

What Makes Fermat's Last Theorem So Hard, Anyway?

Marcus Jaiclin

November 5, 2005

1 Introduction

Most of the material for this talk comes from 13 Lectures on Fermat's Last Theorem, by Paulo Ribenboim, and A Classical Introduction to Modern Number Theory by Kenneth Ireland and Michael Rosen.

Pierre de Fermat lived from 1601 to 1665, and is best known, mathematically, for three things: Fermat's Little Theorem, Fermat Primes and Fermat's Last Theorem. Fermat proved Fermat's Little Theorem during his life, and wrote a small note in one of his books stating his Last Theorem, and mentioned that he had "discovered a truly remarkable proof which this margin is too small to contain." (Ribenboim, pg 1). Then he died. Certainly, a note like that is likely to challenge mathematicians reading his work to try to find his "remarkable proof", and try they did. Noone could find it.

It is arguable whether the name 'Fermat's Last Theorem' should be applied to the result, since he never provided a proof, so I will refer to it as the Fermat Problem. So what is the Fermat Problem? It asks:

Is it possible to find three positive integers x, y, z so that:

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

for some integer power $n \geq 3$?

It was shown, in 1996, by Andrew Wiles (in Princeton, NJ) that the answer is no.

Clearly, there are many solutions if $n = 1$ or 2 . If $n = 1$, the problem is trivial, and for $n = 2$ it is the famous Pythagorean Theorem (another theorem named for someone who didn't prove it). Well-known solutions are $x = 3, y = 4, z = 5$ and $x = 5, y = 12, z = 13$. In fact, the ancient Greeks knew how to generate infinitely many solutions which were different from each other.

Fermat actually left a proof of that there are no solutions when $n = 4$ before he died, and then Euler published a proof in 1770 of the case $n = 3$. The first correct proof for $n = 5$ was published in 1825 by Legendre, 160 years after Fermat's death. The first major progress of solving the entire Fermat Problem for more than one exponent at a time was made by E.E. Kummer in 1847-50 (though progress on special cases was made by Sophie Germain in 1823 and after).

2 Factoring the Fermat Equation

If you want to solve a polynomial, the first thing to do is to try to factor it. Let's see what happens if we start with the case $n = 2$, which we know we can solve. Consider the following:

$$\begin{aligned}x^2 + y^2 &= 25 \\x^2 - (-y^2) &= 25\end{aligned}$$

This puts us in the position of a difference of two squares, which is easy to factor:

$$\begin{aligned}(x + \sqrt{-y^2})(x - \sqrt{-y^2}) &= 25 \\(x + yi)(x - yi) &= 25\end{aligned}$$

We know that $x = 3, y = 4$ is the solution to this, so let's plug that in:

$$(3 + 4i)(3 - 4i) = 25$$

Now, notice that the right side is perfect square, so, if the terms on the left side do not share any prime factors (which is something that we're not entirely sure what that means here), then each of the terms on the left side should also be perfect squares also. Let's check, in this special case:

$$\begin{aligned}(a + bi)^2 &= 3 + 4i \\ (a^2 - b^2) + (2ab)i &= 3 + 4i\end{aligned}$$

which splits into:

$$\begin{aligned}a^2 - b^2 &= 3 & 2ab &= 4 \\ & & a &= \frac{2}{b} \\ \left(\frac{2}{b}\right)^2 - b^2 &= 3 \\ \frac{4}{b^2} - b^2 &= 3 \\ 4 - b^4 &= 3b^2 \\ b^4 + 3b^2 - 4 &= 0\end{aligned}$$

which is a quadratic in b^2 , which factors as:

$$(b^2 + 4)(b^2 - 1) = 0$$

which leaves us with the solutions $b = \pm 1$ (we disregard the solutions $b = \pm 2i$ since b is an integer). This gives us $a = \pm 2$, and so we get $\pm(2 + i)$ as the square roots of $3 + 4i$. Following a very similar calculation, we get $\pm(2 - i)$ as the square roots of $3 - 4i$.

This shows us that the perfect square on the right may be an indicator of a perfect square on the left.

So, can we generalize this? Well, the first step is to look at how to factor the higher degree equations in the Fermat Problem.

To factor $x^3 + y^3$, we'll start with the same trick, of turning it into a difference of two cubes:

$$x^3 - (-y)^3$$

Here, since the power is odd, we can bring the negative inside the cube which is a little more convenient. We'll use a trick that most of you should know, related to the following factorization:

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

or, in general,

$$x^{n+1} - 1 = (x - 1)(x^n + x^{n-1} + \dots + x + 1)$$

This generalizes to:

$$x^{n+1} - y^{n+1} = (x - y)(x^n + x^{n-1}y + x^{n-2}y^2 + \dots + xy^{n-1} + y^n)$$

In our case, we have $-y$ instead of y and 3 instead of $n + 1$ so we get:

$$\begin{aligned}x^3 + y^3 &= (x - (-y))(x^2 + x(-y) + (-y)^2) \\ x^3 + y^3 &= (x + y)(x^2 - xy + y^2)\end{aligned}$$

We'll use the quadratic formula to factor the quadratic there (just think of the y 's as coefficients for now):

$$x = \frac{y \pm \sqrt{(-y)^2 - 4(1)(y^2)}}{2}$$

$$x = \frac{y \pm \sqrt{y^2 - 4y^2}}{2}$$

$$x = y \left(\frac{1 \pm \sqrt{-3}}{2} \right)$$

$$x = y \left(\frac{1}{2} \pm \frac{\sqrt{3}}{2}i \right)$$

Putting these into the factorization, we get:

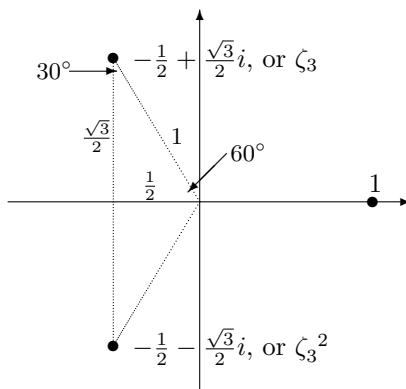
$$x^3 + y^3 = (x + y) \left(x - y \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i \right) \right) \left(x - y \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) \right)$$

$$x^3 + y^3 = (x + y) \left(x + y \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) \right) \left(x + y \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i \right) \right)$$

These complex numbers that show up here are important. If you factor $x^3 - 1$, they also show up:

$$x^3 - 1 = (x - 1) \left(x - \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) \right) \left(x - \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i \right) \right)$$

And so, these are two of the three solutions to the equation $x^3 = 1$. This property gives them their name: complex 3rd roots of unity. The first is usually denoted by the lower case Greek letter zeta, with a subscript which indicates the exponent: ζ_3 . The second is the square of the first (see below), so we denote that one by ζ_3^2 . If you plot them on a plane, you can think of the x -axis as the real part, and the y -axis as the imaginary part, and you get:



You may recognize the coordinates as being the sides of a triangle whose angles are 30-60-90, and so there is 120° between 1 and ζ_3 , and 120° between ζ_3 and ζ_3^2 . Using the 30-60-90 triangle, it is also easy to see that the distance from the origin to each of these points is exactly 1.

If we look at ζ_3 and ζ_3^2 , we see an illustration of how exponents work in complex numbers. When we square a complex number, we can multiply it out (e.g. $\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{1}{4} - \frac{\sqrt{3}}{4}i - \frac{\sqrt{3}}{4}i - \frac{3}{4} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$), or, if we work with the distance from the origin (which we'll call the radius), and the angle from the positive x -axis, we simply have to square the radius and double the angle. So, to find the square of ζ_3 , we get a radius of $1^2 = 1$, and an angle of $2\left(\frac{2\pi}{3}\right) = \frac{4\pi}{3}$. Looking at complex numbers using the radius and angle like this is called *polar coordinates*, which you may have seen at some point in calculus. For higher powers, we simply need to use that power on the radius, and multiply by that power in the angle; for example, we can see that ζ_3^3 has a radius of 1^3 and an angle of $3\left(\frac{2\pi}{3}\right) = 2\pi$, and so $\zeta_3^3 = 1$.

To take roots, we simply need to invert each of these things, so taking the cube root of 1 can be seen as taking the cube root of the distance from the origin ($\sqrt[3]{1} = 1$) and dividing the angle by 3 ($0 \div 3 = 0$). However, we can also think of 1 as having an angle of 2π instead. This gives us a radius of 1 and an angle of $\frac{2\pi}{3}$, which is ζ_3 , or we can think of 1 as having an angle of 4π , which means its cube root could have an angle of $\frac{4\pi}{3}$ which is ζ_3^2 . If we go to 6π , we get back to 1, and the values repeat from there, so there are only three distinct values. (Note: If the angle is not zero, this generally results in infinitely many distinct cube roots.)

So, if we want to consider solutions of $x^n = 1$ in the complex numbers, we will have n different solutions. All of them will be on the circle of radius 1, centered at the origin, and they will be evenly spaced around the circle, with the first one at 1, and each one will have an angle of $\frac{2\pi}{n}$ from the one before it. We will denote them: $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$.

This will allow us to factor the higher power Fermat equations:

$$x^n + y^n = (x + y)(x + \zeta_n y)(x + \zeta_n^2 y) \cdot \dots \cdot (x + \zeta_n^{n-1} y)$$

3 OK, So We've Factored it, What Next?

First, we should make one observation that will simplify things a little bit. If you had a solution (x, y, z) for the problem in exponent 15, for example, then you would have an equation that looked like:

$$x^{15} + y^{15} = z^{15}$$

which we can re-write as:

$$(x^5)^3 + (y^5)^3 = (z^5)^3$$

And so (x^5, y^5, z^5) would be a solution for the Fermat problem in exponent 3, and (x^3, y^3, z^3) would be a solution for the Fermat problem in exponent 5. In general, any solution for an exponent which is a composite number gives a solution for each exponent which is a prime factor of the original exponent. Taking the contrapositive, we can see that, if there are no solutions where the exponent is prime, then there are no solutions if the exponent is composite. Since we have solutions when the exponent is 2, we need to show that there are no solutions when $n = 4$, and for all prime exponents. Since Fermat took care of $n = 4$ for us, we're simply left with the odd prime exponents.

Recall what we saw in working with the solution to the Pythagorean Theorem – in order to consider integer solutions to $x^2 + y^2 = z^2$, we were forced to also consider numbers of the form $a + bi$, where a and b are integers, and $i = \sqrt{-1}$. When we look at the factorization of $x^3 + y^3$, we are faced with two choices, either work with numbers of the form $r + si$, where r and s could be integers, rational or irrational numbers, or we can work with numbers of the form $a + b\zeta_3 + c\zeta_3^2$, where a, b, c are integers. We want to avoid the can of worms that including irrational numbers opens up, so it is best to go with the latter.

In general, to look for solutions of the equation $x^p + y^p = z^p$ for an odd prime p , we will need to consider numbers of the form: $a_0 + a_1\zeta_p + a_2\zeta_p^2 + \dots + a_{p-1}\zeta_p^{p-1}$. This set is denoted $\mathbb{Z}[\zeta_p]$, and is called the p^{th} set of cyclotomic integers. The existence of a solution to the Fermat Problem involves understanding the structure of this set.

This set is a *commutative ring*, which just means that it is a set that has two operations (addition and multiplication), and that these operations satisfy basic properties that you'd want them to satisfy. Both operations are associative (meaning $(a + b) + c = a + (b + c)$, and the same for multiplication), both are commutative (i.e. that $a + b = b + a$), we have elements 1 and 0 which are identities for addition and multiplication, every element has a negative inside the set, and multiplication distributes over addition.

We would like to do what we did before: factor $x^p + y^p$, and then, again assuming that the factors share no prime factors, note that each of the factors must then be p^{th} powers:

$$z^p = x^p + y^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdot \dots \cdot (x + \zeta_p^{p-1} y)$$

It is likely (but, of course, we'll never know) that this is basically what Fermat had in mind. There is, however, a catch, which noone realized until 150 years after his death. For all of the odd primes $p \geq 23$, the collection $\mathbb{Z}[\zeta_p]$ does not have the property of Unique Factorization, meaning that there may be more than one way to factor a number into primes.

To see how this happens, we'll look at a simpler, but related, setting. Consider the collection of numbers $\mathbb{Z}[\sqrt{-5}]$; if we take:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 - (-5) = 6 = 3 \cdot 2$$

To see that $(1 + \sqrt{-5})$ is prime, check what it takes to multiply two elements to get this element:

$$\begin{aligned} (a + b\sqrt{-5})(c + d\sqrt{-5}) &= ac + ad\sqrt{-5} + bc\sqrt{-5} - 5bd \\ &= (ac - 5bd) + (ad + bc)\sqrt{-5} \end{aligned}$$

and, setting coefficients on the left equal to those on the right, we get:

$$\begin{aligned} bc + ad &= 1 & ac - 5bd &= 1 \\ a &= \frac{1 + 5bd}{c} \\ bc + \left(\frac{1 + 5bd}{c}\right)d &= 1 \\ bc^2 - c + (d + 5bd^2) &= 0 \\ c &= \frac{1 \pm \sqrt{1 - 4(b)(d + 5bd^2)}}{2b} \\ c &= \frac{1 \pm \sqrt{1 - 4(bd + 5b^2d^2)}}{2b} \end{aligned}$$

In order for c to be an integer, the term under the square root has to be positive, so:

$$\begin{aligned} 1 - 4(bd + 5b^2d^2) &> 0 \\ -20(bd)^2 - 4bd + 1 &> 0 \\ (bd)^2 + \frac{1}{5}(bd) - \frac{1}{20} &< 0 \\ \left(bd + \frac{1}{10}\right)^2 - \frac{3}{50} &< 0 \end{aligned}$$

Thinking of bd as a single variable, this gives us a parabola that crosses the x -axis at $\frac{-1-\sqrt{6}}{10}$ and at $\frac{-1+\sqrt{6}}{10}$, and is below the x -axis only between these values. Clearly, the only integer value between these values is 0, so this tells us that $bd = 0$, which means either b or d is 0. Back-substituting, this gives us:

$$c = \frac{1 \pm 1}{2b}$$

and so b is nonzero (or else c would be undefined), and d is zero. Since d is zero, c cannot be (or else $(c + d\sqrt{-5})$ would be zero), so we can discard the possibility of the minus in the numerator of c , and get that $c = \frac{1}{b}$. Since c and b are both integers, this makes $c = b = \pm 1$. So, $(c + d\sqrt{-5})$ must be ± 1 , meaning that $(a + b\sqrt{-5}) = \pm(1 + \sqrt{-5})$, and so $(1 + \sqrt{-5})$ is prime, since its only factors are itself and 1 (up to a \pm sign). A very similar argument applies to $1 - \sqrt{-5}$.

How does this affect the Fermat Problem? Take another look at the factorization of the Fermat equation:

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

What we now know is that, each of these must have a factorization where each is a p^{th} power, but we can't know for sure that *every* factorization is into p^{th} powers. In addition, the failure of Unique Factorization also causes a number of other useful divisibility tools to fail, such as one part of the Division Algorithm itself.

4 So Now What Do We Do?

E.E. Kummer is the first mathematician to understand that Unique Factorization is an issue in solving the Fermat problem. He also led the way in understanding what to do about it.

The basic idea in Kummer's approach was to consider the question of divisibility from the opposite direction: look at collections of multiples instead.

An *ideal*, in this context, is simply the collection of all multiples of one or more elements of the ring. For example, in the integers, the set $4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$ is an ideal. An ideal which consists of all of the multiples of a single element is called a *principal ideal*. Another example would be to consider, in the integers, the collection of all numbers which are multiples of both 2 and 3. This consists of: $\{\dots, -12, -6, 0, 6, 12, \dots\}$, which can also be seen as the multiples of 6. In the integers, every ideal is principal, but this fails in the cyclotomic integers, and this failure is intimately related to the failure of Unique Factorization.

Kummer considered, within the ring of cyclotomic integers, the collection of all ideals, thinking of the ideals as elements of a new set. He was able to find many relationships between the collection of ideals and the numbers in the ring. The first thing he did was to note that you can add and multiply ideals, simply by adding or multiplying the numbers in each ideal by the numbers in the other ideal. For example, in the integers, we can form:

$$4\mathbb{Z} + 6\mathbb{Z} = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\} = 2\mathbb{Z}$$

$$4\mathbb{Z} \cdot 6\mathbb{Z} = \{\dots, -48, -24, 0, 24, 48, \dots\} = 24\mathbb{Z}$$

Then, Kummer was able to show that there are no solutions for the Fermat Problem for an odd prime p as long as two properties held for that prime (such a prime is called a *regular prime*):

1. In $\mathbb{Z}[\zeta_p]$, the p^{th} power of any nonprincipal ideal is never principal.
2. Any element of $\mathbb{Z}[\zeta_p]$ which has a multiplicative inverse, and is different from a normal integer by a multiple of p must have a p^{th} root.

This is great, if there are any primes satisfy these two properties. The next step is to figure out which, if any, primes satisfy them. He worked for a long time on this problem, and was able to reduce the problem to a straightforward divisibility criterion:

An odd prime p is regular if and only if p does not divide the numerators of the Bernoulli Numbers $B_1, B_2, \dots, B_{\frac{p-3}{2}}$. Briefly, a Bernoulli Number is a fraction which can be determined in a couple of ways. The easiest way to describe them is as the coefficients in the power series:

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \frac{B_1}{2!}x^2 + \frac{B_2}{4!}x^4 + \dots$$

They are all fractions, and they alternate sign; the even ones are all positive and the odd are negative. An alternative description is to describe them recursively by:

$$b_0 = 1; \binom{k+1}{1}b_k + \binom{k+1}{2}b_{k-1} + \dots + \binom{k+1}{k}b_1 + b_0 = 0, \text{ for } k \geq 1$$

and then $B_k = b_{2k}$. Soon after Kummer discovered their importance in solving the Fermat Problem, two mathematicians independently discovered a complete description of the primes which divide the denominators of the Bernoulli Numbers. Determining which primes divide the numerators turns out to be much, much harder, and is poorly understood to this day. It is known that the numerators grow very quickly, and the denominators much more slowly (the Bernoulli numbers grow a bit faster than $(k^2)^k$).

Much of the progress on the Fermat Problem for another century and a half were small steps which built on Kummer's regularity condition – statements of the form “If we knew this equation involving the numerator of a Bernoulli Number and an odd prime p holds, then we would be able to say that Fermat's Equation has no solutions for that prime p .” No one has yet determined whether there are infinitely many or finitely many regular primes; according to computational tests, about 60% of tested primes are regular, and this ratio has continued to hold as the technology has improved, and so the numbers we can test have grown substantially. In fact, prior to Wiles' proof, no one had been able to show that there were no solutions for any infinite collection of primes. It has been proven that there are infinitely many irregular primes (almost a century after Kummer's work on the problem).