Fermat's Last Theorem

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Consider the Diophantine equation $x^n + y^n = z^n$.

If $n = 2$, we have seen that there are an infinitude of solutions that can (essentially) be parametrized by $\mathbb{Q}$.

Around 1637, in a now-famous marginal note, Fermat claimed to "have discovered a truly wonderful proof" that when $n \geq 3$, this equation has *no* solutions in $\mathbb{N}$, "but the margin is too small to contain it."

A complete proof of Fermat's conjecture eluded mathematicians for over 350 years, when, finally, in the mid 1990s, using the theories of modular forms and elliptic curves, Andrew Wiles finally succeeded in proving what is popularly called "Fermat's Last Theorem."

Fermat's Equation

For $n \geq 3$, we will call the Diophantine equation $x^n + y^n = z^n$ *Fermat's equation (of degree n)*.

We will say that a solution to Fermat's equation is *nontrivial* if $x, y, z \in \mathbb{N}$.

Fermat's conjecture is that, for any $n \geq 3$, there are *no* nontrivial solutions to the equation bearing his name.

Claim. To prove Fermat's conjecture, it suffices to assume $n = 4$ or that n is an odd prime.

Proof. If $n \geq 3$ is a power of two, then $n = 4k$ for some $k \in \mathbb{N}$.

We then have

$$x^n + y^n = z^n \iff (x^k)^4 + (y^k)^4 = (z^k)^4,$$

so that a nontrivial solution of the degree n equation yields a nontrivial solution of the degree 4 equation.

Otherwise, $n = pk$ for some odd prime p, and we have

$$x^n + y^n = z^n \iff (x^k)^p + (y^k)^p = (z^k)^p.$$

Hence a nontrivial solution of the degree n equation yields a nontrivial solution of the degree p equation.

The result follows. □

Infinite Descent

Fermat himself provided the first proof of his conjecture in the case $n = 4$.

In fact, that he discovered the proof of this special case *after* he wrote his marginal note on the general case strongly suggests that Fermat realized his “remarkable” proof was flawed.

We will give Fermat’s (correct) proof, which uses the *Method of Infinite Descent*.

From an assumed nontrivial solution we will construct another “smaller” one. Repeating this procedure we obtain an indefinitely decreasing sequence in $\mathbb{N}$, which is impossible.

This means that there can be no nontrivial solutions at all!

Fermat actually proved the following stronger result, of which his theorem (for $n = 4$) is a corollary.

Theorem 1 (Fermat)

The Diophantine equation $x^4 + y^4 = z^2$ has no solution in $\mathbb{N}$.

Proof. Suppose otherwise. Then there exist $x, y, z \in \mathbb{N}$ so that $x^4 + y^4 = z^2$.

Let $d = \gcd(x, y)$. Then

$$z^2 = d^4 \left(\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 \right) \;\Rightarrow\; d^4 | z^2 \;\Rightarrow\; d^2 | z \text{ (HW)}.$$

Therefore $z/d^2 \in \mathbb{N}$ and

$$\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{z}{d^2}\right)^2.$$

That is, $(x/d, y/d, z/d^2)$ is a nontrivial solution of the same equation, with $\gcd(x/d, y/d) = 1$.

So we may assume $\gcd(x, y) = 1$. It then follows that (x^2, y^2, z) is a primitive Pythagorean triple.

Interchanging x and y, if necessary, we conclude that there exist relatively prime $s > r > 0$ of opposite parity so that

$$x^2 = 2rs, \;\; y^2 = s^2 - r^2, \;\; z = r^2 + s^2.$$

If s is even and r is odd, we then have

$$1 \equiv y^2 \equiv -r^2 \equiv -1 \equiv 3 \pmod 4,$$

which is impossible.

Thus s is odd and $r = 2t$ for some $t \in \mathbb{N}$.

We then have $x^2 = 2rs = 4st$, which implies $(x/2)^2 = st$.

Since $1 = \gcd(r, s) = \gcd(2t, s)$, we must have $\gcd(s, t) = 1$.

By one of our lemmas from last time, we find that $s = a^2$ and $t = b^2$ for some $a, b \in \mathbb{N}$.

We now return to the relationship

$$y^2 = s^2 - r^2 \ \Leftrightarrow \ r^2 + y^2 = s^2,$$

which, since $\gcd(r, s) = 1$, tells us that (r, y, s) is a primitive pythagorean triple.

As we already know that r is even, this means there exist relatively prime $v > u > 0$ of opposite parity so that

$$r = 2uv, \ \ y = v^2 - u^2, \ \ s = u^2 + v^2.$$

We than have

$$2uv = r = 2t = 2b^2 \ \Rightarrow \ uv = b^2 \ \Rightarrow \ u = \xi^2, v = \upsilon^2,$$

for some $\xi, \upsilon \in \mathbb{N}$, since $\gcd(u, v) = 1$, by the earlier referenced lemma.

We now have $s = u^2 + v^2$, $s = a^2$, $u = \xi^2$ and $v = \upsilon^2$.

Substituting the final three equations into the first we obtain

$$\xi^4 + \upsilon^4 = a^2.$$

That is, ξ, υ and a furnish another nontrivial solution to $x^4 + y^4 = z^2$,and that $\gcd(\xi, \upsilon) = 1$ since $\gcd(u, v) = 1$.

Notice that

$$a \le a^2 = s \le s^2 < r^2 + s^2 = z.$$

So every nontrivial solution to $x^4 + y^4 = z^2$ with $\gcd(x, y) = 1$ yields another *with a smaller z value*.

So if a *single* nontrivial solution to $x^4 + y^4 = z^2$ exists, we can construct an indefinitely decreasing sequence of z values in $\mathbb{N}$.

This contradicts the Well Ordering Principle, which means no such solution can exist. □

Remarks.

- One can show that Fermat's proof amounts to repeated division by 2 on the *elliptic curve* (an abelian group) $y^2 = x^3 - 4x$.
- In fact, a sophisticated generalization of the Method of Infinite Descent is central to the proof of the Mordell-Weil Theorem in the theory of elliptic curves.

Fermat's Equation of Degree 4

We can now easily prove:

Corollary 1

The Diophantine equation $x^4 + y^4 = z^4$ has no solution in $\mathbb{N}$.

Proof. This follows from the theorem and the fact that

$$x^4 + y^4 = z^4 \;\Rightarrow\; x^4 + y^4 = (z^2)^2.$$

□

So it "only" remains to prove Fermat's conjecture for odd prime degree.

Fermat's "Remarkable" Proof

So what was Fermat's "remarkable" proof? One can only speculate, but many believe it went as follows.

Recall *Euler's formula*:

$$e^{i\theta} = \cos\theta + i\sin\theta,$$

where $\theta \in \mathbb{R}$ and $i = \sqrt{-1}$.

Using the addition formulae for sine and cosine, one can use Euler's formula to show that

$$e^{i(\theta+\phi)} = e^{i\theta}e^{i\phi}.$$

This, in turn, implies the familiar law of exponents

$$(e^{i\theta})^n = e^{in\theta},$$

for $n \in \mathbb{Z}$.

Let p be an odd prime and set $\zeta_p = e^{2\pi i/p}$. Then

$$\zeta_p^p = (e^{2\pi i/p})^p = e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1.$$

This tells us that, as an element of $\mathbb{C}^\times$, ζ_p has (multiplicative) order dividing p.

Since p is prime, the order is therefore either 1 or p.

Since $\zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} \neq 1$ (exercise), it must be that the order of ζ_p is p.

Note that for any k we have

$$(\zeta_p^k)^p = \zeta_p^{kp} = (\zeta_p^p)^k = 1.$$

So ζ_p^k is a root of the polynomial $X^p - 1$, which has no more that p complex roots.

Because $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ are all distinct, we conclude that

$$X^p - 1 = \prod_{k=0}^{p-1}(X - \zeta_p^k).$$

Now replace X by $-X$:

$$-X^p - 1 = \prod_{k=0}^{p-1}(-X - \zeta_p^k) = (-1)^p \prod_{k=0}^{p-1}(X + \zeta_p^k) = -\prod_{k=0}^{p-1}(X + \zeta_p^k)$$

which implies

$$X^p + 1 = \prod_{k=0}^{p-1}(X + \zeta_p^k).$$

Now set $X = x/y$, with $x, y \in \mathbb{N}$, and clear denominators to get

$$x^p + y^p = \prod_{k=0}^{p-1}(x + y\zeta_p^k)$$

That is, in the *number ring*

$$\mathbb{Z}[\zeta_p] = \{f(\zeta_p) \,|\, f(X) \in \mathbb{Z}[X]\},$$

any solution to $x^p + y^p = z^p$ yields the factorization

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

If the analogue of the FTA holds in $\mathbb{Z}[\zeta_p]$, one can show that this implies

$$x + y\zeta_p = u\alpha^p,$$

where $\alpha \in \mathbb{Z}[\zeta_p]$ and $u \in \mathbb{Z}[\zeta_p]^\times$ (i.e. u has a multiplicative inverse in $\mathbb{Z}[\zeta_p]$).

A bit more work (see *Number Fields* by Marcus) shows that this leads to a contradiction.

So if the elements of $\mathbb{Z}[\zeta_p]$ have unique prime factorizations, $x^p + y^p = z^p$ has no solutions in $\mathbb{N}$!

Many believe that Fermat's alleged proof was along these lines.

But there's a problem: $\mathbb{Z}[\zeta_p]$ *does not* always have the unique factorization property. The first counterexample is $\mathbb{Z}[\zeta_{23}]$.

In fact, there are only finitely many values of p for which the unique factorization hypothesis holds.

Ideals and Regular Primes

In the 19th century, Kummer was able to salvage most of the argument above by considering the so-called *class number* of $\mathbb{Z}[\zeta_p]$, which has to do with *ideal theory*.

He showed that if p does not divide the class number of $\mathbb{Z}[\zeta_p]$, then Fermat's conjecture is true for degree p.

Such primes are called *regular*.

But this is still only a partial victory: it is known that there are infinitely many irregular primes, while the number of regular primes is unknown.

Another Descent

One can also use the Method of Infinite descent to prove the following familiar result.

Theorem 2

Let $n \in \mathbb{Z}$. If n is not a perfect square, then $\sqrt{n}$ is irrational.

Proof. Assume, for the sake of contradiction, that n is not a perfect square, but that $\sqrt{n}$ is rational.

Since n is not a perfect square, we then have

$$\sqrt{n} = k + \frac{a}{b},$$

where $k = [\sqrt{n}]$,$a, b \in \mathbb{N}$ and $0 < a/b < 1$, i.e. $a < b$.

Multiply both sides by b and square to obtain

$$b^2 n = (kb + a)^2 = k^2 b^2 + 2abk + a^2 \;\Rightarrow\; b | a^2 \;\Rightarrow\; a^2 = bc,$$

for some $c \in \mathbb{N}$.

This means that $c/a = a/b$ both represent $\sqrt{n} - [\sqrt{n}]$, but c/a has a smaller denominator than a/b (since $a < b$).

Repeating this process we obtain a strictly decreasing sequence of positive integers, which contradicts the Well Ordering Principle.

□