# FERMAT'S LAST THEOREM FOR REGULAR PRIMES

KEITH CONRAD

For a prime $p$, we call $p$ *regular* when the class number $h_p = h(\mathbf{Q}(\zeta_p))$ of the $p$th cyclotomic field is not divisible by $p$. For instance, all primes $p \leq 19$ have $h_p = 1$, so they are regular. Since $h_{23} = 3$, 23 is regular. All primes less then 100 are regular except for 37, 59, and 67. By the tables in [6], $h_{37} = 37$, $h_{59} = 3 \cdot 59 \cdot 233$ and $h_{67} = 67 \cdot 12739$. It is known that there are infinitely many irregular primes, and heuristics and tables suggest around 61% of primes should be regular [6, p. 63].

The significance of a prime $p$ being regular is that if the $p$th power of an ideal $\mathfrak{a}$ in $\mathbf{Z}[\zeta_p]$ is principal, then $\mathfrak{a}$ is itself principal. Indeed, if $\mathfrak{a}^p$ is principal, then it is trivial in the class group of $\mathbf{Q}(\zeta_p)$. Since $p$ doesn't divide $h_p$, this means $\mathfrak{a}$ is trivial in the class group, so $\mathfrak{a}$ is a principal ideal.

The concept of regular prime was introduced by Kummer in his work on Fermat's Last Theorem (FLT). He proved the following, which we will treat in this paper.

**Theorem 1.** *For a regular prime $p \geq 3$, the equation $x^p + y^p = z^p$ does not have a solution in positive integers $x, y, z$.*

To see how much of an advance this was on Fermat's problem compared to work preceding Kummer, see [4].

Since $p$ is a fixed prime, we henceforth write $\zeta_p$ simply as $\zeta$. The complex conjugate of an element $\alpha$ in $\mathbf{Q}(\zeta)$ is $\overline{\alpha}$. Since complex conjugation is an automorphism of this field, whose Galois group over $\mathbf{Q}$ is abelian, $\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)}$ for any $\alpha$ in $\mathbf{Q}(\zeta)$ and any $\sigma$ in $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$.

We start with some lemmas valid in the $p$th cyclotomic field for any prime $p$.

**Lemma 1.** *In $\mathbf{Z}[\zeta]$, the numbers $1-\zeta, 1-\zeta^2, \ldots, 1-\zeta^{p-1}$ are all associates and $1+\zeta$ is a unit. Also $p = u(1-\zeta)^{p-1}$ for some unit $u$ and $(1-\zeta)$ is the only prime ideal in $\mathbf{Z}[\zeta]$ dividing $p$.*

*Proof.* For $1 \leq j \leq p-1$, $(1-\zeta^j)/(1-\zeta) = 1 + \zeta + \cdots + \zeta^{j-1}$ lies in $\mathbf{Z}[\zeta]$. Writing $1 \equiv jj' \bmod p$, we see the reciprocal $(1-\zeta)/(1-\zeta^j) = (1-\zeta^{jj'})/(1-\zeta^j)$ lies in $\mathbf{Z}[\zeta^j] = \mathbf{Z}[\zeta]$. So $1-\zeta^j$ is a unit multiple of $1-\zeta$. In particular, taking $j = 2$ shows $1+\zeta$ is a unit.

Setting $X = 1$ in the equation $1 + X + \cdots + X^{p-1} = \prod_{j=1}^{p-1}(X - \zeta^j)$ gives

$$p = \prod_{j=1}^{p-1}(1-\zeta^j) = \prod_{j=1}^{p-1}\frac{1-\zeta^j}{1-\zeta}(1-\zeta) = u(1-\zeta)^{p-1},$$

where $u$ is a unit. Taking norms, $p^{p-1} = \mathrm{N}(1-\zeta)^{p-1}$, so $(1-\zeta)$ has prime norm and thus is a prime ideal. Since $(p) = (1-\zeta)^{p-1}$, $(1-\zeta)$ is the only prime ideal factor of $p$. □

**Lemma 2.** *For $v \in \mathbf{Z}[\zeta]^\times$, $v/\overline{v}$ is a root of unity.*

*Proof.* For $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$, $\sigma(\overline{v}) = \overline{\sigma v}$, so $v/\overline{v}$ and all of its $\mathbf{Q}$-conjugates have absolute value 1. Therefore, by a theorem of Kronecker, $v/\overline{v}$ is a root of unity [6, Lemma 1.6]. □

The roots of unity in $\mathbf{Z}[\zeta]$ are $\pm\zeta^j$, and in fact one can show in the preceding lemma that $v/\overline{v}$ is a power of $\zeta$ (i.e., no minus sign), but we won't need that more precise statement. (For a proof, see [6, p. 4].)

The proof of Fermat's Last Theorem for a given exponent $p$ has traditionally been divided into two cases, based on whether the proposed solution $(x, y, z)$ has $p$ not dividing any of $x, y, z$ or $p$ dividing one of them. These cases are respectively called Case I and Case II. Experience shows Case II is much harder to treat than Case I using cyclotomic methods.

From now on, $p$ is a regular prime.

Case I: Suppose $x^p + y^p = z^p$ where $x, y, z$ are nonzero integers with $p$ not dividing any of $x, y$, or $z$. We may of course assume $x$, $y$, and $z$ are pairwise relatively prime. We will derive a contradiction when $p$ is regular.

In $\mathbf{Z}[\zeta]$, factor Fermat's equation as

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

Let's show the factors on the right side generate relatively prime ideals. For $0 \leq j < j' \leq p-1$, any common ideal factor $\mathfrak{d}$ of $(x + \zeta^j y)$ and $(x + \zeta^{j'} y)$ is a factor of the difference

$$x + \zeta^j y - x - \zeta^{j'} y = \zeta^j y(1 - \zeta^{j'-j}) = vy(1 - \zeta)$$

for some unit $v$. (Here we use Lemma 1.) Since $y(1-\zeta)$ divides $yp$, we have $\mathfrak{d}|(yp)$. We also know, by (1), that $\mathfrak{d}$ divides $(z)^p$. Since $yp$ and $z^p$ are relatively prime integers, we conclude $\mathfrak{d}$ is the unit ideal, so the ideals $(x + \zeta^j y)$ are relatively prime.

The product of these ideals is the $p$th power $(z)^p$, so unique ideal factorization implies each factor is a $p$th power. Taking $j = 1$,

$$(x + \zeta y) = \mathfrak{a}^p$$

for some ideal $\mathfrak{a}$. Therefore $\mathfrak{a}^p$ is trivial in the class group of $\mathbf{Q}(\zeta)$. Assuming $p$ is regular, we deduce that $\mathfrak{a}$ is trivial in the class group, so $\mathfrak{a}$ is principal, say $\mathfrak{a} = (t)$ with $t \in \mathbf{Z}[\zeta]$. Thus

$$x + \zeta y = ut^p$$

for some unit $u$ in $\mathbf{Z}[\zeta]$. (If we assumed $\mathbf{Z}[\zeta]$ is a UFD, this deduction would've been immediate from knowing the numbers $x + \zeta^j y$ are pairwise relatively prime: their product is a $p$th power so each one is a $p$th power, up to unit multiple. We can get this conclusion from the weaker assumption that $h_p$ is not divisible by $p$ rather than that $h_p = 1$.)

Writing $t = b_0 + b_1\zeta + \cdots + b_{p-1}\zeta^{p-2}$, with $b_j$ in $\mathbf{Z}$, we get

$$t^p \equiv b_0 + b_1 + \cdots + b_{p-2} \bmod p\mathbf{Z}[\zeta], \tag{2}$$

so $t^p \equiv \overline{t}^p \bmod p\mathbf{Z}[\zeta]$.

By Lemma 2, $u/\overline{u} = \pm\zeta^j$ for some $j$ between 0 and $p-1$. If $u/\overline{u} = \zeta^j$ then

$$\begin{aligned} x + \zeta y &= ut^p \\ &= \zeta^j \overline{u} t^p \\ &\equiv \zeta^j \overline{u}\overline{t}^p \bmod p\mathbf{Z}[\zeta] \\ &\equiv \zeta^j(x + \overline{\zeta} y) \bmod p\mathbf{Z}[\zeta]. \end{aligned}$$

Thus

$$u/\overline{u} = \zeta^j \Longrightarrow x + y\zeta - y\zeta^{j-1} - x\zeta^j \equiv 0 \bmod p\mathbf{Z}[\zeta]. \tag{3}$$

Similarly,

$$u/\overline{u} = -\zeta^j \Longrightarrow x + y\zeta + y\zeta^{j-1} + x\zeta^j \equiv 0 \bmod p\mathbf{Z}[\zeta]. \tag{4}$$

We want to show neither of these congruences can hold when $0 \leq j \leq p-1$ and $x$ and $y$ are integers prime to $p$.

Since $x$ and $y$ are nonzero mod $p$, these congruences appear to show linear dependence over $\mathbf{Z}/p$ among some powers of $\zeta$ in $\mathbf{Z}[\zeta]/p$. However, in $\mathbf{Z}[\zeta]/p$ the powers $1, \zeta, \ldots, \zeta^{p-2}$ are linearly independent over $\mathbf{Z}/p$ since

$$\mathbf{Z}[\zeta]/p \cong \mathbf{Z}[X]/(p, \Phi_p(X)) \cong (\mathbf{Z}/p)[X]/\Phi_p(X) \cong (\mathbf{Z}/p)[X]/(X-1)^{p-1},$$

and $\{1, X, \ldots, X^{p-2}\}$ is a basis of the last ring, over $\mathbf{Z}/p$. For those $j \leq p-1$ such that $1, \zeta, \zeta^{j-1}, \zeta^j$ are distinct powers in the set $\{1, \zeta, \ldots, \zeta^{p-2}\}$, i.e., as long as $0, 1, j-1, j$ are distinct integers with $j \leq p-2$, (3) and (4) both yield a contradiction. So when $3 \leq j \leq p-2$, there is a contradiction in Case I.

The rest of the proof is an accounting exercise in handling the remaining cases $j = 0, 1, 2$, and $p-1$.

First of all, we may take $p \geq 5$, since the equation $x^3 + y^3 = z^3$ has no solutions in integers prime to 3. (Even the congruence $x^3 + y^3 \equiv z^3 \bmod 9$ has no solutions in numbers prime to 3, since the cubes of units mod 9 are $\pm 1$.)

Can $j = p-1$? If so, then the left side of the congruence in (3) becomes

$$x(1-\zeta^{p-1}) + y(\zeta - \zeta^{p-2}) = 2x + (x+y)\zeta + x(\zeta^2 + \cdots + \zeta^{p-3}) + (x-y)\zeta^{p-2},$$

which contradicts linear independence of $1, \zeta, \ldots, \zeta^{p-2} \bmod p$ over $\mathbf{Z}/p$ by looking at the coefficient of, say, $\zeta^2$. There is a similar contradiction in (4) if $j = p-1$.

Can $j = 0$? If so, then (3) becomes $y(\zeta - \zeta^{-1}) \equiv 0 \bmod p\mathbf{Z}[\zeta]$. Since $y$ is not divisible by $p$, we can divide by it and get $\zeta^2 - 1 \equiv 0 \bmod p$, which contradicts linear independence of 1 and $\zeta^2 \bmod p$ since $p \geq 5$. Similarly, (4) with $j = 0$ implies $2x\zeta + y\zeta^2 + y \equiv 0 \bmod p$, so again we get a contradiction.

Setting $j = 2$ in (3) or (4) leads to contradictions of linear independence as well. We now are left with the case $j = 1$. In this case (4) implies $(x+y)(1+\zeta) \equiv 0 \bmod p$, so $x + y \equiv 0 \bmod p\mathbf{Z}$. (Here we use Lemma 1.) Thus $z^p = x^p + y^p \equiv (x+y)^p \equiv 0 \bmod p$, so $p$ divides $z$. That violates the condition of Case I. The only remaining case is $j = 1$ in (3).

To summarize, we have shown that if $x^p + y^p = z^p$ and $x, y, z$ are not divisible by $p$, then $x + \zeta y = ut^p$ where $u/\overline{u} = \zeta$. Setting $j = 1$ in (3) yields

$$x(1-\zeta) + y(\zeta - 1) \equiv 0 \bmod p. \tag{5}$$

Writing $p = u(1-\zeta)^{p-1}$, (5) implies

$$x \equiv y \bmod (1-\zeta)^{p-2}.$$

Since $p-2 \geq 1$ and $x$ and $y$ are in $\mathbf{Z}$, this forces $x \equiv y \bmod p\mathbf{Z}$. Running through the proof with $y$ and $-z$ interchanged, we get $x \equiv -z \bmod p\mathbf{Z}$, so

$$0 = x^p + y^p - z^p \equiv 3x^p \bmod p.$$

Since $p \neq 3$ and $x$ is prime to $p$, we have a contradiction. This settles Case I for $p$ a regular prime. □

Although we used congruences to prove the nonsolvability of $x^p + y^p = z^p$ in integers prime to $p$ (when $p$ is regular), there often are solutions to $x^p + y^p \equiv z^p \bmod p^m$ for large $m$ and $x, y, z$ all prime to $p$. For instance, $1^7 + 30^7 \equiv 31^7 \bmod 49$ and from this one can solve $x^7 + y^7 \equiv z^7 \bmod 7^m$ in numbers prime to 7, for every $m$. So it is rather hard to try proving nonsolvability of Fermat's equation with odd prime exponent using congruences in $\mathbf{Z}$. (This is why many crank proofs of FLT, based on elementary number theory, are doomed to failure.) What we used in the above proof were congruences in $\mathbf{Z}[\zeta]$, not in $\mathbf{Z}$.

We now pass to Case II. Our treatement is taken largely from [5, pp. 31–33].

Case II. Assume Fermat's equation has a solution in nonzero integers $x, y, z$ with at least one number divisible by $p$. Since $p$ is odd, we may write the equation in the symmetric

form $x^p + y^p + z^p = 0$. If $p$ divides two of $x, y$, or $z$, then it divides the third as well. So removing the highest common factor of $p$ from the three numbers, we can assume $p$ divides only one of the numbers, say $p|z$. Writing $z = p^r z_0$, with $z_0$ prime to $p$ and $r \geq 1$, Fermat's equation reads

$$x^p + y^p + w(1-\zeta)^{pr(p-1)} z_0^p = 0. \tag{6}$$

for some unit $w$ in $\mathbf{Z}[\zeta]$ and $p$ not dividing $xyz_0$. Since $(1-\zeta)$ is the only prime over $p$ in $\mathbf{Z}[\zeta]$ and $x, y, z_0$ are in $\mathbf{Z}$, saying $xyz_0$ is not divisible by $p$ in $\mathbf{Z}$ is equivalent to saying $xyz_0$ is not divisible by $(1-\zeta)$ in $\mathbf{Z}[\zeta]$. We now suitably generalize the form of (6), thereby making it easier to prove a stronger result.

**Theorem 2.** *For any regular prime $p \geq 3$, there do not exist $\alpha, \beta, \gamma$ in $\mathbf{Z}[\zeta]$, all nonzero, such that*

$$\alpha^p + \beta^p + \varepsilon(1-\zeta)^{pn}\gamma^p = 0, \tag{7}$$

*where $\varepsilon \in \mathbf{Z}[\zeta]$, $n \geq 1$, and $(1-\zeta)$ does not divide $\alpha\beta\gamma$.*

In particular, (6) and Theorem 2 show Fermat's Last Theorem for exponent $p$ has no solution in Case II when $p$ is regular. The need for allowing a unit coefficient $\varepsilon$ other than 1 is already evident in how Theorem 2 is applied to Case II of FLT.

*Proof.* By (7), we have the ideal equation

$$\prod_{j=0}^{p-1}(\alpha + \zeta^j\beta) = (1-\zeta)^{pn}(\gamma)^p. \tag{8}$$

Since $\gamma$ is nonzero, the left side is nonzero, so $\alpha+\beta, \alpha+\zeta\beta, \ldots, \alpha+\zeta^{p-1}\beta$ are all nonzero.

Unlike Case I, the factors on the left side will not be relatively prime ideals. The plan of the proof is to analyze the ideal factorization of each term on the left and then use the regularity hypothesis to prove certain ideals are principal.

We will work often with congruences in $\mathbf{Z}[\zeta]/(1-\zeta)$ and $\mathbf{Z}[\zeta]/(1-\zeta)^2$. Note $\mathbf{Z}[\zeta]/(1-\zeta) \cong \mathbf{Z}/p$ and (for $p \geq 3$) $\mathbf{Z}[\zeta]/(1-\zeta)^2 \cong (\mathbf{Z}/p)[X]/(1-X)^2$. For any number $\delta(1-\zeta)$ considered modulo $(1-\zeta)^2$, $\delta$ only matters modulo $1-\zeta$, so there are $p$ multiples of $1-\zeta$ in $\mathbf{Z}[\zeta]/(1-\zeta)^2$.

Because $\alpha + \zeta^j\beta \equiv \alpha + \beta \bmod (1-\zeta)$ and the prime $(1-\zeta)$ divides some factor on the left side of (8), it divides all factors on the left side. We want to show some $\alpha + \zeta^{j_0}\beta$ is divisible by $1-\zeta$ twice, i.e., $\alpha + \zeta^{j_0}\beta \equiv 0 \bmod (1-\zeta)^2$.

Assume, to the contrary, that $1-\zeta$ divides each factor on the left side of (8) exactly once. (That is, *assume* $n = 1$.) Then each of the $p$ factors on the left side of (8) reduces to a *nonzero* multiple of $1-\zeta \bmod (1-\zeta)^2$. (Convince yourself of this.) However, there are $p-1$ distinct nonzero multiples of $1-\zeta$ modulo $(1-\zeta)^2$, so we must have

$$\alpha + \zeta^j\beta \equiv \alpha + \zeta^{j'}\beta \bmod (1-\zeta)^2$$

for some $0 \leq j < j' \leq p-1$. Therefore $(1-\zeta^{j'-j})\beta \equiv 0 \bmod (1-\zeta)^2$. Since $1-\zeta^{j'-j}$ is a unit multiple of $1-\zeta$, this congruence forces $1-\zeta$ to divide $\beta$. But that violates the hypothesis of the theorem.

Thus $n \geq 2$ and some $\alpha + \zeta^{j_0}\beta$ is $\equiv 0 \bmod (1-\zeta)^2$. By the previous paragraph, $j_0$ is unique. Replacing $\beta$ with $\zeta^{j_0}\beta$ in the statement of the theorem, we may assume that $j_0 = 0$, so $\alpha + \beta \equiv 0 \bmod (1-\zeta)^2$ and $\alpha + \zeta^j\beta \not\equiv 0 \bmod (1-\zeta)^2$ for $1 \leq j \leq p-1$.

Since $\alpha\beta \not\equiv 0 \bmod 1-\zeta$, the common divisor of any two factors on the left side of (8) is precisely $\mathfrak{d}(1-\zeta)$, where $\mathfrak{d} = (\alpha, \beta)$. Note $(1-\zeta)\mathfrak{d}$ is independent of $j$, so it must appear as a $p$th power on the left side of (8). The complementary divisor of $(1-\zeta)\mathfrak{d}$ in $(\alpha + \zeta^j\beta)$

must be a $p$th power by considering the right side of (8) and unique factorization of ideals. Therefore

$$(\alpha + \zeta^j\beta) = \mathfrak{d}(1-\zeta)\mathfrak{c}_j^p, \qquad (\alpha+\beta) = \mathfrak{d}(1-\zeta)^{np-(p-1)}\mathfrak{c}_0^p,$$

where $1 \leq j \leq p-1$ and $(1-\zeta)$ does not divide any of $\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{p-1}$.

Taking ratios, we see that $\mathfrak{c}_j^p\mathfrak{c}_0^{-p}$ is a principal fractional ideal. Since $p$ is regular, $\mathfrak{c}_j\mathfrak{c}_0^{-1}$ is a principal fractional ideal, so $\mathfrak{c}_j\mathfrak{c}_0^{-1} = t_j\mathbf{Z}[\zeta]$, where $t_j \in \mathbf{Q}(\zeta)^\times$ is prime to $1-\zeta$. The equation of ideals

$$(\alpha+\zeta^j\beta)(\alpha+\beta)^{-1} = (t_j)^p(1-\zeta)^{-p(n-1)}$$

can be written as an elementwise equation

$$\frac{\alpha+\zeta^j\beta}{\alpha+\beta} = \frac{\varepsilon_j t_j^p}{(1-\zeta)^{p(n-1)}}, \tag{9}$$

where $1 \leq j \leq p-1$ and $\varepsilon_j \in \mathbf{Z}[\zeta]^\times$.

Now consider, out of nowhere (!), the elementwise equation

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

Note $\overline{\zeta} = \zeta^{p-1}$. Dividing by $\alpha+\beta \neq 0$ and using (9),

$$\frac{\zeta\varepsilon_{p-1}t_{p-1}^p}{(1-\zeta)^{p(n-1)}} + \frac{\varepsilon_1 t_1^p}{(1-\zeta)^{p(n-1)}} - (1+\zeta) = 0.$$

Clearing denominators,

$$\zeta\varepsilon_{p-1}t_{p-1}^p + \varepsilon_1 t_1^p - (1+\zeta)(1-\zeta)^{p(n-1)} = 0. \tag{10}$$

Write $t_j = x_j/y_j$ for some $x_j, y_j \in \mathbf{Z}[\zeta]$. Since $t_j$ is prime to $1-\zeta$ and $1-\zeta$ generates a prime ideal, $x_j$ and $y_j$ are each divisible by the same power of $1-\zeta$. We can remove this factor from both $x_j$ and $y_j$ and thus assume $x_j$ and $y_j$ are prime to $1-\zeta$. Feeding the formulas $t_1 = x_1/y_1$ and $t_{p-1} = x_{p-1}/y_{p-1}$ into (10) and then clearing denominators,

$$\zeta\varepsilon_{p-1}c_{p-1}^p + \varepsilon_1 c_1^p - (1+\zeta)(1-\zeta)^{p(n-1)}c_0^p = 0$$

where $c_0, c_1, c_{p-1} \in \mathbf{Z}[\zeta]$ are prime to $(1-\zeta)$. Dividing by the (unit) coefficient of $c_{p-1}^p$,

$$c_{p-1}^p + \frac{\varepsilon_1}{\zeta\varepsilon_{p-1}}c_1^p - \frac{1+\zeta}{\zeta\varepsilon_{p-1}}(1-\zeta)^{p(n-1)}c_0^p = 0. \tag{11}$$

This equation is very similar to (7), with $n$ replaced by $n-1$. Note, for instance, the coefficient of $(1-\zeta)^{p(n-1)}c_0^p$ is a unit in $\mathbf{Z}[\zeta]$ and $c_0, c_1, c_{p-1}$ are prime to $(1-\zeta)$.

Comparing (7) and (11), note the coefficient of $\beta^p$ is 1 while the coefficient of $c_1^p$ is surely not 1. If the coefficient of $c_1^p$ were a $p$th power (necessarily the $p$th power of another unit, since the coefficient is itself a unit), then we could absorb the coefficient into $c_1^p$ and obtain an equation just like that in the statement of the theorem, with $n$ replaced by $n-1$.

To show the coefficient of $c_1^p$ is a $p$th power, consider (11) modulo $p$:

$$c_{p-1}^p + \frac{\varepsilon_1}{\zeta\varepsilon_{p-1}}c_1^p \equiv 0 \bmod p\mathbf{Z}[\zeta].$$

Since $c_1^p$ and $c_{p-1}^p$ are congruent to rational integers mod $p\mathbf{Z}[\zeta]$ (see (2)), and also $c_1$ is prime to $1-\zeta$, we can invert $c_1$ modulo $p\mathbf{Z}[\zeta]$ to get

$$\frac{\varepsilon_1}{\zeta\varepsilon_{p-1}} \equiv \text{ rational integer } \bmod p\mathbf{Z}[\zeta].$$

Now we invoke a deep fact.

Kummer's Lemma: Let $p$ is regular and $u$ be a unit in $\mathbf{Z}[\zeta]$. If there is some $m \in \mathbf{Z}$ such that $u \equiv m \bmod p\mathbf{Z}[\zeta]$, then $u$ is the $p$th power of a unit in $\mathbf{Z}[\zeta]$.

For proofs of Kummer's Lemma, see [1, p. 377] or [6, Theorem 5.36]. Somewhere in any proof of Kummer's Lemma, one has to make a connection between units in $\mathbf{Z}[\zeta]$ and the class number $h_p$. Two connections, which each serve as the basis for a proof of Kummer's Lemma, are the facts that 1) adjoining the $p$th root of a unit to $\mathbf{Q}(\zeta)$ is an abelian unramified extension, whose degree over $\mathbf{Q}(\zeta)$ must divide $h_p$ by class field theory, and 2) the index of the group of real cyclotomic units in $\mathbf{Q}(\zeta)$ as a subgroup of all real units is equal to the "plus part" of $h_p$ [6, Theorem 8.2].

Thanks to Kummer's Lemma, we can replace the coefficient of $c_1^p$ in (11) with 1, obtaining

$$c_{p-1}^p + c_1^p + \varepsilon'(1-\zeta)^{p(n-1)}c_0^p = 0.$$

This has the same form and conditions as the original equation, but $n \geq 1$ is replaced with $n-1$. Since we showed that in fact $n \geq 2$, we have $n-1 \geq 1$, so we have a contradiction by descent. □

The greatest difference between our proofs of Case I and Case II is the use of Kummer's Lemma in Case II, which amounts to using subtle relations between the class number and the unit group of the $p$th cyclotomic field. We could afford to be largely ignorant about $\mathbf{Z}[\zeta]^\times$ in the proof of Case I for regular primes, and the proof was much simpler.

Even if $p$ is not regular, Case I continues to be easier than Case II. That is, it is much easier to show (when using cyclotomic methods) that there isn't a solution to $x^p + y^p = z^p$ with $p$ not dividing $xyz$ than with $p$ dividing $xyz$. For example, a theorem of Wieferich [3, p. 221] says that if $x^p + y^p = z^p$ and $p$ doesn't divide any of $x, y, z$, then $2^{p-1} \equiv 1 \bmod p^2$. The only primes less than $3 \times 10^9$ satisfying this congruence are 1093 and 3511. Mirimanoff proved that also $3^{p-1} \equiv 1 \bmod p^2$ if Case I has a solution, and neither 1093 nor 3511 satisfies this congruence. So that settles Case I for all odd primes below $3 \times 10^9$. In fact, it has been shown [6, p. 181] that a counterexample to Fermat in Case I for exponent $p$ implies $q^{p-1} \equiv 1 \bmod p^2$ for all primes $q \leq 89$, and that settles Case I for $p < 7.57 \times 10^{17}$.

Kummer originally thought he proved a much stronger result than Fermat's Last Theorem for regular primes. He believed he had shown for regular $p$ that the equation $\alpha^p + \beta^p = \gamma^p$ has no solution in nonzero $\alpha, \beta, \gamma$ coming from the ring $\mathbf{Z}[\zeta]$, not only from the ring $\mathbf{Z}$. However, in the course of his proof he assumed $\alpha$, $\beta$, and $\gamma$ are pairwise relatively prime. Since $\mathbf{Z}[\zeta]$ is usually not a UFD, this kind of assumption makes no sense. Nevertheless, Kummer's proof was basically sound and Hilbert patched it up. For a proof of this more general result, see [2, Chap. 11] or [4, §V.3]. As in the treatment above, there are two cases: when none of $\alpha, \beta, \gamma$ is divisible by $1-\zeta$ and when one of them is divisible by $1-\zeta$. (Even if $\mathbf{Z}[\zeta]$ is not a UFD, $1-\zeta$ does generate a prime ideal, so divisibility by $1-\zeta$ behaves nicely.) The second case of this argument is basically identical to the proof we gave of Case II above.

Exercises

1. Find a regular prime $p \geq 3$ and an integer $m \geq 1$ for which the congruence $x^p + y^p \equiv z^p \bmod (1-\zeta_p)^m$ has no solutions $x, y, z \in \mathbf{Z}[\zeta_p]$ which are all prime to $1-\zeta_p$.

2. Prove $\mathbf{Z}[\zeta_p]/(1-\zeta_p)^2 \cong (\mathbf{Z}/p)[X]/(1-X)^2$ for $p \geq 3$ and not for $p = 2$.

3. Let $K$ be a number field, with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distinct primes of $\mathcal{O}_K$. For $\alpha \in K^\times$ with $\mathrm{ord}_{\mathfrak{p}_j}(\alpha) = 0$ for all $j$, prove $\alpha = x/y$ where $x, y \in \mathcal{O}_K$ are both prime to all the $\mathfrak{p}_j$. Prove this first in the easier case when all the $\mathfrak{p}_j$ are principal, and then when they need not be principal. (Hint: Thinking of primes as points and the multiplicity of a prime as an order of vanishing, the proof of Prop. 2(2) on p. 40 of Fulton's *Algebraic Curves* may provide some inspiration.)

## References

[1] Borevich, Z. I. and I. R. Shafarevich. "Number Theory," Academic Press, New York, 1966.
[2] Grosswald, E., "Topics from the Theory of Numbers," Macmillan, New York, 1965.
[3] Ireland, K. and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer–Verlag, New York, 1990.
[4] Ribenboim, P., "13 Lectures on Fermat's Last Theorem," Springer–Verlag, New York, 1979.
[5] van der Poorten, A., "Notes on Fermat's Last Theorem," J. Wiley & Sons, New York, 1996.
[6] Washington, L. "An Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York, 1997.