FERMAT'S LAST THEOREM

DYLAN GROOS, NATALIE SCHUDROWITZ, AND KENNETH BERGLUND

Date: May 3, 2016.

Introduction

Pierre de Fermat was a French lawyer-cum-mathematician whose posthumously published works (consisting of notes in texts) in the 17th century revealed a mathematical challenge. Though he boldly claimed to have proven the theorem he had scrawled in the margins of his copy of Diophantus' Arithmetica ("*I have discovered a truly remarkable proof which this margin is too small to contain*") [9], the proof of the theorem remained missing for centuries, despite the efforts of mathematicians worldwide. The famous theorem is known as Fermat's Last Theorem, and states

Theorem. *$x^n + y^n = z^n$ has no nontrivial integer solutions for x, y, and z when $n > 2$.*

While it appears to be a simple theorem, its proof is anything but. It was over three centuries before an acceptable proof was officially generated and announced to the mathematical community. British mathematician Andrew Wiles was its originator, succeeding by "(1) replacing elliptic curves with Galois representations, (2) reducing the problem to a class number formula, (3) proving that formula, and (4) tying up loose ends that arise because the formalisms fail in the simplest degenerate cases" [12]. The complexity of the proof has made countless mathematicians doubt Fermat's claim to a 'truly remarkable proof which this margin is too small to contain.' Many believe Fermat proved his last theorem for n = 4, which was discovered later in letters of correspondence between Fermat and a colleague, then assumed the theorem's infinite property. Thus, either he truly did produce a proof whose substance a physical page could not contain, bypassing 300 years of what was essentially mathematical struggle, or he didn't; the latter, we consider more likely.

Beginnings. Fermat, did, however produce a proof of his theorem in the case that $n = 4$. What follows is the proof that he gave in the 17th century, as related by Silverman [8].

Theorem. *The equation $x^4 + y^4 = z^4$ has no solutions in positive integers x, y, and z.*

As a preliminary outline, using the idea of descent, we are "writing a prime as the sum of two smaller squares to 'descend from a large solution to a small solution." Suppose there is a solution (x, y, z) in positive integers, and use this to produce a new solution (X, Y, Z) in positive integers with $Z < z$ (by descent). By repeating this process, we end up with an infinitely decreasing list of integer solutions $(x_1, y_1, z_1), (x_2, y_2, z_2), \ldots$ with $z_1 > z_2 > \ldots$ However, it is impossible to have infinite list of decreasing positive integers because eventually, the list will reach 0. Therefore, the only way to solve this issue is to claim that our supposition that there is a solution (x, y, z) to $x^4 + y^4 = z^4$ is false. We now proceed to the proof.

Proof. Assume there is a solution (x, y, z) to the equation

$$x^4 + y^4 = z^2.$$

This is a simple restatement of the problem, since the fourth power of any number can be rewritten as the square of that number squared. We are also able to assume that x, y, and z are relatively prime because otherwise we could just factor out any

common factors. Therefore, if we let $a = x^2, b = y^2$ and $c = z$ then (a, b, c) is a primitive pythagorean triple. Remembering what we learned in lectures and earlier chapters in the textbook about primitive pythagorean triples we are able to say that $a = x^2 = st, b = y^2 = \frac{s^2-t^2}{2}, c = z = \frac{s^2+t^2}{2}$. st is equal to a square, so it must be 1 (mod 4) or 0 (mod 4), since these are the only squares mod 4. It is also odd by definition, which means $st \equiv 1(\text{mod } 4)$. s and t are either both 1 (mod 3) or 1 (mod 4). This means $s \equiv t \pmod 4$. Then we have the equation

$$2y^2 = s^2 - t^2 = (s-t)(s+t).$$

s and t are both odd and relatively prime, thus the only common factor of $(s-t)$ and $(s+t)$ is 2. $(s-t)$ is also divisible by 4 (because they are congruent mod 4 and subtracting the two would yield a result of 0 mod 4, or divisible by 4). $(s+t)$ must be twice an odd number. Furthermore, we know that $(s-t)(s+t)$ is twice a square. As a result, we have $s+t = 2u^2$ and $s-t = 4v^2$ with u and $2v$ relatively prime. Using elimination and substitution, we solve for s and t in terms of u and v,

$$s = u^2 + 2v^2, t = u^2 - 2v^2.$$

These equations can be substituted into the formula $x^2 = st$, resulting in

$$x^2 = u^4 - 4v^4$$

or

$$x^2 + 4v^4 = u^4.$$

Rinse and repeat, letting $A = x^2, B = 2v^2$, and $C = u^2$. We now have to show that this new u in u^2 is smaller than the original z, thus showing that the solutions are infinitely decreasing positive integers.(A, B, C) is a primitive pythagorean triple. Again using our knowledge of primitive pythagorean triples, we can find two relatively prime odd integers S and T such that

$$x = A = ST, 2v^2 = B = \frac{S^2 - T^2}{2}, u^2 = C = \frac{S^2 + T^2}{2}.$$

From the middle equality,

$$4v^2 = S^2 - T^2 = (S-T)(S+T).$$

S and T are odd and relatively prime so the greatest common divisor of $(S-T)$ and $(S+T)$ is 2 and their product is a square, giving:

$$S + T = 2X^2, S - T = 2Y^2$$

for some integers X and Y. Using elimination and substitution,

$$S = X^2 + Y^2, T = X^2 - Y^2.$$

Substitute into the equation for u^2,

$$u^2 = \frac{S^2 + T^2}{2} = \frac{(X^2+Y^2)^2 + (X^2-Y^2)^2}{2} = X^4 + Y^4.$$

We now have a new solution (X, Y, u) for our original equation $x^4 + y^4 = z^4$

$$z = \frac{s^2 + t^2}{2} = \frac{(u^2 + 2v^2)^2 + (u^2 - 2v^2)^2}{2} = u^4 + 4v^4$$

where z, u, and v are integers.

Clearly $u < z$, showing that the list of positive integer solutions to $x^4 + y^4 = z^2$, $(x_1, y_1, z_1), (x_2, y_2, z_2), \ldots$ with $z_1 > z_2 > \ldots$ is decreasing infinitely, allowing us to make the claim that there are no solutions because this cannot occur. □

In 1670, Fermat's son published his father's letters, this proof among them, and in 1729, Leonhard Euler read some of Fermat's results [2]. Reading Fermat's work sparked Euler's initial interest in number theory. Euler, along with Carl Friedrich Gauss, proved that there is no solution for $n = 3$; Adrien Legendre and Lejuene Dirichlet, $n = 5$ [8]. Although these proofs are complicated and quite clever, they failed to scratch the surface of the full and final proof of Fermat's Last Theorem, something that would ultimately require different machinery and even entire fields of number theory that hadn't yet been developed.

Sophie Germaine

The full proof of Fermat's Last Theorem had to be slowly shaped over almost 300 years by the chisel of mathematical progress. A diverse and eclectic group of mathematicians contributed to the final Wiles proof in 1994. Sophie Germain, a French mathematician who received an honorary degree from the University of Göttingen, was one these contributors. Despite women having extremely limited academic opportunity in the 18th and 19th centuries, especially in math and science, she was able to study at École Polytechnique in Paris and keep in correspondence with Gauss, both accomplished by way of a male alias, Monsieur Antoine-August Le Blanc [7, 10]. In 1823, following a prolonged fascination with Fermat's Last Theorem and the challenge it presented, she introduced the following theorem:

Theorem. *If n is an odd prime such that $2n + 1$ is also a prime, the equation $x^n + y^n = z^n$ has no integer solutions x, y, z of which none are divisible by n.*

n is defined as a Germain prime if both n and $2n+1$ are primes. Examples include $2, 3, 5, 11 \ldots$ [12]. In other words, Germain's theorem states that given $x^n + y^n = z^n$ where n is a Germain prime, at least one of x, y, or z is divisible by n. This allows us to eliminate an entire class of possible solutions for $n =$ Germain primes $-$ those solutions in which neither x, y, nor z is divisible by n. This leaves behind those solutions x, y, z in which one is divisible by n. Thus, Germain effectively divided the approach to Fermat's Last Theorem into two cases [6, 13]:

Case 1. $x^n + y^n = z^n$ eliminate solutions x, y, z in which none is multiple of n

Case 2. $x^n + y^n = z^n$ eliminate solutions x, y, z in which only one is a multiple of n

Remark. Two divisible by n implies all three are divisible, which is reducible and leaves behind either Case 1 or 2.

This generalized result on Fermat's Last Theorem showed to be important in supporting later research on the topic. It was the first attempt that involved proving Fermat's Last Theorem for infinitely many primes, rather than proving it on a case-by-case basis, which was the previous modus operandi. Germain's proof is as follows:

Proof. We will prove this by contradiction [3]. Suppose there is a solution (x, y, z) to $x^n + y^n = z^n$ such that $n \nmid xyz$. Assume x, y, and z are relatively prime, since if not, they cancel out, forming a primitive triple. We can factor $x^n + y^n$ as

$$(x + y)(x^{n-1} - x^{n-2}y \ldots - xy^{n-2} + y^{n-1}).$$

From this, we deduce that $(x+y)$ and $(x^{n-1}-x^{n-2}y \ldots -xy^{n-2}+y^{n-1})$ are both perfect n^{th} powers, since the factors are relatively prime $(n \nmid xyz)$. If there was a prime factor k common to both $(x + y)$ and $(x^{n-1} - x^{n-2}y \ldots - xy^{n-2} + y^{n-1})$, then $x \equiv -y \pmod{k}$ so that $(x^{n-1} - x^{n-2}y \ldots - xy^{n-2} + y^{n-1}) \equiv nx^{n-1} \pmod{k}$. This isn't possible because if k divides x it necessarily must divide y, which cannot be true, and if k divides n, n has to be k and must divide z^n, and therefore x, which isn't true.

We therefore have $x + y = m^n$ for some integer m. We also have $z - y = j^n$ and $z - x = l^n$. We know that for every integer β,

$\beta^n \equiv \pm 1$ or $0 \pmod{2n + 1}$ implies that $2n + 1$ divides either x, y, or z. Say it divides x:

$2x \equiv m^n + j^n - l^n \equiv 0 \pmod{2n + 1}$.

This implies that $2n + 1$ must divide either m, j, or l. $2n + 1$ can't divide m or l because that would mean it has to divide y or z along with x, which isn't a possibility. The other cases using y and z follow the same reasoning, therefore we have a contradiction. Thus, the theorem is proven by contradiction. □

Further Developments. It is easy to see that if Fermat's Last Theorem could be proven for all primes, the proof for all integers greater than 2 would follow closely. Since any integer n is a product of primes, we have that $p \mid n$ or $n = pm$ and can rewrite

$$A^n + B^n = C^n$$

as

$$(A^m)^p + (B^m)^p = (C^m)^p.$$

Proving Fermat's Last Theorem for all primes greater than 2 therefore seemed the first logical step towards proving the infinite property. Leopold Kronecker, Richard Dedekind, and Ernst Kummer made important contributions in this regard.

Kronecker (1823-1891) revised many earlier ideas on L series, mostly by Dirichlet, and applied them to the Prime Number Theorem to describe the density and distribution of regular prime numbers to infinity [5]. Dedekind (1831-1916) is one of the fathers of modern algebraic number theory. He formulated the correct definition of a ring of integers in a number field and showed the unique factorization for different integer rings [5]. Kummer (1810-1893), perhaps the most important of the three to the history of Fermat's Last Theorem, combined the findings of the other men, along with some of his own research on cyclotomic fields, to prove Fermat's Last Theorem for all regular primes, primes that he defined to have a certain characteristic of divisibility in cyclomatic fields, $p > 2$; an important stepping stone towards the future of the proof of Fermat's Last Theorem. Kummer also defined irregular primes as primes not proven for FLT by this method [5].

He used roots of unity and cyclotomic fields while working in the integer ring $\sqrt{-5}$ to prove the theorem for regular primes. The proof is eloquent, clever, and

complicated, utilizing the most groundbreaking ideas in number theory for the time period. Kummer originally stumbled upon Fermat's Last Theorem while attempting to generalize the law of quadratic reciprocity using cyclotomic fields [11]. While Kummer didn't prove FLT for all primes, he solved it for an infinite number of regular ones; a leap of progress towards solving the infinite characteristic of Fermat's Last Theorem.

Elliptic Curves

Elliptic curves end up playing a pivotal role in the eventual proof of Fermat's Last Theorem. In 1995, Andrew Wiles proved an important conjecture, the Shimura-Taniyama conjecture, which concerns properties of elliptic curves [1]. This proof then implied Fermat's Last Theorem. In order to talk about the proof (which, admittedly, is over our heads), we need to take a brief detour to discuss some of the properties of elliptic curves.

The Basics. Most of the following information about elliptic curves is from Silverman's *A Friendly Introduction to Number Theory* [8]. An elliptic curve has an equation of this form:

$$y^2 = x^3 + ax^2 + bx + c$$

One of the interesting things we can do with elliptic curves is something that we've done repeatedly in this class. We can find rational points on a given elliptic curve and then use geometry to try to find more of them. Let's look at an example:

$$E_1 : y^2 = x^3 + 17$$

We can find out that the points $P = (-2, 3)$ and $Q = (2, 5)$ are on the curve by simple trial and error. The line that connects P and Q is given by the following equation:

$$y = \frac{1}{2}x + 4.$$

If we substitute this in for the y in E_1, we get:

$$0 = x^3 - \frac{1}{4}x^2 - 4x + 1.$$

We already know x = 2 and x = -2 are roots, so we can factor this as

$$0 = (x - 2)(x + 2)(x - \frac{1}{4}).$$

Plugging $x = \frac{1}{4}$ into E_1, we find a new solution $(\frac{1}{4}, \frac{33}{8})$. Then, we can reflect this point onto the lower half of the curve by making the y-coordinate zero. The process then repeats. We can do this infinitely often for E_1 to generate an infinite number of rational points on the curve. In 1922, L.J. Mordell proved a theorem which states that certain elliptic curves have only a finite list of solutions $P_1 = (x_1, y_1), P_2 = (x_2, y_2), ..., P_r = (x_r, y_r)$, with rational coordinates such that we can find every rational solution to a given elliptic curve by finding lines through these pairs of points that intersect with the curve and reflecting to get new points [8]. The curves for which this is true are the curves whose discriminant

$$\Delta(E) = -4a^3c + a^2b^2 - 4b^3 - 27c^2 + 18abc \neq 0.$$

where a, b, and c are defined in the general equation of an elliptic curve given above.

Complications Arise. This is an unusual situation, however. If we examine the curve

$$E_2 : y^2 = x^3 + x,$$

we find that the only rational point is $(0, 0)$. Similarly, for

$$E_3 : y^2 = x^3 - 4x^2 + 16,$$

We only find four rational points: $(0, 4), (0, -4), (4, 4), (4, -4)$. If we try to use the geometric method described above to find more rational points, we can't seem to enlarge our set of points. We call such a collection of points a torsion collection.

Torsion collections are the subject of several theorems [8]. The Nagell-Lutz Theorem says that the coordinates of each member of a torsion collection of an elliptic curve with a non-zero discriminant are integers. Mazur's Theorem states that a torsion collection contains ≤ 15 points for a curve with non-zero discriminant.

Looking at Congruences. We can also analyze elliptic curves in terms of congruences, a very natural extension based on topics we've explored in this class. For instance, the number of points modulo p, which we will call N_p, on the curve from above,

$$E_2 : y^2 = x^3 + x$$

is surprisingly interesting, given that it has only one rational point in non-modular arithmetic. Here is a table of the number of points, N_p, on E_2 modulo p:

p	2	3	5	7	11	13	17	19	23
N_p	2	3	3	7	11	19	15	19	23

For many of the primes, N_p is pretty close to p, but there are some primes for which there is a difference. In *A Friendly Introduction to Number Theory*, Silverman calls the value $a_p = p - N_p$ the p-defect of an elliptic curve, also known as the trace of Frobenius. There are many interesting properties of a_p, but they're not entirely necessary for the brief overview of Wiles's proof of Fermat's Last Theorem.

Torsion Collections and Congruences. The next logical step is to combine the previous two ideas, looking at torsion collections modulo p. Let's return to the curve

$$E_3 : y^2 = x^3 - 4x^2 + 16.$$

Here is a table featuring values for p, N_p, and a_p:

p	2	3	5	7	11	13	17	19	23	29
N_p	2	4	4	9	10	9	19	19	24	29
a_p	0	-1	1	-2	1	4	-2	0	-1	0

A keen eye will notice that most of the values for N_p appear to be congruent to 4 (mod 5), with the exceptions of $p = 2$ and 11. Why is this so?

First, let's go back and look at the rational points on E_3. There are four of them: $(0,4), (0,-4), (4,4)$, and $(4,-4)$. These form a torsion collection. However, since we're working with moduli, we can find new rational points modulo p. One such point is $Q_0 = (1,8)$, which solves the congruence $y^2 \equiv x^3 - 4x^2 + 16 \pmod{17}$. If we find a line between Q_0 and say, $(0,4)$, we can find a new rational point plugging the line into the congruence and factoring. Each of the other three points in the torsion collection works the same way, generating a new point modulo p. We get a total of five new points, Q_0, Q_1, Q_2, Q_3, and Q_4.

This gives us an insight into why N_p is usually congruent to 4 (mod 5). We have the 4 points from the torsion collection, plus a group of five other points generated by using a new point and drawing lines connecting it to the points of the torsion collection.

p =2 and 11, however, still cause us problems. They are called bad primes for E_3, since they lead to double or triple roots mod p. They also have the property that they divide the discriminant of E_3.

$$\Delta(E_3) = -2816 = \left(-(2^8)\right) 11.$$

It All Starts to Come Together. The next section really starts to approach the fringes of our understanding. Let's look at the following expression:

$$\Theta = T\{(1-T)(1-T^{11})\}^2\{(1-T^2)(1-T^{22})\}^2\{(1-T^3)(1-T^{33})\}^2\dots$$

Let's expand this until we reach the term $\{(1-T^{23})(1-T^{253})\}^2$. Then we get $\Theta = -2T^2 - T^3 + 2T^4 + T^5 + 2T^6 - 2T^7 - 2T^8 - 2T^{10} + T^{11} - 2T^{12} + 4T^{13} + 4T^{14} - T^{15} - 4T^{16} - 2T^{17} + 4T^{18} + 2T^{20} + 2T^{21} - 2T^{22} - T^{23}$.

Just as a refresher, here are the values for a_p of E_3 up to 23:

p	2	3	5	7	11	13	17	19	23
a_p	0	-1	1	-2	1	4	-2	0	-1

Amazingly, the values for a_p and the coefficient of the T^p term in the expanded version of Θ line up for all p greater than 3. This is a modularity pattern for E_3. Modularity itself is too complicated to explain, but there is an upside to knowing this terminology. Now, we have everything we need to give a basic explanation of Wiles's proof.

A New Hope. In 1955, in a conference in Japan, the mathematician Yutaka Taniyama began to think about the relationship between elliptic curves and modular forms, objects related to the Θ above [1]. His ideas piqued the interest of French mathematician Andre Weil, whose name is often associated with the conjecture. Tragically, Taniyama committed suicide in 1958, but his friend Goro Shimura continued to refine his conjecture, which states that every elliptic curve is related to a modular form [8]. That is, the value of a_p always follows a modularity pattern. This was known as the Taniyama-Shimura conjecture or modularity conjecture, and this proved to be the key in unlocking Fermat's Last Theorem.

Later, a German mathematician Gerhard Frey began to think about this relationship [1]. He consulted with experts in the field, including Barry Mazur and Ken Ribet, and in 1984, he stated that the Taniyama-Shimura conjecture was related to Fermat's Last Theorem. His idea was to take a potential solution, (a,b,c) to

$$x^p + y^p = z^p$$

and analyze an associated curve [2],

$$E_{a,b} : y^2 = x(x - a^p)(x + b^p).$$

Frey conjectured that this was a very strange curve. He said that its p-defects do not follow a modular pattern. But according to the Taniyama-Shimura conjecture, this was not possible. Later, Ribet was able to prove Frey's conjecture (with some help from Mazur). This now meant that if the Taniyama-Shimura conjecture could be proved, a curve associated with a solution to Fermat's vexing Diophantine equation could not exist. This would further imply that Fermat's Last Theorem was indeed true.

Wiles to the Rescue. This all set the stage for Andrew Wiles, a professor at Princeton University, and one of the most famous mathematical achievements of all time. Wiles, who had been captivated by Fermat's Last Theorem in his youth, now was able to put huge amounts of effort toward proving the Taniyama-Shimura conjecture [1]. He did most of the work alone, only talking to colleagues when he needed help and thought that they wouldn't reveal his work to the wider mathematical community. Wiles's task was made easier after he realized that Fermat's Last Theorem would be proven if he could prove the modularity conjecture for semistable elliptic curves, not necessarily all elliptic curves. A semistable elliptic curve is a curve which, for a bad prime p greater than or equal to 3, the value of a_p is restrained to only ± 1.

In 1993 in Cambridge, England, Wiles revealed his proof to the world [1]. Its complexity is beyond the scope of this paper, but it was essentially a counting argument. He devised a way to "count" the number of modular forms and compare it to the number of semistable elliptic curves [1]. However, there was one problem with the proof, which took a year to rectify. The problem was too highbrow for us to understand, but the solution did involve Wiles's recognition of a connection to his own particular topic of expertise, Iwasawa theory (which itself is also too highbrow for us to understand). In 1995, Wiles was able to say that he had solved a problem that had eluded mathematicians for centuries.

Conclusion

The quest to prove Fermat's Last Theorem took us on a grand tour of mathematical ingenuity. We saw how far elementary techniques could take us. We also began an exploration of elliptic curves and their wonderful properties. We saw that these were related in some way to modular forms, which are very complex and unfortunately beyond our understanding. This paper only really begins to scratch the surface of the ideas that went into the proof of Fermat's Last Theorem. Nevertheless, we hope that the reader has come away with some understanding of the main ideas involved, as well as an appreciation for the fascinating history that was wrought during the three century-long quest to unravel the challenge that is Fermat's Last Theorem.

References

[1] Aczel, Amir A. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem.* New York: Four Walls Eight Windows, 1996. Print.

[2] Cox, David A. *Introduction to Fermat's Last Theorem.* Amherst College. http://math.stanford.edu/~lekheng/flt/cox.pdf.

[3] Edwards, Harold M. "From Euler to Kummer." *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* New York: Springer, 1996. 64. Print.

[4] Lehmer, D.H. and Emma. *On the Case of Fermat's Last Theorem.* Lehigh University. http://projecteuclid.org/download/pdf_1/euclid.bams/1183503473.

[5] Milne, J.S. *Algebraic Number Theory.* 2014. www.jmilnemath.org.

[6] O'Connor, JJ, and EF Robertson. "Fermat's Last Theorem." *History Topics: Numbers and Number Theory Index.* School of Mathematics and Statistics, University of St. Andrews, Feb. 1996. Web. 28 Apr. 2016.

[7] Riddle, Larry. *Sophie Germain and Fermat's Last Theorem.* Agnes Scott College, 2009. https://www.agnesscott.edu/lriddle/women/germain-FLT/SGandFLT.htm.

[8] Silverman, Joseph H. *A Friendly Introduction to Number Theory.* 4th ed. Pearson Education, 2012. Print.

[9] Singh, Simon. "The Whole Story." *Fermat's Last Theorem.* New York: 1st Anchor, 1997. N. pag. *Simon Singh.* 2000. Web. Apr. 27.

[10] Suzuki, Jeff. "France." *Mathematics in Historical Context.* Washington, DC: Mathematical Association of America, 2009. 271. Print.

[11] Varma, Il. *Kummer, Regular Primes, and Fermat's Last Theorem.* California Institute of Technology. http://www.math.harvard.edu/~ila/Kummer.pdf.

[12] Weisstein, Eric W. "Sophie Germain Prime." *Wolfram MathWorld.* Wolfram Research, Inc., n.d. Web. 27 Apr. 2016.

[13] Whitty, Robin. "Germain's Theorem." *Theorem of the Day.* 2000. Web. 28 Apr. 2016.