CHAPTER I: The Origins of the Problem

Section 1: Pierre 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 was a renowned philosopher who created analytic geometry, Gauss was a genius in number theory (and many other fields), Newton and Leibniz developed the calculus – widely considered one of mankind's greatest achievements, and Pascal counts the founding of probability theory among his many claims to fame. Aside from forming an impressive roster of mathematicians, another thing all these greats have in common is a debt of gratitude to Pierre Fermat.

Pierre Fermat (1601-1665) was born in France to wealthy and hard working parents. His father was a leather merchant and his mother came from a family of jurists. Fermat followed his mother's family line, and pursued a degree in the civil laws, graduating from the University of Orleans in 1631. He became a counselor (lawyer) after graduating, and because of the high mortality rate of his colleagues, he advanced rapidly. Within 11 years, Fermat rose to the highest office in Toulouse, his hometown. From an early age, Fermat showed a great deal of interest classical works in many fields such as Latin, philosophy, literature, and mathematics. In the latter field, Fermat made extensive study of the ancient works of Archimedes, Apollonius, Euclid, Pappas, and especially Diophantus. However, in the early 17^{th} century, mathematics was not a profession with employment opportunities outside of private tutoring. So while working as a lawyer, Fermat spent his free time on many mathematical problems and topics that would have enormous impact.

Fermat developed analytic geometry around the same time as Descartes, but Fermat's methods more closely resemble our current method, and even though Descartes was reluctant at first to acknowledge Fermat's work, eventually he did. Fermat also made significant progress on problems that led to the development of the calculus. Around this same time, he 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.

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 and is the focus of this course. 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.

Fermat 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 in Mersenne's "academy" grew angry with Fermat, and believed he posed impossible problems, but most have since been proved.

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. In was in this fashion that Fermat made his famous marginal note:

> "However, it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general any power higher than the second into two powers of like degree. I have discovered a truly remarkable proof which this margin is too small to contain."

Fermat was reading about the Pythagorean Theorem in a Latin translation of *Arithmetica* by the ancient Greek mathematician Diophantus (ca. 200-284). The ancient Greeks saw this theorem from the geometrical perspective; namely, you could literally divide a square into two smaller squares. It was in response to this notion that Fermat left his note in the margin of his book. In mathematical symbols, Fermat was claiming that

$$x^n + y^n = z^n \text{ has no solutions for } n > 2$$

This was not the only such claim left by Fermat. As mentioned, he routinely challenged his friends and colleagues with conjectures and theorems he had claimed to have proved already. Here are a few such claims:

- ***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)

- Every integer of the form $2^{2^n} + 1$ is prime. (Stated 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)

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

- Every prime of the form $4n+1$ is (a) the hypotenuse of exactly one right triangle, (b) its square is the hypotenuse of two right triangles, (c) its cube has three, etc. For example, consider $13 = 4(3)+1$.

  $13^2 = 5^2 + 12^2$ while
  $169^2 = 65^2 + 156^2$ and $169^2 = 119^2 + 120^2$

After his death in 1665, one of his sons published a new edition of *Arithmetica* and included his father's marginal notes. As mathematicians read his conjectures, they set out to prove (or disprove) them. One by one they fell, until just one remained…Fermat's Last Theorem. Of course at this point in history it should properly have been called Fermat's Last *Conjecture* since it hadn't been proven yet. But by the 20th century, it had been verified case-by-case for extremely large values of n and as such most people believed it to be true, even if Fermat was wrong in thinking he had a correct proof.

Another one of Fermat's most lasting contributions to mathematics is his favorite method of proving things – ***the method of infinite descent***. It is a method that is similar to our more recognizable method of proof by contradiction, and it also bears some resemblance to mathematical induction. It works best when trying to prove a negative proposition (asserting that something does not exist for example) but there are ways to adapt it to positive ones as well. We will illustrate it with an example.

Example 1.1.1 Show that the equation $a^2 + b^2 = 3(c^2 + d^2)$ has no solutions in the natural numbers.

Proof: Suppose solutions do exist. Choose one such solution (a_0, b_0, c_0, d_0). So we have

$$a_0{}^2 + b_0{}^2 = 3(c_0{}^2 + d_0{}^2). \qquad (*)$$

This means that 3 divides $a_0{}^2 + b_0{}^2$. The only way this can happen is if 3 divides a_0 and b_0 individually. So there must exist natural numbers a_1 and b_1 such that

$$a_0 = 3a_1 \text{ and } b_0 = 3b_1.$$

Substituting into (*), we get

$$(3a_1)^2 + (3b_1)^2 = 3(c_0{}^2 + d_0{}^2)$$
$$9(a_1)^2 + 9(b_1)^2 = 3(c_0{}^2 + d_0{}^2)$$

$$3(a_1)^2 + 3(b_1)^2 = {c_0}^2 + {d_0}^2$$
$$3({a_1}^2 + {b_1}^2) = {c_0}^2 + {d_0}^2 .$$

But this gives us another solution to the original equation (c_0, d_0, a_1, b_1) in which $a_1 < a_0$ and $b_1 < b_0$. If we order the "size" of each solution by the sum of the four elements, this is a smaller solution. In this fashion, logically we could create an infinite sequence of solutions, each smaller than the previous one. But this is clearly impossible in the natural numbers. So a solution must not exist.

Exercise 1.1.2 In the previous proof, it was stated: "3 divides ${a_0}^2 + {b_0}^2$. The only way this can happen is if 3 divides a_0 and b_0 individually." Prove this. Namely, prove that $3 \mid (a^2 + b^2)$ implies $3 \mid a$ and $3 \mid b$.

Exercise 1.1.3 Perhaps you have seen a proof of the irrationality of $\sqrt{2}$. It normally involves contradiction. Prove it instead using Fermat's method of infinite descent.

Exercise 1.1.4 One of Fermat's conjectures (mentioned above) was that every integer of the form $2^{2^n} + 1$ is prime. Numbers of this form have become known as Fermat Numbers:

$$F_n = 2^{2^n} + 1 \text{ for } n = 0, 1, 2, \ldots$$

Find the first 6 Fermat numbers and verify which of them are prime.

Exercise 1.1.5 Prove that if p is an odd prime, then p is a difference of two squares in one (and only one) way.