Solving Diophantine Equations via Modular Curves

Ekin Özman

Boğaziçi University

May 27, 2016

- Diophantine equation $\Rightarrow$ integer solutions to a polynomial equation with integer coefficients.
  Some examples:

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to a polynomial equation with integer coefficients.
  Some examples:

$\star$ $ax + by = c$

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to a polynomial equation with integer coefficients.
  Some examples:

⋆ $ax + by = c$

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

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to a polynomial equation with integer coefficients.
  Some examples:

⋆ $ax + by = c$

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

⋆ $y^2 = x^3 + ax + b$

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to a polynomial equation with integer coefficients.
  Some examples:

⋆ $ax + by = c$

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

⋆ $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to a polynomial equation with integer coefficients.
  Some examples:

$\star$ $ax + by = c$

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

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

- Diophantine equations define algebraic curves and algebraic surfaces.

Original Statement of FLT

1661-1665

'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.'

Fermat's Last Theorem

Theorem (Wiles, Taylor-Wiles)

The equation

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

has no nonzero integer solutions if $n > 2$.

Fermat's Last Theorem

Theorem (Wiles, Taylor-Wiles)

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.

Fermat's Last Theorem

Theorem (Wiles, Taylor-Wiles)

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.
  Another conic, $x^2 + y^2 = 0.999999$ has no rational solutions,

Fermat's Last Theorem

Theorem (Wiles, Taylor-Wiles)

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.
  Another conic, $x^2 + y^2 = 0.999999$ has no rational solutions, Things may change dramatically!

First General Proof

By Mr. Le Blanc in 1823:

First General Proof

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.

First General Proof

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.

First General Proof

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

Gauss:

Germain & 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.

Modern Approaches-Mordell Conjecture

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.

Modern Approaches-Mordell Conjecture

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 ≥ 2 then the equation has only finitely many rational solutions.

Modern Approaches-Mordell Conjecture

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 ≥ 2 then the equation has only finitely many rational solutions.

Faltings proved Mordell's conjecture in 1983.

Modern Approaches-Mordell Conjecture

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 ≥ 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 $n > 3$.

Modern Approaches-Mordell Conjecture

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 ≥ 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.

Elliptic Curves

Definition

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.

Elliptic Curves

Definition

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.

Definition

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 $E : y^2 = x(x-1)(x+1)$.

Elliptic Curves

Definition

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.

Elliptic Curves

Definition

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.

Elliptic Curves

Definition

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.

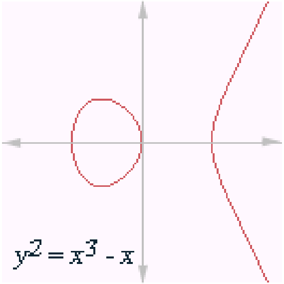
- Given by $y^2 = x^3 + ax + b$, when a, b rational numbers. such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form a group with identity element O.
- Complex solutions of such a cubic form a torus.

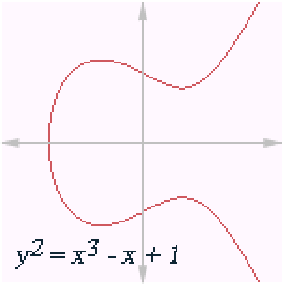
Elliptic Curves

Definition

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 $E(\mathbb{Q})$.

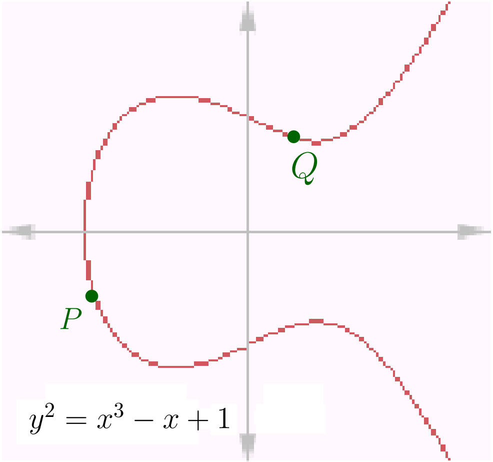




- These curves are not ‘closed’. We should ‘close them up’.
- This is done by adding another point to the curve, ‘*point at* ∞’. Denote this point as O.

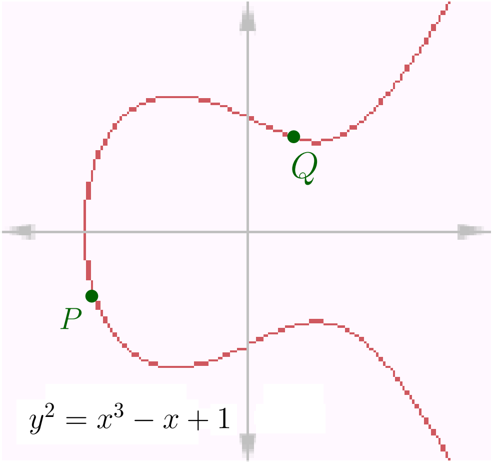
Group Law on Elliptic Curves

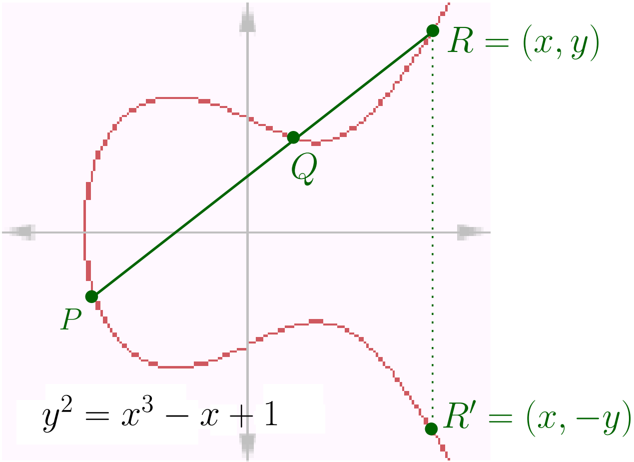
We can ADD points on an elliptic curve, the point at ∞ is the *identity element*.

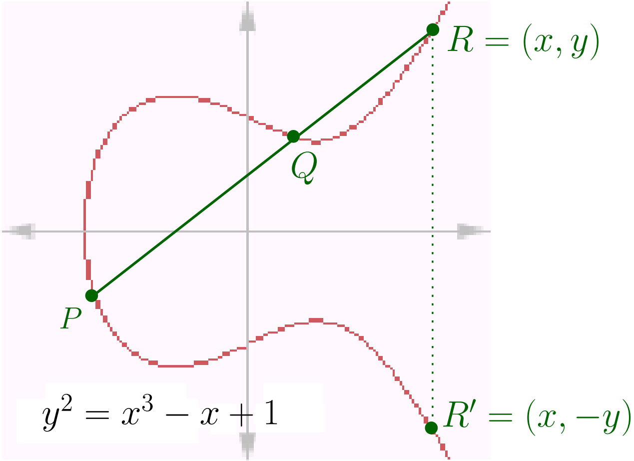


Group Law on Elliptic Curves

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




$R = (x, y)$
Q
P
$y^2 = x^3 - x + 1$
$R' = (x, -y)$



$$P \oplus Q = R'$$

Elliptic Curve mod p

Example

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

Example

$E : y^2 = x^3 - x + 1$, 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, $|E(\mathbb{F}_3)| = 7$.

Elliptic Curve mod p

Example

$E : y^2 = x^3 - x + 1$, 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.

Elliptic Curve mod p

Example

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

- Number of solutions increase as p increases.

Example

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

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

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

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
a_p	-3	-2	-4	2	-5	4	-2	1	-7	-3	2	-9

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

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
a_p	-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 $q = \exp^{2\pi i}$, $a_p = a'_p$?

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

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
a_p	-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 $q = \exp^{2\pi i}$, $a_p = a'_p$?

Example

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

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

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

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

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
a_p	-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 $q = \exp^{2\pi i}$, $a_p = a'_p$?

Example

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

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

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

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

Modular Elliptic Curves(MEC)

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

Modular Elliptic Curves(MEC)

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 Elliptic Curves(MEC)

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 Elliptic Curves(MEC)

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 Elliptic Curves(MEC)

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.)

Modularity Conjecture

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-

Modularity Theorem

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

Every elliptic curve over $\mathbb{Q}$ 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 ℓ, $c_\ell = a_\ell(E_f) = \ell + 1 - |E(\mathbb{F}_\ell)|$

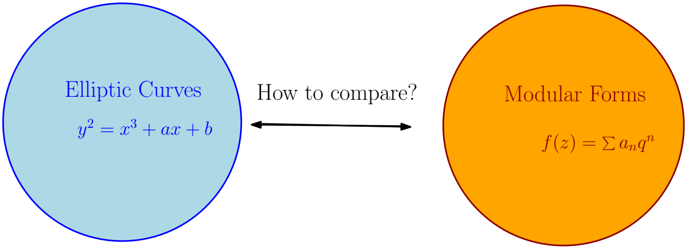
Modularity Theorem

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

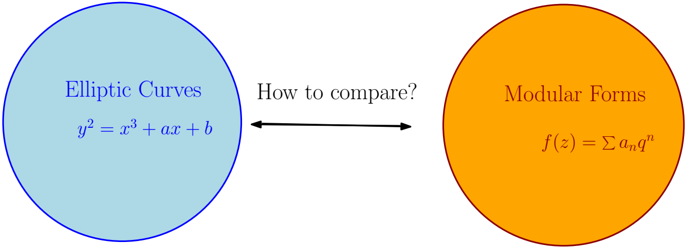
Every elliptic curve over $\mathbb{Q}$ is modular.

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

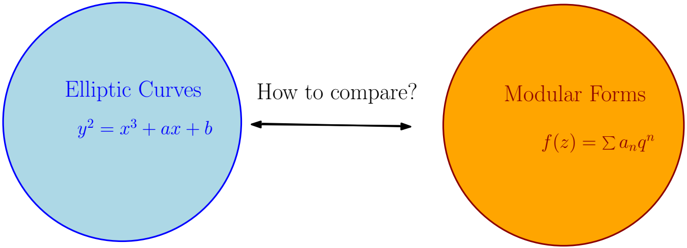
s.t. for almost all primes ℓ, $c_\ell = a_\ell(E_f) = \ell + 1 - |E(\mathbb{F}_\ell)|$



Comparing Different Worlds

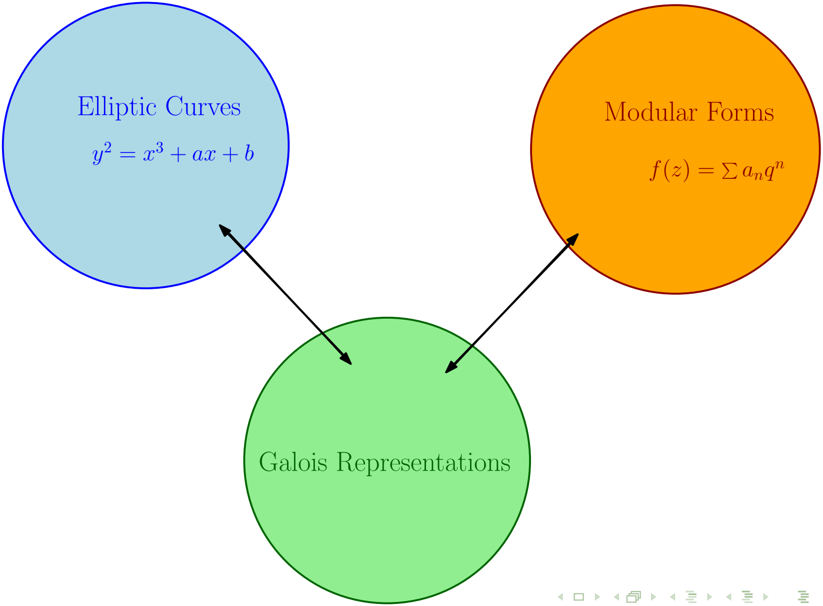


Comparing Different Worlds



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:

- Elliptic Curves

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

- 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?

Ribet's Level Lowering Theorem

Theorem

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` $p \geq 5$

Ribet's Level Lowering Theorem

Theorem

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` $p \geq 5$

- E has an invariant, called conductor, $N_E \in \mathbb{Z}$, easy to compute given the equation of E

Ribet's Level Lowering Theorem

Theorem

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` $p \geq 5$

- E has an invariant, called conductor, $N_E \in \mathbb{Z}$, easy to compute given the equation of E
- N_p is a small integer which divides the conductor of E

Ribet's Level Lowering Theorem

Theorem

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` $p \geq 5$

- E has an invariant, called conductor, $N_E \in \mathbb{Z}$, 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

Ribet's Level Lowering Theorem

Theorem

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` $p \geq 5$

- E has an invariant, called conductor, $N_E \in \mathbb{Z}$, 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: $x^p + y^p = z^p$?

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, $N_E = \Pi_{\ell | abc} \ell$

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, $N_E = \Pi_{\ell | abc} \ell$
- Ribet's formula $\rightarrow N_p = 2$

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.

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

Fermat's Last Theorem

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.

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

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

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.

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!

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.

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).

Summary

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.

Summary

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.

$$\text{Kummer} \stackrel{\texttt{Ideals}}{\to} \text{Mazur} \xrightarrow{\texttt{Eisenstein Ideal}} \text{Frey} \xrightarrow{\texttt{Frey Curve}}$$

$$\text{Serre,Ribet,Taniyama,Shimura} \xrightarrow{\texttt{ST implies FLT}} \text{Wiles} \Rightarrow \text{FLT}$$

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.