Elliptic Curves & Number Theory

R. Sujatha
School of Mathematics
TIFR

Aim: To explain the connection between a simple ancient problem in number theory and a deep sophisticated conjecture about Elliptic Curves (‘arithmetic Geometry’).

Aim: To explain the connection between a simple ancient problem in number theory and a deep sophisticated conjecture about Elliptic Curves ('arithmetic Geometry').

Notation:

$\mathbb{N}$: set of natural numbers $(1, 2, 3, \ldots)$

Aim: To explain the connection between a simple ancient problem in number theory and a deep sophisticated conjecture about Elliptic Curves (‘arithmetic Geometry’).

Notation:

$\mathbb{N}$: set of natural numbers $(1, 2, 3, \ldots)$

$\mathbb{Z}$: set of integers $(\ldots, -3, -2, -1, 0, 1, 2, \ldots)$

Aim: To explain the connection between a simple ancient problem in number theory and a deep sophisticated conjecture about Elliptic Curves ('arithmetic Geometry').

Notation:

$\mathbb{N}$: set of natural numbers $(1, 2, 3, \ldots)$

$\mathbb{Z}$: set of integers $(\ldots, -3, -2, -1, 0, 1, 2, \ldots)$

$\mathbb{Q}$: Rational numbers

- Recall that a real number is rational if it can be expressed in the form $\alpha = \frac{m}{n}$, where m and n are in $\mathbb{Z}$.

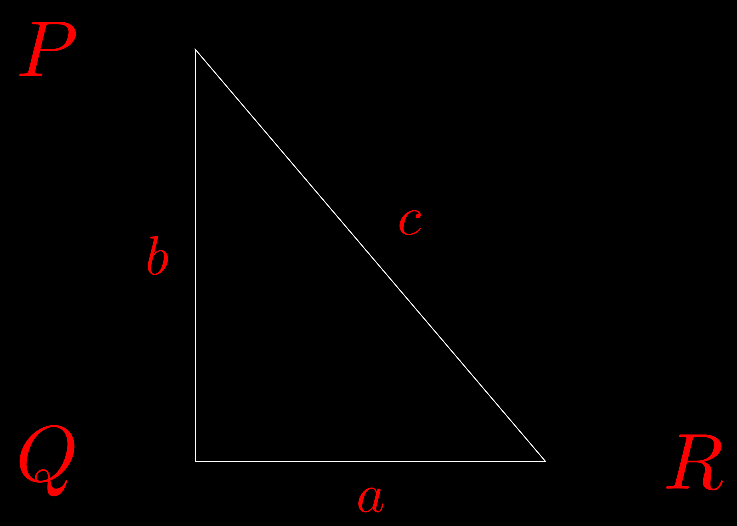
- Irrational numbers: Those which cannot be expressed in the form $m/n,\ m,n \in \mathbb{Z}$.

Example:

$$\sqrt{2}, \quad \pi = 3.1419,\ \frac{1+\sqrt{5}}{2}.$$

Pythagorean Triples:

- PQR is right angled triangle
- Sides have lengths a, b, c.



Pythogoras Theorem: PQR a right angled triangle. Then

$$(PQ)^2 + (QR)^2 = (PR)^2 \quad i.e.\ a^2 + b^2 = c^2.$$

Pythogoras Theorem: PQR a right angled triangle. Then

$$(PQ)^2 + (QR)^2 = (PR)^2 \quad i.e.\ a^2 + b^2 = c^2.$$

Certainly known to ancient Indians ('Sulva Sutras' $\sim$ 8th century BC), (Pythagoras $\sim$ 5th century BC).

Pythogoras Theorem: PQR a right angled triangle. Then

$$(PQ)^2 + (QR)^2 = (PR)^2 \quad i.e.\ a^2 + b^2 = c^2.$$

Certainly known to ancient Indians ('Sulva Sutras' $\sim$ 8th century BC), (Pythagoras $\sim$ 5th century BC).

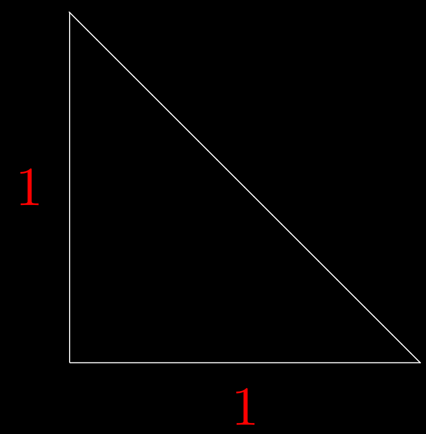
Examples:

$$(3)^2 + (4)^2 = (5)^2$$
$$(12)^2 + (5)^2 = (13)^2$$

- (a, b, c) is called a Pythagoras triple; $(3, 4, 5)$, $(5, 12, 13)$ are Pythagoras triples.

- (a, b, c) is called a Pythagoras triple; $(3, 4, 5), (5, 12, 13)$ are Pythagoras triples.
- There exist infintely many Pythagoras triples in $\mathbb{N}$.

- (a, b, c) is called a Pythagoras triple; $(3, 4, 5), (5, 12, 13)$ are Pythagoras triples.
- There exist infintely many Pythagoras triples in $\mathbb{N}$.
- Note that the Pythagoras Theorem forces one to come to terms with irrational numbers!



$$a = b = 1, \quad c = \sqrt{2}$$

Fundamental Theorem of Arithmetic

Each integer $n > 1$ can be written uniquely *(up to reordering) as a product of powers of primes;*

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

p_i *are distinct prime numbers,* $\alpha_i \in \mathbb{N}$.

Fundamental Theorem of Arithmetic

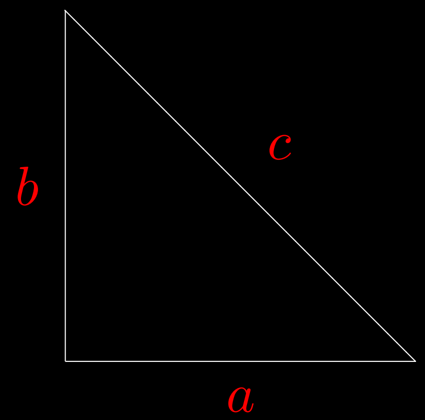
Each integer $n > 1$ can be written uniquely *(up to reordering) as a product of powers of primes;*

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

p_i *are distinct prime numbers,* $\alpha_i \in \mathbb{N}$*.*

Henceforth: Will consider only right angled triangles.

Let T denote a right angled triangle with sides of length a, b, c.



Simple Exercise: Use the fundamental theorem to show that $\sqrt{2}$ is irrational.

Simple Exercise: Use the fundamental theorem to show that $\sqrt{2}$ is irrational.

Of course, usually T has at least one of its sides rational but we want to consider only triangles T having all of its sides with *rational* length.

Simple Exercise: Use the fundamental theorem to show that $\sqrt{2}$ is irrational.

Of course, usually T has at least one of its sides rational but we want to consider only triangles T having all of its sides with *rational* length.

Example:

$$a = \frac{40}{6}, \; b = \frac{9}{6}, \; c = \frac{41}{6}$$

$$\left(\frac{40}{6}\right)^2 + \left(\frac{9}{6}\right)^2 = \left(\frac{41}{6}\right)^2.$$

Definition:

- We say T is *rational* if all the three sides have rational length.

Definition:

- We say T is *rational* if all the three sides have rational length.
- We say T is *primitive* if a, b, c are positive integers and $(a, b, c) = 1$ (i.e. they are *relatively prime* which means a, b, c have no common divisor other than 1).

Definition:

- We say T is *rational* if all the three sides have rational length.
- We say T is *primitive* if a, b, c are positive integers and $(a, b, c) = 1$ (i.e. they are *relatively prime* which means a, b, c have no common divisor other than 1).

Can clearly bring any rational triangle to be similar to a *unique* primitive triangle.

First Observation: If T is primitive, then precisely one of its sides a or b is even.

- If $2|a$ and $2|b$, then as $a^2 + b^2 = c^2$, $2|c \Rightarrow 2$ divides a, b and c; contradicting that T is primitive.

First Observation: If T is primitive, then precisely one of its sides a or b is even.

- If $2|a$ and $2|b$, then as $a^2 + b^2 = c^2$, $2|c \Rightarrow 2$ divides a, b and c; contradicting that T is primitive.

- If a and b are both odd, say $a = 2a_1 + 1$, $b = 2b_1 + 1$; then $a^2 + b^2 = 4k + 2 = c^2 \Rightarrow 2|c^2 \Rightarrow 2|c \Rightarrow 4|c^2$.

First Observation: If T is primitive, then precisely one of its sides a or b is even.

- If $2|a$ and $2|b$, then as $a^2 + b^2 = c^2$, $2|c \Rightarrow 2$ divides a, b and c; contradicting that T is primitive.

- If a and b are both odd, say $a = 2a_1 + 1$, $b = 2b_1 + 1$; then $a^2 + b^2 = 4k + 2 = c^2 \Rightarrow 2|c^2 \Rightarrow 2|c \Rightarrow 4|c^2$.

  But $c^2 = 4k + 2$, hence we get a contradiction.

Second Observation: If T is primitive, then there exist positive integers m, n with $(m, n) = 1$ such that

$$a = n^2 - m^2,\ b = 2mn;\ c = m^2 + n^2$$

Second Observation: If T is primitive, then there exist positive integers m, n with $(m, n) = 1$ such that

$$a = n^2 - m^2,\ b = 2mn;\ c = m^2 + n^2$$

OR

$$a = 2mn,\ b = n^2 - m^2;\ c = m^2 + n^2.$$

Second Observation: If T is primitive, then there exist positive integers m, n with $(m, n) = 1$ such that

$$a = n^2 - m^2,\ b = 2mn;\ c = m^2 + n^2$$

OR

$$a = 2mn,\ b = n^2 - m^2;\ c = m^2 + n^2.$$

- Note that

$$a^2 + b^2 = (n^2 - m)^2 + (2mn)^2 = (n^2 + m^2)^2 = c^2,$$

so we do have a Pythogrean triple.

Let us see why the second observation is true.

Let us see why the second observation is true.

- Assume T to be primitive, then either one of a or b is odd by our first observation.

Let us see why the second observation is true.

- Assume T to be primitive, then either one of a or b is odd by our first observation.

- Let us suppose that a is odd and b is even. Then clearly c is odd, hence $(b, c) = 1$.

Let us see why the second observation is true.

• Assume T to be primitive, then either one of a or b is odd by our first observation.

• Let us suppose that a is odd and b is even. Then clearly c is odd, hence $(b, c) = 1$.

Also $(a, c) = 1$ because $a^2 + b^2 = c^2.$

• Put $w_1 = 1/2(c - a)\ w_2 = 1/2(c + a)$.

Let us see why the second observation is true.

• Assume T to be primitive, then either one of a or b is odd by our first observation.

• Let us suppose that a is odd and b is even. Then clearly c is odd, hence $(b, c) = 1$.

Also $(a, c) = 1$ because $a^2 + b^2 = c^2.$

• Put $w_1 = 1/2(c - a)$ $w_2 = 1/2(c + a)$.

Clearly both w_1 and w_2 are positive integers.

- We prove that w_1 and w_2 are relatively prime i.e. $(w_1, w_2) = 1$.

- We prove that w_1 and w_2 are relatively prime i.e. $(w_1, w_2) = 1$.

Suppose $d|w_1$ and $d|w_2$; then $d|w_1 + w_2$ and $d|w + 2 = w_1$.

Now $w_1 + w_2 = c_1,\ w_2 - w_1 = a \Rightarrow d|c$ and $d|a$.

- We prove that w_1 and w_2 are relatively prime i.e. $(w_1, w_2) = 1$.

Suppose $d|w_1$ and $d|w_2$; then $d|w_1 + w_2$ and $d|w + 2 = w_1$.

Now $w_1 + w_2 = c_1,\ w_2 - w_1 = a \Rightarrow d|c$ and $d|a$.

Contradicts $(a, c) = 1$!

- We prove that w_1 and w_2 are relatively prime i.e. $(w_1, w_2) = 1$.

Suppose $d|w_1$ and $d|w_2$; then $d|w_1 + w_2$ and $d|w + 2 = w_1$.

Now $w_1 + w_2 = c_1,\ w_2 - w_1 = a \Rightarrow d|c$ and $d|a$.

Contradicts $(a, c) = 1$!

$a^2 + b^2 + c^2$ takes the form

$$b^2 = (c^2 - a^2); \frac{b^2}{4} = \frac{c^2 - a^2}{4} \Rightarrow (b/2)^2 = (\frac{c - a}{2})(\frac{c + a}{2}) = w_1 w_2.$$

What We Get: w_1 and w_2 are relatively prime and their product is a square.

What We Get: w_1 and w_2 are relatively prime and their product is a square.

Conclusion (By the fundamental theorem of arithmetic):

What We Get: w_1 and w_2 are relatively prime and their product is a square.

Conclusion (By the fundamental theorem of arithmetic): Both w_1 and w_2 are squares.

$$w_1 = m_1^2,\ w_2 = n^2 \text{ and } (m, n) = 1.$$

But

$$a = w_1 - w_2 = m^2 - n^2$$

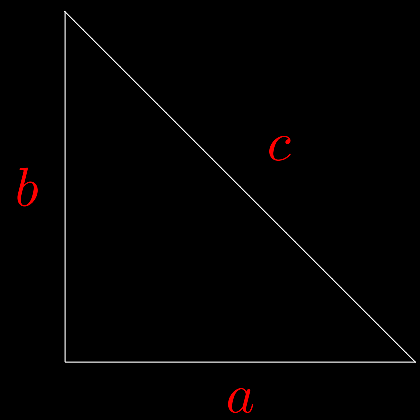
$$c = w_1 + w_2 = m^2 + n^2$$

$$b^2 = c^2 - a^2 \Rightarrow b = 2mn.$$

This concludes the proof of second observation.

Areas

Area of $T = \frac{1}{2}ab$



- Let N be a positive integer. There exist infinitely many T's such that Area $(T) = N$ (choose positve rational numbers a, b such that $ab = 2N$).

- Let N be a positive integer. There exist infinitely many T's such that Area $(T) = N$ (choose positve rational numbers a, b such that $ab = 2N)$.

Key Question: Does there exist a *rational* T with area $(T) = N?$

- Let N be a positive integer. There exist infinitely many T's such that Area $(T) = N$ (choose positve rational numbers a, b such that $ab = 2N$).

Key Question: Does there exist a *rational* T with area $(T) = N?$

(i.e. We want a right angled Δ^{le} with all its sides having rational length and area equal to N).

Definition: We say N is *congruent* if there exists a rational T with Area $(T) = N$.

Definition: We say N is *congruent* if there exists a rational T with Area $(T) = N$.

Example:

- $N = 5$ is congruent $(a, b, c) = (9/6, 40/6, 41/6)$.

Area $= 1/2 \times 9/6 \times 40/6 = 5$.

Definition: We say N is *congruent* if there exists a rational T with Area $(T) = N$.

Example:

• $N = 5$ is congruent $(a, b, c) = (9/6, 40/6, 41/6)$.

Area $= 1/2 \times 9/6 \times 40/6 = 5$.

• $N = 6$ is congruent $(a, b, c) = (3, 4, 5)$.

Definition: We say N is *congruent* if there exists a rational T with Area $(T) = N$.

Example:

• $N = 5$ is congruent $(a, b, c) = (9/6, 40/6, 41/6)$.

Area $= 1/2 \times 9/6 \times 40/6 = 5$.

• $N = 6$ is congruent $(a, b, c) = (3, 4, 5)$.

Arab Mathematicians (and Indian Mathematicians) made tables of congruent numbers (10th century AD).

Example:

$$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, \ldots$$

are all congruent.

Example:

$$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, \ldots$$

are all congruent.

- If N is congruent, so is $N' = d^2 N$, where $d \in \mathbb{Z}$ (If $N = 1/2(ab)$ and (a, b, c) is a Pythagoras triple, consider

$$(a', b', c') = (da, db, dc); 1/2(a'b')1/2(da)(db) = d^2\, N = N').$$

- Therefore we may restrict attention to *square free* natural numbers (i.e. those elements in $\mathbb{N}$ which are not divisible by p^2 for any prime p).

First Obvious Question: Is 1 a congruent number?

- As it was difficult to find a Y with area 1, the ancients tried to show that 1 was not congruent number with many false proofs.

- The first proof that 1 is *not* a congruent number was given by Fermat, a 17th century French lawyer and government official by profession, but a polymath of great erudition.

Theorem (Fermat)

1 is not a congruent number.

Theorem (Fermat)

1 is not a congruent number.

- The proof is a truly marvellous gem of a proof and uses the idea of *infinite descent*.

Theorem (Fermat)

1 is not a congruent number.

- The proof is a truly marvellous gem of a proof and uses the idea of *infinite descent*.

- Basic Idea: (each time the triangles are primitive) Start with $\triangle T_1$ such that $c_1 =$ Area (T_1) is a square; then produce a T_2 such that $c_2 =$ Area T_2 is again a square *and* $c_2 < c_1$.

- Repeating this step, we can construct an infinite sequence of primitive triangles T_i whose area c_i is always a square and

$$c_1 > c_2 > c_3 > \cdots$$

But this cannot go on forever as one cannot have an infinite strictly decreasing sequence of positive integers!

- Repeating this step, we can construct an infinite sequence of primitive triangles T_i whose area c_i is always a square and

$$c_1 > c_2 > c_3 > \cdots$$

But this cannot go on forever as one cannot have an infinite strictly decreasing sequence of positive integers!

- Heart of the argument uses the second observation we made before.

Corollary: The equation $x^4 - y^4 = z^2$ has no solution in integers x, y, z with $xyz \neq 0$.

Corollary: The equation $x^4 - y^4 = z^2$ has no solution in integers x, y, z with $xyz \neq 0$.

Proof: Suppose a solution exists. Put

$$n = x^2,\ m = y^2$$
$$a = n^2 - m^2,\ b = 2mn,\ c = n^2 + m^2$$

so that (a, b, c) is a Pythagoras triple with

$$\text{Area } = (1/2)ab = nm(n^2 - m^2) = x^2y^2(x-y) = x^2y^2z^2.$$

Define T' with sides of length (a', b', c') where

$$a' = \frac{a}{\lambda},\ b' = \frac{b}{\lambda},\ c' = \frac{c}{\lambda},\ \lambda = xyz (\neq 0)$$

$$\text{Area}(T') = 1/2 \cdot \frac{a}{\lambda}\frac{b}{\lambda} = \frac{ab}{2\lambda^2} = \frac{2x^2y^2z^2}{2x^2y^2z^2} = 1.$$

1 is a congruent number, contradiction!

In particular, this shows that $x^4 - y^4 = w^4$ has no solution in integers with $xyw \neq 0$. This would have led Fermat to conjecture his famous **Last Theorem** that for any integer $n \geq 3$, the equation

$$x^n = y^n + z^n.$$

has no solution in integers x, y, z with $xyz \neq 0$!

This is now a celebrated **Theorem of Andrew Wiles**.

non-congruent N: $1, 2, 3, 10, 11, 17, 19, 26, 33, 35 \ldots$.

non-congruent N: $1, 2, 3, 10, 11, 17, 19, 26, 33, 35 \ldots$.

Ancient Question I: Is there an algorithm for deciding in a *finite* number of steps whether a given positive integer N is congruent or not.

non-congruent N: $1, 2, 3, 10, 11, 17, 19, 26, 33, 35 \ldots$.

Ancient Question I: Is there an algorithm for deciding in a *finite* number of steps whether a given positive integer N is congruent or not.

Ancient Question II: Prove that every square free integer of the form $8n+5$ or $8n+6$ or $8n+7$ ($n = 1, 2, \ldots$) is congruent.

Conjecturally, there is a very simple answer to both these Questions, but the *conjecture* is now a **Millennium Problem** worth a million dollars!

Elliptic Curves

This is an area of study which has connections with different branches of mathematics like complex manifolds, algebraic geometry, arithmetic geometry modular forms and of course in recent years in cryptography.

Elliptic Curves

This is an area of study which has connections with different branches of mathematics like complex manifolds, algebraic geometry, arithmetic geometry modular forms and of course in recent years in cryptography.

Perhaps it would be no exaggeration to say that it is an area where endless mining for problems, research and applications is possible!

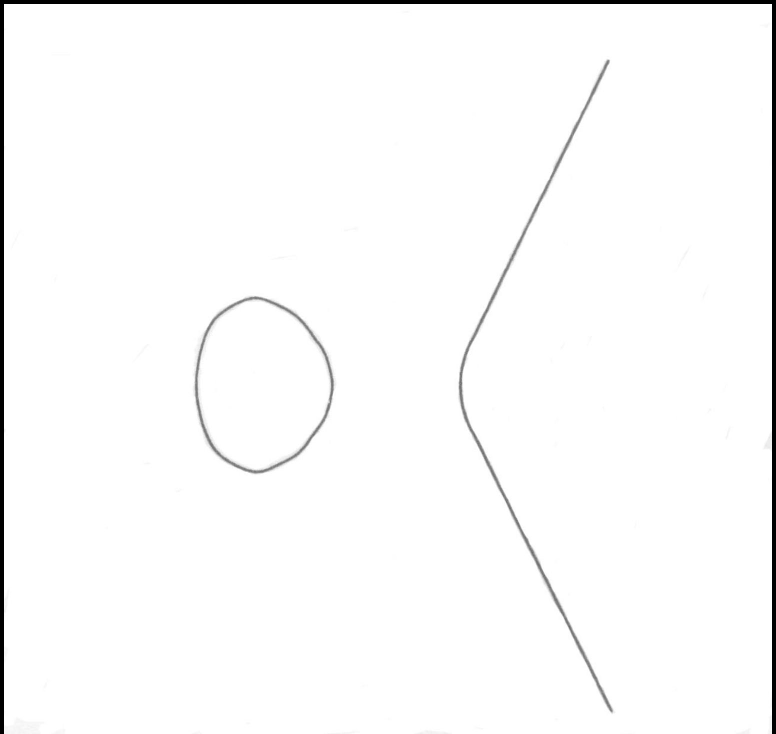
For our purposes today, we shall satisfy ourselves with considering elliptic curves over $\mathbb{Q}$. They can then be studied as *solutions* of equations of the form

$$E : y^2 = f(x)$$

where $f(x)$ is a polynomial over $\mathbb{Q}$ of degree 3. One can even assume that

$$f(x) = ax^3 + cx + d,\ a, c, d \in \mathbb{Q},\ a \neq 0.$$

Its set of *real* points looks like



Why are they relevant to the study of congruent numbers?

Why are they relevant to the study of congruent numbers?

A natural number n is congruent if and only if the *elliptic curve over* $\mathbb{Q}$ defined by

$$E_n : y^2 = x^3 - n^2 x$$

has *infinitely* many solutions over $\mathbb{Q}$.

- To see this equivalence is not too difficult. It follows from Pythagoras identity and transferring one curve to another by ‘birational isomorphisms’.

- To see this equivalence is not too difficult. It follows from Pythagoras identity and transferring one curve to another by ‘birational isomorphisms’.

- Another crucial property that is useful here is that the set of solutions $E(\mathbb{Q})$ for any elliptic curve $E/\mathbb{Q}$ has the structure of an abelian group.

- To see this equivalence is not too difficult. It follows from Pythagoras identity and transferring one curve to another by ‘birational isomorphisms’.

- Another crucial property that is useful here is that the set of solutions $E(\mathbb{Q})$ for any elliptic curve $E/\mathbb{Q}$ has the structure of an abelian group.

- The law of addition on $E(\mathbb{Q})$ is *not* naive coordinate addition; it involves beautiful geometric ideas.

- One knows more about $E(\mathbb{Q})$; in fact it is a *finitely generated* abelian group which in simple words means that a *finite set* suffices to construct all the elements in $E(\mathbb{Q})$. This is known as *Mordell's Theorem*.

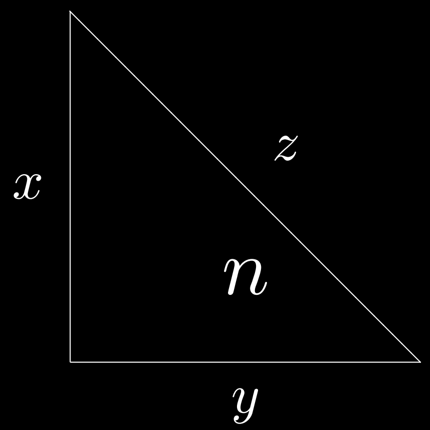
- One knows more about $E(\mathbb{Q})$; in fact it is a *finitely generated* abelian group which in simple words means that a *finite set* suffices to construct all the elements in $E(\mathbb{Q})$. This is known as *Mordell's Theorem*.

- In particular, we have

$$E_n(\mathbb{Q}) = \text{“free infinite part”} \oplus \text{“finite part”}$$

Caution: It might happen that a given elliptic curve E has only one *trivial* point, i.e. $E(\mathbb{Q})$ is a singleton set; this point necessarily lies in the Finite torsion part.

Caution: It might happen that a given elliptic curve E has only one *trivial* point, i.e. $E(\mathbb{Q})$ is a singleton set; this point necessarily lies in the Finite torsion part.



n is a congruent number $\Leftrightarrow E_n : y^2 = x^3 - n^2 x$ has infinitely many rational points.

Known: The “finite” (i.e. torsion) part of $E_n(\mathbb{Q})$ consists of *4* elements.

Thus we are now faced with the

Question: When is $E_n(\mathbb{Q})$ infinite?

- It is at this step that one of the most famous conjectures of the last century intervenes. This is the so-called Birch & Swinnerton-Dyer Conjecture (B-SD) which relates the nature of $E(\mathbb{Q})$ to something completely different!

- It is at this step that one of the most famous conjectures of the last century intervenes. This is the so-called Birch & Swinnerton-Dyer Conjecture (B-SD) which relates the nature of $E(\mathbb{Q})$ to something completely different!

Hasse-Weil L-Functions: We shall not go into the technical definition of this. Suffice it to say that it is a vast ingenious generalisation of the classical Riemann Zeta function.

- It is “built” using information about the number of points that E has over finite fields $\mathbb{F}_p$, as p varies over all primes.

- It is “built” using information about the number of points that E has over finite fields $\mathbb{F}_p$, as p varies over all primes.

Given an elliptic curve $E/\mathbb{Q}$, its Hasse-Weil L-function is denoted by $L(E,s)$, s a complex variable.

- It is “built” using information about the number of points that E has over finite fields $\mathbb{F}_p$, as p varies over all primes.

Given an elliptic curve $E/\mathbb{Q}$, its Hasse-Weil L-function is denoted by $L(E, s)$, s a complex variable.

- It has an expansion into an infinite product, the product varying over all primes.

- It is "built" using information about the number of points that E has over finite fields $\mathbb{F}_p$, as p varies over all primes.

Given an elliptic curve $E/\mathbb{Q}$, its Hasse-Weil L-function is denoted by $L(E, s)$, s a complex variable.

- It has an expansion into an infinite product, the product varying over all primes.
- $L(E, s) = \prod_p (1 - 2a_p p^{-s} + p^{1-2s})^{-1}$.

Can expand this 'Euler product' to get a 'Dirichlet Series', i.e. an infinite sum:

$$L(E,s) = \sum_{n=0}^{\infty} a_n n^{-s} = \sum_{n=0}^{\infty} a_n / n^s.$$

Can expand this ‘Euler product’ to get a ‘Dirichlet Series’, i.e. an infinite sum:

$$L(E,s) = \sum_{n=0}^{\infty} a_n n^{-s} = \sum_{n=0}^{\infty} a_n / n^s.$$

- Deep and important conjectures on convergence properties of this function on the complex plane.

Can expand this ‘Euler product’ to get a ‘Dirichlet Series’, i.e. an infinite sum:

$$L(E,s) = \sum_{n=0}^{\infty} a_n n^{-s} = \sum_{n=0}^{\infty} a_n / n^s.$$

- Deep and important conjectures on convergence properties of this function on the complex plane.

B-SD Conjecture: $E(\mathbb{Q})$ *is infinite if and only if* $L(E,s)$ *vanishes at* $s = 1$ *(i.e.* $L(E,1) = 0$*).*

So we can now reformulate our original Question and ask:

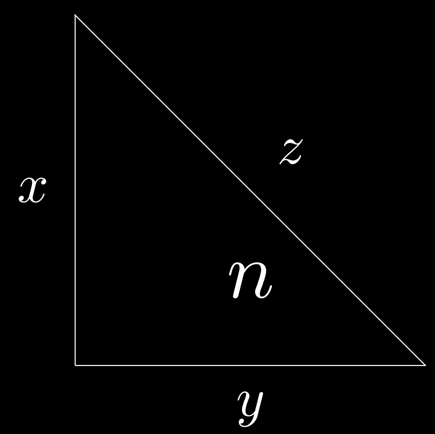
Question: When is $L(E_n, 1) = 0$?

So we can now reformulate our original Question and ask:

Question: When is $L(E_n, 1) = 0$?

• Coates-Wiles(1970's): $L(E_n, 1) \neq 0 \Rightarrow E_n(\mathbb{Q})$ is finite.

• Finding $E(\mathbb{Q})$ for an elliptic curve E is in general very difficult, even with computers! On the other hand, computations with L-functions are more amenable to calculations!



n is a congruent number $\Leftrightarrow E_n : y^2 = x^3 - n^2x$; $E_n(\mathbb{Q})$ is infinite $\Rightarrow L(E_n, 1) = 0$.

Conjecturally (BSD Conjecture) $L(E_n, 1) = 0 \Rightarrow E_n(\mathbb{Q})$ is infinite.

We will connect the vanishing of $L(E_n, 1)$ now to

We will connect the vanishing of $L(E_n, 1)$ now to

Modular forms

This is the next area in mathematics from which we need to draw our artillery now!

Again, this is a vast, fascinating and technical subject in its own right with beautiful connections to elliptic curves.

At its very simplest, a modular form is a holomorphic function $f(z)$ on the upper half plane (which is the part of the complex plane with imaginary part > 0), such that it has a Fourier expansion (called the q-expansion)

$$f(z) = \sum_{n \in \mathbb{Z}}^{\infty} a_n q^n, \; q = e^{2\pi i z}, \; a_n \in \mathbb{C}.$$

- We will consider special modular forms, called "Cusp forms"; these have an expansion

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \ q = e^{2\pi i z}, \ a_n \in \mathbb{C}.$$

- We will consider special modular forms, called "Cusp forms"; these have an expansion

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \; q = e^{2\pi i z}, \; a_n \in \mathbb{C}.$$

Example

$$\begin{aligned} \Delta(z) &= q \prod_{n=1}^{\infty} (1-q^n)^{24} \\ &= \sum_{n=1}^{\infty} \tau(n) q^n \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \ldots \end{aligned}$$

($\tau \rightsquigarrow$ Ramanujan's Tau function).

- Given a modular form (cusp form), it has an L-series associated to it:

$$L(f,s) = \sum_{n=1}^{\infty} a_n/n^s.$$

- Given a modular form (cusp form), it has an L-series associated to it:

$$L(f,s) = \sum_{n=1}^{\infty} a_n/n^s.$$

Let $E_1' : y^2 = x^3 - x$.

- $L(E_1', s)$ related to $L(f,s)$ for some f.

Deep work of Shimura, Waldspurger and Tunnell then allows us to relate $L(E_n, s)$ and $L(f, s)$; the bridge being $L(E_1', s)$. More precisely:

Deep work of Shimura, Waldspurger and Tunnell then allows us to relate $L(E_n, s)$ and $L(f, s)$; the bridge being $L(E_1', s)$. More precisely:

• There exist modular forms g_1, g_2 which are obtained via f;

$$g_1 = \sum_{n=1}^{\infty} a(n)q^n, \;\; g_2 = \sum_{n=1}^{\infty} b(n)q^n$$

such that

$$L(E_n, 1) \overset{\text{related}}{\rightsquigarrow}_{\text{to}} \quad \text{coefficients of } g_1 \;\&\; g_2.$$

Thus we can connect this to our original problem by the following theorem:

Theorem (Tunnell, 1983): $L(E_n, 1) = 0$ *if and only if* $a(n) = 0$ *for* n *odd, or* $b(n/2) = 0$ *for* n *even.* Moreover,

$$a(n) + b(n/2) \neq 0 \Rightarrow L(E_n, 1) \neq 0.$$

Thus we can connect this to our original problem by the following theorem:

Theorem (Tunnell, 1983): $L(E_n, 1) = 0$ *if and only if* $a(n) = 0$ *for* n *odd, or* $b(n/2) = 0$ *for* n *even.* Moreover,

$$a(n) + b(n/2) \neq 0 \Rightarrow L(E_n, 1) \neq 0.$$

In particular, if $a(n) + b(n/2) \neq 0$, then n is not congruent.

We thus have:

We thus have:

n is a congruent number $\Leftrightarrow E_n : y^2 = x^3 - n^2x$; $E_n(\mathbb{Q})$ is infinite

We thus have:

n is a congruent number $\Leftrightarrow E_n : y^2 = x^3 - n^2x$; $E_n(\mathbb{Q})$ is infinite

$\Rightarrow L(E_n, 1) = 0$.

We thus have:

n is a congruent number $\Leftrightarrow E_n : y^2 = x^3 - n^2x$; $E_n(\mathbb{Q})$ is infinite

$\Rightarrow L(E_n, 1) = 0$.

Conjecturally (BSD Conjecture) $L(E_n, 1) = 0 \Rightarrow E_n(\mathbb{Q})$ is infinite.

We thus have:

n is a congruent number $\Leftrightarrow E_n : y^2 = x^3 - n^2x$; $E_n(\mathbb{Q})$ is infinite

$\Rightarrow L(E_n, 1) = 0$.

Conjecturally (BSD Conjecture) $L(E_n, 1) = 0 \Rightarrow E_n(\mathbb{Q})$ is infinite.

Finally, $L(E_n, 1) = 0 \Leftrightarrow a(n) = 0$ for n odd or $b(n/2) = 0$ for n even.

If $a(n) + b(n/2) = 0$, then n is congruent.

$$a(n) + b(n/2) = 0 \Rightarrow L(E_n, 1) = 0.$$

$B - SD$ **conjecture:** $L(E_n, 1) = 0 \Rightarrow E_n(\mathbb{Q})$ is infinite.

If $a(n) + b(n/2) = 0$*, then* n *is congruent.*

$$a(n) + b(n/2) = 0 \Rightarrow L(E_n, 1) = 0.$$

$B - SD$ **conjecture:** $L(E_n, 1) = 0 \Rightarrow E_n(\mathbb{Q})$ is infinite.

Beauty of this result:

If $a(n) + b(n/2) = 0$*, then* n *is congruent.*

$$a(n) + b(n/2) = 0 \Rightarrow L(E_n, 1) = 0.$$

$B - SD$ **conjecture:** $L(E_n, 1) = 0 \Rightarrow E_n(\mathbb{Q})$ is infinite.

Beauty of this result:

Conjecturally it reduces the problem of determining if n is congruent to an algebraic computation involving in finitely many steps ($\sim n^{3/2}$ steps).

Unconditional Results

p prime.

- $p \equiv 3 \bmod 8$, then p is not congruent.

$$(a(p) \neq 0; \text{ e.g. } 43, 443, \ldots)$$

Unconditional Results

p prime.

- $p \equiv 3 \bmod 8$, then p is not congruent.

$$(a(p) \neq 0; \quad \text{e.g.} \quad 43, 443, \ldots)$$

- $n \equiv 1$ mod 8, some n of this form not congruent.

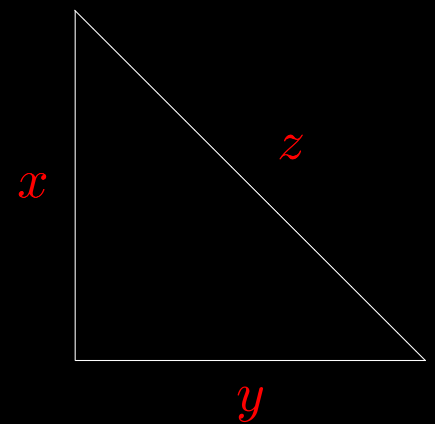
E.g.: $57, 489 \ (a(n) \neq 0)$.

- p, q primes $\equiv 5 \bmod 8$; then $2pq$ is not congruent.

$$(b(pq) \equiv 4 \bmod 8). \quad \text{eg. } 754; (754 = 2.13.29).$$

- Eg: 157 is a congruent number.

Simplest Rational triangle with Area 157 (Computed by D. Zagier).



$$x = \frac{6803298487826435051217540}{411340519227716149383203}$$

$$y = \frac{411340519227716143983203}{2166555693714761309610}$$

$$z = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

I hope I have succeeded in convincing you that deep, intricate and mysterious connections exist in number theory between simply stated problems and areas at the frontier of Modern Research.

Iwasawa theory

This is a theory which provides us an effective tool towards attacking the Birch-Swinnerton Dyer Conjecture.

Iwasawa theory

This is a theory which provides us an effective tool towards attacking the Birch-Swinnerton Dyer Conjecture.

- Unfortunately, even the basic philosophy and ideas in this theory require a sophisticated knowledge and background of mathematics.

Iwasawa theory

This is a theory which provides us an effective tool towards attacking the Birch-Swinnerton Dyer Conjecture.

- Unfortunately, even the basic philosophy and ideas in this theory require a sophisticated knowledge and background of mathematics.

- One of its spectacular applications is in the work of Coates-Wiles stated above.

- My own work focuses on Non-commutative Iwasawa theory. This is a relatively young area of research, classical Iwasawa theory mainly dealt with commutative structures.