Why Fermat had (probably) no proof?

2025-12-18

Introduction

In 1637, Fermat stated that:

> It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrate, or in general any power higher than the second into the power of like degree; I have discovered a truly remarkable proof which this margin is too small to contain." (Dickinson (1938))

This theorem is now known as Fermat's Last Theorem, and it formally says the following.

Theorem 0.1 (Fermat's last theorem)**.** *Let $n \geq 3$ be an integer. The equation*

$$x^n + y^n = z^n$$

has no non-trivial solutions $x, y, z \in \mathbb{Z}$.

First, observe that we can reduce to consider only triples $(x, y, z) \in \mathbb{Z}^3$ with $\gcd(x, y, z) = 1$. In particular, in this situation x, y, z are pairwise coprime: for instance, if a prime ℓ divides x and z, then it divides $z^q - x^q = y^q$, hence it divides y, contradicting $\gcd(x, y, z) = 1$. Moreover, Fermat himself proved the theorem in the case $n = 4$; therefore, using basic properties of powers, it is enough to prove the theorem for $n = q$ where q is an odd prime.

To prove Theorem 0.1 we could naively proceed in the following way. Fix an odd prime $q \geq 3$ and suppose that we had a non-trivial solution $x, y, z \in \mathbb{Z}$ of

$$x^q + y^q = z^q \tag{1}$$

Then, reducing this equation modulo every prime p such that $p \nmid xyz$, we get a non-trivial solution modulo p. Therefore, only finitely many primes p can fail to admit a non-trivial solution modulo p. If we proved that for infinitely many primes p the reduction of Equation 1 modulo p has no non-trivial solution, then we would conclude that Equation 1 has no integer solutions at all.

We will prove that this method cannot work. Indeed, we have the following.

Theorem 0.2. *There exists an integer $N \geq q$ such that for every prime $p > N$, Equation 1 has a non-trivial solution in $\mathbb{F}_p$.*

This theorem tells us a lot more than we would need. Indeed, it says that eventually, for every prime p, there is a non-trivial solution modulo p, while we would only need infinitely many such primes.

Warm up: a special case

Proposition 0.1. *Fix a prime q. There are infinitely many primes p such that 2 has a q-th root in $\mathbb{F}_p$.*

From this proposition we obtain that the equation $x^q + y^q = z^q$ has a non-trivial solution modulo p for infinitely many primes p. Indeed, if $z^q = 2$ in $\mathbb{F}_p$, we can choose $x = y = 1$ and get

$$1^q + 1^q = z^q.$$

Remark 0.1. From Proposition 0.1 we already get that Fermat's last theorem cannot be proven by the naive approach we explained. Indeed, we already found infinitely many non-trivial solutions modulo infinitely many primes.

Proof of Proposition 0.1. This proposition is an easy corollary of Corollary 5 you can find in a previous post about the Chebotarev density theorem, applied to the algebra $A := \mathbb{Z}[X]/(X^q - 2)$. □

Proof of Theorem 0.2

The idea to prove Theorem 0.2 is to use a geometric fact. In particular, we want to study the projective curve

$$X := V_+(X^q + Y^q - Z^q) \subseteq \mathbb{P}^2_{\mathbb{F}_p},$$

where $p \neq q$ are primes. Finding a non-trivial solution in $\mathbb{F}_p$ is the same as finding a point $[x : y : z] \in X(\mathbb{F}_p)$ such that $xyz \neq 0$.

After proving that X satisfies the hypotheses of the Weil conjectures, we will use them to establish, for p large enough, a bound

$$\#X(\mathbb{F}_p) > 3q,$$

where $X(\mathbb{F}_p)$ denotes the $\mathbb{F}_p$-rational points. We will also prove that the points where one coordinate vanishes are $\leq 3q$. Therefore, we will get the theorem as a direct consequence of the bound.

We now state the Weil conjectures in the form we need.

Theorem 0.1 (special case of the Weil conjectures)**.** *Suppose that X is a smooth, geometrically irreducible, projective curve over the field $\mathbb{F}_p$, and let g be the genus of X. The zeta function $\zeta(X,t)$ of X is, by definition,*

$$\zeta(X,t) := \exp\Big(\sum_{m=1}^{\infty} \#X(\mathbb{F}_{p^m})\frac{t^m}{m}\Big).$$

Then $\zeta(X,t)$ is a rational function and can be written as

$$\zeta(X,t) = \frac{P(t)}{(1-t)(1-pt)},$$

where $P(t) \in \mathbb{Z}[t]$ has degree $2g$ and factors as

$$P(t) = \prod_{i=1}^{2g}(1-\alpha_i t) \qquad \textit{with} \qquad |\alpha_i| = \sqrt{p}.$$

Now we are ready to prove Theorem 0.2.

of Theorem 0.2.

- **Step 1:** *There are at most $3q$ points of $X = V_+(X^q + Y^q - Z^q) \subseteq \mathbb{P}^2_{\mathbb{F}_p}$ such that at least one among the coordinates x, y, z vanishes.*

  Proof: Consider the line $z = 0$. On this line, the equation becomes $X^q + Y^q = 0$, which is a homogeneous equation of degree q on $\mathbb{P}^1$, hence it has at most q solutions over any field. Repeating the same argument for the lines $x = 0$ and $y = 0$ gives the claim.

- **Step 2:** *X is a smooth, geometrically irreducible, projective curve of genus $g = \frac{(q-1)(q-2)}{2}$.*

  Proof: X is projective by construction. It is smooth because $p \neq q$: if $F := X^q + Y^q - Z^q$, then

  $$\frac{\partial F}{\partial X} = qX^{q-1}, \qquad \frac{\partial F}{\partial Y} = qY^{q-1}, \qquad \frac{\partial F}{\partial Z} = -qZ^{q-1},$$

  and since $q \not\equiv 0 \pmod p$, these three partial derivatives cannot vanish simultaneously at any point of $\mathbb{P}^2$.

We now prove that X is geometrically irreducible. This means that

$$X \times_{\mathrm{Spec}(\mathbb{F}_p)} \mathrm{Spec}(\bar{\mathbb{F}}_p)$$

(where $\bar{\mathbb{F}}_p$ is an algebraic closure) is an irreducible topological space. If it were reducible, then F would factor in $\bar{\mathbb{F}}_p[X,Y,Z]$ as a product $F = GH$ with $\deg(G), \deg(H) > 0$. By Bézout's theorem we get that $V_+(G) \cap V_+(H) \neq \emptyset$. Pick $P \in V_+(G) \cap V_+(H)$. Then, for every $W \in \{X, Y, Z\}$,

$$\frac{\partial F}{\partial W} = G\frac{\partial H}{\partial W} + H\frac{\partial G}{\partial W},$$

so all partial derivatives of F vanish at P, contradicting smoothness.

Finally, since X is a smooth plane curve of degree q, its genus is $g = \frac{(q-1)(q-2)}{2}$ (by genus-degree formula)

- **Step 3:** *Apply Theorem 0.1.*

  From

  $$\zeta(X,t) = \exp\Big(\sum_{m=1}^{\infty} \#X(\mathbb{F}_{p^m})\frac{t^m}{m}\Big)$$

  we get

  $$\#X(\mathbb{F}_p) = \Big(\frac{\mathrm{d}}{\mathrm{d}t}\log(\zeta(X,t))\Big)\Big|_{t=0}.$$

  Using

  $$\zeta(X,t) = \frac{P(t)}{(1-t)(1-pt)} \quad \text{and} \quad P(t) = \prod_{i=1}^{2g}(1-\alpha_i t),$$

  we obtain

  $$\#X(\mathbb{F}_p) = p + 1 - \sum_{i=1}^{2g}\alpha_i.$$

  Since $|\alpha_i| = \sqrt{p}$ for all i, we deduce the bound

  $$\#X(\mathbb{F}_p) \geq p + 1 - 2g\sqrt{p} = p + 1 - (q-1)(q-2)\sqrt{p}.$$

  Hence, for p large enough (for example, for $p > (q^2+3q)^2$), we have $\#X(\mathbb{F}_p) > 3q$. By Step 1, this implies that there must be a point $[x:y:z] \in X(\mathbb{F}_p)$ with $xyz \neq 0$, i.e. a non-trivial solution modulo p.

$\square$

Extending to p-adic solutions

We can extend the theorem thanks to Hensel's lemma. In particular, we can say the following.

Theorem 0.2 (Extension of Theorem 0.2)**.** *There exists an integer $N \geq q$ such that for every prime $p > N$, the Fermat equation has a non-trivial solution in $\mathbb{Z}_p$ (the p-adics).*

From Theorem 0.2 we get, in particular, a non-trivial solution in every $\mathbb{Z}/p^r\mathbb{Z}$ for every $r \geq 1$ and for every prime $p > N$.

Since we can factorize every integer as a product of primes, this tells us that if m is an integer whose prime divisors are all $> N$, then $x^q + y^q = z^q$ has a non-trivial solution in $\mathbb{Z}/m\mathbb{Z}$.

of Theorem 0.2. Fix a prime $p > N$. From Theorem 0.2 we know that there is a solution $(\bar{a}, \bar{b}, \bar{c}) \in (\mathbb{F}_p^\times)^3$ such that

$$\bar{a}^q + \bar{b}^q = \bar{c}^q \quad \text{in } \mathbb{F}_p.$$

Choose lifts $a, b, c_0 \in \mathbb{Z}_p^\times$ such that $a \equiv \bar{a}$, $b \equiv \bar{b}$, $c_0 \equiv \bar{c} \pmod{p}$. Define the polynomial $g(T) := a^q + b^q - T^q \in \mathbb{Z}_p[T]$.

Then

- $g(c_0) \equiv 0 \pmod{p}$;
- $g'(T) = -qT^{q-1}$, so $g'(c_0) \equiv -q\bar{c}^{q-1} \not\equiv 0 \pmod{p}$ (since $p \neq q$ and $\bar{c} \neq 0$).

By Hensel's lemma there is a unique $c \in \mathbb{Z}_p$ such that $c \equiv c_0 \pmod{p}$ and such that c is a root of g in $\mathbb{Z}_p$. In particular,

$$a^q + b^q = c^q \quad \text{in } \mathbb{Z}_p,$$

so $(a, b, c) \in (\mathbb{Z}_p^\times)^3$ is a non-trivial p-adic solution. □

Conclusion

The key point is that reducing Fermat's equation modulo primes is simply too weak to rule out integer solutions. In fact, for a fixed odd prime exponent q, the Fermat curve

$$X: \; X^q + Y^q = Z^q$$

has $\mathbb{F}_p$-points with all coordinates nonzero for every sufficiently large prime p.

Moreover, Hensel's lemma shows that these solutions often lift to $\mathbb{Z}_p$, and hence to solutions modulo p^r for all $r \geq 1$.

This helps explain why Fermat's marginal claim is implausible: any proof of Fermat's Last Theorem must use information that cannot be recovered by congruences modulo primes.

Dickinson, L. J. 1938. *History of the Theory of Numbers.* New York: Chelsea Publishing Company.