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
DOI: https://doi.org/10.5169/seals-46896

TWO LECTURES ON NUMBER THEORY, PAST AND PRESENT

by André WEIL

To honor the memory of the late Professor Joseph Fels Ritt, his widow donated some funds to endow the Ritt Lecture Series, to be held at Columbia University on the initiative of its Department of Mathematics. The following two lectures, given there in March 1972, were part of this series. As the reader will see, they were "talks" rather than formal lectures, and no attempt has been made to modify their somewhat rambling conversational style; they are reproduced here, with very little editing, from the transcript of a tape-recording; only in the second lecture have a few additions been made, since its content had to be curtailed for lack of time. Thanks are due to Professor H. Clemens and his colleagues of the Department of Mathematics at Columbia University for organizing these lectures, taking them on tape and providing for their transcript.

FIRST LECTURE

I hope that seeing the title you were at once convinced that such a topic could not be covered in two lectures. Perhaps, with optimism, one could attempt to give a bird's eye view of it in two courses of lectures of one year each. So my title should not deceive anyone, because it should immediately be clear that no one could do it justice. The main thesis will be the continuity of number theory for the last three hundred years and the fact that what we are doing now is in direct continuation of what has been done by the greatest number-theorists since Fermat started it all in the seventeenth century.

Those were comfortable times for mathematicians, particularly for number-theorists because they were facing so little competition. In differential and integral calculus, even in the days of Fermat, this was not so, and mathematicians were troubled by some of the things which plague many of our contemporaries; e.g. priorities. It is interesting to notice, however, that in number-theory Fermat was essentially quite alone for the whole of the seventeenth century, and so was Euler for most of the following century,

until Lagrange joined him. Then came Legendre and then, of course, Gauss who already belongs to the nineteenth century and to the modern era. But it is very striking that, for such a long time, things were moving so slowly and in such a leisurely way; one had plenty of time to think about big problems without being bothered by the idea that maybe the next fellow was already cutting the grass under your feet. One could do number-theory in great peace and quiet in those days—indeed a little too much so: Fermat and Euler both complained of being too isolated in that field. I say again that this was far from being so in differential and integral calculus, where Fermat also made decisive contributions. But in number-theory he was alone, and this is one reason why he did not write up what he was doing. At one time he tried to interest Pascal in the subject and persuade him to collaborate with him, but Pascal was not a number-theorist by temperament, he was in bad health, and after a certain moment he became much more interested in religion than in mathematics. So, what Fermat was doing was never properly written up and was left for people like Euler to decipher.

Perhaps, before I go on, I ought to say something about what number-theory is. Housman, the English poet, once got one of those silly letters of inquiry from some literary magazine, asking him and others to define poetry. His answer was "If you ask a fox-terrier to define a rat, he may not be able to do it, but when he smells one he knows it." When I smell number-theory I think I know it, and when I smell something else, I think I know it too. For instance, there is a subject in mathematics (it's a perfectly good and valid subject and it's perfectly good mathematics) which is misleadingly called Analytic Number Theory. In a sense, it was born with Riemann who was definitely not a number-theorist; it was carried on, among others, by Hadamard, and later by Hardy, who were also not number-theorists (I knew Hadamard well); and to the best of my understanding, analytic number theory is *not* number-theory. What characterizes it as analysis (analysis applied to a special kind of problem, where arithmetical terms like "primes" occur frequently) is that it deals mostly with inequalities and asymptotic evaluations; this, to me, characterizes it as being something else than number-theory. I would classify it under analysis, just as probability calculus is a branch of integration theory with a vocabulary of its own. I will give a typical example of the deep gulf that separates number-theorists from an analyst like Hardy. In his famous book about Ramanujan, Hardy could not avoid discussing the "Ramanujan hypothesis" about the Δ-function (the "discriminant" in the theory of modular functions). I will try to say more about this later; for the moment it is enough to say that this is a specific

function arising from the theory of elliptic functions. Expand it into a power series

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n)\, q^n$$

and write the Dirichlet series

$$\sum \frac{\tau(n)}{n^s}$$

with the same coefficients. Ramanujan stated that this has an "Euler product" $\prod_p P_p(p^{-s})^{-1}$, with

$$P_p(T) = 1 - \tau(p)\, T + p^{11}\, T^2$$

for all primes p, and conjectured that, for each p, the roots of the quadratic polynomial $P_p(T)$ have the absolute value $p^{11/2}$ (this is obviously equivalent to the inequality $|\tau(p)| \leqq 2p^{11/2}$). The first statement was proved by Mordell not very long after Ramanujan; the conjecture is still very much of an open problem, although some progress has been made. There is not one among the number-theorists I know who wouldn't be very happy and proud if he could prove it. But Hardy's remarkable comment is: "We seem to have drifted into one of the back-waters of mathematics." To him it was just another inequality; he found it curious that anyone could get deeply interested in it. In fact, he becomes apologetic and explains that, in spite of the apparent lack of interest of this problem it might still have some features which made it not unworthy of Ramanujan's attention.

This story was meant to illustrate the essential difference in taste between number-theorists and other mathematicians. There is also something rather striking in the enthusiasm with which all those who have worked in number-theory speak about it. You will find many such enthusiastic statements in Euler, several in Gauss, more in Hilbert's foreword to his *Zahlbericht*, and so on. I have here a text from the foreword which Gauss wrote for a little volume where Eisenstein put together some of his contributions to number-theory and elliptic functions; we have already seen above how closely the two topics are tied up together. Here are Gauss's words: "The peculiar beauties of these fields have attracted all those who have been active there; but none has expressed this so often as Euler, who, in almost every one of his many papers on number-theory, mentions again and again his delight in such investigations, and the welcome change he finds there from tasks more directly related to practical applications." Then he illustrates Euler's

enthusiasm by quoting his words on receiving a paper by Lagrange on elliptic functions (Gauss is clearly not making any distinction between the two topics). "My admiration was boundless [1], writes Euler, when I heard that Lagrange had thus improved upon my own work."

Having written that, Euler proceeds to improve upon the work of Lagrange. It is a beautiful paper, written at a time when Euler was getting old and was already completely blind; he lost one eye at a comparatively early age and became blind when he was less than sixty. He was then in St. Petersburg, had a number of assistants, and developed a technique for working with their help. As you know, his complete works are still being published; at the moment, there are more than sixty volumes, and there is more to come. The number-theory alone occupies nearly eight volumes.

As an example of his work, I have written here for you, on the blackboard, a formula just as it can be found in Euler:

$$\frac{1 - 2^{n-1} + 3^{n-1} - 4^{n-1} + 5^{n-1} - 6^{n-1} + etc.}{1 - 2^{-n} + 3^{-n} - 4^{-n} + 5^{-n} - 6^{-n} + etc.} =$$

$$= \frac{-1 \cdot 2 \cdot 3 \ldots (n-1)(2^n - 1)}{(2^{n-1} - 1)\pi^n} \cos \frac{n\pi}{2} .$$

It is in a paper read to the Berlin Academy in 1749, but printed only in 1768; the paper (written in French) is entitled *Remarques sur un beau rapport entre les séries de puissances tant directes que réciproques*. Many of you, I hope, have recognized here the functional equation for the zeta-function. In the left-hand side, we have formally the quotient $\zeta(1-n)/\zeta(n)$, except that Euler has written alternating signs to make the series more tractable; the effect of this is merely to multiply $\zeta(n)$ by $1 - 2^{1-n}$, and $\zeta(1-n)$ by $1 - 2^n$. In the right-hand side we have the gamma function, which Euler had invented. Euler proves the formula for every positive integer n (using so-called Abel summation to give a meaning to the divergent series in the numerator of the left-hand side), and conjectures its validity for all n.

This just gives one example of Euler's discoveries in this field. He started his mathematical career as a student of the Bernoullis who were definitely not number-theorists but analysts. Undoubtedly Euler must have had it in his blood, but still it was, in a way, a lucky accident that, as a very young man (he was not quite twenty at the time) he left Basel for St. Petersburg,

---

[1]) « Penitus obstupui... »; Euler was writing in latin.

because no job seemed available elsewhere. St. Petersburg had only just been founded by Peter the Great (who had died in the meanwhile). Peter had made plans for an Academy of Sciences, which his widow carried out. Two of the younger Bernoullis, Nicolas and Daniel, had already gone there; Nicolas had died soon after his arrival. Euler, on getting this appointment, proceeded by ship down the Rhine, as far as Mainz. Then, largely on foot, he went to Lübeck where he took another ship to St. Petersburg which at that time was little more than a glorified village; things were still rather chaotic. Soon Euler was given a good salary and some facilities for his work. Luckily there was a German named Goldbach, now remembered only for "Goldbach's conjecture" ("every even integer is a sum of two primes"); he was a kind of amateur, a man interested in mathematics and in many other things, such as languages. He had known Nicolas Bernoulli in Italy, had settled down in Russia, and had been instrumental in bringing there, first the brothers Bernoulli, then Euler. He was unofficially employed as secretary of the Academy of Sciences, lived mostly in Moscow, and we have all the correspondence between him, the Bernoullis, and Euler. Goldbach, in his amateurish fashion, was fond of number-theory; it was this correspondence which obviously started Euler on a long series of number-theoretical discoveries which he used to communicate to Goldbach before publishing them.

One must realize that Euler had absolutely nothing to start from except Fermat's mysterious-looking statements. Frequently Fermat states flatly "I have proved this", "I have proved that," but then he seems to say the same about "Fermat's equation"

$$x^n = y^n + z^n$$

(more about this later). There were among Fermat's statements, along with the impossibility of that equation, also the fact that every prime of the form $p = 4n + 1$ can be written as $x^2 + y^2$, and similar statements about conditions for a prime to be of the form $x^2 + 3y^2$, $x^2 + 2y^2$, and so on, and a statement about every integer being a sum of four squares. Euler was fascinated by such statements; but he first had to reconstruct for himself all the most basic theorems in number-theory. For instance, there was what is now known as the "little theorem" of Fermat: if p is a prime, then (in modern notation) $x^{p-1} \equiv 1$ modulo p for every integer x, not a multiple of p. For a man who took up Fermat at that time, one statement might well seem just as mysterious as the other, in spite of the ease with which one can verify many of them empirically up to large values. Euler had to reconstruct everything from scratch, all the things that are now to be found in all

elementary textbooks, and which now look so simple on the basis of two concepts, the group concept and the concept of a prime ideal. It took him some time. To begin with, he didn't know that the integers prime to any modulus n make up a group modulo n; of course he didn't have the concept, but also, at first, the existence of an inverse was not immediately obvious. Also there are the facts involved in the statement, which to us looks so elementary, that given a field (e.g. the prime field of integers modulo a prime) any equation in one unknown has at most as many roots in that field as its degree indicates. This was not proved by Euler and Lagrange until about 1760, about thirty years after Euler had started working on number-theory and when he was working on far more difficult questions. He had no way of knowing which questions were simple and which ones were not so. For instance, the fact that all primes $p = 4n + 1$ are of the form $x^2 + y^2$ looked neither more nor less difficult to him than the assertion that an equation of the fifth degree (modulo p, i.e. over a prime field) has at most five roots. In fact, he would have considered the former question as easier because it involves only squares and the other involves fifth powers; following Diophantus and Fermat, Euler took the degree as the first element in the classification of problems; of course, he could guess that there are other aspects, but he could not be sure.

So he had to reconstruct everything from scratch as I said. It is actually very fascinating to see in his correspondence with Goldbach how his ideas developed, how he solved one problem after the other. He solves some question, modulo something else—sometimes he explains "if I could prove this then I could prove that," and Goldbach has some remarks to make about it. Goldbach really took an interest even though he does not seem ever to have contributed anything of real value. As a correspondent, however, he was invaluable to Euler for many years. Later Lagrange appeared on the scene and started corresponding with Euler; he, of course, was a first-rate mathematician, and Euler realized this immediately.

For many years Euler worked on pure number-theory, taking as his starting point only Fermat's work. One main topic was about writing integers and particularly primes as sums of squares. Take e.g. Fermat's assertion that any prime p of the form $p = 4n + 1$ can be written as $p = x^2 + y^2$. Euler proves it in his correspondence to Goldbach in the year 1749; he says "at last now I have the valid and complete proof for this."

That proof is very interesting; I could describe it and explain what it has in common with the proof as one would give it now and in what they differ. But since my time is so limited, I'd rather notice the following case:

$$p = x^2 + 3y^2 .$$

Let's take this as being more characteristic in some ways. Diophantus already knew that there is an identity

$$(x^2+y^2)(u^2+v^2) = (xu-yv)^2 + (xv+yu)^2$$

which guarantees that the product of two sums of two squares is the sum of two squares. The identity, as everybody knows, comes from the fact that

$$(x^2+y^2)(u^2+v^2) = |(x+iy)(u+iv)|^2$$

and therefore the product is the norm of the product of these two complex numbers. Quite similarly, for identities of the form $p = x^2 + 3y^2$, one will use the fact that $x^2 + 3y^2$ is the norm of $x + y\sqrt{-3}$. Euler eventually became completely conscious of this and used the fact frequently; Lagrange also uses it. On one occasion Euler even takes the trouble to compliment Lagrange on the fact that he has made good use of irrational and even, he says, imaginary numbers in his number-theoretic work when most people would think that this is a completely extraneous matter. This shows that the theory of algebraic number-fields goes back to fairly early days; in fact it is tempting to conjecture that already Fermat had used facts of the same kind, although there is no trace of it so far as I know in his writings.

At this stage it is worthwhile to take up the question whether Fermat had really, as he states, proved "Fermat's theorem"; this is not altogether an idle question, although of course one cannot be sure of the answer. The statement occurs as a marginal note in his copy of Diophantus; that copy is lost, but the notes were published by his son after his death; this was not an unreasonable thing to do, since they had clearly been written down with the intention of preparing some systematic work on number-theory, which never took shape. Right at the beginning there occurs the statement that a cube cannot be the sum of two cubes, nor a fourth power the sum of two fourth powers, and, he says, similarly for any power beyond the second. He adds, "I have a wonderful proof of that, but there is no room for it in this margin." He had the proof for fourth powers; indeed, his notes on Diophantus include a complete proof for the impossibility of the equation

$$x^4 - y^4 = z^2 ,$$

which obviously implies the same for the equation $x^4 = y^4 + z^4$. I would guess (knowing what we know about his work) that he had also a complete

proof for the equation $x^3 - y^3 = z^3$; this proof could well have been the same that Euler, after many years of work, finally reconstructed in detail. Interestingly, Euler first proved the impossibility of this equation on the basis of an assumption which (in modern language) amounts to the fact that the field $Q(\sqrt{-3})$ of cubic roots of unity has only one ideal class. Later on, he succeeded in proving that assumption. It is rather clear, in view of everything that Fermat has written, that he had already the equivalent of the fact that the class number of $Q(\sqrt{-3})$ is 1. If you make the similar assumption about n-th roots of unity, then it is not too hard to prove Fermat's theorem for n-th powers; of course we know that the assumption is not true in general. Therefore one might fancy that Fermat had some proof based on this (or some equivalent) assumption, but then realized that it need not be valid for all n. Actually, in his correspondence with foreign mathematicians, Fermat never mentioned his equation for general n; he mentions it repeatedly for cubes. It seems rather unlikely, too, that he could even have attacked seriously the equation $x^5 = y^5 + z^5$, not merely because of its difficulty, but for a reason which I wish to explain now, and which has to do with Fermat's temperament as a mathematician.

Many people think that one great difference between mathematics and physics is that in physics there are theoretical physicists and experimentalists and that a similar distinction does not occur in mathematics. This is not true at all. In mathematics just as in physics the same distinction can be made, although it is not always so clear-cut. As in physics the theoreticians think the experimentalists are there only to get the evidence for their theories while the experimentalists are just as firmly convinced that theoreticians exist only to supply them with nice topics for experiments. To experiment in mathematics means trying to deal with specific cases, sometimes numerical cases. For instance an experiment may consist in verifying a statement like Goldbach's conjecture for all integers up to 1000, or (if you have a big computer) up to one hundred billion. In other words, an experiment consists in treating rigorously a number of special cases until this may be regarded as good evidence for a general statement. There are many ways of making experiments, some of which may involve no little theoretical knowledge; for instance nowadays there are people who are greatly interested in $GL(n)$ and who make experiments by taking first $n = 1$ (which is already non-trivial for many problems) and then $n = 2$ (which may be quite hard). Consequently the first-rate mathematician must have some strength on both sides, but still there is a distinction between temperaments. Now

Fermat was clearly a theoretician. He was interested in general methods and general principles and not really in special cases; this appears in all his work, in analysis as well as in number-theory. Euler, on the other hand, was basically an experimentalist. He was very happy when he could conjecture a general law, and he was willing to spend a great deal of time to prove it; but if, instead of a proof, he had merely some really convincing experimental evidence, that pleased him almost as well. Therefore he tends to branch out in all possible directions, whereas Fermat, being a theoretician, always speaks about "his methods," thus giving us fair indications about the range of his number-theoretic interests. Essentially he was concerned with quadratic forms, chiefly binary, i.e. with quadratic number-fields from the point of view which Gauss was to develop very widely later, and also with so-called Diophantine equations, but always equations of genus one. When Fermat speaks of "my method," this means usually a method for dealing with what is now known as elliptic curves. The equations $x^4 - y^4 = z^2$ and $x^3 = y^3 + z^3$ define such curves, but $x^5 = y^5 + z^5$ does not and so would be beyond the scope of Fermat's normal work.

This is the first time that a connection enters between elliptic curves and number-theory in this very natural way. Some of the most interesting equations are equations of genus one. This of course does not lead to elliptic functions until one starts integrating, and to Fermat and Euler there was a wide gap between differentiation and integration on the one hand, and number-theoretical formulas on the other hand, a gap which now from our present point of view doesn't exist any more; we know how to bridge it. It is striking that Euler became greatly interested in pure number-theory, particularly in proving Fermat's statements, which included the particularly difficult equations of genus one, and also became interested in the topic in at least two more ways. One is indeed closely connected with the equation $x^4 - y^4 = z^2$. Already Leibniz seems to have conjectured that

$$\int \frac{dx}{\sqrt{1-x^4}}$$

cannot be integrated by means of elementary functions (including exponential and trigonometric functions). But Fagnano made the remarkable discovery that the differential equation

$$\frac{dx}{\sqrt{1-x^4}} = \frac{dy}{\sqrt{1-y^4}}$$

has rational integrals. This started Euler. According to Jacobi, the birth-date of the theory of elliptic functions is the day in 1750 when Fagnano's collection of mathematical papers reached the Berlin academy and was submitted to Euler for refereeing. It was already printed, but, as the most prominent member of the Berlin academy, Euler had to say whether the collection was to receive its official approval. He immediately caught fire and started writing a series of papers. It is in this connection that Lagrange, as we have said, came to improve upon Euler's work, whereupon Euler again improved upon Lagrange's work. Euler writes

$$\frac{dx}{\sqrt{P(x)}} = \frac{dy}{\sqrt{P(y)}}$$

where P is a polynomial of the fourth degree. He found that the case of the fourth degree has special features which make it possible to find algebraic integrals for this kind of equation, and also (as he noticed after a while) for

$$\frac{m\,dx}{\sqrt{P(x)}} = \pm\frac{n\,dy}{\sqrt{P(y)}}$$

with arbitrary integers m, n. From our point of view, all this amounts to the addition and multiplication of elliptic functions.

Euler became deeply interested in this, and so was Lagrange, without thinking much about possible connections with number theory. Now if he had studied Fermat's proof of the impossibility of the equation $x^4 - y^4 = z^2$ from that point of view, he would have found that this proof included the formula for the complex multiplication by $1 \pm i$ of this elliptic function. You have only to put together Fermat's formulas to do this. If you iterate this, you have duplication.

The way Fermat does it is the following. First there is the simple formula which gives complex multiplication by $1 + i$. This sends you into the same curve over the complex numbers, but in this case into another curve over the rational numbers. Doing the same again with $1 - i$ brings you back to the initial curve. In a sense he has duplicated the initial given point on the curve. Furthermore, for reasons connected with this particular curve, the process can be inverted. Starting from a given point on the curve, assuming that there is one in rational numbers, you can rationally divide it by $1 - i$ and then again by $1 + i$ so that you have divided it by 2; this gives a point with smaller coordinates on the same curve. This is the "infinite descent,"

which obviously leads to a contradiction since a sequence of integers cannot go on decreasing all the time.

Such is Fermat's proof. Euler (or Fagnano) could have read their formulas simply in Fermat's number-theoretic work if it had occurred to them to look at it that way.

Now we come to other aspects of Euler's work, some of which are also related to elliptic functions. There is one topic where Euler had virtually no predecessor: all his life he liked to play with the formal manipulation of series. The origin of all this was clearly in the discovery by Leibniz of the series

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots .$$

Euler was very much attracted by this kind of result and eventually he made a discovery of which he felt justifiably proud and which was quite sensational at the time:

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots = \frac{\pi^2}{6} .$$

This he discovered in 1736; immediately he sent it to his friend Daniel Bernoulli who by this time was back in Switzerland, and who was deeply impressed. Euler proceeded at once to do the same for all even powers,

$$1 + \frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{4^{2n}} + \dots = \pi^{2n} R \quad (\text{R rational});$$

but, for reasons that he could not discover, the odd powers resisted all his efforts. With this he became quite familiar with the series now known as the zeta-function and noticed that it can be written as an infinite product

$$\sum \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}},$$

now called an Euler product. Then he started playing with relations between infinite sums and infinite products. Incidentally, he noticed that this gives a new proof that there are infinitely many primes, and that a very elementary argument, based on a similar idea, proves that there are infinitely many primes in the two arithmetic progressions $\{4n + 1\}$, $\{4n - 1\}$.

Playing with series and products, he discovered a number of facts which

to him looked quite isolated and very surprising. He looked at this infinite product

$$(1-x)(1-x^2)(1-x^3)\ldots$$

and just formally started expanding it. He had many products and series of that kind; in some cases he got something which showed a definite law, and in other cases things seemed to be rather random. But with this one, he was very successful. He calculated at least fifteen or twenty terms; the formula begins like this:

$$\prod (1-x^n) = 1 - x + x^3 + x^5 + x^7 - x^{12} - x^{15} \ldots$$

where the law, to your untrained eyes, may not be immediately apparent at first sight. In modern notation, it is as follows:

$$\prod_1^{\infty} (1-q^n) = \sum_{-\infty}^{+\infty} (-1)^n q^{\frac{n(3n+1)}{2}}$$

where I've changed x into q since q has become the standard notation in elliptic function-theory since Jacobi. The exponents make up a progression of a simple nature. This became immediately apparent to Euler after writing down some 20 terms; quite possibly he calculated about a hundred. He very reasonably says, "this is quite certain, although I cannot prove it"; ten years later he does prove it. He could not possibly guess that both series and product are part of the theory of elliptic modular functions. It is another tie-up between number-theory and elliptic functions.

He has another very interesting statement which, as we know now, is also connected with elliptic functions. He states that certainly the most natural way of proving theorems about integers being sums of squares would be to compute the powers of this series:

$$x + x^4 + x^9 + x^{16} + \ldots;$$

for instance, the most natural way to prove Fermat's assertion about every number being a sum of four squares would be to get a formula for the fourth power of this series. Here again we are dealing with a problem on elliptic functions, and this is how Jacobi proved Fermat's theorem, long after Lagrange had given a purely arithmetical proof which was soon simplified by Euler himself.

Thus we see that number-theory brings us necessarily to the theory of elliptic functions and conversely; by hindsight, this is now apparent even in Fermat's work, and much more so with Euler. With Gauss's first investi-

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