6 Sophie Germain and Fermat's Last Theorem

Since Fermat stated his Theorem in 1637, all attempts to prove it involved descent arguments for single small values of n. The first general leap forward came with the work of the French mathematician Sophie Germain (1776–1831).[1] With p an odd prime, Germain's approach was to split purported solutions to $x^p + y^p = z^p$ into two cases:

- Case 1: x, y, z pairwise coprime and $p \nmid xyz$
- Case 2: x, y, z pairwise coprime and $p \mid xyz$

She was then able to prove case 1 for all odd primes $p \leq 197$.

Auxiliary Primes

Germain considered primes related to p, so-called *auxiliary primes.* The existence of such can be used to show that solutions to $x^p + y^p = z^p$ must have certain properties.

Definition 6.1. Let p be an odd prime. An *auxiliary prime* to p is any prime of the form $\theta = 2kp + 1$ where $k \in \mathbb{N}$. A prime p such that $2p + 1$ is prime is called a *Germain prime.* It is unknown if there are infinitely many of these.

We give Germain's proof of case 1 of Fermat's Last Theorem whenever p is a Germain prime. First, here are a few examples:

p	Auxiliary Primes
3	$7 = 6 + 1, \quad 13 = 2 \cdot 6 + 1, \quad 19 = 3 \cdot 6 + 1, \quad 31 = 5 \cdot 6 + 1, \quad 37 = 6 \cdot 6 + 1, \ldots$
5	$11 = 10 + 1, \quad 31 = 3 \cdot 10 + 1, \quad 41 = 4 \cdot 10 + 1, \quad 51 = 5 \cdot 10 + 1, \quad 61 = 6 \cdot 10 + 1, \ldots$
7	$29 = 2 \cdot 14 + 1, \quad 43 = 3 \cdot 14 + 1, \quad 71 = 5 \cdot 14 + 1, \quad 113 = 8 \cdot 14 + 1, \ldots$
11	$23 = 22 + 1, \quad 67 = 3 \cdot 22 + 1, \quad 89 = 4 \cdot 22 + 1, \quad 331 = 15 \cdot 22 + 1, \ldots$

Lemma 6.2. *Let x, y be coprime integers and p an odd prime. Then,*

$$\gcd\left(x + y, \frac{x^p + y^p}{x + y}\right) = 1 \text{ or } p$$

Proof. Apply the binomial theorem to $\frac{x^p+y^p}{x+y} = \frac{(x+y-y)^p+y^p}{x+y}$ to obtain

$$\begin{aligned} \frac{x^p + y^p}{x + y} &= py^{p-1} - \binom{p}{2} y^{p-2}(x + y) + \cdots + (x + y)^{p-1} \\ &\implies \gcd\left(x + y, \frac{x^p + y^p}{x + y}\right) \Bigg| py^{p-1} \end{aligned}$$

Since x and y are coprime, we have $x + y$ and y^{p-1} coprime. Thus the required gcd is p or 1. ∎

[1] Public knowledge of her work was hampered by her sex. In much of her correspondence with famous mathematicians of the time (Legendre, Lagrange, Gauss) she pretended to be a man, a common tale among intellectual women of the period. Her work on Fermat's Last Theorem is largely known due to it being used by Legendre to prove the case with exponent $n = 5$.

Lemma 6.3. *Let p be a Germain prime with $q = 2p+1$, and suppose that $x^p + y^p \equiv z^p \pmod q$. Then at least one of x, y, z is divisible by q.*

Proof. Suppose that none of x, y, z are divisible by q. By Fermat's Little Theorem and unique factorization modulo q, we have

$$0 \equiv x^{q-1} - 1 \equiv x^{2p} - 1 \equiv (x^p - 1)(x^p + 1) \implies x^p \equiv \pm 1 \pmod q$$

But then $x^p + y^p \equiv z^p \pmod q$ is impossible!

■

Theorem 6.4 (Germain)**.** *Suppose that p is an odd prime and that $q = 2p+1$ is prime. The case 1 of Fermat's Last Theorem holds for p.*

Proof. For a contradiction, suppose that x, y, z is a solution to case 1 of FLT. The Binomial Theorem tells us that

$$z^p \equiv x^p + y^p \equiv (x+y)^p \pmod p$$

Since $p \nmid z$, we also have $p \nmid x + y$. Lemma 6.2 forces $\gcd\left(x+y, \frac{x^p+y^p}{x+y}\right) = 1$.

Now $z^p = (x+y)\frac{x^p+y^p}{x+y}$ is a product of coprime integers, whence both factors are powers of p:

$$x + y = c^p, \qquad \frac{x^p + y^p}{x+y} = \gamma^p$$

Similarly $p \nmid x \implies x^p = (z-y)\frac{z^p-y^p}{z-y} = (z+(-y))\frac{z^p+(-y)^p}{z+(-y)}$ is a product of powers of p:

$$z - y = a^p, \qquad \frac{z^p - y^p}{z-y} = \alpha^p$$

and also

$$z - x = b^p, \qquad \frac{z^p - x^p}{z-x} = \beta^p$$

By assumption, $x^p + y^p \equiv z^p \pmod q$: by Lemma 6.3 we may assume that exactly one of x, y, z (x say[2]), is divisible by q. Now

$$2x = (x+y) + (z-y) - (z-x) = c^p + a^p - b^p$$

Thus $a^p + c^p \equiv b^p \pmod q$. Lemma 6.3 again says that q must divide one of a, b, c. In fact, since $q \mid x$, and not y or z, it follows that $q \mid a$. But then $y \equiv z \pmod q$ and so,

$$\alpha^p = z^{p-1} + z^{p-2}y + \cdots + y^{p-1} \equiv py^{p-1} \pmod q \quad \text{and,}$$
$$\gamma^p = y^{p-1} - xy^{p-2} + \cdots + x^{p-1} \equiv y^{p-1} \pmod q \qquad (\text{since } q \mid x)$$

It follows that

$$p \equiv \left(\alpha\gamma^{-1}\right)^p \pmod q \implies p^2 \equiv \left(\alpha\gamma^{-1}\right)^{2p} \equiv (\alpha\gamma^{-1})^{q-1} \equiv 1 \pmod q$$
$$\implies p \equiv \pm 1 \pmod q$$

which contradicts $2p + 1 = q$.

■

Referring to our table of auxiliary primes, this proves case 1 of Fermat's Last Theorem for the primes 3, 5, 11, etc.

[2]This is without loss of generality: repeat the remainder of the proof for the cases $q \mid y$ and $q \mid z$ if you like…

Generalizing? Think carefully about the proof: what really depended on $q = 2p + 1$ being prime?

1. Lemma 6.2 has nothing to do with q.
2. We twice needed the idea that $x^p + y^p \equiv z^p \pmod{q} \implies xyz \equiv 0 \pmod{q}$ (Lemma 6.3).
3. We finally needed the observation that $X^p \equiv p \pmod{q}$ has no solution.

We have therefore proved a more general theorem: this was stated by Legendre in 1823 and credited to Germain.

Theorem 6.5. *Suppose p is an odd prime. Suppose that $q = 2kp + 1$ is an auxiliary prime which satisfies the following conditions:*

1. $x^p + y^p + z^p \equiv 0 \pmod{q} \implies xyz \equiv 0 \pmod{q}$
2. $x^p \equiv p \pmod{q}$ *has no solutions*

Then case 1 of Fermat's Last Theorem is true for p.

The first condition has been made symmetric.[3] It is also difficult to work with, so an alternative formulation was found:

Lemma 6.6. *Suppose that p is an odd prime for which $q = 2kp + 1$ is an auxiliary prime. Then condition 1 (of Theorem 6.5) holds if and only if the list of pth powers modulo q contains no consecutive non-zero integers.*

Proof. Suppose that $x^p + y^p + z^p \equiv 0$ and $xyz \not\equiv 0 \pmod{q}$. Then $\exists a \in \mathbb{Z}_p^\times$ such that $ax \equiv 1 \pmod{q}$. But then

$$\begin{aligned}(ax)^p + (ay)^p + (az)^p \equiv 0 &\implies 1 + (ay)^p + (az)^p \equiv 0 \\ &\implies (-az)^p \equiv (ay)^p + 1 \pmod{q}\end{aligned}$$

so that $(-az)^p$ and $(ay)^p$ are consecutive non-zero pth powers.
Conversely, assume that $s^p = t^p + 1$ are consecutive non-zero modulo q. Then

$$(-s)^p + t^p + 1^p \equiv 0 \pmod{q}$$

■

Case 1 of Fermat's Last Theorem has therefore been reduced to a hunt for suitable auxiliary primes.

Examples

1. Suppose that $p = 5$ and $q = 2p + 1 = 11$. Consider the powers

   $$1^5, 2^5, 3^5, \ldots, 10^5 \pmod{11}$$

   It can be seen that we only get 1 and 10 (this is trivial by Euler's criterion for quadratic residues). Certainly the theorem is satisfied.

[3] Since p is odd, $z^p = -(-z)^p$ so this is equivalent to $x^p + y^p \equiv (-z)^p$. Since we are dealing with all integers, the negative sign is irrelevant.

2. For $p = 7$, we have the auxiliary prime $q = 4 \cdot 7 + 1 = 29$. We can explicitly check the powers

$$\{1^7,\ 2^7,\ \ldots, 28^7 \pmod{29}\} = \{1, 12, 17, 28\}$$

These are non-consecutive, and none are the prime 7, so the theorem is satisfied.

3. For $n = 17$, we need to go to $q = 8p + 1 = 137$ to see the result. The powers of $x^{17} \pmod{137}$ are 1, 10, 37, 41, 96, 100, 127, 136. Again, none are consecutive and none are congruent to 17.

Legendre built on Germain's work to show that conditions 1 and 2 hold whenever at least one of $4p + 1$, $8p + 1$, $10p + 1$, $14p + 1$, or $16p + 1$ is also a prime: there is a debate over whether these were known to Germain.[4] Regardless of the attribution, between them they were able to prove case 1 of Fermat's Last Theorem for all primes $p < 197$.
Why did they stop before 197? If $p = 197$, then the first three auxiliary primes $q = 2kp + 1$ are $q = 3547$, 4729 and 7487 (corresponding to $k = 9, 12$ and 19). In the first case we obtain consecutive 197th power residues of 1162, 1163, 2384, 2385. In the second case we find 2036, 2037, 2692, 2693. The third prime works: computing all this by hand was prohibitively difficult!

Later Work

Germain attempted to generalize the approach and ultimately claimed that if $x^p + y^p = z^p$ had a solution, then one of $x + y, y - z, z - x$ must be divisible by p^{2p-1} and by the pth power of all auxiliary primes satisfying conditions 1 and 2. Her intent was to show that any purported solutions to case 1 of Fermat's Last Theorem were absurdly huge.
Unfortunately she couldn't prove this. However she did manage to show that if conditions 1 and 2 hold for *some* q, then one of x, y, z is divisible by p^2, so solutions would have to be very large.

For many many decades afterwards, mathematicians hunted for auxiliary primes and thus proofs for case 1 of Fermat's Last Theorem. Using related methods, the following were established:

- Dickson (1908): proved case 1 for all primes < 7000 except for $p = 6857$.
- Emma Lehmer (1941): proved case 1 for all primes < 253747889.
- Heath-Brown, Fouvry, Adelman (1985): there are infinitely many primes for which we can prove case 1 of Fermat's Last Theorem.

[4] If $q = 6kp + 1$ is an auxiliary prime, then condition 1 of Germain's Theorem does not hold.