V. Number Theory

The history of mathematics in general and the history of number theory in particular virtually go hand in hand. Number theory is one of the oldest fields in mathematics and most of the greatest mathematicians have tried their hand at it. Carl Friedrich Gauss (1777-1855), arguably the greatest mathematician of them all, once said, "Mathematics is the queen of the sciences and the theory of numbers is the queen of mathematics." However, despite its longstanding prominence, when studying number theory and its history, it is possible to look at one particular number theorist from the 17^{th} century as the focal point for all of number theory. His name is Pierre de Fermat.

We met Fermat in the last chapter in the development of the calculus and he also made significant contributions to many other fields, but Fermat is perfectly suited to be both a catalyst and crescendo of number theory research over the years. He is considered the father of modern number theory, his results were far and wide even if unpublished, and one of his conjectures – Fermat's Last Theorem – remained unproved for over 350 years. This remarkable theorem was based on ancient number theory, and the many attempts (by the most remarkable mathematicians in history) to verify it spurred enormous growth in the field. Modern number theory is roughly divided into several different branches: elementary number theory, algebraic number theory and analytic number theory. Fermat's Last Theorem has aspects of all three branches in it, and as we study Fermat and his theorem, we will periodically focus on each branch.

Section 1: Fermat

When we think of the most brilliant people in mathematics in the last 500 years, names like Rene Descartes, Carl Gauss, Isaac Newton, Gottfried Leibniz, and Blaise Pascal are sure to come to mind. Descartes created analytic geometry, Gauss was a genius in number theory (and many other fields), Newton and Leibniz developed the calculus, and Pascal counts the founding of probability theory among his many claims to fame. However, aside from forming an impressive roster of mathematicians, another thing all these greats have in common is a debt of gratitude to Pierre Fermat.

In the last chapter, we saw that Fermat's approach to analytic geometry more closely resembles our current method, and even though Descartes was reluctant at first to acknowledge Fermat's work, eventually he did. We also saw that Fermat make significant progress on problems that led to the development of the calculus. Around this same time, Fermat also worked with Blaise Pascal in formulating the basis of probability. Through many letters with Pascal, he helped lay the foundation of probability theory. While Pascal utilized general mathematical formulae, Fermat relied of direct computation, and his method yielded superior results. All of these achievements would be enough to proclaim Fermat a great mathematician, but Fermat's true love, and the area of his most enduring mathematical contributions, was number theory.

He posed many problems in the field in correspondences with Pascal, Frenicle de Bessy, Christian Huygens, Marin Mersenne, and Gilles Roberval. In many cases he claimed to have solved the stated problem, but would only give further explanation after the recipient had

attempted the problem. Pascal in particular usually ignored the letters, as he had little interest in number theory. Many others grew angry with Fermat and believed he posed impossible problems, but most have since been proved.

- ***Fermat's Little Theorem***: If p is a prime and a and p are relatively prime, then $a^{p-1}-1$ is a multiple of p. (Stated in a letter to de Bessy in 1640, proved by Euler in 1736)

- If p is an odd prime, then p is a difference of two squares in one (and only one) way. For example, $3=2^2-1^2$, $5=3^2-2^2$, $7=4^2-3^2$.

- Every prime of the form $4n+1$ is a sum of two squares. (Stated in a letter to Mersenne in 1640, proved by Euler in 1754)

- Every prime of the form $4n+1$ is (a) once the hypotenuse of a right triangle, (b) its square is twice, (c) its cube is thrice, etc. For example, consider $13=4(3)+1$. Now $13^2=5^2+12^2$, $169^2=65^2+156^2$ and $169^2=119^2+120^2$, etc.

- Every non-negative integer is the sum of four (or fewer) squares. (proved by Lagrange in 1770)

- Every integer of the form $2^{2^n}+1$ is prime. (Sated in the same letter to de Bessy in 1640 and also in a letter to Pascal in 1654. This was disproved by Euler in 1738)

Of particular interest is this last "result". As mentioned, Fermat conjectured that every integer of the form $2^{2^n}+1$ (now called Fermat numbers) was prime. Consider the following table.

n	$2^{2^n}+1$
0	$2^{2^0}+1=3$ (prime)
1	$2^{2^1}+1=5$ (prime)
2	$2^{2^2}+1=17$ (prime)
3	$2^{2^3}+1=257$ (prime)
4	$2^{2^4}+1=65,537$ (prime)

So far, so good. Now we come to the most surprising thing: to date these are the ONLY prime Fermat numbers! Research into Fermat numbers has yielded some very striking results, if not useful. Currently, Fermat numbers have been checked up to $n=2,478,782$. Even if mathematicians cannot factor the number (they are obviously quite large) they are often able to determine whether it is prime or not using Fermat's Little Theorem.

Example 1: Let $F_{14} = 2^{2^{14}} + 1$. This cannot be prime because $2^{F_{14}-1} - 1$ is not a multiple of F_{14} (See Fermat's Little Theorem).

Note however that there may be more prime Fermat numbers, but *so far* the first 5 are the only ones. The smallest Fermat number that is still unknown whether it is prime or composite is $F_{33} = 2^{2^{33}} + 1$.

Fermat resisted many requests to publish his proofs, ideas, and results. In fact, when Roberval offered to edit and publish some of his papers, Fermat said "Whatever of my works is judged worthy of publication, I do not want my name to appear there." He seemed genuinely disinterested in fine-tuning a proof to the point where is could be published. Rather, he enjoyed jotting down a few hints or notes and then announcing the conclusion. Aside from his voluminous collection of letters, from which many of results were retrieved, Fermat left a large collection of theorems/conjectures in the margins of his books. Five years after his death, his son Samuel brought forth a new edition of *Arithmetica* by Diophantus that contained his fathers' marginal notes.

Section 2: Elementary Number Theory

While it easy to say that Fermat is the father of modern number theory, it is of course patently false that he was the first number theorist. As far back as ancient Greece, mathematicians were doing elementary number theory, and of particular interest to the Pythagoreans were the mythical properties of the integers. We have already seen that they initiated the study of amicable numbers, perfect numbers, deficient/abundant numbers, and they also studied figurate numbers (like square, pentagonal, hexagonal), and obviously Pythagorean triples. It was in the section of Diophantus' *Arithmetica* on Pythagorean triples that Fermat noted in the margin:

> *To divide a cube into two cubes, a fourth power into two fourth powers, or in general any power whatever into two powers of the same denomination above the second is impossible, and I have assuredly found a remarkable proof of this, but the margin is too narrow to contain it.*

In other words, the equation $a^n + b^n = c^n$ has no nontrivial solution if $n > 2$. This became Fermat's Last Theorem. We will revisit this theorem in Section 4.

Another famous elementary number theorist was Marin Mersenne (1588-1648). A Minimite friar, Mersenne corresponded with many of the greatest mathematicians of his day. In a time when there were no research journals, Mersenne served as a disseminating body for new results. Upon his death, letters were found from 78 different mathematicians including Fermat, Huygens, Pell, Hobbes, Galileo, and Torricelli. He also regularly opened the monastery for gathering of mathematicians including Desargues, Roberval, Descartes, and both Pascals (father and son).

Although much of his fame can be attributed to this centrality to mathematical research during the century, he is most remembered for his involvement in the search for perfect numbers. Since the days of the early Greeks, mankind had been fascinated with perfect numbers. Mathematicians and non-mathematicians alike were intrigued by their curious properties. Recall that Euclid had a formula for generating even perfect numbers: *if* $2^n - 1$ *is prime, then* $2^{n-1}(2^n - 1)$ *is perfect.* It was quickly determined that for $2^n - 1$ to be prime, n had to be prime as well. As far back as 100 AD, people knew the first four perfect numbers: 6, 28, 496, and 8128. But several conjectures remained:

(1) The n^{th} perfect number P_n has n digits.
(2) If p is prime, is $2^p - 1$ prime?
(3) The last digit alternates between 6 and 8.
(4) Every perfect number is even.

In 1536, Hudalrichus Regius disproved the first two of these conjectures by showing that $2^{11} - 1 = 2047 = 23 \cdot 89$ and finding the 5th perfect number $P_5 = 2^{12}(2^{13} - 1) = 33,550,336$. Then Pietro Cataldi (1548-1626) took the next step forward (dispencing of conjecture #3 in the process) when he found:

$$P_6 = 2^{16}(2^{17} - 1) = 8,589,869,056 \text{ and } P_7 = 2^{18}(2^{19} - 1) = 137,438,691,328.$$

Cataldi also conjectured that $2^p - 1$ would be prime for $p = 23, 29, 31, 37$. In 1640, Fermat disproved the last of these.

So what does this have to do with Marin Mersenne? In 1644, he stated that up to $p = 257$, $2^p - 1$ would be prime for the values: 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257. In 1732 Leonhard Euler showed that $2^{31} - 1$ was indeed prime, giving the 8th perfect number and then in 1738 Euler showed that Mersenne was right (and Cataldi was wrong) in that $2^{23} - 1$ and $2^{29} - 1$ were not prime. But Mersenne was not perfect in his conjecture; in time it was discovered that he made five errors. Three were errors of omission ($2^{61} - 1, 2^{89} - 1$, and $2^{107} - 1$ are all prime) and two errors of commission ($2^{67} - 1$ and $2^{257} - 1$ are not). But considering all the primes numbers up to 257 and their size, Mersenne's conjecture was fairly accurate. In his honor, primes of the form $2^p - 1$ are now called ***Mersenne primes***. With the advent of computers, finding Mersenne primes (and therefore perfect numbers) has become more possible and popular than ever. There are currently 47 known Mersenne primes with the largest being $2^{43,112,609} - 1$ (this number has almost 13 million digits!).

Section 3: Algebraic Number Theory

While elementary number theory is focused on integers and their properties, algebraic number theory is more related to how these properties generalize to other groups of real

numbers. This branch was roughly borne out of the fascination with equation solving we saw in Renaissance Italy.

Recall that in 15th century Italy, mathematicians competed with each other in equation solving contests. Of course the quadratic formula made 2nd degree equations trivial, so they focused on cubic equations. Once formulae to solve these became well known, next up were the quartics. In theory, this could continue indefinitely. Mathematicians soon dispatched of degree 4 equations with the quartic formula and proceeded to attack the quintic. As before, they were looking for a formula, composed of ordinary addition, subtraction, multiplication, divisions, and radicals that would solve an arbitrary 5th degree equation. Seemed like a reasonable goal: quadratic, cubic, and quartic formulae had all been found. Then the most amazing thing happened. At the beginning of the 19th century, two young geniuses Evariste Galois (1811-1832) and Niels Abel (1802-1829) proved that there was no such formula. Both died tragically young (Abel due to illness and Galois in a duel) but the mathematics they created in their short lives advanced algebraic number theory and gave birth to group theory.

The principal number theorists of the 18th century were Joseph Lagrange of France and Leonhard Euler of Switzerland. But in 1777, Carl Friedrich Gauss was born and he would become one of the greatest mathematicians of all time. Legend has it that he was the last mathematician to be knowledgeable of every field of mathematics. In the 100 years after he died, mathematics grew at such a rate, and it such diverse directions, that no one since Gauss can make such an unbelievable claim. His direct contributions are monumental, and he made advancements in the fields of algebra, differential geometry, differential equations, non-Euclidean geometry, complex analysis, real analysis, group theory, topology, and of course number theory. (He also contributed to physics, mechanics, astronomy, geodesy, and magnetism) It is impossible to pinpoint the single item for which Gauss is most famous. In geometry, it is the construction of the 17-gon using only a ruler and compass. In algebra, it is the first completely satisfactory proof of the Fundamental Theorem of Algebra. In number theory, it is his proof of quadratic reciprocity. The details of this wonderful result belong more appropriately in a course on algebraic number theory, but suffice it to say Gauss was a very accomplished mathematician.

Section 4: Analytic Number Theory

It is quite possible that someday generations may look upon the 20th century as the "golden age of number theory." It is the century that saw the first elementary proof of the celebrated Prime Number Theorem in analytic number theory, significant progress on the Riemann Hypothesis (also an analytic number theory result), and most recently the proof of Fermat's Last Theorem (using analytic number theory as well).

One of the greatest mathematicians of the 20th century (maybe even of all-time) was David Hilbert (1862-1943). In his 1900 address to the International Congress of Mathematicians in Paris, Hilbert presented 23 problems/topics/themes he believed should be the main focus in the coming century. He was such an important leader in mathematics that this talk inspired a great deal of research and it is no stretch to say it shaped research for the next 100 years (and counting).

Hilbert's Eighth Problem dealt with several different problems in number theory. Specifically, Riemann's Hypothesis, the Twin Prime Conjecture, and Goldbach's Conjecture. So what are these impressively named conjectures?

If we search through the first hundred positive integers, we may notice some regularity among the primes. This quickly degenerates as we consider more and more integers, and indeed a pattern to the prime numbers has never been found. Primes can be as close together as possible (like 2 and 3, 5 and 7, 41 and 43) and arbitrarily far apart. For example, the 100 numbers from $101!+2$ to $101!+101$ are all composite. This is not the first place where a gap in the primes of this size occurs (note that $101! \approx 9.4 \times 10^{159}$), but it goes to show that primes behave very irregularly at times. Euler defined the function

$$\pi(x) = \text{the number of primes less than } x.$$

The Prime Number Theorem, first formulated independently by Gauss (at age 14 no less) and Legendre, asserts that as $x \to \infty$, $\pi(x)$ is approximately equal to $x/\ln x$. Stated another way, $\lim_{x\to\infty}\left(\frac{\pi(x)}{x/\ln x}\right) = 1$.

Euler attacked the Prime Number Theorem using the zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. This function is defined for all real s values leading to a convergent sum, namely $s > 1$. This has become known as the *Riemann zeta function*, because it was Bernhard Riemann who first extended its domain to the complex numbers. It was in this context that he conjectured that all the non-trivial zeros all have real part equal to $1/2$. This is the celebrated Riemann Hypothesis.

In 1896, Jacques Hadamard and Charles de la Vallée Poussin used Riemann's work to prove (independently) the Prime Number Theorem using complex analysis. However, two surprising things remained true despite the proof of the Prime Number Theorem. First, attempts were still being made to prove it. In fact, in 1948, Selberg and Erdös proved the Prime Number Theorem again, but this time without resorting to complex analysis. The second odd fact after the proof of the Prime Number Theorem was that Riemann's Hypothesis, which was derived from the same work that proved the Prime Number Theorem, remained a challenge and remains so to this day.

The other two conjectures mentioned in Hilbert's Eighth Problem are both easy to state, and yet remained unsolved. Twin primes are primes that differ by two (such as 5 and 7, 17 and 19, 4637 and 4639). The Twin Prime Conjecture simply asserts that there are infinitely many twin primes. The best progress that has been made to date was in 1966 Chen Jing-run showed that there are infinitely many primes p such that $p+2$ is the product of at most two primes.

The last conjecture mentioned in Hilbert's Eighth Problem was stated by Christian Goldbach in a letter to Euler in 1742. Goldbach's Conjecture states that every even number greater than 4 is the sum of two primes. This, too, has had progress towards it. In 1937, Vinogradov showed that every "large" odd number is the sum of three primes, and again in 1966 Jing-run showed that every "large" even number is the sum of either (a) two primes, or (b) a prime and a product of two primes.

Finally, we are brought back to Fermat. Ever since he left that famous marginal note, mathematicians had tried to prove Fermat's Last Theorem (FLT). Recall that Fermat stated that the equation $a^n + b^n = c^n$ has no nontrivial solution if $n > 2$. While he claimed to have had a proof of this (but the margin he was writing in was too small to contain it), no evidence of such a proof has ever been found. The result was shown to be true for individual values of n over the next 200 years. Fermat himself demonstrated the theorem for $n = 4$. Proofs for other specific values of n followed; Euler (in 1747) proved it for $n = 3$, Adrien-Marie Legendre (in 1825) proved it for $n = 5$, Lejeune Dirichlet (in 1832) proved it for $n = 14$, and Gabriel Lame (in 1839) proved it for $n = 7$. During the next 100 years algebraic number theory was developed to tackle the problems encountered by those trying to prove FLT. Led primarily by Richard Dedekind, Ernst Kummer, and Leopold Kronecker, algebraic number theorists succeeded in proving FLT for many values of n, but still a finite list, and very few general results.

The first general result was by Sophie Germain (1776-1831). In 1823, she showed that $a^n + b^n = c^n$ would have no solutions if n was a prime number and $2n+1$ was also prime. In other words, $a^p + b^p = c^p$ has no non-trivial solutions if p is a prime of the form $p = \frac{q-1}{2}$ (for some prime q). Prime numbers of this form (like 2, 3, 5, and 11) are now called ***Germain primes.***

By the middle of the 20th century, number theorists from around the world (specifically Weil and Serre from France, Taniyama and Shimura from Japan, Ribet from the United States, and Frey from Germany) utilized another tool of Fermat's, elliptic curves, to make grand new progress towards a proof. Finally in 1995, Andrew Wiles of England was able to announce he had proven FLT after working on it for years in secrecy. His argument is logically quite simple, even if the mathematics involved is very sophisticated. Read the following, gloss over the technical terms and try and follow the logic.

In 1955, Yutaka Taniyama and Goro Shimura conjectured that every elliptic curve with rational coefficients is modular (the Taniyama-Shimura Conjecture). Then Gerhard Frey (in 1986) associated an elliptic curve to any supposed solution to FLT. Since FLT was not supposed to have any solutions, Frey conjectured that these created elliptic curves of his really didn't exist. Ken Ribet showed in 1990 that Frey's elliptic curves are not modular, contradicting Taniyama-Shimura. Then in 1995, Andrew Wiles proved the Taniyama-Shimura Conjecture and therefore, Fermat's Last Theorem.

Fermat's Last Theorem
Poems

With an integer greater than 2
It's something one simply can't do.
If this margin were fat,
I'd show you all that,
But it's not, so the proof is on you! (Ted Munger)
****
A mathematician named Pierre
Thought "I wonder if someone will care
If I say there's a proof
And then (somewhat aloof)
Admit I can't fit it in there." (Jonathan Matte)
****
Sir Wiles wrote home to his mama
And said "I've improved Taniyama."
His mother replied,
"I am filled with such pride...
And to think I once changed your pajamas." (Jonathan Matte)
****
The proof of the claim of Fermat
Is truly a marvelous tract.
Did Pierre tease us all
'cause the margin was small,
Or his writing was much, much too fat? (Joseph Shaya)
****
We take an elliptic curve E
consider the points killed by 3,
This "rho" must be modular
and by facts which are popular
the proof of Fermat comes for free. (Jeremy Teitelbaum)
****
"My butter, garcon, is writ large in!"
A diner was heard to be chargin'.
"I HAD to write there,"
Exclaimed waiter Pierre,
"I couldn't find room in the margarine." (Howe, Lengstra, and Moulton)
****