Gary Cornell Joseph H. Silverman
Glenn Stevens

Editors

Modular Forms and Fermat's Last Theorem

Springer
New York
Berlin
Heidelberg
Barcelona
Budapest
Hong Kong
London
Milan

Section 2. Kummer's work on cyclotomic fields.

The proof of FLT for the polynomial ring $A = k[T]$ is very short and sweet. It contains the main ideas of the early attempts to prove Fermat's assertion, but is much easier. Why is that? To begin with $\mathbf{Z}$, the ring of rational integers, contains no roots of unity except ± 1. To compensate for this the relevant roots of unity were added to $\mathbf{Z}$ and the arithmetic of the resulting rings investigated. Letting $i = \sqrt{-1}$. C.F. Gauss investigated the ring $\mathbf{Z}[i]$ in his celebrated pair of papers on biquadratic reciprocity [G]. Let $\omega = e^{2\pi i/3}$. The ring $\mathbf{Z}[\omega]$ was investigated by C.G. Jacobi and independently by G. Eisenstein in the course of formulating and proving the law of cubic reciprocity. Gauss had investigated the same ring in an unpublished paper proving FLT for $p = 3$. These authors, and others, also experimented with other roots of unity. For small primes p it turns out that $\mathbf{Z}[\zeta_p]$ is a unique factorization domain. In fact, this is true for all primes p less than 23. G. Lamé, perhaps led astray by this fact, announced in 1847 that he had a proof of FLT. Liouville almost immediately pointed out that he was implicitly assuming unique factorization. Soon thereafter, Liouville received a letter from Kummer which pointed out that not only is the assumption without proof, it is not correct. Kummer had shown three years earlier that $\mathbf{Z}[\zeta_{23}]$ is not a unique factorization domain. As we shall see in a moment, Kummer had done much, much more than that.

There is a story, told by K. Hensel in an address given on the hundredth anniversary of Kummer's birth, that Kummer himself had once constructed a proof of FLT assuming unique factorization and that the error had been pointed out to him by Dirichlet. Although this story has been widely retold in subsequent works on number theory, it is probably incorrect. This was pointed out, with fairly convincing evidence, by H. Edwards in a pair of papers [Ed2,Ed3] which are interesting reading both because of this issue and also for a general historical account of the events of 1844 to 1847 which bear on FLT.

Kummer not only noticed the failure of unique factorization, he invented his theory of ideal numbers to restore this immensely useful property for the rings $\mathbf{Z}[\zeta_p]$. Later, R. Dedekind extended Kummer's work by discussing general rings of algebraic numbers and by reinterpreting Kummer's ideal numbers by means of ideals. Because of the fact that Dedekind's language is so much more familiar to modern readers we will use it rather than Kummer's. The interested reader can consult Edward's book [Ed1] for a discussion of Kummer's point of view.

For the rings under consideration, Kummer proved that every ideal is the product of prime ideals in a unique way. He also defined the usual equivalence relation on ideals, proved the equivalence classes form a group, and that this group is finite. Let's call the ideal class group of $\mathbf{Z}[\zeta_p]$,

Cl_p, and its order, h_p, the class number. We also refer to h_p as the class number of the field $\mathbf{Q}(\zeta_p)$. Unique factorization holds for elements if and only if $h_p = 1$.

Another complication arises when $p \geq 5$. Namely, the unit group will contain elements of infinite order. As is well known the units in $\mathbf{Z}[i]$ are the fourth roots of unity and those in $\mathbf{Z}[\omega]$ are the sixth roots of unity. For $p \geq 5$ we define the elements (set $\zeta_p = \zeta$)

$$\xi_k = \sqrt{\frac{\zeta^k - 1}{\zeta - 1}\,\frac{\zeta^{-k} - 1}{\zeta^{-1} - 1}} = \frac{\sin(k\pi/p)}{\sin(\pi/p)} \quad \text{for } k = 2, 3, \ldots, \frac{p-1}{2}. \tag{2}$$

These elements are easily seen to be units, called cyclotomic units, in $\mathbf{Z}[\zeta_p]$. Kummer shows that they are independent; i.e., they generate a free abelian group of rank $\frac{p-3}{2}$. Let C_p be the subgroup of the unit group E_p generated by the ξ_k and the roots of unity. C_p is called the group of cyclotomic units. Kummer shows that C_p is of finite index in E_p and gives the following beautiful interpretation of the index.

Theorem 2.1. *The index $[E_p : C_p] = h_p^+$, where h_p^+ is the class number of $\mathbf{Q}(\zeta_p + \zeta_p^{-1}) = \mathbf{Q}(\zeta_p)^+$, the maximal real subfield of $\mathbf{Q}(\zeta_p)$.*

Further, it turns out that h_p^+ divides h_p, so that we can define the integer $h_p^- = h_p/h_p^+$, called the relative class number. In the older literature h_p^- and h_p^+ are referred to as the first and second factors of the class number respectively. Kummer also gives a beautiful and important formula for h_p^- which we shall now proceed to explain.

Let χ be a Dirichlet character modulo p. We say that χ is odd if $\chi(-1) = -1$ and even if $\chi(-1) = 1$. Define $B_{1,\chi} = p^{-1}\sum_{a=1}^{p-1}\chi(a)a$. It is easy to see that $B_{1,\chi} = 0$ if χ is even and not trivial. On the other hand:

Theorem 2.2.

$$h_p^- = 2p \prod_{\chi \text{ odd}} \left(-\frac{1}{2}\right) B_{1,\chi}.$$

The numbers $B_{1,\chi}$ are sometimes called generalized Bernoulli numbers. We will relate them to ordinary Bernoulli numbers a little later. First, we mention another of Kummer's important theorems about the class number.

Theorem 2.3. *If p divides h_p^+, then p divides h_p^-.*

Definition. A prime number p is called *regular* if p does not divide h_p, otherwise it is called *irregular*.

As was mentioned in the introduction, Kummer's greatest contribution to FLT was to show that it is true for regular primes. We will sketch a proof of this in Section 3. For the remainder of this section we discuss Kummer's

criterion for regularity which allows one to actually compute whether a given prime is regular or not. We begin by recalling the definition of the Bernoulli numbers and some of their properties (see [BS], [IR], [Ri], or [W]).

The simplest way to define the Bernoulli numbers B_n is by way of the power series expansion

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

From this it is easy to derive the formula

$$(m+1)B_m=-\sum_{k=0}^{m-1}\binom{m+1}{k}B_k.$$

The Bernoulli numbers may now be computed recursively. One finds $B_1=-\frac{1}{2}, B_2=\frac{1}{6}, B_3=0, B_4=-\frac{1}{30}, B_5=0, B_6=\frac{1}{42}$, etc. For $n>1$ and odd one has $B_n=0$. The even numbered Bernoulli numbers grow quite rapidly. In fact, $|B_{2m}|>2(m/\pi e)^{2m}$.

The Bernoulli numbers are rational numbers whose denominators are known thanks to the theorem of Von-Staudt and Claussen. This asserts that the denominator of B_n is the product of those primes p such that $p-1$ divides n. In particular, if $p>3$ the numbers $B_2, B_4, B_6, \ldots, B_{p-3}$ are p-integral.

Let $\mathbf{Z}_p$ denote the p-adic numbers. It is well known that the unit group $\mathbf{Z}_p^*$ contains the $(p-1)^{\text{st}}$ roots of unity, and that there is a character $\omega:(Z/pZ)^*\to Z_p^*$ with the property that $\omega(a)\equiv a \pmod p$ for all rational integers a prime to p. ω is an odd character of order $p-1$. Using Theorem 2.2, one easily derives the following p-adic version.

Theorem 2.2 P.

$$h_p^-=2p\prod_{\substack{i=1\\ i\text{ odd}}}^{p-2}\left(-\frac{1}{2}B_{1,\omega^i}\right)$$

The equality here takes place inside $\mathbf{Z}_p$.

To get Kummer's criterion from this we need the following congruence which is proved in [W, Cor.5.15] using p-adic L-functions and in [Lg1, Theorem 2.5] using the theory of p-adic distributions. Because of its importance we give another, more elementary proof, in the appendix to this paper.

Proposition 2.3. *If n is odd, and $p-1$ does not divide $n+1$, we have*

$$B_{1,\omega^n}\equiv\frac{B_{n+1}}{n+1}\pmod p.$$

We are now in a position to demonstrate the following wonderful result of Kummer.

Theorem 2.4. *A prime number p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$.*

PROOF. By Theorem 2.3 it follows that p divides h_p if and only if p divides h_p^-. We will use the expression for h_p^- given by Theorem 2.2 P.

First consider the case $i=p-2$. We have,

$$pB_{1,\omega^{p-2}}=\sum_{a=1}^{p-1}\omega^{p-2}(a)a\equiv\sum_{a=1}^{p-1}a^{p-1}\equiv p-1\equiv -1\pmod p.$$

Thus,

$$h_p^-\equiv\prod_{\substack{i=1\\ i\text{ odd}}}^{p-4}\left(-\frac{1}{2}B_{1,\omega^i}\right)\equiv\prod_{\substack{i=1\\ i\text{ odd}}}^{p-4}\left(-\frac{1}{2}\frac{B_{i+1}}{i+1}\right)\pmod p.$$

The result follows directly from this congruence.

By using this theorem it is possible to check a given prime for regularity. Kummer showed that the only irregular primes less than 100 are 37, 59, and 67. He later checked all the primes up to 164 and found that 101, 103, 131, 149, and 157 are the only additional irregular primes. At one point he thought that he had a proof that there are infinitely many regular primes. In 1915, K.L. Jensen proved that there are infinitely many irregular primes [Ri; Lecture VI, Section 4]. However, to this day it is not known if there are infinitely many regular primes. It is possible to give a probabilistic argument to show that over 60% of the primes should be regular.

Let's assume that the probability that an even indexed Bernoulli number B_{2m} be divisible by p is $\frac{1}{p}$. If this is so, the probability that none of the numbers $B_2, B_4, \ldots, B_{p-3}$ be divisible by p is

$$\left(1-\frac{1}{p}\right)^{(p-3)/2}\approx e^{-1/2}\approx .6065.$$

This estimate for the percentage of regular primes agrees very well with the experimental evidence [BCEM]. It would be nice to have a rigorous proof.

We end this section with two more of Kummer's results. These two concern units. The first is fairly easy, but very useful. The second is quite deep, and is crucial to Kummer's proof of FLT for regular primes.

Recall some simple facts about $\mathbf{Q}(\zeta_p)$. The prime p is totally ramified in this field and the prime lying above (p) in $\mathbf{Z}[\zeta_p]$ is (λ), where $\lambda=\zeta_p-1$. Note that $\zeta_p\equiv 1 \pmod\lambda$ and $\mathbf{Z}[\zeta_p]/(\lambda)\cong\mathbf{Z}/p\mathbf{Z}$.

Proposition 2.5. *Let u be a unit in $\mathbf{Z}[\zeta_p]$. Then u can be written in a unique way as $\pm\zeta_p^i e$, where i is determined modulo p, and e is real and positive.*

PROOF. Let bar denote, as usual, complex conjugation. Then, $u/\bar{u}$ is a unit such that it and all its conjugates have absolute value 1. By a well known result, $u/\bar{u}$ is a root of unity. By ramification theoretic considerations the only roots of unity in $\mathbf{Z}[\zeta_p]$ are $\pm\zeta_p^i$ for $0 \le i \le p-1$. If $u/\bar{u} = \zeta_p^i$, find an integer j such that $2j \equiv i \pmod{p}$. Then one easily checks $\zeta_p^{-j}u$ is equal to its own conjugate, i.e., is real. The result follows in this case by adjusting the sign.

Suppose $u/\bar{u} = -\zeta^i$. We will show this leads to a contradiction. Choosing j as above, and setting $w = \zeta_p^{-j}u$, we find that w is a unit such that $\bar{w} = -w$. Thus $w^2 = -w\bar{w} = -v$. It follows that $-v \in \mathbf{Z}[\zeta_p]^+$ is a negative unit and so w generates the extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}(\zeta_p)^+$. It would follow that this extension is unramified at p (recall $p \neq 2$). However, it is ramified at p, so we have reached a contradiction.

Corollary. *Let E_p^+ be the real positive units in E_p and C_p^+ be the subgroup of C_p generated by the cyclotomic units ξ_k (see equation (2) above). Then, $E_p^+/C_p^+ \cong E_p/C_p$ and both groups have order h_p^+.*

PROOF. This follows directly from Theorem 2.1 and Proposition 2.5.

We remark that there is another way to finish the proof of the proposition. Suppose w is a unit such that $w = -\bar{w}$. By the remarks preceding the proposition, there is a rational integer M such that $w \equiv M \pmod{\lambda}$. It follows that $M \equiv -M \pmod{\lambda}$ and so $2M \equiv 0 \pmod{\lambda}$. Thus, λ divides M and so also w. However, w is a unit so this is a contradiction.

The final result we need is known as Kummer's lemma. It is simple to state. Any unit in $\mathbf{Q}(\zeta_p)$ which is congruent to a rational integer modulo p is a p^{th} power. The usual proof is by means of a close analysis of the unit group and especially of the local unit group in the completion of $\mathbf{Q}(\zeta_p)$ at the prime (λ). This involves the p-adic logarithm, the local expansion of the p-adic logarithm of the cyclotomic units, etc. The analysis is nicely carried out in Section 6 of Chapter 5 in [B-S]. We give an alternative approach, suggested by Hilbert in his Zahlbericht [H], which depends on the study of ramification in Kummer extensions. This approach brings out more clearly the underlying role played by class field theory.

Lemma 2.6. *Let $\beta \in \mathbf{Z}[\zeta_p]$. Suppose λ does not divide β and that $x^p \equiv \beta \pmod{\lambda^p}$ is solvable. Let K be the field obtained by adjoining $A = \sqrt[p]{\beta}$ to $\mathbf{Q}(\zeta_p)$. Then the extension $K/\mathbf{Q}(\zeta_p)$ is unramified at p.*

PROOF. Suppose $\alpha^p \equiv \beta \pmod{\lambda^p}$ and set $\tau = (A-\alpha)/\lambda$. Then τ is a root of the monic polynomial

$$f(x) = \frac{(\lambda x + \alpha)^p - \beta}{\lambda^p}.$$

Using the fact that $p = u\lambda^{p-1}$ where u is a unit, we see that all the coefficients of $f(x)$ are algebraic integers. Thus, τ is an algebraic integer. A short computation shows that all the coefficients of $f'(x)$ are in (λ) except the constant term $u\alpha^p$ which is prime to (λ). Thus, $f'(\tau)$ is prime to (λ) and it follows that the relative discriminant is prime to (λ). The proof is complete.

Theorem 2.7. *Let p be a regular prime and e a unit in $\mathbf{Q}(\zeta_p)$ which is congruent to a p^{th} power modulo λ^p. Then, e is the p^{th} power of a unit.*

PROOF. Consider the extension $L = \mathbf{Q}(\zeta_p, \sqrt[p]{e})$ of $\mathbf{Q}(\zeta_p)$. This extension is cyclic of degree 1 or p. Suppose the degree is p. By Lemma 2.6, the extension is unramified at p. Since e is a unit it is easy to see it is unramified at every other prime as well. Thus, it is an unramified, abelian extension of degree p and it follows by class field theory that $p|h_p$, which contradicts the assumption that p is regular. Thus, $\sqrt[p]{e} \in \mathbf{Q}(\zeta_p)$ and the theorem follows.

The phrase "it follows by class field theory" can be avoided. The result needed follows from Theorem 94 of Hilbert's Zahlbericht [H; page 155]. We sketch a short cohomological proof of this in the Appendix.

The usual form of Kummer's Lemma can be deduced from Theorem 2.7 as follows. If $e \equiv a \pmod{p}$ with $a \in \mathbf{Z}$ we have $e = a + p\alpha$ with $\alpha \in \mathbf{Z}_p$. Now, $\alpha \equiv b \pmod{\lambda}$ with $b \in \mathbf{Z}$. Thus, $e \equiv a + bp \pmod{\lambda^p}$. Let σ be an element of $Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Then, $e^\sigma/e \equiv 1 \pmod{\lambda^p}$ and is thus a p^{th} power by Theorem 2.7: $e^\sigma = e\eta(\sigma)^p$. Taking the product over all σ and remembering that the norm of a unit is ± 1, we find $\pm 1 = e^{p-1}\eta^p$ for a suitable η and finally, $e = (\pm e\eta)^p$.

Section 3. Fermat's last theorem for regular primes and certain other cases.

Having assembled a number of the powerful tools forged by Kummer, we will now give part of his proof that FLT is true for regular primes. Here is the statement of the full theorem.

Theorem 3.1. *Let p be a regular prime. Then, the equation $x^p + y^p = z^p$ has no solution with $x, y, z \in \mathbf{Z}[\zeta_p]$ and $xyz \neq 0$.*

The proof is usually broken up into two parts. The first case is when λ does not divide xyz and the second case is when λ does divide xyz (recall, $\lambda = \zeta_p - 1$). The first case is easier. If one confines one's attention to $\mathbf{Z}$ rather than $\mathbf{Z}[\zeta_p]$, proofs of the first case can be found in [BS,IR,W] and

many other places. For a proof of the first case in $\mathbf{Z}[\zeta_p]$ see [La] or [H]. We will concentrate on the second case.

It is interesting that Kummer made a simple error at the beginning of his proof of the second case. He asserts that it is no loss of generality to assume that x, y, z are pairwise relatively prime. This is certainly true over $\mathbf{Z}$, but is false over $\mathbf{Z}[\zeta_p]$ because there may be a common divisor which is not principal. Once this is realized it is not hard to alter Kummer's proof so that it holds in full generality. Hilbert does so in Section 172 of [H]. See [La] for another presentation. We give Kummer's proof of the more restricted result because it is relatively short and the main ideas show through more clearly.

Theorem 3.1′. *Let p be a regular prime. Then, the equation*

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

has no solution with $x, y, z \in \mathbf{Z}[\zeta_p]$, $\lambda | xyz$, and x, y, z pairwise relatively prime.

PROOF. Assume x, y, z is such a solution. It is no loss of generality to assume that $\lambda | z$. It follows that λ does not divide x or y. Write $z = \lambda^m z_0$ with $(\lambda, z_0) = 1$. Then, x, y, z_0 is a solution to $X^p + Y^p = \lambda^{mp} Z^p$ with $(xyz_0, \lambda) = 1$, x, y, z pairwise relatively prime, and $m \geq 1$. Let u be a unit in $\mathbf{Z}[\zeta_p]$. We will show that there are no solutions x, y, z to

$$X^p + Y^p = u\lambda^{mp} Z^p \qquad (*)$$

with x, y, z pairwise relatively prime, $(xyz, \lambda) = 1$, and $m \geq 1$. This will prove the theorem.

The strategy is this. Assume such a solution exists. One shows that, in fact, m must be greater than 1. Then one finds a solution of the same type to a similar equation but with m replaced by $m - 1$. This yields a contradiction via "infinite descent."

We need a Lemma.

Lemma 3.2. *Let $v \in \mathbf{Z}[\zeta_p]$ with $(v, \lambda) = 1$. Then, there is a rational integer k such that $\zeta_p^k v \equiv a \pmod{\lambda}$ with $a \in \mathbf{Z}$.*

PROOF. Since the residue class field modulo λ has p elements, we may write $v \equiv m + n\lambda \pmod{\lambda^2}$ where $m, n \in \mathbf{Z}$ and $(m, p) = 1$. Now, $\zeta_p^k = (1+\lambda)^k \equiv 1 + k\lambda \pmod{\lambda^2}$. Thus, $\zeta_p^k v \equiv m + (n + km)\lambda \pmod{\lambda^2}$. Choose k to be a solution of $n + mx \equiv 0 \pmod{p}$ and the Lemma follows.

Now, assume x, y, z is a solution of equation $(*)$ above with $(xyz, \lambda) = 1$ and x, y, z pairwise relatively prime. By Lemma 3.2 we can assume that

$x, y \equiv a, b \pmod{\lambda^2}$ where $a, b \in \mathbf{Z}$. We have,

$$\prod_{i=0}^{p-1} (x + \zeta_p^i y) = u\lambda^{mp} z^p. \qquad (**)$$

It follows that λ must divide at least one term on the left hand side of this equation, and consequently it must divide all the terms. Since $x + y \equiv a + b \pmod{\lambda^2}$, we must have $p \mid a + b$ and so $\lambda^2 \mid x + y$. From equation $(**)$ it now follows that λ^{p+1} divides the left hand side, and so $m > 1$, which is our first goal.

We have $x + \zeta_p^i y = x + y + (\zeta_p^i - 1)y$ and so for $i > 0$, $x + \zeta_p^i y$ is exactly divisible by λ. Thus, passing to ideals, we find $(x+y) = (\lambda)^{p(m-1)+1} C_0$ and $(x + \zeta_p^i y) = (\lambda) C_i$ for $i = 1, 2, \ldots, p-1$, where the C_i for $i = 0, 1, \ldots, p-1$ are pairwise relatively prime principal ideals each of which is prime to (λ). From equation $(**)$ we deduce $C_0 C_1 \ldots C_{p-1} = (z)^p$. It follows that each C_i is a p^{th} power, i.e., $C_i = D_i^p$. Since D_i^p is a principal ideal and p is a regular prime, we deduce that D_i is a principal ideal, i.e., $D_i = (w_i)$ for $w_i \in \mathbf{Z}[\zeta_p]$. Returning to the level of elements, we see that there are units u_0, u_1, u_2 such that

$$x + y = u_0 \lambda^{p(m-1)+1} w_0^p, \quad x + \lambda y = u_1 \lambda w_1^p, \quad x + \lambda^2 y = u_2 \lambda w_2^p.$$

Eliminating x and y from these three equations and dividing the result by u_1, we find units e_2 and e such that

$$w_1^p + e_2 w_2^p = e\lambda^{(m-1)p} w_0^p.$$

Taking congruences modulo λ^p, we see that e_2 is congruent to a p^{th} power modulo λ^p. By Theorem 2.7, $e = f^p$ for some $f \in \mathbf{Z}[\zeta_p]$. Setting $x' = w_1$, $y' = f w_2$, and $z' = w_0$, we see that x', y', z' is a solution to $X^p + Y^p = e\lambda^{(m-1)p} Z^p$ for which $(x'y'z', \lambda) = 1$ and x', y', z' are pairwise relatively prime. We have reached our second goal and so completed the proof of Theorem 3.1′.

Kummer went well beyond the case of regular primes in his attempt to prove FLT in general. He produced some explicit cyclotomic units E_i for $i = 2, 4, \ldots, p-3$ and stated that FLT is true if the following conditions hold; h_p^- is divisible by p but not p^2, and for $i = 2, 4, \ldots, p-3$, B_{pi} is not divisible by p^3 and E_i is not a p^{th} power. He then verified on the basis of this result and Theorem 3.1 that FLT holds for all primes less than 100.

Kummer's work was reconsidered by H.S. Vandiver in the 1920's. He found some problems with the proof of the above mentioned result which he was able to fix. He went on to improve upon Kummer's work in several ways. For example, he proved the following theorem [V], [W; Theorem 9.4].

Theorem 3.3. *Suppose B_{pi} is not divisible by p^3 for $i = 2, 4, \ldots, p-3$ and that h_p^+ is not divisible by p. Then, the second case of FLT is true for p.*

In Chapter 9 of [W] there are further results of Vandiver which give rational criteria for proving the second case of FLT. See, in particular, Theorem 9.5. The first case of FLT can also be tested by even simpler rational criteria (see [LS]). Thus, it became possible to test FLT computationally. Vandiver and his students, using desk calculators, extended Kummer's verification to all primes less than 620. In 1954, using a computer, Vandiver, D.H. Lehmer, and E. Lehmer verified FLT for all primes up to 2,000. In 1955, J.L. Selfridge, C.A. Nicol, and H.S. Vandiver verified FLT up to 4,001. In 1976, S.Wagstaff showed FLT is true for all $p < 125{,}000$. In 1993 it was shown that FLT is true for all primes up to 4 million [BCEM]. This is the largest bound achieved before FLT was proven to hold for all primes p and so all $n > 2$.

Vandiver (1882-1973) made many contributions to FLT and other parts of number theory. For references to some of his work on FLT see his interesting expository article (and the short follow up article) [V]. According to an interesting obituary notice written by D.H. Lehmer [Lmr], Vandiver never graduated from high school. He spent most of his professional life at the University of Texas. He is the only American mentioned in E. Landau's monumental three volume treatise on number theory, *Vorlesungen über Zahlentheorie.*

Vandiver conjectured that h_p^+ is not divisible by p for all primes p. This conjecture is referred to simply as Vandiver's conjecture. Serge Lang has pointed out that Kummer made the conjecture many years earlier in a letter to Kronecker where he refers to it as a "noch zu beweisenden Satz" (Kummer's *Collected Works*, vol. 1, page 85). In any case, it has held up well. In [BCEM] it is verified for all primes less than 4 million. Larry Washington has produced a probabilistic argument [W, page 159] which shows that the number of exceptions to Vandiver's conjecture up to a given bound x should be approximately $\frac{1}{2}\log\log x$. For $x = 4{,}000{,}000$ this is approximately 1.361, so the fact that no counter-example has shown up is perhaps not surprising. On the other hand Washington's reasoning rests on certain randomness assumptions which may or may not hold. In any case, the conjecture is true very often! This is good because, as we shall see in the next section, Vandiver's conjecture has very interesting implications.

Section 4. The structure of the p-class group.

A prime is irregular if A_p, the p-part of the class group of $\mathbf{Q}(\zeta_p)$, is non-trivial. Much work has been devoted to understanding the structure of A_p beginning with Kummer. Important contributions have been made by people like Hilbert, Herbrand, Leopoldt, Iwasawa, Ribet, Mazur, and Wiles, among others. In this section we will review some of this work. Among other things we will show that if one accepts the Vandiver conjecture as true, then it is possible to give a completely satisfying description of the structure of A_p.

We begin with a few preliminary remarks. It is convenient to write the group operation in A_p additively. Also, since p is fixed in this discussion, we will write A instead of A_p. Since A is a torsion p-group, we may consider it as a $\mathbf{Z}_p$-module. It is also a module for the Galois group $G_p = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Thus, A is a module over the group ring $\mathbf{Z}_p[G_p]$. As is well known, $(\mathbf{Z}/p\mathbf{Z})^*$ is isomorphic to G_p, where the automorphism corresponding to a, σ_a, takes ζ_p to ζ_p^a. Let ω be the p-adic valued character introduced in Section 2, and for each i such that $0 \le i < p-1$ define

$$\epsilon_i = \frac{1}{p-1}\sum_a \omega(a)^{-i}\sigma_a \in \mathbf{Z}[G_p].$$

Here as elsewhere in this section, the summation goes from $a = 0$ to $a = p-2$. It is easy to check that these elements constitute a complete set of mutually orthogonal idempotents in the group ring. Define $A_i = \epsilon_i A$. Then,

$$A = \bigoplus_i A_i, \quad \text{and if } x \in A_i, \text{ then } \sigma_a x = \omega(a)^i x.$$

Because of this decomposition, to understand the structure of A, it suffices to understand the structure of each A_i.

The automorphism σ_{-1} is simply complex conjugation. Since $\omega(-1) = -1$, it follows that complex conjugation fixes A_i if i is even, and acts as multiplication by -1 if i is odd. It is not hard to show that the part of A which is fixed by complex conjugation is isomorphic to the p-part of the class group of $\mathbf{Q}(\zeta_p)^+$. Thus, if Vandiver's conjecture is true, $A_i = (0)$ for i even.

A final preliminary comment is that ϵ_0 is a constant times the norm map, and the norm map annihilates the class group. It follows that ϵ_0 simultaneously annihilates and fixes A_0. The conclusion is that $A_0 = (0)$.

Do any other elements of the group ring $\mathbf{Z}[G_p]$ annihilate A? This question is the key to the deeper part of the theory. The answer is that yes, there are other elements beside the norm map which annihilate the class group. The honor of being the first to see this goes (once again) to Kummer. Let l be a rational prime such that $l \equiv 1 \pmod{p}$, $\mathcal{L}$ a prime