AN EASY CASE OF FERMAT'S LAST THEOREM

This writeup based on chapter 1 of *Cyclotomic Fields* by Washington. See also chapter 1 of *Number Fields* by Marcus.

Let $p \geq 5$ be an odd prime. Consider the first primitive pth complex root of unity,

$$\zeta = \zeta_p = e^{2\pi i/p},$$

and the ring $\mathbb{Z}[\zeta]$ of polynomials in ζ having integer coefficients. Suppose that the prime p is such that

$$\mathbb{Z}[\zeta] \textit{ is a unique factorization domain.}$$

We show for such p, the *first case* of the Fermat equation,

$$x^p + y^p = z^p, \quad p \nmid xyz, \qquad x, y, z \text{ nonzero integers},$$

has no solution.

Unique factorization in $\mathbb{Z}[\zeta]$ holds for $p = 2, 3, 5, 7, 11, 13, 17, 19$, but it fails for $p = 23$ and it fails in general. Chapter 1 of Washington's *Cyclotomic Fields* proves the first case of Fermat's Last Theorem under the weaker assumption that p does not divide the class number of $\mathbb{Q}(\zeta)$. The argument is essentially similar to the unique factorization case, the crucial moment being that an ideal whose pth power is principal must itself be principal.

1. Basic facts about $\mathbb{Z}[\zeta]$

This section makes no reference to the assumption that $\mathbb{Z}[\zeta]$ is a unique factorization domain.

Because $\sum_{i=0}^{p-1} \zeta^i = 0$ by the finite geometric sum formula, $\mathbb{Z}[\zeta]$ consists of the $\mathbb{Z}$-linear combinations of any $p-1$ elements of $\{1, \zeta, \ldots, \zeta^{p-1}\}$. Here are some facts about $\mathbb{Z}[\zeta]$, to be cited below.

- Every unit (invertible element) u of $Z[\zeta]$ takes the form $u = \zeta^r u_o$ where, with an overbar denoting complex conjugation, $\overline{u}_o = u_o$. Indeed, the quotient $u/\overline{u}$ is a unit having size 1 as a complex number. As such it at least plausibly takes the form ζ^{2r} (this point will be addressed at the end of this writeup), from which $\zeta^r \overline{u} = \zeta^{-r} u$. Let $u_o = \zeta^{-r} u$, so that indeed $u = \zeta^r u_o$ and $\overline{u}_o = \zeta^r \overline{u} = \zeta^{-r} u = u_o$.
- If $\alpha \in \mathbb{Z}[\zeta]$ then $\alpha^p \equiv_{p\mathbb{Z}[\zeta]} a$ for some $a \in \mathbb{Z}$, because $\alpha = \sum_{i=0}^{p-2} a_i \zeta^i$ where each a_i lies in $\mathbb{Z}$, and so $\alpha^p \equiv_{p\mathbb{Z}[\zeta]} \sum_{i=0}^{p-2} a_i^p \in \mathbb{Z}$.
- The ring structure of $\mathbb{Z}[\zeta]$ makes it a $\mathbb{Z}$-module. If an element $\alpha = \sum_{i=0}^{p-1} a_i \zeta^i$ of $\mathbb{Z}[\zeta]$ has at least one a_i equal to 0, so that the powers of ζ that are present form a $\mathbb{Z}$-linearly independent set (here we use the fact that the polynomial $\sum_{i=0}^{p-1} x^i$ is irreducible in $\mathbb{Z}[x]$), and if some integer n divides α, then n divides each coefficient a_i in $\mathbb{Z}$.

2. The special element $1-\zeta$ of $\mathbb{Z}[\zeta]$

This section shows that $1-\zeta, 1-\zeta^2, \dots, 1-\zeta^{p-1}$ are associate in $\mathbb{Z}[\zeta]$, that $1-\zeta$ is irreducible in $\mathbb{Z}[\zeta]$, and that $(1-\zeta)\mathbb{Z}[\zeta] \cap \mathbb{Z} = p\mathbb{Z}$.

To show that they are associate, consider any $i \in \{1, \dots, p-1\}$. The relation $1-\zeta^i = (1-\zeta)\sum_{k=0}^{i-1} \zeta^k$ shows that $1-\zeta$ divides $1-\zeta^i$ in $\mathbb{Z}[\zeta]$; but also, with $i' \in \{1, \dots, p-1\}$ such that $ii' \equiv 1\ (p)$, the relation

$$1-\zeta = (1-\zeta^i)\sum_{k=0}^{i'-1} \zeta^{ki}$$

shows that $1-\zeta^i$ divides $1-\zeta$ in $\mathbb{Z}[\zeta]$ as well. Thus all of $1-\zeta, 1-\zeta^2, \dots, 1-\zeta^{p-1}$ are associate in $\mathbb{Z}[\zeta]$, because each is associate with $1-\zeta$.

To show that that $1-\zeta$ is irreducible in $\mathbb{Z}[\zeta]$, first note that in the general equality $\prod_{i=1}^{p-1}(x-\zeta^i) = \sum_{j=0}^{p-1} x^j$ (both equal $(x^p-1)/(x-1)$), setting x to 1 gives

$$\prod_{i=1}^{p-1}(1-\zeta^i) = p.$$

Now suppose that $1-\zeta = f(\zeta)g(\zeta)$ where f and g are polynomials over $\mathbb{Z}$. Then $1-\zeta^i = f(\zeta^i)g(\zeta^i)$ for $i = i, \dots, p-1$, and multiplying over i gives, by the previous display,

$$\prod_{i=1}^{p-1} f(\zeta^i) \prod_{i=1}^{p-1} g(\zeta^i) = p.$$

Because the symmetrizations $\prod_{i=1}^{p-1} f(\zeta^i)$ and $\prod_{i=1}^{p-1} g(\zeta^i)$ lie in $\mathbb{Z}$ (here we use some basics of Galois theory and algebraic number theory), they are ± 1 and $\pm p$ without loss of generality and so $f(\zeta)$ is a unit and $g(\zeta)$ is associate to $1-\zeta$ in $\mathbb{Z}[\zeta]$.

The relation $\prod_{i=1}^{p-1}(1-\zeta^i) = p$ shows that the ideal $(1-\zeta)\mathbb{Z}[\zeta] \cap \mathbb{Z}$ of $\mathbb{Z}$ contains $p\mathbb{Z}$, so it equals one of $p\mathbb{Z}$ or $\mathbb{Z}$. It does not equal $\mathbb{Z}$ because $1-\zeta$ is not a unit of $\mathbb{Z}[\zeta]$, and so $(1-\zeta)\mathbb{Z}[\zeta] \cap \mathbb{Z} = p\mathbb{Z}$.

3. Main Proof

Again, assume that p is such that $\mathbb{Z}[\zeta]$ is a unique factorization domain. We show that consequently there exist no nonzero integers x, y, z such that

$$x^p + y^p = z^p, \quad p \nmid xyz.$$

The Fermat equation lets us assume that $\gcd(x, y, z) = 1$, and then that x, y, z are pairwise coprime. Further, the conditions $x \equiv_p y \equiv_p -z$ cannot both hold because they would give $-z^p - z^p \equiv_p z^p$ and so $p \mid 3z$, impossible because $p \geq 5$ and $p \nmid z$. So either $p \nmid x-y$ or $p \nmid x+z$, but in the second case we may replace (y, z) by $(-z, -y)$ and now $p \nmid x-y$; in sum, we may assume that $p \nmid x-y$. We may also note that because $p \nmid z^p = x^p + y^p$ it follows that $p \nmid x+y$. Now the argument is to posit a solution (x, y, z) satisfying all these conditions and derive a contradiction. Again, the conditions are that x, y, z are pairwise coprime and that p divides none of $xyz, x \pm y$.

The Fermat equation $x^p + y^p = z^p$ is

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

The multiplicands $x+y\zeta, x+y\zeta^2, \dots, x+y\zeta^{p-1}$ on the left side are coprime in $\mathbb{Z}[\zeta]$, as follows. If

$$\pi \mid x+y\zeta^i, x+y\zeta^j \quad (\pi \text{ a nonunit})$$

then noting that $\zeta^i - \zeta^j = \zeta^i(1-\zeta^{j-i}) = u(1-\zeta)$ where u is a unit,

$$\pi \mid (x+y\zeta^i) - (x+y\zeta^j) = y(\zeta^i - \zeta^j) = uy(1-\zeta)$$

and with a possibly different unit u,

$$\pi \mid \zeta^j(x+y\zeta^i) - \zeta^i(x-y\zeta^j) = (\zeta^j - \zeta^i)x = u(1-\zeta)x.$$

Thus $\pi \mid 1-\zeta$, because otherwise $\pi \mid x, y$ and so $\pi \mid \gcd(x,y) = 1$. Consequently $\pi = 1-\zeta$ after scaling π by a unit. Now

$$1-\zeta \mid x+y\zeta^i + y(1-\zeta) = x+y$$

and so $x+y$ lies in $(1-\zeta)\mathbb{Z}[\zeta] \cap \mathbb{Z} = p\mathbb{Z}$, but we have noted that this does not hold. So no nonunit π divides $x+y\zeta^i$ and $x+y\zeta^j$ for distinct $i, j \in 0, \dots, p-1$.

The relation $x^p + y^p = z^p$ is now $\prod_{i=0}^{p-1}(x+y\zeta^i) = z^p$ with $x+y\zeta, \dots, x+y\zeta^{p-1}$ coprime in $\mathbb{Z}[\zeta]$. By the assumed unique factorization of $\mathbb{Z}[\zeta]$, each multiplicand is a unit times a pth power, and in particular

$$x+y\zeta = u\alpha^p, \quad u \in \mathbb{Z}[\zeta]^\times,\ \alpha \in \mathbb{Z}[\zeta].$$

From the first bullet of section 1, $u = \zeta^r u_o$ where r is an integer and $\overline{u}_o = u_o$. From the second bullet, $\alpha^p \equiv_{p\mathbb{Z}[\zeta]} a$ where $a \in \mathbb{Z}$. So now,

$$(x+y\zeta)\zeta^{-r} \equiv_{p\mathbb{Z}[\zeta]} u_o a,$$

and similarly with complex conjugates, because $\overline{u}_o = u_o$ and $a \in \mathbb{Z}$,

$$(x+y\zeta^{-1})\zeta^r \equiv_{p\mathbb{Z}[\zeta]} u_o a.$$

Together these two congruences give

$$(x+y\zeta)\zeta^{-r} \equiv_{p\mathbb{Z}[\zeta]} (x+y\zeta^{-1})\zeta^r,$$

and it follows that

$$p \mid x+y\zeta - x\zeta^{2r} - y\zeta^{2r-1} \text{ in } \mathbb{Z}[\zeta].$$

Because $p \geq 5$ the sum in the previous display has at most $p-1$ terms. If $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are distinct then from the third bullet in section 1, because the sum is divisible by p in $\mathbb{Z}[\zeta]$ each of its coefficients is divisible by p in $\mathbb{Z}$. This contradicts the assumption that x and y are coprime. The cases where $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are not all distinct are also handled by the third bullet in section 1 as follows, noting that $1 \neq \zeta$ and $\zeta^{2r} \neq \zeta^{2r-1}$.

- If $\zeta^{2r} = 1$ then $p \mid y\zeta - y\zeta^{-1}$ and so $p \mid y$, contradiction.
- If $\zeta^{2r-1} = 1$ then $p \mid x - y + (y-x)\zeta$ and so $p \mid x-y$, contradiction.
- If $\zeta^{2r} = \zeta$ then $\zeta^{2r-1} = 1$, so this case is already done.
- If $\zeta^{2r-1} = \zeta$ then $p \mid x - x\zeta^2$ and so $p \mid x$, contradiction.

Altogether, the first case of the pth Fermat equation is impossible if $\mathbb{Z}[\zeta]$ is a unique factorization domain.

4. Resolution of a technical point

The first bullet in section 1 says

> *[T]he quotient $u/\overline{u}$ is a unit having size 1 as a complex number. As such it at least plausibly takes the form $\zeta^{2r}\dots$*

We now show that indeed $u/\overline{u} = \zeta^{2r}$ for some r.

Let $\alpha = u/\overline{u}$, an element of $\mathbb{Z}[\zeta]$ such that $\alpha\overline{\alpha} = 1$. Here $\overline{\alpha} = \sigma_{p-1}(\alpha)$ where for $i = 1, \dots, p-1$ the $\mathbb{Z}[\zeta]$ automorphism σ_i fixes $\mathbb{Z}$ and takes ζ to ζ^i. The automorphisms σ_i commute because $(\zeta^i)^{i'} = (\zeta^{i'})^i$, and so in particular, $\overline{\sigma_i(\alpha)} = \sigma_i(\overline{\alpha})$. Compute for any such i,

$$\sigma_i(\alpha)\overline{\sigma_i(\alpha)} = \sigma_i(\alpha)\sigma_i(\overline{\alpha}) = \sigma_i(\alpha\overline{\alpha}) = \sigma_i(1) = 1.$$

That is, not only does α have size 1 as a complex number, but so do all of its conjugates $\sigma_i(\alpha)$.

Now α is a root of unity by a well known argument, as follows. Each power α^n of α satisfies a monic polynomial $f_{\alpha^n}[x] \in \mathbb{Z}[x]$. Because α^n lies in $\mathbb{Z}[\alpha]$, the degree of f_{α^n} is at most the degree of f_α, independently of n. Also, the coefficients of f_{α^n} are the elementary symmetric functions of the conjugates of α^n and these conjugates all have absolute value 1, so the coefficients of f_{α^n} satisfy bounds that are independent of n. Altogether there are only finitely many polynomials f_{α^n}, so only finitely many values α^n, and so α is a root of unity.

As a root of unity in $\mathbb{Z}[\zeta]$, α takes the form ζ^s for some s. Let r be such that $s \equiv_p 2r$ and recall that $\alpha = u/\overline{u}$ to get the desired result $u/\overline{u} = \zeta^{2r}$.