**Fermat’s Last Theorem**

**Early History**

**The Babylonians** (1800-1650 B.C.)
- tables for the case $n = 2$; general formula?

**Pythagoras, Plato** (ca. 550 B.C., ca. 400 B.C.)
- general formula for the case $n = 2$

**Diophantus of Alexandria** (ca. 250 A.D.)
- wrote the *Arithmetica* (13 books, 9 survived)

**Pierre de Fermat** (1601 - 1665)
- formulated FLT, proved the case $n = 4$

**Leonard Euler** (1707 - 1783)
- the case $n = 3$ (1753)

**Carl Friederich Gauss** (1777 - 1855)
- filled in ”details” (gap) in Euler’s proof

**Gabriel Lame** (1795 - 1870)
- the case $n = 5$ (1839);
- attempted a general proof using $\mathbb{Z}[\zeta]$ (1847)

**Peter Gustav Lejeune-Dirichlet** (1805 - 1859)
- the cases $n = 7$ (1828) and $n = 14$ (1832)

**Ernst Edward Kummer** (1810 - 1893)
- $\text{FLT}_p$ is true for all regular primes $p$ (1847/50)
- criterion for determining regular primes (1851);
- in particular, he found (1874) that of the 37 primes $p < 163$, only 8 are irregular (= not regular):
  $37, 59, 67, 101, 103, 131, 149, 157$
  $\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots$  

**1976**: $\text{FLT}_n$ is true for $n < 125,000$ (S. Wagstaff + computer)
2. Observatio Domini Petri de Fermat

Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ulta quadratum postestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane dexteri. Hanc marginis exiguitas non caperet.

On the other hand it is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or generally any power except a square into two powers with the same exponent. I have discovered a truly marvellous proof of this, which however the margin is not large enough to contain.

[Translation: T. Heath]
3. A Basic Principle

**Problem:** Find all the integer solutions \((x, y, z) \in \mathbb{Z}^3\) of the Diophantine equation

\[
F(x, y, z) = 0,
\]

where \(F \in \mathbb{Z}[x, y, z]\) is an integral polynomial.

**Examples:** 1) Fermat polynomial:

\[
F(x, y, z) = F_n(x, y, z) = x^n + y^n - z^n.
\]

2) Elliptic curve:

\[
F(x, y, z) = F_{a,b}(x, y, z) = y^2z - x^3 + axz^2 + bz^3,
\]

where \(a, b \in \mathbb{Z}\) and \(\Delta(F_{a,b}) = 16(4a^3 + 27b^3) \neq 0\).

**Easier Problem:** For each prime number \(p\), solve the congruence

\[
(2) \quad F(x, y, z) \equiv 0 \pmod{p};
\]

this is a finite problem (for each \(p\)), for we need to check only \(p^3\) values. In particular, the number of solutions

\[
N_p^*(F) = \#\{(x, y, z) \in (\mathbb{Z}/p\mathbb{Z})^3 : F(x, y, z) \equiv 0 \pmod{p}\} \\
= \#\{(x, y, z) \in \mathbb{Z}^3 : 0 \leq x, y, z < p \text{ and } p | F(x, y, z)\} \\
\leq p^3 < \infty.
\]

Put: \(N_p(F) = (N_p^*(F) - 1)/(p - 1)\)

= \# of essentially distinct solutions of \((2)\).

**Question:** Do these numbers shed any light on the solutions of \((1)\)?
Basic (Conjectural) Principle: the sequence of numbers

\[ a_p(F) \overset{def}{=} (p + 1) - N_p(F), \quad \text{as } p \to \infty, \]

should determine the nature of the solutions of (1).

For elliptic curves, this principle assumes the form of two very precise conjectures which have been partly verified:

(TWS)–Conjecture: - due to Y. Taniyama (1955), A. Weil (1967), and G. Shimura (1971)

(B/SwD)–Conjecture: - B. Birch, H.P.F. Swinnerton–Dyer (1960’s)

Theorem 1 (Kolyvagin(1988), Murty–Murty(1991)) Let

\[ E : F_{a,b}(x, y, z) = 0 \]

be an elliptic curve satisfying (TWS). Then the sequence \( a_p(E) = p + 1 - N_p(F_{a,b}) \), \( p \to \infty \), determines a (“computable”) constant \( L_E(1) \in \mathbb{R} \). If

\[ L_E(1) \neq 0, \]

then the equation \( F_{a,b}(x, y, z) = 0 \) has only finitely many integral solutions \( (x, y, z) \in \mathbb{Z}^3 \) with \( \gcd(x, y, z) = 1 \), and these can be explicitly calculated.

Note. The above theorem constitutes an explicit algorithm which has been implemented on a MAPLE package called APECS.

Example (Frey). The above leads to a computer proof (a true proof!) of FLT\(_3\) and FLT\(_4\), using only four short computer commands.
4. The TWS–Conjecture

To state this conjecture, we need two concepts:

1) The conductor $N = N_E$ of an elliptic curve $E$: this is a positive integer

$$N \mid \Delta_{a,b}$$

which is closely related to $\Delta_{a,b}$ (and is explicitly computable).

2) The space $S(N) = S_2(\Gamma_0(N))$ of modular forms of level $N$: this consists of (complex-valued) functions of the form

$$f(z) = \sum_{n=1}^{\infty} a_n(f) q^n, \quad \text{with } q = e^{2\pi i z},$$

where the $a_n(f) \in \mathbb{C}$ and the sum converges for $\Im(z) > 0$; these are to satisfy certain additional properties such as the rule

$$f \left( \frac{az + b}{cz + d} \right) = (cz + d)^2 f(z),$$

where $a, b, c, d \in \mathbb{Z}$ are any integers with $ad - bc = 1$ and $N|c$.

**Properties:**

1) $S(N)$ is a finite-dimensional $\mathbb{C}$-vector space of dimension $g_N := \dim_{\mathbb{C}} S(N) \approx \frac{N}{12}$.

2) Each $f \in S(N)$ is uniquely described by its first $2g_N \approx \frac{N}{6}$ Fourier coefficients $a_1(f), \ldots, a_{2g_N}(f)$.

3) $S(N)$ has a distinguished $\mathbb{C}$-basis $H(N) = H^+(N) \cup H^-(N)$. The functions in $H^+(N)$ are called newforms, those in $H^-(N)$ oldforms. For each $N$, these forms are explicitly computable (and have been computed for $N \leq 10^6$).
**Conjecture (TWS):** For every elliptic curve $E$ of conductor $N$, there is a (unique) newform $f(z) = \sum a_n(f)q^n \in H^+(N)$ of level $N$ such that

$$a_p(E) = a_p(f), \quad \text{for all primes } p \nmid N.$$  

**Theorem (Shimura, 1971).** For each $f \in H^+(N)$ with integral Fourier coefficients there is an elliptic curve $E$ (of conductor $N$) such that (4) holds.

**Theorem (Wiles, 1995).** Conjecture (TWS) is true if $N_E$ is squarefree.
5. **TWS\textsubscript{ss} \Rightarrow \text{FLT}**

Suppose \( \text{FLT}_p \) is false: there exist \( a, b, c \in \mathbb{Z} \) with \( abc \neq 0 \) such that

\[
a^p + b^p = c^p.
\]

We may suppose (w.l.o.g.) that \( 2|a \) and that \( p \geq 5 \). Consider the elliptic curve

\[
y^2z = x(x - a^pz)(x + b^pz),
\]

called a *Frey curve*. Then:

1) \( \Delta = (abc)^{2p} \)

2) \( N_E \) is squarefree (since \( 16|a^p \)).

Thus, by Wiles’s theorem, there is an \( f = f_E \in H^+(N_E) \) such that (4) holds.

**Claim:** Such an \( f_E \) does not exist!

**Theorem ("Lowering the Level" - Ribet, 1991)**

*Suppose \( f = f_E \in H^+(N) \) is a newform of level \( N \). For a fixed prime number \( p > 3 \) let \( M_p \) denote the product of the prime numbers \( q > 2 \) such that \( p|\text{expt}_q(\Delta_E) \). Then there exists \( g \in H^+(N/M_p) \) such that*

\[
a_n(g) \equiv a_n(f) \pmod{p}, \quad \text{for all } n \geq 1 \text{ with } \gcd(n, N) = 1.
\]

**Conclusion.** Apply this to \( f_E \) as above. Then by 1) we obtain that \( M_p = \frac{N}{2} \), so by Ribet’s theorem there is a newform \( g \in H^+(2) \). But this is impossible since \( \dim S(2) = 0 \).