The Generalized Fermat Equation

Albert Lopez Bruch

17 October, 2024

Introduction – Pythagorean Triples

Initial question: Which right triangles have integer-valued sides? Eight centuries after Pythagoras, Diophantus first phrased this question as solutions to the equation

$$x^2 + y^2 = z^2, \quad \text{with } x, y, z \in \mathbb{N} \text{ and } \gcd(x, y, z) = 1. \tag{1}$$

Theorem (Diophantus, 3rd C.)

The solutions to (1) *are given by*

$$\{x, y\} = \{2mn, m^2 - n^2\}, \quad z = m^2 + n^2,$$

where $m \geq n$ are positive integers.

Proof.

One factorizes $z^2 = (x + iy)(x - iy)$ and observes that $\gcd(x + iy, x - iy) = 1$. Since $\mathbb{Z}[i]$ is a UFD, $x + iy = u(m + in)^2$, where $u \in \{\pm 1, \pm i\}$ is a unit in $\mathbb{Z}[i]$ and $m, n \in \mathbb{Z}$. $\square$

Introduction – The Fermat Equation

Diophantus' work was lost for centuries, and it wasn't until 1634 when Fermat conjectured that the equation

$$x^n + y^n = z^n, \quad \text{with } x, y, z \in \mathbb{N} \text{ and } \gcd(x, y, z) = 1. \qquad (2)$$

has no solutions for $n \geq 2$, known as Fermat's Last Theorem (FLT). This statement evaded mathematicians for 3 centuries and sparked enormous development. Attempts included

- Infinite descent.
- Understanding of cyclotomic fields.
- Analytic methods.
- Modularity and Galois representations.

Theorem (Wiles, 1994)

The only integer solutions to (2) satisfy $xyz = 0$.

The Generalized Fermat Equation

Even before Wiles' proof, various authors had studied equations of the shape

$$Ax^p + By^q = Cz^r, \quad \text{for fixed } A, B, C.$$

Today we focus on the equation

$$x^p + y^q = z^r, \quad \text{with } x, y, z \in \mathbb{N} \text{ and } \gcd(x, y, z) = 1. \tag{3}$$

Let $\sigma(p, q, r) = 1/p + 1/q + 1/r$ be the signature of (3), and one distinguishes the cases:

1. Spherical case if $\sigma(p, q, r) > 1$.
2. Parabolic case if $\sigma(p, q, r) = 1$.
3. Hyperbolic case if $\sigma(p, q, r) < 1$.

Spherical Case

In this case, if $\sigma(p,q,r) > 1$, then (p,q,r) is one of $(2,2,r)$, $(2,q,2)$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ or $(2,4,3)$.

Theorem

If $\sigma(p,q,r) > 1$, then

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

has infinitely many solutions, and they come in finitely many two-parameter families.

The proof is purely elementary, relying heavily on the parametrization of pythagorean-related equations.

Spherical Case

Example

The solutions to $x^2 + y^4 = z^3$ come in four families, one of which is

$$\begin{cases} x = 4ts(s^2 - 3t^2)(s^4 + 6t^2s^2 + 81t^4)(3s^4 + 2t^2s^2 + 3t^4), \\ y = \pm(s^2 + 3t^2)(s^4 - 18t^2s^2 + 9t^4), \\ z = (s^4 - 2t^2s^2 + 9t^4)(s^4 + 30t^2s^2 + 9t^4) \end{cases}$$

where $\gcd(s, t) = 1$, $s \not\equiv t \pmod 2$ and $3 \nmid s$.

Example

The solutions to $x^2 + y^3 = z^5$ come in 27 distinct families.

Parabolic Case

If $\sigma(p,q,r) = 1$, then

$$(p,q,r) = (2,3,6),\ (2,4,4),\ (2,6,3),\ (3,3,3) \text{ or } (4,4,2).$$

Fermat: $(4,4,2)$ case.

Suppose that $x^4 + y^4 = z^2$ is a non-trivial solution with x odd and minimal z. Then

$$x^2 = m^2 - n^2, \quad y^2 = 2mn, \quad z = m^2 + n^2,$$

and since (x,n,m) is also a pythagorean triple,

$$x = r^2 - s^2, \quad n = 2rs, \quad m = r^2 + s^2$$

for coprime r, s, also pairwise coprime with m. From $y^2 = 4mrs$, we obtain that $r = a^2$, $s = b^2$, $m = c^2$ giving $a^4 + b^4 = c^2$, a contradiction. $\square$

Parabolic Case

The parabolic case is completely solved.

Theorem

The only primitive non-trivial solution of the parabolic case comes from the signature $(p, q, r) = (2, 3, 6)$ *and corresponds to the solution* $3^2 = 2^3 + 1$.

Each equation corresponds to an elliptic curve over $\mathbb{Q}$ of rank 0.

Example (Signature (3, 3, 3))

The equation $x^3 + y^3 = z^3$ can be transformed to $E : Y^2 = X^3 - 432$. One can then show that

$$E(\mathbb{Q}) = \{\mathcal{O}, (36, 12), (36, -12)\} \cong \mathbb{Z}/3\mathbb{Z},$$

giving the trivial solutions $[1 : -1 : 0], [1 : 0 : 1], [0 : 1 : 1]$.

Parabolic Case

Example (Signatures $(2,3,6)$ and $(2,6,3)$)

The equation $x^3 \pm y^6 = z^2$ can be transformed to

$$E^{\pm} : Y^2 = X^3 \pm 1.$$

One then shows that $E^{-}(\mathbb{Q}) = \{\mathcal{O}, (1,0)\} \cong \mathbb{Z}/2\mathbb{Z}$, while

$$E^{+}(\mathbb{Q}) = \{\mathcal{O}, (-1,0), (0,\pm 1), (2,\pm 3)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

The points $(2,\pm 3)$ give rise to the unique solutions $(x,y,z) = (2,\pm 1,\pm 3)$.

Hyperbolic Case

From now on, we consider the *hyperbolic* case $\sigma(p, q, r) < 1$.
Currently, we know the solutions $1^p + 2^3 = 3^2$ and

$$2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2,$$
$$17^7 + 76271^3 = 21063928^2, \; 1414^3 + 2213459^2 = 65^7, \; 9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2 \quad \text{and} \quad 33^8 + 1549034^2 = 15613^3.$$

Conjecture (Beal, 1993)

There are no non-trivial solutions of $x^p + y^q = z^r$ if $1/p + 1/q + 1/r < 1$ and $\min\{p, q, r\} \geq 3$.

A prize of one million dollars is awarded for the solution!
To analyze the progress on this conjecture, we need to look to the cyclotomic and modular approach to FLT.

Hyperbolic Case

Theorem (Darmon, Granville, 1995)

If A, B, C, p, q, r are fixed positive integers with $1/p + 1/q + 1/r < 1$, then the equation

$$Ax^p + By^q = Cz^r$$

has finitely many solutions in coprime non-zero integers x, y, z.

Proof sketch.

One uses $1/p + 1/q + 1/r < 1$ to show the existence of a cover $\phi : D \to \mathbb{P}^1$ such that D has genus ≥ 2 and

- It is only ramified above $0, 1, \infty$.
- All ram degrees above $0, 1, \infty$ divide p, q, r respectively.

If (x, y, z) is a solution, $\phi^{-1}(Ax^p/Cz^q)$ is defined over a number field K unramified away from $2ABCpqr$. Now apply Hermite and Falting's theorem. $\square$

Fermat-Catalan Equation and Cyclotomic Approach

We now consider the Fermat-Catalan equation

$$x^p + y^p = z^q, \quad \text{with } x, y, z \in \mathbb{N} \text{ and } \gcd(x, y, z) = 1.$$

We may assume that p and q are prime, and we consider:

1. FLT(p, q)1 if $p \nmid xyz$. Then
$$z^q = (x + y) \prod_{c=1}^{p-1} (x + y\zeta_p^c)$$
2. FLT(p, q)2 if $p \mid xyz$. Then, if $p \mid z$,
$$z^q = p(x + y) \prod_{c=1}^{p-1} \left(\frac{x + y\zeta_p^c}{1 - \zeta_p} \right)$$

Fermat-Catalan Equation and Cyclotomic Approach

1. FLT(p,q)1 if $p \mid xyz$. Then

$$z^q = (x+y)\prod_{c=1}^{p-1}(x + y\zeta_p^c)$$

2. FLT(p,q)2 if $p \mid xyz$. Then, if $p \nmid z$,

$$z^q = p(x+y)\prod_{c=1}^{p-1}\left(\frac{x+y\zeta_p^c}{1-\zeta_p}\right)$$

If $K = \mathbb{Q}(\zeta_p)$, then $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ and $\alpha = \frac{x+y\zeta_p}{(1-\zeta_p)^e}$ satisfies

$$(\alpha) = \mathfrak{A}^q \quad \text{and} \quad N_{K/\mathbb{Q}}(\alpha) = \frac{z^q}{p^e(x+y)} \tag{4}$$

where $\mathfrak{A}$ is an ideal of K.

Arithmetic understanding of $\mathbb{Q}(\zeta_p)$ together with analytic methods has given remarkable progress.

Theorem (Kummer)

FLT holds for regular primes (i.e primes p such that $p \nmid \mathrm{Cl}(\mathbb{Q}(\zeta_p))$)

Theorem (Granville, Monagan)

If FLT1 has a non-trivial solution, then

$$a^{p-1} \equiv 1 \pmod{p^2} \quad \textit{for } a \in \{2, 3, \ldots, 89\}$$

Corollary: FLT1 has no solutions for $p < 714,591,416,091,389$

Theorem (Mihailescu, 2001)

The only non-trivial solution of the Catalan equation

$$x^p - y^q = 1$$

comes from $3^2 - 2^3 = 1$.

Fermat's Last Theorem

To prove more results about Beal's conjecture, one looks at the main ideas leading to the proof of FLT. Here are the main pillars:

1. Mazur's Theorem on irreducibility of Galois representations of elliptic curves;
2. The modularity theorem, due to Wiles, Breuil, Conrad, Diamond and Taylor;
3. Ribet's level lowering theorem.

Galois Representations

Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime. Since the p-torsion satisfies $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$ and has algebraic coordinates, we has a mod p Galois representation

$$\bar{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Theorem (Mazur, 1978)

- *Let E be an elliptic curve over $\mathbb{Q}$ and $p > 163$ a prime. Then $\bar{\rho}_{E,p}$ is irreducible.*
- *Let E be an elliptic curve over $\mathbb{Q}$ with $E[2] \subseteq E(\mathbb{Q})$ and $p \geq 5$ a prime. Then $\bar{\rho}_{E,\rho}$ is irreducible.*

Mazur's Theorem is equivalent to the statement that any elliptic curve over $\mathbb{Q}$ has no p-isogenies for $p > 163$.

The Modularity Theorem

Let $S_2(N)$ be the space of weight $k = 2$ and level N cusp forms. There is a family of commuting operators

$$T_n : S_2(N) \longrightarrow S_2(N),$$

An eigenform f is a simultaneous eigenvalue for all T_n, and it is normalized if $c_1 = 1$.

Theorem (The Modularity Theorem)

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. There exists a normalized eigenform $f = q + \sum c_n q^n$ of weight 2 and level N such that $c_n \in \mathbb{Z}$, and if $p \nmid \Delta_E$ is prime then $c_p = a_p(E) = p + 1 - |\tilde{E}(\mathbb{F}_p)|$.

Ribet's Level Lowering Theorem

Given an eigenform $f \in S_2(N)$ and a prime p, we can associate

$$\bar{\rho}_{f,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{p^r}),$$

where $r \geq 1$ depends on f (and $r = 1$ if and only if all $c_n \in \mathbb{Z}$).
Fact: $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,p}$ if E corresponds to f.

Theorem (Ribet's Level Lowering Theorem, 1986)

Let E be an elliptic curve over $\mathbb{Q}$ with minimal discriminant Δ and conductor N and let $p \geq 3$ be prime. Suppose

- *the curve E is modular;*
- *the mod p representation $\bar{\rho}_{E,p}$ is irreducible*

Let

$$N_p = N \Big/ \prod_{\substack{\ell \mid N \\ p \mid \mathrm{ord}_\ell(\Delta)}} \ell.$$

Then $\bar{\rho}_{E,p} \sim \bar{\rho}_{g,p}$ for some eigenform g of weight 2 and level N_p.

Proof of Fermat's Last Theorem

Suppose that (x, y, z) is a non-trivial solution of $x^p + y^p = z^p$ for $p \geq 5$. Reorder them so that y is even and $x^p \equiv -1 \pmod 4$. Define the **Frey—Hellegouarch curve**

$$E : Y^2 = X(X - x^p)(X + y^p)$$

with

$$\Delta = x^{2p}y^{2p}z^{2p}2^{-8} \quad \text{and} \quad N = \prod_{\ell \mid \Delta} \ell.$$

We have that E is modular and since $E[2] \subseteq E(\mathbb{Q})$ and $p \geq 5$, the representation $\bar{\rho}_{E,p}$ is irreducible. So Ribet's Theorem applies and $N_p = 2$. This predicts the existence of some eigenform $g \in S_2(2)$. However, $\dim S_2(2) = g(X_0(2)) = 0$, so no non-trivial solution can exist. $\square$

How much do we know?

(p, q, r)	Reference(s)
(n, n, n)	Wiles, Taylor-Wiles
$(n, n, k), k \in \{2, 3\}$	Darmon-Merel, Poonen
$(2n, 2n, 5)$	Bennett
$(2, 4, n)$	Ellenberg, Bennett-Ellenberg-Ng, Bruin
$(2, 6, n)$	Bennett-Chen, Bruin
$(2, n, 4)$	Bennett-Skinner, Bruin
$(2, n, 6)$	Bennett-Chen-Dahmen-Yazdani
$(3j, 3k, n),\ j, k \geq 2$	Immediate from Kraus
$(3, 3, 2n)$	Bennett-Chen-Dahmen-Yazdani
$(3, 6, n)$	Bennett-Chen-Dahmen-Yazdani
$(2, 2n, k),\ k \in \{9, 10, 15\}$	Bennett-Chen-Dahmen-Yazdani
$(4, 2n, 3)$	Bennett-Chen-Dahmen-Yazdani
$(2j, 2k, n),\ j, k \geq 5$prime,$n \in \{3, 5, 7, 11, 13\}$	Anni-Siksek
$(2, 3, n),\ n \in \{6, 7, 8, 9, 10, 15\}$	Poonen-Schaefer-Stoll, Bruin, Zureick-Brown, Siksek, Siksek-Stoll
$(3, 4, 5)$	Siksek-Stoll
$(5, 5, 7),\ (7, 7, 5)$	Dahmen-Siksek

How much do we know?

Essentially two methods of proof:

- For some fixed triples, the problem is reduced to finding $\mathbb{Q}$-rational points on curves of genus ≥ 2.
- Using *Frey—Hellegouarch curves* associated to (p, q, r): elliptic curves $E/\mathbb{Q}$ attached to a solution such that
  1. $\Delta = A \cdot B^p$ where A is a known small integer;
  2. every prime $p \mid B$ divides the conductor exactly once.

Equation	Frey–Hellegouarch Curve
$a^p + b^p = c^2$	$Y^2 = X^3 + 2cX^2 + a^pX$
$a^p + b^p = c^3$	$Y^2 = X^3 + 3cX^2 - 4b^p$
$a^3 + b^3 = c^p$	$Y^2 = X^3 + 3(a-b)X^2 + 3(a^2 - ab + b^2)X$
$a^2 + b^3 = c^p$	$Y^2 = X^3 + 3bX + 2a$

Thank you for listening!