KUMMER'S IDEAS ON FERMAT'S LAST THEOREM

Autor(en): **Ribenboim, P.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **29 (1983)**

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

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-52978

L'Enseignement Mathématique, t. 29 (1983), p. 165-177

KUMMER'S IDEAS ON FERMAT'S LAST THEOREM [1]

by P. Ribenboim

My purpose in this lecture is to present the main ideas of Kummer concerning Fermat's last theorem, to show how his approach to the problem was natural and how he was led to create the theory of cyclotomic fields. I'll discuss his main theorem, as well as his further contributions, and indicate some of the paths they opened in the study of arithmetics.

1. "Fermat's last theorem" is the following statement (not yet proved in all its generality):

(FLT) If $n \geqslant 3$ there does not exist positive integers x, y, z, such that

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

To begin, I note that if $n = 2$ there are such integers, like for example 3, 4, 5:

$$3^2 + 4^2 = 5^2$$

and 5, 12, 13:

$$5^2 + 12^2 = 13^2 .$$

I shall not consider here these "Pythagorean triples" of integers, despite their interesting properties.

In order to prove FLT for every value of the exponent n, it suffices to do it for the exponent $n = 4$ and for every prime exponent $p \geqslant 3$.

Indeed, if n is composite, $n > 2$, it has a factor m which is 4 or an odd prime. If the theorem fails for $n = ml$ (with $l > 1$) if x, y, z are positive integers such that $x^n + y^n = z^n$ then $(x^l)^m + (y^l)^m = (z^l)^m$ and the theorem would fail for m—against the hypothesis.

Fermat discovered a proof of the theorem for the exponent $n = 4$. In this famous proof, Fermat introduced the "method of infinite descent": assuming that the triple of positive numbers (x, y, z) is a solution of Fermat's equation, he succeeded to produce another solution (x', y', z') in positive numbers, with $z > z' > 0$; starting from the new solution and repeating the argument, he would

[1] Lecture at the "Séminaire de Philosophie et Mathématique", Dieudonné-Loi-Thom, Ecole Normale Supérieure, Paris, March 5, 1979.

obtain again a solution (x'', y'', z'') in positive integers, with $z > z' > z'' > 0$. Since $z, z', z'', \ldots$ are integers, this process cannot be repeated indefinitely, and this is a contradiction. Thus Fermat's equation could not have a solution in positive integers.

Euler proved the theorem for the exponent $n = 3$. Another proof for this exponent is due to Gauss; it was found among his papers and it was published after his death. Actually, Gauss showed even more. If $\omega = \frac{-1 + \sqrt{-3}}{2}$ is a cubic root of 1 and if $\mathbf{Q}(\omega) = \mathbf{Q}(\sqrt{-3})$ denotes the field of all numbers of the form $a + b\omega$ (with $a, b \in \mathbf{Q}$)—this field is sometimes called the Eisenstein field—then Gauss showed that if $n = 3$ there are no non-zero elements x, y, z in $\mathbf{Q}(\omega)$ such that $x^3 + y^3 = z^3$.

Legendre wrote papers about Fermat's theorem and reproduced Euler's proof in his book "Théorie des Nombres", thus attracting the attention of the French mathematicians to Fermat's theorem.

The proof for $n = 5$ was done independently, and almost simultaneously by Legendre and Dirichlet (1825/8).

In 1832, Dirichlet proved the theorem for $n = 14$, sensibly easier than the exponent $n = 7$. For the latter, the proof was found by Lamé (1839), and immediately thereafter simplified by Lebesgue (1840).

At this time, there was in Paris a considerable interest for FLT. Besides the mathematicians already mentioned (including Dirichlet, who was spending some time in Paris), Cauchy published a series of substantial papers in number theory. He worked with the so-called "radical polynomials", investigating their decomposition into factors.

In modern language, his research could be translated into a study of the arithmetic of cyclotomic fields. However, he did not succeed in making any major breakthrough in Fermat's problem, as Kummer did soon afterwards.

In 1847, Lamé presented at the Académie des Sciences de Paris, a proof of FLT for an arbitrary exponent. The details were published in Liouville's *Journal de Mathématiques Pures et Appliquées.* However, Liouville noted that the proof was not correct, since Lamé was assuming (without further justification) the uniqueness of decomposition of certain polynomials in roots of unity into products of irreducible factors. This was far from obvious, and it turned out to be false. After some repeated efforts to correct his proof, Lamé realized that there was an essential difficulty, which he was not able to handle.

2. It is against such a background that Kummer began his remarkable work on Fermat's last theorem.

Already in 1837, Kummer published his first paper, written in Latin, about FLT with an even exponent $2n$. He proved:

If $n > 1$ is odd and if there exist positive integers x, y, z such that $gcd(n, xyz) = 1$ and $x^{2n} + y^{2n} = z^{2n}$, then necessarily $n \equiv 1 \pmod 8$.

This is only a partial result. Its proof was very simple and has been found again and again.

If the exponent in Fermat's equation is even it is possible to apply the powerful methods from the theory of quadratic forms. Thus, in December 1977, Terjanian showed: If p is an odd prime and if there exist positive integers x, y, z such that $x^{2p} + y^{2p} = z^{2p}$ then $2p$ divides x or y.

It is quite remarkable that Terjanian's proof is entirely elementary and classical, appealing only to the Jacobi symbol and to the divisibility properties of expressions of the form $\dfrac{x^p \pm y^p}{x \pm y}$.

This suggests the possibility of finding an elementary proof, for the prime exponent p, of the following assertion which is usually called:

The first case of FLT *for the exponent* p:

If x, y, z are positive integers such that $x^p + y^p = z^p$ then p divides xyz.

For such a proof, it will be at least necessary to work with the reciprocity law for the power residue symbol belonging to p.

3. The first important paper by Kummer on Fermat's theorem was conceived since 1844, and appeared in 1847. His method, which we shall soon explain, led him to work with cyclotomic fields. If the prime p is the exponent of the Fermat equation, he considered $\zeta_p = \cos \dfrac{2\pi}{p} + i \sin \dfrac{2\pi}{p}$, a primitive p-th-root of 1, and the field $\mathbf{Q}(\zeta_p)$, consisting of all complex numbers of the form

$$\alpha = a_0 + a_1 \zeta_p + a_2 \zeta_p^2 + \dots + a_{p-2} \zeta_p^{p-2}$$

(with $a_0, a_1, \dots, a_{p-2} \in \mathbf{Q}$). Those numbers with $a_0, a_1, \dots, a_{p-2} \in \mathbf{Z}$ constitute the ring $\mathbf{Z}[\zeta_p]$ of cyclotomic integers (relative to p). Just like for ordinary integers, if $\alpha, \beta \in \mathbf{Q}(\zeta_p)$, ($\alpha$, β non-zero), then α divides β if there exists a cyclotomic integer γ such that $\alpha\gamma = \beta$. Two cyclotomic integers α, β are associated when α divides β and β divides α. The cyclotomic integer α is prime if any cyclotomic integer dividing α is either associated with α or with 1. This theory of divisibility cannot distinguish between associated cyclotomic integers. In particular the cyclotomic integers associated with 1 play the same neutral role as 1, and they are called the units of the cyclotomic field $\mathbf{Q}(\zeta_p)$.

The fundamental theorem of unique factorization of integers should be phrased as follows:

a) Every cyclotomic integer of $\mathbf{Q}(\zeta_p)$ is the product of finitely many prime cyclotomic integers.

b) Any two such decompositions are equal, up to units, that is, if $\alpha = \beta_1\beta_2 \dots \beta_s = \gamma_1\gamma_2 \dots \gamma_t$ where β_i, γ_j are prime cyclotomic integers, then $s = t$ and after an eventual permutation, α_i and β_i are associated (for every $i = 1, \dots, s$).

The assertion (a) is indeed true and easy to prove. But already in 1844, Kummer had discovered that the assertion (b) *does not hold in general*; as a matter of fact, Kummer showed that it is false for $p = 23$.

In a letter sent to Liouville (1847), together with his paper, Kummer explained how he was led to consider a new type of complex numbers, which he called the *ideal numbers*, in order to recover for these numbers the theorem of unique factorization. In another paper, Kummer explained the concept of ideal numbers with an analogy to chemistry. At his time, the existence of certain chemical substances containing fluor radicals had been already ascertained, yet the fluor itself had not been isolated. According to Kummer, fluor was like his ideal numbers, while the radicals containing fluor, which did actually appear in nature, were like the true (= "wirklich") complex numbers.

The very definition of an ideal number, as given by Kummer, was phrased in terms of divisibility properties. This approach has evolved into the concept of "divisor", which presents itself naturally in the theory of algebraic functions.

On the other hand, while trying to understand Kummer's concept, Dedekind gave an interpretation of ideals by means of certain subsets of $\mathbf{Q}(\zeta_p)$. Thus, an ideal (in Dedekind's approach) is a subset I of $\mathbf{Q}(\zeta_p)$ such that: it is closed under addition and $0 \in I$; if $\alpha \in \mathbf{Z}[\zeta_p]$ and $\beta \in I$ then $\alpha\beta \in I$; there exist $\alpha \in \mathbf{Z}[\zeta_p]$, $\alpha \neq 0$, such that $\alpha\beta \in \mathbf{Z}[\zeta_p]$ for every $\beta \in I$. If $I \subset \mathbf{Z}[\zeta_p]$ the ideal is said to be integral, otherwise it is fractional (but not integral). Every $\alpha \in \mathbf{Q}(\zeta_p)$ gives rise to the ideal of its multiples: $(\alpha) = \{\beta\alpha | \beta \in \mathbf{Z}[\zeta_p]\}$ called the principal ideal of α. In order that $(\alpha) = (\beta)$ it is necessary and sufficient that $\alpha = \beta = 0$ or, otherwise, $\alpha\beta^{-1}$ be a unit of $\mathbf{Z}[\zeta_p]$.

The product of the ideals I, J is by definition the ideal consisting of all finite sums of elements $\alpha\beta$, where $\alpha \in I$, $\beta \in J$.

To measure the extent by which there are non-zero ideals which are not principal (i.e., in Kummer's language, "ideal numbers" which are not "numbers") Kummer introduced the following equivalence relation: $I \sim J$ if there exists $\alpha \in \mathbf{Q}(\zeta_p)$, $\alpha \neq 0$, such that $I = (\alpha)J$. The equivalence classes are called the ideal classes or classes of ideals.

To say that there is only one equivalence class in $\mathbf{Q}(\zeta_p)$, means that every ideal of $\mathbf{Q}(\zeta_p)$ is principal. Kummer showed that this means that the unique factorization theorem is true for the elements of the corresponding ring of cyclotomic integers.

Since Kummer showed that this theorem does not hold, for example when $p = 23$, he was led naturally to study the size of the set of classes of ideals.

In this connection he proved the following fundamental result: for each cyclotomic field $\mathbf{Q}(\zeta_p)$ the number of ideal classes is finite. It is called the class number of $\mathbf{Q}(\zeta_p)$ and denoted usually by h_p.

These ideas were developed in a series of important papers, published between 1847 and 1851, one of which appeared in French in Liouville's journal (1851). They contain many of the basic theorems of the future theory of algebraic numbers, for the special class of cyclotomic fields.

4. Now I shall turn to the so-called Kummer's main theorem. Personally, I like to refer to this as his monumental theorem, since it stands on top of a theory, built of all pieces by Kummer, which represented a truly remarkable advance over all the knowledge and techniques at that time.

I'll omit to discuss the purported story of a proof of FLT by Kummer, not later than 1844, in which Kummer had made the mistake of assuming the theorem of unique factorization. This anecdote, propagated by Hensel, is analysed in a paper by Edwards (1975) about the recent discovery of a letter from Liouville to Dirichlet.

The exact statement of Kummer's main theorem of 1847 is the following.

Fermat's last theorem is true for any odd prime exponent p satisfying the following two conditions (expressed here in modern terminology):

1) If an ideal I is such that its p-th power I^p is a principal ideal, then I itself is a principal ideal.

2) If ω is a unit of the cyclotomic field $\mathbf{Q}(\zeta_p)$ and if there exists an ordinary integer $m \in \mathbf{Z}$ such that $\omega \equiv m (\bmod p)$ then ω is the p-th power of a unit.

These were working hypotheses. The problem became therefore to find out for which prime numbers p these hypotheses were satisfied.

First, he proved that condition (1) is equivalent to the following one:

1') p does not divide the class number h_p of the cyclotomic field $\mathbf{Q}(\zeta_p)$.

Moreover, using the results of his deep study of arithmetic of cyclotomic fields, he showed that the condition (1) implies condition (2). This statement is now known as Kummer's "lemma on units". The proof is very delicate and required what is now known as λ-adic methods (where λ is the cyclotomic prime of $\mathbf{Q}(\zeta_p)$ which divides p).

Every prime p satisfying condition (1′) is called a *regular prime*. In other words, Kummer proved:

If p is a regular prime then FLT is true for the exponent p.

As a matter of fact, Kummer showed more: if p is a regular prime, there are no non-zero numbers $\alpha, \beta, \gamma \in \mathbf{Q}(\zeta_p)$ such that $\alpha^p + \beta^p = \gamma^p$. It should be said that Kummer's proof for the non-existence of solutions in $\mathbf{Q}(\zeta_p)$ was erroneous. This was noticed and corrected by Hilbert.

I shall comment on Kummer's proof to show how natural was his reasoning.

Suppose that x, y, z are non-zero integers such that $x^p = z^p - y^p$. It is possible to assume that x y, z are pairwise relatively prime, after dividing by their greatest common divisor. The aim is to arrive at a contradiction. Looking at the above equation, in the lefthand side there is a product, while the righthand side is a difference. It is quite a natural idea to transform the difference into a product; this can be done with the use of $\zeta = \zeta_p$, the p-th root of 1:

$$x^p = z^p - y^p = \prod_{j=0}^{p-1} (z - \zeta^j y)$$

It would be desirable to have the various factors $z - \zeta^j y$ "pairwise relatively prime" and to conclude that each is the p-th-power of a cyclotomic integer. In such a crude way, this is not true. At this point it is necessary to introduce the ideals, for which the unique factorization theorem holds.

Let I be the ideal which is the greatest common divisor of the principal ideals $(z - \zeta^j y)$ (for $j = 0, 1, 2, \ldots, p-1$). Then

$$(z - \zeta^j y) = J'_j I \; (j = 0, 1, \ldots, p-1)$$

where the ideals J'_j are pairwise relatively prime. It follows from the unique factorization theorem for ideals, that each one is a p-th-power; so

$$(z - \zeta^j y) = J_j^p I \; (j = 0, 1, \ldots, p-1)$$

This is how Kummer's proof begins. Then the discussed two cases, whether p does not divide xyz, or p divides xyz.

The proof, with full details, appears in my book, and I do not wish to enter into more explanations in this lecture.

5. After proving his main theorem, Kummer's task was clear.

1°) To characterize or at least to study the regular primes.

2°) To find out whether there are infinitely many regular primes.

3°) To extend his main theorem to irregular prime exponents—at least those satisfying appropriate additional conditions.

Thus, Kummer had to compute the value of the class number h_p. For small values of p, he had computations already before 1850.

Using results communicated to him by Dirichlet, Kummer was able to find an explicit formula for the class number h_p. Namely, he wrote h_p as the product of two positive integers,

$$h_p = h_p^- \cdot h_p^+$$

called respectively the first and second factors of the class number and later interpreted arithmetically.

h_p^+ is equal to the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ consisting of all real numbers in $\mathbf{Q}(\zeta_p)$. Thus h_p^+ is more often called the real class number of $\mathbf{Q}(\zeta_p)$, and hence h_p^- is the relative class number. Kummer's formulas were

$$h_p^- = \frac{1}{(2p)^{\frac{p-3}{2}}} \mid G(\eta)G(\eta^3) \dots G(\eta^{p-2}) \mid$$

$$h_p^+ = \frac{2^{\frac{p-3}{2}}}{R} \prod_{k=1}^{\frac{p-3}{2}} \left| \sum_{j=0}^{\frac{p-3}{2}} \eta^{2kj} \log \mid 1 - \zeta^{g^j} \mid \right|$$

It is not easy to explain some of the quantities appearing in the above formulas to anyone who is not already acquainted with the basic theory of algebraic numbers.

— g denotes a primitive root modulo p;

— for each $j \geqslant 0$, $1 \leqslant g_j \leqslant p-1$ and $g_j \equiv g^j (\mathrm{mod}\ p)$;

— $G(X) = \sum_{j=0}^{p-2} g_j X^j$;

— η is a primitive $(p-1)$-th root of 1;

— R is the regulator of the cyclotomic field, namely $R = 2^{\frac{p-3}{2}} \det(L)$, where L is the following matrix:

$$L = \begin{pmatrix} \log |\varepsilon_1^{(1)}| & \dots & \log \mid \varepsilon_1^{(r)} \mid \\ \dots & \dots & \dots \\ \log \mid \varepsilon_r^{(1)} \mid & \dots & \log \mid \varepsilon_r^{(r)} \mid \end{pmatrix}$$

where

— r_1 is the number of conjugates to the field $\mathbf{Q}(\zeta_p)$ which are contained in the field of real numbers;

— $2r_2$ is the number of such conjugates, which are nor contained in the field of real numbers;

— $r = r_1 + r_2 - 1$;

— $\{\varepsilon_1, ..., \varepsilon_r\}$ is a fundamental system of units of $\mathbf{Q}(\zeta_p)$, that is:

a) if $\varepsilon_1^{e_1} ... \varepsilon_r^{e_r} = 1$ (with $e_1, ..., e_r$ integers) then $e_1 = ... = e_r = 0$

b) if ε is a unit of $\mathbf{Q}(\zeta_p)$ there exists an integer j, $0 \leqslant j \leqslant p - 1$ and integers $e_1, ..., e_r$ such that $\varepsilon = \zeta_p^j \varepsilon_1^{e_1} ... \varepsilon_r^{e_r}$;

— if $\alpha \in \mathbf{Q}(\zeta_p)$ then $\alpha^{(1)}, \alpha^{(2)}, ..., \alpha^{(r_1)}$ denote the conjugates of α which are real, and $\alpha^{(r_1+1)}, \alpha^{(r_1+2)}, ..., \alpha^{(r_1+2r_2)}$ those which are not real, in such a way that $\alpha^{(r_1+r_2+j)}$ is the complex conjugate to $\alpha^{(r_1+r_2)}$ (for $j = 1, ..., r_2$).

Altogether, these formulas are difficult to explain, were hard to discover and visibly are quite unsuitable for explicit computations. Moreover, they are sort of miraculous, if one takes into account that h_p^+, which is an integer, being a class number, is a product of sums of products of logarithms and trigonometric expressions

$$\eta^{2kj} = \cos \frac{4kj\pi}{p-1} + i \sin \frac{4kj\pi}{p-1}.$$

Thus, the computations were already elaborate even for relatively small values of p.

However—and this is an easy remark—what counted for Kummer was not to determine the exact value of h_p, but just to know whether p divides h_p. In this respect, Kummer proved the rather unexpected and deep result:

If p divides h_p^+ then it divides h_p^-.

As a consequence p divides h_p if and only if p divides h_p^-. This represents a considerable advance, if one takes into account that the factor h_p^+ cannot be dealt up to now except with quite powerful and sophisticated methods.

6. Concerning the divisibility of h_p^- by p, Kummer was able to transform the problem into another of a more elementary nature. He proved the following regularity criterion:

p divides h_p^- if and only if there exists an integer k, $1 \leqslant k \leqslant \frac{p-3}{2}$ such that

p^2 divides the sum $\sum_{j=1}^{p-1} j^{2k}$.

Euler had studied these sums and expressed them in terms of the Bernoulli numbers, first considered in the theory of probability.

I recall their definition. By dividing x by $e^x - 1 = \sum_{n=1}^{\infty} \frac{x^n}{n!}$ we may write the coefficients successively as $\frac{B_n}{n!}$ where B_n is the n-th Bernoulli number:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

Thus $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, \ldots$.

These numbers may be obtained recursively from the above definition; thus if $B_0, \ldots, B_{n-1}$ are known then B_n satisfies

$$\binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \ldots + \binom{n+1}{n} B_1 + 1 = 0 .$$

From this it follows that $B_{2n+1} = 0$ for $n \geqslant 1$ and that each B_n is a rational number.

To say that the prime p divides B_{2k} means then p divides its numerator, when B_{2k} is written as an irreducible fraction.

Kummer transformed his first regularity criterion into the following one:

p divides h_p^- if and only if p divides one of the numbers $B_2, B_4, B_6, \ldots, B_{p-3}$.

This appears to be a much more practical criterion, since the Bernoulli numbers may be obtained, at least in theory, recursively. It is true that the recursion formula has an increasing length, however there are other recursion formulas of more technical nature, but smaller length, which allow a considerable simplification in the calculations. Despite everything, a true difficulty lies in the fact that the numerators of the Bernoulli numbers increase at a fantastic speed and the very question of writing these numbers becomes a real problem. Just think, for example, that the numerator of B_{210} has about 250 digits!

7. All the above results, whatever their depth and value, do not allow to forecast whether a given prime number is or is not regular—unless the specific computations are performed. *A fortiori*, they do not give any indication about the distribution of regular primes.

Concerning this question, without entering into long considerations, I want to recall that Kummer computed with bare hands (that is, without any mechanical or electronic devices) the class numbers of $\mathbf{Q}(\zeta_p)$ for $p \leqslant 163$. Thus, he has found the first irregular primes: 37, 59, 67, 101, 103, 131, 149, 157.

He conjectured, without any strong base, that there should exist about as many regular as irregular primes (in a sense which I will explain).

Let us note, in this respect, that Jensen has shown in 1915 that there exist infinitely many irregular primes (even congruent to 3 modulo 4). On the other hand, it has never been shown that there exist infinitely many regular primes. Using heuristic arguments, Siegel has indicated in 1964 that

$$\lim_{N \to \infty} \frac{\text{number of irregular primes } p \leqslant N}{\text{number of primes } p \leqslant N} = 1 - \frac{1}{\sqrt{e}} = 0.39 \ldots .$$

This agrees with the recent explicit computations of Wagstaff up to $N = 125000$.

Kummer has also proved FLT for certain classes of irregular exponents, satisfying additional conditions, rather difficult to be verified. These are very technical results, where Kummer could not avoid commiting mistakes, as it was noted, and partly corrected, by Vandiver in 1922 and 1926.

On the other hand, Kummer's efforts about the first case of FLT were more successful.

He discovered certain congruences involving Bernoulli numbers, which must be satisfied by hypothetical solutions of Fermat's equation. This paper is a typical Kummerian jewel, mixing arithmetical and transcendental methods in an astonishing way. Based on these congruences, he proved that if the first case of FLT fails for the exponent p then p divides B_{p-3} and B_{p-5}. Incidentally, the fact that p divides B_{p-3} had been discovered, earlier by Cauchy and Genocchi.

Mirimanoff extended Kummer's result and proved that p divides B_{p-7} and B_{p-9}. More recently, Morishima proved that p must also divide B_{p-11} and B_{p-13}.

An examination of the most complete tables by Wagstaff, indicate that this phenomenon is extremely rare. In fact, it is very seldom that p divides a large number of Bernoulli numbers (with index at most $p - 3$), and never it divides successive Bernoulli numbers. All this is in relation with the profound structure of the group of classes of ideals and maybe a little understood through the works of Hecke, Scholz, Eichler and Ribet.

What should I say then of Krasner's striking result of 1934? He has shown:

Let $n_0 = (45!)^{88}$. If p is a prime number, $p > n_0$, if $k(p) = [\sqrt[3]{\log p}]$ and if the first case of FLT is false for the exponent p then p divides the $k(p)$ successive Bernoulli numbers $B_{p-3}, B_{p-5}, \ldots, B_{p-k(p)-1}$ (the number n_0 has no special significance and may be reduced with a little care in the proof, yet it remains too large for the theorem to have any practical application).

This theorem, which puts Krasner among the main contributors to the study of FLT, indicates that the first case is plausible.

To conclude, it would be unjust to Kummer not to mention that, even in number theory, he had other contributions and ideas of first magnitude—albeit even more important. They concern the theory of the reciprocity law for the power residue symbol, a forerunner of class field theory. As it turned out, and was shown by Furtwängler already in 1912, and by Hasse in 1926, this theory could also be applied to the study of FLT.

Kummer's work was taken up and amplified by a number of mathematicians who dealt (and will deal) with FLT. There is still much to learn and to understand and the publication of Kummer's Collected Papers in 1975, annotated by Weil, will make it possible for the mathematicians to intently examine his rich ideas.

In my book, I analyse Kummer's work and the more important methods used in the study of Fermat's last theorem; this book contains a long bibliography.

BIBLIOGRAPHY

? FERMAT, P. de. Ad problema XX commentarii in ultimam questionem Arithmeticorum Diophanti. Area trianguli rectanguli in numeris non potest esse quadratus. *Œuvres*, Vol. I, p. 340 (in Latin); Vol. III, p. 271-272 (in French). Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthiers-Villars, Paris, 1891, 1896.

1770 EULER, L. *Vollständige Anleitung zur Algebra.* Royal Acad. of Sciences, St. Petersburg, 1770. See also *Opera Omnia*, Ser. I, Vol. I, 484-489. Teubner, Leipzig-Berlin, 1915.

1823 LEGENDRE, A. M. Sur quelques points d'analyse indéterminée et particulièrement sur le théorème de Fermat. *Mém. de l'Acad. des Sciences, Institut de France*, *6* (1823), 1-60.

1828 DIRICHLET, G. L. Mémoire sur l'impossibilité de quelques équations indéterminées du 5^e degré. *J. reine u. angew. Math.*, *3* (1828), 354-375.

1830 LEGENDRE, A. M. *Théorie des Nombres* (3^e édition), Vol. II. Firmin Didot Frères, Paris, 1830. Reprinted by A. Blanchard, Paris, 1955.

1832 DIRICHLET, G. L. Démonstration du théorème de Fermat pour les 14^e puissances. *J. reine u. angew. Math.*, *9* (1832), 390-393.

1839 LAMÉ, G. Mémoire sur le dernier théorème de Fermat. *C.R. Acad. Sci. Paris*, *9* (1839), 45-46.

1840 LEBESGUE, V. A. Démonstration de l'impossibilité de résoudre l'équation $x^7 + y^7 + z^7 = 0$ en nombres entiers. *J. Math. Pures et Appl.*, *5* (1840), 276-279.

1847 CAUCHY, A. Mémoire sur les racines des équations algébriques à coefficients entiers et sur les polynômes radicaux. *C.R. Acad. Sci. Paris*, *24* (1847), 407-416. Reprinted in *Œuvres Complètes*, (1), 10, 231-239. Gauthier-Villars, Paris, 1897.

1847 CAUCHY, A. Mémoire sur diverses propositions relatives à la Théorie des Nombres. *C.R. Acad. Sci. Paris*, *24*, (1847), 177-183, Reprinted in *Œuvres Complètes*, (1), 10, 360-366. Gauthier-Villars, Paris, 1897.

1847 LAMÉ, A. Mémoire sur la résolution en nombres complexes de l'équation $A^n + B^n + C^n = 0$. *J. Math. Pures et Appl.*, *12* (1847), 172-184.

1852 GENOCCHI, A. Intorno all'espressioni generali di numeri Bernoulliani. *Annali di scienze mat. e fisiche, compilati da Barnaba Tortolini*, *3* (1852), 395-405.

1876 GAUSS, C. F. Zur Theorie der complexen Zahlen: (I) Neue Theorie der Zerlegung der Cuben. *Werke*, Vol. II, p. 389-391. Königl. Ges. d. Wiss. zu Göttingen, 1876.

1893 DEDEKIND, R. Supplement XI to the fourth edition of Dirichlet's *Vorlesungen über Zahlentheorie.* Vieweg, Braunschweig, 1893. Reprinted by Chelsea Publ. Co., New York, 1968.

1905 MIRIMANOFF, D. L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer. *J. reine u. angew. Math.*, *128* (1905), 45-68.

1910 HECKE, E. Über nicht-reguläre Primzahlen und den Fermatschen Satz. *Nachr. Akad. d. Wiss. zu Göttingen* (1910), 420-424.

1912 FURTWÄNGLER, P. Letzter Fermatschen Satz und Eisensteins'ches Reziprozitätsgesetzt. *Sitzungsber. Akad. d. Wiss. Wien, Abt. IIa*, *121* (1912), 589-592.

1915 JENSEN, K. L. Om talteoretiske Egenskaber ved de Bernoulliske tal. *Nyt Tidsskrift f. Math.*, *B*, *26* (1915), 73-83.

1922 VANDIVER, H. S. On Kummer's memoir of 1857 concerning Fermat's last theorem. *Bull. Amer. Math. Soc.*, *28* (1922), 400-407.

1926/1927/1930 HASSE, H. *Bericht über Neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper.* Jahrsber. d. Deutschen Math. Verein., 35 (1926), 1-55; 36 (1927), 233-311; supplementary volume 6, 204 pages. Reprinted in two volumes. Physica Verlag, Würzburg, 1965.

1926 VANDIVER, H. S. Summary of results and proofs concerning Fermat's last theorem. *Proc. Nat. Acad. Sci., U.S.A.*, *12* (1926), 106-109.

1932 SCHOLZ, A. Über die Beziehung der Klassenzahlen quadratischer Zahlkörper zueinander. *J. reine u. angew. Math.*, *166* (1932), 201-203.

1932 MORISHIMA, T. Über die Fermatsche Vermutung, VII. *Proc. Imp. Acad. Japan*, *8* (1932), 63-66.

1934 KRASNER, M. Sur le premier cas du théorème de Fermat. *C.R. Acad. Sci. Paris*, *199* (1934), 256-258.

1964 SIEGEL, C. L. Zu zwei Bemerkungen Kummers. *Nachr. Akad. d. Wiss. zu Göttingen, Math. Phys. Kl.*, *II* (1964), 51-57. Reprinted in *Gesammelte Abhandlungen*, Vol. III, 436-442. Springer-Verlag, New York, 1966.

1965 EICHLER, M. Eine Bemerkung zur Fermatsche Vermutung. *Acta Arithm.*, *II* (1965), 129-131, and 261.

1975 EDWARDS, H. M. The background of Kummer's proof of Fermat's last theorem for regular primes. *Arch. for History of Exact Sciences*, *14* (1975), 219-236.

1976 RIBET, K. A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$. *Invent. Math.*, *34* (1976), 151-162.

1977 TERJANIAN, G. Sur l'équation $x^{2p} + y^{2p} = z^{2p}$. *C.R. Acad. Sci. Paris*, *285* (1977), 973-975.

1978 WAGSTAFF, S. The irregular primes to 125000. *Math. Comp.*, *32* (1978), 583-592.

1979 RIBENBOIM, P. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York, 1979.

Finally, the *Collected Papers* of Kummer, E. E., have been edited by A. Weil and published by Springer-Verlag in 1975, in two volumes, of which the first one is devoted to the papers in number theory.

The articles of Kummer directly connected with Fermat's theorem are the following (pages refer to Volume I of the *Collected Papers*):

1837 (pages 135-141), 1844/1847 (pages 165-192),
1847 (pages 203-210), 1847 (pages 274-297), 1847 (page 298),
1850 (pages 299-322), 1850 (pages 323-335), 1850 (pages 336-344),
1851 (pages 363-484), 1857 (pages 631-638), 1857 (pages 639-672),
1870 (pages 919-944), 1874 (pages 945-954).

(Reçu le 23 septembre 1981)

P. Ribenboim

Queen's University
Kingston K7L 3N6
Ontario
Canada