Commentary

In My Opinion

Cryptography in Crisis

Rarely does mathematics reach the front pages of newspapers, yet for two decades some simple and elegant number theory has enjoyed a very public discussion—but this discussion has been political, not mathematical. The conflict is over the deployment of strong cryptography.[1]

In the mid-1970s Whitfield Diffie, Martin Hellman, and Ralph Merkle proposed that some computations might be of such great complexity that even though both halves of the computation were known (say, by an eavesdropper on the Internet), computing the inverse (decrypting) would not be possible in a reasonable amount of time, thus providing a way to communicate securely over insecure networks. Three MIT computer scientists—Ron Rivest, Len Adleman, and Adi Shamir—used elementary number theory to develop the public-key cryptography system RSA, which not only computes digital signatures (electronic signatures that provide nonrepudiable ratification) but also provides confidentiality.

It was a beautiful application; shortly afterwards the MIT professors found out just how interesting their solution was. As Rivest prepared the work to present at a meeting of the Institute of Electrical and Electronics Engineers in Ithaca, New York, the MIT professors received an odd letter from one J. A. Meyer of Bethesda, Maryland. Meyer claimed that since foreign nationals would be at the conference, discussion of the RSA cryptosystem would violate the International Trafficking in Arms Regulations. An enterprising *Science* reporter discovered Meyer was an employee of the National Security Agency (NSA), which quickly disavowed any connection with the letter, and Rivest gave the talk.

The letter was the precursor of twenty years of government policy. Through a variety of means including export control, the U.S. Government has delayed the deployment of strong cryptography. The latest government effort is key escrow (or key recovery, as it is currently called), in which private keys are stowed so that governments can get to them.

In 1998 the Internet is no longer a theory but a commercial enterprise. And electronic communications are at risk. FBI director Louis Freeh has testified that twenty-three foreign governments routinely target U.S. business for economic espionage. Increasingly, companies are seeking protection for their online operations. RSA Data Security is thriving. However, like all U.S. firms it is prohibited, with only narrow exceptions, from exporting codes with keys greater than 40 bits. These restrictions exist despite a clear demonstration of the inherent weakness of 40-bit cryptosystems: in under four hours a Berkeley graduate student, using the idle time of 250 workstations, was able to break a system encoded with a 40-bit key.

Scientific freedom and human rights are in collision with current government policy. Papers and ideas circulate freely; programs on disks and over the Internet do not. While cryptography research involves collaborations amongst scientists on different continents, U.S. export regulations keep a University of Illinois professor from posting source code for his encryption algorithm on the Internet. And despite the value of the Internet as a communications venue, U.S. export control complicates its use for democratic organizations. An American Association for the Advancement of Science program advising human-rights groups on information security (e.g., on protecting sensitive e-mail from government investigators) cannot give the code to the organizations, but must instead point the groups to foreign Web sites for the information.

The United States Government argues that its policies, by keeping strong cryptography out of shrink-wrapped software (of which the U.S. remains the leading manufacturer), secures national objectives. Cryptography can hide evidence from government investigators, but the lack of strong cryptography leaves an online society dangerously vulnerable. A recent National Research Council panel on cryptography policy, whose members included a former U.S. attorney general and a former deputy director of the NSA, said “the advantages of more widespread use of cryptography outweigh the disadvantages” and recommended “broad availability” of cryptography to legitimate users in the U.S.[2]

U.S. key-recovery proposals are considered problematic at best. Key-recovery centers provide a rich target for those who seek to spy, and key recovery is easily circumvented by using additional forms of cryptography on top of the key-recovery scheme. Finally, it is difficult to implement key recovery internationally. U.S. proposals have received a poor reception, and their main effect has been to hobble industry. Meanwhile, other nations have stepped into the breach.

What exactly does the U.S. seek to export? Secure communications are needed by U.S. companies operating abroad and by scientists, inventors, politicians, and private citizens everywhere. Present U.S. cryptography policy was designed when the enemy was the Soviet Union. Mathematicians, computer scientists, policymakers, users of the Internet—all have a stake in moving U.S. policy to one that promotes communications privacy, economic security, scientific freedom, and human rights.

—Susan Landau
Associate Editor

[1] *A relative term meaning the cryptography is hard to break with current computational power.*

[2] *National Research Council, Commission on Physical Sciences, Mathematics, and Applications, Computer Science and Telecommunications Board, Committee to Study National Cryptography Policy,* Cryptography’s Role in Securing the Information Society *(Kenneth Dam and Herbert Lin, eds.), National Academy Press, 1996.*

Letters

Response to Sadosky's "Forum"

I am writing in response to Professor Sadosky's "Forum" article, "On Issues of Immigration and Employment for Mathematicians" (*Notices*, December 1997).

Sadosky asks, "Since when are mathematicians selected on their ambition to make money?" This is intended to refute Geoff Davis's suggestion ("Mathematicians and the market," *Notices*, November 1997) that economic forces play a significant role in the mathematics labor market. Sadosky's rhetoric misses the point; one might rephrase her question as, "Since when are mathematicians selected on their desire for a full-time, tenure-track job?" It is bad for the field of mathematics if we are losing talented people before they even enter the field because prospects in the job market are so bad.

Sadosky asks, "Is it the American Way to give preference to less-qualified U.S. citizens?" The answer is, "Yes, absolutely." In just about every profession it is quite difficult to hire a nonresident alien as long as there is a qualified resident available for the job—not a more qualified resident, not an equally qualified one, but merely a qualified resident. This is true for doctors, lawyers, engineers, and practically every profession *except* for college and university professors. One might say that this gives unfair preference to permanent residents of the U.S., but removing such immigration barriers would have profound economic consequences. When discussing immigration issues, it is important to consider these potential consequences.

Sadosky doesn't ask, "If the U.S. had such a strong history of importing mathematicians before 1976, then why did the government feel it necessary to make it even easier to import them in 1976? And why again in 1990?" Before 1976 the same immigration restrictions applied to college and university professors as to everyone else; that year several of these restrictions were weakened, but only for academics. In 1990 several more of these restrictions were weakened and, again, primarily for academics. Were these changes beneficial to academia and to mathematics in particular?

Sadosky doesn't ask, "If you believe that U.S. immigration law is a factor in the employment market, what steps should be taken?" She seems to imply that various people (as reported in the *Boston Globe* and the *Wall Street Journal*) have suggested banning immigrants. That sort of suggestion is extreme and could be dismissed out of hand. Of course, I haven't heard that suggestion; instead, I've heard the proposal that the 1990 changes (and/or the 1976 changes) in the immigration law be repealed. This proposal, I think, deserves serious discussion and consideration, something completely lacking in Sadosky's article.

Sadosky doesn't ask, "What role do economic forces, such as immigration law, play in the academic job market? If you alter these forces, what effects should you expect?" Again, these are serious issues, and they deserve serious consideration. I hope the *Notices* will provide a forum for an open discussion of these and similar issues.

John H. Palmieri
Visiting Assistant Professor
University of Notre Dame

(Received December 18, 1997)

Defining Uniform Continuity First Does Not Help

At the risk of prolonging a discussion of pedagogy in the pages of an AMS publication, I wish to say a few things about Peter Lax's proposal in the January *Notices* that we use uniform continuity as an introduction to continuity and limits. The first text I know of that did this was John M. H. Olmsted's two-volume *Calculus with Analytic Geometry*, published in 1966 by Appleton-Century-Crofts. We used it in the late 1960s, but abandoned it about 1970 because our students weren't understanding limits or any kind of continuity any better than they had with other approaches, and they were having to work a lot harder. I think the reason it didn't succeed was that even though only two quantifiers were used in the definition of uniform continuity, that was still too complicated. That is, defining uniform continuity first did not lessen the difficulties with (ϵ, δ) definitions Leonard Gillman eloquently described in the September 1997 *Notices*.

The purpose of limits bears greatly on which definition of limits to use. If the purpose is to serve as the foundation for rigorous arguments in analysis, then the quantifiers in (ϵ, δ) are unavoidable. But the purpose of a limit in a beginning calculus course is to be the foundation for the definitions of the ideas studied, not the foundation of rigorous arguments, and so its definition need only be descriptive. The task is to devise for the student experiences such that having them and thinking about them will provide a foundation of meaning so that the description of a limit will make sense, as will the uses to which the limit is put. My own preference is to emphasize uses of graphs before getting to calculus. Then I can use graphs to describe limits. The test is for the student to tell correctly from the graph of a function whether limits of that function at various points exist, and if so, what they are. It's enough of a foundation for the limit for beginning students, and it's harder than it sounds. It may be that a numeric approach such as Lax's illustration can have meaning if the students have had to think about the accuracy of their input and output. Mine haven't. I've had even less luck with such things than with graphs, and I'm skeptical. But students' backgrounds change, so it's worth another try.

Albert W. Briggs Jr.
Washington College

(Received December 22, 1997)

Elevate the Level of Discussion of Educational Issues

"Calculus Reform — for the $Millions" by Klein and Rosen (*Notices*, November 1997) raises some points that are central to the improvement of mathematics education at every level. But the title and tone of their article almost guarantee that the issues they raise will be discussed only among groups of people who already agree with one another.

It's unlikely that the people signing this letter would be unanimous on any issue of substance in education except that sarcasm and insult have no place in the debate about mathematics education.

This is an extremely important time in mathematics education. Serious scholars are proposing theories that call for major revamping of educational practice. These theories need to be debated and discussed, and the foundations on which they rest need to be ruthlessly scrutinized by everyone involved in mathematics education, especially by the mathematics community. We call on the community to elevate the level of discussion so that the serious work of teaching mathematics can move forward.

Al Cuoco
Education Development Center,
and 19 others

(Received December 22, 1997)

Editor's Note: Al Cuoco informed the *Notices* that the complete list of signatories is available at `http://www.edc.org/LTT/BOS/letter.html`.

Rota and the Theory of Commutative Rings

Gian-Carlo Rota's article "The Many Lives of Lattice Theory" (*Notices*, December 1997) is very interesting and also controversial. It is intended to be so!

May I point out that in spite of belonging to "the sect of algebraic geometers", the authors of *Commutative Algebra*—Oscar Zariski and I—did not hide the fact that for commutative rings the Chinese Remainder Theorem is equivalent with the distributive laws for ideals with respect to intersections and sums (vol. I, pp. 279–281). We even showed that one of the distributive laws implies the other one. The proofs are rather straightforward, much more so than what is proved in the following sections, culminating with the reciprocity law and Kummer's theorem.

On the other hand, I object to G.-C. Rota's saying that "The theory of commutative rings has been torn between two customers: number theory and geometry." On the contrary, by providing a common tool for (diophantine) number theory and algebraic geometry, commutative algebra was instrumental for the cross-fertilization of both theories. It began with Dedekind and Weber, and later the works of A. Weil, A. Grothendieck, P. Deligne, S. Arakelov, G. Faltings, A. Wiles, and many others were striking examples. Also, deep results about "complete-intersection" rings, proved by R. Taylor, provided the finishing touch to A. Wiles's proof of Fermat's theorem.

Pierre Samuel
Université de Paris-Sud, Orsay

(Received December 23, 1997)

Volunteer Work on Electronic Journals Vital

The September 1997 editorial by Steven G. Krantz covered an area, electronic math journals, where there are many important issues which need careful evaluation and investigation; it is therefore unfortunate that the potential problems he highlighted are ones that are comparatively well understood and that have already been solved, with the help of enlightened publishers such as the AMS, by the more thoughtful parts of the academic community. It is, however, your editorial prerogative to use space and time in this way.

Of far greater concern is the author's apparent dismissal of the excellent, pioneering work that many others are doing (paid or unpaid) in adapting the rapidly developing technology to serve the diverse needs of the mathematical community.

It is in particular the voluntary efforts, supported by the more explicitly financed activity of professional bodies and publishers, that keep the community alive and stimulate the necessary investigation into the best methods of achieving both the traditional and future goals of mathematical publishing. The independent, self-motivated nature of this work is essential to its originality and creativity and hence its vitality and utility.

Here are some questions pertinent to an editor of an AMS publication: Is the author aware that vital parts of the software systems used by the AMS in their publishing are also being developed and maintained by similar voluntary work, including much high-quality input from professional mathematicians and AMS employees? Is this also a waste of their time? And will he please apologize to all of his colleagues whose work he has thus disparaged as having a "negative impact"?

I very much hope that the real issues surrounding the purpose and practice of mathematical publishing in the modern world will continue to be covered by the *Notices* and that the AMS will keep its leading and progressive role in all aspects of the use of digital technology. But will you please avoid facile and derogatory editorials, on any subject.

—Chris A. Rowley
LaTeX3 Project

(Received January 20, 1998)

About the Cover

This month's cover image is adapted from the poster for Mathematics Awareness Week 1998 (April 26–May 2), the topic of which is "Mathematics and Imaging".

The original image (upper left) is the sum of the other three. Each pulls out different features of the original. We can think of the image as being synthesized by three different instruments, in a way similar to a musical orchestration where the final sound is the sum of the notes from each instrument.

This mathematical transcription is useful for a more efficient and accurate storage and processing of imaging data, but also provides tools for denoising and identifying structure in images. For example, it can sharpen detail in medical images, such as MRI, and be used to identify particular objects for diagnostic purposes.

Images provided by Ronald Coifman, Yale University.