BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 54, Number 4, October 2017, Pages 547–550
http://dx.doi.org/10.1090/bull/1590
Article electronically published on July 11, 2017

NUMBER THEORY IN THE 20TH CENTURY: PART 1

JOHN TATE

By "number theory" I mean algebraic number theory, and by Part 1, roughly the years 1900–1940. The treatment is very sketchy; I hope at some later date to cover the rest of the century and to fill in some of the gaps and correct any errors in this hasty account.

At the end of the 19th century, Kurt Hensel introduced the idea of the completion k_v of a field k with respect to a discrete valuation v and proved his famous lemma: If $\mathfrak{o}_v$ is the ring of integers in k_v and $f(t)$ is a monic polynomial with coefficients in $\mathfrak{o}_v$, a factorization of $f(t)$ into relatively prime factors modulo the maximal ideal of $\mathfrak{o}_v$ can be lifted to a factorization of $f(t)$.

At that time also, Hilbert, in his "Zahlbericht", reinterpreted the quadratic reciprocity law as a product formula for his norm residue symbol. This product formula has been generalized to the higher K groups by Dustin Clausen.

Let k be a number field, i.e., a field of finite degree over $\mathbf{Q}$. Let $\mathfrak{m}$ be an ideal in the ring of integers $\mathfrak{o}_k$ of k, let $I_\mathfrak{m}$ be the group of fractional ideals prime to $\mathfrak{m}$, and let $P_\mathfrak{m}$ be the group of principal ideals (α) of elements α which are congruent to 1 mod $\mathfrak{m}$ and positive at every real place. In the late 1800s Heinrich Weber had the idea that there should exist an abelian extension K of k such that the prime ideals of k which split completely in K are those in $P_\mathfrak{m}$, and the Galois group $\mathrm{Gal}(K/k)$ is isomorphic to $I_\mathfrak{m}/P_\mathfrak{m}$. He called such an extension K or any subextension of it a *class field* over k. In 1907 Furtwängler showed the existence of such an extension in case $\mathfrak{m} = 1$, the so-called "Hilbert class field". Near the end of the First World War, great progress was made by Teiji Takagi. He showed the existence of a class field for every $\mathfrak{m}$ and that every abelian extension is a class field.

A *character* of k defined mod $\mathfrak{m}$ is a nonzero multiplicative map $\chi : I_\mathfrak{m} \to \mathbf{C}^*$ which is trivial on $P_\mathfrak{m}$. To such a χ, Richard Dedekind associated an "L-series"

$$L(s,\chi) := \sum_\mathfrak{a} \chi(\mathfrak{a})\mathbf{N}\mathfrak{a}^{-s} = \prod_\mathfrak{p} (1 - \chi(\mathfrak{p})\mathbf{N}\mathfrak{p}^{-s})^{-1},$$

the sum being over all integral ideals $\mathfrak{a}$ prime to $\mathfrak{m}$ and the product over the prime ideals not dividing $\mathfrak{m}$, the equality of the two resulting from the unique factorization of ideals into primes. The sum and product converge in the right half-plane $\mathrm{Re}(s) > 1$. In case $\chi = 1$ and $\mathfrak{m} = \mathfrak{o}$ is the full ring of integers in k, this function is called the zeta function of k and is written $\zeta(s) := L(s,1)$. Earlier, in the case $k = \mathbf{Q}$, Dirichlet had used the L-functions to prove his theorem on primes in arithmetic progressions, and Riemann had guessed that $\zeta(s)$ has no zero in the half-plane $\mathrm{Re}(s) > 1/2$, the famous "Riemann hypothesis". One expects the same should hold for all L-functions $L(s,\chi)$.

Received by the editors June 21, 2017.
2010 *Mathematics Subject Classification.* Primary 11Rxx, 11Sxx.

©2017 American Mathematical Society

In 1917 Erich Hecke showed that for all k and all χ the function $L(s,\chi)$ has an analytic continuation to the whole complex s-plane with a simple pole at $s=1$ its only singularity, and it satisfies a simple functional equation relating its value at s to that at $1-s$. He did this not only for L-series $L(s,\chi)$ made with Dedekind's χ, but also those made with a more general kind of multiplicative function χ of ideals which Hecke called a "Grössencharakter" because it varied continuously and was in general of infinite order.

Today we view the group of characters χ of Dedekind and Hecke as the character group of the group C_k of idele classes of our number field k, Dedekind's χ being those of finite order and Hecke's those which are nontrivial on the connected component of C_k.

In 1922 Louis Mordell, an American mathematician who had gone to Cambridge, England, for his PhD and settled in that country, proved that an idea which had earlier occurred to Henri Poincaré was true, namely, that the group $E(\mathbf{Q})$ of rational points on an elliptic curve E defined over $\mathbf{Q}$ is finitely generated. He also conjectured that the set of rational points on a curve of genus >1 is finite. This was proved 60 years later by Gerd Faltings.

Emil Artin got his PhD in Leipzig under Gustav Herglotz in 1921. After a postdoc year in Göttingen, he accepted an offer from Hamburg university, where he spent the next 15 years. In 1923 he introduced a new kind of L-series, associated to a character the Galois group $G=\mathrm{Gal}(K/k)$ of a finite Galois extension K/k of number fields. To explain this, we must recall the key notion of Frobenius automorphism $\mathrm{Frob}_{K/k}(\mathfrak{p})$ associated to a prime ideal $\mathfrak{p}$ of k which is unramified in K. It is an element in $\mathrm{Gal}(K/k)$ which leaves a prime $\mathfrak{P}$ above $\mathfrak{p}$ fixed and acts as raising to the $\mathbf{N}\mathfrak{p}$ power on the residue field $O_K/\mathfrak{P}$ of $\mathfrak{P}$, where $\mathbf{N}\mathfrak{p}$ is the number of elements in the residue class field $O_k/\mathfrak{p}$. Such an element exists, and its conjugacy class depends only on $\mathfrak{p}$. Thus it makes sense to define, for a complex linear representation $\rho: G\to \mathrm{GL}_n(\mathbf{C})$,

$$L(s,\rho,K/k)=\prod_{\mathfrak{p}}\det(I_n-\rho(\mathrm{Frob}_{K/k}\mathfrak{p})\mathbf{N}\mathfrak{p}^{-s}),$$

the product being over all prime ideals $\mathfrak{p}$ of k which are unramified in K. Artin was led to this definition by his investigation of the interrelationships among the Dedekind zeta functions and L-functions of the intermediate fields in a Galois extension. In many cases in which k contains an nth root of unity and $K=k(\alpha^{1/n})$ for some $\alpha\in k$, a classical nth-power reciprocity law showed that Artin's L-function made with a character of the cyclic Galois group coincided with a Dedekind L-function made with a character of the corresponding ideal class group. Artin conjectured that this would be true in general. This meant simply that in the notation above, the isomorphism of $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ with the Galois group of the corresponding class field, which Takagi had proved by showing that they were each products of cyclic groups of the same order, was canonical, associating to each prime ideal $\mathfrak{p}$ not dividing $\mathfrak{m}$ its Frobenius automorphism $\mathrm{Frob}_{K/k}(\mathfrak{p})$. Thus for each $(\alpha)\in P_{\mathfrak{m}}$, we should have $\prod_{\mathfrak{p}}\mathrm{Frob}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(\alpha)}=1$. Artin conjectured this in 1923 and called it the general reciprocity law, noting that, in contrast to all previous such laws, its statement involved no roots of unity He was convinced of its truth, but had no proof.

In 1925, Chebotarev proved his famous density theorem: Let K/k be a Galois extension of number fields, let $G=\mathrm{Gal}(K/k)$, and let C be a conjugacy class in

G. Then the density of the set of primes $\mathfrak{p}$ in O_k such that $\mathrm{Frob}_{K/k}(\mathfrak{p})$ lies in C is proportional to the size of C; in particular the set of $\mathfrak{p}$ which split completely in O_K is $1/n$, where $n = [K : k]$ is the degree of K over k. Chebotarev's theorem is a vast generalization of Dirichlet's theorem on primes in arithmetic progressions.

In 1927, Artin was able finally to prove his reciprocity law by using Chebotarev's method of crossing a given abelian extension with a suitable cyclotomic extension. A key feature of Artin's "non abelian" L-functions is that for a subextension $k \subset E \subset K$ and a representation χ of $\mathrm{Gal}(E/K)$, the L-function of the induced representation $\mathrm{Ind}(\chi)$ of $\mathrm{Gal}(K/k)$ is the same as the L-function of χ. By showing that every character of a finite group is a rational linear combination of characters induced from one-dimensional characters, Artin proved that some power of any one of his non-abelian L-functions is meromorphic, being a quotient of products of Dirichlet L-functions. Later, in 1947, Richard Brauer proved that the "rational" in the previous sentence could be replaced by "integral", hence the L-functions themselves are meromorphic. Artin conjectured that for a character not involving the trivial character they are holomorphic. I believe this is still unproven.

In the early 1930s, Richard Brauer, Helmut Hasse, and Emmy Noether showed that a central simple algebra A over a number field k was determined up to isomorphism by its localizations A_v at the various places v of k, and they were able to determine the structure of the Brauer groups $\mathrm{Br}(k)$ and $\mathrm{Br}(k_v)$ of classes of central simple algebras over a global field k and and its localizations k_v. The "Hasse invariant" map $\mathrm{inv}_v : \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z}$ is injective for every place v of k, surjective for non-archimedean v, with image of order 2 for real v and 0 for almost all v and for complex v. They proved that the sequence $0 \to \mathrm{Br}(k) \to \sum_v \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z} \to 0$, where the third arrow is given by the sum of the Hasse invariants, is exact.

Let $\mathbf{F}_q$ be a finite field with q elements. In his PhD thesis, Artin considered quadratic extensions of the field of rational functions $\mathbf{F}_q(t)$ and proved for them the analogue of the standard theory of quadratic extensions of the field of rational numbers. For such a function field the zeta function is a computable rational function of $t = q^{-s}$. Hence the analogue of the Riemann hypothesis, that its zeros are all on the line $\mathrm{Re}(s) = 1/2$ (i.e., $|t| = q^{-1/2}$) is possible to check. Artin did the check in about 40 special cases with $q = 3,\ 5,$ and 7, and naturally conjectured that it would be true in general.

In the mid-1930s Hasse proved this conjecture in case the quadratic extension is of genus 1, that is, is of the form $\mathbf{F}_q(t)(\sqrt{P(t)})$, where $P(t)$ is a polynomial of degree 3 or 4, using the endomorphisms of the elliptic curve $y^2 = P(t)$. In 1940, André Weil proved the analogue of the Riemann hypothesis for all function fields in one variable over a finite field, by using the positivity of the trace in the correspondence ring of the curve with that function field.

In the early 1930s, Claude Chevalley developed local class field theory independently of the global theory which had been used by Hasse for that purpose. Later he defined the *idele group* $J = J_k$ of k as the restricted product of the multiplicative groups k_v^* of the completions k_v of k over all places of k, relative to the groups of units $\mathfrak{o}_v^*$. One makes J into a locally compact topological group in which, for every finite set S of places v of k containing the ones where K_v is isomorphic to $\mathbf{R}$ or $\mathbf{C}$, the subgroup $J_S := \prod_{v \in S} k_v^* \times \prod_{v \notin S} \mathfrak{o}_v{}^*$ is open, with the product topology. By "restricted product" above, we mean simply that J is the union over all finite sets S as above of the subgroups J_S. Thus an element of J (i.e., an "idele") is simply

an infinite vector $a = (\ldots, a_v, \ldots)$ with one component $a_v \in k_v^*$ for each place v of k, such that a_v is a unit in $(o)_v$ for almost all v. One identifies k^* with a discrete subgroup of J in the obvious way, putting $\alpha = (\ldots, \alpha_v, \ldots)$, where α_v is the image of α under the canonical imbedding of k in its completion k_v. The quotient group $C = C_k := J/k^*$ is the group of *idele classes* of k. The map $a \mapsto (a) := \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$ is a homomorphism of J onto the group I of ideals. For a given integral ideal m, we get, in the notation near the beginning of this opus, a surjection $C \to I_{\mathfrak{m}}/P_{\mathfrak{m}}$ as follows. For an idele a, we choose an element $\alpha \in k^*$ such that a/α is positive at the real places and congruent to 1 mod $\mathfrak{m}$. Then we map the class of an idele a to the element of $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ represented by the quotient of their ideals $(a)/(\alpha)$. In this way we can interpret Hecke's Grössencharakters simply as the characters of the group C of idele classes, and Artin's reciprocity law homomorphisms as an isomorphism of C mod its connected component with the Galois group of the maximal abelian extension of k.

Department of Mathematics, University of Texas at Austin, Austin, Texas