THE FERMAT EQUATION

PETE L. CLARK

1. Fermat's Last Theorem for $n = 4$

The proof of Fermat's Last theorem for $n = 4$ is the only argument of Fermat's that has survived intact. We give it here with a minimum of fuss. The first (and perhaps most important) insight is to dare to prove a slightly stronger result:

Theorem 1. *(Fermat) The equation $X^4 + Y^4 = Z^2$ has no integer solutions (X, Y, Z) with $XYZ \neq 0$.*

Remark: Since $Z^4 = (Z^2)^2$, still less does $X^4 + Y^4 = Z^4$ have any "nontrivial" $\mathbb{Z}$-solutions (i.e., any solutions with $XYZ \neq 0$).

Proof: If not, there exists a solution (x, y, z) with $\gcd(x, y) = 1$ and $z > 0$. (Indeed, if (x, y, z) is a solution and $p|x$ and $p|y$, then $p^4 \mid x^4 + y^4 = z^2$, so $p^2 \mid z$, and then $(x/p, y/p, z/p^2)$ is also a solution. Proceeding in this manner we can find a solution with x and y relatively prime.)

Step 1: x and y have opposite parity (i.e., one is even and one is odd). Indeed, x and y are relatively prime so are not both even. If both were odd then working modulo 4 we would have $x^4 + y^4 \equiv 1 + 1 \equiv 2 \equiv z^2$, but the squares modulo 4 are 0 and 1. Interchanging x and y if necessary, we may therefore assume that:

y is even, **x is odd**; and this implies **z is odd**.

Step 2: Now the key: $(x^2)^2 + (y^2)^2 = z^2$, so (x^2, y^2, z) is a primitive Pythagorean triple. By our study of such things we know that we can write

$$y^2 = 2mn \tag{1}$$

$$x^2 = m^2 - n^2 \tag{2}$$

$$z = m^2 + n^2 \tag{3}$$

Rewrite (2) as $n^2 + x^2 = m^2$. Since $(m, n) = 1$, this is again a primitive Pythagorean triple, and since x is odd, n must be even. Therefore we can again (!!) write

$$n = 2rs$$

$$x = r^2 - s^2$$

$$m = r^2 + s^2$$

with $\gcd(r, s) = 1$. Now

$$m(\frac{n}{2}) = \frac{2mn}{4} = \frac{y^2}{4} = (\frac{y}{2})^2.$$

And since m and $\frac{n}{2}$ are relatively prime, they both must be squares. Similarly, $rs = \frac{2rs}{2} = \frac{n}{2}$ is a square, so r and s must both be squares. So we may put $r = u^2,\ s = v^2,\ m = w^2$ and substitute into $m = r^2 + s^2$ to get

$$w^2 = u^4 + v^4.$$

Since $0 < w$ is an integer and

$$w^4 < w^4 + n^2 = m^2 + n^2 = z,$$

we have $0 < w < z$, and hence (u, v, w) gives a solution with strictly smaller positive final coordinate. Repeating this process, we will get infinitely many solutions, each with a final coordinate a smaller positive integer than the last, and this is clearly a contradiction!

Remark: We did manage to simplify matters by using our parameterization of primitive Pythagorean triples. For comparison, here is a proof that does not use this fact:[1]

Alternate proof: The beginning and Step 1 are as before. Now rewrite and factor:

$$y^4 = z^2 - x^4 = (z + x^2)(z - x^2).$$

Step 2: We claim that $\gcd(z + x^2, z - x^2) = 2$.
Indeed, if an odd prime p divided both $z + x^2$ and $z - x^2$, it would divide their sum, $2z$, hence also divide z, and it would divide their difference, $2x^2$, hence also divide x, but this implies that $p \mid y$, contradicting $\gcd(x, y) = 1$. Certainly both $z + x^2$ and $z - x^2$ are both even, but we cannot have both of them divisible by 4: if $z + x^2 \equiv 0 \pmod 4$, then $z \equiv -1 \pmod 4$, so $z - x^2 \equiv 2 \pmod 4$.

Since $(z + x^2)(z - x^2) = y^4$ is a fourth power, each of $(z + x^2)$ and $(z - x^2)$ must be fourth powers up to powers of 2. More precisely we have either:

Case i: $z - x^2 = 2a^4$, $a > 0$ and odd; and
$z + x^2 = 8b^4$, with $\gcd(a, b) = 1$; or

Case ii: $z - x^2 = 8b^4$,
$z + x^2 = 2a^4$, $a > 0$ and odd, $\gcd(a, b) = 1$.

Step 3: Case (i) is impossible:

$$x^+z - (-x^2 + z) = 2x^2 = -2a^4 + 8b^4 = -2a^4 + 8b^4,$$

so that

$$x^2 = -a^5 + 4b^4 \equiv -1 \pmod 4,$$

a contradiction.

Step 4: So we must be in Case (ii), and then:

$$(z - x^2) + (z + x^2) = 2z = 2a^4 + 8b^4 \implies z = a^4 + 4b^4.$$

Thus we have

$$0 < a < z.$$

[1]We are following Ireland and Rosen's *A Classical Introduction to Modern Number Theory.*

Step 5: Similarly to the above, we have

$$z + x^2 - (z - x^2) = 2x^2 = 2a^4 - 8b^4 \implies x^2 = a^4 - 4b^4,$$

or

$$4b^4 = (a^2 + x)(a^2 - x).$$

Since a and b are relatively prime, this gives a and x are relatively prime. Arguing as in Step 2, we get $\gcd(a^2 + x, a^2 - x) = 2$.

Step 6: We may write

$$a^2 - x = 2c^4$$
$$a^2 + x = 2d^4.$$

Indeed, $\mathrm{ord}_2(4b^4) = 2 + 4\,\mathrm{ord}_2(b) \equiv 2 \pmod 4$, so $\mathrm{ord}_2(a^2 + x) + \mathrm{ord}_2(a^2 - x) \equiv 2 \pmod 4$. If these two mod 4 ord's were 0 and 2 or 3 and 3, than both would be divisible by 4; so the ord's have to both be 1 mod 4, which establishes the claim.

So

$$2a^2 = (a^2 - x) + (a^2 + x) = 2c^4 + 2d^2 \implies a^2 = c^4 + d^4.$$

But since $0 < a < z$, we have found another solution to the equation, namely (c, d, a), with a positive and smaller than z. This leads to an infinite descent, a contradiction!

2. Other cases of Fermat's Last Theorem

I mentioned in class the desire to prove FLT(3), a theorem of Euler. In fact the proof is rather difficult. One part of it fits in well with what we have done: namely, just as we went to the quadratic field $\mathbb{Q}[\sqrt{-1}]$ to factor $a^2 + b^2$, in order to factor $a^3 + b^3$ we will go to the (still quadratic) field $\mathbb{Q}[\zeta_6]$, where $\zeta_6 = e^{\frac{2\pi i}{6}}$ is a primitive 6th root of unity. It turns out that we are lucky that the ring of all algebraic integers in $\mathbb{Q}[\zeta_6]$ – which itself turns out to be $\mathbb{Z}[\zeta_6] = \{a + b\zeta_6 \mid a, b \in \mathbb{Z}\}$ – is a Principal Ideal Domain. The proof is similar to that for the Gaussian integers – we show that any element of the quotient field $\mathbb{Q}[\zeta_6]$ differs from an element of $\mathbb{Z}[\zeta_6]$ by a complex number of norm less than 1. But completing the proof given this knowledge is not at all straightforward – it would probably take two classes on its own, and it seems to me now that we have better uses of our time. Note also that, as I mentioned in class, solving FLT(3) amounts to finding all the rational points on an elliptic curve. This is probably the single most active area of 21st century number theory – both theoretically and computationally – and we have far better methods for this than the *ad hoc* argument that is used to prove FLT(3). Indeed, it is no exaggeration to say that we have software available today that would literally take the equation $x^3 + y^3 = 1$ as input, and would output the result that the only rational points are $(1, 0)$ and $(0, 1)$ – i.e., computers can now prove FLT(3).

On the other hand, one can consider a similar construction for other odd primes p: namely, one can look at the ring $\mathbb{Z}[\zeta_{2p}]$, where ζ_{2p} is a primitive $(2p)$th root of unity. It turns out that whenever this ring is a PID, one can deduce FLT(p). The proof, however, is quite difficult and is not often given even in a first graduate-level course on algebraic number theory.

The bad news is that, just as for imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$, having

unique factorization in $\mathbb{Z}[\zeta_{2p}]$ is, alas, quite rare: it fails for all $p \geq 23$. In fact one can get by with slightly less than the unique factorization in order to push through a proof of FLT(p). Indeed, to any number field K – i.e., a finite degree field extension of $\mathbb{Q}$ – one can associate a number $h(K)$, the **class number**, in such a way that $h(K) = 1$ iff the ring of algebraic integers of K is a PID. The condition that is necessary in order to make the factorization of $a^p + b^p$ over $\mathbb{Z}[\zeta_{2p}]$ useful is that the class number $h(\mathbb{Q}(\zeta_{2p}))$ be indivisible by p. Such a prime is said to be **regular**. In fact there is quite an elementary criterion for regularity: namely that p does not divide the numerator of any of the **Bernoulli numbers** $B_2, \ldots, B_{p-3}$.[2]

Theorem 2. *(Kummer, 1847) FLT(p) holds for p a regular prime.*

A widely believed heuristic says that the chance of a large prime being regular is $e^{\frac{-1}{2}}$, or about 61%. Thus it will probably turn out in the end that Kummer proved "a bit more than half" of FLT. Between this result and Faltings' finiteness theorem (1983), there was, it seems to me, not much real progress.

Ironically, the conjecture about the proportion of regular primes remains open today, even after FLT has been solved. We do not even know whether there exist infinitely many regular primes, although (further irony) we do know that there exist infinitely many *irregular* primes. And one final irony: although the study of the arithmetic of rings of integers in cyclotomic fields did not prove to be the path to the final solution to FLT, it nevertheless has become an important part in modern algebraic number theory, thanks to the work of the 20th century number theorist Kenkichi Iwasawa. Why is this ironic? Because Wiles was a very famous number theorist long before he proved FLT: his early work was on a "Main Conjecture" in Iwasawa Theory.

[2]The Bernoulli numbers – which we will not define here, but see e.g. Wikipedia – are a kind of "rich man's Fibonacci numbers": almost as easy to define and compute, they turn out to have a much deeper role to play in number theory.