quality of the Mathematical Sciences Workforce through Vertical Integration of Cultural Change*, by Margaret Cozzens. This report recounts some successes of the VIGRE program but is not meant to be a formal evaluation.

The NRC's report, *Evaluation of the NSF's Program: Grants for Vertical Integration of Research and Education in the Mathematical Sciences (VIGRE)* was released in August 2009 and is available from the National Academies Press (http://www.nap.edu). It is the result of four meetings over two years during which the study committee interviewed NSF program managers, leaders, and some students involved with VIGRE programs that were successful (renewed) and leaders of some programs that were not renewed or were canceled before the scheduled five-year expiration, and people involved in site visits preliminary to the selection of awardees or to VIGRE grantees at their three-year evaluation point. The committee was also able to review a substantial amount of data collected by NSF and data in site-visit reports and proposal evaluations, although it was denied access to data that NSF is required to keep confidential. The committee conducted an independent survey of all doctorate-granting departments in the U.S. to determine faculty and administration attitudes toward VIGRE and used much of the data collected annually by the American Mathematical Society.

VIGRE began in 1999, so its first grants wrapped up only five years ago, and some of them were renewed and are only now finishing. Because change of the sort envisioned by VIGRE is necessarily slow, as are trends in enrollment and composition of mathematics student bodies, neither NSF nor the NRC expected that this evaluation would be able to discern strong indications of the effectiveness of the program. In addition, data and impressions from interviews are often contradictory, or at least not sufficient to draw firm conclusions, adding to the difficulties in attributing effect to cause in the presence of so many confounding variables. Nevertheless, the committee was able to reach a number of conclusions concerning the VIGRE program and make recommendations for improvements.

The program's instances of clear success suggest that it provides real value, but its instances of failure suggest that some change is needed, and so the committee recommended that the VIGRE program be continued with some programmatic changes. The most important of these changes is that NSF allow greater flexibility in the design of individual grants by giving consideration to proposals that address only some of the goals of the VIGRE program—to date, such proposals would not be entertained—and that there be scope for greater local initiative in finding ways to achieve these goals. Although it is a worthy aspiration for VIGRE program requests for proposals to call simultaneously for vertical integration from undergraduate education to postdoctoral research; for department-wide change across all subdisciplines; and simultaneous and significant change in a department's undergraduate, graduate, and postdoctoral programs, this should not be seen by NSF as the only path to achieving the goals of the program or to realizing the recommendations of the national panels. The committee has seen many examples of benefits to education, breadth of experience, and culture from interactions across *some* vertical divisions, such as postdoctorals mentoring graduate students or graduate students mentoring undergraduates. The experience of the committee members is that there are benefits to connectivity; but it did not see evidence that *all* of those elements of vertical integration need to be present in a department in order to see any benefits. For example, proposals that build on the particular strengths of a department might not necessarily span all educational levels from undergraduate to postdoctorals, and they might involve fewer faculty members but with more release time for each. Another possibility is the inclusion of students preparing to apply advanced mathematics to nonacademic settings, such as those in a professional master's program. Allowing for greater flexibility might encourage institutions with innovative but less inclusive ideas to submit proposals to the VIGRE program. It is notable that NSF has independently broadened its offering of workforce programs through initiatives that complement the VIGRE program, and this recommended broadening of VIGRE is consistent with that larger trend.

The committee recommended that the goals of any future VIGRE program be clear, consistent, and well publicized. In all phases of the award process, the focus must be on both programmatic quality and scientific quality. Data required from proposers and awardees should concentrate on a small number of carefully chosen benchmarks.

Some departments that responded to the committee's survey email felt that the burden of proposal preparation, requiring extensive departmental participation and coordination, was not commensurate with the likelihood of receiving an award. A less burdensome preliminary process might also encourage greater institutional participation. For this reason, the committee recommended that a preproposal step be inserted into the VIGRE application process.

There have been numerous successful individual activities instituted by VIGRE grantees; many of these are included in Margaret Cozzens's book. For example, North Carolina State has begun an "Environmental Statistics Practicum" linking statistics undergraduates and clients; and the University of Chicago brings large numbers of students in grades 7 through 12 for a summer mathematics enrichment program. The University of Illinois at Urbana-Champaign introduced a Research Experience for Graduate Students (REG) to give graduate students in their first and second years an early research experience. The University of Wisconsin introduced Collaborative Undergraduate Research Labs (CURLs) where teams of undergraduates, graduates, and faculty explore mathematical topics, both pure and applied. The University of Washington conducted a Workshop on Working in Industry to inform graduate students and postdocs about careers in industry and national labs. UCLA offers opportunities for graduate students to dip their toes into applications through a program of graduate summer internships with professors in the sciences, engineering, and medicine.

NSF has not established any formal way to ensure that successful initiatives sponsored under VIGRE awards can be maintained at the conclusion of awards. To remedy this, the committee recommended that NSF convert the VIGRE program to one with longer-duration awards: a norm of ten years, if a five-year review is satisfactory, though the second five-year award might be smaller and more focused than the initial award. Accompanying this change, the committee recommends that NSF require winning departments' home institutions to make a commitment to sustain successful new initiatives resulting from VIGRE as the NSF funding phases down.

NSF needs to develop quantifiable goals for the VIGRE program and link these to consistent data requirements for all grantees and throughout the life of the VIGRE program. These steps will aid in maintaining a transparent evaluation process for the revised program and enable NSF to track the successes of individual VIGRE grants, thus informing future decisions about program continuation.

The committee observed that successful innovations at VIGRE sites were not being publicized in a way that maximized the potential for their being implemented at other universities. NSF should take the lead in developing a framework and infrastructure for a central source for information and communication regarding the successful initiatives of individual VIGRE awardees. In addition, all awardees should maintain and provide access to a VIGRE website even after the expiration of their VIGRE awards; and departments should be encouraged to disseminate examples of their VIGRE activities by, for example, developing resources that could be picked up by other departments.

VIGRE is a program designed to increase departmental interaction and cooperation, but it excludes a large portion of the graduate student and postdoctoral population—foreign nationals. Although they may participate in VIGRE activities, they are ineligible for financial support. This decision may be out of NSF's control, but the committee believes that the goals of the VIGRE program as well as the national need to recruit the most talented people worldwide for positions in academe, industry, and government would be well served by the inclusion of foreign nationals in the program. This recommendation is in line with the 2005 report, *Policy Implications of International Graduate Students and Postdoctoral Scholars in the United States,* written by the National Research Council's Committee on Science Engineering and Public Policy.

Although it is difficult to attribute changes in an institution's mathematical sciences department to its VIGRE grant as opposed to other factors, the committee believes that the VIGRE program has produced a number of qualitative changes in mathematics and statistics departments that have held a grant and, through the proposal process, even some that haven't. These include increasing the integration of students and faculty, providing more early opportunities for student research, helping create a more welcoming culture for mathematics education at all levels, and offering a broader and more interdisciplinary range of options.

2009 Annual Survey of the Mathematical Sciences

(First Report, Part II)

2009–2010 Faculty Salaries Report

Polly Phipps, James W. Maxwell, and Colleen A. Rose

This report provides information on the distribution of 2009–2010 academic-year salaries for tenured and tenure-track faculty at four-year mathematical sciences departments in the U.S. by the departmental groupings used in the Annual Survey. (See page 414 for the definitions of the various departmental groupings.) Salaries are described separately by rank. Salaries are reported in current dollars (at time of data collection). Results reported here are based on the departments which responded to the survey with no adjustment for non-response.

Table 1 provides the departmental response rates for the 2009 Faculty Salary Survey. Departments were asked to report for each rank the number of tenured and tenure-track faculty whose 2009–10 academic-year salaries fell within given salary intervals (the survey form is available at `www.ams.org/employment/surveyforms.html`). Reporting salary data in this fashion eliminates some of the concerns about confidentiality but does not permit determination of actual quartiles. Although the actual quartiles cannot be determined from the data gathered, these quartiles have been estimated assuming that the density over each interval is uniform.

When comparing current and prior year figures, one should keep in mind that differences in the set of responding departments may be a significant factor in the change in the reported mean salaries.

Previous Annual Survey Reports

The 2008 First, Second, and Third Annual Survey Reports were published in the *Notices of the AMS* in the February, August, and November 2009 issues respectively. These reports and earlier reports, as well as a wealth of other information from these surveys, are available on the AMS website at `www.ams.org/employment/surveyreports.html`.

Acknowledgements

The Annual Survey attempts to provide an accurate appraisal and analysis of various aspects of the academic mathematical sciences scene for the use and benefit of the community and for filling the information needs of the professional organizations. Every year, college and university departments in the United States are invited to respond. The Annual Survey relies heavily on the conscientious efforts of the dedicated staff members of these departments for the quality of its information. On behalf of the Annual Survey Data Committee and the Annual Survey Staff, we thank the many secretarial and administrative staff members in the mathematical sciences departments for their cooperation and assistance in responding to the survey questionnaires.

Table 1: Faculty Salary Response Rates

Department	Number	Percent
Group I (Public)	23 of 25	92
Group I (Private)	14 of 23	61
Group II	50 of 56	89
Group III	65 of 81	80
Group IV (Statistics)	41 of 57	72
Group IV (Biostatistics)	21 of 31	60
Group Va	10 of 18[*]	56
Group M	97 of 182	53
Group B	310 of 1037	30

[*] The population for Group Va is slightly less than for the Doctorates Granted Survey because four programs do not formally "house" faculty and their salaries.

Other Sources of Data

Vist the AMS website at `www.ams.org/employment/specialreports.html` for a listing of additional sources of data on the Mathematical Sciences.

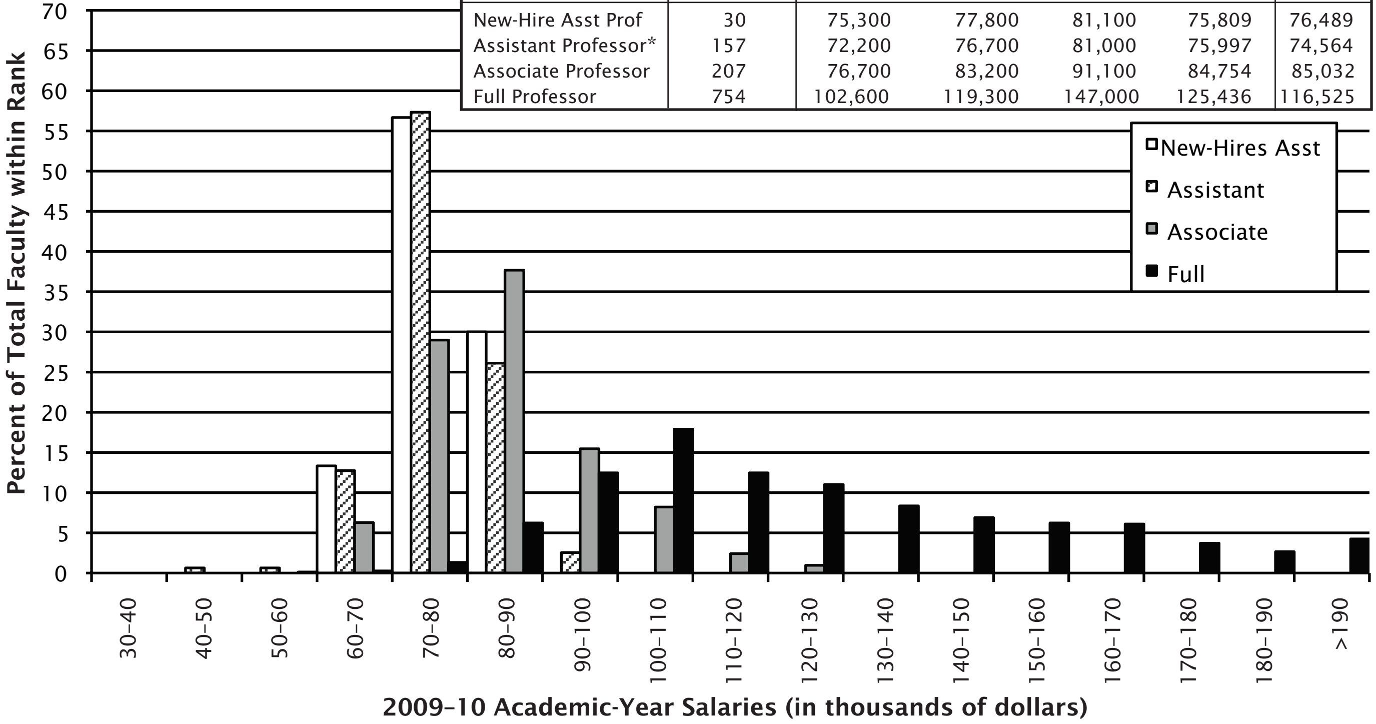
Polly Phipps is a senior research statistician with the Bureau of Labor Statistics. James W. Maxwell is AMS associate executive director for special projects. Colleen A. Rose is AMS survey analyst.

Group I (Public) Faculty Salaries

Doctoral degree-granting departments of mathematics

23 responses out of 25 departments (92%)

	2009–10					2008–09
Rank	No. Reported	Q_1	Median	Q_3	Mean	Mean
New-Hire Asst Prof	30	75,300	77,800	81,100	75,809	76,489
Assistant Professor*	157	72,200	76,700	81,000	75,997	74,564
Associate Professor	207	76,700	83,200	91,100	84,754	85,032
Full Professor	754	102,600	119,300	147,000	125,436	116,525

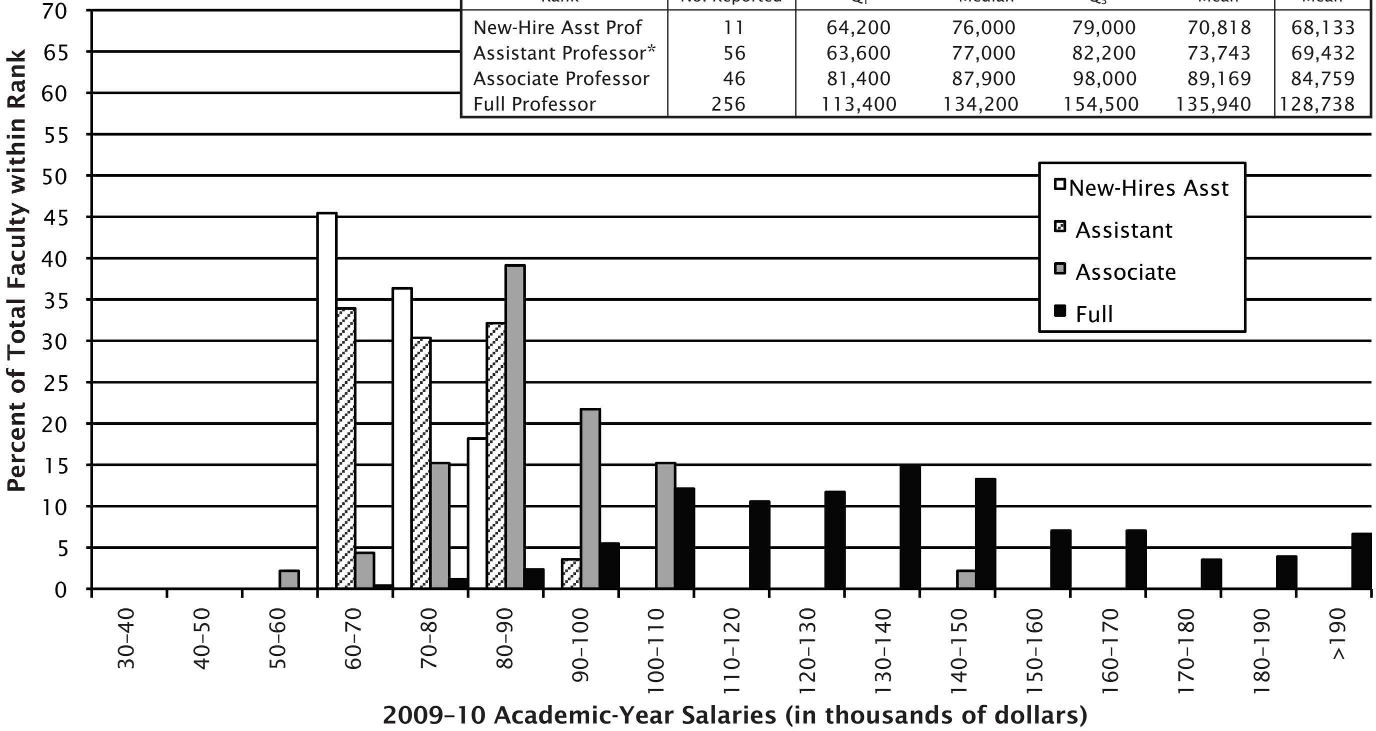


Group I (Private) Faculty Salaries

Doctoral degree-granting departments of mathematics

14 responses out of 23 departments (61%)

	2009–10					2008–09
Rank	No. Reported	Q_1	Median	Q_3	Mean	Mean
New-Hire Asst Prof	11	64,200	76,000	79,000	70,818	68,133
Assistant Professor*	56	63,600	77,000	82,200	73,743	69,432
Associate Professor	46	81,400	87,900	98,000	89,169	84,759
Full Professor	256	113,400	134,200	154,500	135,940	128,738



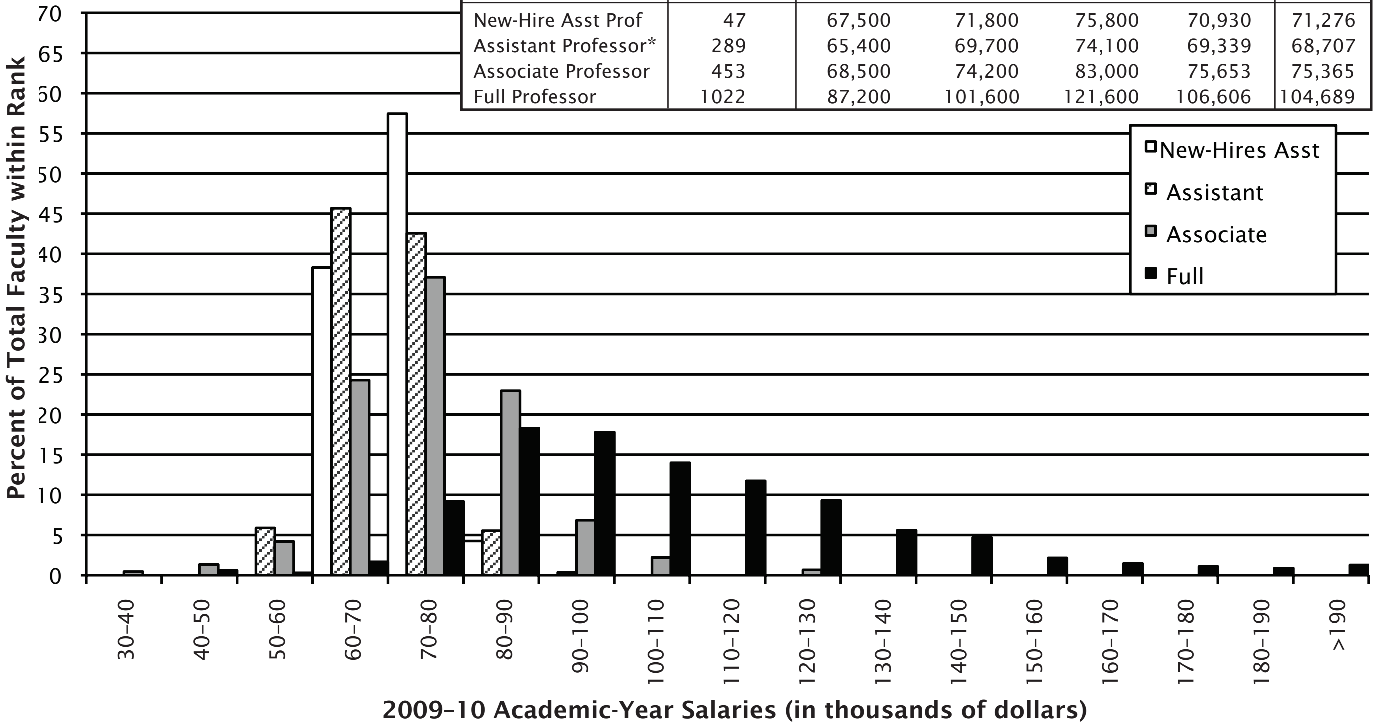
*Includes new hires.

Group II Faculty Salaries

Doctoral degree-granting departments of mathematics

50 responses out of 56 departments (89%)

	2009–10					2008–09
Rank	No. Reported	Q_1	Median	Q_3	Mean	Mean
New-Hire Asst Prof	47	67,500	71,800	75,800	70,930	71,276
Assistant Professor*	289	65,400	69,700	74,100	69,339	68,707
Associate Professor	453	68,500	74,200	83,000	75,653	75,365
Full Professor	1022	87,200	101,600	121,600	106,606	104,689

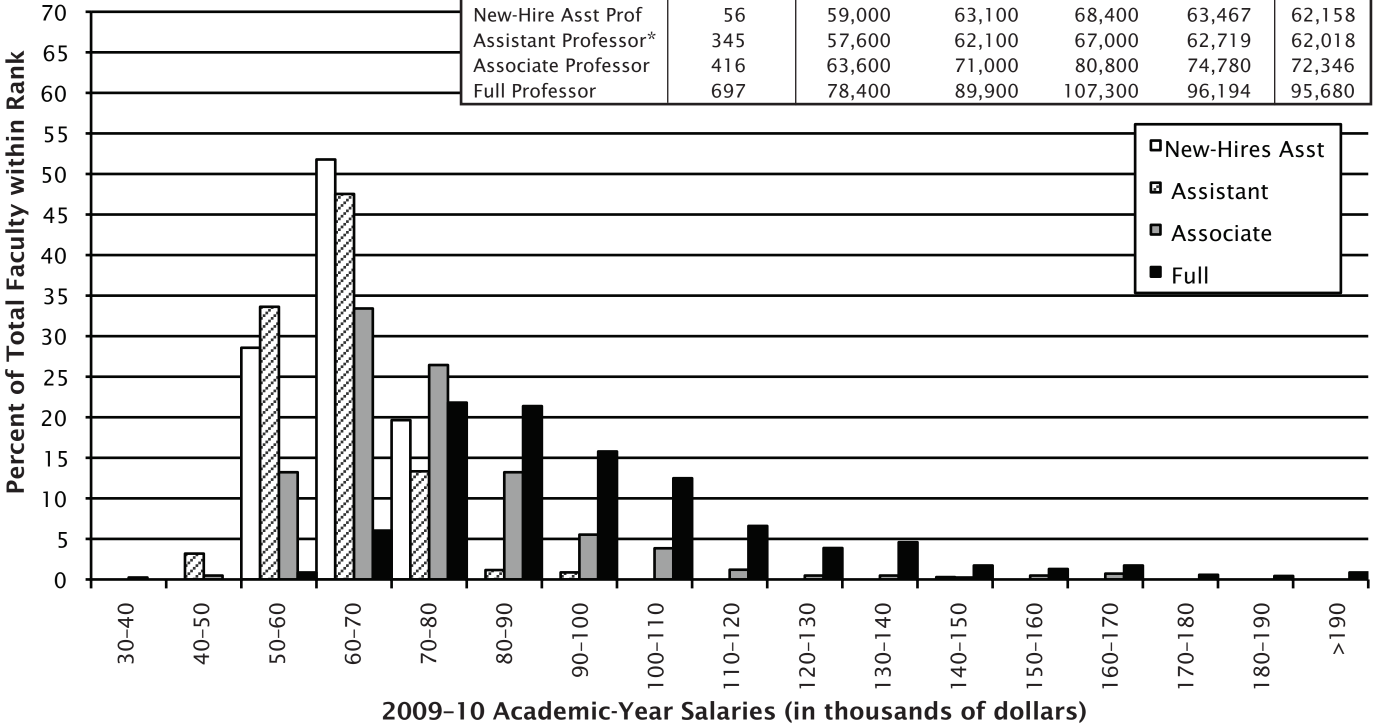


Group III Faculty Salaries

Doctoral degree-granting departments of mathematics

65 responses out of 81 departments (80%)

	2009–10					2008–09
Rank	No. Reported	Q_1	Median	Q_3	Mean	Mean
New-Hire Asst Prof	56	59,000	63,100	68,400	63,467	62,158
Assistant Professor*	345	57,600	62,100	67,000	62,719	62,018
Associate Professor	416	63,600	71,000	80,800	74,780	72,346
Full Professor	697	78,400	89,900	107,300	96,194	95,680



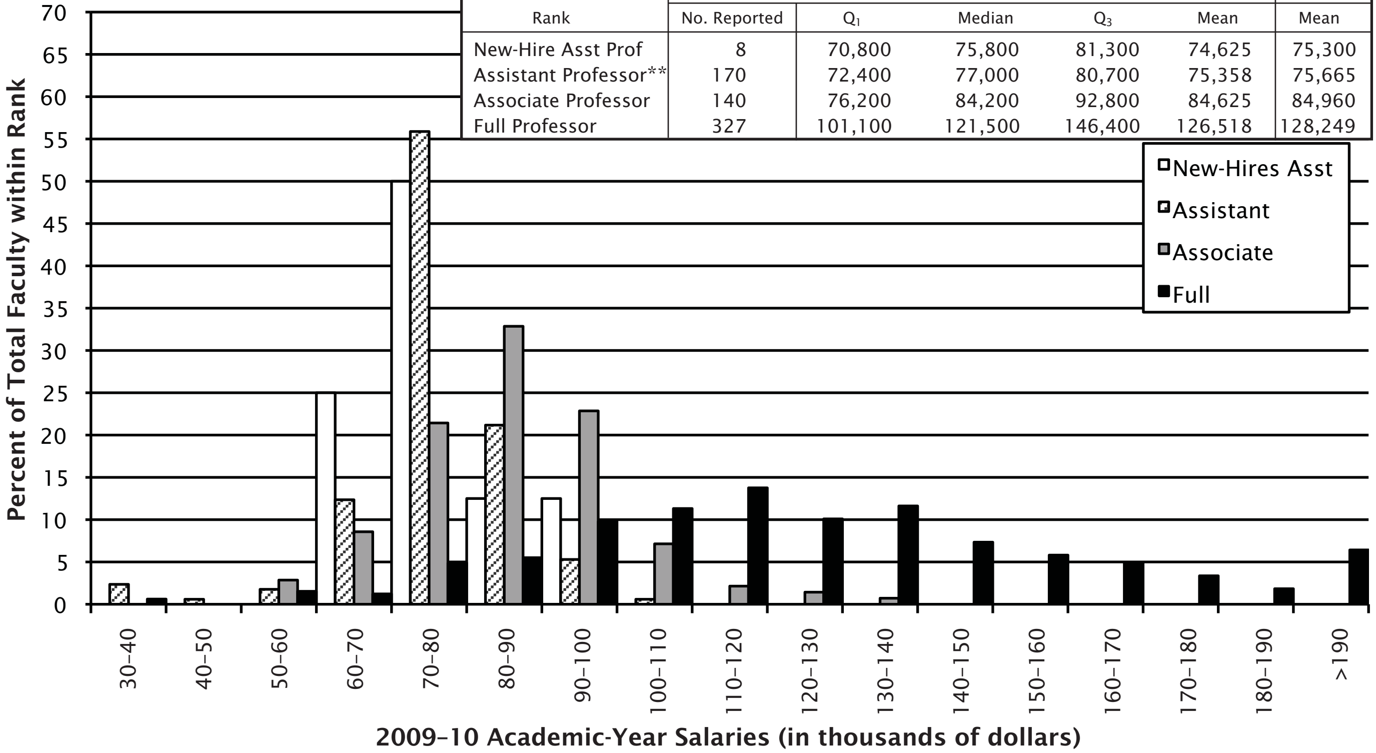
*Includes new hires.

Group IV Statistics Faculty Salaries*

Doctoral degree-granting departments of statistics

41 responses out of 57 departments (72%)

	2009–10					2008–09
Rank	No. Reported	Q₁	Median	Q₃	Mean	Mean
New-Hire Asst Prof	8	70,800	75,800	81,300	74,625	75,300
Assistant Professor**	170	72,400	77,000	80,700	75,358	75,665
Associate Professor	140	76,200	84,200	92,800	84,625	84,960
Full Professor	327	101,100	121,500	146,400	126,518	128,249

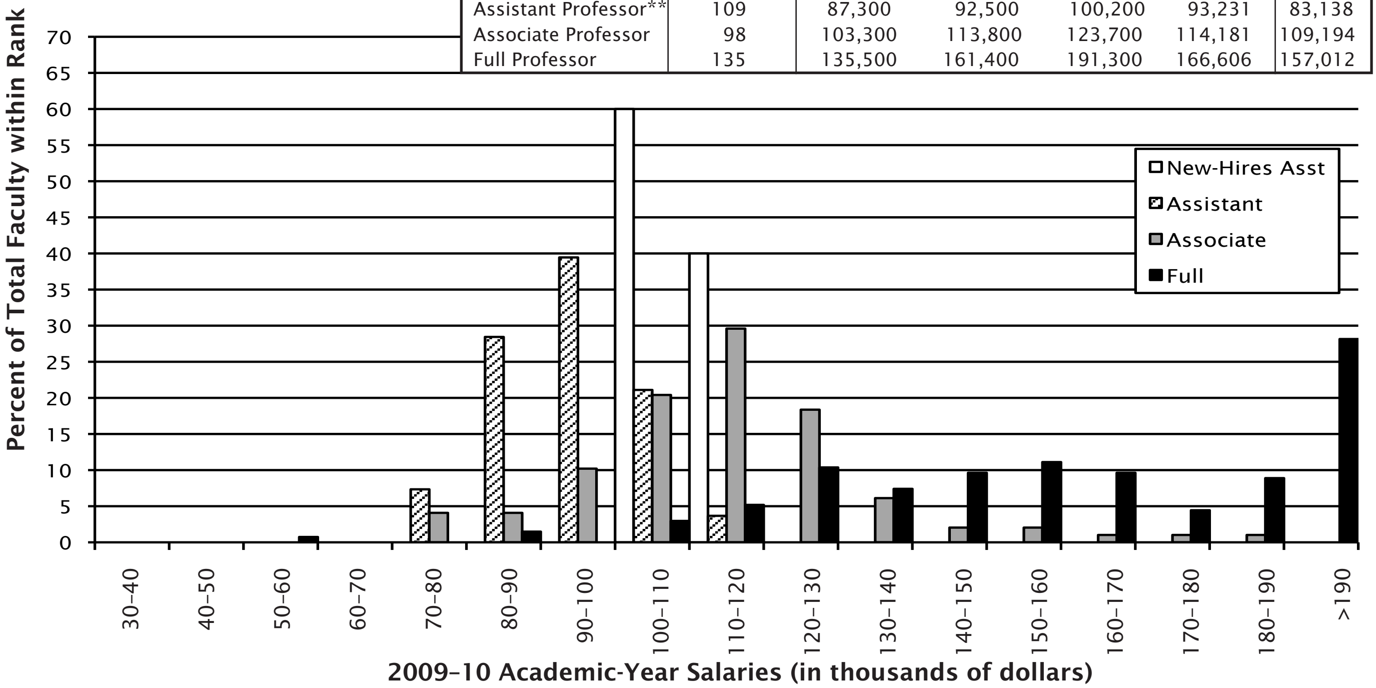


Group IV Biostatistics Faculty Salaries*

Doctoral degree-granting departments of biostatistics

21 responses out of 35 departments (60%)

	2009–10					2008–09
Rank	No. Reported	Q₁	Median	Q₃	Mean	Mean
New-Hire Asst Prof	10	104,400	107,900	114,000	109,209	77,813
Assistant Professor**	109	87,300	92,500	100,200	93,231	83,138
Associate Professor	98	103,300	113,800	123,700	114,181	109,194
Full Professor	135	135,500	161,400	191,300	166,606	157,012



*Faculty salary data provided by the American Statistical Association.

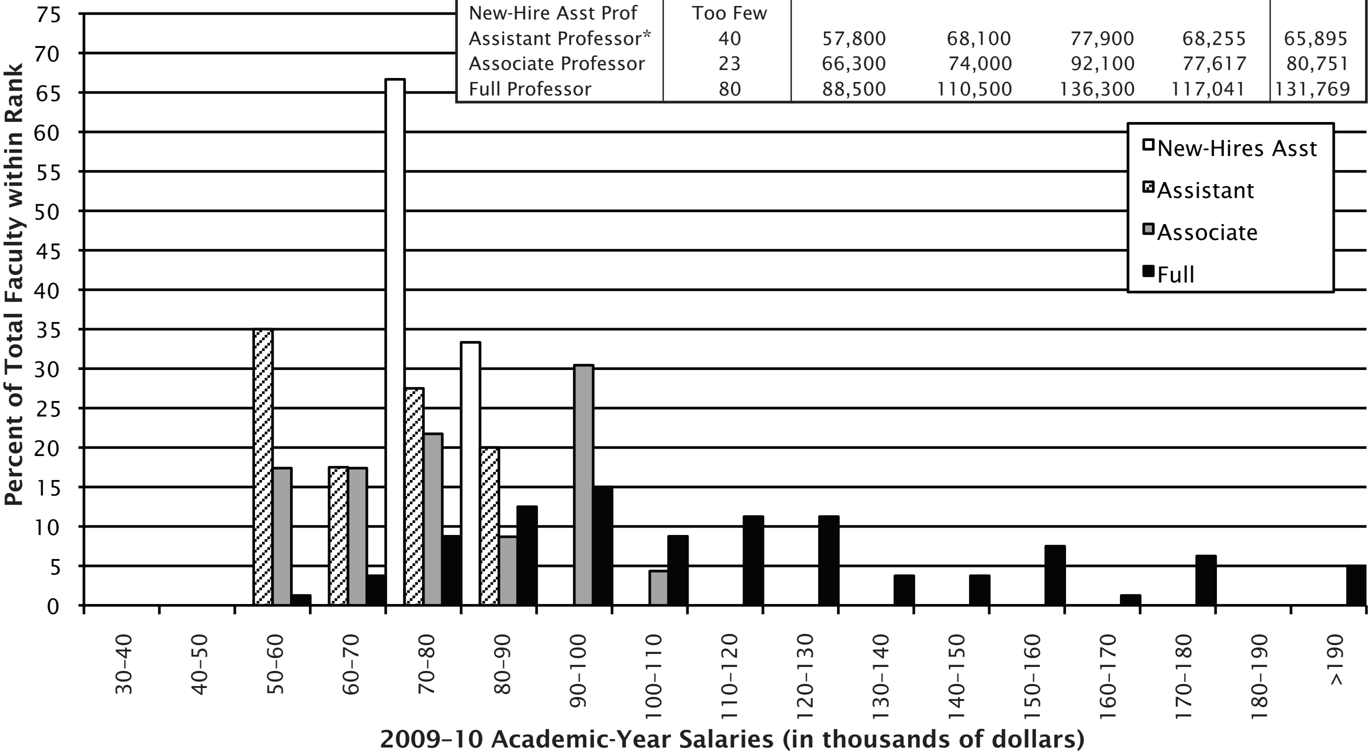
**Includes new hires.

Group Va Faculty Salaries

Doctoral degree-granting departments of applied mathematics

10 responses out of 18 departments (56%)

	2009–10					2008–09
Rank	No. Reported	Q_1	Median	Q_3	Mean	Mean
New-Hire Asst Prof	Too Few					
Assistant Professor*	40	57,800	68,100	77,900	68,255	65,895
Associate Professor	23	66,300	74,000	92,100	77,617	80,751
Full Professor	80	88,500	110,500	136,300	117,041	131,769



*Includes new hires.

Definitions of the Groups

Brief descriptions of the groupings are as follows:

Group I is composed of 48 departments with scores in the 3.00–5.00 range. Group I Public and Group I Private are Group I departments at public institutions and private institutions respectively.

Group II is composed of 56 departments with scores in the 2.00–2.99 range.

Group III contains the remaining U.S. departments reporting a doctoral program, including a number of departments not included in the 1995 ranking of program faculty.

Group IV contains U.S. departments (or programs) of statistics, biostatistics, and biometrics reporting a doctoral program.

Group Va is applied mathematics/applied science; Group Vb, which was no longer surveyed as of 1998–99, was operations research and management science.

Group M contains U.S. departments granting a master's degree as the highest graduate degree.

Group B contains U.S. departments granting a baccalaureate degree only.

Additional information on these groupings along with listings of the actual departments which compose each group is available on the AMS website at www.ams.org/employment/groups_des.html.

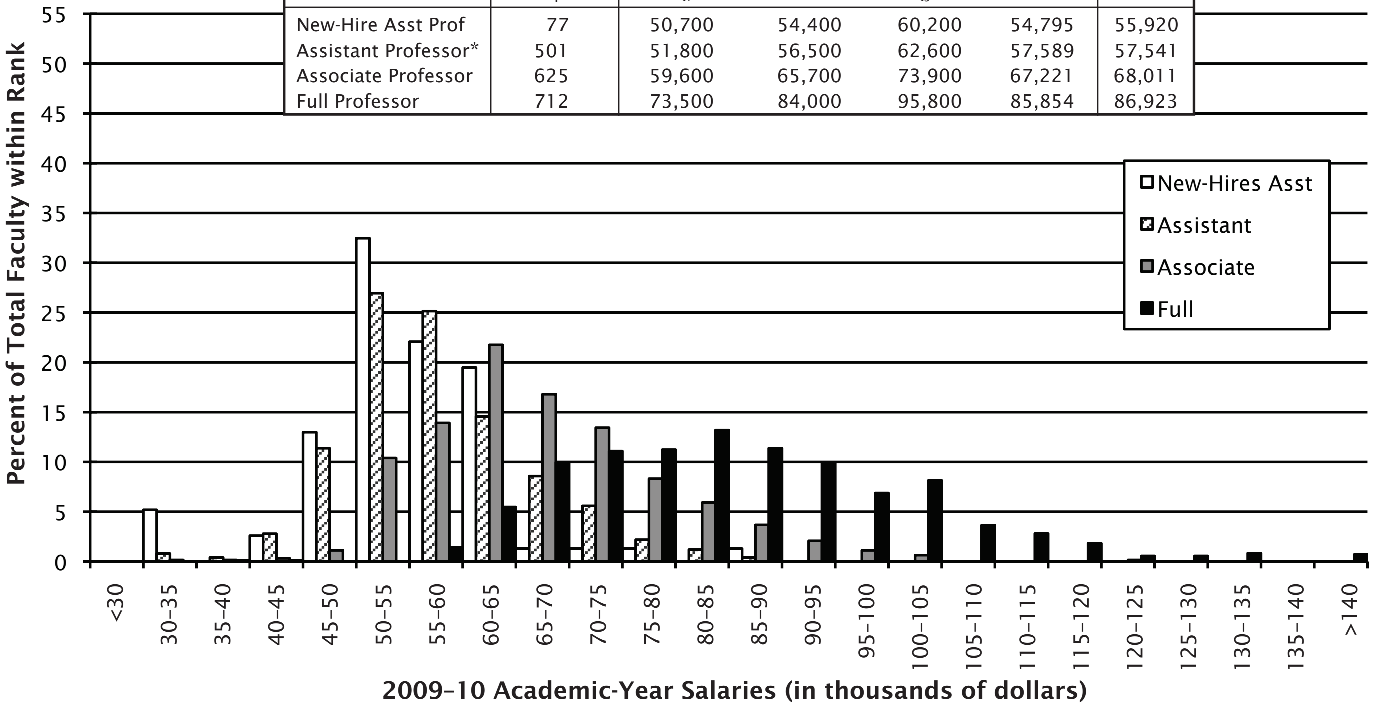
The Annual Survey series begun in 1957 by the American Mathematical Society is currently under the direction of the Data Committee, a joint committee of the American Mathematical Society, the American Statistical Association, the Institute of Mathematical Statistics, the Mathematical Association of America, and the Society of Industrial and Applied Mathematics. The current members of this committee are Richard Cleary, Richard M. Dudley, Susan Geller, John W. Hagood, Abbe H. Herzig, Ellen Kirkman, Joanna Mitro, James W. Maxwell (ex officio), Bart Ng, Polly Phipps (chair), Douglas Ravanel, Jianguo (Tony) Sun, and Marie Vitulli. The committee is assisted by AMS survey analyst Colleen A. Rose. Comments or suggestions regarding this Survey Report may be directed to the committee.

Group M Faculty Salaries

Master's degree-granting departments of mathematics

97 responses out of 182 departments (53%)

	2009–10					2008–09
Rank	No. Reported	Q_1	Median	Q_3	Mean	Mean
New-Hire Asst Prof	77	50,700	54,400	60,200	54,795	55,920
Assistant Professor*	501	51,800	56,500	62,600	57,589	57,541
Associate Professor	625	59,600	65,700	73,900	67,221	68,011
Full Professor	712	73,500	84,000	95,800	85,854	86,923

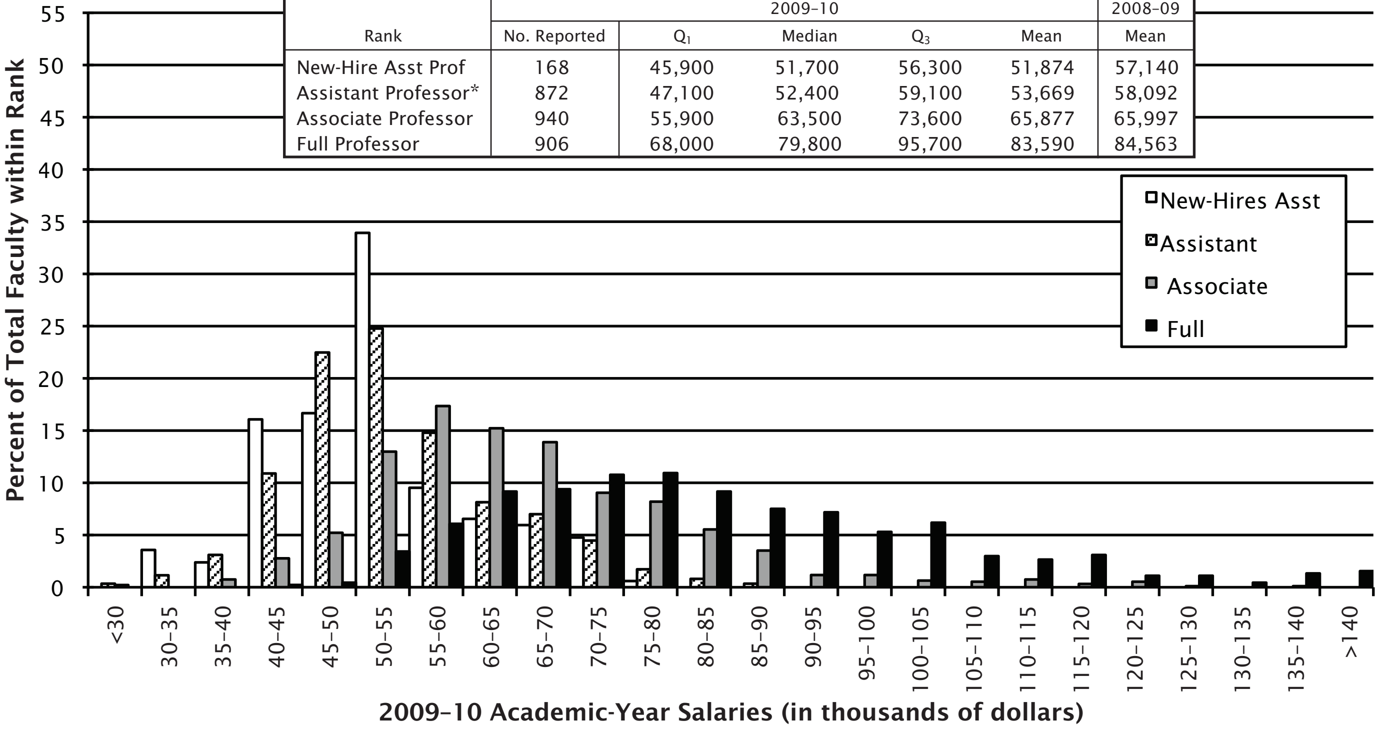


Group B Faculty Salaries

Bachelor's degree-granting departments of mathematics

310 responses out of 1037 departments (30%)

	2009–10					2008–09
Rank	No. Reported	Q_1	Median	Q_3	Mean	Mean
New-Hire Asst Prof	168	45,900	51,700	56,300	51,874	57,140
Assistant Professor*	872	47,100	52,400	59,100	53,669	58,092
Associate Professor	940	55,900	63,500	73,600	65,877	65,997
Full Professor	906	68,000	79,800	95,700	83,590	84,563



*Includes new hires.

Mathematics People

Keller Awarded Sherfield Fellowship

Mitchel Keller of the Georgia Institute of Technology has been awarded a Marshall Sherfield Fellowship for two years' postdoctoral study at a British university. Keller received his bachelor's degree in mathematics from North Dakota State University and will receive his Ph.D. in May 2010 from Georgia Tech. His research interests include combinatorics, particularly finite partially ordered sets; extremal combinatorics; and online combinatorial algorithms. He is assistant director of the Math Genealogy Project and was chosen an Outstanding Teaching Assistant at Georgia Tech in 2008. He hopes to use the fellowship in the Department of Mathematics at the London School of Economics. The fellowships, two of which are awarded each year, are funded by the Marshall Sherfield Fellowship Foundation and administered by the Marshall Commission; they enable American scientists or engineers to undertake postdoctoral research for a period of one to two academic years at a British university or research institute.

—Elaine Kehoe

Rhodes Scholarships Awarded

A student in the mathematical sciences is among thirty-two American men and women who have been chosen as Rhodes Scholars by the Rhodes Scholarship Trust. The Rhodes Scholars were chosen from among 805 applicants from 326 different colleges and universities.

Grace Tiao of Marietta, Georgia, graduated summa cum laude from Harvard College in 2008 with concentrations in English and American literature and language, and in history and science. An environmental scientist, she was manager of a 2008–09 expedition on ecosystem biodiversity in Antarctica, working with a New Zealand university. Tiao was features editor for the *Harvard Advocate,* Harvard's literary magazine, and an editor and staff writer for the *Harvard Science Review*. She also plays first violin in the Harvard Baroque Chamber orchestra. She has interned with the *Paris Review*. At Oxford, she plans to do the B.A. in mathematics and statistics.

—From a Rhodes Scholarship Trust announcement

Siemens Competition

Several students whose work involves the mathematical sciences have won prizes in the Siemens Competition in Math, Science, and Technology. Sean Karson of Trinity Preparatory School, Winter Park, Florida; Dan Liu of Liberal Arts and Science Academy High School, Austin, Texas; and Kevin Chen of William P. Clements High School, Sugar Land, Texas, won the team category and will share a US$100,000 scholarship for their mathematics research, titled "Related missing and decycling edges in directed graphs". The results of this project advance the infrastructure and knowledge of graph theory by shedding new light on a problem that has been open in the mathematics community since 1978. Their approach may open doors to a reduction of bottlenecks in complex networks such as the World Wide Web and transcontinental trade routes, thereby creating faster and more efficient processes. Their mentor was Jian Shen of Texas State University in San Marcos, Texas.

Karson has received the Rensselaer Polytechnic Institute Math and Science Award and is a National Merit Semifinalist. He used his love of puzzles to create a club called Rubik's Revenge to teach middle school students how to solve Rubik's Cube. He plays baseball and volunteers for the Center of Math, Arts, and Science Achievement, a program that encourages elementary school students to get excited about learning math and science. Liu is a member of the Liberal Arts and Science Academy's (LASA) National Honor Society Chapter and participates in the LASA Camerata Orchestra and Science Olympiad Team, as well as the Circle C Select Swim Team. He loves to play badminton and enjoys poker and computer games. Chen has been selected a finalist at the U.S. Computing Olympiad, a semifinalist for the U.S. Physics Olympiad, and regional winner of the Physics Bowl. He was also a three-time U.S. Mathematics Olympiad qualifier. He enjoys practicing piano, playing tennis, and programming games in his free time.

Randy Jia and David Lu of Detroit Country Day School in Beverly Hills, Michigan, received a scholarship of US$30,000 for their joint project in graph theory, "Matching preclusions for augmented cubes". Their project presents a way to measure the strength of a network in the event of link failure. They examined the matching preclusion number as it relates to the augmented cube graph. The augmented cube has been proposed as an example of a network that is resistant to link failure. The team answers the question of how many links need to be broken until it is no longer possible to pair up the nodes in the augmented cube. Their mentor was Eddie Cheng of Oakland University in Rochester, Michigan. Jia is a three-time United States Math Olympiad qualifier and received tenth place in the Michigan Math Prize Competition. He has participated in the Oakland University Summer Mathematics Institute every summer since eighth grade. He participates in various school volunteer opportunities, is a member of his school's track and field team, and enjoys basketball and fishing. He plans to major in finance/economics. Lu is a Science Olympiad participant and an active member of Quizbowl. He has participated in several mathematics competitions and attended the USA Mathematical Olympiad program in ninth grade. He was the MathCounts state winner in seventh and eighth grades and was among the top twelve in the national competition in eighth grade. He aspires to become a mathematics professor. He is a runner and participates in the Detroit Country Day School's cross country team, as well as in track and field.

Lynnelle Ye of Palo Alto High School, Palo Alto, California, received a US$50,000 scholarship for her project, "Chomp on graphs and subsets", in which she studied games in which two players take turns to eliminate nodes, or edges, of a graph. Game theory is applied in fields ranging from economics to engineering to systems in which individuals compete in a shared environment. The aim of the research was to understand the best possible strategy for playing this game and to determine which player will win from each starting graph when each plays her best possible strategy. She was mentored by Tirasan Khandhawit, a graduate student at the Massachusetts Institute of Technology. Ye won a gold medal at the 2008 China Girls Math Olympiad with the highest score on the United States team that year. She is also a three-time Math Olympiad Summer Program (MOSP) qualifier and two-time attendee. She has qualified for the USA Math Olympiad three times and been named to her school's Science Olympiad team each year since 2007. She has also qualified for the Research Science Institute. She enjoys reading, creative writing, art, and ballroom dancing. She hopes to become a professor of mathematics.

Dmitriy Kunisky of Livingston High School, Livingston, New Jersey, was awarded a US$20,000 scholarship for his mathematics project, which concerned the number derivative. His approach consisted of applying more sophisticated techniques from the theory of probability to create new results regarding this function's behavior. These results may have applications both in approaches to long-standing problems of number theory and as a practical application to cryptography. He was mentored by Alex Kontorovich of Brown University. Kunisky hopes to be a research mathematician at a university or an independent laboratory. He is currently a member of the National Honor Society, as well as the French Honor Society, and is recognized as a National Merit Scholarship Semifinalist, an AP Scholar with Distinction, and a Merck State Scholar. He placed second at the West Point Bridge Design Competition. He is president of his school's Organization of Student Tutors, which helps match students needing assistance to students willing to tutor them. He also enjoys reading, watching plays, playing tennis and ultimate Frisbee, and playing the guitar and piano.

—From a Siemens Competition announcement

Mathematics Opportunities

Proactive Recruitment in Introductory Science and Mathematics (PRISM)

The National Science Foundation (NSF) seeks proposals for its program in Proactive Recruitment in Introductory Science and Mathematics (PRISM). Proposals should emphasize improving the lower-division undergraduate (freshman and sophomore) experience in mathematics and statistics, better preparing undergraduates to major in science, engineering, mathematics, and statistics. Of particular interest are activities that share the excitement of science and mathematics with students, inspiring them to pursue and persist in these often demanding areas. Activities should help students understand both the central role of the mathematical sciences in fostering progress in other scientific disciplines and the continuing active development of the mathematical sciences themselves. Projects must include strong plans to proactively identify and recruit capable lower-division students with realistic chances of success in science and mathematics majors, especially those who might not otherwise pursue studies in these fields. The deadline for full proposals is **March 8, 2010.** For more information see the website `http://www.nsf.gov/pubs/2010/nsf10511/nsf10511.htm`.

—From an NSF announcement

Call for Nominations for Prizes of the Academy of Sciences for the Developing World

The Academy of Sciences for the Developing World (TWAS) prizes will be awarded to individual scientists in developing countries in recognition of outstanding contributions to knowledge in eight fields of science.

Eight awards are given each year in the fields of mathematics, medical sciences, biology, chemistry, physics, agricultural sciences, earth sciences, and engineering sciences. Each award consists of a prize of US$15,000 and a plaque. Candidates for the awards must be scientists who have been working and living in a developing country for at least ten years.

The deadline for nominations for the 2010 prizes is **March 31, 2010**. Nomination forms should be sent to: TWAS Prizes, c/o The Abdus Salam International Centre for Theoretical Physics (ICTP), Strada Costiera 11, 1-34151 Trieste, Italy; fax: 39 040 2240-698; email: `prizes@twas.org`. Further information is available on the World Wide Web at `http://www.twas.org/`.

—From a TWAS announcement

Fields-MITACS Undergraduate Summer Research Program

The Fields Institute announces a summer research program for undergraduates to be held during the summer of 2010 at the Fields Institute in downtown Toronto. The program will provide support for up to thirty students to take part in research programs supervised by leading researchers from the Fields Institute sponsoring universities as well as visiting researchers at the Institute. It is planned to be the first in a continuing series of such summer undergradute programs.

Students accepted into the program will receive student residence housing on the campus of the University of Toronto from July 3 to August 28, 2010; financial support for travel to Toronto; a per diem for meals and medical coverage for non-Canadian students during their stay.

Students will be assigned to work on research projects in groups of three or four. It is expected that several of the projects will be related to the Fields summer thematic program on the spread of drug resistance in infectious diseases that will be held at the Institute during July and

August, but other topics will also be the focus of student research groups. In some cases, students may also have the opportunity to spend a week off-site at the home campus of a project supervisor.

Undergraduate students in mathematics-related disciplines are encouraged to apply by: 1) sending a cover letter with a brief personal statement; 2) having an official transcript from their university sent directly to the Fields Institute; and 3) arranging for a letter of reference to be sent to Fields.

The deadline for applications is **February 20, 2010**. Send material to:

Alison Conway, Manager of Scientific Programs
MITACS-Fields Summer Undergraduate Research Program
222 College Street
Toronto, Ontario
Canada M5T 3J1

Note: Students requiring visas for travel to Canada will need to make their own arrangements to obtain the necessary documents. For more information see: `www.fields.utoronto.ca/programs/scientific/10-11/summer-research`.

—Fields Institute announcement

Correction

The photograph below, which appeared in the article "Kalman receives National Medal of Science", *Notices*, January 2010, should have been credited to Ryan K. Morris/National Science & Technology Medals Foundation.

—Sandy Frost

About the Cover

Cryptography issue

This cover is based on the Enigma rotor. The original image was found at the website `http://en.wikipedia.org/wiki/File:Enigma-rotor-stack.jpg`.

The Enigma photo was translated into ASCII using the Ascii Art Generator from Glass-Giant. The cover image was composed using GIMP. Cover work due to Geir Arne Hjelle.

Notices
of the American Mathematical Society
March 2010
Volume 57, Number 3
Numbers at Work and Play
page 334
Can't Decide? Undecide!
page 343
The Brave New World of Bodacious Assumptions in Cryptography
page 357
The Arithmetic Behind Cryptography
page 366
Newark Meeting
page 445
Cryptography Issue
(see page 419)

Correction

I am grateful to Robert Friedman for pointing out an error on page 813 of the article "The Dixmier-Douady invariant for dummies", *Notices*, August 2009. I stated that the vector bundle $V \to X$ used in the construction of $End(V)$ may be taken to have trivial first Chern class. This is correct if V is a line bundle but not in general, since for n-dimensional bundles the correct formula is $c_i(V \otimes L) = c_1(V) + nc_1(L)$. Part 2b of the following theorem must be similarly adjusted.

—Claude Schochet

For Your Information

Program Director Positions at NSF

The Division of Mathematical Sciences (DMS) announces a nationwide search for a number of program director positions at the National Science Foundation (NSF).

NSF program directors bear the primary responsibility for carrying out the NSF's overall mission: to support innovative and merit-reviewed activities in basic research and education that contribute to the nation's technical strength, security, and welfare. To discharge this responsibility requires not only knowledge in the appropriate disciplines but also a commitment to high standards, a considerable breadth of interest and receptivity to new ideas, a strong sense of fairness, good judgment, and a high degree of personal integrity.

Applicants should have a Ph.D. or equivalent training in a field of the mathematical sciences, a broad knowledge of one of the relevant disciplinary areas of the DMS, some administrative experience, a knowledge of the general scientific community, skill in written communication and preparation of technical reports, an ability to communicate orally, and several years of successful independent research normally expected of the academic rank of associate professor or higher. Skills in multidisciplinary research are highly desirable.

Qualified individuals who are women, ethnic/racial minorities, and/or persons with disabilities are strongly urged to apply. No person shall be discriminated against on the basis of race, color, religion, sex, national origin, age, or disability in hiring by the National Science Foundation.

Program director positions recruited under this announcement may be filled under one of the following appointment options:

Visiting Scientist Appointment: Appointment to this position will be made under the Excepted Authority of the NSF Act. Visiting scientists are on unpaid leave status from their home institutions and appointed to NSF's payroll as federal employees. NSF withholds Social Security taxes and pays the home institution's contributions to maintain retirement and fringe benefits (i.e., health benefits and life insurance) either directly to the home institution or to the carrier. Appointments are usually made for up to one year and may be extended for an additional year by mutual agreement.

Intergovernmental Personnel Act (IPA) Assignment: Individuals eligible for an IPA assignment with a federal agency include employees of state and local government agencies or institutions of higher education, Indian tribal governments, and other eligible organizations in instances in which such assignments would be of mutual benefit to the organizations involved. Initial assignments under IPA provisions may be made for a period of up to two years, with a possible extension for up to an additional two-year period. The individual remains an employee of the home institution, and NSF provides funding toward the assignee's salary and benefits. Initial IPA assignments are made for a one-year period and may be extended by mutual agreement.

Temporary Excepted Service Appointment: Appointment to this position will be made under the Excepted Authority of the NSF Act. Candidates who do not have civil service status or reinstatement eligibility will not obtain civil service status if selected. Candidates currently in the competitive service will be required to waive competitive civil service rights if selected. Usual civil service benefits (retirement, health benefits, life insurance) are applicable for appointments of more than one year. Temporary appointments may not exceed three years.

For additional information on NSF's rotational programs, see "Programs for Scientists, Engineers and Educators" on the NSF website at http://www.nsf.gov/about/career_opps.

Applicants should send a letter of interest and vita (preferably via email) to Deborah F. Lockhart, Deputy Division Director, Division of Mathematical Sciences, National Science Foundation, 4201 Wilson Boulevard, Suite 1025, Arlington, Virginia 22230; phone: 703-292-4858; fax: 703-292-9032; email: dlockhar@nsf.gov.

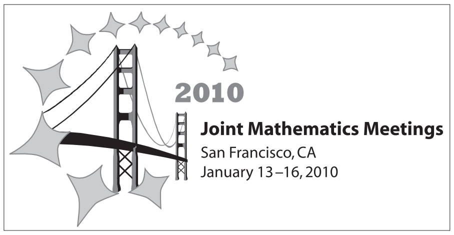
NSF is an Equal Opportunity Employer committed to employing a highly qualified staff that reflects the diversity of our nation. This announcement can also be found at http://www.nsf.gov/publications/pub_summ.jsp?ods_key=dms0601.

—DMS announcement

Inside the AMS

From the AMS Public Awareness Office

Highlights of the 2010 Joint Mathematics Meetings. Approximately 6,000 mathematicians attended the 2010 Joint Mathematics Meetings in San Francisco, California, January 13–16. Researchers presented over 2,000 papers from all specialties of mathematics, ranging from high-level research on new approaches to unsolved theoretical problems to recent applications of math to areas such as climate change, politics, and the arts. In addition, there were poster presentations by undergraduate students, several sessions on improving math education, the first national contest of *Who Wants to Be a Mathematician*, receptions, theatrical presentations, and the annual Mathematical Art Exhibition and Prize Ceremony. See photographs and write-ups about JMM 2010 at `http://www.ams.org/ams/jmm10-highlights.html`.



—Annette Emerson and Mike Breen
AMS Public Awareness Officers
`paoffice@ams.org`

AMS Hosts Congressional Briefing

Each year the AMS hosts a special presentation before members of Congress at a briefing on Capitol Hill. On October 28, 2009, Stuart Geman, professor of applied mathematics at Brown University, discussed the mathematical sciences as an integral component of modern-day technological innovation and development. He presented examples of film restoration and preservation and discussed the derivation of the structure of critical components of the influenza virus. He also noted that the misuse of mathematical and statistical tools can contribute to catastrophic events, such as the underestimation of the risks derived from widely used financial models that set the stage for the recent economic crisis.

Stuart Geman, professor of applied mathematics at Brown University, speaks at the recent congressional briefing in Washington, DC.

—AMS Washington Office

Deaths of AMS Members

C. Edmund Burgess, professor, from Troy, NY, died on November 18, 2004. Born on January 21, 1920, he was a member of the Society for 55 years.

Regina H. Garb, retired professor from Kean University, died on September 29, 2008. Born on June 9, 1922, she was a member of the Society for 39 years.

Jürgen Hurrelbrink, professor, Louisiana State University, died on March 13, 2009. Born on June 13, 1944, he was a member of the Society for 26 years.

Reference and Book List

*The **Reference** section of the* Notices *is intended to provide the reader with frequently sought information in an easily accessible manner. New information is printed as it becomes available and is referenced after the first printing. As soon as information is updated or otherwise changed, it will be noted in this section.*

Contacting the *Notices*

The preferred method for contacting the *Notices* is electronic mail. The editor is the person to whom to send articles and letters for consideration. Articles include feature articles, memorial articles, communications, opinion pieces, and book reviews. The editor is also the person to whom to send news of unusual interest about other people's mathematics research.

The managing editor is the person to whom to send items for "Mathematics People", "Mathematics Opportunities", "For Your Information", "Reference and Book List", and "Mathematics Calendar". Requests for permissions, as well as all other inquiries, go to the managing editor.

The electronic-mail addresses are `notices@math.wustl.edu` in the case of the editor and `notices@ams.org` in the case of the managing editor. The fax numbers are 314-935-6839 for the editor and 401-331-3842 for the managing editor. Postal addresses may be found in the masthead.

Upcoming Deadlines

February 15, 2010: Applications for Enhancing Diversity in Graduate Education (EDGE) Summer Program. See `http://www.edgeforwomen.org/?page_id=5.`

February 15, 2010: Applications for Institute for Pure and Applied Mathematics (IPAM) Research in Industrial Projects for Students (RIPS) undergraduate summer research program. See www.ipam.ucla.edu.

February 15, 2010: Applications for AMS-AAAS Congressional Fellowship. See `http://www.ams.org/government/congressfellowann.html` or contact the AMS Washington Office, telephone: 202-588-1100; email: `amsdc@ams.org.`

February 27, 2010: Entries for AWM Essay Contest. See `http://www.awm-math.org/biographies/contest.html.`

March 1, 2010: Applications for Summer Program for Women in Mathematics (SPWM2010). Contact the director, Murli M. Gupta, email: `mmg@gwu.edu;` telephone: 202-994-4857; or see the website `http://www.gwu.edu/~spwm/.`

March 1, 2010: Applications for Clay Mathematics Institute (CMI) Summer School on Probability and Statistical Physics in Two (and More) Dimensions.

Where to Find It

A brief index to information that appears in this and previous issues of the *Notices.*

AMS Bylaws—*November 2009, p. 1320*

AMS Email Addresses—*February 2010, p. 268*

AMS Ethical Guidelines—*June/July 2006, p. 701*

AMS Officers 2008 and 2009 Updates—*May 2009, p. 651*

AMS Officers and Committee Members—*October 2009, p. 1133*

Conference Board of the Mathematical Sciences—*September 2009, p. 977*

IMU Executive Committee—*December 2009, p. 1465*

Information for *Notices* Authors—*June/July 2009, p. 749*

Mathematics Research Institutes Contact Information—*August 2009, p. 854*

National Science Board—*January 2010, p. 68*

New Journals for 2008—*June/July 2009, p. 751*

NRC Board on Mathematical Sciences and Their Applications—*March 2010, p. 423*

NRC Mathematical Sciences Education Board—*April 2009, p. 511*

NSF Mathematical and Physical Sciences Advisory Committee—*February 2010, p. 272*

Program Officers for Federal Funding Agencies—*October 2009, p. 1126 (DoD, DoE); December 2007, p. 1359 (NSF); December 2009, p. 1464 (NSF Mathematics Education)*

Program Officers for NSF Division of Mathematical Sciences—*November 2009, p. 1313*

See http://www.claymath.org/summerschool or email: summerschool@claymath.org

March 8, 2010: Full proposals for NSF program in Proactive Recruitment in Introductory Science and Mathematics (PRISM). See "Mathematics Opportunities" in this issue.

March 31, 2010: Nominations for 2010 TWAS Prizes. See "Mathematics Opportunities" in this issue.

April 15, 2010: Applications for fall 2010 semester of Math in Moscow. See http://www.mccme.ru/mathinmoscow or write to: Math in Moscow, P.O. Box 524, Wynnewood, PA 19096; fax: +7095-291-65-01; email: mim@mccme.ru. For information on AMS scholarships see http://www.ams.org/outreach/mimoscow.html or write to: Math in Moscow Program, Membership and Programs Department, American Mathematical Society, 201 Charles Street, Providence RI 02904-2294; email: student-serv@ams.org.

May 1, 2010: Applications for May review for National Academies Postdoctoral and Senior Research Associateship Program. See http://sites.nationalacademies.org/PGA/RAP/PGA_050491 or contact Research Associateship Programs, National Research Council, Keck 568, 500 Fifth Street, NW, Washington, DC 20001; telephone 202-334-2760; fax 202-334-2759; email rap@nas.edu.

May 1, 2010: Applications for the fall 2010 program of the Christine Mirzayan Science and Technology Policy Graduate Fellowship program of the National Academies. See http://sites.nationalacademies.org/PGA/policyfellows/index.htm or contact The National Academies Christine Mirzayan Science and Technology Policy Graduate Fellowship Program, 500 Fifth Street, NW, Room 508, Washington, DC 20001; telephone: 202-334-2455; fax: 202-334-1667; email: policyfellows@nas.edu.

May 1, 2010: Applications for AWM Travel Grants. See http://www.awm-math.org/travelgrants.html; telephone: 703-934-0163; or email: awm@awm-math.org. The postal address is: Association for Women in Mathematics, 11240 Waples Mill Road, Suite 200, Fairfax, VA 22030.

June 1, 2010: Applications for NSF's Enhancing the Mathematical Sciences Workforce in the Twenty-First Century (EMSW21) program. See http://www.nsf.gov/pubs/2005/nsf05595/nsf05595.htm.

July 31, 2010: Nominations and applications for the 2010 Monroe H. Martin Prize. Contact R. Roy, Director, Institute for Physical Science and Technology, University of Maryland, College Park, Maryland 20742-2431.

August 1, 2010: Applications for August review for National Academies Postdoctoral and Senior Research Associateship Program. See http://sites.nationalacademies.org/PGA/RAP/PGA_050491 or contact Research Associateship Programs, National Research Council, Keck 568, 500 Fifth Street, NW, Washington, DC 20001; telephone 202-334-2760; fax 202-334-2759; email: rap@nas.edu.

October 1, 2010: Applications for AWM Travel Grants. See http://www.awm-math.org/travelgrants.html; telephone: 703-934-0163; email: awm@awm-math.org; or contact Association for Women in Mathematics, 11240 Waples Mill Road, Suite 200, Fairfax, VA 22030.

November 1, 2010: Applications for November review for National Academies Postdoctoral and Senior Research Associateship Program. See http://sites.nationalacademies.org/PGA/RAP/PGA_050491 or contact Research Associateship Programs, National Research Council, Keck 568, 500 Fifth Street, NW, Washington, DC 20001; telephone 202-334-2760; fax 202-334-2759 email: rap@nas.edu.

Board on Mathematical Sciences and Their Applications, National Research Council

The Board on Mathematical Sciences and Their Applications (BMSA) was established in November 1984 to lead activities in the mathematical sciences at the National Research Council (NRC). The mission of BMSA is to support and promote the quality and health of the mathematical sciences and their benefits to the nation. Following are the current BMSA members.

Tanya Styblo Beder, SB Consulting Corporation

Philip Bernstein, Microsoft Corporation

Patricia Brennan, University of Wisconsin

Emery N. Brown, Massachusetts Institute of Technology, Harvard Medical School

Gerald G. Brown, Naval Postgraduate School

Ricardo Caballero, Massachusetts Institute of Technology

Gunnar Carlsson, Stanford University

Brenda Dietrich, IBM Thomas J. Watson Research Center

Debra Elkins, Allstate Insurance Company

Susan Friedlander, University of Southern California

Peter Wilcox Jones, Yale University

Kenneth L Judd, Stanford University

C. David Levermore, (Chair), University of Maryland

Charles M. Lucas, Deer Isle Consulting

Vijayan N. Nair, University of Michigan

Claudia Neuhauser, University of Minnesota

J. Tinsley Oden, University of Texas at Austin

Donald Saari, University of California at Irvine

J. B. Silvers, Case Western Reserve University

George Sugihara, University of California, San Diego.

The postal address for BMSA is: Board on Mathematical Sciences and Their Applications, National Academy of Sciences, Room K974, 500 Fifth Street, NW, Washington, DC 20001; telephone: 202-334-2421; fax: 202-334-2422/2101; email: bms@nas.edu; website: http://www7.nationalacademies.org/bms/BMSA_Members.html.

Book List

The Book List highlights books that have mathematical themes and are aimed at a broad audience potentially including mathematicians, students, *and the general public. When a book has been reviewed in the* Notices*, a reference is given to the review. Generally the list will contain only books published within the last two years, though exceptions may be made in cases where current events (e.g., the death of a prominent mathematician, coverage of a certain piece of mathematics in the news) warrant drawing readers' attention to older books. Suggestions for books to include on the list may be sent to* `notices-booklist@ams.org`.

*Added to “Book List” since the list's last appearance.

The Archimedes Codex: How a Medieval Prayer Book Is Revealing the True Genius of Antiquity's Greatest Scientist, by Reviel Netz and William Noel. Da Capo Press, October 2007. ISBN 978-03068-1580-5. (Reviewed September 2008.)

The Calculus of Friendship: What a Teacher and Student Learned About Life While Corresponding About Math, by Steven Strogatz. Princeton University Press, August 2009. ISBN-13: 978-06911-349-32.

The Calculus Wars: Newton, Leibniz, and the Greatest Mathematical Clash of All Time, by Jason Socrates Bardi. Thunder's Mouth Press, April 2007. ISBN-13: 978-15602-5992-3. (Reviewed May 2009.)

Chez les Weils (French), by Sylvie Weil. Buchet-Chastel, January 2009. ISBN-13: 978-22830-236-93.

Crocheting Adventures with Hyperbolic Planes, by Daina Taimina. A K Peters, March 2009. ISBN-13: 978-15688-145-20.

Decoding the Heavens: A 2,000-Year-Old Computer—and the Century-Long Search to Discover Its Secrets, by Jo Marchant. Da Capo Press, February 2009. ISBN-13: 978-03068-174-27.

Embracing the Wide Sky: A Tour Across the Horizons of the Human Mind, by Daniel Tammet. Free Press, January 2009. ISBN-13: 978-14165-696-95.

Ernst Zermelo: An Approach to His Life and Work, by Heinz-Dieter Ebbinghaus. Springer, April 2007. ISBN-13 978-3-540-49551-2. (Reviewed August 2009.)

Gaming the Vote (Why Elections Aren't Fair and What We Can Do About It), by William Poundstone. Hill and Wang, February 2009. ISBN-13: 978-08090-489-22.

The Housekeeper and the Professor, by Yoko Ogawa. Picador, February 2009. ISBN-13: 978-03124-278-01.

How to Think Like a Mathematician: A Companion to Undergraduate Mathematics, by Kevin Houston. Cambridge University Press, March 2009. ISBN-13: 978-05217-197-80.

Leonhard Euler and His Friends: Switzerland's Great Scientific Expatriate, by Luis-Gustave du Pasquier (translated by John S. D. Glaus). CreateSpace, July 2008. ISBN: 978-14348-332-73.

Lewis Carroll in Numberland: His Fantastical Mathematical Logical Life: An Agony in Eight Fits, by Robin Wilson. W. W. Norton & Company. ISBN-13: 978-03930-602-70.

Logic's Lost Genius: The Life of Gerhard Gentzen, by Eckart Menzler-Trott, Craig Smorynski (translator), Edward R. Griffor (translator). AMS-LMS, November 2007. ISBN-13: 978-0-8218-3550-0.

The Mathematical Mechanic: Using Physical Reason to Solve Problems, by Mark Levi. Princeton University Press. ISBN: 978-0691140209.

*_Mathematicians: An Outer View of the Inner World_, by Mariana Cook, Princeton University Press, June 2009. ISBN13: 978-0-691-13951-7.

Mathematicans Fleeing from Nazi Germany: Individual Fates and Global Impact, by Reinhard Siegmund-Schultze. Princeton University Press, July 2009. ISBN 978-0-691-14041-4.

Mathematicians of the World, Unite!: The International Congress of Mathematicians: A Human Endeavor, by Guillermo P. Curbera. A K Peters, March 2009. ISBN-13: 978-15688-133-01.

Mathematics and Common Sense: A Case of Creative Tension, by Philip J. Davis. A K Peters, October 2006. ISBN 1-568-81270-1. (Reviewed June/July 2009.)

Mathematics Emerging: A Sourcebook 1540–1900, by Jacqueline Stedall. Oxford University Press, November 2008. ISBN-13: 978-01992-269-00.

Mathematics in Ancient Iraq: A Social History, by Eleanor Robson. Princeton University Press, August 2008. ISBN-13: 978-06910-918-22. (Reviewed in this issue.)

Mathematics in India, by Kim Plofker. Princeton University Press, January 2009. ISBN-13: 978-06911-206-76. (Reviewed in this issue.)

Mathematics in 10 Lessons: The Grand Tour, by Jerry P. King. Prometheus Books, May 2009. ISBN: 978-1-59102-686-0.

The Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook, by Victor J. Katz et al. Princeton University Press, July 2007. ISBN-13: 978-0-6911-2745-3.

The Millennium Prize Problems, edited by James Carlson, Arthur Jaffe, and Andrew Wiles. AMS, June 2006. ISBN-13: 978-08218-3679-8. (Reviewed December 2009.)

More Mathematical Astronomy Morsels, by Jean Meeus. Willmann-Bell, 2002. ISBN 0-943396743.

The Numbers Game: The Commonsense Guide to Understanding Numbers in the News, in Politics, and in Life, by Michael Blastland and Andrew Dilnot. Gotham, December 2008. ISBN-13: 978-15924-042-30.

The Numerati, by Stephen Baker. Houghton Mifflin, August 2008. ISBN-13: 978-06187-846-08. (Reviewed October 2009.)

Out of the Labyrinth: Setting Mathematics Free, by Robert Kaplan and Ellen Kaplan. Oxford University Press, January 2007. ISBN-13: 978-0-19514-744-5. (Reviewed June/July 2009.)

A Passion for Discovery, by Peter Freund. World Scientific, August 2007. ISBN-13: 978-9-8127-7214-5.

Perfect Rigor: A Genius and the Mathematical Breakthrough of the Century, by Masha Gessen. Houghton Mifflin Harcourt, November 2009. ISBN-13: 978-01510-140-64.

Picturing the Uncertain World: How to Understand, Communicate, and Control Uncertainty Through Graphical Display, by Howard Wainer, Princeton University Press, April 2009. ISBN-13: 978-06911-375-99.

Plato's Ghost: The Modernist Transformation of Mathematics, by Jeremy Gray. Princeton University Press, September 2008. ISBN-13: 978-06911-361-03. (Reviewed February 2010.)

The Princeton Companion to Mathematics, edited by Timothy Gowers (June Barrow-Green and Imre Leader, associate editors). Princeton University Press, November 2008. ISBN-13: 978-06911-188-02. (Reviewed November 2009.)

Proofs from THE BOOK, by Martin Aigner and Günter Ziegler. Expanded fourth edition, Springer, October 2009. ISBN-13: 978-3-642-00855-9

Pythagoras' Revenge: A Mathematical Mystery, by Arturo Sangalli. Princeton University Press, May 2009. ISBN-13: 978-06910-495-57.

Recountings: Conversations with MIT Mathematicians, edited by Joel Segel. A K Peters, January 2009. ISBN-13: 978-15688-144-90.

Roger Boscovich, by Radoslav Dimitric (Serbian). Helios Publishing Company, September 2006. ISBN-13: 978-09788-256-21.

Sacred Mathematics: Japanese Temple Geometry, by Fukagawa Hidetoshi and Tony Rothman. Princeton University Press, July 2008. ISBN-13: 978-0-6911-2745-3.

Solving Mathematical Problems: A Personal Perspective, by Terence Tao. Oxford University Press, September 2006. ISBN-13: 978-0-199-20560-8. (Reviewed February 2010.)

Sphere Packing, Lewis Carroll, and Reversi, by Martin Gardner. Cambridge University Press, July 2009. ISBN: 978-0521756075.

Strange Attractors: Poems of Love and Mathematics, edited by Sarah Glaz and JoAnne Growney. A K Peters, November 2008. ISBN-13: 978-15688-134-17. (Reviewed September 2009.)

The Strangest Man, by Graham Farmelo. Basic Books, August 2009. ISBN-13: 978-04650-182-77.

Super Crunchers: Why Thinking-by-Numbers Is the New Way to Be Smart, by Ian Ayres. Bantam, August 2007. ISBN-13: 978-05538-054-06. (Reviewed April 2009.)

Tools of American Math Teaching, 1800–2000, by Peggy Aldrich Kidwell, Amy Ackerberg-Hastings, and David Lindsay Roberts. Johns Hopkins University Press, July 2008. ISBN-13: 978-0801888144. (Reviewed January 2010.)

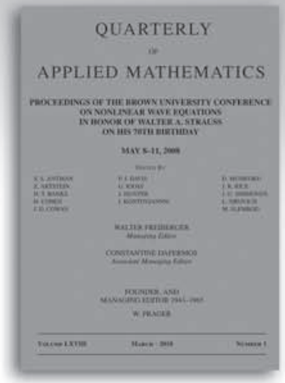
The Unfinished Game: Pascal, Fermat, and the Seventeenth-Century Letter That Made the World Modern, by Keith Devlin. Basic Books, September 2008. ISBN-13: 978-0-4650-0910-7.

What Is a Number?: Mathematical Concepts and Their Origins, by Robert Tubbs. Johns Hopkins University Press, December 2008. ISBN-13: 978-08018-901-85.

What's Happening in the Mathematical Sciences, by Dana Mackenzie. AMS, 2009. ISBN-13: 978-08218-447-86.

Why Does E=mc²? (And Why Should We Care?), by Brian Cox and Jeff Forshaw. Da Capo Press, July 2009. ISBN-13: 978-03068-175-88.

Zeno's Paradox: Unraveling the Ancient Mystery Behind the Science of Space and Time, by Joseph Mazur. Plume, March 2008 (reprint edition). ISBN-13: 978-0-4522-8917-8.



American Mathematical Society

AMS Award for Mathematics Programs *That Make a Difference*

Deadline: September 15, 2010

This award was established in 2005 in response to a recommendation from the AMS's Committee on the Profession that the AMS compile and publish a series of profiles of programs that:

1. aim to bring more persons from underrepresented minority backgrounds into some portion of the pipeline beginning at the undergraduate level and leading to advanced degrees in mathematics and professional success, or retain them once in the pipeline;

2. have achieved documentable success in doing so; and

3. are replicable models.

Two programs are highlighted annually.

Nomination process: Letters of nomination may be submitted by one or more individuals. Nomination of the writer's own institution is permitted. The letter should describe the specific program(s) for which the department is being nominated as well as the achievements that make the program(s) an outstanding success, and may include any ancillary documents which support the success of the program. The letter of nomination should not exceed two pages, with supporting documentation not to exceed three more pages. Up to three supporting letters may be included in addition to these five pages.

Send nominations to:
Programs That Make a Difference
c/o Ellen Maycock
American Mathematical Society
201 Charles Street
Providence, RI 02904
or via email to ejm@ams.org

Recent Winners:
2009: Department of Mathematics at the University of Mississippi; Department of Statistics at North Carolina State University.

2008: Summer Undergraduate Mathematical Science Research Institute (SUMSRI), Miami University (Ohio); Mathematics Summer Program in Research and Learning (Math SPIRAL), University of Maryland, College Park.

2007: Enhancing Diversity in Graduate Education (EDGE), Bryn Mawr College and Spelman College; and Mathematical Theoretical Biology Institute (MTBI), Arizona State University.

AMS
American Mathematical Society
www.ams.org

Mathematics Calendar

Please submit conference information for the Mathematics Calendar through the Mathematics Calendar submission form at http://www.ams.org/cgi-bin/mathcal-submit.pl. The most comprehensive and up-to-date Mathematics Calendar information is available on the AMS website at http://www.ams.org/mathcal/.

March 2010

1–May 28 **Doc-Course IMUS**, IMUS, University of Sevilla, Sevilla, Spain. (Dec. 2009, p. 1478)

8–12 **AIM Workshop: Mock Modular Forms in Combinatorics and Arithmetic Geometry**, American Institute of Mathematics, Palo Alto, California. (Jun./Jul. 2009, p. 770)

8–12 **Graphs and Arithmetic**, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec) H3T 1J4, Canada.

8–12 **Workshop on Graphs and Arithmetic**, Centre de recherches mathématiques, Université de Montréal, Montréal, Canada. (Oct. 2009, p. 1148)

8–June 11 **Long Program: Model and Data Hierarchies for Simulating and Understanding Climate**, Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California. (Apr. 2009, p. 526)

9–12 **Model and Data Hierarchies for Simulating and Understanding Climate: Tutorials**, Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles,CA (Nov. 2009, p. 1359)

* 13–15 **Fifth National Conference on Applicable Mathematics in Wave Mechanics and Vibrations (5th WMVC-2010)**, Kakatiya University, Warangal, A.P, 506009, India.
Description: This is an interdisciplinary event consisting of invited talks, contributed papers and panel discussion to be organized by the department of Mathematics, Kakatiya University, in collaboration with the Von Karman Society, West Bengal, India. The conference will encompass the general area of wave mechanics and vibrations. The mathematical modeling procedures in this area contribute to a considerable number of engineering and health care problems over a large number of length scales. The objective of the conference is to bring together scientists, engineers, and researchers on a common platform for "knowledge transfer".
Information: http://www.kakatiya.ac.in, www.kuwarangal.com.

14–17 **2010 Interpore Conference and Annual Meeting, Texas A&M, Mar 2010**, Texas A&M University, College Station, Texas. (Feb. 2010, p. 304)

15–19 **Arizona School of Analysis with Applications**, University of Arizona, Tucson, Arizona. (Feb. 2010, p. 304)

15–19 **Localization techniques in equivariant cohomology**, American Institute of Mathematics, Palo Alto, California. (May 2009, p. 659)

15–19 **MSRI—Research workshop: Homology Theories of Knots and Links**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1478)

17–19 **IAENG International Conference on Operations Research 2010**, Regal Kowloon Hotel, Hong Kong, China. (Aug. 2009, p. 863)

This section contains announcements of meetings and conferences of interest to some segment of the mathematical public, including ad hoc, local, or regional meetings, and meetings and symposia devoted to specialized topics, as well as announcements of regularly scheduled meetings of national or international mathematical organizations. A complete list of meetings of the Society can be found on the last page of each issue.

An announcement will be published in the *Notices* if it contains a call for papers and specifies the place, date, subject (when applicable), and the speakers; a second announcement will be published only if there are changes or necessary additional information. Once an announcement has appeared, the event will be briefly noted in every third issue until it has been held and a reference will be given in parentheses to the month, year, and page of the issue in which the complete information appeared. Asterisks (*) mark those announcements containing new or revised information.

In general, announcements of meetings and conferences carry only the date, title of meeting, place of meeting, names of speakers (or sometimes a general statement on the program), deadlines for abstracts or contributed papers, and source of further information. If there is any application deadline with respect to participation in the meeting, this fact should be noted. All communications on meetings and conferences in the mathematical sciences should be sent to the Editor of the *Notices* in care of the American Mathematical Society in Providence or electronically to notices@ams.org or mathcal@ams.org.

In order to allow participants to arrange their travel plans, organizers of meetings are urged to submit information for these listings early enough to allow them to appear in more than one issue of the *Notices* prior to the meeting in question. To achieve this, listings should be received in Providence **eight months** prior to the scheduled date of the meeting.

The complete listing of the Mathematics Calendar will be published only in the September issue of the *Notices*. The March, June/July, and December issues will include, along with new announcements, references to any previously announced meetings and conferences occurring within the twelve-month period following the month of those issues. New information about meetings and conferences that will occur later than the twelve-month period will be announced once in full and will not be repeated until the date of the conference or meeting falls within the twelve-month period.

The Mathematics Calendar, as well as Meetings and Conferences of the AMS, is now available electronically through the AMS website on the World Wide Web. To access the AMS website, use the URL: http://www.ams.org/.

17–26 **Second International School on Geometry and Physics. Geometric Langlands and Gauge Theory**, Centre de Recerca Matemàtica, UAB, E-08193 Bellaterra, Barcelona, Spain. (Nov. 2009, p. 1359)

18–20 **44th Spring Topology and Dynamics Conference 2010**, Mississippi State University, Starkville, Mississippi. (Sept. 2009, p. 1027)

18–20 **Workshop on Categorical Topology**, University of Azores, Ponta Delgada, Island of São Miguel, Azores, Portugal. (Dec. 2009, p. 1478)

18–21 **First International Conference on Mathematics and Statistics, AUS-ICMS '10**, American University of Sharjah (AUS), Sharjah, United Arab Emirates. (Jun./Jul. 2009, p. 770)

21–26 **MSRI—Symplectic and Contact Topology and Dynamics: Puzzles and Horizons**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1478)

22–26 **Computer Methods for L-functions and Automorphic Forms**, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec) H3T 1J4, Canada. (Feb. 2010, p. 304)

22–26 **Conference "Recent Advances in Function Related Operator Theory"**, Hotel "Rincon of the Seas", Rincon, Puerto Rico.

22–26 **Equation Hierarchies for Climate Modeling**, Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California. (Sept. 2009, p. 1028)

26–28 **CoNE Revisited: Celebrating the Inspirations of Michael O. Albertson**, Smith College, Northampton, Massachusetts. (Jan. 2010, p. 73)

27–28 **AMS Southeastern Section Meeting**, University of Kentucky, Lexington, Kentucky. (Sept. 2009, p. 1028)

29–April 2 **AIM Workshop: Computational optimization for tensor decompositions**, American Institute of Mathematics, Palo Alto, California. (Jun./Jul. 2009, p. 770)

30–April 1 **Second International Conference on Engineering Systems Management and Its Applications ICESMA2010**, American University of Sharjah, Sharjah, United Arab Emirates. (Oct. 2009, p. 1148)

April 2010

5–9 **PDEs, relativity and nonlinear waves**, Granada, Spain. (Jan. 2010, p. 73)

6–10 **Workshop on Iwasawa Theory over Function Fields of Characteristic p**, Centre de Recerca Matemàtica Apartat 50 E-08193, Bellaterra, Spain. (Jan. 2010, p. 73)

6–June 25 **Trimester in Combinatorics and Control: Workshop, School, Advanced Course, Research in Teams, and International Conference**, Madrid and Zaragoza, Spain. (Jan. 2010, p. 73)

* 9–11 **4th Podlasie Conference on Mathematics**, Bialystok University of Technology, Bialystok, Poland.
Description: The conference is organized by the Bialystok Branch of the Polish Mathematical Society. Besides the plenary session, four special sessions are planned: Algebra, Applications of Mathematics in Economy and Finance, Control Theory and Dynamical Systems, Mathematical Foundations of Computer Science. Participants are expected to give a talk in one of these sessions.
Language: English will be the official language of the conference. There will also be a Session on Didactics and Popularization of Mathematics, held in Polish.
Invited speakers: André Leroy (Université d'Artois, France), Andrzej Nowicki (Nicolaus Copernicus University, Poland), Christian Pötzsche (Münich University of Technology, Germany), Andrzej Skowron (Warsaw University, Poland), Łukasz Stettner (Institute of Mathematics of Polish Academy of Sciences, Poland), Aleksander Strasburger (Warsaw University of Life Sciences, Poland), Delfim Torres (Universidade de Aveiro, Portugal).
Information: `http://katmat.pb.bialystok.pl/pcm10`.

10–11 **AMS Central Section Meeting**, Macalester College, St. Paul, Minnesota. (Sept. 2009, p. 1028)

* 10–11 **8th Annual Graduate Student Topology and Geometry Conference**, University of Michigan, Ann Arbor, Michigan.
Description: Inviting graduate students from all over the country in topology and geometry to meet and give talks over two days.
Keynote speakers: Douglas Ravenel and Alan Reid.
Young faculty speakers: Moon Duchin, Tom Fiore, Benjamin Schmidt.
Deadline: To apply: February 9, 2010.
Information: Expository talk submissions welcome. Funding Available. Visit: `http://www-personal.umich.edu/~jmeyster/topologyconference/home.html`.

12–14 **SIAM Conference on Imaging Science (IS10)**, Chicago, Illinois. (Dec. 2009, p. 1478)

12–16 **Advanced Course and Workshop on Drinfeld Modules and L-functions**, Centre de Recerca Matemàtica Apartat 50 E-08193, Bellaterra, Spain. (Jan. 2010, p. 74)

12–16 **Climate Modeling: Numerical Hierarchies for Climate Modeling**, Introduction for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California. (Aug. 2009, p. 863)

12–16 **Computer Security and Cryptography**, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec) H3T 1J4, Canada. (Nov. 2009, p. 1359)

12–16 **IMA Workshop: Transport and Mixing in Complex and Turbulent Flows**, Institute for Mathematics and its Applications (IMA), University of Minnesota, Minneapolis, Minnesota. (Apr. 2009, p. 526)

14–17 **International Workshop on Multivariate Risks and Copulas**, Mohamed Khider University of Biskra, Algeria. (Aug. 2009, p. 863)

14–18 **International Conference on Fundamental Structures of Algebra in honor of the 70th birthday of Professor S¸erban Basarab**, Faculty of Mathematics and Computer Science, Ovidius University, Constanta, Romania. (Nov. 2009, p. 1359)

15–17 **35th Spring Lectures Series, 2010 "Minimal Surfaces and Mean Curvature Flow"**, University of Arkansas, Fayetteville, Arkansas. (Aug. 2009, p. 864)

17–18 **AMS Western Section Meeting**, University of New Mexico, Albuquerque, New Mexico. (Sept. 2009, p. 1028)

19–23 **Counting Points: Theory, Algorithms and Practice**, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec), H3T 1J4 Canada. (Jan. 2010, p. 74)

21–23 **Bone Tissue: Hierarchical Simulations for Clinical Applications**, Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California. (Jan. 2010, p. 74)

23–25 **Midwest Algebra, Geometry and their Interactions Conference MAGIC'10**, University of Notre Dame, Notre Dame, Indiana. (Dec. 2009, p. 1479)

28–May 1 **SIAM Conference on Data Mining (SDM10)**, Columbus, Ohio. (Dec. 2009, p. 1479)

May 2010

* 2–June 30 **Intensive period on: "Configuration Spaces: Geometry, Combinatorics and Topology"**, Centro di Ricerca Matematica Ennio De Giorgi, Pisa, Italy.
Description: First Announcement: The importance of configuration spaces has been growing steadily in central areas of mathematics often related to theoretical physics, hyperplane arrangements, and combi-

natorics. Despite their simple definition, configuration spaces admit important, broad applications with deep classical ties to knot theory, homotopical algebra, the theory of operands as well as conformal field theory. The theory of configuration spaces also has links to the study of low dimensional topology, and combinatorics. The aim of this initiative is to bring together in Pisa some of the leading experts in these different, but significantly overlapping areas, and to inform on the current state of the art, also promoting interaction among experts in order to foster new developments. This period includes minicourses, seminars, and two workshops May 24–26 and June 21–25 and is part of the CRM PISA 2010 scientific programme.

Scientific Committee: Anders Bjorner, Fred Cohen, Corrado De Concini, Claudio Procesi, Mario Salvetti.

Deadline: No attendance fee. Required registration to be made by March 15, 2010.

Information: `http://www.crm.sns.it/hpp/events/event.html?id=121`.

3–7 **Advanced Course on Foliations: Dynamics-Geometry-Topology**, Centre de Recerca Matemàtica (CRM), Bellaterra, Barcelona, Spain. (Sept. 2009, p. 1028)

3–7 **Second International Workshop on Zeta Functions in Algebra and Geometry**, Universitat de les Illes Balears, Palma de Mallorca, Spain. (Jan. 2010, p. 74)

3–7 **Simulation Hierarchies for Climate Modeling**, Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California. (Sept. 2009, p. 1029)

* 7–9 **Connections in Geometry and Physics 2010**, Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada.

Description: GAP 2010 brings together researchers who work at the interface between geometry and physics. It also serves to increase Canada's presence and visibility in geometry within the international mathematical community. The format of the conference will again combine three separate but related themes in geometry and physics, which we expect will result in a very interesting mixture of talks.

Themes: Mathematical relativity, gauge theory, and mirror symmetry.

Confirmed speakers so far: S. Alexakis (Toronto); V. Bouchard (Calgary); J. Bryan (UBC); F. Cachazo (Perimeter); J. Kamnitzer (Toronto); H. Reall (Cambridge); M.T. Wang (Columbia); S.T. Yau (Harvard). There will be at least four more speakers, plus short talks by local area postdocs.

Organizers: J. Gomis (Perimeter), M. Gualtieri (Toronto), S. Karigiannis (Waterloo), R. Moraru (Waterloo), R. Myers (Perimeter), M. Wang (McMaster).

Informattion: For the latest information and to register, visit the website: `http://www.math.uwaterloo.ca/~gap`.

10–14 **MSRI—Symplectic Geometry, Noncommutative Geometry and Physics**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1479)

13–15 **International Conference Devoted to the Memory of Academician M. Kravchuk (1892–1942)**, National Technical University of Ukraine, Kyiv, Ukraine. (Feb. 2010, p. 304)

14–15 **A Celebration of Mathematics and the 40th Anniversary of Jeffery Hall**, Queen's University, Kingston, Ontario, Canada. (Feb. 2010, p. 304)

16–22 **ESF Mathematics Conference in partnership with EMS and ERCOM Algebraic Methods in Dynamical Systems**, The Institute of Mathematics Conference Centre, Bedlewo, Poland. (Feb. 2010, p. 304)

17–20 **25th Annual Shanks Lecture and Conference: Optimal Configurations on the Sphere and Other Manifolds**, Vanderbilt University, Nashville, Tennessee. (Sept. 2009, p. 1029)

17–20 **The Seventh International Conference on Computational Physics**, Fragrant Hill Hotel, Beijing, China. (Feb. 2010, p. 304)

17–21 **AIM Workshop: Supercharacters and combinatorial Hopf algebras**, American Institute of Mathematics, Palo Alto, CA. (Nov. 2009, p. 1359)

* 17–21 **NSF/CBMS Regional Research Conference in the Mathematical Sciences, Nonlinear Water Waves with Applications to Wave-Current Interactions and Tsunamis**, The University of Texas-Pan American, Edinburg, Texas.

Speaker: The principal speaker will be Professor Adrian Constantin, Chair of Partial Differential Equations at the University of Vienna, Austria.

Additional invited lectures: Will also be featured by other leading experts, including Professors J. Bona, A. Degasperis, J. Escher, A. S. Fokas, R. Johnson, W. Strauss, J. F. Toland, E. Varvaruca, and possibly others. Participation is open to scientists working at research level on theoretical and practical aspects of the conference's topic.

Support: Some limited support is available for travel and local expenses. Underrepresented groups are strongly encouraged to apply.

Information: `http://www.math.utpa.edu/nsf-cbms2010.html`.

17–22 **Frobenius splitting in algebraic geometry, commutative algebra, and representation theory**, University of Michigan, Ann Arbor, MI. (Nov. 2009, p. 1359)

* 18–22 **6th Conference on Function Spaces**, Southern Illinois University, Edwardsville, Illinois.

Description: Following the tradition of previous conferences, the meeting will cover a broad range of topics including Function Algebras, Banach Algebras, Spaces & Algebras of Analytic Functions, LP Spaces, Geometry of Banach Spaces, Isometries of Function Spaces, and related problems. We expect a small grant from the NSF to help to defray the local cost and the registration fee; priority will be given to young mathematicians (including graduate students) without any other source of support.

Information: `http://www.siue.edu/MATH/conference2010/`.

22–23 **AMS Eastern Section Meeting**, New Jersey Institute of Technology, Newark, New Jersey. (Sept. 2009, p. 1029)

23–26 **SIAM Conference on Mathematical Aspects of Materials Science (MS10)**, Doubletree Hotel Philadelphia, Philadelphia, Pennsylvania. (Aug. 2009, p. 864)

23–28 **Conformal maps: from probability to physics**, Monte Verita, Ascona, Ticino, Switzerland. (Feb. 2010, p. 304)

23–29 **Almost Complex Geometry and Foliations**, University of Lille-1, Villeneuve d'Ascq, France. (Dec. 2009, p. 1479)

* 23–29 **2010 Talbot Workshop: Twisted K-theory and Loop Groups**, Breckenridge, Colorado.

Description: The workshop will constitute a weeklong retreat with talks and organized discussions during the mornings and evenings; the afternoon schedule will be kept clear for informal discussions and collaborations. The workshop will generally focus on understanding the relationship between the representation theory of a loop group LG and the equivariant twisted K-theory of G. Specifically, talks will develop the geometric approach to the representation theory of loop groups, K-theory and its twisted variant, basic computations of K-theory, Dirac operators and the families index theorem, extended topological field theories and Chern-Simons theory, conformal field theory and the WZW model, and recent work on extending Chern-Simons and gauged Gromov-Witten theory. The workshop discussions will have an expository character and will be aimed at graduate students and junior faculty interested in this area.

Information: If you are interested in participating, please apply at: `http://math.mit.edu/talbot/`.

24–28 **Applied Linear Algebra—in Honor of Hans Schneider**, Department of Mathematics, Faculty of Science, Novi Sad, Serbia. (Aug. 2009, p. 864)

24–28 **Data Hierarchies for Climate Modeling**, Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, California. (Sept. 2009, p. 1029)

25–28 **8th AIMS Conference on Dynamical Systems, Differential Equations and Applications**, Dresden, Germany. (Jun./Jul. 2009, p. 770)

25–29 **BALWOIS 2010: Fourth International Scientific Conference**, Ohrid, Republic of Macedonia. (Jun./Jul. 2009, p. 771)

25–June 2 **The 14th Conference on Modern Group Analysis**, Storforsen Hotel, Vidsel (near Lulea, Sweden). (Dec. 2009, p. 1480)

26–28 **International Conference on Computational Mathematics (ICCM) 2010 Waorkshop on Advances in Numerical Partial Differential Equations**, Holiday Inn Tobu Narita 320-1 TOKKO, CHIBA NARITA, CHIBA, 286-0106 JAPAN. (Nov. 2009, p. 1360)

26–28 **Workshop in ICCM 2010 on Advances in Numerical Partial Differential Equations (NPDEs)**, Holiday Inn Tobu Narita 320-1 TOKKO, CHIBA NARITA, CHIBA, 286-0106 JAPAN. (Nov. 2009, p. 1360)

26–29 **Workshop on Combinatorial and Additive Number Theory (CANT 2010)**, CUNY Graduate Center, New York, New York. (Feb. 2010, p. 305)

27–28 **From A=B to Z=60, A Conference in Honor of Doron Zeilberger's 60th Birthday**, Rutgers University, Piscataway,New Jersey. (Nov. 2009, p. 1360)

31–June 4 **Emerging Topics in Dynamical Systems and Partial Differential Equations**, Barcelona, Spain. (Dec. 2009, p. 1480)

* 31–June 5 **International conference on complex analysis dedicated to the memory of A. A. Gol'dberg**, Ivan Franko National University of Lviv, Lviv, Ukraine.
Description: The conference on complex analysis dedicated to the memory of Anatolii Gol'dberg (1930-2008) will take place in Lviv (Ukraine), May 31-June 5, 2010.
Topics: Complex analysis of one variable; complex analysis of several variables; complex approximation and continued fractions.
Main Organizers: The Lviv Mathematical Society and Ivan Franko National University of Lviv.
Information: `http://www.franko.lviv.ua/faculty/mechmat/Departments/TFTJ/analysis10/index.html`.

June 2010

* 1–4 **3rd International Conference (Chaos2010) on Chaotic Modeling, Simulation and Applications**, Chania, Crete, Greece.
Description: This is a reminder for the call for abstract submission (deadline December 20, 2009).
Topics: The general topics and the special sessions proposed for the Conference (Chaos2010) include but are not limited to: Chaos and Nonlinear Dynamics, Stochastic Chaos, Chemical Chaos, Data Analysis and Chaos, Hydrodynamics, Turbulence and Plasmas, Optics and Chaos, Chaotic Oscillations and Circuits, Chaos in Climate Dynamics, Geophysical Flows, Biology and Chaos, Neurophysiology and Chaos, Hamiltonian systems, Chaos in Astronomy and Astrophysics, Chaos and Solitons, Micro- and Nano-Electro-Mechanical Systems, Neural Networks and Chaos, Ecology and Economy.
Information: For more information and electronic abstract submission please visit the conference website at: `http://www.cmsim.info/` and send email to: `secretariat@cmsim.info`.

1–5 **IMA Workshop: Natural Locomotion in Fluids and on Surfaces: Swimming, Flying, and Sliding**, Institute for Mathematics and its Applications (IMA), University of Minnesota, Minneapolis, Minnesota. (Apr. 2009, p. 526)

* 2–4 **Klein conference**, Centro Internacional de Encuentros Matemáticos (CIEM), Castro Urdiales, Spain.
Description: The Klein project is an initiative of the International Commision for Mathematical Instruction (ICMI), the maximum international institution regarding Math Education, inspired by Felix Kleins' famous book "Elementary Mathematics from an Advanced Standpoint", published one century ago. The project is intended as a stimulus for mathematics teachers, to help them make connections between the mathematics they teach, or can be asked to teach, and the field of mathematics, taking into account the evolution of this field over the last century. As part of the project, several "Klein conferences" are going to take place around the World. CIEM will organize a Klein conference in Spain in June 2010. Several members of the design team, an international panel of eight people chaired by Bill Barton, will attend.
Goal: The main goal of the conference is to give the Spanish mathematical community as a whole the opportunity of getting involved in the project.
Information: `http://www.ciem.unican.es/klein2010`.

2–5 **Number Theory and Representation Theory—A conference in honor of Dick Gross' 60th birthday**, Science Center, Harvard University, Cambridge, Massachusetts. (Jun./Jul. 2009, p. 771)

3–5 **12th Chico Topology Conference**, Chico, California. (Jan. 2010, p. 74)

7–11 **AIM Workshop: Low dimensional structures in dynamical systems with variable time lags**, American Institute of Mathematics, Palo Alto,CA. (Nov. 2009, p. 1360)

7–11 **International Conference on Applied Mathematics (with the first William Benter Prize in Applied Mathematics)**, City University of Hong Kong, Hong Kong. (Feb. 2010, p. 305)

7–11 **International Functional Analysis Meeting in Valencia on the Occasion of the 80th Birthday of Professor Manuel Valdivia**, University of Valencia, Valencia, Spain. (Feb. 2010, p. 305)

7–11 **7th Annual Conference on Theory and Applications of Models of Computation- TAMC 2010**, Charles University, Prague, Czech Republic. (Feb. 2010, p. 305)

8–9 **2010 Clay Research Conference**, Institut Henri Poincaré, Paris, France. (Dec. 2009, p. 1480)

* 8–11 **Nonlinear evolution equations**, Hotel "Conchiglia d'oro", Mondello (Palermo), Italy.
Description: The conference will be devoted to the discussion of some rapidly developing topics in degenerate and singular parabolic equations. In particular it will focus on Harnack inequalities, entropy methods and asymptotics, regularity theory, for solutions of nonlinear evolution equations. A session for contributed talks of young researchers will be scheduled.
Information: `http://www.imati.cnr.it/~gianazza/mondello2010`.

10–12 **Geometric and Probabilistic Aspects of General Relativity**, University of Strasbourg, Strasbourg, France. (Oct. 2009, p. 1148)

13–18 **48th International Symposium on Functional Equations**, Batz-sur-Mer, France. (Nov. 2009, p. 1360)

* 13–18 **GNAMPA - ERC Summer School**, Ischia, Italy.
Description: A Summer School in Calculus of Variations and PDEs will be held in Ischia (Italy) at Continental Terme Hotel, June 13–18, 2010.
Invited Lecturers: Luis Caffarelli, University of Texas at Austin (Regularity theory for quasilinear and fully nonlinear equations); Vicent Caselles, University Pompeu Fabra (The total variation model in image processing); Neil Trudinger, Australian National University (to be announced); Cedric Villani, Ecole Norm. Sup. Lyon (Smooth and nonsmooth geometrical aspects of optimal transport). Graduate students, and postdoctoral fellows are encouraged to apply for financial support.
Organizers: Luigi Ambrosio, Nicola Fusco.
Information: The application form for financial support and all information about the school can be found on the website: `http://www.dma.unina.it/~geometric_inequalities/events.html`.

14–17 **SIAM Conference on Discrete Mathematics (DM10)**, Austin, Texas. (Dec. 2009, p. 1480)

* 14–18 **Group Actions in Topology and Geometric Group Theory, The Third Group Action Forum Conference**, Adam Mickiewicz University, Poznan, Poland. (Feb. 2010, p. 305)
Description: The conference topics will focus on smooth group actions on manifolds and symmetry in geometric group theory. To investigate this theme, we hope to have a variety of talks ranging from the geometry and topology of manifolds to discrete group actions on CAT(0) spaces and buildings.
Information: `http://gaf.astagor.net/events/poznan2010`.

15–19 **The Thirteenth International Conference on "Hyperbolic Problems: Theory, Numerics and Applications"**, Beijing, People's Republic of China.

16–21 **XI International Conference "Current Geometry"**, Vietri sul Mare Salerno, Italy. (Feb. 2010, p. 305)

16–23 **Budapest Semesters in Mathematics 25th Anniversary Reunion and Conference**, Budapest, Hungary. (Nov. 2009, p. 1360)

17–19 **Coimbra Meeting on 0-1 Matrix Theory and Related Topics**, Department of Mathematics, University of Coimbra, Portugal. (Jun./Jul. 2009, p. 771)

17–19 **[FG60] Computational and Geometric Topology**, Bertinoro, Forli, Italy. (Feb. 2010, p. 305)

18–August 15 **Geometry, Topology, and Dynamics of Character Varieties**, Institute for Mathematical Sciences, National University of Singapore, Singapore. (Aug. 2009, p. 864)

19–24 **International Algebraic Conference dedicated to the 70th birthday of A. V. Yakovlev**, St. Petersburg, Russia. (Feb. 2010, p. 305)

20–25 **The Twelfth National Conference in Algebra (China)**, Northwest Normal University, Lanzhou, Gansu, China. (Feb. 2010, p. 305)

21–25 **Harmonic Analysis and Related Topics**, Instituto Superior Técnico, IST, Lisbon, Portugal. (Feb. 2010, p. 305)

* 21–25 **International Conference on Algebras and Lattices**, Prague, Czech Republic.
Description: The primary subject of the conference is universal algebra and lattice theory, including their applications in other areas.
Speakers: The program will feature invited lectures by Andrei Bulatov, Ralph Freese, Christian Herrmann, Marcin Kozik, Petar Markovic, Miklos Maroti, Ralph McKenzie, George McNulty, Michael Pinsker, Mark Sapir, and Mikhail Volkov.
Information: `http://www.karlin.mff.cuni.cz/~ical/`.

21–26 **"Alexandru Myller" Mathematical Seminar Centennial Conference**, "Al. I. Cuza" University of Iaşi, Romania. (Jun./Jul. 2009, p. 771)

21–26 **2nd International Conference for Promoting the Application of Mathematics in Technical and Natural Sciences (AMiTaNS'10)**, Sozopol, Bulgaria.

22–25 **Group Representation Theory and Related Topics**, EPFL, Centre Interfacultaire Bernoulli, Lausanne, Switzerland. (Feb. 2010, p. 306)

22–July 2 **RMMC 2010: Conservation Laws and Applications**, University of Wyoming, Laramie, Wyoming. (Jan. 2010, p. 75)

24–27 **ACA 2010: Applications of Computer Algebra**, Vlora, Albania. (Jan. 2010, p. 75)

* 25–29 **Conference "Algebraic Geometry, Algebraic K-theory, and Motives", dedicated to Andrei Suslin's 60th birthday**, Steklov Mathematical Institute, St. Petersburg, Russia.
Organizing committee: Ivan Panin, Andreas Rosenschon, Serge Yagunov.
Information: `http://www.pdmi.ras.ru/EIMI/2010/ag/`.

26–30 **2010 International Conference on Topology and its Applications**, Nafpaktos, Greece. (Jun./Jul. 2009, p. 771)

28–July 2 **The Józef Marcinkiewicz Centenary Conference (JM 100)**, A. Mickiewicz University, Faculty of Mathematics and Computer Science, Poznańoznań, Poland. (Aug. 2009, p. 864)

28–July 3 **Teichmüller Theory and its Interactions in Mathematics and Physics**, Centre de Recerca Matemàtica, Bellaterra, Spain. (Dec. 2009, p. 1480)

* 28–July 4 **The Second International School-seminar "Nonlinear Analysis And Extremal Problems"**, Institute for System Dynamics and Control Theory SB RAS, Irkutsk, Russia.
Description: Institute for System Dynamics and Control Theory SB RAS, Sobolev Institute of Mathematics, Siberian Branch of the Russian Academy of Science and Institute of Mathematics and Mechanics, Ural Branch of the Russian Academy of Science jointly organize the second international school-seminar "Nonlinear analysis and extremal problems".
Aim: To introduce young researchers to some topics of current research in the fields of: nonlinear analysis and its applications; dynamical systems; evolution equations and partial differential equations; calculus of variations and optimal control. The main part of the school-seminar will consist of series of lectures of leading scientists in the above fields, and the rest of the time will be devoted to short communications of the participants.
Information: `http://idstu.irk.ru/?q=node/461`.

* 28–July 16 **RTG Summer School on Inverse Problems & Partial Differential Equations**, University of Washington, Seattle, Washington.
Description: The Research Training Group in the Department of Mathematics at the University of Washington will host a summer school for advanced undergraduates and beginning graduate students on Inverse Problems & Partial Differential Equations. Students will attend lectures in the morning and problem sessions in small groups with mentors in the afternoon.
Topics: Two mini-courses will be given: 1. Gunther Uhlmann, Peter Kuchment: The Radon Transform and the X-Ray Transform; 2. Hart Smith: Orthogonal Bases and Multi-scale Analysis.
Deadline: Apply online by April 1, 2010.
Information: On-campus accommodation and meals will be provided, plus a travel allowance of up to $500. (The Summer School is supported by an NSF Research Training Grant. Support is restricted to U.S. citizens/permanent residents. Applications from international students may be considered, but international students must provide their own support for travel, accommodation, and meals.) Visit: `http://www.math.washington.edu/ipde`.

29–July 4 **23nd International Conference on Operator Theory**, West University of Timisoara, Timisoara, Romania. (Feb. 2010, p. 306)

30–July 2 **The 2010 International Conference of Applied and Engineering Mathematics**, Imperial College, London, U.K. (Dec. 2009, p. 1480)

July 2010

4–17 **40th Probability Summer School**, Saint-Flour, France. (Feb. 2010, p. 306)

5–9 **11th International Conference on p-adic Functional Analysis**, Universite Blaise Pascal, Les Cezeaux, Aubiere, France. (Oct. 2009, p. 1148)

5–9 **Modular Conference: Arithmetic of Modular Forms and Modularity Results**, Centre de Recerca Matemàtica Apartat 50 E-08193, Bellaterra, Spain. (Jan. 2010, p. 75)

6–8 **Conference on Industrial and Applied Mathematics**, Bandung Institute of Technology, Bandung, Indonesia (Nov. 2009, p. 1360)

* 6–9 **17th Workshop on Logic, Language, Information and Computation (WoLLIC 2010)**, University of Brasília, Brasília, Brazil.

Description: WoLLIC is an annual international forum on inter-disciplinary research involving formal logic, computing and programming theory, and natural language and reasoning. Each meeting includes invited talks and tutorials as well as contributed papers. The Seventeenth WoLLIC will be held in BrasÌlia, Brazil, from July 6th to 9th, 2010. It is sponsored by the Association for Symbolic Logic (ASL), the Interest Group in Pure and Applied Logics (IGPL), the The Association for Logic, Language and Information (FoLLI), the European Association for Theoretical Computer Science (EATCS), the Sociedade Brasileira de Computação (SBC), and the Sociedade Brasileira de Lógica (SBL).
Information: `http://wollic.org/wollic2010/`.

* 7–9 **Jornadas de Matem · tica Discreta y Algorotmica**, Centro Internacional de Encuentros Matemáticos (CIEM), Castro Urdiales, Spain.
Description: These "Jornadas" on Discrete Mathematics bring together, every two years, researchers related to both theoretical and applied discrete mathematics. Although their scope was originally Spanish, more and more European and international researchers are coming to recent editions.
Speakers: The 7th edition will be hosted by CIEM in July 2010, and will have the following invited speakers: Imre Bárány, Renyi Institute y University College London; Marc Noy, Universitat Politècnica de Catalunya; Igor Shparlinski, Macquarie University.
Information: `http://www.ciem.unican.es/encuentros/jmda2010/`.

* 10–14 **International Conference: The Sixth Dynamical Systems and Applications-2010**, Sea Life Hotel, Antalya, Turkey.
Aims and Topics of the Conference: The main aim of this conference is to provide impetus, motivation, and to bring together researchers and scientists working in the fields of Dynamical Systems and Applications by providing a forum for the academic exchange of ideas and recent research works. The proposed technical program of the conference will include contributed talks and keynote lectures. The areas of interest include but are not limited to: Ordinary and Partial Differential Equations, Difference Equations and Applications, Analysis and Applications, Applied Mathematics and Dynamical Systems.
Information: `http://faculty.uaeu.ac.ae/hakca/Antalya-Dynamic-Systems-2010/Antalya.htm`.

11–14 **24th European Conference on Operational Research (EURO XXIV)**, FCUL - University of Lisbon, Lisbon, Portugal. (Jan. 2010, p. 75)

12–14 **2010 International Conference on Theoretical and Mathematical Foundations of Computer Science (TMFCS-10)**, Orlando, Florida. (Feb. 2010, p. 306)

12–August 6 **Statistical Challenges Arising from Genome Resequencing**, Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom. (Sept. 2009, p. 1030)

12–15 **SIAM Conference on the Life Sciences (LS10)**, The David L. Lawrence Convention Center, Pittsburgh, Pennsylvania. (Apr. 2009, p. 526)

12–16 **2010 SIAM Annual Meeting (AN10)**, The David L. Lawrence Convention Center, Pittsburgh, Pennsylvania. (Apr. 2009, p. 526)

13–17 **5th International Conference on Origami in Science, Mathematics and Education (5OSME)**, Singapore Management University, Singapore, Singapore. (Jan. 2010, p. 75)

15–30 **XIII Summer Diffiety School**, Santo Stefano del Sole (Avellino), Italy. (Jan. 2010, p. 75)

19–August 13 **Gyrokinetics in Laboratory and Astrophysical Plasmas**, Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom. (Sept. 2009, p. 1031)

25–31 **The XXI School of Algebra**, Brasília, Brazil. (Dec. 2009, p. 1481)

26–30 **Analysis on Graphs and its Applications**, Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom. (Dec. 2009, p. 1481)

26–30 **6th International Conference on Lévy Processes: Theory and Applications**, Technical University of Dresden, Dresden, Germany. (Apr. 2009, p. 526)

26–August 6 **Winter School on Topics in Noncommutative Geometry**, Departamento de Matematica, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina. (Apr. 2009, p. 526)

27–31 **LinStat'2010 - International Conference on Trends and Perspectives in Linear Statistical Inference**, Polytechnic Institute of Tomar, Portugal. (Jan. 2010, p. 75)

28–30 **The Mathematics of Klee & Grunbaum: 100 Years in Seattle**, University of Washington, Seattle, Washington. (Feb. 2010, p. 306)

August 2010

* 1–7 **Perspectives in High Dimensions**, Case Western Reserve University, Cleveland, Ohio 44106.
Description: The aim of the conference is to reflect on recent and future developments in broadly understood geometric functional analysis, with emphasis on interactions with other subfields of mathematics and with other mathematical sciences, including but not limited to computer science, mathematical physics and statistics.
Scientific Committee: The scientific program will be set up under the guidance of the Scientific Committee consisting of: J. Bourgain, E. Candes, P. Diaconis, B. Klartag, S. Szarek, S. Vempala, R. Vershynin, E. Werner.
Supporters: The NSF via Focused Research Grant, which involves CWRU, Kent State Univ., Univ. of Michigan and Univ. of Missouri. We expect to be able to provide support to a substantial number of participants, with priority given to graduate students, junior researchers and to those lacking their own research funding, as well as to members of underrepresented groups.
Information: For more information see the conference Web page and/or contact one of the organizers listed there; `http://www.case.edu/artsci/math/perspectivesInHighDimensions/`.

2–6 **AIM Workshop: Differentiable structures on finite sets**, American Institute of Mathematics, Palo Alto, California. (Dec. 2009, p. 1481)

2–6 **Formal Power Series and Algebraic Combinatorics 2010**, San Francisco State University, San Francisco, CA, USA. (Nov. 2009, p. 1360)

2–13 **Third Hands-On Research in Complex Systems School**, University of Buea, Buea, Cameroon. (Dec. 2009, p. 1481)

4–7 **Jairo Charris Seminar 2010: Algebraic Aspects of Darboux Transformations, Quantum Integrable Systems and Supersymmetric Quantum Mechanics**, Universidad Sergio Arboleda, Sede Rodrigo Noguera Laborde, Santa Marta, Colombia. (Dec. 2009, p. 1481)

8–11 **Functional Analysis and Operator theory**, Indian Statistical Institute, Bangalore, India. (Aug. 2009, p. 864)

9–13 **Permutation Patterns 2010**, Dartmouth College, Hanover, New Hampshire. (Feb. 2010, p. 306)

11–14 **The Fourth International Conference on Neural, Parallel & Scientific Computations**, ICNPSC-4, Department of Mathematics, Morehouse College, Atlanta, Georgia. (Dec. 2009, p. 1481)

11–December 22 **Mathematical and Statistical Approaches to Climate Modelling and Prediction**, Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom. (Sept. 2009, p. 1031)

12–15 **International Conference on Recent Trends in Graph Theory and Combinatorics, ICRTGC-2010**, Cochin, India. (Jun./Jul. 2009, p. 771)

13–17 **ICM Satellite Conference on Probability and Stochastic Processes**, Indian Statistical Institute, Bangalore, India. (Dec. 2009, p. 1481)

14–17 **Satellite Conference of ICM 2010 on Mathematics in Science and Technology**, India Habitat Centre, Lodhi Road, New-Delhi, India. (Nov. 2009, p. 1360)

15–19 **Geometric, Asymptotic, Combinatorial Group Theory with Applications (GAGTA)**, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec), H3T 1J4 Canada. (Jan. 2010, p. 75)

16–19 **SIAM Conference on Nonlinear Waves and Coherent Structures (NW10)**, Sheraton Society Hill Hotel, Philadelphia, Pennsylvania. (Nov. 2009, p. 1361)

16–December 17 **MSRI Future Scientific Programs: Inverse Problems and Applications**, Mathematical Sciences Research Institute, Berkeley, California. (Aug. 2009, p. 864)

16–December 17 **MSRI Future Scientific Programs: Random Matrix Theory, Interacting Particle Systems and Integrable Systems**, Mathematical Sciences Research Institute, Berkeley, California. (Aug. 2009, p. 864)

16–December 22 **Partial Differential Equations in Kinetic Theories**, Isaac Newton Institute for Mathematical Sciences, Cambridge, United Kingdom. (Sept. 2009, p. 1031)

19–20 **MSRI—Connections for Women: Inverse Problems and Applications**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1482)

20–25 **Third International Conference on Boundary Value Problems, Integral Equations and Related Problems**, Beijing and Baoding, Hebei, China. (Aug. 2009, p. 864)

23–27 **International Workshop on Geodesics**, Chern Institute of Mathematics, Nankai University, Tianjin, China. (Jun./Jul. 2009, p. 771)

23–27 **MSRI—Introductory Workshop on Inverse Problems and Applications**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1482)

23–27 **Topics in Algorithmic and Geometric Group and Semigroup Theory**, Centre de recherches mathèmatiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec) H3T 1J4 Canada. (Jan. 2010, p. 76)

27–31 **Differential Geometry and its Applications**, Masaryk University, Faculty of Science, Brno, Czech Republic, Europe. (Feb. 2010, p. 306)

30–September 3 **Complexity and Group-based Cryptography**, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec) H3T 1J4 Canada. (Jan. 2010, p. 76)

September 2010

2–4 **Moduli spaces**, Institut de Recherche Mathématique Avancée, University of Strasbourg, France. (Jan. 2010, p. 76)

7–10 **First International Workshop on Differential and Integral Equations with Applications in Biology and Medicine**, Aegean University, Karlovassi, Samos island, Greece. (Oct. 2009, p. 1148)

7–11 **International Conference "Modern Stochastics: Theory and Applications II"**, Kyiv National Taras Shevchenko University, Kyiv, Ukraine. (Feb. 2010, p. 306)

7–11 **Logic, Algebra and Truth Degrees 2010**, Prague, Czech Republic. (Feb. 2010, p. 307)

7–12 **Geometry, Dynamics, Integrable Systems 2010**, Mathematical Institute SANU, Belgrade, Serbia. (Feb. 2010, p. 307)

11–17 **NAFSA 9–The 9th International School on Nonlinear Analysis, Function Spaces and Applications**, Trest Castle, Czech Republic. (Oct. 2009, p. 1148)

12–17 **ESF Mathematics Conference in Partnership with EMS and ERCOM/INI: Highly Oscillatory Problems: From Theory to Applications**, The Isaac Newton Institute, Cambridge, United Kingdom. (Feb. 2010, p. 307)

13–17 **Third International Congress on Mathematical Software [ICMS'2010—developers meeting]**, Department of Mathematics, Kobe University, Kobe, Japan. (Feb. 2010, p. 307)

13–17 **Random Matrix Theory and Its Applications I**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1482)

13–December 17 **Modern Trends in Optimization and Its Application**, Institute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeles, CA. (Nov. 2009, p. 1361)

*15–18 **Conference in Numerical Analysis (NumAn 2010): Recent Approaches to Numerical Analysis: Theory, Methods and Applications**, Great Arsenale (Old Venetian Harbor) Chania, Island of Crete, Greece.
Description: The themes of NumAn2010 are in the broad area of numerical analysis and applications, including: numerical methods and algorithms, numerical computing and software, applications of numerical methods to science, engineering, biology, finance, etc. - parallel and high-performance numerical computation - scientific computing. The aims of the conference are: 1. to bring together and bequeath scientific activities, directions and pursuits of scientists on subjects that pertain to the conference, 2. to foster an exchange of views and ideas, 3. to study the theoretical background required for methods, algorithms and techniques used in applications, 4. to search directions of theoretical results towards applications, 5. to highlight open problems and future directions of numerical analysis.
Deadline: We invite interested researchers to submit one-page abstracts, for lecture or poster presentations, on topics pertaining to the themes of the conference by Monday March 1, 2010.
Information: `http://numan2010.science.tuc.gr`.

17–19 S^4 **Conference on Symmetry, Separation, Superintegrability and Special Functions**, School of Mathematics, University of Minnesota, Minneapolis, Minnesota. (Feb. 2010, p. 307)

20–21 **MSRI—Connections for Women: An Introduction to Random Matrices**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1482)

20–24 **10th International Conference on Parametric Optimization and Related Topics (paraoptX)**, Karlsruhe Institute of Technology, Karlsruhe, Germany. (Dec. 2009, p. 1482)

*20–25 **XVI Geometrical Seminar**, Hotel Breza, Vrnjacka banja, Serbia.
Description: All topics in Geometry with their applications, as well as other subjects related to the main themes are welcome.
Information: Visit `http://tesla.pmf.ni.ac.rs/geometrijski_seminar/XVI%20GEOMETRICAL%20SEMINAR.htm`.

20–October 1 **Berlin Mathematical School Summer School 2010 on Discretization in Geometry and Dynamics**, Technische Universität Berlin, Germany. (Oct. 2009, p. 1148)

*21–24 **The 3rd International Conference on Nonlinear Dynamics**, National Technical University "Kharkov Polytechnical Institute", Kharkov, Ukraine.
Organizers: National Tech. Univ., Kharkov, Ukraine; McGill Univ., Canada; Aberdeen Univ., UK; Glascow Univ., UK; Kiev Inst. of Mech., Ukraine. Topics: Analytical and numerical methods in nonl. dynamics; Resonances and bifurcations; Nonl. normal modes; Transient and localization; Chaotic dynamics; Nonl. dynamics of continuous systems; Nonl. dynamics of structures and machines; Vibro-creep problems and other problems of nonl. dynamics. Call for papers: A one-page abstract must be sent to the e-mail: `Conference.kpi.nld@gmail.com`. The deadline for the abstract submission: Feb. 28, 2010. Co-Chairmen of

the Sci. Committee: M. Cartmell (UK), V. Kubenko (Ukraine), Yu. Mikhlin, C. Pierre (Canada), M. Wiercigroch (UK).
Contact: D. Breslavsky, Yu. Mikhlin, L. Kurpa, A. Larin, National Tech. Univ., 21 Frunze str., Kharkov, 61002, Ukraine; Phone: +38-057-7076032; Fax: +38-057-7076601.
Information: `http://kpispu.org.ua/en/ND2010_conference`.

* 23–26 **Second International Conference on Numerical Analysis and Approximation Theory: NAAT 2010**, Department of Applied Mathematics of the Faculty of Mathematics and Computer Science, Babes- Bolyai University, Cluj-Napoca, Romania.
Description: The topics of interest include: functions approximation, integral operators, differential operators, numerical analysis and stability methods, positive operators, rate of convergence, splines, wavelets, stochastic processes, approximation of linear functionals.
Information: `http://naat.math.ubbcluj.ro/`.

October 2010

2–3 **AMS Eastern Section Meeting**, Syracuse University, Syracuse, New York. (Sept. 2009, p. 1032)

4–9 **Group Actions and Dynamics**, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357, Montréal (Québec) H3T 1J4 Canada. (Jan. 2010, p. 76)

9–10 **AMS Western Section Meeting**, University of California, Los Angeles, California. (Sept. 2009, p. 1032)

10–15 **International Conference in Systems Biology (ICSB)**, Edinburgh International Conference Centre, The Exchange, Edinburgh, EH3 8EE, Scotland. (Jan. 2010, p. 76)

11–15 **Equations and First-order Properties in Groups**, Centre de recherches mathématiques, Université de Montrèal, Pavillon André-Aisenstadt, 2920, Chemin de la tour, room 5357 Montréal (Québec) H3T 1J41 Canada. (Jan. 2010, p. 76)

* 20–22 **International Conference in Modeling Health Advances 2010**, San Francisco, California.
Description: The purpose of this conference is to bring all the people working in the area of epidemiology under one roof and encourage mutual interaction. The conference ICMHA'10 is held under the World Congress on Engineering and Computer Science WCECS 2010. The WCECS 2010 is organized by the International Association of Engineers (IAENG), a non-profit international association for the engineers and the computer scientists. The congress has the focus on the frontier topics in the theoretical and applied engineering and computer science subjects. All submitted papers will be under peer review and accepted papers will be published in the conference proceeding (ISBN: 978-988-17012-0-6).
Draft Paper Submission Deadline: July 2, 2010.
Information: `http://www.iaeng.org/WCECS2010/ICMHA2010.html`.

26–29 **SIAM Conference on Applied Linear Algebra (LA09)**, Embassy Suites Hotel, Monterey Bay-Seaside, California. (Sept. 2009, p. 1032)

29–31 **AMS Central Section Meeting**, Notre Dame University, Notre Dame, Indiana. (Sept. 2009, p. 1032)

November 2010

6–7 **AMS Southeastern Section Meeting**, University of Richmond, Richmond, Virginia. (Sept. 2009, p. 1032)

8–10 **2010 IEEE International Conference on Technologies for Homeland Security**, Westin Hotel, Waltham, Massachusetts. (Feb. 2010, p. 307)

8–12 **MSRI—Inverse Problems: Theory and Applications**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1482)

December 2010

6–10 **MSRI—Random Matrix Theory and its Applications II**, Mathematical Sciences Research Institute, Berkeley, California. (Dec. 2009, p. 1482)

25–27 **International Conference on Current trends in Mathematics**, Allahabad, Uttar Pradesh, India. (May 2009, p. 659)

29–31 **ICCAM 2010: "International Conference on Computational and Applied Mathematics" Symposium Partial Differential Equations:Modeling, Analysis and Numerical Methods**, First Hotel Bangkong 2 Soi Somprasong 1, Petchaburi Road, Tanonphayathai, Rajthavee, Bangkok 10400 Thailand. (Nov. 2009, p. 1361)

January 2011

10–May 20 **MSRI Future Scientific Programs: Arithmetic Statistics**, Mathematical Sciences Research Institute, Berkeley, California. (Aug. 2009, p. 864)

10–May 20 **MSRI Future Scientific Programs: Free Boundary Problems, Theory and Applications**, Mathematical Sciences Research Institute, Berkeley, California. (Aug. 2009, p. 864)

* 23–25 **ACM-SIAM Symposium on Discrete Algorithms (SODA11)**, Holiday Inn, San Francisco Golden Gateway, San Francisco, California.
Description: SODA is jointly sponsored by the ACM Special Interest Group on Algorithms and Computation Theory and the SIAM Activity Group on Discrete Mathematics.
Information: `http://www.siam.org/meetings/da11/`.

The following new announcements will not be repeated until the criteria in the next to the last paragraph at the bottom of the first page of this section are met.

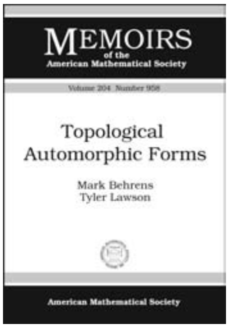
May 2011

* 22–26 **SIAM Conference on Applications of Dynamical Systems (DS11)**, Snowbird Ski and Summer Resort, Snowbird, Utah.
Description: This conference is sponsored by the SIAM Activity Group on Dynamical Systems.
Information: `http://www.siam.org/meetings/ds11/`.

New Publications Offered by the AMS

To subscribe to email notification of new AMS publications, please go to http://www.ams.org/bookstore-email.

Algebra and Algebraic Geometry


MEMOIRS of the American Mathematical Society
Volume 204 Number 958
Topological Automorphic Forms
Mark Behrens
Tyler Lawson
American Mathematical Society

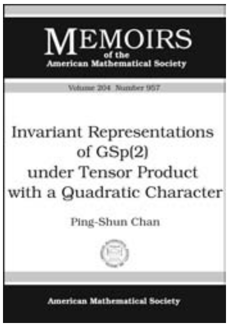
Topological Automorphic Forms

Mark Behrens, *Massachusetts Institute of Technology, Cambridge, MA*, and **Tyler Lawson**, *University of Minnesota, Minneapolis, MN*

Contents: p-divisible groups; The Honda-Tate classification; Tate modules and level structures; Polarizations; Forms and involutions; Shimura varieties of type $U(1, n-1)$; Deformation theory; Topological automorphic forms; Relationship to automorphic forms; Smooth G-spectra; Operation on *TAF*; Buildings; Hypercohomology of adele groups; $K(n)$-local theory; Example: chromatic level 1; Bibliography; Index.

Memoirs of the American Mathematical Society, Volume 204, Number 958

March 2010, 136 pages, Softcover, ISBN: 978-0-8218-4539-4, LC 2009049931, 2000 *Mathematics Subject Classification:* 55N35; 55Q51, 55Q45, 11G15, **Individual member US$44**, List US$74, Institutional member US$59, Order code MEMO/204/958


MEMOIRS of the American Mathematical Society
Volume 204 Number 957
Invariant Representations of GSp(2) under Tensor Product with a Quadratic Character
Ping-Shun Chan
American Mathematical Society

Invariant Representations of GSp(2) under Tensor Product with a Quadratic Character

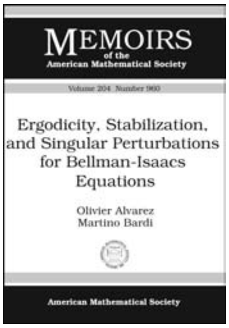
Ping-Shun Chan, *Ohio State University, Columbus, OH*

Contents: Introduction; ε-endoscopy for GSp(2); The trace formula; Global lifting; The local picture; Appendix A. Summary of global lifting; Appendix B. Fundamental lemma; Bibliography; List of symbols; Index.

Memoirs of the American Mathematical Society, Volume 204, Number 957

March 2010, 172 pages, Softcover, ISBN: 978-0-8218-4822-7, LC 2009049914, 2000 *Mathematics Subject Classification:* 11F70, 11F72, 11F85, **Individual member US$46**, List US$77, Institutional member US$62, Order code MEMO/204/957

Analysis


MEMOIRS of the American Mathematical Society
Volume 204 Number 960
Ergodicity, Stabilization, and Singular Perturbations for Bellman-Isaacs Equations
Olivier Alvarez
Martino Bardi
American Mathematical Society

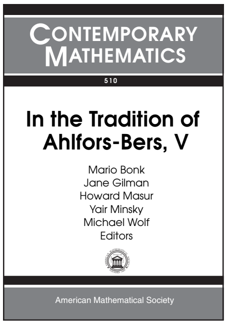
Ergodicity, Stabilization, and Singular Perturbations for Bellman-Isaacs Equations

Olivier Alvarez, *Université de Rouen, Mont-Saint Aignan, France*, and **Martino Bardi**, *Università di Padova, Italy*

Contents: Introduction and statement of the problem; Abstract ergodicity, stabilization, and convergence; Uncontrolled fast variables and averaging; Uniformly nondegenerate fast diffusion; Hypoelliptic diffusion of the fast variables; Controllable fast variables; Nonresonant fast variables; A counterexample to uniform convergence; Applications to homogenization; Bibliography.

Memoirs of the American Mathematical Society, Volume 204, Number 960

March 2010, 77 pages, Softcover, ISBN: 978-0-8218-4715-2, LC 2009049941, 2000 *Mathematics Subject Classification:* 35Bxx, 35Kxx, 93C70, 49N70; 49L25, 60J60, 91A23, 93E20, **Individual member US$38**, List US$64, Institutional member US$51, Order code MEMO/204/960



CONTEMPORARY MATHEMATICS

510

In the Tradition of Ahlfors-Bers, V

Mario Bonk
Jane Gilman
Howard Masur
Yair Minsky
Michael Wolf
Editors

American Mathematical Society

In the Tradition of Ahlfors–Bers, V

Mario Bonk, *University of Michigan, Ann Arbor, MI*, **Jane Gilman**, *Rutgers University, Newark, NJ*, **Howard Masur**, *University of Chicago, IL*, **Yair Minsky**, *Yale University, New Haven, CT*, and **Michael Wolf**, *Rice University, Houston, TX*, Editors

The Ahlfors–Bers Colloquia commemorate the mathematical legacy of Lars Ahlfors and Lipman Bers. The core of this legacy lies in the fields of geometric function theory, Teichmüller theory, hyperbolic geometry, and partial differential equations. However, the work of Ahlfors and Bers has impacted and created interactions with many other fields of mathematics such as algebraic geometry, dynamical systems, topology, geometric group theory, mathematical physics, and number theory. Recent years have seen a flowering of this legacy with an increased interest in their work.

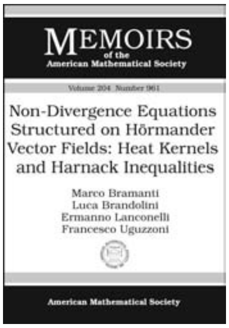
This current volume contains articles on a wide variety of subjects that are central to this legacy. These include papers in Kleinian groups, classical Riemann surface theory, translation surfaces, algebraic geometry and dynamics. The majority of the papers present new research, but there are survey articles as well.

Contents: **J. Belk** and **S. Koch**, Iterated monodromy for a two-dimensional map; **J. Bowman**, Orientation-reversing involutions of the genus 3 Arnoux-Yoccoz surface and related surfaces; **E. Bujalance** and **F.-J. Cirre**, A family of Riemann surfaces with orientation reversing automorhisms; **L. Arenas-Carmona** and **A. M. Rojas**, Unramified prime covers of hyperelliptic curves and pairs of p-gonal curves; **A. Carocca**, **H. Lange**, **R. E. Rodríguez**, and **A. M. Rojas**, Prym and Prym-Tyurin varieties: A group-theoretical construction; **V. Charette**, **T. A. Drumm**, and **W. Goldman**, Stretching three-holed spheres and the Margulis invariant; **B. Farb** and **H. Masur**, Teichmüller geometry of moduli space, II: $\mathcal{M}(S)$ seen from far away; **D. Gabai**, **R. Meyerhoff**, and **P. Milley**, Mom technology and hyperbolic 3-manifolds; **U. Hamenstädt**, Dynamical properties of the Weil-Petersson metric; **J. H. Hubbard** and **R. L. Miller**, Equidistribution of horocyclic flows on complete hyperbolic surfaces of finite area; **L. Ji** and **S. A. Wolpert**, A cofinite universal space for proper actions for mapping class groups; **M. Kapovich**, On sequences of finitely generated discrete groups; **R. P. Kent IV** and **C. J. Leininger**, A fake Schottky group in mod(S); **D. D. Long** and **A. W. Reid**, Eigenvalues of hyperbolic elements in Kleinian groups; **V. Malik**, Primitive words and self-intersections of curves on surfaces generated by the Gilman-Maskit discreteness algorithm; **K. Matsuzaki**, Symmetric groups that are not the symmetric conjugates of Fuchsian groups; **K. Ohshika** and **H. Miyachi**, Uniform models for the closure of the Riley slice; **G. Mondello**, Poisson structures on the Teichmüller space of hyperbolic surfaces with conical points.

Contemporary Mathematics, Volume 510

April 2010, 329 pages, Softcover, ISBN: 978-0-8218-4732-9, LC 2009045524, 2000 *Mathematics Subject Classification:* 14H15, 20H10, 28A75, 30F40, 30C62, 32G15, 54E40, 57M50, **AMS members US$79**, List US$99, Order code CONM/510

Differential Equations



MEMOIRS of the American Mathematical Society

Volume 204 Number 961

Non-Divergence Equations Structured on Hörmander Vector Fields: Heat Kernels and Harnack Inequalities

Marco Bramanti
Luca Brandolini
Ermanno Lanconelli
Francesco Uguzzoni

American Mathematical Society

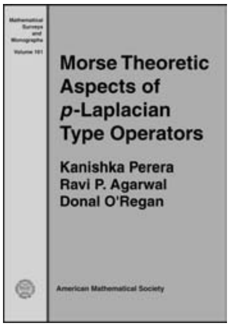
Non-Divergence Equations Structured on Hörmander Vector Fields: Heat Kernels and Harnack Inequalities

Marco Bramanti, *Politecnico di Milano, Italy*, **Luca Brandolini**, *Università di Bergamo, Bologna, Italy*, and **Ermanno Lanconelli** and **Francesco Uguzzoni**, *Università di Bologna, Italy*

Contents: Introduction; *Part I: Operators with constant coefficients:* Overview of Part I; Global extension of Hörmander's vector fields and geometric properties of the CC-distance; Global extension of the operator H_A and existence of a fundamental solution; Uniform Gevray estimates and upper bounds of fundamental solutions for large $d\,(x,y)$; Fractional integrals and uniform L^2 bounds of fundamental solutions for large $d\,(x,y)$; Uniform global upper bounds for fundamental solutions; Uniform lower bounds for fundamental solutions; Uniform upper bounds for the derivatives of the fundamental solutions; Uniform upper bounds on the difference of the fundamental solutions of two operators; *Part II: Fundamental solution for operators with Hölder continuous coefficients:* Assumptions, main results and overview of Part II; Fundamental solution for H: the Levi method; The Cauchy problem; Lower bounds for fundamental solutions; Regularity results; *Part III: Harnack inequality for operators with Hölder continuous coefficients:* Overview of Part III; Green function for operators with smooth coefficients on regular domains; Harnack inequality for operators with smooth coefficients; Harnack inequality in the non-smooth case; Epilogue; References.

Memoirs of the American Mathematical Society, Volume 204, Number 961

March 2010, 123 pages, Softcover, ISBN: 978-0-8218-4903-3, LC 2009050034, 2000 *Mathematics Subject Classification:* 35H20, 35A08, 35K65; 35H10, 35A17, **Individual member US$41**, List US$69, Institutional member US$55, Order code MEMO/204/961



Mathematical Surveys and Monographs

Volume 161

Morse Theoretic Aspects of p-Laplacian Type Operators

Kanishka Perera
Ravi P. Agarwal
Donal O'Regan

American Mathematical Society

Morse Theoretic Aspects of p-Laplacian Type Operators

Kanishka Perera and **Ravi P. Agarwal**, *Florida Institute of Technology, Melbourne, FL*, and **Donal O'Regan**, *National University of Ireland, Galway, Ireland*

The purpose of this book is to present a Morse theoretic study of a very general class of homogeneous operators that includes the p-Laplacian as a special case. The p-Laplacian operator is a quasilinear differential operator that arises in many applications such as non-Newtonian fluid flows and turbulent filtration in porous media. Infinite dimensional Morse theory has been used extensively to study semilinear problems, but only rarely to study the p-Laplacian.

The standard tools of Morse theory for computing critical groups, such as the Morse lemma, the shifting theorem, and various linking and local linking theorems based on eigenspaces, do not apply to quasilinear problems where the Euler functional is not defined on a Hilbert space or is not C^2 or where there are no eigenspaces to work with. Moreover, a complete description of the spectrum of a quasilinear operator is generally not available, and the standard sequence of eigenvalues based on the genus is not useful for obtaining nontrivial critical groups or for constructing linking sets and local linkings. However, one of the main points of this book is that the lack of a complete list of eigenvalues is not an insurmountable obstacle to applying critical point theory.

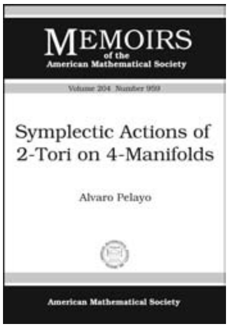
Working with a new sequence of eigenvalues that uses the cohomological index, the authors systematically develop alternative tools such as nonlinear linking and local splitting theories in order to effectively apply Morse theory to quasilinear problems. They obtain nontrivial critical groups in nonlinear eigenvalue problems and use the stability and piercing properties of the cohomological index to construct new linking sets and local splittings that are readily applicable here.

Contents: Morse theory and variational problems; Abstract formulation and examples; Background material; Critical point theory; p-Linear eigenvalue problems; Existence theory; Monotonicity and uniqueness; Nontrivial solutions and multiplicity; Jumping nonlinearities and the Dancer-Fučík spectrum; Indefinite eigenvalue problems; Anisotropic systems; Bibliography.

Mathematical Surveys and Monographs, Volume 161

April 2010, approximately 202 pages, Hardcover, ISBN: 978-0-8218-4968-2, 2000 *Mathematics Subject Classification:* 58E05, 47J05, 47J10, 35J60, **AMS members US$55**, List US$69, Order code SURV/161

Geometry and Topology



Symplectic Actions of 2-Tori on 4-Manifolds

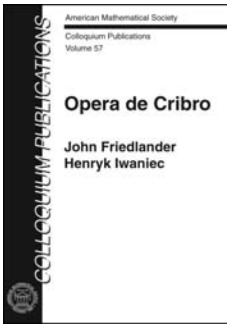
Alvaro Pelayo, *University of California at Berkeley, CA*

Contents: Introduction; The orbit space; Global model; Global model up to equivariant diffeomorphisms; Classification: Free case; Orbifold homology and geometric mappings; Classification; The four-dimensional classification; Appendix: (sometimes symplectic) orbifolds; Bibliography.

Memoirs of the American Mathematical Society, Volume 204, Number 959

March 2010, 81 pages, Softcover, ISBN: 978-0-8218-4713-8, LC 2009049943, 2000 *Mathematics Subject Classification:* 53D35; 57M60, 53C12, 55R10, **Individual member US$38**, List US$64, Institutional member US$51, Order code MEMO/204/959

Number Theory



Opera de Cribro

John Friedlander, *University of Toronto, ON, Canada*, and **Henryk Iwaniec**, *Rutgers University, Piscataway, NJ*

This monograph represents the state of the art both in respect of coverage of the general methods and in respect of the actual applications to interesting problems.

A unique feature of this monograph is how the authors take great pains to explain the fundamental ideas behind the proofs and to show how to approach a question in a correct fashion. So, this book is not just another monograph useful for consultation; rather, it is a teaching instrument of great value both for the specialist and the beginner in the field.

The authors must be congratulated for this exceptional monograph, the first of its kind for depth of content as well as for the effort made to explain the 'why' and not limiting themselves to the 'how to'. This is a true masterpiece that will prove to be indispensable to the serious researcher for many years to come.

—***Enrico Bombieri, Institute for Advanced Study***

This is a truly comprehensive account of sieves and their applications, by two of the world's greatest authorities. Beginners will find a thorough introduction to the subject, with plenty of helpful motivation. The more practised reader will appreciate the authors' insights into some of the more mysterious parts of the theory, as well as the wealth of new examples. No analytic number theorist should be without this volume, but it will not have a place on my bookshelves—it will be permanently on my desk!

—***Roger Heath-Brown, University of Oxford, Fellow of Royal Society***

This is a comprehensive and up-to-date treatment of sieve methods. The theory of the sieve is developed thoroughly with complete and accessible proofs of the basic theorems. Included is a wide range of applications, both to traditional questions such as those concerning primes, and to areas previously unexplored by sieve methods, such as elliptic curves, points on cubic surfaces and quantum ergodicity. New proofs are given also of some of the central theorems of analytic number theory; these proofs emphasize and take advantage of the applicability of sieve ideas.

The book contains numerous comments which provide the reader with insight into the workings of the subject, both as to what the sieve can do and what it cannot do. The authors reveal recent developments by which the parity barrier can be breached, exposing golden nuggets of the subject, previously inaccessible. The variety in the topics covered and in the levels of difficulty encountered makes this a work of value to novices and experts alike, both as an educational tool and a basic reference.

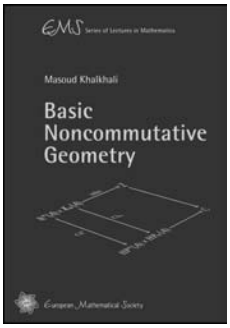
Contents: Sieve questions; Elementary considerations on arithmetic functions; Bombieri's sieve; Sieve of Eratosthenes-Legendre; Sieve principles and terminology; Brun's sieve—The big bang; Selberg's sieve—Kvadrater er positiv; Sieving by many residue classes; The large sieve; Molecular structure of sieve weights; The beta-sieve; The linear sieve; Applications to linear sequences; The semi-linear sieve; Applications—Choice but not prime; Asymptotic sieve and the parity principle; Combinatorial identities; Asymptotic sieve for primes; Equidistribution of quadratic roots; Capturing Gaussian primes; Primes represented by polynomials; Level of distribution of arithmetic sequences; Primes in short intervals; The least prime in an arithmetic progression; Almost-prime sieve; Mean-values of arithmetic functions; Differential-difference equations; Bibliography; Index.

Colloquium Publications, Volume 57

May 2010, approximately 529 pages, Hardcover, ISBN: 978-0-8218-4970-5, LC 2009046518, 2000 *Mathematics Subject Classification:* 11N35, 11N36; 11N05, 11N13, 11N32, 11N37, 11J71, 11E25, **AMS members US$82**, List US$103, Order code COLL/57

New AMS-Distributed Publications

Analysis



Basic Noncommutative Geometry

Masoud Khalkhali, *University of Western Ontario, London, Ontario, Canada*

This book provides an introduction to noncommutative geometry and some of its applications. It can be used either as a textbook for a graduate course on the subject or for self-study. It will be useful for graduate students and researchers in mathematics and theoretical physics and all those who are interested in gaining an understanding of the subject. One feature of this book is the wealth of examples and exercises that help the reader to navigate through the subject. While background material is provided in the text and in several appendices, some familiarity with basic notions of functional analysis, algebraic topology, differential geometry, and homological algebra at a first-year graduate level is helpful.

Developed by Alain Connes since the late 1970s, noncommutative geometry has found many applications to long-standing conjectures in topology and geometry and has recently made headways in theoretical physics and number theory. The book starts with a detailed description of some of the most pertinent algebra-geometry correspondences by casting geometric notions in algebraic terms, then proceeds to the idea of a noncommutative space and how it is constructed. The last two chapters deal with homological tools: cyclic cohomology and Connes–Chern characters in K-theory and K-homology, culminating in one commutative diagram expressing the equality of topological and analytic index in a noncommutative setting. Applications to integrality of noncommutative topological invariants are given as well.

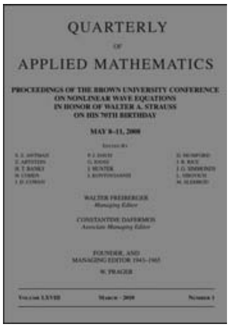
A publication of the European Mathematical Society (EMS). Distributed within the Americas by the American Mathematical Society.

Contents: Examples of algebra-geometry correspondences; Noncommutative quotients; Cyclic cohomology; Connes–Chern character; Appendices; Bibliography; Index.

EMS Series of Lectures in Mathematics, Volume 10

December 2009, 239 pages, Softcover, ISBN: 978-3-03719-061-6, 2000 *Mathematics Subject Classification:* 58-02, 58B34, **AMS members US$38**, List US$48, Order code EMSSERLEC/10

Differential Equations



Proceedings of the Brown University Conference on Nonlinear Wave Equations in Honor of Walter A. Strauss on his 70th Birthday, May 8–11, 2008

Walter Freiberger, *Brown University, Providence, RI*, Editor

This volume is a special issue of the *Quarterly of Applied Mathematics* journal. It represents the proceedings of the conference in honor of Walter Strauss's 70th birthday held at Brown University (Providence, RI) in May of 2008. The issue offers a collection of original and expository articles devoted to the study of nonlinear wave equations. The articles cover a wide range of topics, including scattering theory, dispersive waves, classical field theory, mathematical fluid mechanics, kinetic theory, and stability theory. The book offers a nice cross-section of current trends and research directions in the study of nonlinear wave equations.

Published by Brown University and distributed worldwide by the American Mathematical Society.

Contents: Y. Guo, Introduction to the Brown University Nonlinear Wave Equations Conference papers; **C. Morawetz**, Introduction. Dinner speech; **M. Grillakis**, The mathematics of W. A. Strauss and his contributions to analysis; **H. Andréasson**, **M. Kunze**, and **G. Rein**, Gravitational collapse and the formation of black holes for the spherically symmetric Einstein–Vlasov system; **C. Bardos** and **N. J. Mauser**, One particle equations for many particle quantum systems: The MCTHDF method; **N. Burq**, **P. Gérard**, and **N. Tzvetkov**, High frequency solutions of the nonlinear Schrödinger equation on surfaces; **G.-Q. Chen**, **M. Slemrod**, and **D. Wang**, A fluid dynamic formulation of the isometric embedding problem in differential geometry; **A. Constantin**, On the particle paths in solitary waves; **W. Craig** and **C. Sulem**, Asymptotics of surface waves over random bathymetry; **J. Ginibre** and **G. Velo**, Quadratic Morawetz inequalities and asymptotic completeness in the energy space for nonlinear Schrödinger and Hartree equations; **R. Glassey**, **J. Schaeffer**, and **S. Pankavich**, Time decay for solutions to one-dimensional two component plasma equations; **Y. Guo**, Bounded solutions for the Boltzmann equation; **Y. Guo** and **Y. Han**, Critical Rayleigh number in Rayleigh–Bénard convection; **J. Shatah**, Space-time resonances; **T. C. Sideris**, Energy splitting for solutions of multi-dimensional isotropic symmetric hyperbolic equations.

March 2010, 178 pages, Softcover, 2000 *Mathematics Subject Classification:* 35-06, 35Lxx, 35Qxx, List US$49, Order code QAMSP2

Discrete Mathematics and Combinatorics

Discrete Mathematics in Statistical Physics

Introductory Lectures

Martin Loebl, *Charles University, Prague, Czech Republic*

This book first describes connections between some basic problems and technics of combinatorics and statistical physics. The discrete mathematics and physics terminology are related to each other. Using the established connections, some exciting activities in one field are shown from a perspective of the other field. The purpose of the book is to emphasize these interactions as a strong and successful tool. In fact, this attitude has been a strong trend in both research communities recently.

It also naturally leads to many open problems, some of which seem to be basic. This book aims to help make these exciting problems attractive to advanced students and researchers.

This item will also be of interest to those working in mathematical physics.

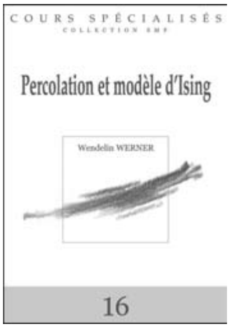
A publication of Vieweg Verlag. The AMS is exclusive distributor in North America. Vieweg Verlag Publications are available worldwide from the AMS outside of Germany, Switzerland, Austria, and Japan.

Contents: Basic concepts; Introduction to graph theory; Trees and electrical networks; Matroids; Geometric representations of graphs; Game of dualities; The zeta function and graph polynomials; Knots; 2D Ising and dimer models; Bibliography; List of figures; Index.

Vieweg Advanced Lectures in Mathematics

October 2009, 187 pages, Softcover, ISBN: 978-3-528-03219-7, 2000 *Mathematics Subject Classification:* 05-01, 82-01, 05A15, 05C30, 82B20, **AMS members US$48**, List US$53, Order code VWALM/11

Probability



Percolation et Modèle d’Ising

Wendelin Werner, *Université Paris Sud, Orsay, France*

These lecture notes provide a mathematical introduction to the study of random lattice-based models from statistical physics. Through the study of percolation and of the Ising model, the author introduces the notion of phase transitions and describes some classical techniques. One of the main goals of these notes is also to present recent results of Stanislav Smirnov concerning the conformal invariance of these models in two-dimensional space.

This item will also be of interest to those working in mathematical physics.

A publication of the Société Mathématique de France, Marseilles (SMF), distributed by the AMS in the U.S., Canada, and Mexico. Orders from other countries should be sent to the SMF. Members of the SMF receive a 30% discount from list.

Contents: Introduction; *Partie I. Percolation:* Unicité de la composante connexe infinie; Inégalités de corrélation; Décroissance exponentielle; *Partie II. Percolation critique sur le réseau triangulaire:* La théorie de Russo–Seymour–Welsh; La formule de Cardy–Smirnov; Quelques exercices sur la percolation; *Partie III. FK-percolation et modèle d’lsing:* FK-percolation sur des graphes finis; FK-percolation en volume infini; Bref retour sur Ising et Potts; *Partie IV. FX-percolation et modèle d’Ising sur le réseau carré:* FK-percolation sur le réseau carré; Invariance conforme du modèle d’Ising; Quelques exercices sur la FK-percolation; Commentaires bibliographiques; Bibliographie.

Cours Spécialisés—Collection SMF, Number 16

November 2009, 161 pages, Hardcover, ISBN: 978-2-85629-276-1, 2000 *Mathematics Subject Classification:* 60-01, 82-01, 82B05, 82B20, 82B26, 82B27, 82B43, **Individual member US$54**, List US$60, Order code COSP/16

Classified Advertisements

Positions available, items for sale, services available, and more

DELAWARE

COLLEGE OF MATHEMATICS, NATURAL SCIENCES, AND TECHNOLOGY
Department of Mathematical Sciences
Chairperson/Associate or Full Professor
Readvertisement

Delaware State University invites applications for position of chairperson of Department of Mathematical Sciences. The department offers baccalaureate and master's degrees in mathematics and mathematical sciences, and has an interdisciplinary Ph.D. program in applied mathematics. The department also supports the mathematics component of the university's general education program. The successful candidate must have a Ph.D. in mathematics, mathematics education, or a closely related field. The candidate must have experience in research, teaching, and service and have a successful record in grant writing and publication. The candidate should also have outstanding leadership, interpersonal, and communication skills. Application requires 1) application letter, 2) curriculum vitae, 3) research statement, 4) teaching philosophy, 5) administrative philosophy, 6) transcripts (official transcripts will be required prior to employment), 7) evidence of authorization to work in the United States, and 8) two letters of reference sent to: Maranda Thompkins, College of Mathematics, Natural Sciences, and Technology, Delaware State University, 1200 N. DuPont Highway, Dover, DE 19901. Applications will be considered until the position is filled. For first consideration, send completed application by March 19, 2010.

000023

KENTUCKY

WESTERN KENTUCKY UNIVERSITY
Department of Mathematics
Analysis Search

The Department of Mathematics and Computer Science at Western Kentucky University invites applications for a tenure-track position at the assistant professor level in the general area of analysis. This appointment is to begin August 15, 2010. While all qualified candidates are encouraged to apply, preference will be given to those working in the areas of harmonic analysis, potential theory, approximation theory, and special functions. Candidates are required to have a Ph.D. in mathematics or a closely related discipline by August 15, 2010. The salary will be commensurate with experience. In addition to the teaching load the successful candidate will be expected to have an active research program while participating and contributing to department and university service.

Western Kentucky University (WKU) is located in Bowling Green, KY and is a research institution with over 20,000 students. WKU is conveniently located just 50 miles from the metro Nashville, TN, area. WKU is committed to the promotion of stewardship and student engagement.

Applications must include the standard AMS cover sheet, a vita, transcripts of graduate work, a statement of teaching philosophy, a research statement, and at least three letters of recommendation with at least one addressing teaching. Only complete applications will receive full consideration. Please mail paper copies of the application to:

Dr. Tilak Bhattacharya,
Analysis Search Committee Chair,
Department of Mathematics,
Western Kentucky University,
1906 College Heights Blvd, #11078,
Bowling Green, KY 42101-1078

Review of applications will begin on March 1, 2010, and continue until the position is filled. Western Kentucky University is an EEO/AA Employer.

For this type of employment, state law requires a state and national criminal history background check as a condition of employment. For further information, please see our website: `http://www.wku.edu/mathcs`.

000021

AUSTRIA

DOCTORAL COLLEGE
'Discrete Mathematics' in Graz

The newly founded Doctoral College in Discrete Mathematics, which we understand in a very broad sense, offers a competitive research environment and English language Ph.D. program which is run jointly by TU Graz, Karl Franzens University Graz, and Montanuniversitaet Leoben. We offer ten Ph.D. positions for up to four years, starting from October

Suggested uses for classified advertising are positions available, books or lecture notes for sale, books being sought, exchange or rental of houses, and typing services.

The 2010 rate is $3.25 per word. No discounts for multiple ads or the same ad in consecutive issues. For an additional $10 charge, announcements can be placed anonymously. Correspondence will be forwarded.

Advertisements in the "Positions Available" classified section will be set with a minimum one-line headline, consisting of the institution name above body copy, unless additional headline copy is specified by the advertiser. Headlines will be centered in boldface at no extra charge. Ads will appear in the language in which they are submitted.

There are no member discounts for classified ads. Dictation over the telephone will not be accepted for classified ads.

Upcoming deadlines for classified advertising are as follows: April 2010 issue–January 28, 2010; May 2010 issue–February 26, 2010; June/July 2010 issue–April 28, 2010; August 2010 issue–May 28, 2010; September 2010–June 28, 2010; October 2010 issue–July 29, 2010.

U.S. laws prohibit discrimination in employment on the basis of color, age, sex, race, religion, or national origin. "Positions Available" advertisements from institutions outside the U.S. cannot be published unless they are accompanied by a statement that the institution does not discriminate on these grounds whether or not it is subject to U.S. laws. Details and specific wording may be found on page 536 (vol. 56).

Situations wanted advertisements from involuntarily unemployed mathematicians are accepted under certain conditions for free publication. Call toll-free 800-321-4AMS (321-4267) in the U.S. and Canada or 401-455-4084 worldwide for further information.

Submission: Promotions Department, AMS, P.O. Box 6248, Providence, Rhode Island 02940; or via fax: 401-331-3842; or send email to `classads@ams.org`. AMS location for express delivery packages is 201 Charles Street, Providence, Rhode Island 20904. Advertisers will be billed upon publication.

2010. Applications are accepted until all positions are filled, but priority is given to those received until April 19, 2010. Please visit: `http://www.math.tugraz.at/discrete/` for details. Prior enquiries are welcome: `discrete@tugraz.at`.

000022

CHILE

PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
Departamento de Matemáticas

The Department of Mathematics invites applications for two tenure-track positions at the assistant professor level beginning either March or August 2011. Applicants should have a Ph.D. in mathematics, proven research potential either in pure or applied mathematics, and a strong commitment to teaching and research. The regular teaching load for assistant professors consists of three one-semester courses per year, reduced to two during the first two years. The annual salary will be US$38,000. Please send a letter indicating your main research interests, potential collaborators in our department (`http://www.mat.puc.cl`), detailed curriculum vitae, and three letters of recommendation to:

Director
Departamento de Matemáticas,
Pontificia Universidad Católica de Chile,
Av. Vicuña Mackenna 4860,
Santiago, Chile;
fax: (56-2) 552-5916;
email: `mchuaqui@mat.puc.cl`

For full consideration, complete application materials must arrive by June 30, 2010.

000020

KUWAIT

KUWAIT UNIVERSITY
Facutly of Science
Kuwait

The Department of Mathematics and Computer Science at the Faculty of Science, Kuwait University invites applications for the academic year 2010/2011, in the following specialized areas: algebra, analysis, dynamical systems, computational mathematics, optimization, financial mathematics and applied mathematics.

Required Qualifications:

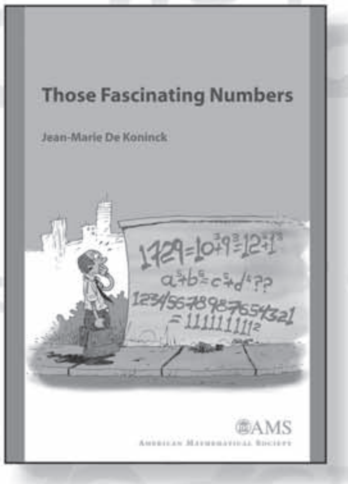
Applicants should have bachelor's, master's and doctorate degrees in mathematics from a reputable university. The applicant's GPA in the first university degree should be 3 out of 4 or its equivalent. Research experience and publications in refereed international journals are also required. A full command of English as well as a minimum of 2 years experience in university teaching in the specified field. The successful candidates are expected to have a strong commitment and dedication to quality teaching and research. For further information refer to the website: `http://www.science.kuniv.edu.kw/`.

To apply send by express mail/courier service or email, within six weeks of the date of announcement, a copy of this ad, a completed application form, with required documents as stated in the application form as well as detailed CV, a copy of the passport and three recommendation letters, to the following address:

Administration for Academic Staff Affairs
Academic Staff Appointment Department
Kuwait University, Khaldiya Campus
Block 3, Al Firdous Street, Building No: 3
Khaldiya, State of Kuwait;
tel: 00965-24844189; fax: 00965-24849562;
email: `Vpaa.faculty@ku.edu.kw`

For application forms refer to website: `http://www.kuniv.edu/ku/Downloads/index.htm`.

000024



Moving?

Please make sure that the AMS Notices and Bulletin find their new home.

Notices
of the American Mathematical Society
BULLETIN
of the
AMERICAN MATHEMATICAL SOCIETY

- Email your new address to us: amsmem@ams.org
- or make the change yourself online at: www.ams.org/cml-update
- or send the information to:

Member and Customer Services
American Mathematical Society
201 Charles Street
Providence, RI 02904-2294 USA
Phone: (800) 321-4267 (US & Canada)
(401) 455-4000 (Worldwide)

AMS
American Mathematical Society
www.ams.org

Meetings & Conferences of the AMS

IMPORTANT INFORMATION REGARDING MEETINGS PROGRAMS: AMS Sectional Meeting programs do not appear in the print version of the *Notices*. However, comprehensive and continually updated meeting and program information with links to the abstract for each talk can be found on the AMS website. See `http://www.ams.org/meetings/`. Final programs for Sectional Meetings will be archived on the AMS website accessible from the stated URL and in an electronic issue of the *Notices* as noted below for each meeting.

Lexington, Kentucky

University of Kentucky

March 27–28, 2010

Saturday – Sunday

Meeting #1057

Southeastern Section
Associate secretary: Matthew Miller
Announcement issue of *Notices*: January 2010
Program first available on AMS website: February 11, 2010
Program issue of electronic *Notices*: March 2010
Issue of *Abstracts*: Volume 31, Issue 2

Deadlines

For organizers: Expired
For consideration of contributed papers in Special Sessions: Expired
For abstracts: Expired

The scientific information listed below may be dated. For the latest information, see `www.ams.org/amsmtgs/sectional.html`.

Invited Addresses

Percy A. Deift, Courant Institute–New York University, *Open problems in integrable systems and random matrix theory*.

Irina Mitrea, Worcester Polytechnic Institute, *Recent progress in the area of elliptic boundary value problems on rough domains*.

Bruce Reznick, University of Illinois at Urbana Champaign, *The secret lives of polynomial identities*.

Bernd Ulrich, Purdue University, *Title to be announced*.

Doron Zeilberger, Rutgers University, *3x+1* (Erdős Memorial Lecture).

Special Sessions

Advances in Algebraic Coding Theory, **Heide Gluesing-Luerssen**, University of Kentucky, and **Jon-Lark Kim**, University of Louisville.

Advances in Algebraic Statistics, **Sonja Petrović**, University of Illinois, Chicago, and **Ruriko Yoshida**, University of Kentucky.

Advances in Algebraic and Geometric Combinatorics, **Richard Ehrenborg** and **Margaret A. Readdy**, University of Kentucky.

Analysis and Control of Dispersive Partial Differential Equations, **Michael J. Goldberg** and **Bingyu Zhang**, University of Cincinnati.

Combinatorial Algebra, **Juan C. Migliore**, University of Notre Dame, and **Uwe Nagel**, University of Kentucky.

Commutative Algebra, **Alberto Corso**, University of Kentucky, **Claudia Polini**, University of Notre Dame, and **Bernd Ulrich**, Purdue University.

Complex Analysis and Potential Theory, **James E. Brennan** and **Vladimir Eiderman**, University of Kentucky.

Financial Mathematics and Statistics, **Kiseop Lee**, University of Louisville, and **Jose Figueroa-Lopez**, Department of Statistics, Purdue University.

Function Theory, Harmonic Analysis, and Partial Differential Equations, **Joel Kilty**, Centre College, **Irina Mitrea**, Worcester Polytechnic Institute, and **Katharine Ott**, University of Kentucky.

Geometric Function Theory and Analysis on Metric Spaces, **John L. Lewis**, University of Kentucky, and **Nageswari Shanmugalingam**, University of Cincinnati.

Homotopy Theory and Geometric Aspects of Algebraic Topology, **Serge Ochanine**, University of Kentucky, and **Marian F. Anton**, Centre College.

Interactions between Logic, Topology, and Complex Analysis, **Matt Insall**, Missouri University of Science and Technology, and **Malgorzata Marciniak**, University of Toledo.

Inverse Problems, Riemann-Hilbert Problems, and Nonlinear Dispersive Equations, **Peter A. Perry**, University of Kentucky, and **Peter Topalov**, Northeastern University.

Large Scale Matrix Computation, **Qiang Ye**, University of Kentucky, and **Lothar Reichel**, Kent State University.

Mathematical Economics, **Adib Bagh** and **Robert E. Molzon**, University of Kentucky.

Mathematical Problems in Mechanics and Materials Science, **Michel E. Jabbour** and **Chi-Sing Man**, University of Kentucky, and **Kazumi Tanuma**, Gunma University.

Mathematical String Theory, **Al Shapere**, Department of Physics and Astronomy, University of Kentucky, **Eric Sharpe**, Physics Department, Virginia Polytechnic Institute and State University, and **Mark A. Stern**, Duke University.

Mathematics Outreach, **Carl W. Lee** and **David C. Royster**, University of Kentucky.

Matroid Theory, **Jakayla Robbins**, University of Kentucky, and **Xiangqian Zhou**, Wright State University.

Multivariate and Banach Space Polynomials, **Richard A. Aron**, Kent State University, and **Lawrence A. Harris**, University of Kentucky.

Noncommutative Algebraic Geometry, **Dennis S. Keeler** and **Kimberly Retert**, Miami University.

Partial Differential Equations in Geometry and Variational Problems, **Luca Capogna**, University of Arkansas, and **Changyou Wang**, University of Kentucky.

Recent Progress in Numerical Methods for Partial Differential Equations, **Alan Demlow**, University of Kentucky, and **Xiaobing H. Feng**, University of Tennessee at Knoxville.

Relative Homological Algebra, **Edgar E. Enochs**, University of Kentucky, and **Alina C. Iacob**, Georgia Southern University.

Sharp Spectral Estimates in Analysis, Geometry, and Probability, **Richard S. Laugesen** and **Bartlomiej Siudeja**, University of Illinois.

Spectral and Transport Properties of Schrödinger Operators, **Peter D. Hislop**, University of Kentucky, and **Jeffrey H. Schenker**, Michigan State University.

St. Paul, Minnesota

Macalester College

April 10–11, 2010

Saturday – Sunday

Meeting #1058

Central Section
Associate secretary: Georgia Benkart
Announcement issue of *Notices*: February 2010
Program first available on AMS website: February 25, 2010
Program issue of electronic *Notices*: April 2010
Issue of *Abstracts*: Volume 31, Issue 2

Deadlines

For organizers: Expired
For consideration of contributed papers in Special Sessions: Expired
For abstracts: February 16, 2010

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/sectional.html.

Invited Addresses

Charles Doering, University of Michigan, *Title to be announced.*

Matthew James Emerton, Northwestern University, *Title to be announced.*

Vladimir Touraev, Indiana University, *Title to be announced.*

Peter Webb, University of Minnesota, *Title to be announced.*

Special Sessions

Applications of a Geometric Approach to Chaotic Dynamics (Code: SS 16A), **Evelyn Sander**, George Mason University, **Judy Kennedy**, Lamar University, and **James Yorke**, University of Maryland.

Cohomology and Representation Theory of Algebraic Groups and Related Structures (Code: SS 7A), **Christopher Bendel**, University of Wisconsin-Stout, **Bobbe Cooper**, University of Minnesota, and **Terrell Hodge**, Western Michigan University.

Combinatorial Representation Theory (Code: SS 3A), **Tom Halverson**, Macalester College, and **Victor Reiner**, University of Minnesota.

Commutative Ring Theory (Code: SS 5A), **Michael Axtell**, University of St. Thomas, and **Joe Stickles**, Millikin University.

Differential Equations and Applications (Code: SS 15A), **Nicolai Tarfulea**, Purdue University Calumet, and **Catalin Turc**, Case Western Reserve University.

Fractals, Convolution Measures, and Frames (Code: SS 13A), **Keri Kornelson**, University of Oklahoma, and **Karen Shuman**, Grinnell College.

Geometric Flows, Moving Frames and Integrable Systems (Code: SS 8A), **Gloria Mari-Beffa**, University of Wisconsin-Madison, and **Peter Olver**, University of Minnesota.

Hecke Algebras and Deformations in Geometry and Topology (Code: SS 11A), **Matthew Douglass** and **Anne Shepler**, University of North Texas.

Mathematical Developments in Cell and Systems Biology (Code: SS 14A), **Anastasios Matzavinos**, Iowa State University, and **Nicoleta Eugenia Tarfulea**, Purdue University Calumet.

Matrices and Graphs (Code: SS 9A), **Luz M. DeAlba**, Drake University, **Adam Berliner**, St. Olaf College, **Leslie Hogben**, Iowa State University, and **In-Jae Kim**, Minnesota State University.

Partition Theory and the Combinatorics of Symmetric Functions (Code: SS 6A), **Eric S. Egge**, Carleton College, and **Kristina Garrett**, St. Olaf College.

Pattern Formation in Biological Systems (Code: SS 12A), **Magdalena Skolarska**, University of St. Thomas, and **Chad Topaz**, Macalester College.

Physical Knotting and Linking and its Applications (Code: SS 10A), **Eric Rawden**, University of St. Thomas,

Yuanan Diao, University of North Carolina at Charlotte, and **Claus Ernst**, Western Kentucky University.

Probabilistic and Extremal Combinatorics (Code: SS 2A), **Ryan Martin** and **Maria Axenovich**, Iowa State University.

Quantum Invariants of 3-manifolds and Modular Categories (Code: SS 1A), **Thang Le**, Georgia Institute of Technology, **Eric Rowell**, Texas A&M University, and **Vladimir Touraev**, Indiana University.

Universal Algebra and Order (Code: SS 4A), **Jeffrey Olson**, Norwich University, **Jeremy Alm**, Illinois College, **Kristi Meyer**, Wisconsin Lutheran College, and **Japheth Wood**, Bard College.

Albuquerque, New Mexico

University of New Mexico

April 17–18, 2010

Saturday – Sunday

Meeting #1059

Western Section
Associate secretary: Michel L. Lapidus
Announcement issue of *Notices*: February 2010
Program first available on AMS website: March 4, 2010
Program issue of electronic *Notices*: April 2010
Issue of *Abstracts*: Volume 31, Issue 3

Deadlines

For organizers: Expired

For consideration of contributed papers in Special Sessions: Expired

For abstracts: February 23, 2010

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/sectional.html.

Invited Addresses

Kenneth Bromberg, University of Utah, *Title to be announced.*

Danny Calegari, California Institute of Technology, *Title to be announced.*

Ioana Dumitriu, University of Washington, *Title to be announced.*

Steffen Rohde, University of Washington, *Title to be announced.*

Special Sessions

Dyadic and Non-Dyadic Harmonic Analysis (Code: SS 2A), **M. Cristina Pereyra**, University of New Mexico, and S**tephanie A. Salomone**, University of Portland.

Financial Mathematics: The Mathematics of Financial Markets and Structures (Code: SS 4A), **Maria Cristina Mariani**, University of Texas at El Paso, **Ionut Florescu**, Stevens Institute of Technology, and **Maria P. Beccar-Varela**, University of Texas at El Paso.

Function Spaces, PDEs and Nonlinear Analysis (Code: SS 10A), **Osvaldo Mendez**, **Behzad Rouhani**, and **Mohamed Amine Khamsi**, University of Texas at El Paso.

Geometric Combinatorics (Code: SS 6A), **Art M. Duval**, University of Texas at El Paso, and **Jeremy Martin**, University of Kansas.

Geometric Function Theory (Code: SS 14A), **Lukas Geyer**, Montana State University, and **Donald Marshall** and **Steffen Rohde**, University of Washington.

Geometric Structures and PDEs (Code: SS 8A), **Charles Boyer** and **Dimiter Vassilev**, University of New Mexico.

Harmonic Analysis and Partial Differential Equations (Code: SS 5A), **Matthew Blair**, University of New Mexico, and **Hart Smith**, University of Washington.

Kleinian Groups and Teichmüller Theory (Code: SS 15A), **Kasra Rafi**, University of Oklahoma, **Hossein Namaze**, University of Texas, and **Kenneth Bromberg**, University of Utah.

Positivity in Noncommutative Settings (Code: SS 12A), **Roger Roybal**, California State University Channel Islands, and **Terry Loring**, University of New Mexico.

Random Matrix Theory and Applications (Code: SS 13A), **Ioana Dumitriu**, University of Washington, and **Raj Rao**, University of Michigan.

Selected Topics in Analysis and Numerics for PDEs (Code: SS 11A), **Thomas Hagstrom**, Southern Methodist University, and **Stephen Lau** and **Jens Lorenz**, University of New Mexico.

Strongly-nonlinear Phenomena: Theory and Applications to Nonlinear Optics, Hydrodynamics, Bose–Einstein Condensation and Biology (Code: SS 9A), **Alejandro Aceves**, Southern Methodist University, and **Alexander Korotkevich** and **Pavel Lushnikov**, University of New Mexico.

Subjects in between Pure and Applied Mathematics (Code: SS 7A), **Hanna Makaruk** and **Robert Owczarek**, Los Alamos National Laboratory.

Topics in Geometric Group Theory (Code: SS 1A), **Matthew Day**, California Institute of Technology, **Daniel Peter Groves**, University of Illinois at Chicago, **Jason Manning**, SUNY at Buffalo, and **Henry Wilton**, California Institute of Technology.

Trends in Commutative Algebra (Code: SS 3A), **Louiza Fouli**, New Mexico State University, and **Janet Vassilev**, University New Mexico.

Newark, New Jersey

New Jersey Institute of Technology

May 22–23, 2010

Saturday – Sunday

Meeting #1060

Eastern Section
Associate secretary: Steven H. Weintraub
Announcement issue of *Notices*: March 2010
Program first available on AMS website: April 8, 2010

Program issue of electronic *Notices*: May 2020
Issue of *Abstracts*: Volume 31, Issue 3

Deadlines

For organizers: Expired
For consideration of contributed papers in Special Sessions: Expired
For abstracts: March 30, 2010

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/sectional.html.

Invited Addresses

Simon Brendle, Stanford University, *Hamilton's Ricci flow and the sphere theorem in geometry*.

Konstantin M. Mischaikow, Rutgers University, *Computational topology applied to the global dynamics of nonlinear systems*.

Ricardo H. Nochetto, University of Maryland, *Curvature driven flows in deformable domains*.

Richard E. Schwartz, Brown University, *Polygonal outer billiards*.

Special Sessions

Automorphic Forms, L-functions, and Applications (Code: SS 6A), **Ameya Pitale**, American Institute of Mathematics, and **Anantharam Raghuram**, Oklahoma State University.

Biomembranes: Modeling, Analysis, and Computation (Code: SS 16A), **Ricardo H. Nochetto** and **Dionisios Margetis**, University of Maryland.

Elliptic and Parabolic Problems in Geometry (Code: SS 12A), **Simon Brendle**, Stanford University, and **Mu-Tao Wang**, Columbia University.

Expandable Computations, Algorithms, Methodologies and Experiments for Engineering Interpretation (Code: SS 1A), **Mustapha S. Fofana**, Worcester Polytechnic Institute, **Marie D. Dahleh**, Harvard School of Engineering and Applied Sciences, Harvard University, and **Kenji Kawashima**, Precision and Intelligence Laboratory, Tokyo Institute of Technology.

Financial Mathematics (Code: SS 9A), **Tim S.T. Leung**, Johns Hopkins University.

Graph Theory (Code: SS 10A), **Nathan W. Kahl**, Seton Hall University, **Michael J. Ferrara**, University of Colorado at Denver, and **Arthur H. Busch**, University of Dayton.

Groups, Computations, and Applications (Code: SS 2A), **Delaram Kahrobaei**, City University of New York.

Homology Theories for Knots and Skein Modules (Code: SS 3A), **Mikhail Khovanov**, Columbia University, and **Jozef H. Przytycki** and **Radmila Sazdanovic**, George Washington University.

Invariants of Knots, Links, and 3-Manifolds (Code: SS 4A), **Abhijit Champanerkar** and **Ilya S. Kofman**, College of Staten Island, CUNY, and **Philip J. P. Ording**, Medgar Evers College, CUNY.

Lie Algebras and Representation Theory (Code: SS 8A), **Gautam Chinta**, City College, City University of New York, **Andrew Douglas**, New York City College of Technology, City University of New York, and **Bart Van Steirteghem**, Medgar Evers College, City University of New York.

Logic and Groups (Code: SS 17A), **Peggy Dean**, **Claire Wladis**, and **Marcos Zyman**, Borough of Manhattan Community College, City University of New York.

Mathematical Neuroscience: Modeling, Analysis, and Simulations (Code: SS 14A), **Horacio G. Rotstein**, New Jersey Institute of Technology.

Mathematics and Computations of Fluid Dynamics (Code: SS 15A), **Yuan N. Young**, New Jersey Institute of Technology.

Mathematics of Optics and Matter Waves (Code: SS 13A), **Roy Goodman**, New Jersey Institute of Technology.

Nonlinear Waves (Code: SS 19A), **A. David Trubatch**, Montclair State University.

Recent Trends in Cayley Graphs to Model Interconnection Networks (Code: SS 18A), **Daniela Ferrero**, Texas State University, and **Beth Novick**, Clemson University.

Teichmüller Theory, Hyperbolic Geometry, and Complex Dynamics (Code: SS 5A), **Zheng Huang**, College of Staten Island, CUNY, and **Ren Guo**, University of Minnesota.

Topological and Computational Dynamics (Code: SS 7A), **Jean-Philippe Lessard**, Institute for Advanced Study and Rutgers University, and **Konstantin M. Mischaikow**, Rutgers University.

Vortex Dynamics: Theory and Applications (Code: SS 11A), **Denis Blackmore**, New Jersey Institute of Technology, **Morten Brøns**, Technical University of Denmark, and **Chjan Lim**, Rochester Polytechnic Institute.

Accommodations

Participants should make their own arrangements directly with the hotel. When making a reservation identify yourself as attending the AMS Meeting at the New Jersey Institute of Technology. The AMS is not responsible for rate changes or for the quality of the accommodations. **Hotels have varying cancellation or early checkout penalties; be sure to ask for details when making your reservation.**

Hampton Inn, 100 Passaic Avenue, Harrison, NJ 07102, phone 973-483-1900. Rates start at US$129 per night, plus occupancy tax for single/double rooms. Refer to the group code: AMS. **Deadline for reservations is April 21, 2010.** Be sure to check the cancellation policy. Amenities include: Shuttle to/ from airport and NJIT from 7:00 a.m. to 11:00 p.m., complimentary continental breakfast, complimentary high speed wireless Internet access in public areas and guest rooms, fitness center, and restaurant. The hotel is approximately one mile to campus. For more information please visit http://www.hamptoninnandsuitesnewark.com/.

Hilton Newark Gateway, 1 Gateway Center, Newark, NJ 07102, phone: 973-622-5000. Rates start at US$139 per night, plus occupancy tax single/double rooms. **Deadline for reservations is April 21, 2010**. Be sure to check the cancellation policy. There is a complimentary shuttle to and from the airport. At the airport, follow signs to the Monorail station P4 and look for the Hilton Newark Gateway shuttle. Overnight parking is US$21 per day. Wireless Internet is US$5.95 per day. The hotel is approximately 1.5 miles to campus. For more information please visit http://www1.hilton.com/en_US/hi/hotel/EWRHGHF-Hilton-Newark-Penn-Station-New-Jersey/services.do.

Daily Dormitory Rates at New Jersey Institute of Technology:

All rooms share a bathroom. All rooms are lockable, include desks and have beds with linens (that will need to be made by the guest). Linens and towels are provided once at the beginning of the stay.

Private Room (Single) US$54

Shared Room (Double) US$43

Linen will be an additional US$10 per person for any stay less than one week.

For reservations contact: Sandy Worley, Assistant Director of Residence Life, 180 Bleeker Street, Newark, NJ 07103; Phone: 973-596-3039; Fax: 973-596-8197; email: reslife@njit.edu; Web: http://www.njit.edu/reslife.

Special Information

The AMS sectional meeting will be held in conjunction with the 2010 Frontiers in Applied and Computational Mathematics (FACM) meeting. The FACM meetings are held annually at NJIT, with the 2010 meeting to run May 21–23, 2010, with a focus on mathematical fluid dynamics. For further information see the FACM website: http://m.njit.edu/Events/FACM10/.

Food Service

Food and beverages within easy walking distance during the meeting can be found in the following places: NJIT Campus Center, Rutgers-Newark Campus Center—right across the street (MLK Blvd.) from NJIT; Essex County College Campus Center—two blocks west along MLK Blvd. of NJIT; Two Subway restaurants within two blocks of campus on Central Ave.; Kilkenny Alehouse, 27 Central Ave.; McGovern's Tavern, 58 New St. Please see Campus Map for exact locations. Also, a list of these and other local restaurants will be available at the registration desk.

Local Information and Campus Map

To view a campus map please visit: http://www.njit.edu/about/visit/njit-buildings.php. Also, the link to the NJIT neighborhood (University Heights) map is: http://www.njit.edu/about/visit/universityheights.php.

Other Activities

AMS Book Sale: Stop by the on-site AMS Bookstore—review the newest titles from the AMS, enter the FREE book drawing, enjoy up to 25% off all titles or even take home the new AMS T-shirt! Complimentary coffee will be served courtesy of AMS Membership Services.

AMS Editorial Activity: An acquisitions editor from the AMS Book program will be present to speak with prospective authors. If you have a book project that you would like to discuss with the AMS, please stop by the book exhibit.

Parking

Parking for all AMS meeting attendees is to be provided in the Parking Deck (#19 on the campus map).

Registration and Meeting Information

Registration will take place in the Lobby area on the first floor of Kupfrian Hall, from 7:30 a.m. to 4:00 p.m. on Saturday, May 22, and 8:00 a.m. to noon on Sunday, May 23. Special Sessions will take place in Kupfrian Hall and Cullimore Hall.

Registration fees: (payable on-site only) US$40/AMS members; US$60/nonmembers; US$5/emeritus members, students, or unemployed mathematicians. Fees are payable by cash, check, VISA, Mastercard, Discover, or American Express.

Travel

Driving Directions—(Note: for destination information for NJIT please use the following address: 154 Summit Street, Newark, NJ 07102.)

Garden State Parkway (GSP): Take exit 145 to Route 280 East, then follow Route 280 East directions.

New Jersey Turnpike: Take exit 15W to Route 280 West, then follow Route 280 West directions.

Route 280 West: After drawbridge, take Exit 14B (Broad Street/MLK Blvd.). At bottom of exit ramp, make a left. Go one block to stop sign. Make a left on MLK Blvd. Go five lights to Warren Street. Make a right on Warren Street. Go two blocks to Colden Street. Make a left on Colden Street. Follow signs to NJIT Parking Deck.

Route 280 East: Take Exit 13 (First Street/Newark). At light, make a right on First Street. Go three lights to W. Market Street. Make the soft left on W. Market Street. Go four lights to MLK Blvd. Make a left on MLK Blvd. Go one light to Warren Street. Make a left on Warren Street. Go two blocks to Colden Street. Make a left on Colden Street. Follow signs to NJIT Parking Deck.

Route 1 & 9 North & South: Take exit marked Newark, Route 21 (McCarter Highway). Get in the right lane on the bridge and take the Broad Street exit. Go about 1 mile. Make a left on Court Street. Make a right at third light on MLK Blvd. Make a left at fifth light on Warren Street. Go two blocks to Colden Street. Make a left on Colden Street. Follow signs to NJIT Parking Deck.

Route 78: Take Route 78 to the Garden State Parkway. Follow GSP directions.

Route 22: Take Route 22 to Route 21 North. Follow directions for Route 21 North.

Route 21 North: Get in the right lane on the bridge and take the Broad Street exit. Go about 1 mile. Make a left on Court Street. Make a right at third light on MLK Blvd. Make a left at fifth light on Warren Street. Go two blocks to Colden Street. Make a left on Colden Street. Follow signs to the NJIT Parking Deck.

Route 21 South: From 21 South, turn right on Bridge Street shortly after passing beneath Route 280 overpass. Turn left on Broad Street. Go one block and turn right on Washington Place. Go one block and turn left on Halsey Street. Go one block and turn right on Central Avenue.

Make the third left on MLK Blvd. At first light, turn right on Warren Street. Go two blocks to Colden Street. Make a left on Colden Street. Follow signs to NJIT Parking Deck.

New York Thruway: Thruway to Exit 14A, Garden State Parkway. Follow GSP directions above.

George Washington Bridge: NJ Turnpike South to Exit 15W. Follow Route 280 West directions above.

Lincoln Tunnel: West on Route 3 to NJ Turnpike South to Exit 15W. Follow Route 280 West directions above.

From Brooklyn, Queens and Long Island: Take Verrazano-Narrows Bridge (Interstate 278) and follow 278 across Staten Island. Cross Goethels Bridge. Follow signs to New Jersey Turnpike North then follow New Jersey Turnpike directions above.

Public Transportation: In addition to the information below please visit `http://www.njtransit.com/var/var_servlet.srv?hdnPageAction=NLRTo/Newark_Broad_St_Station.html`.

Newark Liberty International Airport

Five miles from NJIT campus. A minibus (Newark Airlink) or taxi service connects the airport with Penn Station in Newark. Bus, city subway, and taxi connections may be obtained at the station. (Note: Train service is available directly from Newark Liberty International Airport to Newark Penn Station.)

Newark Penn Station

Connections to the NJIT campus may be made by bus, city subway, or taxi.

Morris & Essex Line Broad Street Station

A five-block walk to the NJIT campus via MLK Blvd. or University Ave. to Central Avenue. Taxi service is also available for a minimal price. NJ Transit Light Rail is also available. (Note: the Light Rail route requires a switch at Newark's Penn Station; this mode of transport will take you some time).

Car Rental

Avis is the official car rental company for the sectional meeting in New Jersey. All rates include unlimited free mileage. Weekend daily rates are available from noon Thursday to Monday at 11:59 p.m. Rates do not include any state or local surcharges, tax, optional overages, or gas refueling charges. Renters must meet Avis's age, driver, and credit requirements. For the best available rate and to make a reservation please call Avis at 800-331-1600 or go online at `http://www.avis.com`. Please use the AMS meeting **Avis Discount Number J098887**.

Weather

May weather is generally pleasant with average high temperatures of 72 degrees and average low temperatures of 49 degrees. The median temperature is 60 degrees. Average precipitation is 4.42 inches. For-up-to-the-minute weather please visit `http://www.weather.com/outlook/driving/local/USNM0004`.

Information for International Participants

Visa regulations are continually changing for travel to the United States. Visa applications may take from three to four months to process and require a personal interview, as well as specific personal information. International participants should view the important information about traveling to the U.S. found at `http://www7.nationalacademies.org/visas/Traveling_to_US.html` and `http://travel.state.gov/visa/index.html`. If you need a preliminary conference invitation in order to secure a visa, please send your request to `dls@ams.org`.

If you discover you do need a visa, the National Academies website (see above) provides these tips for successful visa applications:

* Visa applicants are expected to provide evidence that they are intending to return to their country of residence. Therefore, applicants should provide proof of "binding" or sufficient ties to their home country or permanent residence abroad. This may include documentation of the following:

– family ties in home country or country of legal permanent residence

– property ownership

– bank accounts

– employment contract or statement from employer stating that the position will continue when the employee returns;

* Visa applications are more likely to be successful if done in a visitor's home country than in a third country;

* Applicants should present their entire trip itinerary, including travel to any countries other than the United States, at the time of their visa application;

* Include a letter of invitation from the meeting organizer or the U.S. host, specifying the subject, location and dates of the activity, and how travel and local expenses will be covered;

* If travel plans will depend on early approval of the visa application, specify this at the time of the application;

* Provide proof of professional scientific and/or educational status (students should provide a university transcript).

This list is not to be considered complete. Please visit the websites above for the most up-to-date information.

Berkeley, California

University of California Berkeley

June 2–5, 2010

Wednesday – Saturday

Meeting #1061

Eighth Joint International Meeting of the AMS and the Sociedad Matemática Mexicana.
Associate secretary: Susan J. Friedlander
Announcement issue of *Notices*: April 2010
Program first available on AMS website: April 22, 2010

Program issue of electronic *Notices*: June 2010
Issue of *Abstracts*: Volume 31, Issue 3

Deadlines

For organizers: Expired
For consideration of contributed papers in Special Sessions: February 16, 2010
For abstracts: April 13, 2010

The scientific information listed below may be dated. For the latest information, see `www.ams.org/amsmtgs/internmtgs.html`.

Invited Addresses

Alejandro Adem, University of British Columbia and PIMS, *Homotopy theory and spaces of representations.*

Peter W-K Li, University of California Irvine, *What do we know about open manifolds?*

Ernesto Lupercio, CINVESTAV, *Title to be announced.*

Victor Perez Abreu, CIMAT, *On convolutions and infinite divisibility of probability measures.*

Alberto Verjovsky, IM-UNAM, *Title to be announced.*

Maciej Zworski, University of California Berkeley, *Random perturbations in discrete quantization.*

Special Sessions

Algebraic Topology and Related Topics (Code: SS 3A), **Alejandro Adem**, University of British Columbia, **Gunnar E. Carlsson** and **Ralph L. Cohen**, Stanford University, and **Ernesto Lupercio**, CINVESTAV.

Analytic Aspects of Differential Geometry (Code: SS 2A), **Nelia Charalambous**, ITAM, **Lizhen Ji**, University of Michigan, and **Jiaping Wang**, University of Minnesota.

Commutative Algebra and Representation Theory (Code: SS 7A), **David Eisenbud** and **Daniel M. Erman**, University of California, Berkeley, **Jose Antonio de la Pena**, UNAM, and **Rafael Villareal**, Cinvestav-IPN.

Complex Analysis and Operator Theory (Code: SS 10A), **Maribel Loaiza**, **Enrique Ramirez de Arellano**, and **Nikolai Vasilevski**, CINVESTAV, **Ilya M. Spitkovsky**, College of William & Mary, and **Kehe Zhu**, State University of New York at Albany.

Dynamical Systems (Code: SS 4A), **Alberto Verjovsky**, IM-UNAM, and **Rodrigo Perez**, Indiana University-Purdue University, Indianapolis.

Graph Theory and Combinatorics with Emphasis on Geometric and Topological Aspects (Code: SS 9A), **Gelasio Salazar**, Instituto de Fisica, Universidad Autonoma de San Luis Potosi, and **Dan S. Archdeacon**, University of Vermont.

Harmonic Analysis, Microlocal Analysis, and Partial Differential Equations (Code: SS 1A), **Gunther Uhlmann**, University of Washington, and **Salvador Perez Esteva**, UNAM.

Low-Dimensional Topology (Code: SS 8A), **Kenneth L. Baker**, University of Miami, and **Enrique Ramirez Losada**, CIMAT.

Singularity Theory and Algebraic Geometry (Code: SS 6A), **David Eisenbud**, University of California, Berkeley, **Anatoly S. Libgober**, University of Illinois at Chicago, **Jose Seade**, UNAM, and **Xavier Gomez-Mont**, CIMAT.

Toeplitz Operators and Discrete Quantum Models (Code: SS 5A), **Alejandro Uribe**, University of Michigan, and **Maciej Zworski**, University of California, Berkeley.

Syracuse, New York

Syracuse University

October 2–3, 2010

Saturday – Sunday

Meeting #1062

Eastern Section
Associate secretary: Steven H. Weintraub
Announcement issue of *Notices*: June/July 2010
Program first available on AMS website: August 19, 2010
Program issue of electronic *Notices*: October
Issue of *Abstracts*: Volume 31, Issue 4

Deadlines

For organizers: March 2, 2010
For consideration of contributed papers in Special Sessions: June 15, 2010
For abstracts: August 10, 2010

The scientific information listed below may be dated. For the latest information, see `www.ams.org/amsmtgs/sectional.html`.

Invited Addresses

Alan Frieze, Carnegie-Mellon University, *Title to be announced.*

Yan Guo, Brown University, *Title to be announced.*

William Minicozzi, Johns Hopkins University, *Title to be announced.*

Andrei Zelevinsky, Northeastern University, *Title to be announced.*

Special Sessions

Difference Equations and Applications (Code: SS 2A), **Michael Radin**, Rochester Institute of Technology.

Graphs Embedded in Surfaces, and Their Symmetries (Code: SS 4A), **Jack E. Graver** and **Mark E. Watkins**, Syracuse University.

Mathematical Image Processing (Code: SS 5A), **Lixin Shen** and **Yuesheng Xu**, Syracuse University.

Nonlinear Analysis and Geometry (Code: SS 1A), **Tadeusz Iwaniec**, **Leonid V. Kovalev**, and **Jani Onninen**, Syracuse University.

Several Complex Variables (Code: SS 3A), **Dan F. Coman** and **Evgeny A. Poletsky**, Syracuse University.

Los Angeles, California

University of California Los Angeles

October 9–10, 2010

Saturday – Sunday

Meeting #1063

Western Section
Associate secretary: Michel L. Lapidus
Announcement issue of *Notices*: August 2010
Program first available on AMS website: August 26, 2010
Program issue of electronic *Notices*: October 2010
Issue of *Abstracts*: Volume 31, Issue 4

Deadlines

For organizers: March 10, 2010
For consideration of contributed papers in Special Sessions: June 22, 2010
For abstracts: August 17, 2010

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/sectional.html.

Invited Addresses

Greg Kuperberg, University of California Davis, *Title to be announced.*

Cris Moore, University of New Mexico, *Title to be announced.*

Stanley Osher, University of California Los Angeles, *Title to be announced.*

Terence Tao, University of California Los Angeles, *Title to be announced* (Einstein Public Lecture in Mathematics).

Melanie Wood, Princeton University, *Title to be announced.*

Special Sessions

Applications of Nonlinear PDE (Code: SS 5A), **Susan J. Friedlander** and **Igor Kukavica**, University of Southern California.

Combinatorics and Probability on Groups (Code: SS 3A), **Jason Fulman** and **Robert Guralnick**, University of Southern California, and **Igor Pak**, University of California Los Angeles.

Extremal and Probabilistic Combinatorics (Code: SS 4A), **Benny Sudakov**, University of California Los Angeles, and **Jacques Verstraete**, University of California San Diego.

Large Cardinals and the Continuum (Code: SS 2A), **Matthew Foreman**, University of California Irvine, **Alekos Kechris**, California Institute for Technology, **Itay Neeman**, University of California Los Angeles, and **Martin Zeman**, University of California Irvine.

Mathematical Models of Random Phenomena (Code: SS 7A), **Mark Burgin**, University of California Los Angeles, and **Alan C. Krinik**, California State Polytechnic University Pomona.

Recent Trends in Probability and Related Fields (Code: SS 6A), **Marek Biskup**, University of California Los Angeles, **Yuval Peres**, Microsoft Research, and **Sebastien Roch**, University of California Los Angeles.

Topology and Symplectic Geometry (Code: SS 1A), **Robert Brown** and **Ciprian Manolescu**, University of California Los Angeles, and **Stefano Vidussi**, University of California Riverside.

Notre Dame, Indiana

Notre Dame University

November 5–7, 2010

Friday – Sunday

Meeting #1064

Central Section
Associate secretary: Georgia Benkart
Announcement issue of *Notices*: September 2010
Program first available on AMS website: September 23, 2010
Program issue of electronic *Notices*: November 2010
Issue of *Abstracts*: Volume 31, Issue 4

Deadlines

For organizers: March 8, 2010
For consideration of contributed papers in Special Sessions: July 27, 2010
For abstracts: September 14, 2010

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/sectional.html.

Invited Addresses

Laura DeMarco, University of Illinois at Chicago, *Title to be announced.*

Jordan Ellenberg, University of Wisconsin, *Title to be announced.*

David Fisher, Indiana University, *Title to be announced.*

Jared Wunsch, Northwestern University, *Title to be announced.*

Special Sessions

Algebraic and Topological Combinatorics (Code: SS 9A), **John Shareshian**, Washington University, and **Bridget Tenner**, DePaul University.

Commutative Algebra and Its Interactions with Algebraic Geometry (Code: SS 2A), **Claudia Polini**, University of Notre Dame, **Alberto Corso**, University of Kentucky, and **Bernd Ulrich**, Purdue University.

Groups, Representations, and Characters (Code: SS 4A), **James P. Cossey**, University of Akron, and **Mark Lewis**, Kent State University.

Hilbert Functions in Commutative Algebra and Algebraic Combinatorics (Code: SS 3A), **Fabrizio Zanello**, Michigan Technological University, **Juan Migliore**, University of Notre Dame, and **Uwe Nagel**, University of Kentucky.

Interdisciplinary Session on Deterministic and Stochastic Partial Differential Equations (Code: SS 5A), **Nathan Glatt-Holtz**, Indiana University, and **Vlad Vicol**, University of Southern California.

Nonlinear Evolution Equations (Code: SS 7A), **Alex Himonas** and **Gerard Misiolek**, University of Notre Dame.

Number Theory and Physics (Code: SS 8A), **Adrian Clingher**, University of Missouri St. Louis, **Charles Doran**, University of Alberta, **Shabnam N. Kadir**, Wilhelm Leibniz Universitat, and **Rolf Schimmrigk**, Indiana University.

Quasigroups, Loops, and Nonassociative Division Algebras (Code: SS 6A), **Clifton E. Ealy**, Western Michigan University, **Stephen Gagola**, University of Arizona, **Julia Knight**, University of Notre Dame, **J. D. Phillips**, Northern Michigan University, and **Petr Vojtechovsky**, University of Denver.

Singularities in Algebraic Geometry (Code: SS 1A), **Nero Budur**, University of Notre Dame, and **Lawrence Ein**, University of Illinois at Chicago.

Richmond, Virginia

University of Richmond

November 6–7, 2010

Saturday – Sunday

Meeting #1065

Southeastern Section
Associate secretary: Matthew Miller
Announcement issue of *Notices*: September 2010
Program first available on AMS website: September 23, 2010
Program issue of electronic *Notices*: November
Issue of *Abstracts*: Volume 31, Issue 4

Deadlines

For organizers: March 8, 2010
For consideration of contributed papers in Special Sessions: July 27, 2010
For abstracts: September 14, 2010

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/sectional.html.

Invited Addresses

Matthew H. Baker, Georgia Institute of Technology, *Title to be announced.*

Michael J. Field, University of Houston, *Title to be announced.*

Sharon R. Lubkin, North Carolina State University, *Title to be announced.*

Stefan Richter, University of Tennessee, Knoxville, *Title to be announced.*

Special Sessions

Operator Theory (Code: SS 2A), **Stefan Richter**, University of Tennessee, and **William T. Ross**, University of Richmond.

Pucon, Chile

December 15–18, 2010

Wednesday – Saturday

Meeting #1066

First Joint International Meeting between the AMS and the Sociedad de Matematica de Chile.
Associate secretary: Steven H. Weintraub
Announcement issue of *Notices*: June 2010
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: To be announced
Issue of *Abstracts*: To be announced

Deadlines

For organizers: April 15, 2010
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/internmtgs.html.

AMS Invited Addresses

Ricardo Baeza, Universidad de Talca, Chile, *Title to be announced.*

Igor Dolgachev, University of Michigan, *Title to be announced.*

Andres Navas, Universidad de Santiago de Chile, *Title to be announced.*

Rodolfo Rodriguez, Universidad de Concepcion, *Title to be announced.*

Gunther Uhlmann, University of Washington, *Title to be announced.*

S. R. Srinivasa Varadhan, New York University, *Title to be announced.*

AMS Special Sessions

Arithmetic of Quadratic Forms and Integral Lattices **Maria Ines Icaza**, Universidad de Talca, Chile, **Wai Kiu Chan**, Wesleyan University, and **Ricardo Baeza**, Universidad de Talca, Chile.

Automorphic Forms and Dirichlet Series, **Yves Martin**, Universidad de Chile, Chile, and **Solomon Friedberg**, Boston College.

Complex Algebraic Geometry, **Giancarlo Urzua** and **Eduardo Cattani**, University of Massachusetts.

Foliations and Dynamics, **Andrés Navas**, Universidad de Santiago de Chile, and **Rostislav Grigorchuk**, University of Texas.

Group Actions: Probability and Dynamics, **Andres Navas**, Universidad de Santiago de Chile, and **Rostislav Grigorchuk**, University of Texas.

Non-Associative Algebras, **Alicia Labra**, Universidad de Chile, and **Kevin McCrimmon**, University of Virginia.

New Orleans, Louisiana

New Orleans Marriott and Sheraton New Orleans Hotel

January 5–8, 2011

Wednesday – Saturday
Joint Mathematics Meetings, including the 117th Annual Meeting of the AMS, 94th Annual Meeting of the Mathematical Association of America, annual meetings of the Association for Women in Mathematics (AWM) and the National Association of Mathematicians (NAM), and the winter meeting of the Association for Symbolic Logic (ASL), with sessions contributed by the Society for Industrial and Applied Mathematics (SIAM).
Associate secretary: Steven H. Weintraub
Announcement issue of *Notices*: October 2010
Program first available on AMS website: November 1, 2010
Program issue of electronic *Notices*: January 2011
Issue of *Abstracts*: Volume 32, Issue 1

Deadlines

For organizers: April 1, 2010
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Statesboro, Georgia

Georgia Southern University

March 12–13, 2011

Saturday – Sunday
Southeastern Section
Associate secretary: Matthew Miller
Announcement issue of *Notices*: To be announced
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: To be announced
Issue of *Abstracts*: To be announced

Deadlines

For organizers: August 12, 2010
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Iowa City, Iowa

University of Iowa

March 18–20, 2011

Friday – Sunday
Central Section
Associate secretary: Georgia Benkart
Announcement issue of *Notices*: To be announced
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: To be announced
Issue of *Abstracts*: To be announced

Deadlines

For organizers: July 16, 2010
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Worcester, Massachusetts

College of the Holy Cross

April 9–10, 2011

Saturday – Sunday
Eastern Section
Associate secretary: Steven H. Weintraub
Announcement issue of *Notices*: To be announced
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: To be announced
Issue of *Abstracts*: To be announced

Deadlines

For organizers: September 9, 2010
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Las Vegas, Nevada

University of Nevada

April 30 – May 1, 2011

Saturday – Sunday
Western Section
Associate secretary: Michel L. Lapidus
Announcement issue of *Notices*: To be announced
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: To be announced
Issue of *Abstracts*: To be announced

Deadlines

For organizers: To be announced
For consideration of contributed papers in Special Sessions: To be announced

For abstracts: To be announced

The scientific information listed below may be dated. For the latest information, see www.ams.org/amsmtgs/sectional.html.

Special Sessions

Advances in Modeling, Numerical Analysis and Computations of Fluid Flow Problems (Code: SS 2A), **Monika Neda**, University of Nevada Las Vegas.

Geometric PDEs (Code: SS 1A), **Matthew Gursky**, Notre Dame University, and **Emmanuel Hebey**, Universite de Cergy-Pontoise.

Lincoln, Nebraska

University of Nebraska-Lincoln

October 14–16, 2011

Friday – Sunday
Central Section
Associate secretary: Georgia Benkart
Announcement issue of *Notices*: August 2011
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: October 2011
Issue of *Abstracts*: To be announced

Deadlines

For organizers: To be announced
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Salt Lake City, Utah

University of Utah

October 22–23, 2011

Saturday – Sunday
Western Section
Associate secretary: Michel L. Lapidus
Announcement issue of *Notices*: To be announced
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: To be announced
Issue of *Abstracts*: To be announced

Deadlines

For organizers: To be announced
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Boston, Massachusetts

John B. Hynes Veterans Memorial Convention Center, Boston Marriott Hotel, and Boston Sheraton Hotel

January 4–7, 2012

Wednesday – Saturday
Joint Mathematics Meetings, including the 118th Annual Meeting of the AMS, 95th Annual Meeting of the Mathematical Association of America, annual meetings of the Association for Women in Mathematics (AWM) and the National Association of Mathematicians (NAM), and the winter meeting of the Association for Symbolic Logic (ASL), with sessions contributed by the Society for Industrial and Applied Mathematics (SIAM).
Associate secretary: Michel L. Lapidus
Announcement issue of *Notices*: October 2011
Program first available on AMS website: November 1, 2011
Program issue of electronic *Notices*: January 2012
Issue of *Abstracts*: Volume 33, Issue 1

Deadlines

For organizers: April 1, 2011
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

San Diego, California

San Diego Convention Center and San Diego Marriott Hotel and Marina

January 9–12, 2013

Wednesday – Saturday
Joint Mathematics Meetings, including the 119th Annual Meeting of the AMS, 96th Annual Meeting of the Mathematical Association of America, annual meetings of the Association for Women in Mathematics (AWM) and the National Association of Mathematicians (NAM), and the winter meeting of the Association for Symbolic Logic (ASL), with sessions contributed by the Society for Industrial and Applied Mathematics (SIAM).
Associate secretary: Georgia Benkart
Announcement issue of *Notices*: October 2012
Program first available on AMS website: November 1, 2012
Program issue of electronic *Notices*: January 2012
Issue of *Abstracts*: Volume 34, Issue 1

Deadlines

For organizers: April 1, 2012
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Baltimore, Maryland

Baltimore Convention Center, Baltimore Hilton, and Marriott Inner Harbor

January 15–18, 2014

Wednesday – Saturday

Joint Mathematics Meetings, including the 120th Annual Meeting of the AMS, 97th Annual Meeting of the Mathematical Association of America, annual meetings of the Association for Women in Mathematics (AWM) and the National Association of Mathematicians (NAM), and the winter meeting of the Association for Symbolic Logic, with sessions contributed by the Society for Industrial and Applied Mathematics (SIAM).

Associate secretary: Matthew Miller
Announcement issue of *Notices*: October 2013
Program first available on AMS website: November 1, 2013
Program issue of electronic *Notices*: January 2013
Issue of *Abstracts*: Volume 35, Issue 1

Deadlines

For organizers: April 1, 2013
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

San Antonio, Texas

Henry B. Gonzalez Convention Center and Grand Hyatt San Antonio

January 10–13, 2015

Saturday – Tuesday

Joint Mathematics Meetings, including the 121st Annual Meeting of the AMS, 98th Annual Meeting of the Mathematical Association of America, annual meetings of the Association for Women in Mathematics (AWM) and the National Association of Mathematicians (NAM), and the winter meeting of the Association of Symbolic Logic, with sessions contributed by the Society for Industrial and Applied Mathematics (SIAM).

Associate secretary: Steven H. Weintraub
Announcement issue of *Notices*: October 2014
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: January 2015
Issue of *Abstracts*: Volume 36, Issue 1

Deadlines

For organizers: April 1, 2014
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Seattle, Washington

Washington State Convention & Trade Center and the Sheraton Seattle Hotel

January 6–9, 2016

Wednesday – Saturday

Joint Mathematics Meetings, including the 122nd Annual Meeting of the AMS, 99th Annual Meeting of the Mathematical Association of America, annual meetings of the Association for Women in Mathematics (AWM) and the National Association of Mathematicians (NAM), and the winter meeting of the Association of Symbolic Logic, with sessions contributed by the Society for Industrial and Applied Mathematics (SIAM).

Associate secretary: Michel L. Lapidus
Announcement issue of *Notices*: October 2015
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: January 2016
Issue of *Abstracts*: Volume 37, Issue 1

Deadlines

For organizers: April 1, 2015
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Atlanta, Georgia

Hyatt Regency Atlanta and Marriott Atlanta Marquis

January 4–7, 2017

Wednesday – Saturday

Joint Mathematics Meetings, including the 123rd Annual Meeting of the AMS, 100th Annual Meeting of the Mathematical Association of America, annual meetings of the Association for Women in Mathematics (AWM) and the National Association of Mathematicians (NAM), and the winter meeting of the Association of Symbolic Logic, with sessions contributed by the Society for Industrial and Applied Mathematics (SIAM).

Associate secretary: Georgia Benkart
Announcement issue of *Notices*: October 2016
Program first available on AMS website: To be announced
Program issue of electronic *Notices*: January 2017
Issue of *Abstracts*: Volume 38, Issue 1

Deadlines

For organizers: April 1, 2016
For consideration of contributed papers in Special Sessions: To be announced
For abstracts: To be announced

Meetings and Conferences of the AMS

Associate Secretaries of the AMS

Western Section: Michel L. Lapidus, Department of Mathematics, University of California, Surge Bldg., Riverside, CA 92521-0135; e-mail: `lapidus@math.ucr.edu`; telephone: 951-827-5910.

Central Section: **Georgia Benkart** (after January 31, 2010), University of Wisconsin-Madison, Department of Mathematics, 480 Lincoln Drive, Madison, WI 53706-1388; e-mail: `benkart@math.wisc.edu`; telephone: 608-263-4283.

Eastern Section: **Steven H. Weintraub**, Department of Mathematics, Lehigh University, Bethlehem, PA 18105-3174; e-mail: `steve.weintraub@lehigh.edu`; telephone: 610-758-3717.

Southeastern Section: **Matthew Miller,** Department of Mathematics, University of South Carolina, Columbia, SC 29208-0001, e-mail: `miller@math.sc.edu`; telephone: 803-777-3690.

The Meetings and Conferences section of the *Notices* gives information on all AMS meetings and conferences approved by press time for this issue. Please refer to the page numbers cited in the table of contents on this page for more detailed information on each event. Invited Speakers and Special Sessions are listed as soon as they are approved by the cognizant program committee; the codes listed are needed for electronic abstract submission. For some meetings the list may be incomplete. **Information in this issue may be dated. Up-to-date meeting and conference information can be found at `www.ams.org/meetings/`.**

Meetings:

Important Information Regarding AMS Meetings

Potential organizers, speakers, and hosts should refer to page 92 in the January 2010 issue of the *Notices* for general information regarding participation in AMS meetings and conferences.

Abstracts

Speakers should submit abstracts on the easy-to-use interactive Web form. No knowledge of LaTeX is necessary to submit an electronic form, although those who use LaTeX may submit abstracts with such coding, and all math displays and similarily coded material (such as accent marks in text) must be typeset in LaTeX. Visit `http://www.ams.org/cgi-bin/abstracts/abstract.pl`. Questions about abstracts may be sent to `abs-info@ams.org`. Close attention should be paid to specified deadlines in this issue. Unfortunately, late abstracts cannot be accommodated.

Conferences: (see `http://www.ams.org/meetings/` for the most up-to-date information on these conferences.)

Co-sponsored conferences:

February 18–22, 2010: AAAS Meeting in San Diego, CA (please see `www.aaas.org/meetings` for more information).

March 18-21, 2010: First International Conference on Mathematics and Statistics, AUS-ICMS '10, American University of Sharjah, Sharjah, United Arab Emirates (please see `http://www.aus.edu/conferences/icms10/` for more information).

May 24-29, 2010: From Carthage to the World, the Isoperimetric Problem of Queen Dido and its Mathematics Ramifications, Carthage, Tunisia (for more information please see `http://math.arizona.edu/~dido/welcome.html`).

June 17-19, 2010: Coimbra Meeting on 0-1 Matrix Theory and Related Topics, University of Coimbra, Portugal (for more information please see `http://www.mat.uc.pt/~cmf/01MatrixTheory`).

CAMBRIDGE

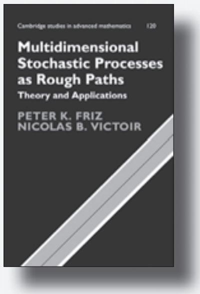
Outstanding Titles in Mathematics!

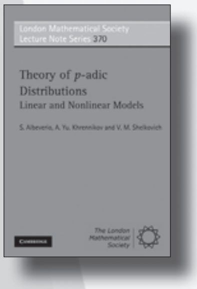
New Titles in the
Lecture Notes in Logic Series!

Kurt Gödel
Essays for his Centennial
Edited by Solomon Feferman, Charles Parsons, and Stephen G. Simpson
Lecture Notes in Logic
$90.00: Hardback: 978-0-521-11514-8: 375 pp.

A Framework for Priority Arguments
Manuel Lerman
Lecture Notes in Logic
$75.00: Hardback: 978-0-521-11969-6: 176 pp.

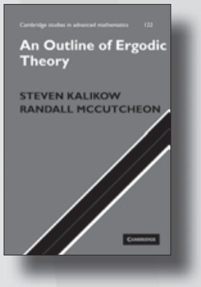
Multidimensional Stochastic Processes as Rough Paths
Theory and Applications
Peter K. Friz and Nicolas B. Victoir
Cambridge Studies in Advanced Mathematics
$85.00: Hardback: 978-0-521-87607-0: 675 pp.



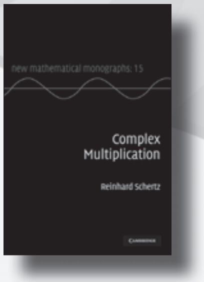

London Mathematical Society Lecture Note Series 370
Theory of p-adic Distributions
Linear and Nonlinear Models
S. Albeverio, A. Yu. Khrennikov and V. M. Shelkovich

Theory of *p*-adic Distributions
Linear and Nonlinear Models
S. Albeverio, A. Yu Khrennikov, and V. M. Shelkovich
London Mathematical Society Lecture Note Series
$70.00: Paperback: 978-0-521-14856-6: 350 pp.

An Outline of Ergodic Theory
Steven Kalikow and Randall McCutcheon
Cambridge Studies in Advanced Mathematics
$59.00: Hardback: 978-0-521-19440-2: 160 pp.

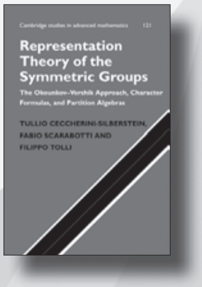


Moonshine - The First Quarter Century and Beyond
Proceedings of a Workshop on the Moonshine Conjectures and Vertex Algebras
Edited by James Lepowsky, John McKay, and Michael P. Tuite
London Mathematical Society Lecture Note Series
$78.00: Paperback: 978-0-521-10664-1: 400 pp.

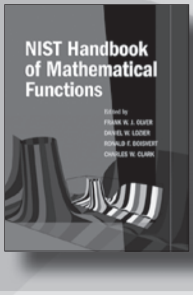


Complex Multiplication
Reinhard Schertz
New Mathematical Monographs
$99.00: Hardback: 978-0-521-76668-5: 375 pp.

Representation Theory of the Symmetric Groups
The Okounkov-Vershik Approach, Character Formulas, and Partition Algebras
Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli
Cambridge Studies in Advanced Mathematics
$75.00: Hardback: 978-0-521-11817-0: 430 pp.


Representation Theory of the Symmetric Groups
The Okounkov-Vershik Approach, Character Formulas, and Partition Algebras
TULLIO CECCHERINI-SILBERSTEIN, FABIO SCARABOTTI AND FILIPPO TOLLI

NIST Handbook of Mathematical Functions
Companion to the Digital Library of Mathematical Functions
Edited by Frank W. J. Olver, Daniel W. Lozier, Ronald F. Boisvert, and Charles W. Clark
$99.00: Hardback: 978-0-521-19225-5: 966 pp.
$50.00: Paperback: 978-0-521-14063-8



Prices subject to change.

www.cambridge.org/us/mathematics • 800.872.7423

CAMBRIDGE
UNIVERSITY PRESS

American Mathematical Society

JMM Bestsellers 2010

2010 Joint Mathematics Meetings San Francisco, CA

Lectures on Fractal Geometry and Dynamical Systems

Yakov Pesin and **Vaughn Climenhaga**, *Pennsylvania State University, University Park, PA*

This volume is published in cooperation with the Mathematics Advanced Study Semesters.

Student Mathematical Library, Volume 52; 2009; 314 pages; Softcover; ISBN: 978-0-8218-4889-0; List US$51; AMS members US$41; Order code STML/52

Low-Dimensional Geometry

From Euclidean Surfaces to Hyperbolic Knots

Francis Bonahon, *University of Southern California, Los Angeles, CA*

This volume was co-published with the Institute for Advanced Study/Park City Mathematics Institute.

Student Mathematical Library, Volume 49; 2009; 384 pages; Softcover; ISBN: 978-0-8218-4816-6; List US$54; AMS members US$43; Order code STML/49

Low Dimensional Topology

Tomasz S. Mrowka, *Massachusetts Institute of Technology, Cambridge, MA*, and **Peter S. Ozsváth**, *Columbia University, New York, NY*, Editors

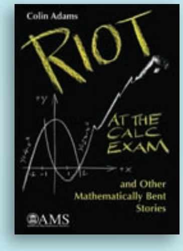
Titles in this series are co-published with the Institute for Advanced Study/Park City Mathematics Institute. Members of the Mathematical Association of America (MAA) and the National Council of Teachers of Mathematics (NCTM) receive a 20% discount from list price.

IAS/Park City Mathematics Series, Volume 15; 2009; 315 pages; Hardcover; ISBN: 978-0-8218-4766-4; List US$69; AMS members US$55; Order code PCMS/15

Mathematics and Music

David Wright, *Washington University, St. Louis, MO*

Mathematical World, Volume 28; 2009; 161 pages; Softcover; ISBN: 978-0-8218-4873-9; List US$35; AMS members US$28; Order code MAWRLD/28



Riot at the Calc Exam and Other Mathematically Bent Stories

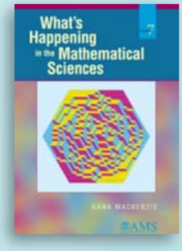
Colin Adams, *Williams College, Williamstown, MA*

2009; 271 pages; Softcover; ISBN: 978-0-8218-4817-3; List US$32; AMS members US$26; Order code MBK/62

How to Teach Mathematics, Second Edition

Steven G. Krantz, *Washington University, St. Louis, MO*

1999; 307 pages; Softcover; ISBN: 978-0-8218-1398-0; List US$27; AMS members US$22; Order code HTM/2



What's Happening in the Mathematical Sciences, Volume 7

Dana Mackenzie

What's Happening in the Mathematical Sciences, Volume 7; 2009; 127 pages; Softcover; ISBN: 978-0-8218-4478-6; List US$19.95; AMS members US$15.95; Order code HAPPENING/7

AMS BOOKSTORE www.ams.org/bookstore

TEXTBOOKS FROM THE AMS

AMS American Mathematical Society

0002-9920(201003)57:3;1-2