

First Lecture

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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 $p^{1/2}$ (this is obviously equivalent to the inequality $|\tau(p)| \leq 2p^{1/2}$). 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 black-board, a formula just as it can be found in Euler:

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

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

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

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

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:

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

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:

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

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 ≥ 2 , and, for all integers $n > 0$, the alternating sum $1 - 2^n + 3^n - \dots$. 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;