Section 3: Problems Generalizing

Fermat's Last Theorem (FLT) states that if $n > 2$, then $x^n + y^n = z^n$ implies $xyz = 0$. In other words, the only solutions to $x^n + y^n = z^n$ are trivial. We have seen proofs for the cases $n = 3$ and $n = 4$ in the two previous sections. Many other cases were proved independently over the years:

n	Proved by	When
3	Fermat?	
	Leonhard Euler	1747
4	Fermat	1637
5	Adrien-Marie Legendre	1825
	Gustav Lejeune Dirichlet	1825
7	Gabriel Lamé	1839
14	Gustav Lejeune Dirichlet	1832

It is worth mentioning that after the $n = 4$ case had been resolved, FLT only needed to be verified for odd prime exponents. When Dirichlet proved the case $n = 14$, he had actually been attempting to prove $n = 7$, but proved a weaker theorem instead. In any case, all of these results were for specific cases. It would obviously be impossible to prove the complete FLT case-by-case. A more general approach was necessary.

Exercise 2.3.1 Show that once FLT had been verified for $n = 4$, it only needed to be verified for odd prime exponents. (Hint: suppose it was already known to be true for odd prime exponents. Show that it is true for composite exponents also.)

The first progress in generality came from Sophie Germain (1776-1831). In these days, it was highly unusual for a woman to be taken seriously in any scientific field. In fact, when she began her correspondence with the leading mathematician of her time Carl Gauss, she identified herself as Monsieur LeBlanc. Despite this obstacle, she was an accomplished mathematician and when Gauss learned her true identity he said,

> *When a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men to familiarize herself with these thorny researches, succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of them, then without a doubt she must have the noblest courage, quite extraordinary talents, and a superior genius.*

With regards to FLT, Germain showed that if p and $2p+1$ are both prime, then $x^p + y^p = z^p$ implies that one of x, y, z is divisible by p. (Primes p of this form – with $2p+1$ also prime – are now called ***Germain primes*** in her honor.) This was not a result about one particular, it was the first result that was general and it was used by Legendre, Dirichlet, and Lamé to prove their special cases. But still a general solution eluded mathematicians.

Exercise 2.3.2 Germain primes are primes p for which p is also prime. The first four are 2, 3, 5, and 11. Find the next five.

So what was the trouble? When Euler "proved" the $n = 3$ case he didn't use the argument we outlined in Section 2.2. But as we mentioned, he was familiar with those methods, so despite his error in logic, he is still given credit. His error was in fact repeated in 1847. On March 1, Lamé announced a proof of Fermat's Last Theorem, but he made the same incorrect assumption that Euler had made 100 years earlier. Surprisingly, it has to do with how differently real numbers behave compared to complex numbers.

It is worth noting that prior to the 18th century imaginary numbers were not widely accepted. Just 200 years earlier they were completely unheard of. The Italian number theorists of the Renaissance first tried working with square roots of negative numbers, but only temporarily. They would allow their use during a problem, but still did not fully admit their existence and imaginary numbers were not allowed as solutions. One hundred years before Euler, Rene Descartes believed they were such nonsense that he termed them "imaginary". By Euler's time, mathematicians were warming to the notion that arithmetic and algebra could work with imaginary numbers – thanks in no small part to Euler and his advocacy of them (in fact, it was Euler to whom the symbol i is credited). But it turns out that some fairly natural properties of the integers are lost when we extend to certain sets of complex numbers.

In $\mathbb{Z}$, we have unique factorization. In other words, there is exactly one way to factor integers into their prime factors (up to their order). What Euler and Lamé had done was factor over an extension of the integers; complex numbers of the form $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} : a, b \in \mathbb{Z}\}$ for some integer $d > 0$. It was Joseph Liouville who first suggested the idea of factoring $x^n + y^n = z^n$ into linear factors over the complex numbers. But when Lamé presented his proof in 1847, it was the same Liouville who pointed out that unique factorization was a necessity, but he was not sure it held. Once this problem was discovered mathematicians focused their attention on proving uniqueness of factorization. Two weeks after Lamé announced his proof, Pierre Wantzel made the following amazing claim about unique factorization that seems a bit hopeful in retrospect:

> *It is true for n = 2, n = 3 and n = 4 and one easily sees that the same argument applies for n > 4.*

Wantzel was incorrect. It can be shown that in $\mathbb{Z}[\sqrt{-5}]$, 2, 3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are all irreducible (i.e. prime). So the number 6 has two distinct factorizations:

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

Example 2.3.3 Let's see how $1+\sqrt{-5}$ is irreducible. This will require the notion of a ***norm*** of a number. The norm of $a+b\sqrt{-d}$ is $N(a+b\sqrt{-d}) = a^2 + db^2$. The important property will need of norms is the following: if $\alpha, \beta \in \mathbb{Z}[\sqrt{-d}]$, then $N(\alpha\beta) = N(\alpha)N(\beta)$.

Now clearly even in $\mathbb{Z}$, every number has many factorizations. For example, the number $7 = 1 \cdot 7 = (-1)(-7) = 1 \cdot 1 \cdot (-1) \cdot (-7)$. But multiplying by 1 and -1 should not count. In general, any number that has a norm of 1 is called a ***unit***. When factor a number uniquely, we don't use units. So with this understanding 7 cannot be factored in $\mathbb{Z}$, hence it is prime.

Back to $1+\sqrt{-5}$. Suppose it did factor in $\mathbb{Z}[\sqrt{-5}]$ without using units. The there exist $a+b\sqrt{-5}$ and $c+d\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ such that

$$1+\sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5}) .$$

Taking norms of both sides, we have

$$6 = (a^2+5b^2)(c^2+5d^2) .$$

But this product is taking place in $\mathbb{Z}$, where we do have unique factorization. Since $6 = 2 \cdot 3$ (recall we are not factoring using units), we must have either $a^2+5b^2 = 2$ or $a^2+5b^2 = 3$. It can easily be seen that both are impossible. So $1+\sqrt{-5}$ cannot factor.

Exercise 2.3.4 Find two distinct factorizations of 21 in $\mathbb{Z}[\sqrt{-5}]$ and show that all four factors are irreducible.

A couple of months later, Liouville presented a letter to the Paris Académie from Eduard Kummer which confirmed that unique factorization is lost, but detailed a potential fix of the problem. Kummer introduced the concept of ***ideal complex numbers*** and used his new theory to find conditions under which a prime is ***regular***, and then proved FLT for all regular primes. This was remarkable progress, for mathematicians believed there were infinitely many regular primes. But this has remained unproved. In 1917, it was finally shown that there are infinitely many irregular primes.

Exercise 2.3.5 This exercise requires you to teach me what a regular prime is. There is more than one definition out there, find one you understand and explain it to me. Do not assume I know what any advanced terms are. Define and explain everything.

Kummer's work was highly influential. (It led to many proofs of individual cases of FLT over the years. With the help of computers in the latter half of the 20th Century, FLT was proven

for specific values of n up to 4,000,000 by 1993.) But clearly to prove FLT in general a different approach was needed. The 20th Century saw such a breakthrough involving a variety of complex topics in the new field of analytic number theory. In Chapter 3, we will outline the relevant theory and finally sketch out the final proof of Fermat's Last Theorem.