Elliptic Curves.

Number theory is concerned with the study of the mysterious and hidden properties of the most basic mathematical objects, namely the integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$$

and the rational numbers

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z} \text{ & } n \neq 0 \right\}.$$

Elliptic curves are the first non-trivial (they are of "genus 1") examples of curves, e.g.

$$E_1 : y^2 = x^3 - x$$

$$E_2 : y^2 + y = x^3 + x^2 + x$$

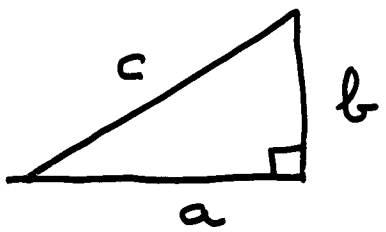
In my lecture today, I want to explain to you why these two elliptic curves have utterly mysterious number-theoretic properties, which we strongly believe to be true, but which we still cannot prove today. In fact, we will be illustrating a conjecture which we believe to be true for all elliptic curves, and even, in some form, for a vast

of other algebraic varieties and their avatars (which the pure mathematicians like to call motives). But the first of these curves is of great importance historically, and the second illustrates a parallel phenomenon which has just been discovered.

The oldest unsolved problem in mathematics.

Historically, it is a problem about right-angled triangles, but as I shall explain later it is really a problem about the elliptic curve E_1. It can be traced back at least to the 10th century in Arab manuscripts (Al-Kazin), but it is possibly much older. In the 17th century, Fermat gave a wonderful proof of the first special case of the problem. It also led him to his Last Theorem (now solved by Andrew Wiles). But the general form of the original problem remains unsolved, despite the fact that conjecturally there is a very beautiful and mysterious answer to it. I want to stress the mystery of this conjectural answer, and then discuss a similar mystery for the curve E_2.

Pythagoras' theorem.

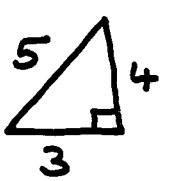


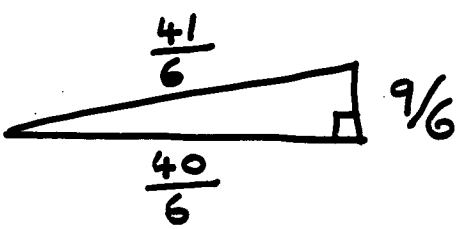
$$c^2 = a^2 + b^2.$$

The discovery of this theorem led inexorably to the introduction of irrational numbers, e.g. $a = b = 1$, $c = \sqrt{2}$ is irrational.

Defn. We say a right-angled triangle Δ is rational if all three lengths a, b, c are rational numbers.

e.g.





Now suppose we fix an integer $N \geq 1$. Clearly there then exist infinitely many right-angled triangles Δ such that

$$\text{Area}(\Delta) = \frac{1}{2}ab = N$$

(choose any two rational numbers a, b with $ab = 2N$ and solve for c from $c^2 = a^2 + b^2$).

Key Question. Does there exist a rational Δ with $\text{Area}(\Delta) = N$?

Classic example of an arithmetic (or diophantine) problem. It has a trivial answer if we drop the hypothesis that Δ is rational.

Arab mathematicians (and possibly other mathematicians earlier in Asia) made tables of the N with this property.

Defn. We say N is congruent if there exists a rational Δ with $\text{Area}(\Delta) = N$.

The following examples of congruent numbers were found

5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31,
34, 37, 38, 39, 41, 46, 47, ...

This is a table of square free N (N is square free if $N = p_1 \cdots p_n$, where the p_i are distinct prime numbers).

Dilemma of the Ancients. Is 1 congruent?

No one could find a rational Δ with $\text{Area}(\Delta) = 1$. After many false earlier claims (Fibonacci...)

THEOREM (Fermat). 1 is not a congruent number.

Proof is very beautiful, but elementary enough to explain to High School students.

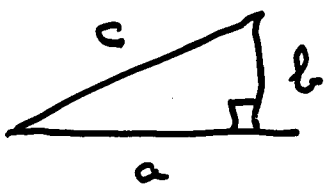
COROLLARY. The equation $x^4 - y^4 = z^2$ has no solution in integers x, y, z with $xyz \neq 0$.

Proof. (Assuming theorem). Suppose there is a solution in integers x, y, z with $xyz \neq 0$.
Put

$$n = x^2, \quad m = y^2.$$

Put

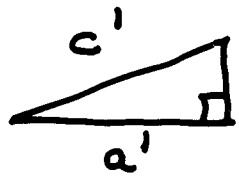
$$a = n^2 - m^2, \quad b = 2nm, \quad c = n^2 + m^2$$



$$a^2 + b^2 = c^2$$

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

$\lambda = xyz$



$$a' = \frac{a}{\lambda}, \quad b' = \frac{b}{\lambda}, \quad c' = \frac{c}{\lambda}.$$

In particular, this shows that the equation

$$x^4 = y^4 + w^4$$

has no solution in integers x, y, w with $xyw \neq 0$.
This is the only written evidence that we have of what led Fermat to his last theorem.
By using similar arguments, other mathematicians proved certain integers were non-congruent :-

Non-congruent square free N

1, 2, 3, 10, 11, 17, 19, 26, 33, 35, 42, 43, ...

Oldest Problem 1. Prove that there is an algorithm for deciding in a finite number of steps whether a given integer N is congruent or not.

Oldest Problem 2. Prove that every square free integer of the form

$$8n+5,\ 8n+6,\ 8n+7 \quad (n=0,1,2,\dots)$$

is congruent.

Solution of these problems is one of the great challenges of number theory, and probably of all of mathematics.

What is perhaps even more surprising is that there is a simple conjectural answer to both problems, which I now want to explain. Define

$$q(T) = T\prod_{n=1}^{\infty}(1-T^{8n})(1-T^{16n})$$

$$\theta_k(T) = 1 + 2\sum_{n=1}^{\infty} T^{2kn^2} \qquad (k=1,2).$$

We simply view these both as formal power series in T with coefficients in $\mathbb{Z}$. We now define two sequence of integers $a(n)$, $b(n)$ $(n=1,2,\dots)$ by the expansions

$$q(T)\theta_1(T) = \sum_{n=1}^{\infty} a(n)T^n$$

$$q(T)\theta_2(T) = \sum_{n=1}^{\infty} b(n)T^n.$$

It is clear that each $a(n)$ and $b(n)$ can be computed in a finite number of steps by the evident algorithm of multiplying the two formal power series. For example, we find:-

$a(1) = 1$	$b(1) = 1$
$a(3) = 2$	$b(3) = 0$
$a(5) = 0$	$b(5) = 2$
$a(11) = -2$	$b(11) = 0$
$a(13) = 0$	$b(13) = -2$
$a(15) = 0$	$b(15) = 0$
$a(17) = -4$	$b(17) = 0$ ...

CONJECTURE (Birch-Swinnerton-Dyer-Tunnell). Let N be any odd square free positive integer. Then

(i) N is congruent $\Leftrightarrow a(N) = 0$;

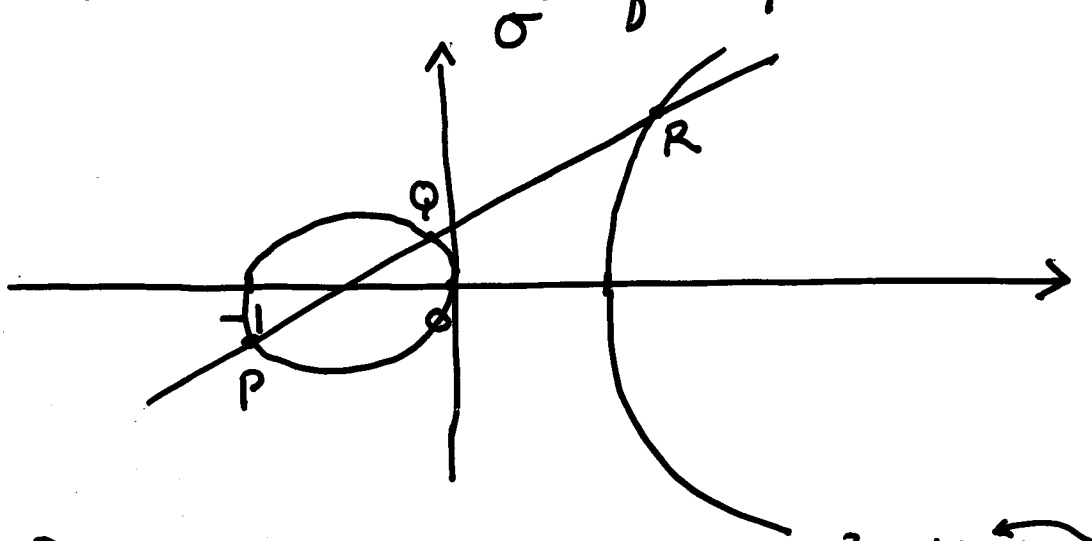
(ii) $2N$ is congruent $\Leftrightarrow b(N) = 0$.

If this conjecture is true, it solves both Oldest problem 1 and Oldest problem 2. One direction of the conjecture is known

THEOREM (C. Wiles). Let N be an odd square free positive integer. If $a(N) \neq 0$, N is not congruent. If $b(N) \neq 0$, then $2N$ is not congruent.

Key question. Where did this mysterious algorithm come from?

In fact, it comes from the fact that there is an elementary link between these problems and the arithmetic of E_1.



$$E_1(\mathbb{C}) = \{(u,v) : u,v \in \mathbb{C} \text{ & } v^2 = u^3 - u\} \cup \{O\}$$ ← point at ∞

$E_1(\mathbb{C})$ has a canonical algebraic group law $\oplus$ (same as the one coming from elliptic integrals) characterized by:-

(i) $P \oplus O = P$ for all P in $E_1(\mathbb{C})$

(ii) $P \oplus Q \oplus R = O$ when P, Q, R are collinear.

$K \subset \mathbb{C}$ any subfield.

$$E_1(K) = \{(u,v) : u,v \in K \text{ & } v^2 = u^3 - u\} \cup \{O\}$$

Fact $E_1(K)$ is always a subgroup of $E_1(\mathbb{C})$.

Inspired by Fermat's proof that 1 is not congruent, Mordell proved the following important result :-

THEOREM (Mordell). For every finite extension field K of $\mathbb{Q}$, $E_1(K)$ is a finitely generated abelian group.

Hence, by the structure theorem for finitely generated abelian groups,

$$E_1(K) \xrightarrow{\sim} \mathbb{Z}^{g_K} \oplus B_K,$$

where $g_K \geq 0$ and B_K is a finite group. In particular,

$$E_1(K) \text{ is infinite} \iff g_K > 0.$$

What has this got do with the congruent number problem? We have the following elementary lemma :-

LEMMA. (i) 1 is congruent $\iff$ $E_1(\mathbb{Q})$ is infinite.
(ii) If $N > 1$ is square free, N is congruent $\iff$ $E_1(\mathbb{Q}(\sqrt{N}))$ is infinite.

$$\mathbb{Q}(\sqrt{N}) = \{a + b\sqrt{N} : a, b \in \mathbb{Q}\}$$

This lemma has one immediate corollary

COROLLARY If there exists one right-angled triangle of area N which is rational, then there exist infinitely many such triangles.

Key Question. How can we decide in a finite number of steps whether $E_1(\mathbb{Q}(\sqrt{N}))$ is infinite.

No algorithm has ever been proven to work, but conjecturally there is a beautiful and mysterious algorithm which should always work. It involves a mathematical object which is far more complicated than those we have considered so far, namely the complex L-function of E_1 over the field $\mathbb{Q}(\sqrt{N})$.

To define this complex L-function, I have to explain a little elementary algebraic number theory. Let J_N be the ring of algebraic integers of $\mathbb{Q}(\sqrt{N})$. In J_N, we only have unique factorization into prime ideals.

Notation. v - a prime ideal of J_N, v divides the rational prime p_v

$k_v = J_N/v$, $\#(k_v) = q_v$.

Defn. m_v = no. of solutions of the congruence

$$y^2 \equiv x^3 - x^4 \bmod v$$

Here we think of x and y as lying in the finite field k_v.

Defn. $a_v = q_v - m_v$.

Defn. The complex L-function of E_1 over $\mathbb{Q}(\sqrt{N})$ is defined by the Euler product

$$L(E_1/\mathbb{Q}(\sqrt{N}), s) = \prod_{v \nmid 2} \left(1 - a_v q_v^{-s} + q_v^{1-2s}\right)^{-1}.$$

This Euler product only converges for $R(s) > \frac{3}{2}$, but an important theorem due to Deuring and Weil tells us that it can be extended to a function which is entire.

CONJECTURE (Birch & Swinnerton-Dyer).

$L(E_1/\mathbb{Q}(\sqrt{N}), s)$ has a zero at $s = 1$ of order exactly $g_{\mathbb{Q}(\sqrt{N})}$ = rank of $E_1(\mathbb{Q}(\sqrt{N}))$.

In particular, $E_1(\mathbb{Q}(\sqrt{N}))$ is infinite $\iff L(E_1/\mathbb{Q}(\sqrt{N}), 1) = 0$.

Philosophically, it seems utterly mysterious that the arithmetic question of how big $E_1(\mathbb{Q}(\sqrt{N}))$ is should be bound up with the order of the zero of $L(E_1/\mathbb{Q}(\sqrt{N}), s)$ at $s = 1$.

But it does explain our earlier algorithm. Tunnell proved that there exists a real number $w_N \neq 0$ such that

$$L(E_1/\mathbb{Q}(\sqrt{N}), 1) = w_N \times \begin{cases} a(N) \text{ if } N \text{ is odd} \\ b(N/2) \text{ if } N \text{ is even} \end{cases}$$

Moreover, like all the L-functions of number theory, $L(E_1/\mathbb{Q}(\sqrt{N}), s)$ has a simple functional equation. Put $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$, and define

$$\Lambda(E_1/\mathbb{Q}(\sqrt{N}), s) = \Gamma_{\mathbb{C}}(s)^2 L(E_1/\mathbb{Q}(\sqrt{N}), s)$$

THEOREM. There exists $\varepsilon_N = \pm 1$ and a real number $A_N > 0$ such that

$$\Lambda(E_1/\mathbb{Q}(\sqrt{N}), s) = \varepsilon_N A_N^s \Lambda(E_1/\mathbb{Q}(\sqrt{N}), 2-s).$$

In particular, $L(E_1/\mathbb{Q}(\sqrt{N}), s)$ has a zero at $s = 1$ of odd multiplicity iff $\varepsilon_N = -1$.

But number theory has a simple alternative way of calculating the sign ε_N. It gives

THEOREM. $\varepsilon_N = +1$ if $N \equiv 1, 2, 3 \bmod 8$ and $\varepsilon_N = -1$ if $N \equiv 5, 6, 7 \bmod 8$.

Thus the phenomenon of all square free N with $N \equiv 5, 6, 7 \bmod 8$ being congruent is at last explained by $L(E_1/\mathbb{Q}(\sqrt{N}), s)$ having a zero of odd multiplicity at $s = 1$.

I now want to end by discussing some related phenomena for the curve

$$E_2 : \quad y^2 + y = x^3 + x^2 + x$$

In fact, Mordell's theorem holds for all elliptic curves, and so we have

THEOREM. For every finite extension K of $\mathbb{Q}$, $E_2(K)$ is a finitely generated abelian group.

$$E_2(K) \cong \mathbb{Z}^{g_K} \oplus B_K.$$

Of course, g_K and B_K depend on the elliptic curve, and will be different for E_1 and E_2.

However, the analogue of Fermat's theorem holds, and we have

$$E_2(\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}.$$

For any finite extension K of $\mathbb{Q}$, we can define analogously the L-function $L(E_2/K, s)$,

$N > 1$ <u>cube</u> free.

$$\mathbb{Q}(\sqrt[3]{N}) = \{a + b\sqrt[3]{N} + c(\sqrt[3]{N})^2 : a, b, c \in \mathbb{Q}\}.$$

It is ~~only~~ known that $L(E_2/\mathbb{Q}(\sqrt[3]{N}), s)$ also has a ~~meromorphic~~ <u>holomorphic</u> continuation to the whole complex plane. This result is already deep, ~~and conjecturally [illegible]~~ The one thing that is easy to do is to compute the <u>sign</u> in its functional equation. By doing this, V. <u>Dokchitser</u>, a student in Cambridge, found the surprising result.

<u>THEOREM</u> (Dokchitser). For <u>every</u> cube free integer $N > 1$, $L(E_2/\mathbb{Q}(\sqrt[3]{N}), s)$ has a zero at $s = 1$ of <u>odd</u> order.

Of course, the conjecture of Birch and Swinnerton-Dyer is made for all elliptic curves.

CHALLENGE. Prove that $E_2(\mathbb{Q}(\sqrt[3]{N}))$ is infinite for every cube free $N > 1$.

Let me end by saying that these are not isolated phenomena, but special cases of rather general behaviour of elliptic curves over fields like $\mathbb{Q}(\sqrt{N})$, $\mathbb{Q}(\sqrt[3]{N})$.