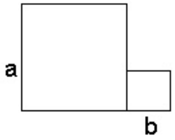
Beyond Fermat's Last Theorem

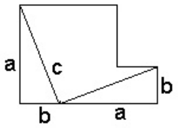
David Zureick-Brown

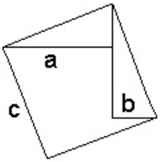
Emory University

Wake Forest University, Colloquium

$$\boxed{a^2 + b^2 = c^2}$$







Basic Problem (Solving Diophantine Equations)

Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$ be polynomials and let R be a ring (e.g., $R = \mathbb{Z}, \mathbb{Q}$).

Problem

Describe the set

$$\left\{(a_1, \ldots, a_n) \in R^n : \forall i, f_i(a_1, \ldots, a_n) = 0\right\}.$$

Basic Problem (Solving Diophantine Equations)

Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$ be polynomials and let R be a ring (e.g., $R = \mathbb{Z}$, $\mathbb{Q}$).

Problem

Describe the set

$$\left\{(a_1, \ldots, a_n) \in R^n : \forall i, f_i(a_1, \ldots, a_n) = 0\right\}.$$

Fact

Solving diophantine equations is hard.

Hilbert's Tenth Problem

The ring $R = \mathbb{Z}$ is especially hard.

Hilbert's Tenth Problem

The ring $R = \mathbb{Z}$ is especially hard.

Theorem (Davis-Putnam-Robinson 1961, Matijasevič 1970)

There does not exist an algorithm solving the following problem:

input: $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$;

output: YES / NO *according to whether the set*

$$\left\{(a_1, \ldots, a_n) \in \mathbb{Z}^n : \forall i, f_i(a_1, \ldots, a_n) = 0\right\}$$

is non-empty.

Hilbert's Tenth Problem

The ring $R = \mathbb{Z}$ is especially hard.

Theorem (Davis-Putnam-Robinson 1961, Matijasevič 1970)

There does not exist an algorithm solving the following problem:

input: $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$;

output: YES / NO *according to whether the set*

$$\left\{(a_1, \ldots, a_n) \in \mathbb{Z}^n : \forall i, f_i(a_1, \ldots, a_n) = 0\right\}$$

is non-empty.

This is *still open* for many other rings (e.g., $R = \mathbb{Q}$).

Fermat's Last Theorem

Theorem (Wiles et. al)

The only solutions to the equation

$$x^n + y^n = z^n, n \geq 3$$

are multiples of the triples

$$(0,0,0), \quad (\pm 1, \mp 1, 0), \quad \pm(1,0,1), \quad (0, \pm 1, \pm 1).$$

Fermat's Last Theorem

Theorem (Wiles et. al)

The only solutions to the equation

$$x^n + y^n = z^n, n \geq 3$$

are multiples of the triples

$$(0,0,0), \quad (\pm 1, \mp 1, 0), \quad \pm(1,0,1), \quad (0, \pm 1, \pm 1).$$

This took 300 years to prove!

Fermat's Last Theorem

Theorem (Wiles et. al)

The only solutions to the equation

$$x^n + y^n = z^n, n \geq 3$$

are multiples of the triples

$$(0,0,0), \quad (\pm 1, \mp 1, 0), \quad \pm(1,0,1), \quad (0, \pm 1, \pm 1).$$

This took 300 years to prove!

Template for the proof of FLT

Step 1: Assume there is a counterexample $a^p + b^p = c^p$.

Step 2: (Frey) Build an elliptic curve with strange properties:

$$E_{(a,b,c)} \colon y^2 = x(x - a^p)(x + b^p)$$
$$j = \frac{2^8 \left(c^{2p} - a^p b^p\right)^3}{(abc)^{2p}}$$
$$\Delta = 2^{-8}(abc)^{2p}.$$

Step 3: (Ribet) Show that the Frey curve $E_{(a,b,c)}$ is not modular.

Step 4: Prove that every elliptic curve over $\mathbb{Q}$ is modular.

Modularity is now a theorem

Theorem (Wiles 1995; Breuil-Conrad-Diamond-Taylor 2002)

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

Basic Problem: $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$

- **Qualitative**:
  - Does there exist a solution?
  - Do there exist infinitely many solutions?
  - Does the set of solutions have some extra structure (e.g., geometric structure, group structure).

Basic Problem: $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$

- **Qualitative**:
  - Does there exist a solution?
  - Do there exist infinitely many solutions?
  - Does the set of solutions have some extra structure (e.g., geometric structure, group structure).
- **Quantitative**
  - How many solutions are there?
  - How large is the smallest solution?
  - How can we explicty find all solutions (and prove that we have them all)?

Basic Problem: $f_1, \ldots, f_m \in \mathbb{Z}[x_1, ..., x_n]$

- **Qualitative**:
  - Does there exist a solution?
  - Do there exist infinitely many solutions?
  - Does the set of solutions have some extra structure (e.g., geometric structure, group structure).
- **Quantitative**
  - How many solutions are there?
  - How large is the smallest solution?
  - How can we expliclty find all solutions (and prove that we have them all)?
- **Implicit question**
  - Why do equations have (or fail to have) solutions?
  - Why do some have many and some have none?
  - What underlying mathematical structures control this?

Example: Pythagorean triples

Lemma

The equation

$$x^2 + y^2 = z^2$$

has infinitely many non-zero coprime solutions.

Example: Pythagorean triples

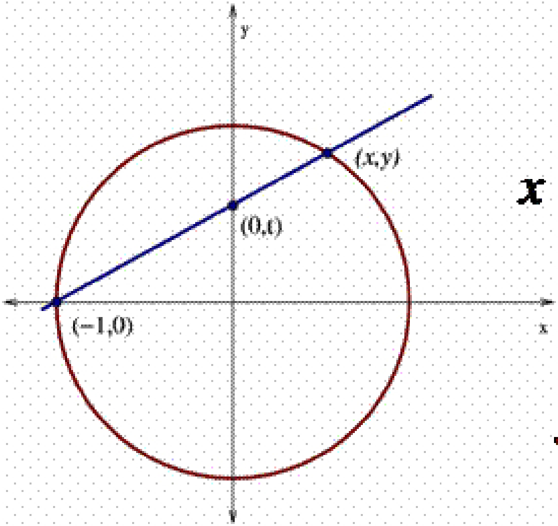
Lemma

The equation

$$x^2 + y^2 = z^2$$

has infinitely many non-zero coprime solutions.

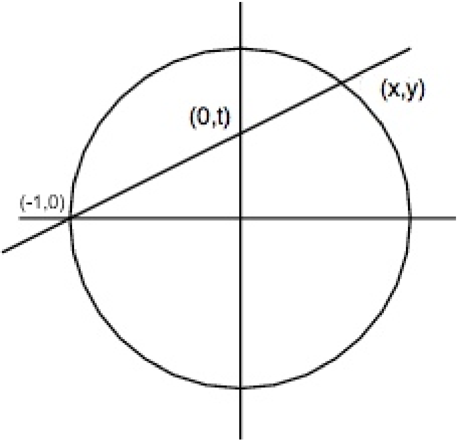
Lets work this out in detail.



$$x = \frac{a}{c} \qquad y = \frac{b}{c}$$

$$x^2 + y^2 = 1$$

Pythagorean triples



$$\text{Slope} = \quad t = \frac{y}{x+1}$$

$$x = \frac{1-t^2}{1+t^2}$$

$$y = \frac{2t}{1+t^2}$$

Pythagorean triples

Lemma

The solutions to

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

are all multiples of the triples

$$\boxed{a = 1 - t^2} \quad \boxed{b = 2t} \quad \boxed{c = 1 + t^2}$$

The Mordell Conjecture

Example

The equation $y^2 - x^2 = 1$ has infinitely many solutions.

The Mordell Conjecture

Example

The equation $y^2 - x^2 = 1$ has infinitely many solutions.

Theorem (Faltings)

For $n \geq 5$, the equation

$$y^2 - x^n = 1$$

has only finitely many solutions.

Fermat Curves

Question

Why is Fermat's last theorem believable?

1. $x^n + y^n - z^n = 0$ looks like a surface (3 variables)
2. $x^n + y^n - 1 = 0$ looks like a curve (2 variables)

Mordell Conjecture

Consider $y^2 = (x^2 - 1)(x^2 - 2)(x^2 - 3)$.

This is a cross section of a torus. The **genus** is the number of holes.

Conjecture (Mordell)

A curve of genus $g \geq 2$ has only finitely many rational solutions.

Fermat Curves

Question

Why is Fermat's last theorem believable?

1. $x^n + y^n - 1 = 0$ is a curve of genus $(n-1)(n-2)/2$.
2. Mordell implies that for **fixed** $n > 3$, the nth Fermat equation has only finitely many solutions.

Fermat Curves

Question

What if $n = 3$?

1. $x^3 + y^3 - 1 = 0$ is a curve of genus $(3-1)(3-2)/2 = 1$.
2. We were lucky; $Ax^3 + By^3 = Cz^3$ can have infinitely many solutions.

Congruent number problem

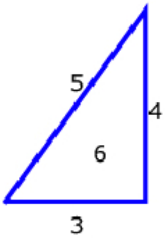
The pair of equations

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

has **infinitely many** solutions. **How large** Is the smallest solution? How many **digits** does the smallest solution have?

Congruent number problem

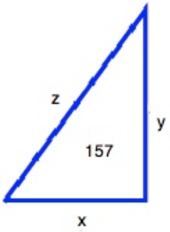
$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 6}$$



$$3^2 + 4^2 = 5^2,\ 3 \cdot 4 = 2 \cdot 6$$

Congruent number problem

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$



Congruent number problem

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

has **infinitely many** solutions. **How large** Is the smallest solution? How many **digits** does the smallest solution have?

Congruent number problem

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

has **infinitely many** solutions. **How large** Is the smallest solution? How many **digits** does the smallest solution have?

$$x = \frac{157841 \cdot 4947203 \cdot 52677109576}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441}$$

$$y = \frac{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 52677109576}$$

$$z = \frac{20085078913 \cdot 1185369214457 \cdot 9425458255024420419074 80}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 52677109576}$$

Congruent number problem

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

has **infinitely many** solutions. **How large** Is the smallest solution? How many **digits** does the smallest solution have?

$$x = \frac{157841 \cdot 4947203 \cdot 52677109576}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441}$$

$$y = \frac{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 52677109576}$$

$$z = \frac{20085078913 \cdot 1185369214457 \cdot 9425458255024420419074801}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 52677109576}$$

The denominator of z has **44 digits**!

Congruent number problem

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

has **infinitely many** solutions. **How large** Is the smallest solution? How many **digits** does the smallest solution have?

$$x = \frac{157841 \cdot 4947203 \cdot 52677109576}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441}$$

$$y = \frac{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 52677109576}$$

$$z = \frac{20085078913 \cdot 1185369214457 \cdot 9425458255024420419074801}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 52677109576}$$

The denominator of z has **44 digits**!
How did anyone ever find this solution?

Congruent number problem

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

has **infinitely many** solutions. **How large** Is the smallest solution? How many **digits** does the smallest solution have?

$$x = \frac{157841 \cdot 4947203 \cdot 52677109576}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441}$$

$$y = \frac{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 52677109576}$$

$$z = \frac{20085078913 \cdot 1185369214457 \cdot 942545825502442041907480}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 52677109576}$$

The denominator of z has **44 digits**!
How did anyone ever find this solution?
"Next" soluton has **176 digits**!

Back of the envelope calculation

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.

Back of the envelope calculation

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.
- Num, den$(x, y, z) \leq 10^{44} \sim 10^{264}$ many, $\mathbf{10^{258}}$ **mins** $=$ $\mathbf{10^{252}}$ **years**.

Back of the envelope calculation

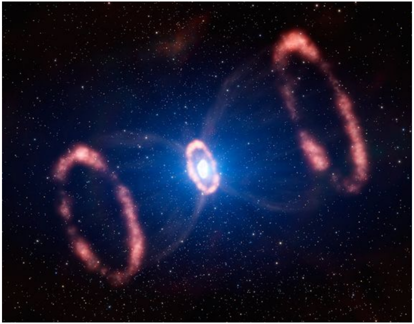
$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.
- Num, den$(x, y, z) \leq 10^{44} \sim 10^{264}$ many, $\mathbf{10^{258}}$ **mins** $=$ $\mathbf{10^{252}}$ **years**.
- 10^9 many computers in the world – so $\mathbf{10^{243}}$ **years**

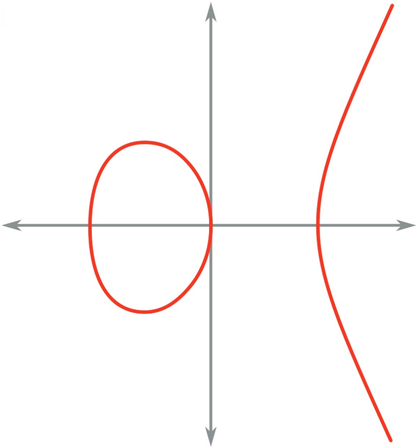
Back of the envelope calculation

$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.
- Num, den$(x, y, z) \leq 10^{44} \sim 10^{264}$ many, $\mathbf{10^{258}}$ **mins** $=$ $\mathbf{10^{252}}$ **years**.
- 10^9 many computers in the world – so $\mathbf{10^{243}}$ **years**
- Expected time of 'heat death' of universe – $\mathbf{10^{100}}$ **years**.

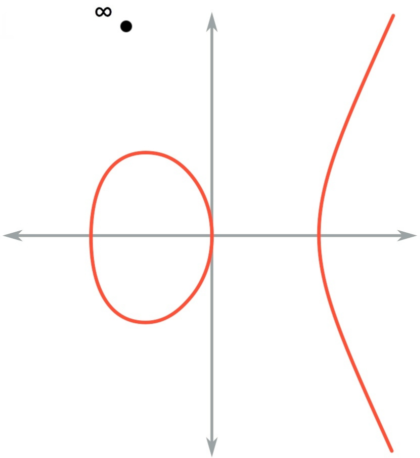


Elliptic Curves



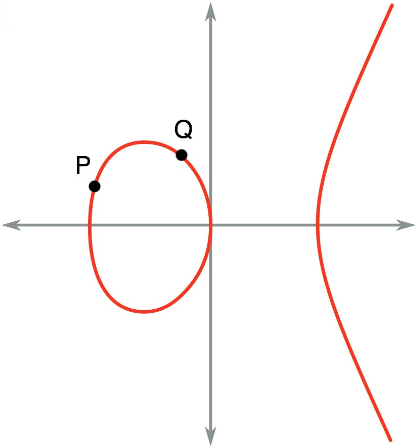
$$E : y^2 = x^3 + ax + b$$

Elliptic Curves - point at infinity



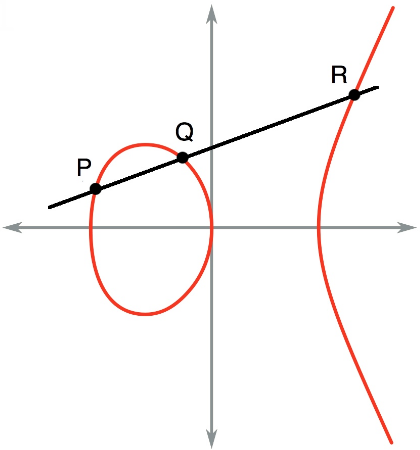
$$E\colon zy^2 = x^3 + axz^2 + bz^3$$
$$\infty = [0 : 1 : 0]$$

Elliptic Curves – addition



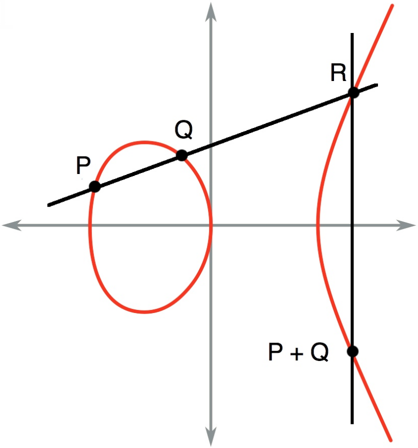
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$Q = (x_1, y_1) \in \mathbb{Q}^2$$

Elliptic Curves – addition

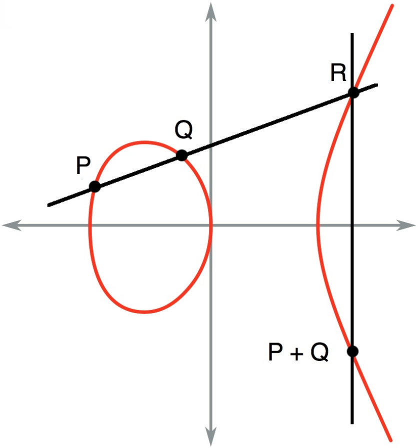


$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$Q = (x_1, y_1) \in \mathbb{Q}^2$$
$$R = (x_2, y_2) \in \mathbb{Q}^2$$

Elliptic Curves – addition



$$E:\ y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$Q = (x_1, y_1) \in \mathbb{Q}^2$$
$$R = (x_2, y_2) \in \mathbb{Q}^2$$
$$P + Q = (x_2, -y_2) \in \mathbb{Q}^2$$

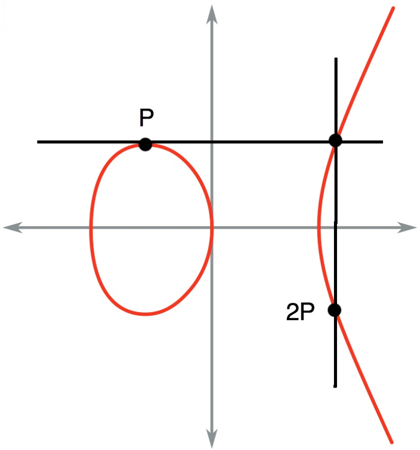


$$E: y^2 = x^3 + ax + b$$

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$$

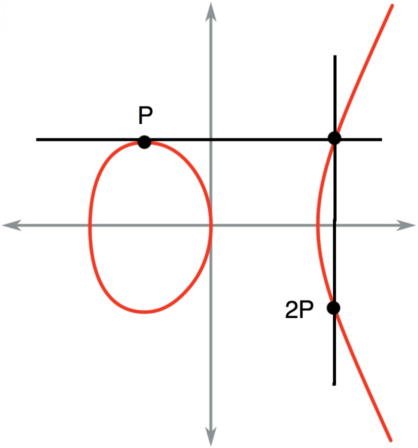
$$(P\ ,\ Q) \quad \mapsto P + Q$$

Elliptic Curves - duplication



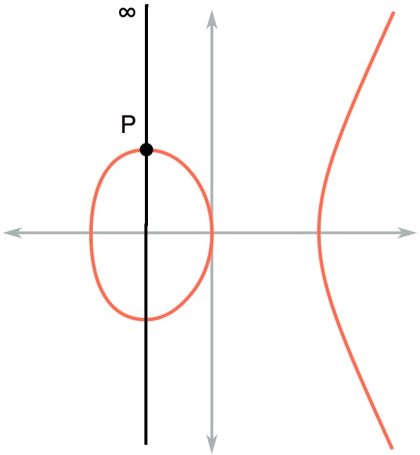
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$

Elliptic Curves - duplication



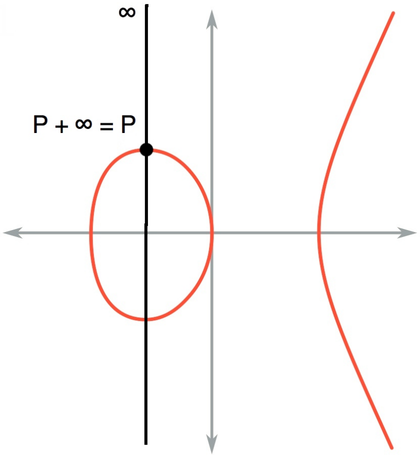
$$E: y^2 = x^3 + ax + b$$
$$P = (x_0, y_0) \in \mathbb{Q}^2$$
$$2P = (x_3, y_3) \in \mathbb{Q}^2$$

Elliptic Curves – identity



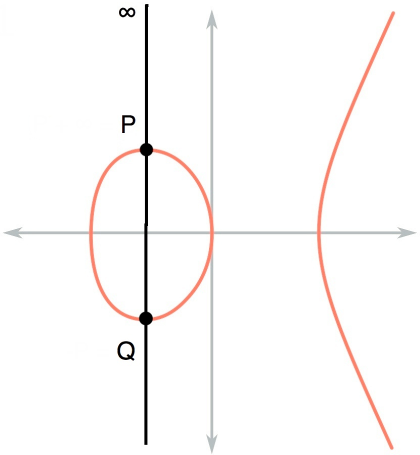
$$E : y^2 = x^3 + ax + b$$

Elliptic Curves – identity



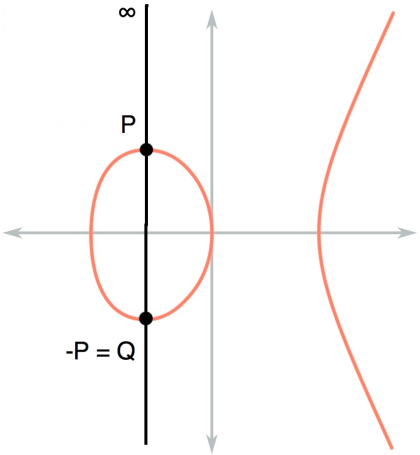
$$E : y^2 = x^3 + ax + b$$

Elliptic Curves – inverses



$$E: y^2 = x^3 + ax + b$$

Elliptic Curves – inverses



$$E: y^2 = x^3 + ax + b$$

Elliptic Curves – torsion subgroup

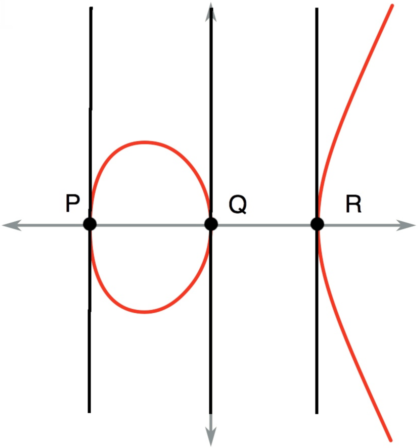
Let $n \in \mathbb{Z}$ be an integer.

Definition

The *n-torsion subgroup* $E[n]$ of E is defined to be

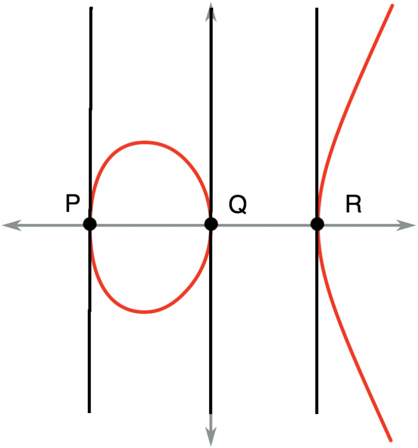
$$\ker\left(E \xrightarrow{[n]} E\right) := \{P \in E : nP := P + \ldots + P = \infty\}.$$

Elliptic Curves – two torsion



$$E\colon y^2 = x^3 + ax + b$$

Elliptic Curves – two torsion



$$E\colon y^2 = x^3 + ax + b$$
$$2P = 2Q = 2R = \infty$$

Fermat Surfaces

Conjecture

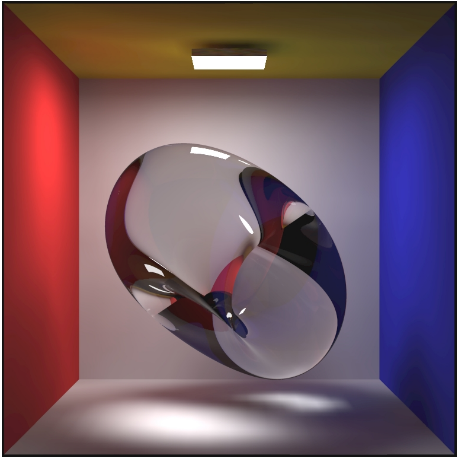
The only solutions to the equation

$$x^n + y^n = z^n + w^n, n \geq 5$$

satisfy $xyzw = 0$ or lie on the lines 'lines' $x = \pm y$, $z = \pm w$ (and permutations).

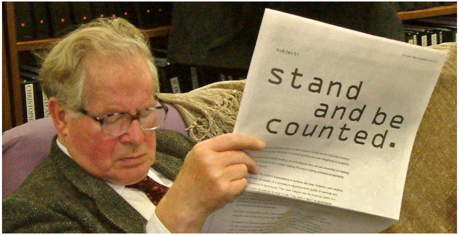
The Swinnerton-Dyer K3 surface

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$



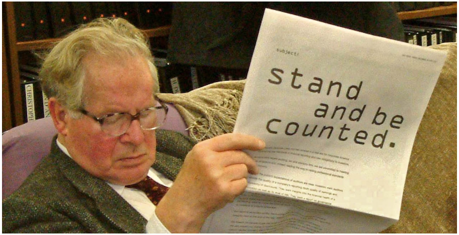
The Swinnerton-Dyer K3 surface

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$



The Swinnerton-Dyer K3 surface

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$



Two 'obvious' solutions – $(\pm 1 : 0 : 0)$.

The Swinnerton-Dyer K3 surface

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$

- Two 'obvious' solutions – $(\pm 1 : 0 : 0)$.

The Swinnerton-Dyer K3 surface

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$

- Two ‘obvious’ solutions – $(\pm 1 : 0 : 0)$.
- The next smallest solutions are $(\pm\frac{1484801}{1169407}, \pm\frac{1203120}{1169407}, \pm\frac{1157520}{1169407})$.

The Swinnerton-Dyer K3 surface

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$

- Two 'obvious' solutions – $(\pm 1 : 0 : 0)$.
- The next smallest solutions are $(\pm\frac{1484801}{1169407}, \pm\frac{1203120}{1169407}, \pm\frac{1157520}{1169407})$.

Problem

Find another solution.

The Swinnerton-Dyer K3 surface

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$

- Two 'obvious' solutions – $(\pm 1 : 0 : 0)$.
- The next smallest solutions are $(\pm\frac{1484801}{1169407}, \pm\frac{1203120}{1169407}, \pm\frac{1157520}{1169407})$.

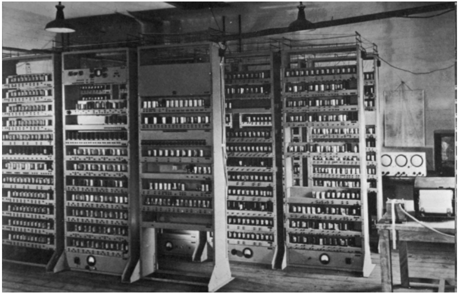
Problem

Find another solution.

(Mathematicians aren't sure if there are any more!)

Back of the envelope calculation

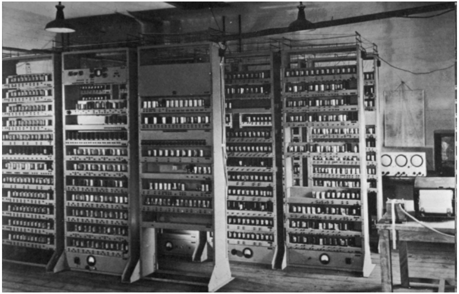
$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$



- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.

Back of the envelope calculation

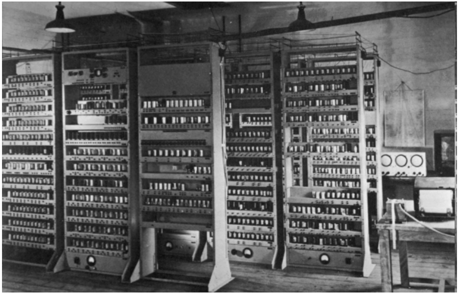
$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$



- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.
- Num, den$(x, y, z) \leq 1500000 \sim 10^{37}$ many, $\mathbf{10^{31}}$ **mins** $=$ $\mathbf{10^{25}}$ **years**.

Back of the envelope calculation

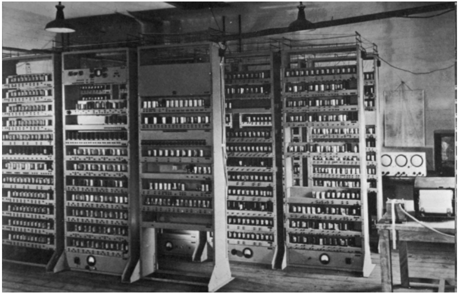
$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$



- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.
- Num, den$(x, y, z) \leq 1500000 \sim 10^{37}$ many, $\mathbf{10^{31}}$ **mins** $=$ $\mathbf{10^{25}}$ **years**.
- 10^9 many computers in the world – so $\mathbf{10^{16}}$ **years**

Back of the envelope calculation

$$\boxed{x^4 + 2y^4 = 1 + 4z^4}$$



- Num, den$(x, y, z) \leq 10 \sim 10^6$ many, **1 min** on Emory's computers.
- Num, den$(x, y, z) \leq 1500000 \sim 10^{37}$ many, $\mathbf{10^{31}}$ **mins** $=$ $\mathbf{10^{25}}$ **years**.
- 10^9 many computers in the world – so $\mathbf{10^{16}}$ **years**
- Age of the universe – **13.75** $\pm$ **.11 billion years** (roughly $\mathbf{10^{10}}$).

Fermat-like equations

Theorem (Poonen, Schaefer, Stoll)

The coprime integer solutions to $x^2 + y^3 = z^7$ *are the* 16 *triples*

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1),$$

Fermat-like equations

Theorem (Poonen, Schaefer, Stoll)

The coprime integer solutions to $x^2 + y^3 = z^7$ are the 16 triples

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$

Fermat-like equations

Theorem (Poonen, Schaefer, Stoll)

The coprime integer solutions to $x^2 + y^3 = z^7$ *are the* 16 *triples*

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2),$$

Fermat-like equations

Theorem (Poonen, Schaefer, Stoll)

The coprime integer solutions to $x^2 + y^3 = z^7$ *are the* 16 *triples*

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113),$$
$$(\pm 21063928, -76271, 17).$$

Generalized Fermat Equations

Problem

What are the solutions to the equation $x^a + y^b = z^c$*?*

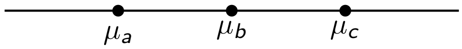
Generalized Fermat Equations

Problem

What are the solutions to the equation $x^a + y^b = z^c$*?*

Theorem (Darmon and Granville)

Fix $a, b, c \geq 2$*. Then the equation* $x^a + y^b = z^c$ *has only finitely many coprime integer solutions iff* $\chi = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 \leq 0$*.*



Known Solutions to $x^a + y^b = z^c$

The 'known' solutions with

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$$

are the following:

$$1^p + 2^3 = 3^2$$

$$2^5 + 7^2 = 3^4, 7^3 + 13^2 = 2^9, 2^7 + 17^3 = 71^2, 3^5 + 11^4 = 122^2$$

$$17^7 + 76271^3 = 21063928^2, 1414^3 + 2213459^2 = 65^7, 9262^3 153122832 = 113^7$$

$$43^8 + 96222^3 = 30042907^2, 33^8 + 1549034^2 = 15613^3$$

Known Solutions to $x^a + y^b = z^c$

The ‘known’ solutions with

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$$

are the following:

$$1^p + 2^3 = 3^2$$

$$2^5 + 7^2 = 3^4, 7^3 + 13^2 = 2^9, 2^7 + 17^3 = 71^2, 3^5 + 11^4 = 122^2$$

$$17^7 + 76271^3 = 21063928^2, 1414^3 + 2213459^2 = 65^7, 9262^3 153122832 = 113^7$$

$$43^8 + 96222^3 = 30042907^2, 33^8 + 1549034^2 = 15613^3$$

Problem (Beal’s conjecture)

These are all solutions with $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 < 0$.

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman-Zagier)

This is a complete list of coprime non-zero solutions such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman-Zagier)

This is a complete list of coprime non-zero solutions such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

$100,000 prize for proof of conjecture...

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman-Zagier)

This is a complete list of coprime non-zero solutions such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0$.

\$100,000 prize for proof of conjecture...

...or even for a counterexample.

Examples of Generalized Fermat Equations

Theorem (Poonen, Schaefer, Stoll)

The coprime integer solutions to $x^2 + y^3 = z^7$ are the 16 triples

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113),$$
$$(\pm 21063928, -76271, 17).$$

Examples of Generalized Fermat Equations

Theorem (Poonen, Schaefer, Stoll)

The coprime integer solutions to $x^2 + y^3 = z^7$ are the 16 triples

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113),$$
$$(\pm 21063928, -76271, 17).$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{7} - 1 = -\frac{1}{42} < 0$$

Examples of Generalized Fermat Equations

Theorem (Poonen, Schaefer, Stoll)

The coprime integer solutions to $x^2 + y^3 = z^7$ are the 16 triples

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113),$$
$$(\pm 21063928, -76271, 17).$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{7} - 1 = -\frac{1}{42} < 0$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0$$

Examples of Generalized Fermat Equations

Theorem (Darmon, Merel)

Any pairwise coprime solution to the equation

$$x^n + y^n = z^2, n > 4$$

satisfies $xyz = 0$.

Examples of Generalized Fermat Equations

Theorem (Darmon, Merel)

Any pairwise coprime solution to the equation

$$x^n + y^n = z^2, n > 4$$

satisfies $xyz = 0$.

$$\frac{1}{n} + \frac{1}{n} + \frac{1}{2} - 1 = \frac{2}{n} - \frac{1}{2} < 0$$

Other applications of the modular method

The ideas behind the proof of FLT now permeate the study of diophantine problems.

Other applications of the modular method

The ideas behind the proof of FLT now permeate the study of diophantine problems.

Theorem (Bugeaud, Mignotte, Siksek 2006)

The only Fibonacci numbers that are perfect powers are

$$F_0 = 0,\ F_1 = F_2 = 1,\ F_6 = 8,\ F_{12} = 144.$$

Examples of Generalized Fermat Equations

Theorem (Klein, Zagier, Beukers, Edwards, others)

The equation

$$x^2 + y^3 = z^5$$

Examples of Generalized Fermat Equations

Theorem (Klein, Zagier, Beukers, Edwards, others)

The equation

$$x^2 + y^3 = z^5$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} - 1 = \frac{1}{30} > 0$$

Examples of Generalized Fermat Equations

Theorem (Klein, Zagier, Beukers, Edwards, others)

The equation

$$x^2 + y^3 = z^5$$

has infinitely many coprime solutions

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} - 1 = \frac{1}{30} > 0$$

Examples of Generalized Fermat Equations

Theorem (Klein, Zagier, Beukers, Edwards, others)

The equation

$$x^2 + y^3 = z^5$$

has infinitely many coprime solutions

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} - 1 = \frac{1}{30} > 0$$

$$(T/2)^2 + H^3 + (f/12^3)^5$$

1. $f = st(t^{10} - 11t^5s^5 - s^{10})$,
2. $H =$ Hessian of f,
3. $T =$ a degree 3 covariant of the dodecahedron.

(p, q, r) such that $\chi < 0$ and the solutions to $x^p + y^q = z^r$ have been determined.

$\{n, n, n\}$	Wiles, Taylor-Wiles, building on work of many others
$\{2, n, n\}$	Darmon-Merel, others for small n
$\{3, n, n\}$	Darmon-Merel, others for small n
$\{5, 2n, 2n\}$	Bennett
$(2, 4, n)$	Ellenberg, Bruin, Ghioca $n \geq 4$
$(2, n, 4)$	Bennett-Skinner; $n \geq 4$
$\{2, 3, n\}$	Poonen-Shaefer-Stoll, Bruin. $6 \leq n \leq 9$
$\{2, 2\ell, 3\}$	Chen, Dahmen, Siksek; primes $7 < \ell < 1000$ with $\ell \neq 31$
$\{3, 3, n\}$	Bruin; $n = 4, 5$
$\{3, 3, \ell\}$	Kraus; primes $17 \leq \ell \leq 10000$
$(2, 2n, 5)$	Chen $n \geq 3^*$
$(4, 2n, 3)$	Bennett-Chen $n \geq 3$
$(6, 2n, 2)$	Bennett-Chen $n \geq 3$
$(2, 6, n)$	Bennett-Chen $n \geq 3$

(2,3,10) Theorem

$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{10} - 1 = -\frac{1}{15}$ is maximal among unsolved Fermat equations.

(2,3,10) Theorem

$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{10} - 1 = -\frac{1}{15}$ is maximal among unsolved Fermat equations.

Theorem (ZB., 2011)

The only coprime integer solutions to the equation

$$x^2 + y^3 = z^{10}$$

are the 12 triples

$$(\pm 1, -1, 0), (\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 3, -2, \pm 1).$$

(2,3,10) Theorem

$\chi = \frac{1}{2} + \frac{1}{3} + \frac{1}{10} - 1 = -\frac{1}{15}$ is maximal among unsolved Fermat equations.

Theorem (ZB., 2011)

The only coprime integer solutions to the equation

$$x^2 + y^3 = z^{10}$$

are the 12 triples

$$(\pm 1, -1, 0), (\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 3, -2, \pm 1).$$

It is the first generalized Fermat equation of the form $x^2 + y^3 = z^n$ conjectured to have only trivial solutions.

$(3^2 + (-2)^3 = 1^n$ is considered to be trivial.)

The Mazur-Ellenberg threefold

$$V\colon\ x_0^4 y_0^5 + x_1^4 y_1^5 + x_2^4 y_2^5 = 0 \subset \mathbb{P}^2 \times \mathbb{P}^2.$$

The Mazur-Ellenberg threefold

$$V\colon\ x_0^4y_0^5 + x_1^4y_1^5 + x_2^4y_2^5 = 0 \subset \mathbb{P}^2 \times \mathbb{P}^2.$$

$$A + B + C = 0 \rightsquigarrow \text{ solution to } V$$

The Mazur-Ellenberg threefold

$$V\colon\ x_0^4y_0^5 + x_1^4y_1^5 + x_2^4y_2^5 = 0 \subset \mathbb{P}^2 \times \mathbb{P}^2.$$

$$A + B + C = 0 \rightsquigarrow \text{ solution to } V$$

$$p^4 = (p)^4(1)^5$$

$$p^5 = (1)^4(p)^5$$

$$p^{12} = (p^3)^4(1)^5$$

$$p^{13} = (p^2)^4(p)^5$$

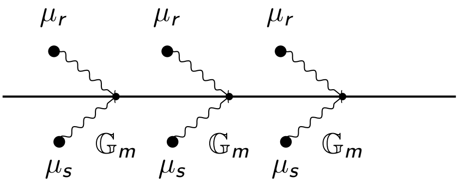
$$p^{20} = (p^5)^4(1)^5 = (1)^4(p^4)^5$$

Theorem

$$V\colon\ x_0^4y_0^5 + x_1^4y_1^5 + x_2^4y_2^5 = 0 \subset \mathbb{P}^2 \times \mathbb{P}^2.$$

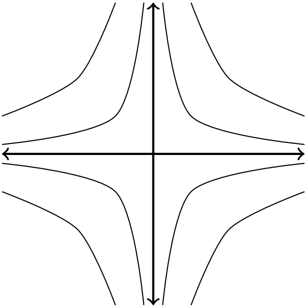
Theorem (ZB)

$V - Z$ is log general type; in particular, the Lang-Vojta conjecture implies Fermat's last theorem and most cases of the generalized Fermat conjecture.



Theorem

$$[\mathbb{C}^2/\mathbb{C}^*], \ \ t \cdot (x, y) = (t^r x, t^{r-1} y)$$



$\to$