Canad. Math. Bull. Vol. **20** (2), 1977

LECTURE—RECENT RESULTS ON FERMAT'S LAST THEOREM

BY
P. RIBENBOIM*

This text is an elaboration of a lecture delivered at the First Winter Meeting of the Canadian Mathematical Congress, December 1975. Subsequently, this same lecture was presented at various occasions, (Colloquium at Université Pierre et Marie Curie, in Paris; Seventh Iranian Mathematical Congress in Tabriz; Université de Paris-Sud à Orsay, Illinois Institute of Technology in Chicago, Colloquium at the University of Toronto, and at the University of Waterloo).

It has been known since ancient times that there exist integers x, y, z, all different from zero, such that $x^2+y^2=z^2$.

Fermat proved that if $n=4$ there does not exist integers x, y, z, all different from zero, and such that $x^4+y^4=z^4$.

Fermat claimed that the same holds for every exponent $n \geq 3$. This assertion, as yet unproved for all exponents n, is called "Fermat's last theorem" (FLT).

It is easy to see that it suffices to prove FLT for prime exponents $p>2$, (since it holds for $n=4$).

It trying to prove it, one is led to consider the following statement:

"There does not exist integers x, y, z, all not multiples of p, such that $x^p+y^p=z^p$." Or, in other words, if x, y, z are integers and $x^p+y^p=z^p$ then p divides xyz.

If this statement is true we say that the *first case of* FLT holds for the exponent p.

Before discussing the modern developments, it is perhaps worth mentioning very briefly the earlier results.

Euler and Gauss gave independent proofs of FLT for $n=3$. Legendre and Dirichlet settled the theorem for $n=5$ (around 1825). Dirichlet proved it for $n=14$ (in 1832). Lamé and Lebesgue gave proofs for $n=7$ in 1840. A false "proof" for an arbitrary exponent was proposed by Lamé. But the error was detected by Liouville and Dirichlet. The deficiency originated in the fact that the unique factorization theorem fails in general for cyclotomic integers. This led Kummer to deep studies of the arithmetic of cyclotomic fields, culminating

Received by the editors Feb 8, 1977

* Queen's University, Kingston, Ontario, Canada.

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

with his monumental theorem (1847–1850): FLT is true for every exponent which is a regular prime.

I shall return in more detail to Kummer's result and explain what is a regular prime.

All these early developments are rather well-known. So instead of continuing to describe them, I shall immediately turn to the recent advances. There has been considerable work on the subject—it is true of a rather diverse quality—so it is necessary to make a selection of the results. My purpose is to show the various angles of attack, the different techniques involved and to invoke important historical developments.

I'll now state 10 recent results and soon later I'll discuss how they were obtained.

(I) **Wagstaff (1976).** FLT holds for every prime exponent $p < 125000$.

(II) **Brillhart, Tonascia & Weinberger (1971).** The 1st case of FLT holds for every prime exponent $p < 3 \times 10^9$.

But the first case holds also for larger primes; in fact

(III) **The first case of FLT holds for the largest prime known today.**

The above results were on the optimistic side. But some mathematicians thought that there might be a counter-example. How large should be the smallest counter-example for a given exponent p?

(IV) **Inkeri proved in 1953.** If the 1st case fails for the exponent p, if x, y, z are integers, $0 < x < y < z$, $p \nmid xyz$, $x^p + y^p = z^p$, then

$$x > \left(\frac{2p^3 + p}{\log(3p)}\right)^p$$

And in the general case,

$$x > \frac{1}{2} p^{3p-4}$$

Moreover, Pérez Cacho proved in 1958 that in the first case, $y > \frac{1}{2}(p^2P + 1)^p$, where P is the product of all primes q such that $q - 1$ divides $p - 1$.

There might also be only finitely many solutions. In this respect:

(V) **Inkeri & Hyyrö proved in 1964.** (a) Given p and $M > 0$ there exist at most finitely many triples (x, y, z), such that $0 < x < y < z$, $x^p + y^p = z^p$, and $y - x$, $z - y < M$.

(b) There exist at most finitely many triples (x, y, z) such that $0 < x < y < z$, $x^p + y^p = z^p$, and x is a prime-power.

For each such triple, we have the effective majoration (and this is a very important new feature):

$$x < y < \exp \exp[2^p(p-1)^{10(p-1)}]^{(p-1)^2}$$

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

Another sort of result, this time for even exponents:

(VI) **Long showed in 1960 that:** if the last digit of n is 4 or 6 then there does not exist x, y, z, integers prime to n, such that $x^n + y^n = z^n$.

The possibility that FLT (or even its first case) holds for infinitely many prime exponents is still open.

In this respect we have:

(VII) **Rotkiewicz proved in 1965.** If Schinzel's conjecture on Mersenne numbers is true then there exist infinitely many primes p such that the first case of FLT holds for p.

The next results are intimately related with the class group of the cyclotomic fields $\mathbb{Q}(\zeta)$, where ζ is a primitive p^{th} root of 1.

(VIII) **Vandiver's theorem of 1934 states:** If the second factor h^+ of the class number of $\mathbb{Q}(\zeta)$ is not a multiple of p, then the first case holds for p.

(IX) **Skula showed in 1972.** If the p-Sylow subgroup of the class group of $\mathbb{Q}(\zeta)$ is cyclic then the 1^{st} case of FLT holds for p.

(X) **Brückner showed in 1975 that:** If the 1^{st} case fails for p, then the irregularity index of p, $ii(p) = \#\{k = 2,4,\ldots,p-3 \mid p$ divides the Bernoulli number $B_k\}$ satisfies

$$ii(p) > \sqrt{p} - 2.$$

Now, I shall explain the significance of these various theorems and computations.

(I) Obviously Wagstaff obtained his result with the most modern computers. But what is the theory behind it?

Kummer's theorem asserted that FLT holds for the prime exponents p which are regular. A prime p is said to be regular if p does not divide the class number h of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive p^{th} root of 1. Kummer showed that it is equivalent that p does not divide the first factor h^* of the class number. Since the computation of the class number, or even of its first factor, is rather difficult, and much more so, due to its rapid growth, with p, it was imperative to find a more amenable criterion. Kummer characterized the regular primes p by the condition:

$$p \nmid B_{2k} \quad \text{for} \quad 2k = 2,4,\ldots,p-3.$$

Here B_{2k} denotes a Bernoulli number. These are defined by the formal power series expansion

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

They may be obtained recursively; moreover if n is odd, $n \geq 3$ then $B_n = 0$.

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

The number of indices $2k$ such that $2 \leq 2k \leq p-3$ and $p \mid B_{2k}$ is called the irregularity index of p. The prime p is irregular if its irregularity index $ii(p) \geq 1$. By Kummer's theorem it suffices to consider the irregular primes.

Vandiver gave a practical criterion to determine whether p is irregular, by means of the congruence

$$\frac{4^{p-2k}+3^{p-2k}-6^{p-2k}-1}{4k} B_{2k} \equiv \sum_{p/6<a<p/4} a^{2k-1} \pmod{p}$$

The advantage of such a congruence is that it involves a sum of relatively few summands, contrary to the previous congruences. If the above congruence does not lead to a decision because the right-hand side and the left-hand factor are both multiples of p, then other similar congruences have to be used. Once it is known that p is irregular, the following criterion is used (Vandiver, 1954 and Lehmer, Lehmer & Vandiver, 1954):

Let p be an irregular prime, let $P = rp+1$ be a prime such that $P < p^2 - p$ and let t be an integer such that $t^r \not\equiv 1 \pmod{P}$. If $p \mid B_{2k}$, with $2 \leq 2k \leq p-3$ let

$$d = \sum_{n=1}^{(p-1)/2} n^{p-2k}$$

and

$$Q_{2k} = \frac{1}{t^{rd/2}} \prod_{a=1}^{(p-1)/2} (t^{ra}-1)^{a^{p-1-2k}}$$

If $Q_{2k}^r \not\equiv 1 \pmod{p}$ for all $2k$ such that $p \mid B_{2k}$, then FLT holds for the exponent p.

This criterion lends itself well to the computer.

In his extensive calculations, Wagstaff has also noted many facts about the irregular primes. The maximum irregularity found is 5. Moreover, if $x = 125000$:

$$\frac{\#\,(\text{irregular primes } p \leq 125000)}{\#\,(\text{primes } p \leq 125000)} \approx 0.39248 \approx 1 - \frac{1}{\sqrt{e}} = 0.39347$$

This confirms a heuristic prevision by Siegel (1964).

Let me recall now various interesting results about regular and irregular primes.

It is suspected that there exists infinitely many regular primes, but this has never been proved. On the other hand, Jensen proved in 1915 that there exist infinitely many irregular primes. Actually they are abundant in the following sense. Metsänkylä and Yokoi proved independently in 1975, extending work of Montgomery, that, given $N \geq 3$, if H is a proper sub-group of the additive group $\mathbb{Z}/N\mathbb{Z}$ then there exist infinitely many irregular primes p such that p modulo N does not belong to H.

On the other hand, in 1971 Metsänkylä obtained the puzzling result:. there exist infinitely many irregular primes p which satisfy either one of the congruences $p = 1 \pmod 3$, $p \equiv 1 \pmod 4$. But he couldn't decide whether in each one congruence class lies infinitely many irregular primes.

So it is rather startling that it is possible—and not too difficult—to show that there are infinitely many irregular primes, and, up to now, not that there are infinitely many regular ones, even though heuristically these are much more numerous.

Among the many conjectures—which should be difficult to prove—let me mention:

(1) there exist primes with arbitrarily large irregularity index

(2) there exist infinitely many primes with given irregularity index

(3) there exists a prime p and some index $2k$ such that $p^2 \mid B_{2k}$, $2 \leq 2k \leq p-3$.

(II) The fact that the first case holds for all prime exponents less that 3×10^9 depends on the scarcity of primes p satisfying the congruence $2^{p-1} \equiv 1 \pmod{p^2}$.

Fermat's little theorem says that if p is a prime and $p \nmid m$ then $m^{p-1} \equiv 1 \pmod p$. Hence the quotient $q_p(m) = (m^{p-1} - 1)/p$ is an integer. It is called the Fermat quotient of p with base m.

In 1909 Wieferich proved the following theorem:

If the first case of FLT fails for the exponent p, then p satisfies the stringent congruence $2^{p-1} \equiv 1 \pmod{p^2}$; or equivalently $q_p(2) \equiv 0 \pmod p$.

This theorem had a new feature, insofar that it gave a condition involving only the exponent p, and not a would-be solution (x, y, z) of Fermat's equation—as in most of the previous results. The original proof of Wieferich's theorem was very technical, based on the so-called Kummer congruences for the first case:

If $p \nmid xyz$ and $x^p + y^p + z^p = 0$, then for $2k = 2, 4, \ldots, p-3$, we have the congruences (for a real variable v)

$$\left[\frac{d^{2k} \log(x + e^v y)}{dv^{2k}}\right]_{v=0} \times B_{2k} \equiv 0 \pmod p$$

(as well as the similar congruences for (y, x), (x, z), (z, x), (y, z), (z, y)). These congruences were obtained with intricate considerations on the arithmetic of the cyclotomic field and transcendental methods (which, as a matter of fact, may be replaced by p-adic methods).

Thus, it suffices to show that $2^{p-1} \not\equiv 1 \pmod{p^2}$ to guarantee that the first case holds for p. For a few years no such p was found. Only in 1913 Meissner showed that $p = 1093$ satisfies $2^{p-1} \equiv 1 \pmod{p^2}$. The next prime satisfying this congruence was discovered by Beeger in 1922; it is $p = 3511$. Since then,

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

computations have been performed up to 3×10^9 and no other such prime has ever been found. Thus for all but these two primes the first case holds.

The handling of these exceptional primes was actually done by a similar criterion.

Indeed, in 1910 Mirimanoff gave another proof of Wieferich's theorem and also showed that if the first case fails for p then $3^{p-1}\equiv 1 \pmod{p^2}$. $p=1093$ and 3511 do not satisfy the above congruence.

Several more criteria of the same kind were successively obtained by various authors. In 1914 Frobenius and Vandiver showed that $q_p(5)\equiv 0 \pmod p$ and $q_p(11)\equiv 0 \pmod p$, if the first case fails for p. Successively, Pollaczek, Vandiver, Morishima proved that $q_p(m)\equiv 0 \pmod p$ must hold for all primes $m\leq 31$. Morishima claimed to have proved the same criterion up to $m=43$, however in 1948 Gunderson pointed out substantial gaps in the proof. Nevertheless, in the meantime, Rosser, Lehmer & Lehmer using the above criteria (up to $m=43$), and Bernoulli polynomials to estimate the number of lattice points in a certain simplex of the real vector space of 14 dimensions, gave the following well-known bounds:

If the first case fails for p then $p>252\times 10^6$. However, these computations were based on uncertain criteria. On the other hand, they have been superseded by the bound of 3×10^9, obtained by straight computer work.

(III) The largest prime known today is the Mersenne number $M_q=2^q-1$ where $q=19937$. It has 6002 digits. Its primality was discovered by Tuckermann in 1971, using the famous Lucas test for $q\equiv 1 \pmod 4$: M_q is prime if and only if M_q divides W_q. The numbers W_q are defined by recurrence: $W_2=-4$, $W_{n+1}=W_n^2-2$, so the sequence is -4, 14, 194, ...

But how was it possible to show that the first case holds for such a big exponent?

As a matter of fact, this is a consequence of Wieferich's criterion. It follows from a result which was proved successively by Mirimanoff, Landau, Vandiver, Spunar, Gottschalk. Namely:

Suppose that there exists m not a multiple of p, such that $mp=a\pm b$, where all the prime factors of a and of b are at most 31 (this depends on the Fermat quotient criteria). Then the first case holds for p. Therefore, it holds for all Mersenne primes $M_q=2^q-1$, as well as for many more numbers.

Does there exist an infinity of prime numbers p satisfying the property of the preceding proposition? This is an open problem.

In 1968 Puccioni proved:

If this set of primes is finite then for all primes $l\leq 31$, $l\not\equiv \pm 1 \pmod 8$ the set $M_l=\{q \mid l^{q-1}\equiv 1\ (q^3)\}$ is infinite.

Primes in M_l are very hard to find, but this doesn't preclude these sets being infinite.

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

(IV) The first lower bound for a counter-example to FLT was given by Grünert in 1856. He showed that if $0<x<y<z$ and $x^n+y^n=z^n$ then $x>n$. So it is useless to try to find a counter-example with small numbers. For example, if $n=101$ the numbers involved in any counter-example would be at least 102^{101}.

It was easy to improve this lower bound. Based on congruences of Carmichael (1913), if $x^p+y^p=z^p$, $0<x<y<z$ then necessarily $x>6p^3$.

But, with some clever manipulations Inkeri came to the lower bound already stated. Taking into account that the first case holds for all prime exponents $p<3\times 10^9$, then

$$x>\left(\frac{2\times 3^3\times 10^{27}+3\times 10^9}{\log(9\times 10^9)}\right)^{3\times 10^9}$$

This is a very large number; it has more than 80 billion digits!

Similarly, for the general case we may take $p=125000$, hence

$$x>\frac{1}{2}(125\times 10^3)^{4\times 10^5}$$

and this number has anyway more than 3 billion digits.

It is therefore safe to say that no counter-example to the theorem will ever be available. As a matter of comparison, I have inquired about some physical constants, as they have been estimated by the physicists.

For example, the radius of the known universe is estimated to be 10^{28} cms. The radius of the atomic nucleus, of the order of 10^{-13} cms. And the number of nuclei that may be packed in the universe, just about $(10^{28+13})^3=10^{123}$—a very modest number indeed!

But I should add that the above data are rather controversial, and I have quoted them only to underline the enormous disparity between the sizes of the candidates to be counter-example to FLT, and the reputedly largest physical constants.

This being said, mathematicians would better try to prove FLT, or at least some weak form of it.

(V) For example, it might be possible to show that the Fermat equation has at most finitely many solutions. It could even be that the number of solutions might be bounded by an effectively computable bound. I should warn however that this has not yet been proved.

It is only under a further restriction that a finiteness result was proved by Inkeri. He considered would-be solutions (x, y, z) such that the integers are not too far apart, more precisely $y-x<M$, and $z-y<M$, where $M>0$ is given in advance. Then the problem becomes actually one of counting integer solutions of an equation involving only 2 variables. For this purpose there are theorems of Siegel, or Landau, Thue, Roth, or similar ones. Actually Inkeri & Hyyrö used

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

the following version. Let m, n be integers, $\max\{m, n\} \geq 3$. Let $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$, with distinct roots. If a is an integer, $a \neq 0$, then the equation $f(X) = aY^m$ has at most finitely many solutions in integers.

With this theorem they proved the statement (a). Concerning (b), I wish to mention that it answers in part a conjecture of Abel (1823).

Abel conjectured that if $x^p + y^p + z^p = 0$ (with non-zero integers x, y, z) then, at any rate, x, y, z cannot be prime-powers. I suppose that Abel might have in mind a procedure, which would allow to produce from a non-trivial solution (x, y, z) another one (x_1, y_1, z_1), where the minimum number of prime factors of the integers x_1, y_1, z_1 is strictly smaller than it was for x, y, z. In this situation he would "descend" on this number, until finding a solution with some prime-power integer—and if this turned out to be impossible, he would have proved FLT.

Up to now Abel's conjecture is not completely settled. Sauer in 1905, Mileikowski in 1932 obtained some results. In 1954 Möller proved:

If $x^n + y^n = z^n$, $0 < x < y < z$, if n has r distinct odd prime factors then z, y have at least $r+1$ distinct prime factors, while x has at least r such factors. If $n = p$ is a prime, this tells that y, z cannot be prime-powers. Moreover, if p does not divide xyz, then x also cannot be a prime power (as proved by Inkeri in 1946). It remains only to settle the case $p \mid xyz$, and to show that x is not a prime-power.

For the moment, Inkeri succeeded in proving that there are at most finitely many triples (x, y, z), as above, where x is a prime-power. Using the methods of Baker, which give effective upper bounds for the integral solutions of certain diophantine equations, Inkeri showed, as we stated, that

$$x < y < \exp \exp[2^p(p-1)^{10(p-1)}]^{(p-1)^2}$$

I pause now to indicate other very interesting use of Baker's estimations.

The famous Catalan problem is the following: to show that the only solution (x, y, m, n) of the equation $x^m - y^n = 1$ is $x = 3$, $m = 2$, $y = 2$, $n = 3$.

This problem is still open. However, with Baker's methods, Tijdeman has proved that there are at most finitely many solutions, which are effectively bounded.

Closely related is the following conjecture, which is a generalization of a theorem of Landau (published in his last book of 1959):

Let $a_1 < a_2 < \cdots$ be the increasing sequence of all integers which are proper powers (i.e., squares, cubes, etc...) Then $\lim_{n\to\infty}(a_{n+1} - a_n) = \infty$.

In Landau's result, he considered two fixed exponents m, n and the sequence of *mth* powers and *nth* powers.

(VI) Now I turn to a much more elementary result.

In his very first paper on Fermat's problem, published in 1837, Kummer

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

considered Fermat's equation with exponent $2n$, where n is odd. And he showed that if it has a non-trivial solution, $x^{2n}+y^{2n}=z^{2n}$, with $gcd(n, xyz)=1$ then $n\equiv 1 \pmod 8$.

So, there exists infinitely many primes p such that the first case is true for the exponent $2p$.

Kummer's result was rediscovered several times. It was also improved. For example, in 1960 Long showed that if $gcd(n, xyz)=1$, $x^{2n}+y^{2n}=z^{2n}$ then $n\equiv 1$ or $49 \pmod{120}$. Some more elementary manipulation implies if $m\equiv 4$ or $6 \pmod{10}$ then $X^m+Y^m=Z^m$ cannot have solution (x, y, z), with $gcd(m, xyz)=1$.

(VII) Schinzel's conjecture has been supported by numerical evidence. Up to now, it has never been found a square factor for any Mersenne number. Moreover if p^2 divides a Mersenne number then $p>9\times 10^8$.

Rotkiewicz's theorem states that the truth of Schinzel's conjecture implies that there exist infinitely many primes p such that $2^{p-1}\not\equiv 1 \pmod{p^2}$. Hence by Wieferich's theorem, there would exist infinitely many primes p for which the first case holds. I believe, however, that the proof of this last statement, and the proof of Schinzel's conjecture seem equally difficult.

(VIII) To explain well the meaning of Vandiver's result, it is appropriate to return to Kummer's monumental theorem:

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

By definition, p is a regular prime if p does not divide the class number $h=h(p)$ of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive *pth* root of 1. As I have already mentioned, Kummer was led to study the arithmetic of cyclotomic fields, to take care of the phenomenon of non-unique factorization into primes. To recover such uniqueness Kummer created the concept of "ideal numbers". Later Dedekind interpreted these ideal numbers essentially as what we know today as ideals. However, it should be said that Kummer ideal numbers were in fact today's divisors. Besides the ideal numbers, he considered of course the actual numbers, namely the elements of the cyclotomic field. For the ideal numbers the unique factorization theorem was proved true. Ideal numbers were put in an equivalence class when one is the product of the other by an actual number. Kummer showed that the number of such equivalence classes is finite—it is called the class number of the cyclotomic field and usually denoted by h.

Moreover, Kummer indicated precise formulas for the computation of h. He wrote $h=h^*h^+$ where

$$h^*=\frac{1}{(2p)^{(p-3)/2}}\,|G(\eta)G(\eta^3)\dots G(\eta^{p-2})|$$

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

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

In the above formulae, η is a primitive $(p-1)th$ root of 1, g is a primitive root modulo p, for each j, he defines g_j by $1 \leq g_j \leq p-1$ and $g_j \equiv g^j \pmod p$, moreover $G(X) = \sum_{j=1}^{p-2} g_j X^j$, and R is the regulator of the cyclotomic field, which is a certain invariant linked to the so-called units of the field.

h^* is called the first factor, while h^+ is the second factor of the class-number.

Kummer proved that h^*, h^+ are integers—rather an unpredictable fact, due to the defining expressions. Actually, he recognized h^+ as being the class number of the real cyclotomic field $\mathbb{Q}(\zeta+\zeta^{-1})$. He gave also the following interpretation of h^+. Let U be the group of units of $\mathbb{Q}(\zeta)$, i.e., all $\alpha \in \mathbb{Z}[\zeta]$ such that there exists $\beta \in \mathbb{Z}[\zeta]$ such that $\alpha\beta = 1$. Let U^* denote the set of those units which are real positive numbers. For every k, $2 \leq k \leq (p-1)/2$, let $\delta_k = \sqrt{(1-\zeta^k)/(1-\zeta) \times (1-\zeta^{-k})/(1-\zeta^{-1})}$, so δ_k is a real positive unit of $\mathbb{Q}(\zeta)$. Let V be the subgroup of U^* generated by all these $(p-3)/2$ "circular" units. Kummer showed that $h^+ = (U^* : V)$, the index of V in U^*.

Moreover, he proved that if p does not divide h^* then p does not divide h^+. Therefore p is a regular prime if and only if p does not divide h^*. Hence, he proceeded to compute h^* for all primes $p \leq 163$ and he found the following irregular primes $p = 37, 59, 67, 101, 131, 149, 157$. Based on his computations, he conjectured that, asymptotically, the first factor $h^* = h^*(p)$ of the class number grows as

$$h^*(p) \sim \frac{p^{(p+3)/4}}{2^{(p-3)/2}\pi^{(p-1)/2}}$$

This conjecture, which agrees with recent numerical evidence, has yet to be proved. The best result in this direction is due to Siegel (1964) who proved:

$$\log h^*(p) \sim \frac{p}{4} \log p.$$

More recently, in a still unpublished paper, Masley & Montgomery showed that if $p \geq 200$ then

$$(2\pi)^{-p/2} p^{(p-25)/4} \leq h^*(p) \leq (2\pi)^{-p/2} p^{(p+31)/4}$$

Concerning the growth of the first factor Ankeny & Chowla proved in 1951 that there exists p_0 such that $h^*(p)$ is monotonically increasing for $p \geq p_0$. It is nowadays conjectured by Inkeri and Lepistö that one may take $p_0 = 19$.

The second factor is much more difficult to handle, since it is tied with the inner structure of the group of units. It was Kummer who already found the first example. $p = 163$, for which $h^+(p)$ is even. However not many more examples were known before 1965, when Ankeny, Chowla & Hasse, using a lemma of Davenport and class field theory, proved: if q is a prime, $n > 1$, if $p = (2qn)^2 + 1$ is a prime then $h^+(p) > 2$.

If $p \mid h^*(p)$ but $p \nmid h^+(p)$ the cyclotomic field is called properly irregular. It is called improperly irregular if $p \mid h^+(p)$ hence also $p \mid h^*(p)$. It is not known whether there exist improperly irregular cyclotomic fields.

Vandiver, Pollaczek, Dénes and Morishima studied irregular fields. In 1934 Vandiver proved that the first case holds for all properly irregular exponents p.

(IX) Skula's result was obtained by a deeper probing of the group of ideal classes. A simpler proof was given by Brückner.

(X) To explain the scope of the latest of Brückner's theorems, let Γ be the ideal class group of (ζ), h the class number. If p is irregular then $\Gamma \neq p\Gamma$ so $\gamma_p = \dim(\Gamma/p\Gamma) \geq 1$ (when $\Gamma/p\Gamma$ is considered as a vector space over the field with p elements). In 1965, Eichler proved that if the first case fails then $\gamma_p > \sqrt{p}-2$. However, the computation of γ_p is difficult. Brückner succeeded in relating the above dimension γ_p with the irregularity index $ii(p)$, and proved that if the first case fails for p then more than $\sqrt{p}-2$ Bernoulli numbers B_{2k} (with $2 \leq 2k \leq p-3$) are multiples of p.

Historically, this fits into a series of classical results. Cauchy (1841) and Genocchi (1862) proved that if the first case fails for p then B_{p-3} is a multiple of p. In 1857, Kummer showed that both B_{p-3} and B_{p-5} must be multiples of p. Later, Mirimanoff showed that B_{p-7} and B_{p-9} must also be multiples of p.

In 1934 Krasner proved quite an interesting result: there exists a prime p_0 (which could be effectively computed) such that if $p \geq p_0$ and if the first case of FLT fails for p, then the k Bernoulli numbers $B_{p-3}, B_{p-5}, \cdots B_{p-(2k+1)}$ are all multiples of p; in this statement $k = [\sqrt[3]{\log p}]$. Thus, in the event of failure of the first case of FLT a reasonably large number of successive Bernoulli numbers would be multiples of p. Even though this number is essentially smaller than the one indicated by Brückner's theorem, in this case these Bernoulli numbers are successive. This is a most unlikely conclusion, pointing out to the fact that the first case of Fermat's theorem may well be true.

Bibliography

Abel, N. H., *Extraits de quelques lettres à Holmböe* (1823). Werke, vol. **2,** pages 254–255.

Ankeny, N. C., Chowla, S. and Hasse, H., *On the class number of the maximal real subfield of a cyclotomic field.* J. f. d. reine u. angew. Math., **217,** 1965, pages 217–220.

Ankeny, N. C. & Chowla, S., *The class number of the cyclotomic field.* Can. J. Math. **3,** 1951, pages 486–494.

Bachmann, P., *Niedere Zahlentheorie.* Teubner, Leipzig, 1910 (reprinted Chelsea, New York, 1966).

——— *Das Fermatproblem in seiner bisherigen Entwicklung.* Walter de Gruyter, Berlin, 1919.

Beeger, N. G. W. H., *On a new case of the congruence* $2^{p-1} \equiv 1(p^2)$. Messenger of Mathematics, **51,** 1922, pages 149–150.

Borevich, Z. I. and Shafarevich, I. R., *Number Theory.* Academic Press, New York, 1966.

Brillhart, J., Tonascia, J. and Weinberger, R., *On the Fermat quotient.* Computers in Number Theory, pages 213–222. Academic Press, New York, 1971.

Brückner, H., *Zum Beweis des ersten Falles der Fermatschen Vermutung für pseudoreguläre Primzahlen* (*Bemerkungen zur vorstehender Arbeit von L. Skula*). J.f.d. reine u. angew. Math., **253,** 1972, pages 15–18.

Carmichael, R. D., *Note on Fermat's last theorem.* Bull. Amer. Math. Soc., Vol. **19,** 1913, pages 233–236.

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

Cauchy, A., *Mémoire sur diverses propositions relatives à la théorie des nombres.* C.R. Acad. Sci. Paris, **25,** 1847, pages 177–183 also at Oeuvres Complètes (1), 10, pages 360–366.

Dénes, P., *Uber irreguläre Kreiskörper.* Publ. Math. Debrecen, **3,** 1954, pages 17–23.

Eichler, M., *Eine Bemerkung zur Fermatschen Vermutung.* Acta Arith., **11,** 1965, pages 129–131 (Errata) page 261.

Frobenius, G., *Über den Fermatschen Satz, III. Sitzungsberichte d.Berliner Akad.* d. Wiss, **22,** 1914, pages 129–131 (also Collected Works, vol. 3, page 648–676; Springer Verlag, Berlin, 1968).

Genocchi, A., *Intorno all' expressioni generali di numeri Bernoulliani.* Annali di scienze mat. e fisiche, computate da Barnaba Tortolini, **3,** 1852, pages 395–405 (Roma).

Gottschalk, E., *Zum Fermatschen Problem.* Math. Annalen. **115,** 1938, pages 157–158.

Grünert, J. A., Archiv. Math..Phys., **26,** 1856, pages 119–120.

Gunderson, N. G., *Derivation of Criteria for the First Case of Fermat's Last Theorem and the Combination of these Criteria to produce a New Lower Bound for the Exponent.* Thesis, Cornell University, 1948.

Hilbert, D., *Die Theorie der algebraischen Zahlkörper.* Jahresbericht der Deutschen Mathematikervereinigung, **4,** 1897, pages 175–546. Also in Gesammelte Abhandlungen, Vol. **I,** Springer, Berlin, 1932 (reprinted Chelsea Publ. Co. New York, 1965).

Inkeri, K., *Untersuchungen über die Fermatsche Vermutung.* Annales Acad. Sci. Fennicae, Ser. A, I, Nr **33,** 1946, pages 1–60.

——— *Abschätzungen für eventuelle Lösungen der gleichung im Fermatschen Problem.* Ann. Univ. Turku, Ser. A., 1953, Nr. **1,** pages 3–9.

Inkeri, K. and Hyyrö, S., *Uber die Anzahl der Lösungen einiger Diophantischer Gleichungen.* Annales Univ. Turku, Ser. A., 1964, Nr. **78,** pages 3–10.

Jensen, K. L., *Om talteoretiske Egenskaber ved de Bernoulliske tal.* Nyt Tidsskrift f. Math., **26,** B, 1915, pages 73–83.

Krasner, M., *Sur le premier cas du théorème de Fermat.* C. R. Acad. Sci. Paris, 199, 1934, pages 256–258.

Kummer, E. E.,(*) *De aequatione* $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$ *per numeros integros resolvenda.* J.f.d. reine u. angew. Math., **17,** 1837, pages 203–209.

——— *Beweis des Fermat's chen Satzes der Unmöglichkeit von* $x^\lambda+y^\lambda=z^\lambda$ *fur eine unendliche Anzahl Primzahlen* λ. Berlin. Monatsber. 1847, pages 132–139, 140–141, 305–319. Reprinted in Collected Papers, vol. **I,** pages 274–297.

——— *Bestimmung der Anzahl nicht äquivalenter Classen für die aus* λ*-ten Wurzel der Einheit gebildeten complexen Zahlen und die Idealen factoren derselben.* J.f. reine u. angew. Math., **40,** 1850, pages 93–116.

——— *Zwei besondere untersuchungen über die Classen-Anzahl und über die Einheiten der aus* λ*-ten Würzeln der Einheit gebildeten complexen Zahlen.* J.f. reine u. angew Math., **40,** 1850, pages 117–129.

——— *Allgemeiner Beweis des Fermat'schen Satzes, daß die Gleichung* $x^\lambda+y^\lambda=z^\lambda$ *durch ganzen Zahlen unlösbar ist.* J.f.d. reine u. angew Math., **40,** 1850, pages 130–138.

Kummer, E. E., *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda=1$ *gebildeten complexen Zahlen, fur den Fall daß die Klassenzahl durch* λ *theilbar ist, nebst Anwendungen derselben auf einen weiteren Beweis des letztes Fermatschen Lehrsatzes.* Math. Abhandl. d. Königl. Akad. d. Wissenschaften, 1857, pages 41–74.

Kummer, E. E., *Über diejenigen Primzahlen* λ *für welche die Klassenzahl der aus* λ*-ten Einheitswurzeln gebildeten complexen Zahlen durch* λ *theilbar ist.* Monatsber. Königl. Preuss. Akad. d. Wiss. zu Berlin. 1874 pages 239–248.

Lehmer, D. H. & E., *On the first case of Fermat's last theorem.* Bull. Amer. M. Soc. **47,** 1941, pages 139–142.

Lehmer, D. H., Lehmer, E., Vandiver, H. S., *An application of high speed computing to Fermat's last theorem.* Proc. Nat. Acad. Sci. U.S.A. **40,** 1954, pages 25–33.

(*) The papers of Kummer are now easily accessible in the volume 1 of his Collected Papers" edited by A. Weil, Springer Verlag, Berlin, 1975.

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

Long, L., *A note on Fermat's theorem.* Math. Gaz., **44,** 1960, pages 261–262.

Meissner, W., *Uber die Teilbarkeit von 2^P-2 durch das Quadrat der Primzahl $p = 1093$.* Sitzungsberichte Akad. d. Wiss, Berlin, 1913, pages 663–667.

Metsänkylä, T., *Note on the distribution of irregular primes.* Ann. Acad. Sci. Fenn., Ser. A I 492, 1971, 7 pages.

——— *Distribution of irregular prime numbers.* J. reine u. angew. Math, **282,** 1976, pages 126–130.

Mileikowsky, E. N., *Elementarer Beitrag zur Fermatschen Vermutung.* J.f.d. reine u. angew. Math. **166,** 1932, pages 116–117.

Mirimanoff, D., *L'equation indéterminée $x^l+y^l+z^l=0$ et le critérium de Kummer.* J.f. reine u. angew. Math., **128,** 1905, pages 45–68.

Mirimanoff, D., *Sur le dernier théorème de Fermat et le critérium de M. A. Wieferich.* Enseignement Math., 1909–11, pages 455–459.

Mirimanoff, D., *Sur le dernier théorème de Fermat.* Comptes Rendus Acad. Sci. Paris, **150,** 1910, pages 204–206.

Möller, K., *Untere Schränke fur die Anzahl der Primzahlen, aus denen x, y, z des Fermatschen Gleichung $x^n+y^n=z^n$ bestehen muss.* Math. Nach. **14,** 1955, pages 25–28

Montgomery, H. L., *Distribution of irregular primes.* Illinois J. Math., **9,** 1965, pages 553–558.

Morishima, T., *Über den Fermatschen Quotienten.* Japanese J. of Math., **8,** 1931, pages 159–173.

——— *Über die Einheiten und Idealklassen des Galoisschen Zahlkörpers und die Theorie des Kreiskörpers der l^2-ten Einheitswurzeln.* Jap. Journal of Math., **10,** 1933, pages 83–126.

Pérez-Cacho, L., *On some questions in the theory of numbers (in Spanish).* Rev. Mat. Hisp. Amer. **(4), 18,** 1958, pages 10–27 and 113–124.

Pollaczek, F., *Über den grössen Fermat'schen Satz.* Sitzungsber. Akad. Wien, **126,** Abt. IIa, 1917, pages 45–59.

——— *Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswürzeln.* Math. Z., **21,** 1924, pages 1–37.

Puccioni, S., *Un teorema per una resoluzioni parziali del famoso problema di Fermat.* Archimede **20,** 1968, pages 219–220.

Rosser, J. B., *A new lower bound for the exponent in the first case of Fermat's last theorem.* Bull. Amer. Math. Soc. **46,** 1940, pages 299–304.

Rotkiewicz, A., *Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n tels ques $n^2 \mid 2^n-2$.* Matematicky Vesnik, **2,** 17, 1965, pages 78–80.

Sauer, R., *Eine polynomische Verallgemeinerung des Fermatschen Satzes.* Dissertation Giessen, 1905.

Siegel, C. L., *Zu zwei Bermerkungen Kummers.* Nachr. Akad. Wiss. Göttingen. Math. Phys. Kl. **II,** 1964, pages 51–57. Gesammelte Abhandlungen vol. **III,** Springer Verlag, New York, 1966, pages 436–442.

Sierpiński, W., *A Selection of Problems in the Theory of Numbers.* Macmillan, New York, 1964.

Skula, L., *Eine Bemerkung zu dem ersten Fall der fermatschen Vermutung.* J.f.d. reine u. angew. Math., **253,** 1972, pages 1–14.

Spunar, V. M., *On Fermat's last theorem, III.* J. Wash. Acad. Sci., **21,** 1931, pages 21–23.

Stafford, Elizabeth and Vandiver, H. S. *Determination of some properly irregular cyclotomic fields.* Proc. Nat. Acad. Sci., **16,** 1930, pages 139–150.

Tuckerman, B., *The 24th Mersenne prime.* Proc. Nat. Acad. Sci., 1971, pages 2319–2320 (I.B.M. Research).

Vandiver, H. S., *Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's last theorem.* J. reine u. angew. Math. **144,** 1914, pages 314–318.

——— *A note on Fermat's last theorem.* Trans. A.M.S., **15,** 1914, pages 202–204.

——— *Fermat's last theorem and the second factor in the cyclotomic class number.* Bull. Amer. Math. Soc. **40,** 1934, pages 118–126.

——— *On basis systems for groups of ideal classes in a properly irregular cyclotomic field.* Proc. Nat. Acad. Sci., **25,** 1939, pages 586–591.

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press

——— *On the composition of the group of ideal classes in a properly irregular cyclotomic field.* Monatshefte f. Math. u. Phys., **48,** 1939, pages 369–380.

——— *Examination of methods of attack of the second case of Fermat's last theorem.* Proc. Nat. Acad. Sci., **40,** 1954, pages 732–735.

Wagstaff, S. S., *Fermat's last theorem is true for any exponent less than 125000.* Communicated by letter.

——— *Fermat's last theorem is true for any exponent less than 100000.* Notices A.M.S., **23,** 1975, page A-53, abstract 731–10–35.

Wieferich, A., *Zum letzten Fermat'schen Theorem.* J. reine u. angew. Math. **136,** 1909, pages 293–302.

Yokoi, H., *On the distribution of irregular primes.* J. Nb. Theory **7,** 1975, pages 71–76.

DEPT. OF MATH
QUEEN'S UNIVERSITY
KINGSTON, ONTARIO.

https://doi.org/10.4153/CMB-1977-036-2 Published online by Cambridge University Press