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

William M. Faucette

University of West Georgia

Summer 2021

Outline

Diophantine Equations

A Little Number Theory

Diophantine Equations

A **Diophantine equation** is a polynomial equation, usually involving two or more variables, so that the only solutions of interest are the integer ones.

A Diophantine equation of degree one is a **linear Diophantine equation**.

As an example, the Diophantine $3x + 2y = 10$ has solutions

$$\begin{cases} x = 2 + 2t \\ y = 2 - 3t \end{cases}, \quad t \in \mathbb{Z}.$$

First Problem: The Case $n = 2$

First Problem: The Case $n = 2$

Pythagorean Triples

Unquestionably one of the most famous Diophantine equations is that of finding nontrivial integer solutions to the sides of a right triangle.

Problem

Find all nontrivial integer solutions of

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

having no common factor.

First Problem: The Case $n = 2$

Problem

Find all nontrivial integer solutions of

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

having no common factor.

We first note that if any two of x, y, or z are even, then the third must be even, contradicting the hypothesis that x, y, and z have no common factor.

So, at most one of x, y, and z can be even.

First Problem: The Case $n = 2$

Problem

Find all nontrivial integer solutions of

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

having no common factor.

Suppose x and y are both odd. Then x^2 and y^2 are both odd, so their sum, z^2 is even. If z^2 is even, then z must be even.

Problem

Problem

Find all nontrivial integer solutions of

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

having no common factor.

Looking at the equation

$$x^2 + y^2 \equiv z^2 \mod 4,$$

Since z is even, then $z^2 \equiv 0 \mod 4$.

Problem

Problem

Find all nontrivial integer solutions of

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

having no common factor.

On the other hand, since x and y are both odd, $x, y \equiv 1 \mod 2$, so $x^2, y^2 \equiv 1 \mod 4$, and $x^2 + y^2 \equiv 2 \mod 4$.

This contradicts the preceding slide where $x^2 + y^2 = z^2 \equiv 0 \mod 4$.

So, z must be odd and exactly one of x and y is even.

Looking at a Larger Ring: $\mathbb{Z}[i]$

Looking For Solutions in $\mathbb{Z}[i]$

Problem

Find all nontrivial integer solutions of

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

having no common factor.

Rather than looking at solutions in the integers, we look at solutions in a slightly larger ring, the Gaussian integers, denoted $\mathbb{Z}[i]$. This is the ring of all complex numbers of the form $\{a + bi \mid a, b \in \mathbb{Z}\}$.

Looking For Solutions in $\mathbb{Z}[i]$

An element p in a ring R is **prime** if whenever p divides a product ab of elements of R, then p divides a or p divides b.

An element u in a ring R is a **unit** if it has a multiplicative inverse.

A ring R is a **unique factorization domain** (a UFD) if every element of R that is not a unit can be written as a product of prime elements, uniquely up to order and multiplication by units.

The ring of Gaussian integers, $\mathbb{Z}[i]$, is a unique factorization domain. The units in this ring are ± 1 and $\pm i$.

Looking For Solutions in $\mathbb{Z}[i]$

Problem

Find all nontrivial integer solutions of

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

having no common factor.

In the ring of Gaussian integers, the left side of this equation factors:

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

Looking For Solutions in $\mathbb{Z}[i]$

Problem

Find all nontrivial integer solutions of

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

having no common factor.

Suppose π is a prime element in $\mathbb{Z}[i]$ which divides z. Then π^2 divides z^2, whereby π^2 divides

$$(x + iy)(x - iy).$$

Looking For Solutions in $\mathbb{Z}[i]$

Suppose π divides both $(x + iy)$ and $(x - iy)$. Then π divides their sum, $2x$. Hence π divides both z and $2x$.

However, z and $2x$ are relatively prime integers (since z is odd and z and x have no common factors), so there exist integers m, n so that

$$mz + 2nx = 1.$$

Since π divides both z and $2x$, this equation tells us that π divides 1, which says π is a unit. This is a contradiction.

So, $(x + iy)$ and $(x - iy)$ are relatively prime in $\mathbb{Z}[i]$.

Looking For Solutions in $\mathbb{Z}[i]$

In $\mathbb{Z}[i]$, we have

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

Any prime π which divides z must divide either $(x + iy)$ or $(x - iy)$, but not both.

Since π^2 divides z^2, π^2 divides either $(x + iy)$ or $(x - iy)$.

It follows that $x + iy$ is a square in $\mathbb{Z}[i]$.

Looking For Solutions in $\mathbb{Z}[i]$

Let's say

$$x + iy = (a + ib)^2, \quad a, b \in \mathbb{Z}.$$

Then

$$x + iy = (a^2 - b^2) + i(2ab)$$

and

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= (x + iy)(x - iy) \\ &= [(a^2 - b^2) + i(2ab)][(a^2 - b^2) - i(2ab)] \\ &= (a^2 - b^2)^2 + 4a^2b^2 \\ &= (a^2 + b^2)^2. \end{aligned}$$

Looking For Solutions in $\mathbb{Z}[i]$

From this, we can see that

$$\begin{aligned} x &= a^2 - b^2 \\ y &= 2ab \\ z &= a^2 + b^2, \end{aligned}$$

where a, b are integers.

Since x, y and z are pairwise relatively prime, we must have a and b are relatively prime and not both odd.

This representation will give us all primitive Pythagorean triples.

Second Problem: Generalization to $n = 3$

Second Problem

Generalizing slightly, we get a problem that is very easy to solve.

Problem

Find all nontrivial integer solutions of

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

having no common factor.

Second Problem

Problem

Find all nontrivial integer solutions of

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

having no common factor.

Once again, if 3 divides two of x, y, or z, then 3 divides all three, contradicting the hypothesis that these numbers have no common factor. So, we have two cases:

1. 3 divides none of x, y, or z
2. 3 divides exactly one of x, y, or z

Second Problem

Problem

Find all nontrivial integer solutions of

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

having no common factor.

We will only consider the first case: 3 divides none of x, y, or z.

Second Problem

Problem

Find all nontrivial integer solutions of

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

having no common factor.

In this case, the only cubes modulo 9 not divisible by 3 are ± 1.

But then $x^3 + y^3 \equiv -2, 0,$ or $2 \mod 9$.

But $z^3 \equiv \pm 1 \mod 9$. So, in the first case, $x^3 + y^3 = z^3$ has no nontrivial integer solutions.

An Observation

An Observation

If we look at the equation $x^n + y^n = z^n$ for n composite, we have the following observation. If p is a prime factor of n, say $n = pm$, then

$$\begin{aligned} x^n + y^n &= z^n \\ x^{pm} + y^{pm} &= z^{pm} \\ (x^m)^p + (y^m)^p &= (z^m)^p. \end{aligned}$$

From this we see if there is no solution for a prime exponent p, there is no solution for any exponent that is a multiple of p.

So we need only show that if $p > 3$ is an odd prime, then $x^p + y^p = z^p$ has no solution in the nonzero integers x, y, z.

A Third Problem: $x^p + y^p = z^p$

Third Problem

This observation leads us to another generalization:

Problem

For a prime number $p > 3$, show the equation

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

has no nonzero integral solution.

Again, we limit ourselves to the first case where p divides none of x, y, or z.

Looking at a Larger Ring: $\mathbb{Z}[\omega]$

Let $\omega = e^{2\pi i/p}$, a primitive p^{th} root of unity. Then the p^{th} roots of 1 are $1, \omega, \omega^2, \ldots, \omega^{p-1}$ and each of these is a root of the polynomial $t^p - 1$. Since there are p of these, these are all the roots of this polynomial.

So, in the ring $\mathbb{Z}[\omega]$, we have

$$t^p - 1 = (t-1)(t-\omega)(t-\omega^2)\cdots(t-\omega^{p-1}).$$

We Need Two Lemmas

In the equation

$$t^p - 1 = (t-1)(t-\omega)(t-\omega^2)\cdots(t-\omega^{p-1}),$$

we can divide both sides by $t-1$ to get

$$(t-\omega)(t-\omega^2)\cdots(t-\omega^{p-1}) = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

Setting $t = 1$, we get

Lemma

$$(1-\omega)(1-\omega^2)\cdots(1-\omega^{p-1}) = p.$$

We Need Two Lemmas

In the equation

$$t^p - 1 = (t-1)(t-\omega)(t-\omega^2)\cdots(t-\omega^{p-1}),$$

set $t = -x/y$. Remembering that p is odd and doing a bit of algebra, we get

Lemma

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

What we have done here is to factor $x^p + y^p$ into p linear factors in the ring $\mathbb{Z}[\omega]$.

Looking at a Larger Ring: $\mathbb{Z}[\omega]$

Problem

For a prime number $p > 3$, show the equation

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

has no nonzero integral solution.

In the ring $\mathbb{Z}[\omega]$, the left side of this equation factors:

$$(x + y)(x + y\omega)(x + y\omega^2) \cdots (x + y\omega^{p-1}) = z^p.$$

Looking at a Larger Ring: $\mathbb{Z}[\omega]$

Our problem then is to show the equation

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

has no nonzero integral solutions in $\mathbb{Z}[\omega]$.

Looking at a Larger Ring: $\mathbb{Z}[\omega]$

Assuming $\mathbb{Z}[\omega]$ is a unique factorization domain, let $\pi \in \mathbb{Z}[\omega]$ be a prime dividing z.

Then π^p divides z^p, whereby π^p divides

$$(x + y)(x + y\omega)(x + y\omega^2) \cdots (x + y\omega^{p-1}).$$

Looking For Solutions in $\mathbb{Z}[\omega]$

Suppose π divides more than one of the factors, say both $(x + y\omega^k)$ and $(x + y\omega^\ell)$, $0 \leq k < \ell \leq p - 1$.

Then π divides the linear combination

$$(x + y\omega^\ell) - \omega^{\ell-k}(x + y\omega^k) = (1 - \omega^{\ell-k})x.$$

Looking For Solutions in $\mathbb{Z}[\omega]$

Recalling our first lemma, we have that

$$(1-\omega)(1-\omega^2)\cdots(1-\omega^{p-1})x = px.$$

and knowing that π divides $(1-\omega^{\ell-k})x$, we have π divides px.

So, π divides both z and px.

Looking For Solutions in $\mathbb{Z}[\omega]$

Since z and px are relatively prime in $\mathbb{Z}$, there exist integers a, b so that $az + bpx = 1$. It follows that π divides 1, a contradiction.

So, all the factors in the product

$$(x + y)(x + y\omega)(x + y\omega^2) \cdots (x + y\omega^{p-1})$$

are relatively prime in $\mathbb{Z}[\omega]$.

Looking For Solutions in $\mathbb{Z}[\omega]$

It now follows that each factor of the product is a p^{th} power in $\mathbb{Z}[\omega]$, so

$$x + y\omega = u\alpha^p$$

for some $\alpha, u \in \mathbb{Z}[\omega]$, with u a unit.

Thus we have a multiplicative problem in the ring $\mathbb{Z}[\omega]$.

Looking For Solutions in $\mathbb{Z}[\omega]$

So, assuming that $\mathbb{Z}[\omega]$ is a UFD, it can be shown that $x + y\omega$ has the form $u\alpha^p$ for some $\alpha \in \mathbb{Z}[\omega]$ and some unit $u \in \mathbb{Z}[\omega]$.

It can then be shown that the equation $x + y\omega = u\alpha^p$, with x and y not divisible by p, implies that $x \equiv y \mod p$.

Similarly, writing $x^p + (-z)^p = (-y)^p$, we obtain $x \equiv -z \mod p$.

But then

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \mod p$$

implying that $p \mid 3x^p$. Since $p \nmid x$ and $p \neq 3$, this is a contradiction.

Big Oops!

How Embarrassing!

In a famous incident, the French mathematician Gabriel Lamé gave a talk at the Paris Academy in 1847 in which he claimed to prove Fermat's last theorem using the approach just presented.

How Embarrassing!

Joseph Liouville immediately questioned the step in Lamé's proof in which he assumed that, in order to show that each factor $x + y\omega^k$ is a p^{th} power, it suffices to show that the factors are relatively prime in pairs and their product is a p^{th} power.

In other words, Liouville questioned Lamé's assumption that $\mathbb{Z}[\omega]$ is a UFD.

Lamé couldn't justify his assumption and Fermat's Last Theorem remained unproved for almost 150 years.

Looking For Solutions in $\mathbb{Z}[\omega]$

Ernst Kummer attempted to prove Fermat's conjecture by considering whether the unique factorization property in $\mathbb{Z}$ and $\mathbb{Z}[i]$ generalizes to the ring $\mathbb{Z}[\omega]$.

Unfortunately it does not. For example if $p = 23$, then not all members of $\mathbb{Z}[\omega]$ factor uniquely into irreducible elements. In other words $\mathbb{Z}[\omega]$ is not a unique factorization domain (UFD) for $p = 23$.

It is, however, a UFD for all primes less than 23. For these primes it is not difficult to show that $x^p + y^p = z^p$ has no case 1 solutions.

Can We Fix This?

Can We Fix This?

Kummer and mathematician Richard Dedekind (1831–1916) discovered that unique factorization was lost simply because there were "not enough numbers" in $\mathbb{Z}[\omega]$.

They investigated the idea of adding "ideal points" to $\mathbb{Z}[\omega]$ so that we again have unique factorization.

Can We Fix This?

Kummer and Dedekind generalized the following facts about divisibility of integers:

1. An ideal point α should divide 0.
2. If α divides a and b, then α must divide $a \pm b$.
3. If α divides a, then α divides ra for any $r \in \mathbb{Z}[\omega]$.
4. An ideal point π is prime if, whenever π divides a product ab in $\mathbb{Z}[\omega]$, then π divides a or π divides b.

Can We Fix This?

If we convert Kummer and Dedekind's work into modern terms, let I be a subset of a ring R.

1. 0 should be an element in I.
2. If a and b are in I, then $a \pm b$ are in I.
3. If a is in I, then ra is in I for all $r \in R$.
4. An ideal point I is prime if, whenever ab is in I, either a is in I or b is in I.

We now recognize "ideal points" as ideals in a ring and "prime ideal points" as prime ideals in a ring.

And now you know where the terminology came from.

Can We Fix This?

Mathematician Richard Dedekind (1831–1916) discovered that although elements of $\mathbb{Z}[\omega]$ will not factor uniquely into irreducible elements, *ideals* in this ring always factor uniquely into a product of prime *ideals*. For primes p that are "regular"—yet another technical use of an overused word in mathematics—an ideal must be principal which forces $x + y\omega$ to be a p^{th} power of a prime ideal.

Looking For Solutions in $\mathbb{Z}[\omega]$

As we noted before, this leads to a contradiction, showing that $x^p + y^p = z^p$ has no case 1 solutions (i.e., solutions for which $p \nmid xyz$) when p is a regular prime.

Looking For Solutions in $\mathbb{Z}[\omega]$

It is also possible, although somewhat more difficult to show that no case 2 solution exist for regular primes. Thus Fermat's conjecture can be proved for all regular primes p, hence for all integers n which have at least one regular prime factor. Unfortunately, irregular primes exist. For example, 37, 59, 67,.... In fact there are infinitely many. On the other hand, it is not known if there are infinitely many regular primes.

A Definition

We define an equivalence relation on the set of ideals of $\mathbb{Z}[\omega]$ as follows: For ideals A and B in $\mathbb{Z}[\omega]$, $A \sim B$ if $\alpha A = \beta B$ for some $\alpha, \beta \in \mathbb{Z}[\omega]$.

It turns out there are only finitely many equivalence classes of ideals under $\sim$. The number of classes is the *class number* of the ring $\mathbb{Z}[\omega]$ is finite and denoted by the letter h. The class number is then a function of p. The equivalence classes of ideals, called *ideal classes,* form an abelian group under multiplication, the *ideal class group*.

A Definition

A prime p is **regular** if p does not divide the order h of its ideal class group.

In this case, the ideal class group contains no element of order p. It follows from Lagrange's Theorem, that if I^p is principal, i.e. the identity in the ideal class group, then I is also principal.

A Partial Solution

A Partial Solution

Shortly after Lamé's embarrassing lecture, Kummer used his result on the arithmetic of the fields $\mathbb{Q}(\omega)$, the fraction field of the integral domain $\mathbb{Z}[\omega]$ to prove Fermat's last theorem for all regular primes, i.e., for all primes p such that p does not divide the class number of $\mathbb{Q}(\omega)$, for ω is a primitive p^{th} root of 1.

A Complete Solution

A Complete Solution

Fermat's Last Theorem was proved by Andrew Wiles as a consequence of his proof of the Shimura-Taniyama-Weil conjecture. The results were first announced in a series of lectures at Cambridge in June 1993.

As often happens in the case of complicated proofs of extremely difficult problems, there were some gaps in the argument that had to be filled in, and this process was not completed until 1995.

A Complete Solution

Wiles was educated at Merton College, Oxford (B.A., 1974), and Clare College, Cambridge (Ph.D., 1980). Following a junior research fellowship at Cambridge (1977–80), Wiles held an appointment at Harvard University, Cambridge, Massachusetts, and in 1982 he moved to Princeton University, where he became professor emeritus in 2012. Wiles subsequently joined the faculty at Oxford.

A Complete Solution

In recognition of his proof of the Shimura-Taniyama-Weil conjecture, he was awarded a special silver plaque—he was beyond the traditional age limit of 40 years for receiving the gold Fields Medal—by the International Mathematical Union in 1998. He also received the Wolf Prize (1995–96), the Abel Prize (2016), and the Copley Medal (2017).

A Note of Thanks

Thank you for attending.