FERMAT'S LAST THEOREM AND THE HISTORY OF NUMBER THEORY

Euclid, c. 300 BC. The equation known as the "Pythagorean Theorem" was known to many ancient cultures long before Pythagoras himself. There is evidence that the ancient Egyptians, Babylonians, Indians, and Chinese all knew the relationship among the sides of a right triangle. The ancients also knew a few *Pythagorean triples*, meaning threesomes of integers a, b, c with $a^2 + b^2 = c^2$. The formula that generates *all* the Pythagorean triples, however, is credited to Euclid. Let's investigate how it can be derived.

A Pythagorean triple (a, b, c) is *primitive* if no positive integer (other than 1) divides all three numbers. To generate all the Pythagorean triples, it's enough just to generate the primitive ones.

Exercise 1. Let (a, b, c) be a primitive Pythagorean triple. Show that either a is even and b is odd, or else a is odd and b is even.

Exercise 2. a) This will help with the algebra in the next part: Let's say ax^2+bx+c is a polynomial with *rational* coefficients. If r_1 is one of the roots, what is the other root r_2? If r_1 is rational, show that r_2 is rational also. b) Let C be the circle $x^2 + y^2 = 1$. Choose a number $u > 1$, and let L be the line that runs through $(0, u)$ and $(1, 0)$. Let $P(x, y)$ be the intersection point of L with C which is not $(1, 0)$. Show that P has rational coordinates if u is rational, and vice versa. c) Let $u = p/q$ be a fraction in lowest terms. Derive a formula for a Pythagorean triple in terms of p and q.

Exercise 3. a) Show that if a and b are integers, then $GCD(a - b, a + b)$ is either 1 or 2. When is it 2? b) Show that if a and b are positive integers, $GCD(a, b) = 1$, and ab is a square number, then a and b must both be square numbers. c) Let's say $GCD(x, y) = 1$ and x and y are both odd. Let $p = (x + y)/2$ and $q = (x - y)/2$. Show that $GCD(p, q) = 1$.

c) Derive Euclid's formula a different way: Let $x^2+y^2 = z^2$, with $GCD(x, y, z) = 1$, y even. Turn this into $(z - y)(z + y) = x^2$ and apply a) and b).

Pierre de Fermat, 1601 – 1665. The study of "Number Theory" as we know it today has to do with the study of the whole numbers $1, 2, 3, \ldots$. Modern number theory began with efforts to solve equations with integer solutions. Solving such "Diophantine" equations was a favorite topic of Pierre de Fermat, a judge from Toulouse, France. One of Fermat's many mathematical achievements was the method of "descent", whereby if an equation has one solution in positive integers,

then it necessarily has a smaller one. This leads to a contradiction, because the solutions can't keep getting smaller forever!

Exercise 4. a) Show that $x^2 = 3y^2$ can't have any solutions in nonzero integers x, y. b) Show that $x^3 + 3y^3 + 9z^3 = 0$ can't have any solutions in nonzero integers x, y, z.

Fermat was able to show that $x^4 - y^4 = z^2$ could never have a solution in nonzero integers x, y, z. This is a world-class application of his method of descent.

Exercise 5. Assume that $x^4 - y^4 = z^2$ with x odd and y even. Assume also that $GCD(x, y, z) = 1$.

(1) Show that $x^2 + y^2 = s^2$ and $x^2 - y^2 = t^2$ for odd integers s and t with $GCD(s, t) = 1$.
(2) Show that if $u = (s + t)/2$ and $v = (s - t)/2$, then $u^2 + v^2 = x^2$ and $2uv = y^2$. Also show that $GCD(u, v) = 1$.
(3) Show that either u is even and v is odd, or else u is odd and v is even.
(4) Assume u is odd and v is even. Use Euclid's formula to show there are integers p and q with $u = p^2 - q^2$, $v = 2pq$, $x = p^2 + q^2$. Show also that $GCD(p, q) = 1$.
(5) Since $y^2 = 2uv$, there are integers a and b with $u = a^2$, $v = 2b^2$.
(6) Combine the equations $v = 2pq$ and $v = 2b^2$ to show that $p = c^2$, $q = d^2$ for integers c and d with $GCD(c, d) = 1$.
(7) FINALLY, show that $a^2 = c^4 - d^4$. Since $a < x$, we have found a "smaller" solution to the equation $x^4 - y^4 = z^2$ than the original.

Exercise 6. a) Using Fermat's result, show that $x^4 + y^4 = z^4$ has no solutions in nonzero integers x, y, z. b) Show that a right triangle with integer sides could never have a perfect square for its area.

Around 1637, Fermat famously wrote in the margins of his copy of Diophantus' book *Arithmetica*:

> 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 like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.

In other words, $x^n + y^n = z^n$ has no solutions in nonzero integers x, y, z whenever $n > 2$ is an integer. A complete proof of "Fermat's Last Theorem" eluded mathematicians until 1994, due to the work of Andrew Wiles, Richard Taylor, and many, many, *many* others. Do you think Fermat really did have a "marvelous proof"?

Exercise 7. Let's say you want to prove Fermat's Last Theorem for every exponent $n > 2$. We've already done the $n = 4$ case. Show that it is enough only to prove the case where n is an odd prime.

Proofs for specific exponents were given in the years following Fermat's death. Using Fermat's method of descent, Euler (1770) gave a proof of the $n = 3$ case. Legendre and Dirichlet (1823) gave a proof of the $n = 5$ case, and Lamé (1839) gave a proof of the $n = 7$ case. At this point the proofs were getting very complicated indeed, and there seemed to be no chance that someone could prove all the cases at once, or even *more than one* case at once. Until...

Sophie Germain, 1776 – 1831 was a French mathematician whose most famous contribution to number theory was a proof of Fermat's Last Theorem which covers cases for many different values of n at once. She corresponded with Carl Gauss under the pseudonym "Monsieur Le Blanc." When Germain's identity was revealed to Gauss, his reply was:

> But how to describe to you my admiration and astonishment at seeing my esteemed correspondent Monsieur Le Blanc metamorphose himself into this illustrious personage who gives such a brilliant example of what I would find it difficult to believe. A taste for the abstract sciences in general and above all the mysteries of numbers is excessively rare: one is not astonished at it: the enchanting charms of this sublime science reveal only to those who have the courage to go deeply into it. But 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 doubt she must have the noblest courage, quite extraordinary talents and superior genius. Indeed nothing could prove to me in so flattering and less equivocal manner that the attractions of this science, which has enriched my life with so many joys, are not chimerical, [than] the predilection with which you have honored it.

Before studying Germain's contribution to Fermat's Last Theorem, we need the notion of "modular arithmetic." For integers n and m, say $n \mod m$ is the remainder you get when you divide m into n. Thus $100 \bmod 9 = 1$. (The standard notation for this is $100 \equiv 1 \pmod 9$.)

Exercise 8. Calculate: $1^4 \bmod 5$, $2^4 \bmod 5$, $3^4 \bmod 5$, $4^4 \bmod 5$. Also: $1^{10} \bmod 11$, $2^{10} \bmod 11$, $3^{10} \bmod 11$, ... What's the pattern? (Hint: for $2^{10} \bmod 11$, you can first compute $2^5 \bmod 11$, and then square the result.)

Exercise 9. Use "Fermat's Little Theorem" to show that if p is an odd prime and a is an integer not divisible by p, then $a^{(p-1)/2} \bmod p = \pm 1 \bmod p$.

Exercise 10. Let's assume $x^5 + y^5 + z^5 = 0$, with none of x, y, z being divisibly by 5. (One or more of the variables might be negative.) Assume $GCD(x, y, z) = 1$. Derive a contradiction through the following steps:

(1) $-z^5 = (x + y)(x^4y - x^3y^2 + x^2y^3 - xy^3 + y^4)$. Show that the factors $x + y$ and $x^4y - x^3y^2 + x^2y^3 - xy^3 + y^4$ have a GCD of 1.
(2) Deduce that $x + y = A^5$ and $x^4y - x^3y^2 + x^2y^3 - xy^3 + y^4 = T^5$ for integers A and T. Similarly, $x + z = B^5$ and $z + y = C^5$ for integers B and C.
(3) Apply Exercise 9 to the equation $x^5 + y^5 + z^5 = 0$ to show that one of the integers x, y, z must be divisible by 11. Let's assume z is divisible by 11 – the cases where 11 divides one of the other variables will be very similar.
(4) Show that $-A^5 + B^5 + C^5 = 2z$. Deduce that one of the integers A, B or C must be divisible by 11.
(5) If 11 divides B or C, you'll get a contradiction because then 11 would divide all three of the numbers x, y and z. By elimination, A must be divisible by 11.
(6) By combining the equations $x+y = A^5$ and $x^4y-x^3y^2+x^2y^3-xy^3+y^4 = T^5$ with the fact that A is divisible by 11, show that $T^5 \bmod 11 = 5y^4 \bmod 11$.
(7) Use the equation $z + y = C^5$ to show that $y \bmod 11 = \pm 1 \bmod 11$.
(8) Combine the previous two steps to find a contradiction!

Sophie Germain's Theorem says: If p is an odd prime and $2p+1$ is also prime, then $x^p + y^p + z^p = 0$ has no solutions in integers x, y, z none of which are divisible by p. A prime p for which $2p + 1$ is also prime is called a "Germain" prime. Thus $3, 5, 11, 19, 23$ are all Germain primes. Unfortunately it is not known whether there are infinitely many Germain primes.

Carl Gauss, 1777-1855. Carl Gauss was not only one of the greatest mathematicians in history, but also a top notch astronomer, geometer, physicist, statistician...you name it! Gauss was not all that interested in Fermat's Last Theorem, although he did develop an original proof of the $n = 3$ case. However, Gauss was the first to discover that Diophantine equations could be solved by extending outside the realm of ordinary integers and into new systems of *complex numbers*.

Exercise 11. a) We know $x^2 - y^2$ factors as $(x + y)(x - y)$, but how does $x^2 + y^2$ factor? b) It was known to Gauss that numbers of the form $a + bi$ with a and b integers possess the same properties of unique factorization as the ordinary integers. These numbers are called *Gaussian integers*. In particular, we have something like Exercise 3, part (b). Granting this, do the following: Suppose $x^2 + y^2 = z^2$ with $GCD(x, y, z) = 1$ and y even. Show that $x + iy = (p + qi)^2$ for integers p and q. Deduce Euclid's formula for a third time!

Challenge Problems. a) Use Gaussian integers to show that $x^2 + 1 = y^3$ has no solutions in positive integers. (Factor the left hand side of the equation.) b) The numbers of the form $a + b\sqrt{-2}$, where a and b are ordinary integers, also satisfy the property of Exercise 3, part (b). Find all integer solutions to $x^2 + 2 = y^3$.