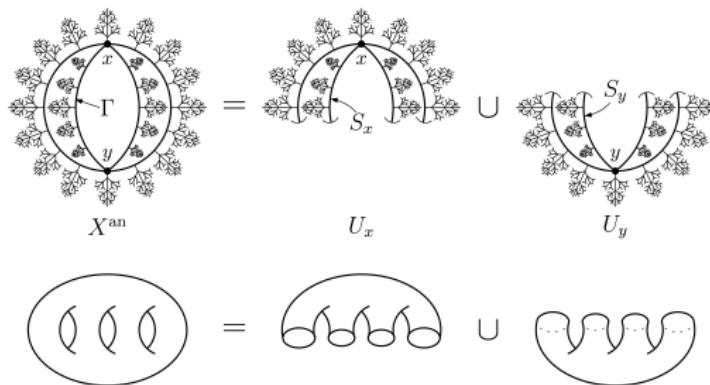


# Diophantine and tropical geometry

David Zureick-Brown

Slides available at <http://www.math.emory.edu/~dzb/slides/>

The Ohio State University  
March 25, 2021



# Basic Problem (Solving Diophantine Equations)

## Setup

Let  $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$  be polynomials.

Let  $R$  be a ring (e.g.,  $R = \mathbb{Z}, \mathbb{Q}$ ).

## Problem

*Describe the set*

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

## 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:**  $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ ;

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

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

*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:**  $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ ;

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

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

*is non-empty.*

This is also *known* for many rings (e.g.,  $R = \mathbb{C}, \mathbb{R}, \mathbb{F}_q, \mathbb{Q}_p, \mathbb{C}(t)$ ).

# 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:**  $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ ;

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

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

*is non-empty.*

This is also *known* for many rings (e.g.,  $R = \mathbb{C}, \mathbb{R}, \mathbb{F}_q, \mathbb{Q}_p, \mathbb{C}(t)$ ).

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!



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

## 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:  $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$

## 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 explicitly **find** all solutions? (With proof?)

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

### 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 explicitly **find** all solutions? (With proof?)

### 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

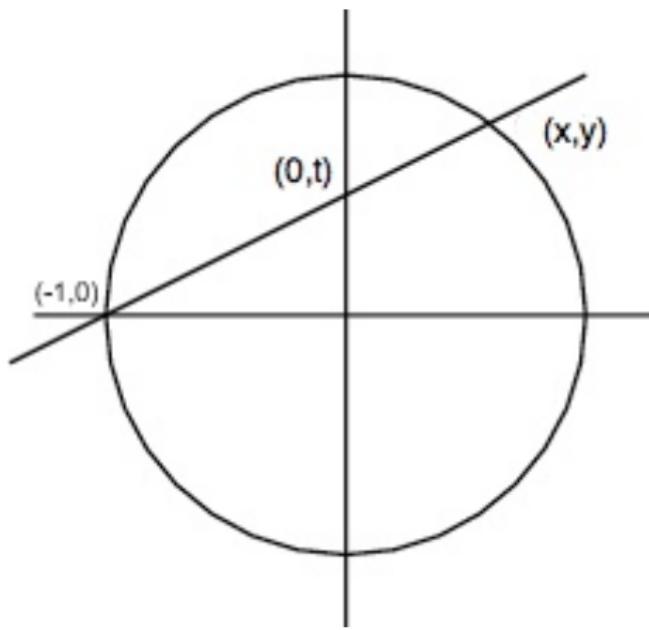
## Lemma

*The equation*

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

*has infinitely many non-zero coprime solutions.*

# Pythagorean triples



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

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

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

# Pythagorean triples

## Lemma

*The solutions to*

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

*are all multiples of the triples*

$$a = 1 - t^2$$

$$b = 2t$$

$$c = 1 + t^2$$

# 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.

# 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.

## Theorem (Faltings)

For  $n \geq 5$ , the equation

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

has only finitely many solutions if  $f(x)$  is squarefree, with degree  $> 4$ .

# Fermat Curves

## Question

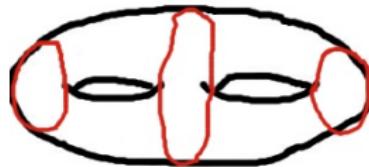
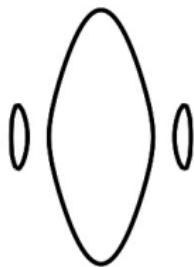
Why is Fermat's last theorem believable?

- 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

## Example

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



This is a cross section of a two holed 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  $n$ th Fermat equation has only finitely many solutions.

# Fermat Curves

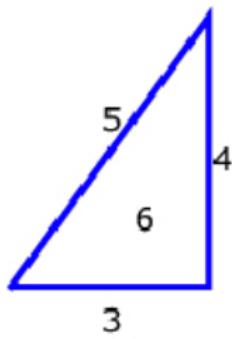
## Question

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

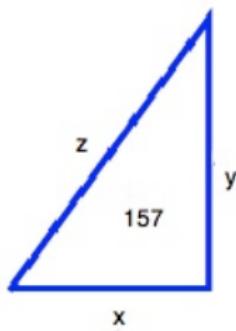
$$x^2 + y^2 = z^2, xy = 2 \cdot 6$$



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

# Congruent number problem

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



# Congruent number problem

The pair of equations

$$x^2 + y^2 = z^2, \quad xy = 2 \cdot 157$$

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

# Congruent number problem

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

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

# Congruent number problem

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

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

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

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

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

# Congruent number problem

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

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!**

# Congruent number problem

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

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?

# Congruent number problem

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

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” solution has **176 digits**!

## Back of the envelope calculation (as of 2011)

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

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

## Back of the envelope calculation (as of 2011)

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

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

## Back of the envelope calculation (as of 2011)

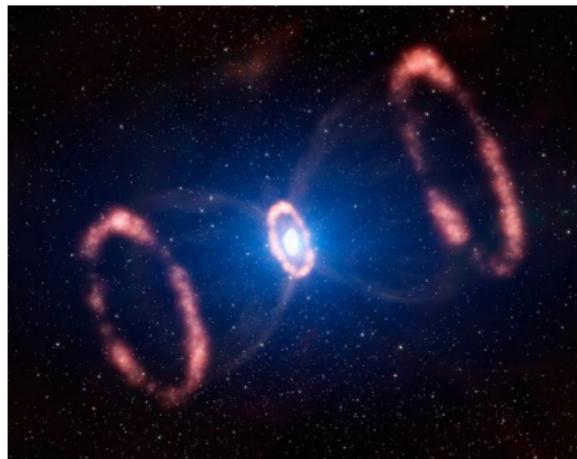
$$x^2 + y^2 = z^2, xy = 2 \cdot 157$$

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

# Back of the envelope calculation (as of 2011)

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

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



# Fermat Surfaces

## Conjecture

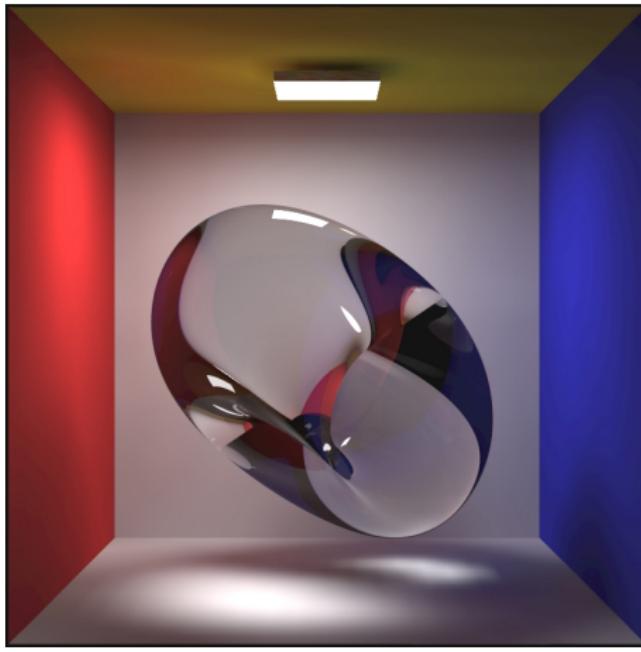
The only solutions to the equation

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

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

# The Swinnerton-Dyer K3 surface

$$x^4 + 2y^4 = 1 + 4z^4$$



# The Swinnerton-Dyer K3 surface

$$x^4 + 2y^4 = 1 + 4z^4$$



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

# The Swinnerton-Dyer K3 surface

$$x^4 + 2y^4 = 1 + 4z^4$$

- 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.*

## Remark

- ➊  **$10^{16}$  years** to find via brute force.
- ➋ Age of the universe –  **$13.75 \pm .11$  billion years** (roughly  $10^{10}$ ).

# 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*

$$\begin{aligned} & (\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1), \\ & (\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \\ & (\pm 21063928, -76271, 17). \end{aligned}$$

# Generalized Fermat Equations

## Problem

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

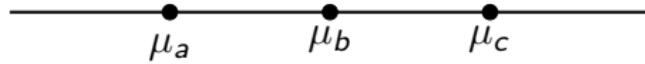
# Generalized Fermat Equations

## 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:

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

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

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

$$9262^3 + 153122832^2 = 113^7$$

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

# 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:

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

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

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

$$9262^3 + 153122832^2 = 113^7$$

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

## 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

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0.$$

\$1,000,000 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

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 < 0.$$

\$1,000,000 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*

$$\begin{aligned} & (\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1), \\ & (\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \\ & (\pm 21063928, -76271, 17). \end{aligned}$$

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

# Examples of Generalized Fermat Equations

Theorem (Poonen, Schaefer, Stoll)

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

$$\begin{aligned} & (\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1), \\ & (\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \\ & (\pm 21063928, -76271, 17). \end{aligned}$$

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

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

# Examples of Generalized Fermat Equations

Theorem (Darmon, Merel)

*Any pairwise coprime solution to the equation*

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

*satisfies  $xyz = 0$ .*

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

# 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  $H = \text{Hessian of } f$ ,
- ③  $T = \text{a degree 3 covariant of the dodecahedron}$ .

$(p, q, r)$  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 $n \geq 3$  |

$(p, q, r)$  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 $n \geq 3$  |
| $(2, 3, 10)$      | <b>ZB</b>  |

# Faltings' theorem / Mordell's conjecture

Theorem (Faltings, Vojta, Bombieri)

*Let  $X$  be a smooth curve over  $\mathbb{Q}$  with genus at least 2. Then  $X(\mathbb{Q})$  is finite.*

Example

For  $g \geq 2$ ,  $y^2 = x^{2g+1} + 1$  has only finitely many solutions with  $x, y \in \mathbb{Q}$ .

# Uniformity

## Problem

- ① Given  $X$ , compute  $X(\mathbb{Q})$  exactly.
- ② Compute bounds on  $\#X(\mathbb{Q})$ .

## Conjecture (Uniformity)

There exists a constant  $N(g)$  such that every smooth curve of genus  $g$  over  $\mathbb{Q}$  has at most  $N(g)$  rational points.

## Theorem (Caporaso, Harris, Mazur)

*Lang's conjecture  $\Rightarrow$  uniformity.*

# Uniformity numerics

|                   |     |     |     |     |     |     |             |
|-------------------|-----|-----|-----|-----|-----|-----|-------------|
| $g$               | 2   | 3   | 4   | 5   | 10  | 45  | $g$         |
| $B_g(\mathbb{Q})$ | 642 | 112 | 126 | 132 | 192 | 781 | $16(g + 1)$ |

## Remark

Elkies studied K3 surfaces of the form

$$y^2 = S(t, u, v)$$

with lots of rational lines, such that  $S$  restricted to such a line is a perfect square.

# Main Theorem (partial uniformity for curves)

## Theorem (Katz–Rabinoff–ZB)

Let  $X$  be *any* curve of genus  $g$  and let  $r = \text{rank}_{\mathbb{Z}} \text{Jac}_X(\mathbb{Q})$ . Suppose  $r < g - 2$ . Then

$$\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28$$

## Tools

*p*-adic integration on annuli

comparison of different analytic continuations of *p*-adic integration

Non-Archimedean (Berkovich) structure of a curve [BPR]

Combinatorial restraints coming from the Tropical canonical bundle

# $p$ -adic integration

(Chabauty, Coleman) There exists  $V \subset H^0(X_{\mathbb{Q}_p}, \Omega_X^1)$  with  $\dim_{\mathbb{Q}_p} V \geq g - r$  such that,

$$\int_P^Q \omega = 0 \quad \forall P, Q \in X(\mathbb{Q}), \omega \in V$$

## Example

$$X: y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$$

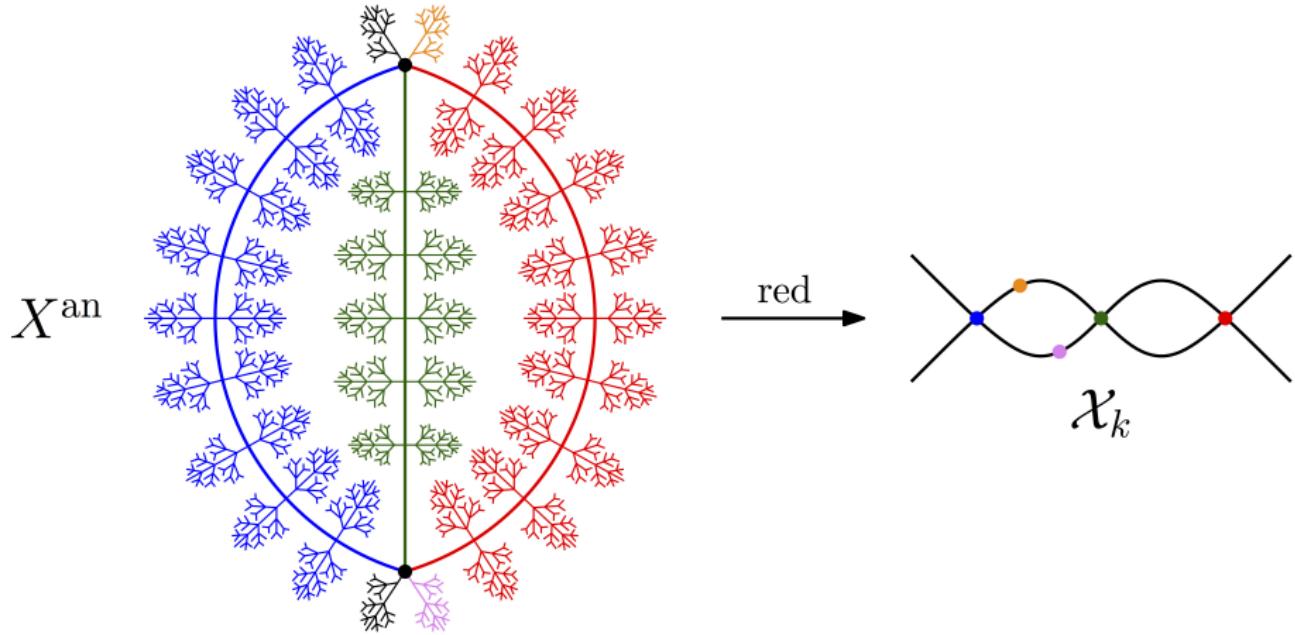
- ① Points reducing to  $\tilde{Q} = (0, 1)$  are given by

$$x = p \cdot t, \text{ where } t \in \mathbb{Z}_p$$

$$y = \sqrt{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1} = 1 + x^2 + \dots$$

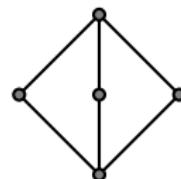
②  $\int_{(0,1)}^{P_t} \frac{xdx}{y} = \int_0^t (x - x^3 + \dots) dx$

# Berkovich picture



# Baker–Payne–Rabinoff and the slope formula

(Dual graph  $\Gamma$  of  $X_{\mathbb{F}_p}$ )



(Contraction Theorem)  $\tau: X^{\text{an}} \rightarrow \Gamma$ .

(Combinatorial harmonic analysis/potential theory)

$f$  a meromorphic function on  $X^{\text{an}}$

$F := (-\log |f|) \big|_{\Gamma}$  associated tropical, piecewise linear function

$\text{div } F$  combinatorial record of the slopes of  $F$

(Slope formula)  $\tau_* \text{div } f = \text{div } F$

# Berkovich picture

