NOTES ON FERMAT'S LAST THEOREM IV

ceNTRe
Macquarie University
NSW 2109 Australia

A. J. van der Poorten

Centre for Number Theory Research, Macquarie University

Again in 1850 the Académie des Sciences de Paris offered a golden medal and a prize of 3000 *Francs to the mathematician who would solve Fermat's problem.*

In 1856 it determined to withdraw the question from competition but to award the medal to Kummer 'for his beautiful researches on the complex numbers composed of roots of unity and integers'.

P. Ribenboim, in part translating Cauchy.

All we really will need about ideal numbers is that, according to their purpose, there is unique factorisation into ideals in every number field. But there is a bonus. An element α corresponds to the *principal* ideal (α), and so do its *associates* $\eta\alpha$, where η is any unit. Thus ideals hide units, as it were, which is great. Of course, *vice versa* the ideal (α) corresponds to one or other of the *associates* $\eta\alpha$ of α, where η is some unit; that's not so good. But Kummer copes.

The regular case: An odd prime p is *regular* if, roughly speaking, one can do common sense arithmetic — as regards Fermat's Last Theorem — in the field $\mathbb{Q}(\zeta)$, where $\zeta = \zeta_p$ is a primitive p-th root of unity. In his first arguments of 1847 Kummer works subject to the assumptions that the p-th power of an ideal can be treated as a number in the field, and the truth of a lemma concerning p-th powers of units that I mention below. A little later he found that both of these conditions follow from the regularity of p.

We recall that in the p-th cyclotomic field the integers are $a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, with the $a_i \in \mathbb{Z}$.

Our object is to demonstrate the impossibility of

$$x^p + y^p + z^p = 0$$

in nonzero rational integers x, y and z.

Case I p regular (Kummer). We begin with the first case of the FLT, thus when $p \nmid xyz$.

Then

$$x^p + y^p = \prod_j (x + \zeta^j y) = -z^p ,$$

1991 *Mathematics Subject Classification.* 11D41, 11-01.

Work supported in part by grants from the Australian Research Council and a research agreement with Digital Equipment Corporation.

and the factors $x+\zeta^j y$ are relatively prime, since their only possible common divisor is a factor of p, whilst $p\nmid z$. Hence each is a p-th power — technically, each *principal ideal* $(x+\zeta^j y)$ is the p-th power of an ideal of $\mathbb{Q}(\zeta)$. When p is regular it follows that we have

$$x+\zeta y=\eta\alpha^p\,,$$

where α is an integer, and η a unit of $\mathbb{Q}(\zeta)$ [compare $36=-4\cdot-9$, and note that -4 is a square times a unit -1, not just a square].

The difficulty is that $\mathbb{Q}(\zeta)$ has nontrivial units η. But Kummer succeeded in proving that $\eta/\overline{\eta}$ is always a p-th root of unity, ζ^{2a}, say.

Now if

$$\alpha=a_0+a_1\zeta+\cdots+a_{p-2}\zeta^{p-2}\quad\text{then}\quad\alpha^p\equiv a_0+a_1+\cdots+a_{p-2}\pmod p\,,$$

so $\alpha^p\equiv\overline{\alpha}^p\pmod p$, and we have

$$x+\zeta y\equiv(x+\overline{\zeta}y)\zeta^{2a}\pmod p\quad\text{or}\quad x(1-\zeta^{2a})+y(\zeta-\zeta^{2a-1})\pmod p\,.$$

But the latter is impossible if $p\nmid xy$, unless $2a\equiv1\pmod p$, in which case $p\mid x-y$. But then, by symmetry, we can also establish $p\mid y-z$ and $p\mid z-x$, so

$$0=x^p+y^p+z^p\equiv3x^p\equiv3x\pmod p\,,$$

whence $p\mid x$ if $p>3$, and that is a contradiction.

Finally, for completeness, FLT I with $p=3$ is impossible by Sophie Germain. One need only note that all cubes not divisible by $7=2\cdot3+1$ are $\equiv\pm1\pmod 7$.

Case II p regular (Kummer). Suppose, without loss of generality, that $p\mid z$, and put $\lambda=1-\zeta$. Recall that the significance of λ is that the principal ideal (λ) satisfies $(\lambda)^{p-1}=(p)$.

Suppose also that we already have the Case I result for integers α, β, γ of $\mathbb{Q}(\zeta)$, thus that there is no nontrivial solution of

$$\alpha^p+\beta^p+\gamma^p=0\quad\text{if}\quad(p,\alpha\beta\gamma)=1\,.$$

We consider the apparently more general equation

$$\alpha^p+\beta^p=\varepsilon\lambda^{np}\gamma^p\,,$$

with ε a unit, and α, β, γ nonzero integers of $\mathbb{Q}(\zeta)$. We will use descent on n, and so may suppose that α and β are prime to λ.

Firstly, one remarks that we may further suppose that α and β each have the property of being congruent to a rational integer modulo λ^2. The idea is that, since, for example, we are only given α^p, there is no loss in replacing α by $\zeta^k\alpha$.

[Since $\zeta=1-\lambda$, we have $\zeta^k\equiv1-k\lambda\pmod{\lambda^2}$. So if $\alpha\equiv l+m\lambda\pmod{\lambda^2}$ then

$$\zeta^k\alpha\equiv(1-k\lambda)(l+m\lambda)\equiv l+(m-lk)\lambda\pmod{\lambda^2},$$

and it suffices to choose k so that $lk \equiv m \pmod p$.]

A major Hilfsatz (Kummer's lemma) that Kummer will need is the following: *Let η be a unit of $\mathbb{Q}(\zeta)$ and suppose there is a rational integer a so that*

$$\eta \equiv a \mod \lambda^p .$$

Then η is the p-th power of a unit of $\mathbb{Q}(\zeta)$.

We can rewrite our equation in terms of ideals as

$$\prod_{r=0}^{p-1}(\alpha + \zeta^r\beta) = (\lambda)^{np}(\gamma)^p .$$

One notices that the ideals on the left do each have a common factor (λ), and that $\lambda \mid \alpha+\beta$ implies $\lambda^2 \mid \alpha+\beta$, so $n > 1$. Any other common factor $\mathfrak{d}$, say, must be a common factor of (α) and (β). For the rest, the ideals on the left must be p-th powers. So we have

$$(\alpha + \zeta^r\beta) = \mathfrak{d}(\lambda)\mathfrak{a}_r^p \quad \text{and} \quad (\alpha+\beta) = \mathfrak{d}(\lambda)^{p(n-1)+1}\mathfrak{a}_0^p .$$

The point is that the ideals $\mathfrak{a}^p$ may be viewed just as p-th powers of integers of $\mathbb{Q}(\zeta)$. Now consider the identity (known, somehow, in the transcendence trade as 'Siegel's identity')

$$(\zeta - \overline{\zeta})(\alpha+\beta) + (\overline{\zeta} - 1)(\alpha + \zeta\beta) + (1-\zeta)(\alpha + \overline{\zeta}\beta) = 0 .$$

After dividing by λ we have integers α'', β' and γ' so that

$$\varepsilon'\lambda^{p(n-1)}\gamma'^p = \beta'^p + \varepsilon''\alpha''^p$$

for units ε' and ε''. But, in effect by Fermat's (little) theorem, a p-th power of an integer of $\mathbb{Q}(\zeta)$ is a rational integer mod p, so ε'' is a rational integer mod p. Thus, and here we invoke Kummer's lemma, ε'' is the p-th power of some unit. Hence we have an integer α' in $\mathbb{Q}(\zeta)$ so that

$$\varepsilon'\lambda^{p(n-1)}\gamma'^p = \beta'^p + \alpha'^p ,$$

contradicting the minimality of n.

About cyclotomic fields. The class number h of a number field measures the extent to which unique factorisation fails; technically h is the *order* of the *group* of ideal *classes*, that is, of ideals modulo the class of *principal* ideals. A cyclotomic field $\mathbb{Q}(\zeta_p)$ is said to be *regular* if $p \nmid h$.

It has been known for a long while (Jensen 1915) that there are infinitely many irregular primes. Curiously, since heuristically the majority of primes are regular, it is not known that there are infinitely many regular primes.

The class number h^+ of the *real* cyclotomic field $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ is a divisor of h. It also happens that $h^+=[E:E_0]$ is the *index* of the subgroup of the units of $\mathbb{Q}(\zeta_p)$ generated by the *real cyclotomic units*

$$\left|\frac{1-\zeta^r}{1-\zeta}\right| = \frac{\sin r\pi/p}{\sin \pi/p} \qquad r=2,3,\dots,\tfrac{1}{2}(p-1)$$

in the group E of positive real units of $\mathbb{Q}(\zeta)$.

Kummer showed that if $p \mid h^+$ then $p \mid h_* = h/h^+$. Thus whenever $p \mid h$ certainly $p \mid h_*$. Kummer found a criterion for $p \mid h_*$ that could be reasonably conveniently checked, at least for small p, say less than 100. It is, I believe, still not known whether in fact ever $p \mid h^+$.

To be precise, Kummer showed that if $p \mid h_*$ then p divides (the numerator of) a Bernoulli number B_{2k} with $2 \le 2k \le p-3$. The irregular primes less than 100 are 37, 59 and 67 (for example, $37 \mid B_{32}$ and $59 \mid B_{44}$).

By 1857 had completed an analysis of the irregular case to an extent that allowed him to deal with the cases for which p divides at most one of the numbers B_2, B_4, $\dots$, B_{p-3}, thereby proving the FLT beyond exponent $n=100$.

I don't see much point here in struggling to explain the calculations which Kummer has to carry out, other than to say that in 1850 Kummer shows that $p \mid h_*$ if and only if there is some integer k with $1 \le k \le (p-3)/2$, so that p^2 divides the sum $\sum_{j=1}^{p-1} j^{2k}$. This explains the appearance of the Bernoulli numbers.

However, by shying away from technicalities and gory details, I do threaten to miss the point of Kummer's contributions to mathematics. Sure, the ancients are a little hard to read, because of poor notation and conventions now strange to us, because they find some things, now easy to us, difficult; and, I guess, because they gloss over some things we now find difficult. And to top that off, they often fail to write in American English. It was no great surprise to hear John Coates say, at the time of the Coates–Wiles work on the Birch–Swinnerton-Dyer conjectures in the complex multiplication case, that core ideas had come from reading Kummer (the context was, I think, remarks in praise of Kurt Mahler — who would admonish us to read the masters). Some years later, Thaine's contributions could even be recognised by me as an ingenious transfer of Kummer's ideas from the cyclotomic to the elliptic case. Indeed, Kummer introduced p-adic analysis some sixty years before Hensel.

Specifically, it had been known since 1840 by work of Clausen and of von Staudt that if $k \ge 1$ then $B_{2k}+\sum_{(p-1)|2k} 1/p$ is a rational integer. Here and in the sequel p denotes only prime numbers. It follows that if $p-1 \mid 2k$ then $pB_{2k} \equiv -1 \pmod{p}$. Kummer proves that if $p-1 \nmid k$ then p does not divide the denominator of B_k/k, and that if, further, $k \equiv k' \pmod{p^n}$ then $(1-p^{k-1})B_k/k \equiv (1-p^{k'-1})B_{k'}/k'$ $\pmod{p^{n+1}}$. These congruences were just mysterious oddities until Kubota and Leopoldt interpreted them in 1964 in terms of p-adic interpolation of the Riemann ζ-function. And so, on to p-adic L-functions. Thus, after all, in the work of Kummer we find the genesis of the eventual solution of Fermat's Last Theorem.

Most of this material comes from lectures I prepared c. 1977, when I was probably aided by Le Veque and by Ribenboim *op. cit.*; I looked at Neal Koblitz, *p-adic Numbers, p-adic analysis, and zeta-functions*, GTM 58, Springer-Verlag 1977, for my concluding remarks.