Fermat's Last Theorem for Regular Primes

S. M.-C.

22 September 2015

Abstract

Fermat famously claimed in the margin of a book that a certain family of Diophantine equations have no solutions in integers. For over 300 years Fermat's claim remained unsolved, and it provided motivation for many important developments in algebraic number theory. We will develop some of the foundational ideas of modern algebraic number theory in the context of Fermat's Last Theorem, and sketch a proof in the special case that the exponent is a so-called regular prime. No background will be assumed.

1 Introduction

In 1637, French mathematician Pierre de Fermat scribbled a claim in the margin of his copy of Diophantus' *Arithmetica*: the equation $x^n + y^n = z^n$ has no (non-trivial) solutions in integers for $n > 2$. He continued, "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

Fermat often claimed theorems without writing down a proof, and over time all his assertions were proven; except for the one above, which therefore became known as Fermat's Last Theorem. It was finally proven in 1994 using very advanced number theory techniques. In the 350 years it remained an open problem, it inspired many great advances in number theory.

There is one particular idea that we'll discuss that is central to modern algebraic number theory, namely ideals in number fields. We'll start with an easy case of Fermat's Last Theorem, then try and fail to apply the same ideas to prove the Theorem in general. Next we develop some algebraic number theory to fix what was broken, and finally we'll see some special cases in which the proof does generalize.

2 Pythagorean Triples and $n = 4$

First we discuss two easier cases. These will be more computational, first because the computations are rather easy and second to give a concrete idea of the methods involved, so that we can skip hard computations later and still understand what the ideas are.

The case $n = 2$ is not covered by Fermat's Last Theorem; indeed, there are many solutions to the equation $x^2 + y^2 = z^2$, known as Pythagorean triples because they give the sides of a right triangle satisfying the Pythagorean Theorem. In this case, instead of proving solutions don't exist, the question is: how can we find all solutions?

The strategy for solving this problem is to look at factorization in the integers. We first factor the equation, and then we continue looking at the factorizations of the integers we obtain, and this allows us to extract a general form that all Pythagorean triples take.

The general (mostly obvious) facts about factorization of integers we will need are these: if d divides a and b then d divides $a + b$; if d divides a then it divides ab for any b; and, of course, every integer has a unique factorization into primes.

First note that if any two of x, y, z are divisible by d then the third is also (because e.g. if d divides x and y then d^2 divides $x^2 + y^2 = z^2$ and d divides z). Thus we can divide out any common factors to assume that no two of x, y, z have a common factor. Then a slightly more complicated congruence argument shows that (after possibly exchanging x and y) both y and z are odd, while x is even.

The essential idea to find all Pythagorean triples is to change the original equation $x^2 + y^2 = z^2$ into $x^2 = z^2 - y^2$ and then factor as $x^2 = (z + y)(z - y)$. Since x, $z + y$, and $z - y$ are all even we can choose u, v, w such that $x = 2u$, $z + y = 2v$, and $z - y = 2w$. Then we have $u^2 = vw$. Note also that v, w have no common factors, for any common factor would also be a common factor of $v + w = z$ and $v - w = y$, and we have assumed that y and z have no common factors.

Since v, w are coprime the equation $u^2 = vw$ implies that both v and w are squares themselves, i.e. $v = r^2$ and $w = s^2$ for some integers r, s. This is because e.g. every prime p dividing v must divide u^2, so p^2 divides u^2, and thus (since v, w are coprime) p^2 divides v. We find that our triple x, y, z has the form $z = r^2 + s^2$, $y = r^2 - s^2$, and a bit of computation shows $x = 2rs$. In fact every choice of r, s (subject to some unimportant constraints) produces a Pythagorean triple in this way, and so we have found a method of producing all Pythagorean triples.

This is an interesting result by itself, but we can also use it to prove the case $n = 4$ of Fermat's Last Theorem. In fact, something stronger can be proved: there are no non-trivial solutions to $x^4 + y^4 = z^2$. Again the general idea of the proof is to look at factorization in the integers.

Suppose there is a solution in integers x, y, z. Then x^2, y^2, z form a Pythagorean triple, $(x^2)^2 + (y^2)^2 = z^2$, and by our previous work there are integers r, s such that $x^2 = 2rs$, $y^2 = r^2 - s^2$, and $z = r^2 + s^2$. Now $y^2 + s^2 = r^2$ is another Pythagorean triple, and so there are further integers a, b such that $s = 2ab$, $y = a^2 - b^2$, and $r = a^2 + b^2$.

Now $x^2 = 2rs = 4ab(a^2 + b^2)$. Note ab and $a^2 + b^2$ have no common factors: a, b are coprime, so a factor of ab is a factor of a or b but not both, and therefore not a factor of $a^2 + b^2$. The equation above shows $ab(a^2 + b^2)$ is a square, and so by the usual factorization argument both ab and $a^2 + b^2$ are squares, say $a^2 + b^2 = Z^2$. The same argument again shows that a and b are both squares, say $a = X^2$ and $b = Y^2$. We then have $X^4 + Y^4 = Z^2$.

To conclude the proof we observe that $|Z| \leq |Z|^2 = |r| < |z|$; that is, we've started with a solution $x^4 + y^4 = z^2$, and we've constructed a solution $X^4 + Y^4 = Z^2$ with Z strictly smaller than z (in absolute value). By repeating this process we could get another still smaller solution, and so on forever; but no chain of decreasing positive integers can go on forever, so we reach a contradiction. Put another way, we could require that $x^4 + y^4 = z^2$ was the solution with the smallest possible z, and our construction produces a solution with a smaller z, which is a contradiction. Thus we conclude that there is no solution to $x^4 + y^4 = z^2$, and this establishes Fermat's Last Theorem for $n = 4$.

This method is known as *infinite descent*: given a solution in integers, show that in fact there is a smaller solution, and then by repeating we would obtain an infinite descending chain of smaller and smaller solutions. But there is no infinite descending chain of positive integers, so we are at a contradiction, and the only possible conclusion is that we were mistaken at first in assuming the existence of a solution.

3 Rings and Fields

Fermat himself gave this proof for the case $n = 4$. After this, to prove the general case it's enough to prove there are no solutions when $n = p$ is an odd prime. To see this, suppose $a^n + b^n = c^n$ is any solution for any $n > 2$. Then n may be a power of 2 (and greater than 2, so divisible by 4), in which case $a^{n/4}, b^{n/4}, c^{n/4}$ is a solution to $x^4 + y^4 = z^4$; or else n is divisible by an odd prime p, in which case $a^{n/p}, b^{n/p}, c^{n/p}$ is a solution to $x^p + y^p = z^p$. Thus if there are no solutions for $n = 4$ or $n = p$ an odd prime, then there are no solutions for any exponent. We can now restrict our attention to the equation $x^p + y^p = z^p$, for p an odd prime.

In 1847, nearly 200 years after Fermat's original claim, another French mathematician Lamé announced a proof of Fermat's Last Theorem (for odd prime exponents). It was quickly discovered to be incorrect, but the basic idea (which may or may not be due to Lamé) points in a fruitful direction. In order to describe Lamé's idea, we have to introduce some new objects.

If you know what rings and fields are, great. If you don't know, I encourage you to think of them like this. A ring is a set of numbers that can be added, subtracted, and multiplied (while staying within the set); a field is a set of numbers that can be added, subtracted, multiplied, and divided (while staying within the set). (To be more precise, in this talk we can take "number" to mean "complex number", but rings and fields are of course more general). The example you should keep in mind at all times, especially for this talk, is that the integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ form a ring and the rational numbers $\mathbb{Q} = \{\ldots, -1, 0, 1, 2, \frac{1}{2}, 3, \frac{2}{3}, \ldots\}$ form a field.

Since division is not always possible in a ring, it is interesting to ask when one number *does* divide another. This is the question of factorization. We say that b divides a, or write $b \mid a$, if there is another number c in our ring so that $a = bc$, i.e. the product of b and c is a. For the integers $\mathbb{Z}$ this is the familiar definition; e.g. 3 divides 6 because $6 = 3 \cdot 2$, but 5 does not divide 6 because there's no integer c so that $6 = 5 \cdot c$. (Notice that divisibility is not an interesting notion in fields, because everything divides everything else, e.g. in the rational numbers 5 does divide 6 because $6 = 5 \cdot \frac{6}{5}$). In sufficiently nice rings, including all the rings we'll encounter, every element can be factored as a product of primes (in case you're familiar, in this talk I'll intentionally use the word "prime" to mean either "prime" or "irreducible"). Just as you'd expect, you can just keep factoring a number into smaller and smaller pieces until it doesn't factor anymore, and you've written it as a product of primes.

In addition to the rational numbers, we're interested in *algebraic number fields* (or just number fields for short), which we get by adding to the rational numbers a number which is the root of some polynomial. For example, you may be familiar with the imaginary unit i, defined by $i^2 = -1$ (which is a root of the polynomial $x^2 + 1 = 0$). We can adjoin i to the rational numbers to get the field $\mathbb{Q}(i)$, whose elements are numbers of the form $a + bi$ with a, b rational. For those of you who are familiar, we get this by $\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2 + 1)$. As a more general example, let ζ_n be a root of $x^n - 1 = 0$ (which we require to be primitive, meaning it is not a root of $x^m - 1 = 0$ for $m < n$). We call ζ_n a (primitive) n^{th} *root of unity*. For p prime, the number field $\mathbb{Q}(\zeta_p)$ consists of numbers $a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2}$ with a_i rational. (Note that we don't need to include a ζ_p^{p-1} term, because as you can check $\zeta_p^{p-1} = -1 - \zeta_p - \zeta_p^2 - \cdots - \zeta_p^{p-2}$, so ζ_p^{p-1} can be expressed in terms of lower powers).

Just as the rational numbers contain a distinguished ring, namely the integers, we want to distinguish a subring of a number field with similar properties. Number fields are supposed to be "like the rational numbers", so they should each have a "ring of integers". It turns out that the correct fact to generalize is the following: if a monic polynomial with integer coefficients has a roots in the rational numbers, then in fact that root is an integer. (Recall monic means the leading coefficient is 1). That is, the integers are distinguished among rational numbers as being those rational numbers that are roots of monic polynomials with integer coefficients.

This is easy to see: suppose

$$\left(\tfrac{a}{b}\right)^n + c_{n-1}\left(\tfrac{a}{b}\right)^{n-1} + \cdots + c_1\left(\tfrac{a}{b}\right) + c_0 = 0,$$

with $a, b, c_0, \ldots, c_{n-1}$ all integers and $\frac{a}{b}$ in lowest form. Then multiplying by b^n gives

$$a^n + c_{n-1}ba^{n-1} + \cdots + c_1b^{n-1}a + c_0b^n = 0,$$

or equivalently

$$a^n = b(-c_{n-1}a^{n-1} - c_{n-2}ba^{n-2} - \cdots - c_1b^{n-2}a - c_0b^{n-1}).$$

This shows that b divides a^n; but we also assumed that $\frac{a}{b}$ was in lowest form, and this is only possible if $b = \pm 1$. Thus $\frac{a}{b}$ was an integer all along.

Inspired by this, define an *algebraic integer* to be a root of a monic polynoimal with integer coefficients. For example, $x^2 + 1$ is a monic polynomial with integer coefficients, so its roots i and $-i$ are algebraic integers. Similarly, $x^n - 1$ for any n is such a polynomial, so our roots of unity ζ_n are algebraic integers.

We define our distinguished ring in a number field as follows. Every number field has a *ring of (algebraic) integers* consisting of all elements of the number field which are roots of a monic polynomial with integer coefficients; that is, the set of algebraic integers in a number field forms a ring. For example, the ring of integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$, meaning all numbers of the form $a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2}$ with a_i integers.

4 Lamé's Attempt

The idea is this: we're interested in finding integer (or rational) solutions to $x^n + y^n = z^n$, but we don't have to restrict ourselves to integers the whole time. If we want to rearrange some furniture in a small room, then even if we like the size of the room, it would be helpful to expand the room while we rearrange furniture and then contract it back to the original size at the end. Similarly, when we're interested in finding rational solutions to some equation, it's often a helpful intermediate step to consider our equation in a bigger field. Instead of looking at factorization in integers, as we did for the $n = 2$ and $n = 4$ cases, we'll look at factorization in the ring of integers of a number field.

So, suppose we have a solution x, y, z in integers to the equation $x^p + y^p = z^p$. Then in the ring $\mathbb{Z}[\zeta_p]$ of algebraic integers in $\mathbb{Q}(\zeta_p)$, we have the equation

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

Lamé's idea was to first show that the terms $(x+y)$, $(x+\zeta_p y)$, have no common factors, then conclude from the above equation that each term $(x+y)$, $(x+\zeta_p y)$, etc. is itself a p^{th} power, and try to produce a contradiction by infinite descent in the same spirit as the case $n = 4$.

This argument fails for a subtle reason. The elements of the ring $\mathbb{Z}[\zeta_p]$ can indeed be factored into prime elements of the ring, but such a factorization *may not be unique*! To give an example in a simpler number field, consider the ring of integers $\mathbb{Z}[\sqrt{-5}]$ of the number field $\mathbb{Q}(\sqrt{-5})$, whose elements have the form $a + b\sqrt{-5}$. Then it's not terribly hard to check that 2, 3, $1+\sqrt{5}$, and $1-\sqrt{5}$ are all prime elements of $\mathbb{Z}[\sqrt{-5}]$, so 6 has two distinct factorizations:

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

Because of the failure of unique factorization, we can't in general make the essential step in the above proof, from the equation $(x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1}y) = z^p$ to the claim that $(x+y)$, $(x+\zeta_p y)$ etc. are all p^{th} powers. It may be that the factorization on the left hand side is different from the factorization on the right hand side, and perhaps not every prime factor on the left hand side occurs to a p^{th} power.

5 Ideal Numbers

This is an unfortunate situation to be in, but we can dream of a better one. Perhaps there is some notion of "ideal numbers" in a ring of integers, for which unique factorization is restored. What could such a thing be?

For a start, there are some basic properties we want divisibility to have for our ideal numbers. If an ideal number divides an element a of our ring of integers, then it should divide ab for every b in our ring. Furthermore, if it divides a and b, then it should divide $a + b$.

The key insight is that to describe an "ideal number", the collection of numbers that it divides is actually enough. Define an *ideal* $\mathfrak{a}$ in a ring to be a subset of the ring such that if a is in $\mathfrak{a}$ then ab is in $\mathfrak{a}$ for every b in the ring, and if a, b are in $\mathfrak{a}$ then $a + b$ is in $\mathfrak{a}$. We think of the elements of $\mathfrak{a}$ as the elements of the ring that $\mathfrak{a}$ divides. With this in mind we have a natural definition of primes: define an ideal $\mathfrak{p}$ to be *prime* if whenever ab is in $\mathfrak{p}$, either a or b is in $\mathfrak{p}$. We can multiply ideals by letting $\mathfrak{ab}$ be the smallest ideal containing ab for all a in $\mathfrak{a}$ and b in $\mathfrak{b}$.

Consider the set of ideals in a ring of integers. Every element a of the ring produces an ideal (a) of all elements divisible by a. Such ideals are called *principal*. Furthermore, the product of two principal ideals $(a)(b)$ is the ideal of elements dividing the product, namely (ab). However, there may also be ideals that are not principal, in which case we really have expanded our notion of divisibility. (In general we denote by $(a_1, \ldots, a_n)$ the smallest ideal containing $a_1, \ldots, a_n$).

Remarkably, by introducing ideals, unique factorization is restored: every ideal in a ring of integers can be written uniquely as a product of prime ideals. For example, in the equation

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

the factors are no longer themselves prime, and we now have the further factorizations

$$\begin{aligned}
(2) &= (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2, \\
(3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = \mathfrak{p}_3\mathfrak{p}_4, \\
(1 + \sqrt{5}) &= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, \\
(1 - \sqrt{5}) &= (2, 1 - \sqrt{-5})(3, 1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4.
\end{aligned}$$

Thus our factorization

$$(6) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

is now unique.

We now think of a ring of integers in terms of its ideals. In the same way, we can think of the corresponding number field in terms of fractional ideals. A *fractional ideal* is a subset of a number field such that if a an element of the number field is in $\mathfrak{a}$ then ab is in $\mathfrak{a}$ for all b in the ring of integers (note not the number field), and if a, b are in $\mathfrak{a}$ then $a + b$ is in $\mathfrak{a}$.

We can define products of fractional ideals in precisely the same way as products of ideals. With respect to this product, the fractional ideals of a number field form an abelian group, and the principal fractional ideals form a subgroup. Define the *ideal class group* of a number field to be the group of fractional ideals modulo the subgroup of principal fractional ideals, and define the *class number* of a number field to be the order of its ideal class group.

The class number of a number field is a measure of the extent to which unique factorization fails. Unique factorization may not hold in the original ring of integers, but after expanding to ideals it does. Since elements of the ring of integers produce principal ideals, the class number essentially measures the number of new ideals we had to add to restore unique factorization.

6 Regular Primes

Thus if the class number of $\mathbb{Q}(\zeta_p)$ is 1, this means that every ideal is principal, and unique factorization of ideals implies that the ring of integers $\mathbb{Z}[\zeta_p]$ has unique factorization as well. In this case the proof of Lamé succeeds in establishing Fermat's Last Theorem. However, this is not a very far-reaching special case. The only odd primes for which $\mathbb{Q}(\zeta_p)$ has class number 1 are $3, 5, 7, 11, 13, 17, 19$.

But there is a weaker condition for which the argument can be salvaged. A prime p is called *regular* if p does not divide the class number of $\mathbb{Q}(\zeta_p)$. It turns out that regularity is a strong enough condition to salvage the proof of Fermat's Last Theorem.

Theorem 6.1. *Let p be a regular prime, i.e. an odd prime for which p does not divide the class number of $\mathbb{Q}(\zeta_p)$. Then the equation $x^p + y^p = z^p$ has no non-trivial solution in integers.*

Sketch of proof. It's helpful to handle the proof in two cases, depending on whether or not one of x, y, z is divisible by p.

Case 1: Suppose $x^p + y^p = z^p$ with x, y, z pairwise coprime and not divisible by p. Then we can write

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

First, we show that all the factors on the right hand side are relatively prime. Then, since the left hand side is a p^{th} power, we can conclude that each factor on the right hand side is the p^{th} power of some *ideal*, by unique factorization of ideals.

So for example we have $(x + \zeta_p y) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ in $\mathbb{Z}[\zeta_p]$. That is, $\mathfrak{a}^p$ is a principal ideal, so it is the identity in the ideal class group of $\mathbb{Q}(\zeta_p)$. But if $\mathfrak{a}^p$ is the identity in the class group and the order of the class group (i.e. the class number) is not divisible by p, we can use basic facts from group theory to conclude that $\mathfrak{a}$ itself must be trivial in the class group. Thus $\mathfrak{a}$ is principal, say $\mathfrak{a} = (a)$, and $x + \zeta_p y = a^p$ is the p^{th} power of an actual element of $\mathbb{Z}[\zeta_p]$ after all.

Observe how we get the same result, that the factors are all p^{th} powers, just from the assumption that p is regular instead of the much stronger assumption that $\mathbb{Z}[\zeta_p]$ has unique factorization. The rest of the proof of Case 1 uses this fact and examines factorization in $\mathbb{Z}[\zeta_p]$ to derive a contradiction, and we conclude that there is no solution $x^p + y^p = z^p$ with x, y, z pairwise coprime and not divisible by p.

Case 2: This case is more difficult, because if p divides one of x, y, z then it may no longer be true in our factorization

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

that all factors on the right hand side are relatively prime. However, the proof makes the same use of regularity, concluding that an ideal is principal because its p^{th} power is principal, and then uses factorization in $\mathbb{Z}[\zeta_p]$ to construct an infinite descent. □

How significant of a special case is this? It's not clear. There seem to be many regular primes: among the 24 odd primes less than 100, only three are irregular: 37, 59, and 67. And it is conjectured that approximately 60% of all primes are regular. However, this has not been proven; and indeed, it is not even known whether or not there are infinitely many regular primes. On the other hand, it is known that there are infinitely many irregular primes. But all in all, in practice one finds that many primes are regular, so this seems to be a significant accomplishment.

References

[1] Keith Conrad. *Fermat's Last Theorem for Regular Primes*. Available at http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/fltreg.pdf.

[2] Harold M. Edwards. *Fermat's last theorem*, volume 50 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. A gentle introduction to algebraic number theory, Corrected reprint of the 1977 original.