BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 41, Number 1, Pages 127–133
S 0273-0979(03)00999-6
Article electronically published on October 29, 2003

Number theory in function fields, by Michael Rosen, Springer-Verlag, New York, 2002, xii+358 pp., $49.95, ISBN 0-387-95335-3

We begin with a short (obviously incomplete) historical summary related to the book being reviewed. A complex number α is said to be "algebraic" if there is a polynomial $0 \neq p(x)$ with integer coefficients such that $p(\alpha) = 0$; otherwise α is said to be "transcendental". The first recorded instance of mathematicians encountering an "irrational" algebraic number appears to be the ancient Greeks. Indeed, if one considers a square with unit sides, then, of course, by the Pythagorean Theorem a diagonal must have length $\sqrt{2}$. To Pythagoras (and his followers) is also due the result that $\sqrt{2}$ cannot be expressed as the quotient of integers. One story has it that Hippasus, the person who revealed this irrationality, died at sea in a shipwreck, "struck by the wrath of the gods."

As history evolved, so did mathematicians' views about numbers. During the sixteenth century cubic equations were discussed by the Italian algebraists G. Cardano and R. Bombelli ([v1], Part C §2). In particular a very curious phenomenon appeared with equations like $x^3 = 15x + 4$. Here one readily finds that $x = 4$ is a root and, after division by $x-4$, that the other two roots are also real. However, the Italian school had developed methods to handle such an equation directly. These methods do give the correct real roots but *only* through the use of quantities like $\sqrt[3]{2 + \sqrt{-121}}$, which are obviously non-real. This caused Cardano to have serious misgivings. Bombelli was concerned enough to call the square roots of negative numbers "sophistic" ([v1], p. 60) but eventually was persuaded of the correctness of the formulae; such quantities therefore began to be used in algebra and analysis. Instead of Bombelli's description, we now have "imaginary numbers" lying in the larger realm of "complex numbers".

With the proof by Gauss of the Fundamental Theorem of Algebra, it became reasonable to wonder how large a subset of $\mathbb{C}$ was occupied by the algebraic numbers. Many of the classical constants of mathematics, such as e (Hermite, 1873) and π (Lindemann, 1882) were shown to be transcendental. (Lindemann's result also flies in the face of ancient perceptions; there are biblical verses, for instance, where $\pi = 3$.) Still it came as yet another major surprise when in 1874 G. Cantor proved that "almost all" complex numbers must be transcendental by non-constructive set-theoretic means.

To the Greeks, and in particular Euclid, is also due the wonderful proof that the set of prime numbers is infinite. From this time on, issues about prime numbers have been of central concern to mathematicians. As mathematicians became more familiar with the techniques of calculus, advances in our understanding of prime numbers became possible. Indeed, it fell to Euler in the eighteenth century to set the stage for all future such research by introducing the "zeta-function" $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. From elementary calculus one knows that $\zeta(s)$ converges for all $s > 1$

2000 *Mathematics Subject Classification.* Primary 11R58, 11G09, 11R60.

and that $\zeta(1)$, which is the harmonic series, diverges. Euler also makes the fundamental observation that

$$\zeta(s) := \prod_{p \text{ prime}} (1 - p^{-s})^{-1}. \tag{1}$$

Upon taking logs and letting s tend to 1 from the right, he deduced that $\sum_{p \text{ prime}} 1/p$ *also* diverges. Euler further established that $\pi^{-2n}\zeta(2n)$ is a rational number for positive integers n.

Euler's work on primes marks a major advance over Euclid, as it gives some information on the distribution of the set of primes inside the set of all positive integers. However, it was Riemann [R1] in the nineteenth century who illuminated fully the incredible force of Euler's ideas. In the years since Euler, the power of mathematical analysis (real and complex) had grown greatly. In particular, Riemann had at his disposal *Fourier analysis* and the *Poisson summation formula*. Riemann showed that $\zeta(s)$ has a natural interpretation as a meromorphic function on the whole complex plane via the equation

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = 1/2 \int_0^\infty t^{s/2}(\theta(it) - 1)\,\frac{dt}{t}, \tag{2}$$

where $\Gamma(s) = \int_0^\infty e^{-t}t^s\,\frac{dt}{t}$ is Euler's Gamma-function, $i^2 = -1$, and $\theta(z) = \sum_{n=-\infty}^{\infty} e^{in^2\pi z}$ is a classical theta-function. Poisson summation establishes that $\theta(z)$ satisfies the functional equation (as a "modular form of weight 1/2") $\theta(-1/z) = (z/i)^{1/2}\theta(z)$; this, in turn, implies that $\pi^{-s/2}\Gamma(s/2)\zeta(s)$ is invariant under $s \mapsto 1-s$. Finally, Riemann used the complex zeroes of $\zeta(s)$ to give a formula approximating the number of primes less than a given positive number x. The zeroes of $\zeta(s)$ are of two kinds: "trivial zeroes" arising from poles of $\Gamma(s/2)$ and "critical zeroes"; the famous *Riemann-hypothesis* is the expectation that the critical zeroes will be of the form $1/2 + it$, $t \in \mathbb{R}$.

Prime numbers have fascinated mathematicians for many other reasons besides their location. For instance, given a prime number p one has the associated finite field $\mathbb{F}_p := \mathbb{Z}/(p)$ and one can study its properties; in particular, if x is an integer, one can ask whether $x + (p)$ is a square in the field $\mathbb{Z}/(p)$. Let $p \neq 2$ and let q be another odd prime. It turns out that the question of whether p is a square modulo q is intimately related to the question of whether q is a square modulo p; this relationship is codified in Gauss' famous *Law of quadratic reciprocity*. Gauss greatly desired to extend this law to congruences of higher degree. To do so, he studied the "Gaussian integers" $\{a + bi\}$ where a, b are integers; in particular, Gauss was able to extend the concept of unique factorization of integers to the Gaussian integers marking the beginning of the systematic treatment of algebraic numbers. To go further, E. Kummer studied the system $R_\zeta := \{a_1 + a_2\zeta + \cdots + a_j\zeta^j\}$ where the a_t are integers and ζ is a primitive p-th root of unity. When $p = 23$ Kummer discovered, to his dismay, that it was no longer possible to extend unique factorization and then spent the next few years trying to rectify the situation ([Co1], p. 85).

Kummer was followed in this quest by R. Dedekind. Dedekind focused on what we now call the ideal theory of the rings R_ζ (and, in fact, the "algebraic integers" associated to any algebraic number). Dedekind realized that while unique factorization of elements is quite rare, there is *always* unique factorization of ideals. That is, any ideal I can be expressed as the product (ideal) of a finite number of "prime ideals" (i.e., ideals $\mathfrak{p}$ of R_ζ where $R_\zeta/\mathfrak{p}$ is a finite field), and this factorization is

unique in the same way the factorization of an integer is. This marked a tremendous advance and opened the way for modern number theory.

By the latter half of the nineteenth century a very powerful analogy began to be appreciated by algebraists: the same techniques work to describe both algebraic numbers and compact Riemann surfaces. That two such disparate areas of mathematics can be united at all is remarkable. However, it is almost impossible to quantify just how powerful this analogy actually is; the list of fundamental advances in number theory obtained by such reasoning would be very long indeed. The first publication to explicitly reason in this fashion appears to be the sensational 1882 memoir [DW1] of Dedekind-Weber (see also [Di1], §VI.1). Here for instance Dedekind-Weber show how the points of the Riemann-surface can be reinterpreted in the ideal-theoretic language.

As an example of the power of this approach, one now sees how to "compactify" fields of numbers. Indeed, if X is a compact Riemann surface and K is the associated field of meromorphic functions, then the points of X are in $1-1$ correspondence with the absolute values of K (one simply measures the order of zero of the function at a given point), that is the inequivalent ways to measure the "size" of an element of K. Let k then be a "number field" obtained from addition and multiplication by adjoining a fixed algebraic number θ to the rational numbers $\mathbb{Q}$. Every prime ideal $\mathfrak{p}$ in Dedekind's sense gives rise to one such absolute value simply by measuring how divisible an element $x \in k$ is at $\mathfrak{p}$ (in geometric language, the "order of zero"). These absolute values are called the "finite primes". There are, however, other, more classical, ways to measure size. Indeed, let $\sigma\colon k \to \mathbb{C}$ be a field embedding (i.e., a homomorphism of fields); then we simply define $|x|_\sigma := |\sigma(x)|$ where $|?|$ is the standard absolute value of a complex number. Of course if $\sigma'(x) = \overline{\sigma(x)}$ (where $\bar{?}$ is the complex conjugate), then $|x|_{\sigma'} = |x|_\sigma$ and this is the only such relationship.

The finite set of absolute values of k that we obtain in this fashion are then called "the infinite (or Archimedean) primes" of the number field, and they do, in fact, "fill in the holes". Indeed, on a compact Riemann surface (and only on a compact surface!) one knows that the number of zeroes of a meromorphic function equals the number of poles. A multiplicative version of this for the number field k is the *product formula*, which states that the product of all absolute values (suitably normalized) of an element $x \neq 0$ equals 1; this is only possible when the infinite primes are included.

It is well-known that the topology of a compact Riemann surface is dictated by its genus defined as $1/2$ the number of 1-dimensional holes of the surface. The analogy with number fields suggests that these too should have a "genus", and one such was defined by A. Weil (see p. 214, [N1]).

There is one glaring difference between the field K of meromorphic functions on X and a number field k: Evaluating a function $f \in K$ at a point of X gives a mapping of K to $\mathbb{C} \cup \infty$; at a finite prime $\mathfrak{p}$ of k the same construction gives a map of k to $\mathbb{F}_\mathfrak{p} \cup \infty$ where $\mathbb{F}_\mathfrak{p}$ is a *finite field*. Thus the analogy between number fields and Riemann surfaces leads to an even stronger analogy between number fields and the function fields of smooth, projective, geometrically connected algebraic curves defined over some finite field $\mathbb{F}_q$ (e.g., [D1]); indeed, we still have the same geometric picture as for Riemann surfaces, but now we also have finite quotient fields! Both types of fields are termed *global fields*, and they are the basic elements of study of modern number theory.

For instance, the classical results of E. Artin and G. Whaples [AW1] show that global fields are characterized by the product formula and the finitude of the quotient fields. Let $\mathfrak{K}$ be a global field and let $\mathfrak{L}$ be obtained by adjoining the roots of an irreducible polynomial $p(t) \in \mathfrak{K}[t]$ which has simple roots (this is automatic for irreducible polynomials over a number field but *not* for function fields). The extension $\mathfrak{L}/\mathfrak{K}$ is said to be "Galois", and indeed one associates to $\mathfrak{L}/\mathfrak{K}$ a group G of permutations of these roots called the "Galois group". The Galois group acts precisely as the group of field-symmetries of $\mathfrak{L}/\mathfrak{K}$ in exact analogy with the topological case of coverings of Riemann surfaces. If $\mathfrak{p}$ is the absolute value of $\mathfrak{K}$ with an associated finite field, then, via the theory of finite fields, we can associate a canonical conjugacy class in G called the "Frobenius conjugacy class at $\mathfrak{p}$".

If the group G is abelian, then one has a very satisfactory description of $\{\mathfrak{L}, G\}$ called "class-field theory" [AT1], [Ro1]. For instance, one can use this to show that all abelian extensions of the rational numbers $\mathbb{Q}$ can be described by adjoining roots of unity to $\mathbb{Q}$; this is the famous *Kronecker-Weber Theorem*. Notice that the roots of unity are precisely the division-points of the exponential function; i.e., values of e^z at the points $\frac{n2\pi i}{m}$, integers n and $m \neq 0$. A similar description of abelian extensions also exists for fields obtained by adjoining the square root of a negative integer; here one uses the well-known analytic description of elliptic curves.

One calls the number of elements in the finite field at $\mathfrak{p}$ the norm of $\mathfrak{p}$ and writes it "$N\mathfrak{p}$". One then associates to $\mathfrak{K}$ the zeta-function

$$\zeta_{\mathfrak{K}}(s) := \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}\,, \tag{3}$$

which is obviously a massive generalization of Euler's equation (1). When $\mathfrak{p}$ is an Archimedean prime, one attaches a factor created from the Gamma-function. More generally, one attaches a similar product to systems of equations (varieties, etc.) over $\mathfrak{K}$. These complex functions have (or are conjectured to have) analytic continuations and functional equations in the fashion of $\zeta(s)$. All of these constructions can be put into a common formalism, due to E. Artin, using representations of the Galois groups G. To each conjugacy class one attaches a unique characteristic polynomial; these polynomials have (or, again, should have) integer coefficients, and they lead to analytic functions, called L-series, as in (3). One further expects, in a very precise way due to Langlands, that these L-series are attached to generalizations of modular forms called "automorphic representations".

The zeta-function of a global function field over the field $\mathbb{F}_q$ was also first defined by E. Artin [Ar1]. Remarkably, all such functions turn out to be of the form $R(q^{-s})$ where $R(u)$ is the quotient of two polynomials with integral coefficients. Thus these zeta-functions are algebraic in nature and can be handled via powerful algebraic techniques. In particular, the analog of the Riemann hypothesis was shown by A. Weil [We1] following H. Hasse. The corresponding Langlands Conjectures have just recently been established by L. Lafforgue [Laf1]. These function field results have had a continuing influence on the theory for number fields; see, for instance, [KS1].

Let $k = \mathfrak{K} = \mathbb{F}_q(T)$, $A = \mathbb{F}_q[T]$ and K the field of formal Laurent series in $1/T$ over $\mathbb{F}_q$. The field K has an absolute value on it inherited from the point ∞ on the projective line over $\mathbb{F}_q$ such that A is discrete and K/A is compact, exactly as $\mathbb{R}/\mathbb{Z}$ is isomorphic to a circle. In the 1930's L. Carlitz [Ca1] showed how one can develop a powerful analog of the exponential function in this situation. Here

is a brief summary of this construction; let ξ be a constant and put $L = A\xi$. Clearly, $L = \cup_m A(m)\xi$ where $A(m)$ is the (finite dimensional) $\mathbb{F}_q$-vector space of polynomials of degree $< m$. We associate to $A(m)\xi$ the polynomial in z defined by $e_\xi^{(m)}(z) := z \prod_{0 \neq \alpha \in A(m)} \left(1 - \frac{z}{\alpha\xi}\right)$. Classical results in algebra assure us that $e_\xi^{(m)}(z)$ is $\mathbb{F}_q$-*linear*; i.e., $e_\xi^{(m)}(\zeta_1 z_1 + \zeta_2 z_2) = \zeta_1 e_\xi^{(m)}(z_1) + \zeta_2 e_\xi^{(m)}(z_2)$ where $\{\zeta_1, \zeta_2\} \subseteq \mathbb{F}_q$.

The functions $e_\xi^{(m)}(z)$, $m = 1, 2, ...$, converge to a function $e_\xi(z)$ which is an entire (i.e., can be expressed as a power series in z which converges for all elements of K) $\mathbb{F}_q$-linear function. Carlitz shows that there is a specific $\xi = \xi_C$ which has the functional equation $e_{\xi_C}(Tz) = Te_{\xi_C}(z) + e_{\xi_C}(z)^q$. (More on the Carlitz exponential, which looks like e^z, below). In 1974 D. Hayes [H1] showed how to use the division values of $e_{\xi_C}(z)$ to obtain abelian extensions just as one uses e^z over the rational numbers.

By the 1970's non-Archimedean analysis (i.e., analysis over fields obtained by completing a global field at some discrete absolute value) had also progressed a great deal. In particular, due to the labors of J. Tate, R. Kiehl, and others, mathematicians had a good theory ("rigid analytic spaces") of global non-Archimedean analysis complete with analogs of Serre's famous G.A.G.A. theorems (comparing analytic and algebraic objects). Using this theory, in 1974 V.G. Drinfeld [Dr1] published a complete treatment of analytic functions like $e_{\xi_C}(z)$ but where one can use an arbitrary function field (over $\mathbb{F}_q$) $\mathfrak{K}$ and arbitrary rank "lattices". Thus Drinfeld obtains not only analogs of the classical exponential function but also analogs of those functions occurring in the analytic theory of elliptic curves and so on. Moreover, Drinfeld shows that these objects, now called "Drinfeld modules", can be parameterized by modular varieties which can also be described via rigid analysis and analogs of the classical upper half-plane. Drinfeld further constructed abelian extensions and established an important part of the two-dimensional form of Langlands' conjectures for global function fields. In [Go2], it is explained how Drinfeld modules lead to the shtuka used in Lafforgue's n-dimensional result.

The work of Carlitz, and more importantly Drinfeld, marked another change in our views on global fields and in particular global function fields. Here, for the first time, was an analytic theory of arithmetic objects (Drinfeld modules) very similar in nature to the classical theories of such great utility in algebraic number theory, together with a similar description of their moduli, *but* using analysis in finite characteristic. For instance one could construct on these spaces functions with transformation formulas quite similar to that of classical modular forms (see, for instance, [Go1]). Due to the recent work of G. Böckle [Boc2], [Go4] we now know that these functions give rise to L-series via "Hecke operators" just as with classical modular forms. Moreover, the standard formalism used to construct L-series mentioned above carries over very readily to Drinfeld modules, again leading to a theory of L-series [Boc1] and gamma functions [Th1], [ABP1] involving only finite characteristic analysis; an analog of Euler's formula on $\zeta(2n)$ is easily established in this context. While some general results are known about these functions and their zeroes [Wa1], [Go3], most of the general principles of the theory are still unknown. Indeed, there are many wide-open areas where even a good guess still remains out of reach.

Which brings us to the book by Michael Rosen. In it, one has an excellent (and, to the author's knowledge, unique) introduction to the global theory of function fields covering both the classical theory of Artin, Hasse, Weil *and* presenting an introduction to Drinfeld modules (in particular, the Carlitz module and its exponential). So the reader will find the basic material on function fields and their history (i.e., Weil differentials, the Riemann-Roch Theorem, etc.) leading up to Bombieri's proof of the Riemann hypothesis first established by Weil. In addition, one finds chapters on Artin's primitive root conjecture for function fields, Brumer-Stark theory, the ABC Conjecture, results on class numbers and so on. Each chapter contains a list of illuminating exercises. Rosen's book is perfect for graduate students, as well as other mathematicians fascinated by the amazing similarities between number fields and function fields.

References

[A1] G. Anderson: t-motives, *Duke Math. J.* **53** (1986) 457-502. MR **87j:**11042

[ABP1] G. Anderson, W. D. Brownawell, M. Papanikolas: Determination of the algebraic relations among special Γ-values in positive characteristic, *Ann. Math.* (to appear).

[Ar1] E. Artin: Quadratische Körper im Gebiete der höheren Kongruenzen I, II, *Math. Z.* **19** (1924) 153-246 (= *Coll. Papers*, 1-94).

[AT1] E. Artin, J. Tate: *Class Field Theory*, Benjamin, New York-Amsterdam (1968). MR **36:**6383

[AW1] E. Artin, G. Whaples: Axiomatic characterization of fields by the product formula for valuations, *Bull. Amer. Math. Soc.* **51** (1945) 469-492. MR **7:**111f

[Boc1] G. Böckle: Global L-functions over function fields, *Math. Ann.* **323** (2002) 737-795. MR **2003e:**11052

[Boc2] G. Böckle: An Eichler-Shimura isomorphism over function fields between Drinfeld modular forms and cohomology classes of crystals, Lecture Notes in Math. (to appear) (preprint, available at `http://www.math.ethz.ch/~boeckle/`).

[Ca1] L. Carlitz: On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1** (1935) 137-168.

[Co1] L. Corry: *Modern Algebra and the Rise of Mathematical Structures*, Birkhäuser, Basel (1996). MR **97i:**01023

[D1] R. Dedekind: Abriss einer Theorie höheren Congruenzen in Bezug auf einen reelen Rrimzahl-Modulus, *J. Reine Angew. Math.* **54** (1857) 1-26.

[DW1] R. Dedekind, H. Weber: Theorie der algebraischen Funktionen einer Verändlichen, *J. Reine Angew. Math* **92** (1882) 181-290.

[Di1] J. Dieudonné: *History of Algebraic Geometry*, Wadsworth, Monterey (1985). MR **86h:**01004

[Dr1] V.G. Drinfeld: Elliptic modules, *Math. Sbornik* **94** (1974) 594-627; English transl.: *Math. U.S.S.R. Sbornik* **23** (1976) 561-592. MR **52:**5580

[Dr2] V.G. Drinfeld: Elliptic modules II, *Math. U.S.S.R. Sbornik* **31** (1977) 159-170. MR **55:**12644

[Go1] D. Goss: The Algebraist's Upper Half Plane, *Bull. Amer. Math. Soc.* **2** No. 3 (May 1980) 391-415. MR **81g:**10042

[Go2] D. Goss: What is a shtuka? *Notices of the Amer. Math. Soc.* Vol. 50 No. 1 (2003) 36-37.

[Go3] D. Goss: The impact of the infinite primes on the Riemann hypothesis for characteristic p valued L-series, in: *Algebra, Arithmetic, and Geometry with Applications Papers from Shreeram S. Abhyankar's 70th Birthday Conference*, Springer (to appear).

[Go4] D. Goss: Can a Drinfeld module be modular? *J. Ramanujan Math. Soc.* **17** No. 4 (2002) 221-260.

[H1] D. Hayes: Explicit class field theory for rational function fields, *Trans Amer. Math. Soc.* **189** (1974) 77-91. MR **48:**8444

[KS1] N. Katz, P. Sarnak: Zeroes of zeta functions and symmetry, *Bull. Amer. Math. Soc. (N.S.)* **36** (1999) 1-26. MR **2000f:**11114

[Laf1] L. Lafforgue: Chtoucas de Drinfeld et correspondance de Langlands, *Invent. Math.* **147** (2002) 1-241. MR **2002m:**11039

[N1] J. Neukirch: *Algebraic Number Theory*, Springer, Berlin-Heidelberg-New York (1999). MR **2000m:**11104

[R1] B. Riemann: Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse, *Monatsberichte der Berliner Akademie* (1859); *Gesammelte Werke,* Teubner, Leipzig (1892).

[Ro1] P. Roquette: Class field theory in characteristic p, its origin and development. *Class field theory—its centenary and prospect* (Tokyo, 1998) Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo (2001). MR **2002g:**11156

[Th1] D. Thakur: Gamma functions for function fields and Drinfeld modules, *Ann. Math. (2)* **134** (1991) 25-64. MR **92g:**11058

[v1] B.L. van der Waerden: *A History of Algebra*, Springer, Berlin-Heidelberg-New York (1985). MR **87e:**01001

[Wa1] D. Wan: On the Riemann hypothesis for the characteristic p zeta function, *J. Number Theory* **58** (1996) 196-212. MR **97c:**11064

[We1] A. Weil: *Variétés Abéliennes et Courbes Algébriques*, Hermann (1971). MR **10:**621d

David Goss
The Ohio State University
E-mail address: goss@math.ohio-state.edu