Solving Diophantine Equations via Modular Curves

Ekin Özman

Boğaziçi University

May 27, 2016

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ - 三 - のへぐ

$$\star ax + by = c$$

$$\star ax + by = c$$

*
$$x^n + y^n = z^n \Rightarrow$$
 Fermat's Equation

$$\star$$
 ax + by = c

*
$$x^n + y^n = z^n \Rightarrow$$
 Fermat's Equation

$$\star y^2 = x^3 + ax + b$$

< ロ > < 同 > < 三 > < 三 > < 三 > < ○ < ○ </p>

$$\star ax + by = c$$

- * $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- * $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve

$$\star ax + by = c$$

- * $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- * $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve
- Diophantine equations define algebraic curves and algebraic surfaces.

▲ロト ▲ 理 ト ▲ 王 ト ▲ 王 - り へ (~)

Original Statement of FLT



1661-1665

Arithmeticorum Liber II. intervallars sumtrorum 1. minor autem c'hic & des saller les c' bit a' S. M.

hoc foperaddere 10. Ter igitur a. adici-

1 N. atque ideo muior 1 N. + 2. Oportet en Les deshois & pridaç & renharises itaque 4 N. + 4. triples elle ad 2. & ad- 1) ur f. C Tes varpiges at 7. vpic des huc fupersödere to. Ter iginar 1. adici mudde fi pi ni i. ben urb et "Fander its mitarbus to. requester 4 N. + 4. & d. 1. jerne i destud ni 3. fand he blar. fets N. 3. Erit ergo minor 3. maior 5. & an at 5. 6 A suider At ... 3 mair el

IN STARSTIONEM FIL

CONDITIONIS appofice ealon ratio ell que & appofice precedenti quellori, sil enin Canore intera vequalerrazionervali enserven fermere intervalio quedenceun, & Canore interva les cuints locaris Adelbaser, y manifelhan ell.

QVESTIO VIII.

PROPOSITIVE quadratum disidere TON Shrangfordi repairer datasi di indues quadratos, Imperatum fit ve Ton Shrangfordi ve datasi di primus 1 Q. Oportet igitur 16 - 1 Q. rqua-les effe quadrato. Fingo quadratum à nu-meris quotquot liburin, cum defectu rot vtrimque defection & a fimilious auferannilia, fient 5 Q. aquales 16 N. & fit 1 N. " Erit igitur alter quadratorum W. alter verb W & virisfore Samma eft 47 feu 16. Se sterque qualentat eff.

16. dieidatur in duos quadratos, Ponatur Janes en die empejamut, ent veragte b weren Surveyous post. Stion Les unddas et Afriles discissions west line 20 400 winteren qued continct laten ipfins 16. Is mer bal a meine af fau têr i v e efte a s N. - 4. ipie ipter quedrates ette, a vebage, fau et fa briefe af F. eine $4 \cdot Q + 16 - 16$ N. her equilation vie de s med see fau dates fau de se fau dates fau 4 Q. + 10. - 10 Commenis adiciatur saide er er. mirs im genin er saide Juracour sant sant mentala i heibe. al bes insine fatter, distance for i for aufanieri, ei sieren fatchalt of, miner Tue, Sens ball err' einererischlar, b A put einermier Tue, & a Sie munitiere man venetionerla, ine seradat of . and for interpre my abarth.

OBSERVATIO DOMINI PETRI DE FERMAT.

Them enter in dass cabes , out enclosed estantia in dass anderstanderster Co gener ditter nallam in infaitum vitra quadratum pateflatem in daes ein dem neminis fer eft dinidere enixe rei demenftrationem mirabilen fant debeni. Hane marginis exignitas non caperet.

OVÆSTIO 1X.

R duidere in doos quadratos. Ponavnitatum, quot conflat latus disidendi. Ello itaque a N. - 4. crunt quadrati, hic

ETTO de mise de mpisses de ter turfas primi latus i N. alterius vero i su susiro, nolego (* int., i) su tripe ensecunque semettorum com defediu tot di interferen Asilent' inter igi i si date presive midan You do of A saile at \$ Elo inspiri N. – a crutt quantati, no: line ga regiona a lap e-mensiona quanda di anti a conservato a la conservato di anti a conserva Ineres at very abure by she duraness with

'It is impossible to separate a cube into two cubes or a fourth power into fourth powers or, in general, any power greater than the second powers of like degree. I have discovered a truly marvelous demonstration, which this margin is too narrow to contain.' ◆□▶ ◆□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

The equation

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

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

has no nonzero integer solutions if n > 2.

The equation

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

has no nonzero integer solutions if n > 2.

- $n = 1 \Rightarrow x + y = c$, has infinitely many solutions
- $n = 2 \Rightarrow x^2 + y^2 = z^2$, has infinitely many solutions, Pythagorean triple.

◆□▶ ◆□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

The equation

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

has no nonzero integer solutions if n > 2.

- $n = 1 \Rightarrow x + y = c$, has infinitely many solutions
- n = 2 ⇒ x² + y² = z², has infinitely many solutions, Pythagorean triple. Another conic, x² + y² = 0.999999 has no rational solutions,

< ロ > < 同 > < 三 > < 三 > < 三 > < ○ < ○ </p>

The equation

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

has no nonzero integer solutions if n > 2.

- $n = 1 \Rightarrow x + y = c$, has infinitely many solutions
- n = 2 ⇒ x² + y² = z², has infinitely many solutions, Pythagorean triple. Another conic, x² + y² = 0.999999 has no rational solutions, Things may change dramatically!

First General Proof

By Mr. Le Blanc in 1823:



By Mr. Le Blanc in 1823:

Theorem

If p and 2p + 1 are both prime, then $x^p + y^p = z^p$ has no solutions for which xyz is not divisible by p.

▲□▶ ▲□▶ ▲□▶ ▲□▶ = 三 のへで

By Mr. Le Blanc in 1823:

Theorem

If p and 2p + 1 are both prime, then $x^p + y^p = z^p$ has no solutions for which xyz is not divisible by p.

▲□▶ ▲□▶ ▲□▶ ▲□▶ = 三 のへで

By Mr. Le Blanc in 1823:

Theorem

If p and 2p + 1 are both prime, then $x^p + y^p = z^p$ has no solutions for which xyz is not divisible by p.





1776-1831

"Monsieur Leblanc"

◆□▶ ◆□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Germain & Gauss

◆□▶ ◆□▶ ◆目▶ ◆目▶ 目 のへの

Gauss:

Gauss:

'...when a woman, because of her sex, our customs and prejudices, encounters infinitely more obstacles than men, yet overcomes these fetters and penetrates that which is most hidden, she doubtless has the most noble courage, extraordinary talent and superior genius. Nothing could prove to me in a more flattering and less equivocal way that the attractions of that science, which have added so much joy to my life, are not chimerical, than the favor with which you have honored it..'

...cinsiyetinden, geleneklerimiz ve önyargılarımızdan ötürü bir kadın, erkeklere oranla çok daha fazla engelle karşılaşıyor, yine de bu engelleri alt ediyor ve gizli saklı olana nüfuz edebiliyorsa, şüphesiz ki o çok asil bir cesarete, olağanüstü bir yeteneğe ve üstün bir dehaya sahiptir. Hiçbir şey bana, hayatıma büyük bir mutluluk katan o bilimin cazibesinin asılsız olmadığını, o cazibeyi şereflendirişinizden daha hoş ve kesin bir şekilde ispatlayamaz.

Theorem

Two dimensional surfaces in 3 dimensional space can be classified according to their genus.

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

Theorem

Two dimensional surfaces in 3 dimensional space can be classified according to their genus.

▲□▶ ▲□▶ ▲ □▶ ▲ □▶ ▲ □ ▶ ④ ヘ ⊙

Definition

The genus is the number of holes in the surface.

Theorem

Two dimensional surfaces in 3 dimensional space can be classified according to their genus.

Definition

The genus is the number of holes in the surface.

Mordell conjectured in 1922: If complex number solutions of a Diophantine equation form a surface of genus \geq 2 then the equation has only finitely many rational solutions.

うつん 川 エー・エー・ エー・ ひゃう

Theorem

Two dimensional surfaces in 3 dimensional space can be classified according to their genus.

Definition

The genus is the number of holes in the surface.

Mordell conjectured in 1922: If complex number solutions of a Diophantine equation form a surface of genus \geq 2 then the equation has only finitely many rational solutions.

うつん 川 エー・エー・ エー・ ひゃう

Faltings proved Mordell's conjecture in 1983.

Theorem

Two dimensional surfaces in 3 dimensional space can be classified according to their genus.

Definition

The genus is the number of holes in the surface.

Mordell conjectured in 1922: If complex number solutions of a Diophantine equation form a surface of genus \geq 2 then the equation has only finitely many rational solutions.

Faltings proved Mordell's conjecture in 1983. The result of Faltings $\Rightarrow x^n + y^n = z^n$ can have only finitely many solutions for n > 3.

ふちゃ 御 えばやえばや (日本)

Theorem

Two dimensional surfaces in 3 dimensional space can be classified according to their genus.

Definition

The genus is the number of holes in the surface.

Mordell conjectured in 1922: If complex number solutions of a Diophantine equation form a surface of genus \geq 2 then the equation has only finitely many rational solutions.

Faltings proved Mordell's conjecture in 1983. The result of Faltings $\Rightarrow x^n + y^n = z^n$ can have only finitely many solutions for n > 3.

Granville and **Heath-Brown**: the number of solutions of FLT -if they exist- decreases as the exponent *n* increases, i.e. FLT is '*almost always*' true, if there are solutions they are few and very far between.

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

◆□▶ ◆□▶ ◆□▶ ◆□▶ ● □ ● ○○○

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

• Given by $y^2 = x^3 + ax + b$, when *a*, *b* rational numbers.

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ◆ □ ▶ ◆ □ ▶ ◆ □ ▶

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

• Given by $y^2 = x^3 + ax + b$, when a, b rational numbers. such as $E: y^2 = x(x-1)(x+1)$.

うつん 川 エー・エー・ エー・ ひゃう

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

• Given by $y^2 = x^3 + ax + b$, when a, b rational numbers. such as $E: y^2 = x(x-1)(x+1)$.

うつん 川 エー・エー・ エー・ ひゃう

• No cusp or self-intersection.

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

• Given by $y^2 = x^3 + ax + b$, when a, b rational numbers. such as $E: y^2 = x(x-1)(x+1)$.

うつん 川 エー・エー・ エー・ ひゃう

- No cusp or self-intersection.
- Solutions form a group with identity element *O*.

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

• Given by $y^2 = x^3 + ax + b$, when a, b rational numbers. such as $E: y^2 = x(x-1)(x+1)$.

うつん 川 エー・エー・ エー・ ひゃう

- No cusp or self-intersection.
- Solutions form a group with identity element *O*.
- Complex solutions of such a cubic form a torus.

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b rational numbers. such as $E: y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form a group with identity element *O*.
- Complex solutions of such a cubic form a torus.

•
$$E(\mathbb{Q}) = \{(x, y) | x, y \in \mathbb{Q}, y^2 = x^3 + ax + b\},\ y^2 = x(x-1)(x+1)$$
 has only 4 points in $E(\mathbb{Q})$.



- These curves are not 'closed'. We should 'close them up'.
- This is done by adding another point to the curve, 'point at ∞'. Denote this point as O.

Group Law on Elliptic Curves

We can ADD points on an elliptic curve, the point at ∞ is the *identity element*.



Group Law on Elliptic Curves

We can ADD points on an elliptic curve, the point at ∞ is the *identity element*.





▲□▶▲□▶▲目▶▲目▶ 目 のへの



 $P\oplus Q=R' \qquad \texttt{ADAGE} = \texttt{OQC}$
Elliptic Curve mod p

Example

 $E: y^2 = x^3 - x + 1, \text{ find solutions mod 3.} \\ E(\mathbb{F}_3) = \{(0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\}.$

< ロ > < 同 > < 三 > < 三 > < 三 > < ○ < ○ </p>

 $E: y^2 = x^3 - x + 1$, find solutions mod 3. $E(\mathbb{F}_3) = \{(0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\}$. Note that point at ∞ is always in the set of solutions, $|E(\mathbb{F}_3)| = 7$.

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

 $E: y^2 = x^3 - x + 1$, find solutions mod 3. $E(\mathbb{F}_3) = \{(0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\}$. Note that point at ∞ is always in the set of solutions, $|E(\mathbb{F}_3)| = 7$.

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ◆ □ ▶ ◆ □ ▶ ◆ □ ▶

We can do this modulo many other primes p. Say N_p is the number of solutions mod p.

 $E: y^2 = x^3 - x + 1$, find solutions mod 3. $E(\mathbb{F}_3) = \{(0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\}$. Note that point at ∞ is always in the set of solutions, $|E(\mathbb{F}_3)| = 7$.

We can do this modulo many other primes p. Say N_p is the number of solutions mod p.

p	3	5	7	11	13	17	19	23	29	31	37	41
N _p	7	8	12	10	19	14	22	23	37	35	36	51

うつん 川 エー・エー・ エー・ ひゃう

• Number of solutions increase as *p* increases.

 $E: y^2 = x^3 - x + 1$, find solutions mod 3. $E(\mathbb{F}_3) = \{(0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\}$. Note that point at ∞ is always in the set of solutions, $|E(\mathbb{F}_3)| = 7$.

We can do this modulo many other primes p. Say N_p is the number of solutions mod p.

p	3	5	7	11	13	17	19	23	29	31	37	41
Np	7	8	12	10	19	14	22	23	37	35	36	51

うつん 川 エー・エー・ エー・ ひゃう

- Number of solutions increase as p increases.
- Hasse's Theorem: $|N_p (p+1)| \le 2\sqrt{p}$.

a _p :	$a_{\rho} = \rho + 1 - N_{\rho}, E : y^{2} = x^{3} - x + 1$												
	p	3	5	7	11	13	17	19	23	29	31	37	41
	Np	7	8	12	10	19	14	22	23	37	35	36	51
	a _p	-3	-2	-4	2	-5	4	-2	1	-7	-3	2	-9

◆□▶ ◆□▶ ▲目▶ ▲目▶ ▲□▶

р	3	5	7	11	13	17	19	23	29	31	37	41
Np	7	8	12	10	19	14	22	23	37	35	36	51
ap	-3	-2	-4	2	-5	4	-2	1	-7	-3	2	-9

- Can we predict a_p ?
- For instance, is there a complex function f(z) which has power series representation $\sum_{n=1}^{\infty} a'_n q^n$ where $q = \exp^{2\pi i}$,

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

$$a_p = a'_p$$
?

$a_p = p + 1 - N_p, E$:	$y^2 = x^3 - x + $	1
--------------------------	--------------------	---

р	3	5	7	11	13	17	19	23	29	31	37	41
Np	7	8	12	10	19	14	22	23	37	35	36	51
ap	-3	-2	-4	2	-5	4	-2	1	-7	-3	2	-9

- Can we predict a_p ?
- For instance, is there a complex function f(z) which has power series representation $\sum_{n=1}^{\infty} a'_n q^n$ where $q = \exp^{2\pi i}$,

$$a_p = a'_p$$
?

For $E: y^2 = x^3 - x + 1$, there is such a complex function:

$$q$$
- $3q^3$ - $2q^5$ - $4q^7$ + $6q^9$ + $2q^{11}$ - $5q^{13}$ + $6q^{15}$ + $4q^{17}$ - $2q^{19}$ + $12q^{21}$

+ 1
$$q^{23}$$
- q^{25} -9 q^{27} - 7 q^{29} - 3 q^{31} -6 q^{33} +8 q^{35} + 2 q^{37} +15 q^{39} - 9 q^{41} +.

$a_p = p + 1 - N_p, E$:	$y^2 = x^3 - x + $	1
--------------------------	--------------------	---

р	3	5	7	11	13	17	19	23	29	31	37	41
Np	7	8	12	10	19	14	22	23	37	35	36	51
ap	-3	-2	-4	2	-5	4	-2	1	-7	-3	2	-9

- Can we predict a_p ?
- For instance, is there a complex function f(z) which has power series representation $\sum_{n=1}^{\infty} a'_n q^n$ where $q = \exp^{2\pi i}$,

$$a_p = a'_p$$
?

For $E: y^2 = x^3 - x + 1$, there is such a complex function:

$$q$$
- $3q^3$ - $2q^5$ - $4q^7$ + $6q^9$ + $2q^{11}$ - $5q^{13}$ + $6q^{15}$ + $4q^{17}$ - $2q^{19}$ + $12q^{21}$

+ 1 $q^{23}-q^{25}-9q^{27}-7q^{29}-3q^{31}-6q^{33}+8q^{35}+2q^{37}+15q^{39}-9q^{41}+$.

Can we predict a_p ? Yes, first observed by Eichler.

Consider the equation of a circle $x^2 + y^2 = a^2$, this can be parametrized by $x = a \cos t$, $y = a \sin t$.

Consider the equation of a circle $x^2 + y^2 = a^2$, this can be parametrized by $x = a \cos t$, $y = a \sin t$.

• A MEC is an extension of this idea to the more complicated complex plane, with a special non-Euclidean geometry.

< ロ > < 同 > < 三 > < 三 > < 三 > < ○ < ○ </p>

Consider the equation of a circle $x^2 + y^2 = a^2$, this can be parametrized by $x = a \cos t$, $y = a \sin t$.

• A MEC is an extension of this idea to the more complicated complex plane, with a special non-Euclidean geometry.

< ロ > < 同 > < 三 > < 三 > < 三 > < ○ < ○ </p>

 Modular forms are some special differential forms on modular curves.

Consider the equation of a circle $x^2 + y^2 = a^2$, this can be parametrized by $x = a \cos t$, $y = a \sin t$.

- A MEC is an extension of this idea to the more complicated complex plane, with a special non-Euclidean geometry.
- Modular forms are some special differential forms on modular curves.
- Modular forms on the complex plane have symmetries wrt the more complicated transformations $f(z) \mapsto f(\frac{az+b}{cz+d})$.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

Consider the equation of a circle $x^2 + y^2 = a^2$, this can be parametrized by $x = a \cos t$, $y = a \sin t$.

- A MEC is an extension of this idea to the more complicated complex plane, with a special non-Euclidean geometry.
- **Modular forms** are some special differential forms on modular curves.
- Modular forms on the complex plane have symmetries wrt the more complicated transformations $f(z) \mapsto f(\frac{az+b}{cz+d})$.
- Modular forms have power series representations i.e. they can be written as $\sum_{n=1}^{\infty} a'_n q^n$ where $q = \exp^{2\pi i}$.
- a MEC is an elliptic curve which can be 'parametrized' by a modular form. (The a_p 's coming from the e.c. correspond to the coefficients of a modular form a'_p .)

Taniyama(55) and Shimura(57): Every elliptic curve over rational numbers is parametrized by a modular form. OR Every elliptic curve over \mathbb{Q} is modular.



Taniyama, 1927-1958



Shimura, 1930-

・ ロ ト ・ 同 ト ・ 日 ト ・ 日 ト

Modularity Theorem

by Wiles, Taylor-Wiles, Breuil, Conrad, Diamond, Taylor

Every elliptic curve over $\ensuremath{\mathbb{Q}}$ is modular.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

Modularity Theorem

by Wiles, Taylor-Wiles, Breuil, Conrad, Diamond, Taylor

Every elliptic curve over \mathbb{Q} is modular.

$$f = q + \sum c_n q^n \leftrightarrow E_f/\mathbb{Q}$$

s.t. for almost all primes $\ell, c_\ell = a_\ell(E_f) = \ell + 1 - |E(\mathbb{F}_\ell)|$

< ロ > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

Modularity Theorem

by Wiles, Taylor-Wiles, Breuil, Conrad, Diamond, Taylor

Every elliptic curve over \mathbb{Q} is modular.

$$f = q + \sum c_n q^n \leftrightarrow E_f/\mathbb{Q}$$

s.t. for almost all primes $\ell, c_{\ell} = a_{\ell}(E_f) = \ell + 1 - |E(\mathbb{F}_{\ell})|$



◆□▶ ◆□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Comparing Different Worlds



<□ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Comparing Different Worlds



A third object is needed....

Comparing Different Worlds



In order to understand the ideas behind the proof of Modularity theorem one needs to know a lot about:

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ のへぐ

Elliptic Curves

In order to understand the ideas behind the proof of Modularity theorem one needs to know a lot about:

▲□▶ ▲□▶ ▲□▶ ▲□▶ = 三 のへで

- Elliptic Curves
- Modular Forms

In order to understand the ideas behind the proof of Modularity theorem one needs to know a lot about:

- Elliptic Curves
- Modular Forms
- Galois Representations

How to use these ideas to solve Diophantine equations such as FLT?

▲ロト ▲□ ト ▲ ヨ ト ▲ ヨ ト つくぐ

E elliptic curve over \mathbb{Q} . If *E* satisfies a technical condition then *E* corresponds to a special modular form (called **newform**) of level N_p .

◆□▶ ◆□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Technical condition:= E doesn't have an isogeny whose kernel has size p for a prime $p \ge 5$

E elliptic curve over \mathbb{Q} . If *E* satisfies a technical condition then *E* corresponds to a special modular form (called **newform**) of level N_p .

Technical condition:= E doesn't have an isogeny whose kernel has size p for a prime $p \ge 5$

E has an invariant, called conductor, *N_E* ∈ ℤ, easy to compute given the equation of *E*

◆□▶ ◆□▶ ◆□▶ ◆□▶ ● □ ● ○○○

E elliptic curve over \mathbb{Q} . If *E* satisfies a technical condition then *E* corresponds to a special modular form (called **newform**) of level N_p .

Technical condition:= E doesn't have an isogeny whose kernel has size p for a prime $p \ge 5$

- *E* has an invariant, called conductor, *N_E* ∈ ℤ, easy to compute given the equation of *E*
- N_p is a small integer which divides the conductor of E

うつん 川 エー・エー・ エー・ ひゃう

E elliptic curve over \mathbb{Q} . If *E* satisfies a technical condition then *E* corresponds to a special modular form (called **newform**) of level N_p .

Technical condition:= E doesn't have an isogeny whose kernel has size p for a prime $p \ge 5$

- *E* has an invariant, called conductor, *N_E* ∈ ℤ, easy to compute given the equation of *E*
- N_p is a small integer which divides the conductor of E

うつん 川 エー・エー・ エー・ ひゃう

There is an explicit recipe to find N_p

E elliptic curve over \mathbb{Q} . If *E* satisfies a technical condition then *E* corresponds to a special modular form (called **newform**) of level N_p .

Technical condition:= E doesn't have an isogeny whose kernel has size p for a prime $p \ge 5$

- *E* has an invariant, called conductor, N_E ∈ ℤ, easy to compute given the equation of *E*
- N_p is a small integer which divides the conductor of E
- There is an explicit recipe to find N_p
- Given N_p there are only finitely many newforms of level N_p .

Frey Elliptic Curve

How to use Ribet's theorem to solve FLT: $x^p + y^p = z^p$?

(ロ)

Frey Elliptic Curve

How to use Ribet's theorem to solve FLT: $x^{p} + y^{p} = z^{p}$?

Assume FLT has a solution and associate the solution to an elliptic curve *E* called the Frey curve if possible.

Definition

Say a, b, c is a nontrivial solution to FLT_p , i.e. $a^p + b^p = c^p$ then

$$E_{a,b,c}: y^2 = x(x-a^p)(x+b^p)$$

is called Frey elliptic curve.

Frey elliptic curve has very strange properties.

- E satisfies the 'technical condition' i.e. E doesn't have any p-isogenies (by a theorem of Mazur)
- Conductor of E, $N_E = \prod_{\ell \mid abc} \ell$

Frey Elliptic Curve

How to use Ribet's theorem to solve FLT: $x^p + y^p = z^p$?

Assume FLT has a solution and associate the solution to an elliptic curve *E* called the Frey curve if possible.

Definition

Say a, b, c is a nontrivial solution to FLT_p , i.e. $a^p + b^p = c^p$ then

$$E_{a,b,c}: y^2 = x(x-a^p)(x+b^p)$$

is called Frey elliptic curve.

Frey elliptic curve has very strange properties.

- E satisfies the 'technical condition' i.e. E doesn't have any p-isogenies (by a theorem of Mazur)
- Conductor of E, $N_E = \prod_{\ell \mid abc} \ell$
- Ribet's formula $\rightarrow N_p = 2$

Say *a*, *b*, *c* is a nontrivial solution to FLT_p , i.e. $a^p + b^p = c^p$ then

$$E_{a,b,c}: y^2 = x(x-a^p)(x+b^p)$$

◆□▶ ◆□▶ ◆□▶ ◆□▶ ● □ ● ○○○

is called Frey elliptic curve.

Ribet's formula $\rightarrow N_p = 2$ Therefore by Ribet's thm:

Say *a*, *b*, *c* is a nontrivial solution to FLT_p , i.e. $a^p + b^p = c^p$ then

$$E_{a,b,c}: y^2 = x(x-a^p)(x+b^p)$$

▲ロト ▲ 理 ト ▲ 王 ト ▲ 王 - り へ (~)

is called Frey elliptic curve.

Ribet's formula $\rightarrow N_p = 2$ Therefore by Ribet's thm:

 $\Rightarrow E_{a,b,c}$ is associated to a newform of level $N_p = 2$.

Say *a*, *b*, *c* is a nontrivial solution to FLT_p , i.e. $a^p + b^p = c^p$ then

$$E_{a,b,c}: y^2 = x(x-a^p)(x+b^p)$$

うつん 川 エー・エー・ エー・ ひゃう

is called Frey elliptic curve.

Ribet's formula $\rightarrow N_p = 2$ Therefore by Ribet's thm:

- $\Rightarrow E_{a,b,c}$ is associated to a newform of level $N_p = 2$.
- \Rightarrow But there is no such newform!

Say a, b, c is a nontrivial solution to FLT_p , i.e. $a^p + b^p = c^p$ then

$$E_{a,b,c}: y^2 = x(x-a^p)(x+b^p)$$

is called Frey elliptic curve.

Ribet's formula $\rightarrow N_p = 2$ Therefore by Ribet's thm:

- $\Rightarrow E_{a,b,c}$ is associated to a newform of level $N_p = 2$.
- \Rightarrow But there is no such newform!
- \Rightarrow Hence, contradiction, FLT doesn't have a solution (*a*, *b*, *c*).
Wiles was the person who did the important final work on the theorem by proving a form of the modularity conjecture needed to prove FLT, the entire enterprise was the work of many people. And it is all their contributions, taken together, which brought the final solution.

Wiles was the person who did the important final work on the theorem by proving a form of the modularity conjecture needed to prove FLT, the entire enterprise was the work of many people. And it is all their contributions, taken together, which brought the final solution.

 $\begin{array}{c} \text{Kummer} \stackrel{\text{Ideals}}{\rightarrow} \text{Mazur} \stackrel{\text{Eisenstein Ideal}}{\rightarrow} \text{Frey} \stackrel{\text{Frey Curve}}{\rightarrow} \\ \text{Serre,Ribet,Taniyama,Shimura} \stackrel{\text{ST implies FLT}}{\rightarrow} \text{Wiles} \Rightarrow \text{FLT} \end{array}$

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

Barry Mazur:

'Number theory produces, without effort, innumerable problems which have a sweet, innocent air about them, tempting flowers; and yet ... number theory swarms with bugs, waiting to bite the tempted flower-lovers who, one bitten, are inspired to excess of effort!. '

(From number theory as gadfly)

Sayı teorisi, çok da çaba sarf etmeden, tatlı ve masum, sayısız problem üretir; gönülçelen çiçekler gibidir. Ama aynı sayı teorisi, baştan çıkmış çiçek severleri ısırmayı bekleyen böceklerle doludur. kişi bir kere ısırılmaya görsün, aşırı çaba sarf etmeye hevesli hale gelir.