Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 20 (1974)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: TWO LECTURES ON NUMBER THEORY, PAST AND PRESENT
Autor: Weil, André
Kapitel: Second Lecture
DOI: https://doi.org/10.5169/seals-46896

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 28.11.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

gations, which he did not publish, and then with Jacobi and more or less simultaneously with Abel in their famous work on elliptic functions, the two theories are brought together. This was a necessary development, and in many essentials brings us where we are today, because today what we are doing is to elaborate on those various trends, pushing them further, but always trying to keep in mind their mutual relationships.

Second Lecture

In Bourbaki's historical note on the calculus, it is said that the history of mathematics should proceed in the same way as the musical analysis of a symphony. There are a number of themes. You can more or less see when a given theme occurs for the first time. Then it gets mixed up with the other themes, and the art of the composer consists in handling them all simultaneously. Sometimes the violin plays one theme, the flute plays another, then they exchange, and this goes on.

The history of mathematics is just the same. You have a number of themes; for instance, the zeta-function; you can state exactly when and where this one started, namely with Euler in the years 1730 to 1750, as we saw yesterday. Then it goes on and eventually gets inextricably mixed up with the other themes. It would take a long volume to disentangle the whole story.

I will now spend some time discussing this particular theme, the zeta-function and its functional equation. As we saw yesterday, this equation was stated and partly proved by Euler as early as 1749. His proof consisted in calculating $\zeta(n)$ for all even integers $\geqq 2$, and, for all integers $n > 0$, the alternating sum $1 - 2^n + 3^n - \ldots$ What does that mean? Euler has of course a reputation for his supposedly reckless handling of divergent series. But no one who in his life has done so many numerical calculations with series as Euler can fail to make the difference between convergence and divergence; or perhaps it would be more correct to say that the distinction is between calculably convergent series and the others; from this point of view, $\zeta(n)$ is practically as bad for $n > 1$ as for $n < 0$; in both cases, it has to be transformed into something else that lends itself to numerical calculation. Actually, whenever Euler discusses a divergent series, he says exactly what he means; the only thing with which one could quarrel (and with which his contemporaries did quarrel) was his view that all "reasonable" methods of summation for a divergent series must lead to the same result;

this is of course meaningless as long as you cannot formulate a criterion for "reasonableness," and Euler had no such criterion, only an extensive experience with such matters and a good intuitive feeling. In the case of the series $1 - 2^n + 3^n - \ldots$, he uses what we call Abel summation; he takes the power-series

$$F(x) = x - 2^n x^2 + 3^n x^3 - \ldots;$$

he finds that it represents a rational function, and then takes its value for $x = 1$. This he is able to do by using the so-called Euler-Maclaurin summation formula, which is what brings in the Bernoulli numbers. If you go back to his original publication, you find that he did apply that formula in a rather reckless fashion; later on he gave more satisfactory procedures. But his instinct was perfectly sound.

Euler did not stop at the zeta-function; he also considered several series of the form $\Sigma\, c(n) \,.\, n^{-s}$, where $c(n)$ depends only upon the value of n modulo N for some small value of N. But this topic does not appear to have been pursued further before Dirichlet, in the 1830's, took it up and recognized in such series a major tool for number-theoretic investigations—an accomplishment which appropriately conferred upon them the name of "Dirichlet series," even though Dirichlet himself very properly acknowledges his debt to Euler.

Dirichlet introduced both L-series over the rational numbers, such as

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where χ is a character (the essential thing at the moment is that χ as a function of n is periodic, i.e. $\chi(n+a) = \chi(n)$ for all n and some a) and also series of the form

$$\sum_{m,n} \frac{1}{(am^2 + bmn + cn^2)^s}$$

where a, b, and c are integers. These we would now classify as zeta-functions and L-series belonging to quadratic number fields. This second series involves a quadratic form and we know—indeed already Dirichlet knew, not clearly, but in a general way—that the theory of binary quadratic forms (expressions like $a\,m^2 + b\,m\,n + c\,n^2$, where m, n are indeterminates and a, b, c are integers) is essentially equivalent with what we call the theory of quadratic number-fields.

The next episodes in our story belong to analysis rather than number-theory, but they have to be mentioned here. It is amusing to note that, in 1849, there were two entirely independent publications by two very respectable mathematicians, both giving the functional equation of the L-series

$$1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots .$$

One of them, Schlömilch, published it as an exercise for advanced students in the *Archiv der Mathematik und Physik*; the other, Malmquist, included it, also without proof, in a paper in *Crelle's Journal*, and added similar statements for two other such series, with the remark that "he seemed to remember having seen something of that kind in Euler." Of course, if $L(s)$ is the above series, both $L(s)$ and $L(1-s)$ are convergent (though not absolutely) in the critical strip, and the statement was made only for that strip, so that the question of analytic continuation did not arise. In 1858, a professor in Dorpat, Clausen, sent to the *Archiv* a solution of Schlömilch's "exercise," done in orthodox fashion by using Cauchy's calculus of residues. Clearly they all regarded such matters as routine.

From our point of view, the case of Riemann is more curious. Of all the great mathematicians of the last century, he is outstanding for many things, but also, strangely enough, for his complete lack of interest for number-theory and algebra. This is really striking, when one reflects how close he was, as a student, to Dirichlet and Eisenstein, and, at a later period, also to Gauss and to Dedekind who became his most intimate friend. During Riemann's student days in Berlin, Eisenstein tried (not without some success, he fancied) to attract him to number-theory. In 1855, Dedekind was lecturing in Göttingen on Galois theory, and one might think that Riemann, interested as he was in algebraic functions, might have paid some attention. But there is not the slightest indication that he ever gave any serious thought to such matters. It is clearly as an analyst that he took up the zeta-function. Perhaps his attention had been drawn to the papers of Schlömilch and Malmquist in 1849, and of Clausen in 1858. Anyway, to him the analytic continuation of the zeta-function and its functional equation may well have seemed a matter of routine; what really interested him was the connection with the prime number theorem, and those aspects which we now classify as "analytic number-theory," which to me, as I have told you, is not number-theory at all. Nevertheless, there are two aspects of his famous 1859 paper on the zeta-function which are of vital importance to us here.

In the first place, he gives two proofs for the functional equation, and it is his second proof which concerns us now; this is the proof which connects the zeta-function, by means of what we call now the "Mellin transformation," with the function

$$f(q) = q + q^4 + q^9 + \dots .$$

We have seen that Euler had already considered $f(q)$, but merely as a formal power-series. As Riemann observes, this, or rather the function $2f(q) + 1$, is essentially Jacobi's theta-function. With this, a new "musical theme" enters into our symphony, a theme to which the work of Hecke on modular forms has given great prominence, and which is now very familiar to all those who are working in that field.

Just as the functional equation for $\zeta(s)$ relates the values of ζ at s and at $1 - s$, the theta-function has a functional equation relating its values at $q = e^{2\pi i\tau}$ and at $q' = e^{-2\pi i/\tau}$, and Riemann found that the former is a direct consequence of the latter. The equation for the theta-function had already been found by Gauss, as we know from his private papers; but he had never published it. It came out for the first time in Jacobi's work on elliptic functions, where the theta-function is an essential ingredient; Jacobi gave it more and more prominence in his later treatment of that topic, and Riemann must have been very familiar with it, not only from Jacobi's *Fundamenta*, but also from Eisenstein's lectures on elliptic functions which he heard during his first year as a student in Berlin. Here we may note that Jacobi was primarily an analyst but also deeply interested in number-theory, and that he used his theta-function for a proof of Fermat's theorem on sums of four squares, precisely as Euler had predicted almost a hundred years before.

But perhaps Riemann's main contribution to number-theory consisted in drawing attention to what we call the Riemann hypothesis. Here I may point out that in the old days, when one used the word "hypothesis" or "conjecture" (in German, *Vermutung*), this was not to be taken as simply a form of wishful thinking. Nowadays these two are often confused. For instance, the so-called "Mordell conjecture" on Diophantine equations says that a curve of genus at least two with rational coefficients has at most finitely many rational points. It would be nice if this were so, and I would rather bet for it than against it. But it is no more than wishful thinking because there is not a shred of evidence for it, and also none against it. In the old days, the word conjecture was reserved (and I suggest that it might

still be usefully reserved) for the case when there is some reasonably convincing evidence. For instance, when Euler first made the statement

$$\prod_n (1-q^n) = \sum (-1)^n q^{\frac{n(3n+1)}{2}}$$

that I quoted yesterday, he had calculated a very large number of terms, and reasonably regarded this as good evidence.

Similarly, when Riemann conjectured the Riemann hypothesis, he had much more up his sleeve than is proved in his paper; he knew, not only that there are infinitely many zeros of the zeta function on the straight line $Re(s) = \frac{1}{2}$, but that in some sense most of them are there; this was later disengaged from his private papers by Siegel (see Siegel's *Collected Works*, vol. I, no. 18).

I repeat that Riemann's interest was purely analytical, and he and some of his successors (for instance, Hadamard and de la Vallée Poussin) regarded this as a problem in analysis. In retrospect, it is clear to us that it is not so. Somehow, in some way that we cannot explain, the Riemann hypothesis expresses truly number-theoretical properties of algebraic number fields. The reason for this view lies essentially in the analogy with function fields over finite fields where the Riemann hypothesis has been proved and where it is an essentially arithmetical, although partly algebraic-geometric property.

After Riemann, the next major step was to introduce zeta-functions for arbitrary algebraic number-fields; this was done by Dedekind. Dedekind fully realized the value of these functions for the theory of algebraic number-fields. He found their Euler product as a direct consequence of his ideal theory, and he found their relation with the number of ideal-classes. There he had the work of Dirichlet to guide him, and, just as Dirichlet, he made no attempt to get the analytic continuation of his zeta-functions. It was enough for him that the series was obviously convergent for $Re(s) > 1$ and that its behavior for s tending to 1 is decisive for the calculation of the class number. The analytic continuation was carried out much later by Hecke.

With this, however, we have already entered into the theory of algebraic number-fields, whose history cannot be separated from that of quadratic forms and from the laws of reciprocity; new themes have come into play. Therefore we must now go back two centuries, and make a fresh start with Fermat.

Fermat grouped his number-theoretical investigations chiefly around two problems. One was the study of diophantine equations of genus one, for instance the famous equations $z^2 = x^4 - y^4$ and $z^3 = x^3 - y^3$. The

other was: given N, what are the integers, and particularly what are the primes, which can be written in the form $x^2 \pm N y^2$? He solved the problem to his full satisfaction for the forms $x^2 + y^2$, $x^2 + 3y^2$, $x^2 \pm 2y^2$. For instance, he found that a prime can be written as $x^2 + 3y^2$ if and only if it is congruent to 1 modulo 3. But, when he came to investigate the form $x^2 + 5y^2$, he found something that greatly puzzled him, and which he states as follows. Firstly, the possibility of p being of this form depends upon the residue of the prime p, not merely modulo 5, but modulo 20. To us this is clear, because $x^2 + 5y^2$ depends upon the quadratic number field $Q(\sqrt{-5})$, and since -5 is congruent to -1 modulo 4, the discriminant of the field is -20. To Fermat this may already have come as a slight surprise. But what really puzzled him was the following fact which he discovered empirically—that is to say, by numerical experimentation. Of course, for trivial congruence reasons, no prime which is congruent to 3 or to 7 modulo 20 can be of the form $x^2 + 5y^2$; nevertheless, as Fermat observed empirically but could not prove, the product of two such primes, or the square of such a prime, can always be written as $x^2 + 5y^2$.

This is very characteristic in the history of mathematics. When there is something that is really puzzling and cannot be understood, it usually deserves the closest attention because some time or other some big theory will emerge from it. In fact, we would explain the above phenomenon like this. In the number-field $Q(\sqrt{-5})$, there are two ideal classes; Hilbert's classfield over it is the biquadratic field $Q(i, \sqrt{-5})$, contained in the field generated by the 20th roots of unity. Luckily, this is abelian over the rational field. Therefore, the behavior of a prime p in the field $Q(\sqrt{-5})$, including the class to which its ideal prime factors belong if it does split in that field, depends only upon the residue of p modulo 20. Consequently, if p is congruent to 1 or 9 modulo 20, it can be written as $x^2 + 5y^2$; if it is congruent to 3 or 7, it can be represented by the other form of discriminant 20, that is by $2x^2 + 2xy + 3y^2$, but the product of any two such primes can be written as $x^2 + 5y^2$; in all other cases no such representation is possible. All this can also be expressed in the language of the classes and genera of quadratic forms, as Gauss would have done, but to us that language is less illuminating.

Coming back to Fermat's problem, however, there is an obvious necessary condition for the prime p to be of the form $x^2 \mp N y^2$; it is that p should be a "divisor" of that form, i.e. that p should divide $x^2 \mp N y^2$ for suitable values of x, y, not both multiples of p. This, as we know, is a much

simpler question; it just means that $\pm N$ must be congruent to a square: $\pm N \equiv (x/y)^2$ modulo p. That is, $\pm N$ is what already Euler started calling a quadratic residue for the prime p. For a given p, it is easy (for instance, by complete enumeration of the integers modulo p) to find out which are the quadratic residues.

But the serious problem comes when you ask what are the primes for which a given $\pm N$ is a quadratic residue. Numerical experimentation indicates that those primes arrange themselves into a number of arithmetic progressions, either modulo N or modulo $4N$, as the case may be.

This fact was empirically discovered by Euler after many years of thinking about such questions; he published it in his late work. Of course, once the problem had been clearly stated, it did not really take an Euler to find the answer by numerical experimentation. Legendre, who gave the first clear formulation of the law of quadratic reciprocity in 1785, was apparently not aware that Euler had already found it. Even Gauss seems to have missed that statement in Euler's paper; perhaps this was because it did not matter to him; he had not only found it but fully proved it; moreover, the statement was in Legendre, and Legendre had given a partial proof. It is surprising, in a way, that Euler, who had worked at it all his life, and was such a strong mathematician, did not prove it. Anyway, the first proof was completed by Gauss on the 8th of April 1796, just before his 19th birthday, and it is rightly regarded as one of his great achievements. With it, we have another main theme for our symphony; also in this, as you see, Euler had had a big share.

Gauss alone, however, was responsible for the next development, the law of biquadratic reciprocity. Very early he started thinking about the extension of the quadratic reciprocity law to cubic and biquadratic residues, and then he noticed that such laws cannot even be properly conjectured within the context of rational numbers; they require the fields of cubic roots and of fourth roots of unity. As I pointed out yesterday, already Euler had complimented Lagrange on his bold use of irrational "and even imaginary" numbers in number-theoretical questions; they had both seen, for instance, that numbers of the form $x + y\sqrt{-N}$, where x and y are ordinary integers, are of great value in discussing the form $x^2 + Ny^2$. Gauss undoubtedly knew this; but, in his published work, he never went so far; he only introduced the Gaussian integers $x + y\sqrt{-1}$ in his great work on biquadratic residues. In connection with this, I shall allow myself a digression to tell a personal anecdote.

In 1947, in Chicago, I felt bored and depressed, and, not knowing what to do, I started reading Gauss's two memoirs on biquadratic residues, which I had never read before. The Gaussian integers occur in the second paper. The first one deals essentially with the number of solutions of equations $a\,x^4 - b\,y^4 = 1$ in the prime field modulo p, and with the connection between these and certain Gaussian sums; actually the method is exactly the same that is applied in the last section of the *Disquisitiones* to the Gaussian sums of order 3 and the equations $a\,x^3 - b\,y^3 = 1$. Then I noticed that similar principles can be applied to all equations of the form $a\,x^m + b\,y^n + c\,z^r + \ldots = 0$, and that this implies the truth of the so-called "Riemann hypothesis" (of which more later) for all curves $a\,x^n + b\,y^n + c\,z^n = 0$ over finite fields, and also a "generalized Riemann hypothesis" for varieties in projective space with a "diagonal" equation $\sum a_i x_i^n = 0$. This led me in turn to conjectures about varieties over finite fields, some of which have been proved later by Dwork, Grothendieck, M. Artin and Lubkin, and some of which are still open.

In this same connection, I may also mention in passing some biographical puzzles. In the very last entry in his diary, in 1814, Gauss makes a statement about the number of solutions of $1 = x^2 + y^2 + x^2\,y^2$ in the prime field modulo p, which is equivalent to the "Riemann hypothesis" for that curve; he says he has discovered this "by induction" (i.e. empirically). If we put $z = y\,(1+x^2)$, we get $z^2 = 1 - x^4$, so that the curve can be treated easily by the method of his first paper on biquadratic residues. Surely he must have noticed this, since otherwise he would not have added that "this connects beautifully the lemniscatic functions with biquadratic residues"; but neither Dedekind nor Bachmann could see the connection. It is also puzzling to find him writing in that diary, in 1813, that he had finally mastered the theory of biquadratic residues "after almost seven years of concentrated efforts" (and "on the same day when his second son was born"; clearly he regards the former event as much more important) and then to find that he had already said the same in a letter to Sophie Germain in 1807 (dated "the day of my 30th birthday"). Does that mean that in 1807 he had discovered the main facts, but that he found the proofs only much later? In his second memoir on the subject, he still describes those results as a "most recondite mystery" and postpones the proofs to a later occasion; but, not long after that, Jacobi had the audacity of sending him a brilliant and rather short proof, and this may have discouraged Gauss from ever publishing his own.

Before we go on, however, with the reciprocity laws, we must say more about the appearance of algebraic number-fields. We have seen how Euler

and Lagrange started using algebraic numbers. As we have said, Gauss must have been aware of the relation between binary quadratic forms and quadratic fields. To have introduced the group of classes of binary quadratic forms of given discriminant had been Gauss's specific contribution (the concept of classes, and the finiteness of the class-number, had been discovered by Lagrange and further exploited by Legendre); but this did not immediately influence the study of quadratic fields; of course, in the case of the Gaussian integers, the class number is 1. On the other hand, Dirichlet proved (and Hermite almost proved) the theorem on the units in a ring of algebraic integers. But even Dirichlet and Eisenstein did not see how to circumvent the basic difficulty in the multiplicative theory of algebraic numbers, which we express by saying that the class-number need not be 1; it was left for Kummer, by a stroke of genius, to solve it once for all with his "ideal factors." This happened in 1845, and we can follow the story in detail in Kummer's letters to his former pupil Kronecker.

Actually what Kummer did was to determine explicitly all the valuations in the cyclotomic field $Q(\varepsilon)$, where ε is a primitive root of unity of prime order l; thus, he was at the same time determining the prime ideal decomposition of rational primes in that field. He extended this later to fields $Q(\varepsilon)$ where ε is a primitive n-th root of unity, and in part to the "Kummer fields" $Q(\varepsilon, \xi^{1/n})$ where ξ is in $Q(\varepsilon)$; for $n = 2$, this includes the quadratic fields. He applied this to Fermat's theorem, not that he attached any great importance to it, but, just like Gauss, he regarded it as a good testing ground for the theory of cyclotomic fields. But he and Eisenstein also used that theory extensively in their work on the higher reciprocity laws, where quite possibly there are valuable ideas which have not yet been fully exploited; the same can perhaps also be said of the connections discovered by Eisenstein between elliptic functions and the cubic and biquadratic reciprocity laws.

Eisenstein died very young. Kummer never bothered about the extension of ideal theory to all algebraic number-fields; he was quite willing to leave this to others, and it was done by Dedekind and by Kronecker.

Now, since our time is so limited, we must take a big jump, right into the present century, and we come to Artin and to what he did with two of our main themes, the zeta-function and the reciprocity laws. Already Hilbert had realized that all reciprocity laws had to do with abelian extensions of algebraic number-fields; this, of course, was based on the concept of the Galois group, and Kronecker had made essential contributions to the subject. Hilbert conjectured many of the basic facts about abelian extensions of number-fields; he proved some, and Furtwängler and Takagi proved the

others. But the edifice still lacked a roof until Artin conjectured and then proved his law of reciprocity, one main part of which can be explained as follows. Let K be an abelian extension of degree n of a number-field k; let $Z(s)$ be the Dedekind zeta-function for K; then $Z(s)$ can be split into n factors which are L-functions attached to k. Such L-functions, which were first defined by H. Weber in 1897, are the direct generalization of those which had been introduced earlier by Dirichlet, and Hecke's proof for the functional equation of the zeta-function is also valid for them.

Most of you will not see the connection between this and the original law of quadratic reciprocity of Euler, Legendre and Gauss; even Gauss might not have seen it at once, but perhaps Dirichlet would. Nevertheless—here you have to take me on trust—there is a straight line, a clear line, connecting one with the other.

Here, at the hands of a great artist, two themes have been so fused together that only a careful analysis can separate them. But I must not fail to mention another development, also due to Artin. Dedekind and Weber, taking as their model Dedekind's theory of the algebraic number-fields, had treated the fields of algebraic functions of one variable over the prime field modulo p; this can be regarded as the theory of the congruences $F(x,y) \equiv 0$ modulo p, where F is any polynomial with integral coefficients. There is no difficulty in extending this to algebraic curves over all finite fields. Artin, in his thesis, showed how Dedekind's definition of the zeta-function for an algebraic number-field can be applied to such function-fields. To him, the new zeta-functions looked almost as mysterious as Dedekind's, although he had found that they were rational functions of p^{-s}; in particular, he saw no reason for hoping that the Riemann hypothesis for them would be easier to prove than the classical one. Nevertheless, this was done less than 25 years later, by a combination of number-theory and algebraic geometry. As we have noted above, the conjecture or theorem in Gauss's last entry in his diary is just a special case of this result; on the other hand, its extension to algebraic varieties is still an unsolved problem.

Here we have already reached our present front-line at one of its most sensitive points. Now let us go back to Gauss for a minute, and to his theory of binary quadratic forms. Looking at this as being, in essence, a theory of quadratic fields, we saw it develop into the theory of all algebraic number-fields. On the other hand, already Gauss took up another generalization, to quadratic forms in any number of variables; this line was pursued after him, for instance, by Hermite, Eisenstein, H. Smith, Minkowski, and more recently Siegel. From a modern point of view, this is the arithmetical

theory of the orthogonal groups, while the theory of algebraic number-fields may be regarded as dealing with another kind of group, namely the so-called algebraic toruses; the latter point of view was already quite apparent in the work of Dirichlet and of Hermite on the units of those fields. All this can be subsumed now under one catchword: the arithmetical theory of algebraic groups (in particular, the so-called reductive groups).

With this we have again come so close to the present day that I can at least point out to you two of the most promising lines of advance. As we said, Artin's reciprocity law, which in a sense contains all previously known laws of reciprocity as special cases, deals with a strictly commutative problem. It establishes a relation between the most general extension of a number-field with a commutative Galois group on the one hand, and on the other hand the multiplicative group over that field. Where do we go from there? Well—of course we take up the non-commutative case.

In modern notation, the multiplicative group in one variable is called $GL(1)$. Leibniz would not have regarded this group as trivial, since a good deal of his work was concerned with the exponential and logarithmic functions; the same may be said about Euler; but perhaps many later writers would have looked at it with contempt. Nevertheless, there is a sense in which classfield theory and Artin's law of reciprocity are nothing but the theory of $GL(1)$ over a number-field, and now we are up against the problem of dealing with $GL(n)$ in a comparable sense. This is a huge problem; it is only quite recently that Jacquet and Langlands, for instance, have made some inroad into the study of $GL(2)$; their work indicates that there is a definite connection with Artin's non-abelian L-functions, so that the theme of the zeta-function appears here once more, and once more in some counterpoint with the reciprocity laws. Perhaps even the Riemann hypothesis will play a role here in some mysterious way.

But for a while now I have abandoned the theme of elliptic functions, modular functions and curves of genus 1, although it never really vanished out of sight; Eisenstein, Kronecker, H. Weber took good care to keep it going, and so did Fueter and Hasse more recently, in connection with complex multiplication and with the Riemann hypothesis in elliptic function-fields. But above all Hecke took up the subject of modular functions and put it back into number-theory where it always belonged, after Poincaré and Klein had vainly tried to push it into function-theory (of course Poincaré was too good a mathematician not to know that it had also its arithmetical aspects, and he wrote a paper entitled *L'arithmétique et les fonctions fuchsiennes* which is still worth reading). In a sense, this is again the theory

of $GL(2)$, but seen from a rather different angle; here, too, Dirichlet series and generalizations of the old laws of reciprocity play a prominent role. This is not the time to give details, but I may refer you, for example, to the work of Shimura to indicate what I mean.

With this I hope to have convinced you that there is a complete continuity in the main lines of development in number-theory, at least from the days of Euler down to the present day. I could not hope to do more; if I have convinced you of this, I have more than accomplished my purpose.

Epilogue

(July 1973)

Reference has been made above to my conjectures of 1948, which included the extension of the "Riemann hypothesis" to algebraic varieties of arbitrary dimension over finite fields.

Those conjectures have now been proved by Deligne. In the meanwhile, he had also shown, in conjunction with the work of Ihara, that their truth would imply the truth of Ramanujan's conjecture on the τ-function, which has been described above as "very much of an open problem".

Number-theory is not standing still.

(Reçu le 11 juin 1973)

André Weil
The Institute for Advanced Study
Princeton, N.J., 08540