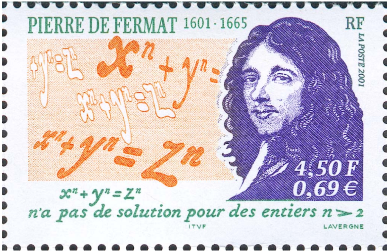
Fermat's Last Theorem: A very brief outline of its proof

Karl Dilcher

Supplementary class to MATH 4070/5070

November 30, 2018



“I have discovered a truly marvelous proof that it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. This margin is too narrow to contain it."

– Fermat

teruallo quadratorum, & Canones iidem hîc etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 - 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quot continet latus ipsius 16. esto à 2 N. - 4. ipse igitur quadratus erit 4 Q. + 16. - 16 N. hæc æquabuntur vnitatibus 16 - 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$. & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ις διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ςς. ὅσων δή ποτε λείψει τοσούτων μο ὅσων ἐστὶν ἡ τῶν ις μο πλευρά. ἔστω ςς β λείψει μο δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μο ις [λείψει ςς ις] ταῦτα ἴσα μονάσι ις λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ις. καὶ γίνεται ὁ ἀριθμὸς ις πέμπτων. ἔσται ὁ μὲν σνς εἰκοστοπέμπτων. ὁ δὲ ρμδ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοστόπεμπτα, ἤτοι μονάδας ις. καὶ ἔστιν ἑκάτερος τετράγωνος.

Fermat's Last Theorem (FLT):
Given an integer $n \geq 3$, there are no $a, b, c \in \mathbb{Z}$ such that

$$a^n + b^n = c^n.$$

Fermat's Last Theorem (FLT):
Given an integer $n \geq 3$, there are no $a, b, c \in \mathbb{Z}$ such that

$$a^n + b^n = c^n.$$

Note: It suffices to consider $n = 4$ and $n = p$, an odd prime.

Fermat's Last Theorem (FLT):
Given an integer $n \geq 3$, there are no $a, b, c \in \mathbb{Z}$ such that

$$a^n + b^n = c^n.$$

Note: It suffices to consider $n = 4$ and $n = p$, an odd prime.

1. Some Historical Milestones

(1) Fermat; assertion made around 1637.

Fermat's Last Theorem (FLT):
Given an integer $n \geq 3$, there are no $a, b, c \in \mathbb{Z}$ such that

$$a^n + b^n = c^n.$$

Note: It suffices to consider $n = 4$ and $n = p$, an odd prime.

1. Some Historical Milestones

(1) Fermat; assertion made around 1637.

(2) Early attempts, up to 1847:
$n = 3, 4, 5, 7, 14$; some criteria.

(3) First breakthrough: Kummer’s work, 1844–1850s

(3) First breakthrough: Kummer's work, 1844–1850s

Kummer's Theorem:
$a^p + b^p = c^p$ has no solutions when p is *regular*,
i.e., p does not divide the class number h of the cyclotomic field
$\mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/p}$.

(3) First breakthrough: Kummer's work, 1844–1850s

Kummer's Theorem:
$a^p + b^p = c^p$ has no solutions when p is *regular*,
i.e., p does not divide the class number h of the cyclotomic field $\mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/p}$.

Ernst Eduard Kummer
1810 - 1893

(4) Numerous further results based on Kummer’s work, improved criteria, computations. FLT settled for all

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),
- $p < 2000$ (Vandiver, 1952),

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),
- $p < 2000$ (Vandiver, 1952),
- $p < 125\,000$ (Wagstaff, 1976),

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),
- $p < 2000$ (Vandiver, 1952),
- $p < 125\,000$ (Wagstaff, 1976),
- $p < 4\,000\,000$ (Buhler et al., 1993).

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),
- $p < 2000$ (Vandiver, 1952),
- $p < 125\,000$ (Wagstaff, 1976),
- $p < 4\,000\,000$ (Buhler et al., 1993).

(5) Second breakthrough:
Mordell's conjecture proved by Faltings, 1983.

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),
- $p < 2000$ (Vandiver, 1952),
- $p < 125\,000$ (Wagstaff, 1976),
- $p < 4\,000\,000$ (Buhler et al., 1993).

(5) Second breakthrough:
Mordell's conjecture proved by Faltings, 1983.
Consequence:
Fermat's equation has at most finitely many solutions.

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),
- $p < 2000$ (Vandiver, 1952),
- $p < 125\,000$ (Wagstaff, 1976),
- $p < 4\,000\,000$ (Buhler et al., 1993).

(5) Second breakthrough:
Mordell's conjecture proved by Faltings, 1983.
Consequence:
Fermat's equation has at most finitely many solutions.

(6) Final breakthrough:
Wiles, 1993 and Taylor & Wiles, 1994.

(4) Numerous further results based on Kummer's work, improved criteria, computations. FLT settled for all

- $p < 100$ (Kummer, 1850s),
- $p < 2000$ (Vandiver, 1952),
- $p < 125\,000$ (Wagstaff, 1976),
- $p < 4\,000\,000$ (Buhler et al., 1993).

(5) Second breakthrough:
Mordell's conjecture proved by Faltings, 1983.
Consequence:
Fermat's equation has at most finitely many solutions.

(6) Final breakthrough:
Wiles, 1993 and Taylor & Wiles, 1994.

(7) Further developments, refinements, extensions.

After this very brief outline, back to the 3 breakthrough result.

After this very brief outline, back to the 3 breakthrough result.

Kummer's Theorem:

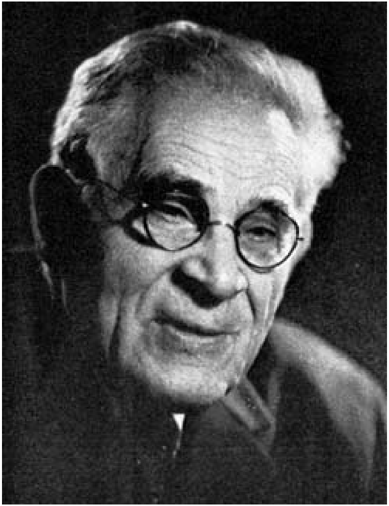
That's what MATH 4070/5070 was all about.

After this very brief outline, back to the 3 breakthrough result.

Kummer's Theorem:

That's what MATH 4070/5070 was all about.

So, let's have a brief look at Mordell's Conjecture.



Louis Joel Mordell
1888 - 1972

In 1953 Mordell retired from the Sadleirian Chair but he most certainly did not retire from mathematics; **almost half** of Mordell's 270 publications appeared **after his retirement**. Nor did retirement mean that he lived a quiet life at his home in Cambridge. On the contrary he delighted in accepting appointments as Visiting Professor (in places such as Toronto, Ghana, Nigeria, **Mount Allison**, Colorado, Notre Dame and Arizona), delighted in adding yet another university to the list of places at which he had been invited to speak (with a final total of around 190), and delighted in sharing his enjoyment of mathematics with as many young people as he could.

– http://www-history.mcs.st-and.ac.uk/

2. Mordell's Conjecture

2. Mordell's Conjecture

Genus of a surface:

Roughly speaking, the number of "holes" or "handles".

- Sphere: genus 0;
- torus: genus 1.

2. Mordell's Conjecture

Genus of a surface:
Roughly speaking, the number of “holes" or “handles".
• Sphere: genus 0;
• torus: genus 1.

Connection with Fermat:
Rewrite $a^n + b^n = c^n$ as

2. Mordell's Conjecture

Genus of a surface:
Roughly speaking, the number of “holes" or “handles".
• Sphere: genus 0;
• torus: genus 1.

Connection with Fermat:
Rewrite $a^n + b^n = c^n$ as

$$x^n + y^n - 1 = 0.$$

Does it have *rational* solutions?

L. J. Mordell's idea:
Given a polynomial equation $Q(x, y) = 0$,
look at all its *complex* solutions.

This is related to a surface (a “compact Riemann surface"), so the genus makes sense, and will be called the “genus of the algebraic curve" defined by $Q(x, y) = 0$.

This is related to a surface (a “compact Riemann surface"), so the genus makes sense, and will be called the “genus of the algebraic curve" defined by $Q(x, y) = 0$.

Mordell’s Conjecture (1922; Faltings, 1983):
A polynomial equation $Q(x, y) = 0$ with rational coefficients and genus $g \geq 2$ has only finitely many solutions.

This is related to a surface (a “compact Riemann surface"), so the genus makes sense, and will be called the “genus of the algebraic curve" defined by $Q(x, y) = 0$.

Mordell’s Conjecture (1922; Faltings, 1983):
A polynomial equation $Q(x, y) = 0$ with rational coefficients and genus $g \geq 2$ has only finitely many solutions.

The genus of the curve

$$x^n + y^n - 1 = 0$$

is $(n-1)(n-2)/2$, which is ≥ 2 for $n \geq 4$.

This is related to a surface (a “compact Riemann surface"), so the genus makes sense, and will be called the “genus of the algebraic curve" defined by $Q(x, y) = 0$.

Mordell’s Conjecture (1922; Faltings, 1983):
A polynomial equation $Q(x, y) = 0$ with rational coefficients and genus $g \geq 2$ has only finitely many solutions.

The genus of the curve

$$x^n + y^n - 1 = 0$$

is $(n-1)(n-2)/2$, which is ≥ 2 for $n \geq 4$.

Hence:
Fermat’s equation has at most finitely many solutions for $n \geq 4$.

Gerd Faltings
1954 –

Faltings received the 1986 Fields Medal for this achievement.

Another consequence of Faltings' theorem:

FLT is true for "almost all" n.

Another consequence of Faltings' theorem:

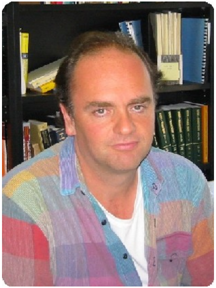
FLT is true for "almost all" n.

In other words, the asymptotic density of the exponents n for which FLT is true is 1.
(A. Granville and R. Heath-Brown, independently, 1985).

Another consequence of Faltings' theorem:

FLT is true for "almost all" n.

In other words, the asymptotic density of the exponents n for which FLT is true is 1.
(A. Granville and R. Heath-Brown, independently, 1985).



3. The Frey Elliptic Curve

Up to the 1980s:
The only successful approach to FLT was via cyclotomic fields.

At that time, however, further progress seemed to be stalling.

3. The Frey Elliptic Curve

Up to the 1980s:
The only successful approach to FLT was via cyclotomic fields.

At that time, however, further progress seemed to be stalling.

Some fundamental new ideas were introduced by
Y. Hellegouarch (1975) and G. Frey (1982).

Idea: Suppose that FLT is false, i.e., suppose there exist nonzero $a, b, c \in \mathbb{Z}$, pairwise coprime, such that

$$a^p + b^p = c^p$$

(p an odd prime).

Idea: Suppose that FLT is false, i.e., suppose there exist nonzero $a, b, c \in \mathbb{Z}$, pairwise coprime, such that

$$a^p + b^p = c^p$$

(p an odd prime).

Then define the “Frey elliptic curve" $\mathcal{F}$ over $\mathbb{Q}$ by

$$y^2 = x(x - a^p)(x + b^p). \tag{1}$$

Idea: Suppose that FLT is false, i.e., suppose there exist nonzero $a, b, c \in \mathbb{Z}$, pairwise coprime, such that

$$a^p + b^p = c^p$$

(p an odd prime).

Then define the “Frey elliptic curve" $\mathcal{F}$ over $\mathbb{Q}$ by

$$y^2 = x(x - a^p)(x + b^p). \tag{1}$$

Since

$$b^p + a^p = c^p \quad \text{and} \quad a^p + (-c)^p = (-b)^p$$

are also solutions, we may as well assume that we have $a \equiv -1 \pmod 4$ and b is even.

Elliptic curves have a number of “invariants"; one of them is the *discriminant*, defined by

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2,$$

where x_1, x_2, x_3 are the roots of the RHS in (1).

Elliptic curves have a number of “invariants"; one of them is the *discriminant*, defined by

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2,$$

where x_1, x_2, x_3 are the roots of the RHS in (1).

With $x_1 = 0$, $x_2 = -a^p$, $x_3 = b^p$, the discriminant is

$$(0 - (-a^p))^2(-a^p - b^p)^2(b^p - 0)^2 = a^{2p}b^{2p}c^{2p},$$

(recall that $a^p + b^p = c^p$.)

Frey remarked that it is very unusual for a discriminant to be a high perfect power.

Frey remarked that it is very unusual for a discriminant to be a high perfect power.

He suggested that it might contradict the “Taniyama-Shimura-Weil" (TSW) Conjecture.

Frey remarked that it is very unusual for a discriminant to be a high perfect power.

He suggested that it might contradict the "Taniyama-Shimura-Weil" (TSW) Conjecture.

K. Ribet proved in 1986 that the TSW conjecture does indeed imply FLT.

Frey remarked that it is very unusual for a discriminant to be a high perfect power.

He suggested that it might contradict the "Taniyama-Shimura-Weil" (TSW) Conjecture.

K. Ribet proved in 1986 that the TSW conjecture does indeed imply FLT.

Wiles picked up on this and set out to prove the TSW conjecture, working in isolation for the following 7 years.

Gerhard Frey
1944–

Ken Ribet
1947–

4. The Main Ingredients

If a prime ℓ divides the discriminant then it divides differences of the roots x_1, x_2, x_3.

So either two or all three roots are congruent mod ℓ.

4. The Main Ingredients

If a prime ℓ divides the discriminant then it divides differences of the roots x_1, x_2, x_3.

So either two or all three roots are congruent mod ℓ.

Definition: The curve is called *semistable* if only 2 roots are congruent mod $\ell > 3$.

4. The Main Ingredients

If a prime ℓ divides the discriminant then it divides differences of the roots x_1, x_2, x_3.

So either two or all three roots are congruent mod ℓ.

Definition: The curve is called *semistable* if only 2 roots are congruent mod $\ell > 3$.

Lemma: Every Frey curve is semistable.

4. The Main Ingredients

If a prime ℓ divides the discriminant then it divides differences of the roots x_1, x_2, x_3.

So either two or all three roots are congruent mod ℓ.

Definition: The curve is called *semistable* if only 2 roots are congruent mod $\ell > 3$.

Lemma: Every Frey curve is semistable.

Proof: If $\ell \mid a^{2p}b^{2p}c^{2p}$, then ℓ divides only one of a^p, b^p, c^p since they are coprime. The result follows from the roots being $0, a^p, -b^p$ (recall $c^p = a^p + b^p$).

Conjecture (Taniyama-Shimura-Weil):
Every elliptic curve over $\mathbb{Q}$ is modular.

Conjecture (Taniyama-Shimura-Weil):
Every elliptic curve over $\mathbb{Q}$ is modular.

Theorem (Wiles): Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Conjecture (Taniyama-Shimura-Weil):
Every elliptic curve over $\mathbb{Q}$ is modular.

Theorem (Wiles): Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Corollary: Every Frey curve is modular.

Conjecture (Taniyama-Shimura-Weil):
Every elliptic curve over $\mathbb{Q}$ is modular.

Theorem (Wiles): Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Corollary: Every Frey curve is modular.

Contradiction: (Ribet)
A Frey curve *cannot* be modular.

Conjecture (Taniyama-Shimura-Weil):
Every elliptic curve over $\mathbb{Q}$ is modular.

Theorem (Wiles): Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Corollary: Every Frey curve is modular.

Contradiction: (Ribet)
A Frey curve *cannot* be modular.

Question: What does “modular" mean??

5. Finite Fields, Projective Plane

Main idea:
Consider elliptic curves not over $\mathbb{Q}$,
but over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, i.e., mod p,
where p is a prime. It can happen that the discriminant is $\neq 0$,
but $\equiv 0 \pmod{p}$.

5. Finite Fields, Projective Plane

Main idea:
Consider elliptic curves not over $\mathbb{Q}$,
but over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, i.e., mod p,
where p is a prime. It can happen that the discriminant is $\neq 0$,
but $\equiv 0 \pmod{p}$.

Example: $y^2 = x^3 - 5$. Discriminant is

$$-10\,800 = -2^4 \cdot 3^3 \cdot 5^2.$$

So it is not an elliptic curve over $\mathbb{F}_p$ for $p = 2, 3, 5$.

5. Finite Fields, Projective Plane

Main idea:
Consider elliptic curves not over $\mathbb{Q}$,
but over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, i.e., mod p,
where p is a prime. It can happen that the discriminant is $\neq 0$,
but $\equiv 0 \pmod{p}$.

Example: $y^2 = x^3 - 5$. Discriminant is

$$-10\,800 = -2^4 \cdot 3^3 \cdot 5^2.$$

So it is not an elliptic curve over $\mathbb{F}_p$ for $p = 2, 3, 5$.

These primes are said to have “bad reduction" and must be avoided.

The primes of bad reduction are multiplied together (with certain exponents) to give the *conductor* N of the curve.

The primes of bad reduction are multiplied together (with certain exponents) to give the *conductor* N of the curve.

Alternative Definition:
A curve is semistable if its conductor is squarefree.

The primes of bad reduction are multiplied together (with certain exponents) to give the *conductor* N of the curve.

Alternative Definition:
A curve is semistable if its conductor is squarefree.

We know: The “point at infinity" plays an important role. To account for this point, we introduce the “projective plane".

The primes of bad reduction are multiplied together (with certain exponents) to give the *conductor* N of the curve.

Alternative Definition:
A curve is semistable if its conductor is squarefree.

We know: The “point at infinity" plays an important role. To account for this point, we introduce the “projective plane".

Roughly speaking: The collection of all points

$$(x, y, z) \in \mathbb{R}^3 \setminus (0, 0, 0),$$
$$(x, y, z) \sim (ax, ay, az).$$

The primes of bad reduction are multiplied together (with certain exponents) to give the *conductor* N of the curve.

Alternative Definition:
A curve is semistable if its conductor is squarefree.

We know: The "point at infinity" plays an important role. To account for this point, we introduce the "projective plane".

Roughly speaking: The collection of all points

$$(x, y, z) \in \mathbb{R}^3 \setminus (0, 0, 0),$$
$$(x, y, z) \sim (ax, ay, az).$$

All "finite points" can be identified with $(x, y, 1)$, and the points at infinity with $(x, y, 0)$.

The primes of bad reduction are multiplied together (with certain exponents) to give the *conductor* N of the curve.

Alternative Definition:
A curve is semistable if its conductor is squarefree.

We know: The “point at infinity" plays an important role. To account for this point, we introduce the “projective plane".

Roughly speaking: The collection of all points

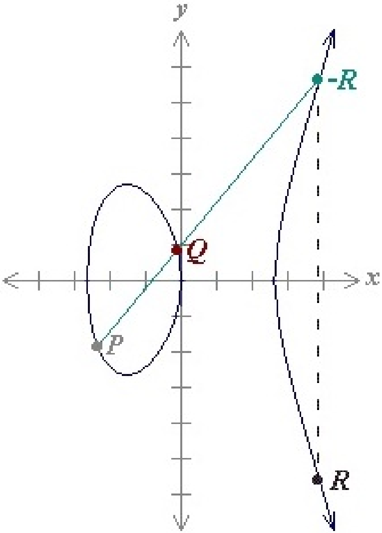
$$(x, y, z) \in \mathbb{R}^3 \setminus (0, 0, 0),$$
$$(x, y, z) \sim (ax, ay, az).$$

All “finite points" can be identified with $(x, y, 1)$, and the points at infinity with $(x, y, 0)$.

The “point at infinity" that serves as identity in the elliptic curve group is then $\mathcal{O} = (0, 1, 0)$.

What is the “elliptic curve group"?

What is the “elliptic curve group"?



$$y^2 = x^3 - 7x$$

We want to count points on a curve over $\mathbb{F}_p$.

We want to count points on a curve over $\mathbb{F}_p$.

First, to put this into perspective, how many points does a line over $\mathbb{F}_p$,

$$ax + by = c,$$

in the projective plane have?

We want to count points on a curve over $\mathbb{F}_p$.

First, to put this into perspective, how many points does a line over $\mathbb{F}_p$,

$$ax + by = c,$$

in the projective plane have?

“Homogenize" by introducing a variable z:

$$ax + by = cz.$$

We want to count points on a curve over $\mathbb{F}_p$.

First, to put this into perspective, how many points does a line over $\mathbb{F}_p$,

$$ax + by = c,$$

in the projective plane have?

"Homogenize" by introducing a variable z:

$$ax + by = cz.$$

When $z = 0$: Given $y = 1$, exactly one x
When $z = 1$: For each y, exactly one x
Total: $p + 1$ solutions.

How about elliptic curves?
What's the number b_p of solutions over $\mathbb{F}_p$?
How much does this value differ from the “standard" $p + 1$?

How about elliptic curves?
What's the number b_p of solutions over $\mathbb{F}_p$?
How much does this value differ from the “standard" $p+1$?
Call the difference a_p. Then

$$b_p = p + 1 - a_p.$$

How about elliptic curves?
What's the number b_p of solutions over $\mathbb{F}_p$?
How much does this value differ from the “standard" $p+1$?
Call the difference a_p. Then

$$b_p = p + 1 - a_p.$$

Example: $y^2 = x^3 + 22$ over $\mathbb{F}_5$.
Homogenize: $y^2 z = x^3 + 22z^3$.
Reduce modulo 5: $y^2 z = x^3 + 2z^3$.
Find solutions (“trial and error"):

How about elliptic curves?
What's the number b_p of solutions over $\mathbb{F}_p$?
How much does this value differ from the "standard" $p+1$?
Call the difference a_p. Then

$$b_p = p + 1 - a_p.$$

Example: $y^2 = x^3 + 22$ over $\mathbb{F}_5$.
Homogenize: $y^2 z = x^3 + 22z^3$.
Reduce modulo 5: $y^2 z = x^3 + 2z^3$.
Find solutions ("trial and error"):

$$(x, y, z) = (0, 1, 0), \qquad \begin{array}{l} (2, 0, 1) \\ (3, 2, 1) \\ (3, 3, 1) \\ (4, 1, 1) \\ (4, 4, 1) \end{array}$$

Hence $b_5 = 6$, and thus $a_5 = 0$.

The surprise now is:
These numbers a_p will appear in a different, seemingly unrelated setting as Fourier coefficients of certain functions.

6. Modular Forms

Recall from complex analysis:

$$g(z) = \frac{az+b}{cz+d}, \qquad ad - bc \neq 0,$$

$(a, b, c, d \in \mathbb{C})$ is called a *Möbius map*.

6. Modular Forms

Recall from complex analysis:

$$g(z) = \frac{az+b}{cz+d}, \qquad ad - bc \neq 0,$$

($a, b, c, d \in \mathbb{C}$) is called a *Möbius map*.
It maps circles on $\mathbb{C} \cup \{\infty\}$ to circles on $\mathbb{C} \cup \{\infty\}$
(this includes straight lines in $\mathbb{C}$)
and is *conformal* (angle-preserving).

6. Modular Forms

Recall from complex analysis:

$$g(z) = \frac{az+b}{cz+d}, \qquad ad - bc \neq 0,$$

($a, b, c, d \in \mathbb{C}$) is called a *Möbius map*.
It maps circles on $\mathbb{C} \cup \{\infty\}$ to circles on $\mathbb{C} \cup \{\infty\}$
(this includes straight lines in $\mathbb{C}$)
and is *conformal* (angle-preserving).

The **modular group** is the group of all Möbius maps

$$g(z) = \frac{az+b}{cz+d},$$

with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

6. Modular Forms

Recall from complex analysis:

$$g(z) = \frac{az+b}{cz+d}, \qquad ad - bc \neq 0,$$

($a, b, c, d \in \mathbb{C}$) is called a *Möbius map*.
It maps circles on $\mathbb{C} \cup \{\infty\}$ to circles on $\mathbb{C} \cup \{\infty\}$
(this includes straight lines in $\mathbb{C}$)
and is *conformal* (angle-preserving).

The **modular group** is the group of all Möbius maps

$$g(z) = \frac{az+b}{cz+d},$$

with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

It maps the upper-half plane
$\mathbb{H} = \{x + iy \mid y > 0\}$ into itself.

The modular group can (basically) be identified with the group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

The modular group can (basically) be identified with the group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Subgroups of these turn out to be more interesting: Define

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

The modular group can (basically) be identified with the group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Subgroups of these turn out to be more interesting: Define

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

We want to consider functions on $\mathbb{H}$ which “transform well" under one of the subgroups $\Gamma_0(N)$. In particular, we require that there be an integer k such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \text{for all} \quad \gamma \in \Gamma_0(N).$$

For $\gamma = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, we have $f(z+1) = f(z)$,
so f must have a Fourier expansion

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

For $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we have $f(z+1) = f(z)$,
so f must have a Fourier expansion

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

If only non-negative powers of q are involved, and a few other technical conditions are satisfied, then this function is called

- a **modular form** of weight k on $\Gamma_0(N)$.
- N is called the *level* of f.

For $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we have $f(z+1) = f(z)$,
so f must have a Fourier expansion

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

If only non-negative powers of q are involved, and a few other technical conditions are satisfied, then this function is called

- a **modular form** of weight k on $\Gamma_0(N)$.
- N is called the *level* of f.

We further specialize the set of modular forms.

There is a family of operators, called “Hecke operators", acting on the space of modular forms of given weight and level. Eigenvectors of Hecke operators are called *eigenforms*.

For $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we have $f(z+1) = f(z)$,
so f must have a Fourier expansion

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad q = e^{2\pi i z}.$$

If only non-negative powers of q are involved, and a few other technical conditions are satisfied, then this function is called

- a **modular form** of weight k on $\Gamma_0(N)$.
- N is called the *level* of f.

We further specialize the set of modular forms.

There is a family of operators, called “Hecke operators", acting on the space of modular forms of given weight and level. Eigenvectors of Hecke operators are called *eigenforms*.

There are other technical conditions that make a modular form a “cusp form" and a “new form".

Suppose now we have a modular form $f(z)$ which is

- of weight 2 and level N,
- an eigenform,
- a cusp form,
- a new form.

Suppose now we have a modular form $f(z)$ which is

- of weight 2 and level N,
- an eigenform,
- a cusp form,
- a new form.

Under these conditions it can be normalized so that

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \qquad a_1 = 1.$$

Suppose now we have a modular form $f(z)$ which is

- of weight 2 and level N,
- an eigenform,
- a cusp form,
- a new form.

Under these conditions it can be normalized so that

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \qquad a_1 = 1.$$

Now suppose that all other coefficients a_n are integers.

Suppose now we have a modular form $f(z)$ which is
- of weight 2 and level N,
- an eigenform,
- a cusp form,
- a new form.

Under these conditions it can be normalized so that

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \qquad a_1 = 1.$$

Now suppose that all other coefficients a_n are integers.

Then there exists an elliptic curve with
- integer coefficients,
- conductor N,
- the a_p (as defined earlier) agreeing with the Fourier coefficients of f.

Y. Taniyama (1927–1958) was the first to suggest (mid-1950s):

Every elliptic curve arises in this manner;
such curves are called *modular*.

Y. Taniyama (1927–1958) was the first to suggest (mid-1950s):

Every elliptic curve arises in this manner;
such curves are called *modular*.

G. Shimura (1930–) expanded on this idea, and

A. Weil (1906–1998) made it more precise:

Y. Taniyama (1927–1958) was the first to suggest (mid-1950s):

Every elliptic curve arises in this manner;
such curves are called *modular*.

G. Shimura (1930–) expanded on this idea, and

A. Weil (1906–1998) made it more precise:

Taniyama-Shimura-Weil Conjecture:
Every elliptic curve over $\mathbb{Q}$ is modular.

Taniyama-Shimura-Weil Conjecture:
Every elliptic curve over $\mathbb{Q}$ is modular.

Recall:

Theorem (Wiles):
Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Taniyama-Shimura-Weil Conjecture:
Every elliptic curve over $\mathbb{Q}$ is modular.

Recall:

Theorem (Wiles):
Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Corollary: Every Frey curve is modular.

Taniyama-Shimura-Weil Conjecture:
Every elliptic curve over $\mathbb{Q}$ is modular.

Recall:

Theorem (Wiles):
Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Corollary: Every Frey curve is modular.

Contradiction: (Ribet)
A Frey curve *cannot* be modular.

Taniyama-Shimura-Weil Conjecture:
Every elliptic curve over $\mathbb{Q}$ is modular.

Recall:

Theorem (Wiles):
Every *semistable* elliptic curve over $\mathbb{Q}$ is modular.

Corollary: Every Frey curve is modular.

Contradiction: (Ribet)
A Frey curve *cannot* be modular.

This proves Fermat's Last Theorem.

Andrew John Wiles (1953 –)

Wednesday 23 June 1993, around 10.30 a.m.
The Newton Institute, Cambridge, England

“Having written the theorem on the blackboard he said, ‘I will stop here’, and sat down".

It didn't quite end there . . .

It didn’t quite end there . . .

Later in 1993 it became clear that there was a serious gap in Wiles’ proof.

It didn't quite end there . . .

Later in 1993 it became clear that there was a serious gap in Wiles' proof.

Wiles and Richard Taylor (a former student) spent almost a year trying to repair the proof.

It didn't quite end there . . .

Later in 1993 it became clear that there was a serious gap in Wiles' proof.

Wiles and Richard Taylor (a former student) spent almost a year trying to repair the proof.

At first they had no success.

It didn't quite end there . . .

Later in 1993 it became clear that there was a serious gap in Wiles' proof.

Wiles and Richard Taylor (a former student) spent almost a year trying to repair the proof.

At first they had no success.

In September, 1994, they finally succeeded.

It didn't quite end there . . .

Later in 1993 it became clear that there was a serious gap in Wiles' proof.

Wiles and Richard Taylor (a former student) spent almost a year trying to repair the proof.

At first they had no success.

In September, 1994, they finally succeeded.

Two manuscripts were submitted, and published in 1995, one joint with Taylor.

It didn’t quite end there . . .

Later in 1993 it became clear that there was a serious gap in Wiles’ proof.

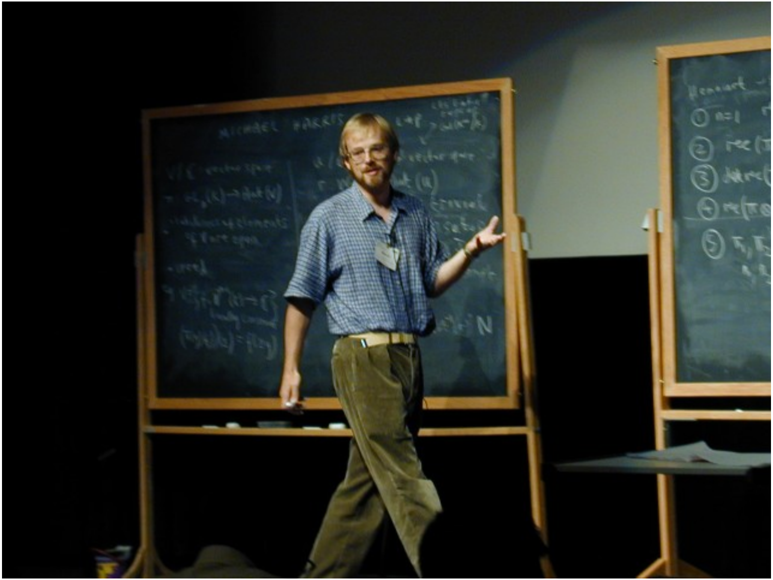
Wiles and Richard Taylor (a former student) spent almost a year trying to repair the proof.

At first they had no success.

In September, 1994, they finally succeeded.

Two manuscripts were submitted, and published in 1995, one joint with Taylor.

Wiles received the famous “Wolfskehl Prize" in 1997.



Richard Taylor (1962 –), Princeton, 1999

Later developments:

Recall that Wiles proved the TSW-conjecture “only" for semistable curves.

Later developments:

Recall that Wiles proved the TSW-conjecture “only" for semistable curves.

The full conjecture was later proved by
C. Breuil, B. Conrad, F. Diamond, and R. Taylor;
announced 1999, published 2001.
(Using methods first developed by Wiles).

The generalized Fermat conjecture:
Consider

$$x^p + y^q = z^r, \qquad (p, q, r \in \mathbb{N}, 1/p + 1/q + 1/r < 1).$$

Are there solutions in integers x, y, z that have no common divisor?

The generalized Fermat conjecture:
Consider

$$x^p + y^q = z^r, \qquad (p, q, r \in \mathbb{N}, 1/p + 1/q + 1/r < 1).$$

Are there solutions in integers x, y, z that have no common divisor?

Conjecture (Darmon, Granville, 1990's):
The above equation has precisely 10 nontrivial solutions.

The generalized Fermat conjecture:
Consider

$$x^p + y^q = z^r, \qquad (p, q, r \in \mathbb{N}, 1/p + 1/q + 1/r < 1).$$

Are there solutions in integers x, y, z that have no common divisor?

Conjecture (Darmon, Granville, 1990's):
The above equation has precisely 10 nontrivial solutions.

For instance, the 10th solution is

$$33^8 + 1549034^2 = 15613^3.$$

The generalized Fermat conjecture:
Consider

$$x^p + y^q = z^r, \qquad (p, q, r \in \mathbb{N}, 1/p + 1/q + 1/r < 1).$$

Are there solutions in integers x, y, z that have no common divisor?

Conjecture (Darmon, Granville, 1990's):
The above equation has precisely 10 nontrivial solutions.

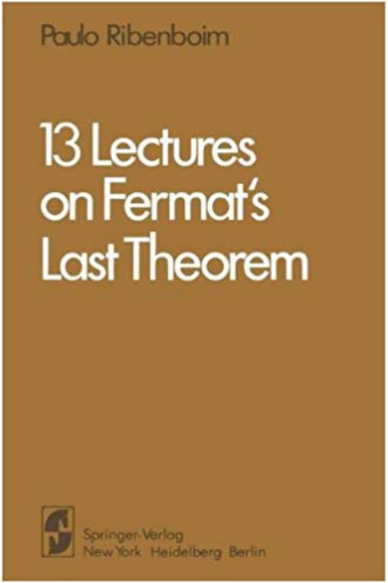
For instance, the 10th solution is

$$33^8 + 1549034^2 = 15613^3.$$

Some partial results are known.

Henri Darmon
McGill Univ.

Andrew Granville
Univ. de Montréal


Paulo Ribenboim
13 Lectures on Fermat's Last Theorem
Springer-Verlag
New York Heidelberg Berlin

Thank you

7 Kč ČESKÁ REPUBLIKA
PIERRE DE FERMAT 1670
$x^n + y^n = z^n$
ANDREW WILES 1995
2000 SVĚTOVÝ ROK MATEMATIKY

Cartoons were removed due to copyright concerns.
Please visit
`http://www.sciencecartoonsplus.com/`
or get these books: