Chapter 6

The Last Theorem

NOTE: This chapter is just an outline as we didn't have time to cover this this semester.

More generally that just getting non-existence of solutions to certain Diophantine equations, we can also obtain necessary conditions for solutions to Diophantine equations. We illustrate this here by saying a little bit about Fermat's Last Theorem.

Let $n \in \mathbb{N}$. A solution (x, y, z) to the Diophantine equation

$$x^n + y^n = z^n \tag{6.0.1}$$

is said to be **trivial** if $xyz = 0$, i.e., if at least one of x, y and z is 0. Note there are infinitely many solutions with $xyz = 0$ and they are easy to describe. E.g., if $y = 0$, this reduces to $x^n = z^n$, which means $x = z$ or $x = \pm z$, depending on whether n is odd or even.

Theorem 6.0.1. Fermat's last theorem *For $n \geq 3$, $x^n + y^n = z^n$ has no nontrivial solutions over $\mathbb{Z}$. In particular, it has no solutions in positive integers.*

The story is Fermat claimed in 1637 in a margin of a copy of *Arithmetica* (an Ancient Greek text by Diophantus) to have a beautiful proof, but said the proof could not fit in the margin. For centuries, mathematicians tried to find a proof of this, and it was eventually proven in 1995 by Andrew Wiles with help from Richard Taylor, building on the work of many others and using mathematics far beyond what was available in Fermat's time. For a long time, people wondered if Fermat really had a proof, and this was one of the romanticized mysteries of mathematics. But what is generally suspected now is that Fermat did have proofs for $n = 3$ and $n = 4$, and possibly some other cases, and probably he thought he had an argument which would work in general but turned out to be incorrect (which Fermat may or may not have realized himself later).

I had hoped to have 2–3 lectures to discuss Fermat's last theorem in class, but ran out of time. Here is what I had hoped to do:

- reduce proving Fermat's last theorem to the cases $n = 4$ and n is prime (it's an easy exercise you can do yourself)
- prove the $n = 4$ case of Fermat's last theorem using descent like Fermat, by showing that $x^4 - y^4 = z^2$ has no "primitive" solutions

- prove or at least sketch the $n = 3$ case of Fermat's last theorem using unique factorization in $\mathbb{Z}[\zeta_3]$
- explain, roughly, how knowing unique factorization in $\mathbb{Z}[\zeta_p]$ would prove the $n = p$ case of Fermat's last theorem (in 1847 Lamé used this idea to give a flawed proof—Kummer noted the proof doesn't work for all primes because he already knew $\mathbb{Z}[\zeta_p]$ doesn't always have unique factorization[1]), and what we know about when $\mathbb{Z}[\zeta_p]$ has unique factorization or not

Maybe I will write some of this the next time I teach this course. I only include now a partial elementary result on the $n = 3$ case of Fermat's Last Theorem.

Proposition 6.0.2. *If there is a nontrivial solution to $x^3 + y^3 = z^3$ (i.e., a solution over $\mathbb{Z}$ with x, y, z all nonzero), then there is a solution with exactly one of x, y, z divisible by 7.*

Proof. First, if there is a nontrivial solution to $x^3 + y^3 = z^3$, we may replace x, y and z with x/d, y/d and z/d where d is the gcd of x, y and z to get what is called a primitive solution, i.e., one where no prime p divides all of x, y and z. □

[1] So now Lamé is probably best known in number theory for this mistake. *C'est dommage!* He seems to otherwise have been a good mathematician.