Fermat's Last Theorem
Due: Friday, June 4th

> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.
>
> —Pierre de Fermat

The statement above is commonly known as *Fermat's Last Theorem*. It was found written in the margins of Fermat's copy of *Arithmetica*, an ancient number theory text by Diophantus. In modern language, one might write: If x, y, and z are nonzero integers and n is an integer greater than 2, then

$$x^n + y^n \neq z^n.$$

It was in 1637 that Fermat made this famous note and mentioned his tantalizing "truly marvelous" proof. However, no complete proof was ever found in Fermat's notes or papers. For nearly 400 years, mathematicians tried to prove Fermat's Last Theorem. Some of the greatest minds worked on this problem, including Euler, Legendre, Gauss, Dirichlet, Kummer, and others. While special cases were solved, the general problem resisted all attacks and it was suspected that no complete proof would ever be found. Indeed, in a 1988 episode of *Star Trek: The Next Generation*, entitled *The Royale*, Captain Picard notes that the theorem has not yet been proved—this episode takes place in the year 2365!

The world was astonished when in 1993, after working in secret for 7 years, Andrew Wiles announced a proof of Fermat's last theorem at a mathematics conference. After a careful review of the proof, a small error was found. Nevertheless in 1994 the proof was fixed and the rest is history. Andrew Wiles' proof is extremely sophisticated and consumes around 100 pages. It is a triumph of human thought and comparable only to the greatest achievements of mankind.

The discussion that follows is modeled off of the presentation and exercises found in the following texts, I encourage you to investigate them:

- *Elements of Abstract Algebra* by Allan Clark.
- *Number Fields* by Daniel Marcus
- *Abstract Algebra* by Ronald Solomon.

Basic observations concerning $x^n + y^n = z^n$

We'll start by having you explore some basic facts about the equation

$$x^n + y^n = z^n.$$

Exercise 1 *Given an integer n, classify all trivial integer solutions to*

$$x^n + y^n = z^n.$$

*A **trivial solution** is one where at least one of x, y, or z is zero.*

Exercise 2 *Prove that given n, if there is a nontrivial integer solution to*

$$x^n + y^n = z^n,$$

*then this solution is a multiple of a **pair-wise relatively prime** solution. That is, every solution is a multiple of a solution x, y, z such that*

$$(x, y) = 1, \qquad (x, z) = 1, \qquad (y, z) = 1.$$

Exercise 3 *Explain why if there is a nontrivial solution to*

$$x^n + y^n = z^n,$$

in some euclidean domain, then this solution is a multiple of a pair-wise relatively prime solution in this euclidean domain.

The case when $n = 2$: $x^2 + y^2 = z^2$

In this section, we seek to find integer solutions to the equation:

$$x^2 + y^2 = z^2$$

A solution to such an equation is called a **Pythagorean triple**. Of particular interest to us are Pythagorean triples x, y, z that are pair-wise relatively prime. Pythagorean triples which are pair-wise relatively prime are called **primitive Pythagorean triples.** From our work in Exercise 2, we see that that every Pythagorean triple is a multiple of a primitive Pythagorean triple.

Exercise 4 *Prove that if $m \in \mathbb{Z}$ is a perfect square, then*

$$m \equiv 0 \pmod 4 \qquad \textit{or} \qquad m \equiv 1 \pmod 4.$$

Exercise 5 *Prove that if x, y, z is a primitive Pythagorean triple, then either x is even or y is even, but not both. Moreover, prove that z is odd.*

While we want to find all Pythagorean triples in the integers, we will actually work in the Gaussian integers, $\mathbb{Z}[i]$. Starting with

$$x^2 + y^2 = z^2,$$

we'll factor the left-hand side to obtain

$$(x + yi)(x - yi) = z^2.$$

Exercise 6 *Letting $x + iy$ be as above and $\pi \in \mathbb{Z}[i]$ be a prime element such that $\pi \mid (x+yi)$, prove that $\pi \nmid (x-yi)$. Hint, use the previous exercise to seek a contradiction by comparing how π relates to*

$$(x + yi) + (x - yi) \qquad \text{and} \qquad (x + yi)(x - yi).$$

Lemma 1 *Letting $x+iy$ be as above and u be a unit in $\mathbb{Z}[i]$, we may write*

$$x + yi = u\alpha^2$$

for some unique $\alpha \in \mathbb{Z}[i]$.

Proof Let π be a prime element in $\mathbb{Z}[i]$ such that $\pi \mid (x + yi)$. There exists some exponent $e \in \mathbb{N}$ such that

$$\pi^e \mid (x + yi) \qquad \text{and} \qquad \pi^{e+1} \nmid (x + yi).$$

We claim that e is an even number. Since

$$(x + yi)(x - yi) = z^2$$

and by Exercise 6, $\pi \nmid (x - yi)$,

$$\pi^e \mid z^2 \qquad \text{and} \qquad \pi^{e+1} \nmid z^2.$$

In particular we see that e must be even. Since $\mathbb{Z}[i]$ is a UFD, we obtain

$$x + yi = u \cdot \prod_{i=1}^{s} \pi_i^{e_i}.$$

We'll have that each e_i is even and then can write

$$\alpha = \prod_{i=1}^{s} \pi_i^{e_i/2}.$$

Hence, $(x + yi) = u\alpha^2$. ■

Now set $\alpha = a + bi$ and note that the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. We now see that one of the following will hold:

$$(x + yi) = u\alpha^2 = a^2 + 2abi - b^2 \qquad (u = 1) \qquad (1)$$

$$(x + yi) = u\alpha^2 = -a^2 - 2abi + b^2 \qquad (u = -1) \qquad (2)$$

$$(x + yi) = u\alpha^2 = a^2 i + 2ab - b^2 i \qquad (u = i) \qquad (3)$$

$$(x + yi) = u\alpha^2 = -a^2 i - 2ab + b^2 i \qquad (u = -i) \qquad (4)$$

Exercise 7 *Explain why WLOG we may ignore equations* (3) *and* (4)*.*

Grouping the real terms and imaginary terms together we conclude that if x, y, and z are Pythagorean triples, then

$$x = \pm(a^2 - b^2), \qquad y = \pm 2ab, \qquad z = \pm(a^2 + b^2).$$

This classifies all Pythagorean triples. Note that it was critical to this argument that $\mathbb{Z}[i]$ is a UFD.

The case when $n = 4$: $x^4 + y^4 \neq z^4$

If $x^4 + y^4 = z^4$ has a nontrivial integer solution, then so does $x^4 + y^4 = w^2$. WLOG w is a positive integer. Let x, y, and w be a solution with the smallest possible value for w.

Exercise 8 *Prove that WLOG, x is odd.*

Exercise 9 *Explain why we may write*

$$x^2 = a^2 - b^2, \qquad y^2 = 2ab, \qquad w = a^2 + b^2,$$

with a and b positive, $(a, b) = 1$, and exactly one of a or b being even.

Exercise 10 *Explain why we may write*

$$x = c^2 - d^2, \qquad b = 2cd, \qquad a = c^2 + d^2,$$

with c and d positive, $(c, d) = 1$, and exactly one of c or d being even.

Exercise 11 *Prove that c, d, and a are pairwise relatively prime. Noting that $y^2 = 4acd$, conclude that c, d, and a are all perfect squares, say*

$$c = r^2, \qquad d = s^2, \qquad a = t^2.$$

Exercise 12 *Explain why we must conclude that $r^4 + s^4 = t^2$, and that $t < w$.*

Exercise 13 *Explain how we have proved that $x^4 + y^4 = z^4$ has no nontrivial integer solutions.*

The case when $n = 3$: $x^3 + y^3 \neq z^3$

While Fermat's Last Theorem for $n = 4$ boiled down to understanding Pythagorean triples, Fermat's Last Theorem for $n = 3$ is a bit trickier. We'll start the proof with the following exercise from our text:

Exercise 14 *Show that the ring $\mathbb{Z}[\omega]$, where*

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$$

is equal to the set

$$\{a + b\omega : a, b \in \mathbb{Z}\}.$$

Exercise 15 *Given a detailed plot of 1, ω, and ω^2 in the complex plane.*

Exercise 16 *Prove that $\mathbb{Z}[\omega]$ is a euclidean domain where*

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$$

and $d(a + b\omega) = a^2 - ab + b^2$. Hint, see the proof of the fact that $\mathbb{Z}[i]$ is a euclidean domain and think about the following elementary claim from geometry: Given a rhombus of side length a, any point in the rhombus is at most of distance a from any corner.

We will now prove that the equation

$$x^3 + y^3 = z^3$$

has no nontrivial solutions in $\mathbb{Z}[\omega]$. Since $\mathbb{Z} \subset \mathbb{Z}[\omega]$, this will prove Fermat's Last Theorem for $n = 3$. Note that by Exercise 2 and Exercise 3, we need only prove that there cannot be a pair-wise relatively prime solution in $\mathbb{Z}[\omega]$. The next exercise will give some indication as to why we have chosen to work in $\mathbb{Z}[\omega]$.

Exercise 17 *Prove that in $\mathbb{Z}[\omega]$*

$$x^3 + y^3 = (x + y)(x\omega + y\omega^2)(x\omega^2 + y\omega).$$

Exercise 18 *Prove that*

$$(x + y) + (x\omega + y\omega^2) + (x\omega^2 + y\omega) = 0.$$

At this point, we'll need some more experience working in $\mathbb{Z}[\omega]$ before we can proceed. We'll start by setting $\lambda = 1 - \omega$ and considering the following exercise:

Exercise 19 *Prove that λ is a prime number in $\mathbb{Z}[\omega]$.*

Exercise 20 *Compute λ^2 and use this to prove that $\lambda \mid 3$, and hence 3 is not prime in $\mathbb{Z}[\omega]$.*

Lemma 2 *Every number in $\mathbb{Z}[\omega]$ is congruent to 0, 1, or -1 modulo λ.*

Proof Note that since $\lambda = 1 - \omega$, we have that $\omega = 1 - \lambda$. Hence given $a + b\omega \in \mathbb{Z}[\omega]$, we have

$$\begin{aligned} a + b\omega &= a + b(1 - \lambda) \\ &= a + b - b\lambda. \end{aligned}$$

Hence $a + b\omega \equiv a + b \pmod{\lambda}$. Since λ divides 3, our congruence is established. ■

Exercise 21 *Prove that given any $\alpha \in \mathbb{Z}[\omega]$, λ divides the product:*

$$\alpha \cdot (\alpha + 1) \cdot (\alpha - 1)$$

From this we obtain the following lemma:

Lemma 3 *Given $\xi \in \mathbb{Z}[\omega]$, if λ does not divide ξ, then*

$$\xi^3 \equiv \pm 1 \pmod{\lambda^4}.$$

Proof By Lemma 2, $\xi \equiv \pm 1 \pmod{\lambda}$. In other words, $\xi = \pm 1 + \alpha\lambda$. So

$$\begin{aligned} \xi^3 \mp 1 &= (\xi \mp 1)(\xi \mp \omega)(\xi \mp \omega^2) && (\bigstar) \\ &= (\pm 1 + \alpha\lambda \mp 1)(\pm 1 + \alpha\lambda \mp \omega)(\pm 1 + \alpha\lambda \mp \omega^2) \\ &= (\alpha\lambda)(\pm 1 + \alpha\lambda \mp \omega)(\pm 1 + \alpha\lambda \mp \omega^2). \end{aligned}$$

With some algebra we may write

$$\begin{aligned} (\alpha\lambda)(\pm 1 + \alpha\lambda \mp \omega)(\pm 1 + \alpha\lambda \mp \omega^2) &= \alpha\lambda \cdot (\alpha \pm 1)\lambda \cdot (\alpha \mp 1)\lambda && (\bigstar\bigstar) \\ &= \lambda^3 \cdot \alpha \cdot (\alpha \pm 1) \cdot (\alpha \mp 1). \end{aligned}$$

By the exercise above, λ divides $\alpha \cdot (\alpha \pm 1) \cdot (\alpha \mp 1)$ and hence λ^4 divides $\xi^3 \mp 1$, showing that $\xi^3 \equiv \pm 1 \pmod{\lambda^4}$. ■

Exercise 22 *Carefully explain the lines* ($\bigstar$) *and* ($\bigstar\bigstar$) *above.*

Corollary 4 *If x, y, and z are elements of $\mathbb{Z}[\omega]$ such that*

$$x^3 + y^3 + z^3 = 0,$$

then at least one of x, y, or z are divisible by λ.

Proof Seeking a contradiction, suppose that none of x, y, or z are divisible by λ. In this case,

$$x^3 \equiv \pm 1 \pmod{\lambda^4}, \qquad y^3 \equiv \pm 1 \pmod{\lambda^4}, \qquad z^3 \equiv \pm 1 \pmod{\lambda^4}.$$

Since λ^4 clearly divides 0, λ^4 must divide the right-hand side of the equation above, namely $x^3 + y^3 + z^3$. Examining the values of the norm d of $\mathbb{Z}[\omega]$, $1 \leqslant d(x^3 + y^3 + z^3) \leqslant 9$, but $d(\lambda) = 3$ and so $d(\lambda^4) = 81$. Hence λ^4 cannot divide $x^3 + y^3 + z^3$, a contradiction. ■

Exercise 23 *Prove that if $x, y, z \in \mathbb{Z}[\omega]$ is a nontrivial solution for*

$$x^3 + y^3 = z^3,$$

then WLOG $\lambda \mid z$.

Exercise 24 *Explain why if $x, y, z \in \mathbb{Z}[\omega]$ is a nontrivial solution for*

$$x^3 + y^3 = z^3$$

where $\lambda \mid z$, then there is a minimal positive integer e along with a solution x', y', z' where $\lambda^e \mid z'$ and $\lambda^{e+1} \nmid z'$.

We are now ready to finish our proof. Seeking a contradiction, if Fermat's Last Theorem is false for $n = 3$ in $\mathbb{Z}[\omega]$, then there exists a minimal positive integer e along with a solution $x^3 + y^3 = z^3$ such that:

(a) x, y, and z are pair-wise relatively prime in $\mathbb{Z}[\omega]$.

(b) $\lambda^e \mid z$ and $\lambda^{e+1} \nmid z$.

We will arrive at a contradiction by showing that e as described above cannot be minimal. Considering a minimal solution, $x, y, z \in \mathbb{Z}[\omega]$, by Exercise 17 we have that

$$(x + y)(x\omega + y\omega^2)(x\omega^2 + y\omega) = z^3.$$

Since $\lambda \mid z$, we see that $\lambda \mid (x + y)(x\omega + y\omega^2)(x\omega^2 + y\omega)$.

Exercise 25 *Since $(x, y) = 1$, there exists $u, v \in \mathbb{Z}$ such that*

$$ux + vy = 1.$$

Briefly explain how the fact that λ is prime along with the following computation

$$\begin{aligned}
\lambda &= (v - u\omega)(x + y) + \omega^2(v - u)(x\omega + y\omega^2), \\
\lambda &= (v\omega - u)(x\omega + y\omega^2) + (u\omega - v)(x\omega^2 + y\omega), \\
\lambda &= \omega^2(v - u)(x\omega^2 + y\omega) + (u - v\omega)(x + y),
\end{aligned}$$

shows that λ is the GCD of $(x + y)$, $(x\omega + y\omega^2)$, and $(x\omega^2 + y\omega)$.

Exercise 26 *Prove that there exist $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ such that*

$$(x + y) = \lambda\alpha, \qquad (x\omega + y\omega^2) = \lambda\beta, \qquad (x\omega^2 + y\omega) = \lambda\gamma,$$

with α, β, and γ pair-wise relatively prime in $\mathbb{Z}[\omega]$.

The upshot of the exercises above is that

$$\begin{aligned}
(x + y)(x\omega + y\omega^2)(x\omega^2 + y\omega) &= z^3 \\
\lambda\alpha \cdot \lambda\beta \cdot \lambda\gamma &= z^3 \\
\alpha\beta\gamma &= \frac{z^3}{\lambda^3}.
\end{aligned}$$

Since α, β, and γ are pair-wise relatively prime in $\mathbb{Z}[\omega]$, they all must be perfect cubes. Here it is of crucial importance that $\mathbb{Z}[\omega]$ is a UFD. Hence there exist x_0, y_0, and z_0 pair-wise relatively prime in $\mathbb{Z}[\omega]$ such that

$$x_0^3 = \alpha, \qquad y_0^3 = \beta, \qquad z_0^3 = \gamma.$$

Exercise 27 *Prove that $\alpha + \beta + \gamma = 0$.*

We have now found pair-wise relatively prime $x_0, y_0, z_0 \in \mathbb{Z}[\omega]$ such that

$$x_0^3 + y_0^3 + z_0^3 = 0.$$

By Corollary 4, we see that λ must divide one of these elements.

Exercise 28 *Explain why we must conclude that $\lambda^{e+1} \mid z$.*

Exercise 29 *Explain how we have just proved that $x^3 + y^3 = z^3$ has no nontrivial integer solutions.*

Final thoughts

In the proof of Fermat's Last Theorem for $n = 3$, it was essential that we had unique factorization in $\mathbb{Z}[\omega]$. One obstacle to finding a general proof is the fact that Kummer rings, rings of the form $\mathbb{Z}[\zeta_n]$ where $\zeta_n = e^{2\pi i/n}$, are not necessarily UFD's. Andrew Wiles avoided this obstacle by taking a completely different approach—he proved the Taniyama-Shimura Conjecture. Interestingly enough, Wiles' proof of Fermat's Last Theorem actually only covers the cases when $n \geqslant 5$. Hence, the work we did above is still a necessary part of the proof.

We have now classified all Pythagorean triples and completed proofs of Fermat's Last Theorem for $n = 3$, and $n = 4$. We have given but one proof of each of these results. Other proofs exist—and they are fascinating.