Elliptic curves

LMS Summer School 2023

Lewis Combes

University of Sheffield

Diophantine equations

A **Diophantine equation** is an integer polynomial equation in two or more variables.

Diophantine equations

A **Diophantine equation** is an integer polynomial equation in two or more variables.

The only solutions of a Diophantine equation we care about are *integral* solutions. And sometimes rational solutions.

Diophantine equations

A **Diophantine equation** is an integer polynomial equation in two or more variables.

The only solutions of a Diophantine equation we care about are *integral* solutions. And sometimes rational solutions.

Examples:

- $x^2 + y^2 = z^2$
- $x^3 + y^3 = z^3$
- $x^2 - y^3 = 1$
- $x^3 + (x+1)^3 + (x+2)^3 = y^3$

The simplest Diophantine equation

The simplest Diohpantine equation is the linear equation in two variables:

$$ax + by = c$$

for integers a, b, c.

The simplest Diophantine equation

The simplest Diohpantine equation is the linear equation in two variables:

$$ax + by = c$$

for integers a, b, c. The solutions to this equation can be found by a simple rearrangement:

$$y = \frac{c - ax}{b}.$$

The simplest Diophantine equation

The simplest Diohpantine equation is the linear equation in two variables:

$$ax + by = c$$

for integers a, b, c. The solutions to this equation can be found by a simple rearrangement:

$$y = \frac{c - ax}{b}.$$

The integral solutions to this equation are well-understood. There are infinitely many solutions, or none, depending on the gcd of a, b and whether it divides c.

The next-hardest Diophantine equation

After linear equations, come quadratic equations.

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

The next-hardest Diophantine equation

After linear equations, come quadratic equations.

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Finding the rational solutions to these equations is a solved problem, and uses the *p-adic numbers*.

What is an elliptic curve?

Going up to degree 3, we get equations of the form:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

What is an elliptic curve?

Going up to degree 3, we get equations of the form:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

We can use linear transformations to put this equation in a "standard form":

$$E : y^2 = x^3 + Ax + B,$$

for some $A, B \in \mathbb{Q}$. This is an **elliptic curve**.

Points on elliptic curves

$$E : y^2 = x^3 - 4x + 4$$

Points on E:

$$\begin{aligned}(x, y) &= (-1, \sqrt{7}) \\ &= (-5, \sqrt{-101}) \\ &= \left(\frac{\sqrt[3]{18 - 2\sqrt{33}}}{\sqrt[3]{3}^2} - \frac{\sqrt[3]{2}^5}{\sqrt[3]{27 - 3\sqrt{33}}}, 0 \right) \\ &= (310, 5458)\end{aligned}$$

Rational points on elliptic curves

One again, we care about rational points on these curves. Figuring out whether there are is **hard**.

Rational points on elliptic curves

One again, we care about rational points on these curves. Figuring out whether there are is **hard**.

Example:

$$y^2 = x^3 + x + 29 \rightsquigarrow \text{no rational points}$$
$$y^2 = x^3 + x + 30 \rightsquigarrow 1 \text{ rational point}$$
$$y^2 = x^3 + x + 31 \rightsquigarrow \text{infinitely many rational points}$$

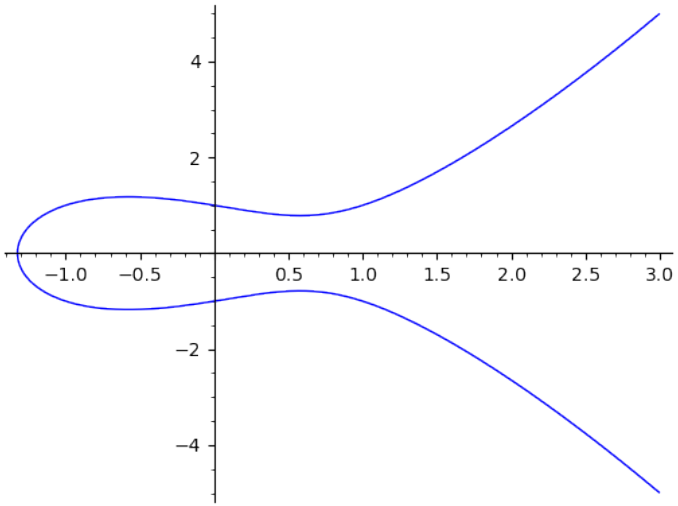
Rational points on elliptic curves

One again, we care about rational points on these curves. Figuring out whether there are is **hard**.

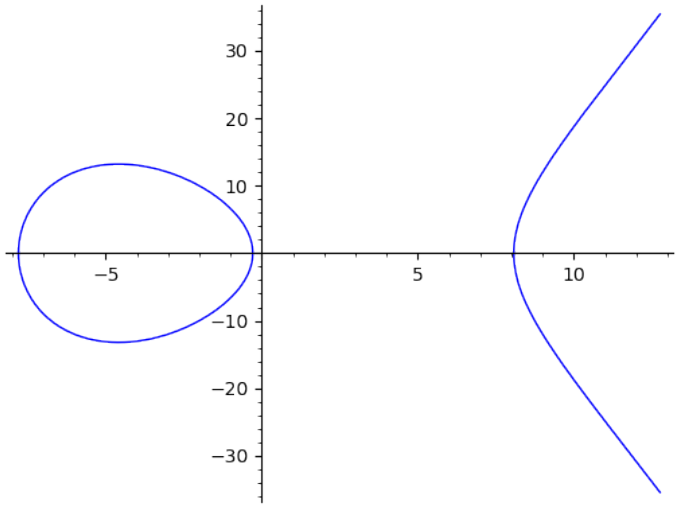
Example:

$$y^2 = x^3 + x + 29 \rightsquigarrow \text{no rational points}$$
$$y^2 = x^3 + x + 30 \rightsquigarrow 1 \text{ rational point}$$
$$y^2 = x^3 + x + 31 \rightsquigarrow \text{infinitely many rational points}$$

There is an algorithm to figure out the exact number of points that always works. Nobody knows if it *does* always work. If you can prove it does, you can claim a \$1,000,000 prize from the Clay Institute.



(a) $y^2 = x^3 - x + 1$



(b) $y^2 = x^3 - 63x - 18$

Figure: Elliptic curve pictures borrowed from the LMFDB.

The first elliptic curve

Diophantus of Alexandria wrote *Arithmetica* around 200AD. It consisted of many problems that we would recognise as Diophantine equations.

One such problem invites the reader: *"to divide a given number into two numbers such that their product is a cube minus its side."*

$$Y(a - Y) = X^3 - X.$$

The first elliptic curve

Diophantus of Alexandria wrote *Arithmetica* around 200AD. It consisted of many problems that we would recognise as Diophantine equations.

One such problem invites the reader: *"to divide a given number into two numbers such that their product is a cube minus its side."*

$$Y(a - Y) = X^3 - X.$$

Diophantus went on to find solutions in the case of $a = 6$:

$$6Y - Y^2 = X^3 - X.$$

Can you spot any easy ones?

The first elliptic curve (cont.)

$$E : 6Y - Y^2 = X^3 - X.$$

Easiest solution: $(X, Y) = (0, 0)$.

The first elliptic curve (cont.)

$$E : 6Y - Y^2 = X^3 - X.$$

Easiest solution: $(X, Y) = (0, 0)$.

Unsatisfying to us, and probably Diophantus too. Ancient Greek mathematics was concerned with real quantities. Negatives and zeros were generally understood to be ignored as "less interesting".

The first elliptic curve (cont.)

$$E : 6Y - Y^2 = X^3 - X.$$

Easiest solution: $(X, Y) = (0, 0)$.

Unsatisfying to us, and probably Diophantus too. Ancient Greek mathematics was concerned with real quantities. Negatives and zeros were generally understood to be ignored as "less interesting".

Another easy(ish) solution: $(X, Y) = (1, 6)$.

The first elliptic curve (cont.)

$$E : 6Y - Y^2 = X^3 - X.$$

Easiest solution: $(X, Y) = (0, 0)$.

Unsatisfying to us, and probably Diophantus too. Ancient Greek mathematics was concerned with real quantities. Negatives and zeros were generally understood to be ignored as "less interesting".

Another easy(ish) solution: $(X, Y) = (1, 6)$.

Less-obvious solution: $(X, Y) = \left(\frac{664}{169}, -\frac{11220}{2197}\right)$.

The first elliptic curve (cont.)

$$E : 6Y - Y^2 = X^3 - X.$$

Easiest solution: $(X, Y) = (0, 0)$.

Unsatisfying to us, and probably Diophantus too. Ancient Greek mathematics was concerned with real quantities. Negatives and zeros were generally understood to be ignored as "less interesting".

Another easy(ish) solution: $(X, Y) = (1, 6)$.

Less-obvious solution: $(X, Y) = \left(\frac{664}{169}, -\frac{11220}{2197}\right)$.

A non-obvious solution: $(X, Y) = \left(-\frac{10370209823}{214448643396}, -\frac{797444260812577}{99308164475680056}\right)$.

The first elliptic curve (cont.)

Clearly something mysterious going on. Diophantus himself produced the solution

$$(X, Y) = \left(\tfrac{17}{9}, \tfrac{26}{27}\right).$$

He does so using **the group law** on the elliptic curve.

The first elliptic curve (cont.)

Clearly something mysterious going on. Diophantus himself produced the solution

$$(X, Y) = \left(\tfrac{17}{9}, \tfrac{26}{27}\right).$$

He does so using **the group law** on the elliptic curve.

A **group** is a set G with a binary operation $\cdot$ such that

1. For all $g, h \in G$, one has $g \cdot h \in G$
2. There is a distinguished element Id_G such that $g \cdot \mathrm{Id}_G = \mathrm{Id}_G \cdot g = g$ for all $g \in G$.
3. For every $g \in G$, there is a $g^{-1} \in G$ such that $g \cdot g^{-1} = \mathrm{Id}_G$.
4. The operation $\cdot$ is **associative**—i.e. $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.

The first elliptic curve (cont.)

Clearly something mysterious going on. Diophantus himself produced the solution

$$(X, Y) = \left(\tfrac{17}{9}, \tfrac{26}{27}\right).$$

He does so using **the group law** on the elliptic curve.

A **group** is a set G with a binary operation $\cdot$ such that

1. For all $g, h \in G$, one has $g \cdot h \in G$
2. There is a distinguished element Id_G such that $g \cdot \mathrm{Id}_G = \mathrm{Id}_G \cdot g = g$ for all $g \in G$.
3. For every $g \in G$, there is a $g^{-1} \in G$ such that $g \cdot g^{-1} = \mathrm{Id}_G$.
4. The operation $\cdot$ is **associative**—i.e. $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.

The group law on elliptic curves

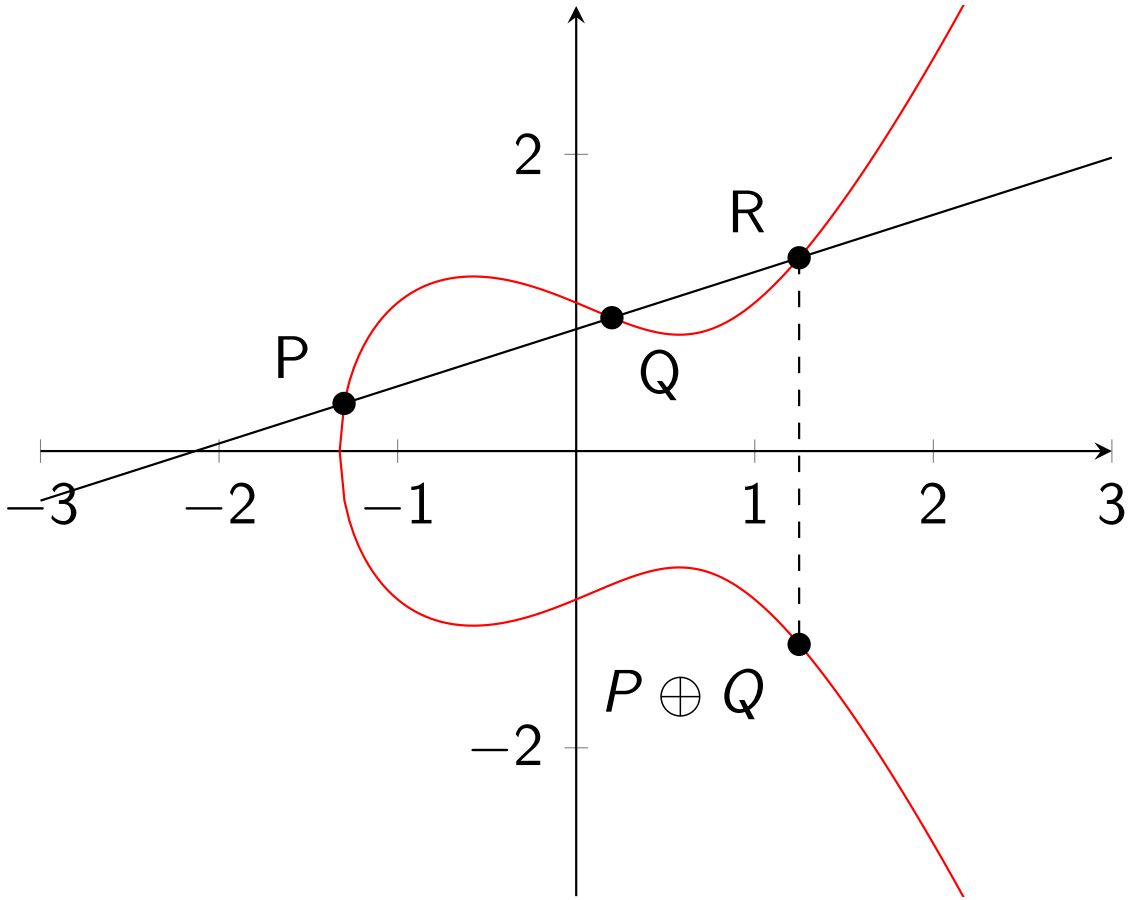


Figure: Elliptic Curve addition.

The group law on elliptic curves (cont.)

Diophantus used the group law (though he did not know it) to produce his solution $(X, Y) = \left(\frac{17}{9}, \frac{26}{27}\right)$ to $E : 6Y - Y^2 = X^3 - X$.

The group law on elliptic curves (cont.)

Diophantus used the group law (though he did not know it) to produce his solution $(X, Y) = \left(\frac{17}{9}, \frac{26}{27}\right)$ to $E : 6Y - Y^2 = X^3 - X$.

Starting with the simpler solution $P = (-1, 6)$, one can use the group law by adding P to itself to get a new solution.

The group law on elliptic curves (cont.)

Diophantus used the group law (though he did not know it) to produce his solution $(X, Y) = \left(\frac{17}{9}, \frac{26}{27}\right)$ to $E : 6Y - Y^2 = X^3 - X$.

Starting with the simpler solution $P = (-1, 6)$, one can use the group law by adding P to itself to get a new solution.

It is a long and tedious calculation.

```
> E;
Elliptic Curve defined by y^2 - 6*y = x^3 - x over Rational Field
> P:=RationalPoints(E : Bound:=50)[6];
> P;
(1 : 6 : 1)
> time P+P;
(-17/9 : 26/27 : 1)
Time: 0.000
>
```

So what?

The group law on elliptic curves is **special**. A random curve is very unlikely to have a group law. This makes studying elliptic curves somewhat feasible, relative to curves defined by polynomials of higher degree.

So what?

The group law on elliptic curves is **special**. A random curve is very unlikely to have a group law. This makes studying elliptic curves somewhat feasible, relative to curves defined by polynomials of higher degree.

Points on an elliptic curve E have the structure of a **finitely-generated abelian group**.

So what?

The group law on elliptic curves is **special**. A random curve is very unlikely to have a group law. This makes studying elliptic curves somewhat feasible, relative to curves defined by polynomials of higher degree.

Points on an elliptic curve E have the structure of a **finitely-generated abelian group**. The group of rational points, written $E(\mathbb{Q})$, takes the special form

$$E(\mathbb{Q}) \simeq T + \mathbb{Z}^r.$$

Two parts:

- T: finite subgroup of **torsion points**,
- r: the number of independent generators of infinite order, called the **rank.**

The mysterious rank

The torsion subgroup T is well-understood. In fact, it has been classified exactly. There are only 15 possible groups T can be.

The rank is much more mysterious.

$$y^2 = x^3 + x + 29 \rightsquigarrow \text{no rational points}$$
$$y^2 = x^3 + x + 30 \rightsquigarrow 1 \text{ rational point}$$
$$y^2 = x^3 + x + 31 \rightsquigarrow \text{infinitely many rational points}$$

The mysterious rank

The torsion subgroup T is well-understood. In fact, it has been classified exactly. There are only 15 possible groups T can be.

The rank is much more mysterious.

$$y^2 = x^3 + x + 29 \rightsquigarrow r = 0 \ \& \ T = C_1$$
$$y^2 = x^3 + x + 30 \rightsquigarrow r = 0 \ \& \ T = C_2$$
$$y^2 = x^3 + x + 31 \rightsquigarrow r = 1 \ \& \ T = C_1$$

Birch and Swinnerton-Dyer's conjecture

In the year 2000, the Clay Institute issued a list of seven **Millenium Prize Problems**. The Birch and Swinnerton-Dyer conjecture is one of these problems.

Birch and Swinnerton-Dyer's conjecture

In the year 2000, the Clay Institute issued a list of seven **Millenium Prize Problems**. The Birch and Swinnerton-Dyer conjecture is one of these problems.

BSD describes exactly how to find the rank of an elliptic curve E. It is one of the first major conjectures in number theory to arise from large-scale computer calculations.

Birch and Swinnerton-Dyer's conjecture

In the year 2000, the Clay Institute issued a list of seven **Millenium Prize Problems**. The Birch and Swinnerton-Dyer conjecture is one of these problems.

BSD describes exactly how to find the rank of an elliptic curve E. It is one of the first major conjectures in number theory to arise from large-scale computer calculations.

Fundamental idea: look at the elliptic curves modulo prime numbers.

Birch and Swinnerton-Dyer's conjecture

In the year 2000, the Clay Institute issued a list of seven **Millenium Prize Problems**. The Birch and Swinnerton-Dyer conjecture is one of these problems.

BSD describes exactly how to find the rank of an elliptic curve E. It is one of the first major conjectures in number theory to arise from large-scale computer calculations.

Fundamental idea: look at the elliptic curves modulo prime numbers.

It is **not enough** to find points on a curve mod p and lift them to $\mathbb{Q}$.

Birch and Swinnerton Dyer's conjecture (cont.)

However, it is still worth a try.

Principle: if an elliptic curve has rank > 0, it has "lots of points", so it should still have "lots of points" $(\mathrm{mod}\ p)$.

Birch and Swinnerton Dyer's conjecture (cont.)

However, it is still worth a try.

Principle: if an elliptic curve has rank > 0, it has "lots of points", so it should still have "lots of points" $(\mathrm{mod}\ p)$.

Birch and Swinnerton-Dyer developed the conjecture in the 1960s.

(c) Birch and Swinnerton-Dyer

(d) Computers in the 1960s

Elliptic curves over $\mathbb{F}_p$

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$$E : y^2 = x^3 - x + 9$$

Let $p = 5$. A **point on E over $\mathbb{F}_5$** is a pair $(x, y) \in \mathbb{F}_p^2$ satisfying E.

Elliptic curves over $\mathbb{F}_p$

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$$E : y^2 = x^3 - x + 9$$

Let $p = 5$. A **point on E over $\mathbb{F}_5$** is a pair $(x, y) \in \mathbb{F}_p^2$ satisfying E.

E.g. $(x, y) = (4, 2)$.

Hasse-Weil bound tell us

$$-2\sqrt{p} + p + 1 \leq \#E(\mathbb{F}_p) \leq 2\sqrt{p} + p + 1.$$

or, if you prefer,

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}.$$

BSD example

The original statement of the conjecture is the following:

$$\prod_{p \leq X} \frac{\#E(\mathbb{F}_p)}{p} \approx C \log(X)^{\mathrm{rank}(E)}$$

as $X \to \infty$. Here C is some constant.

BSD example

The original statement of the conjecture is the following:

$$\prod_{p \leq X} \frac{\#E(\mathbb{F}_p)}{p} \approx C \log(X)^{\mathrm{rank}(E)}$$

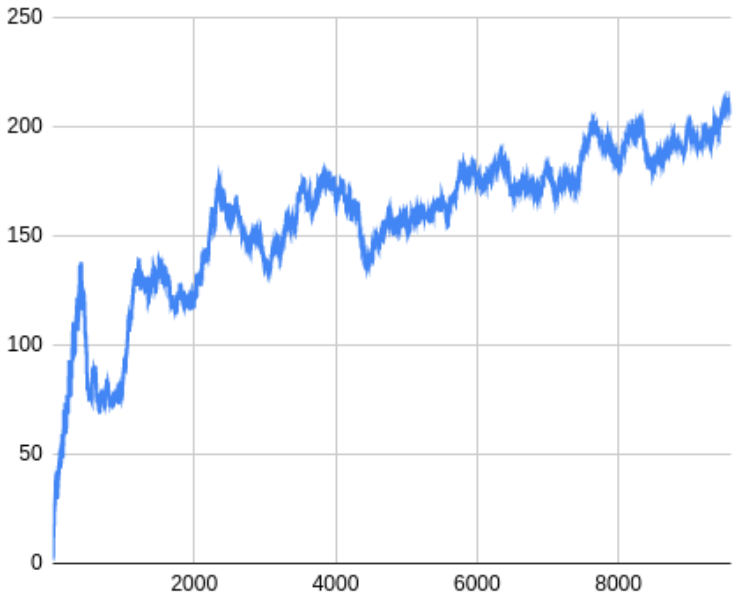
as $X \to \infty$. Here C is some constant.

E.g. $E_1 : y^2 = x^3 - x + 9$, and $E_2 : y^2 = x^3 - x + 5$.

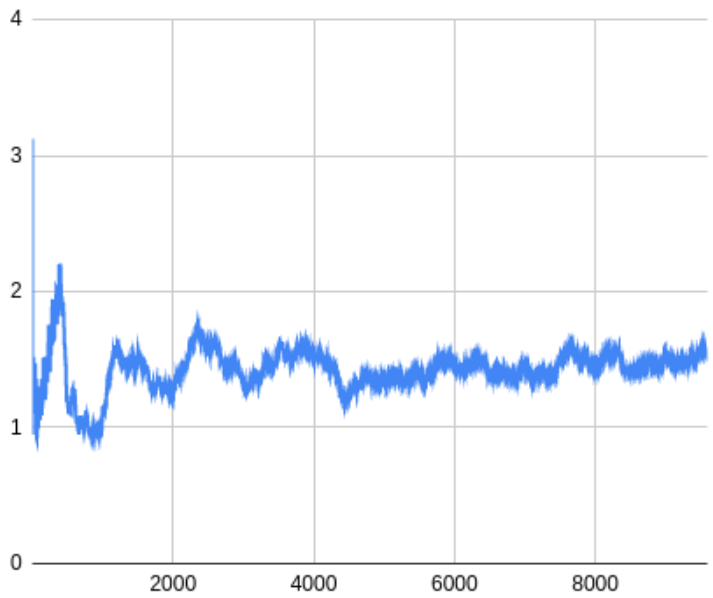
p	2	3	5	7	11	13	17	19	23	29	31	37
$\#E_1(\mathbb{F}_p)$	3	4	8	9	16	15	24	16	32	36	37	39
$\#E_2(\mathbb{F}_p)$	3	1	8	7	13	10	17	20	18	36	30	32

Which one of these curves "should" have rank > 0?

BSD example (cont.)

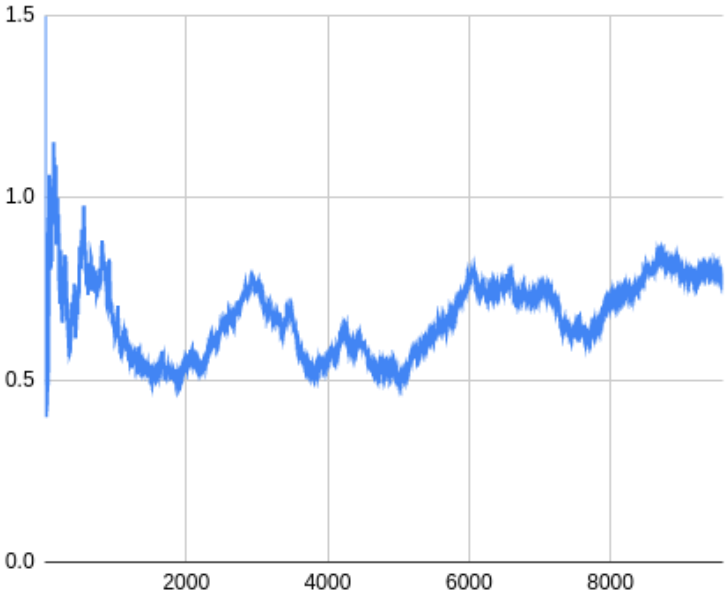


(e) $\prod_{n \leq X} \frac{\#E_1(\mathbb{F}_p)}{p}$

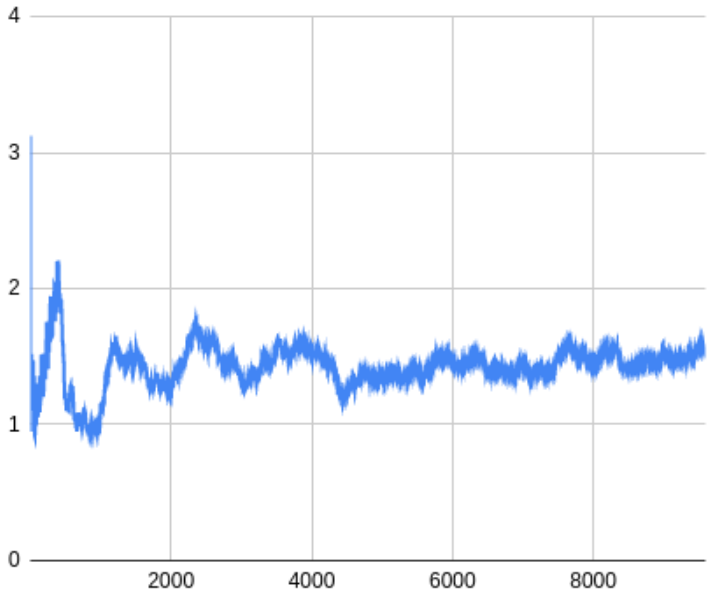


(f) $\prod_{n \leq X} \frac{\#E_2(\mathbb{F}_p)}{p}$

BSD example (cont.)



(k) $\frac{1}{\log(X)^2} \prod_{n \leq X} \frac{\#E_1(\mathbb{F}_p)}{p}$



(l) $\prod_{n \leq X} \frac{\#E_2(\mathbb{F}_p)}{p}$

Current state of BSD

Combining the work of Coates & Wiles, Gross & Zagier, Kolyvagin, Wiles, Taylor & Wiles and Breuil-Conrad-Diamond-Taylor, one has the following:

Theorem (due to everyone above + more)

BSD is true for all elliptic curves of rank 0 and rank 1.

Current state of BSD

Combining the work of Coates & Wiles, Gross & Zagier, Kolyvagin, Wiles, Taylor & Wiles and Breuil-Conrad-Diamond-Taylor, one has the following:

Theorem (due to everyone above + more)

BSD is true for all elliptic curves of rank 0 and rank 1.

For ranks ≥ 2, nothing is known. We can't even provably *verify* the conjecture for ranks ≥ 4.

Current state of BSD

Combining the work of Coates & Wiles, Gross & Zagier, Kolyvagin, Wiles, Taylor & Wiles and Breuil-Conrad-Diamond-Taylor, one has the following:

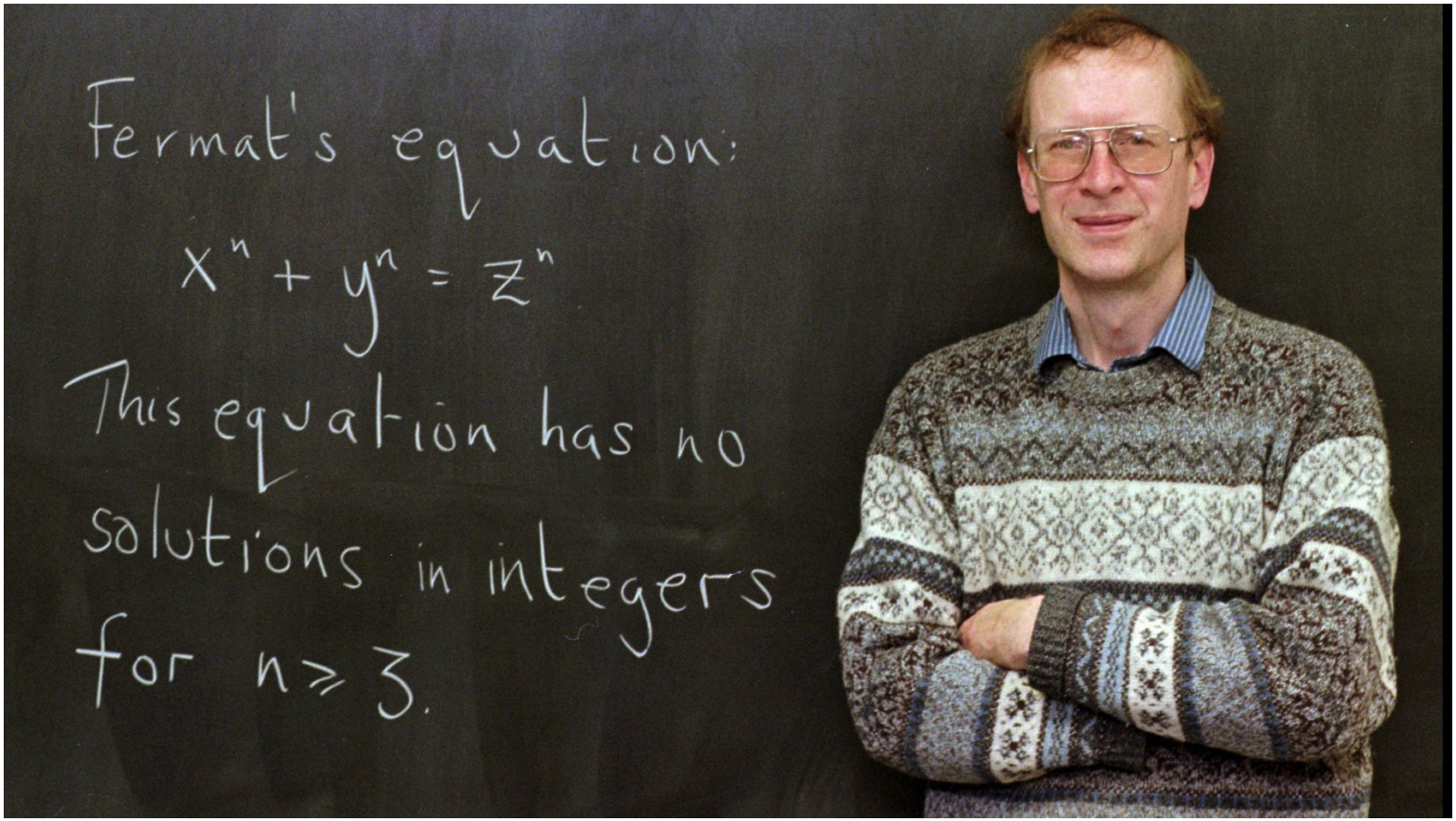
Theorem (due to everyone above + more)

BSD is true for all elliptic curves of rank 0 and rank 1.

For ranks ≥ 2, nothing is known. We can't even provably *verify* the conjecture for ranks ≥ 4.

The Clay Institute's \$1,000,000 is still waiting to be claimed...

Fermat's Last Theorem



Fermat's Last Theorem (cont.)

Wiles' strategy: start with an assumed solution $a^p + b^p = c^p$ for a prime p. Use this to create an elliptic curve

$$E : y^2 = x(x - a^p)(x + b^p)$$

called a **Frey curve**.

Fermat's Last Theorem (cont.)

Wiles' strategy: start with an assumed solution $a^p + b^p = c^p$ for a prime p. Use this to create an elliptic curve

$$E : y^2 = x(x - a^p)(x + b^p)$$

called a **Frey curve**.

Because $a, b, c \in \mathbb{Z}$, the curve E ends up having very special properties.

Fermat's Last Theorem (cont.)

Wiles' strategy: start with an assumed solution $a^p + b^p = c^p$ for a prime p. Use this to create an elliptic curve

$$E : y^2 = x(x - a^p)(x + b^p)$$

called a **Frey curve**.

Because $a, b, c \in \mathbb{Z}$, the curve E ends up having very special properties.

In particular, it cannot be **modular**. Wiles proved that all* elliptic curves *are* modular, so the solution leads to a curve that can't exist.