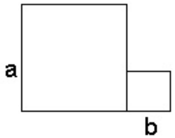
Beyond Fermat’s Last Theorem

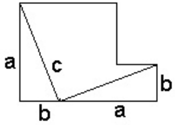
David Zureick-Brown
Amherst College

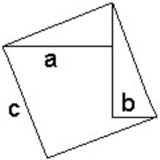
Slides available at http://dmzb.github.io/

University of California, Irvine Colloquium
March 5, 2026

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







Basic Problem (Solving Diophantine Equations)

Let $f_1, \ldots, f_m$ be polynomials with integer coefficients, e.g.,

$$x^2 + y^2 + 1$$
$$x^3 - y^2 - 2$$
$$2y^2 + 17x^4 - 1$$

Basic problem: solve polynomial equations

Describe the set

$$V(f_1, \ldots, f_m) = \left\{(a_1, \ldots, a_n) \in \mathbb{Z}^n : \forall i,\, f_i(a_1, \ldots, a_n) = 0\right\},$$

i.e., the set of integer solutions to those polynomials

Fact

Solving Diophantine equations is difficult.

Basic Problem (Solving Diophantine Equations)

Let $f_1, \ldots, f_m$ be polynomials with integer coefficients, e.g.,

$$x^2 + y^2 + 1 = 0$$
$$x^3 - y^2 - 2 = 0$$
$$2y^2 + 17x^4 - 1 = 0$$

Basic problem: solve polynomial equations

Describe the set

$$V(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n : \forall i,\, f_i(a_1, \ldots, a_n) = 0\},$$

i.e., the set of integer solutions to those polynomials

Fact

Solving Diophantine equations is difficult.

Hilbert's Tenth Problem

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

There does not exist an algorithm solving the following problem:

***input**: integer polynomials* $f_1, \ldots, f_m$ *in variables* $x_1, ..., x_n$*;*

***output**:* $\mathrm{YES} / \mathrm{NO}$ *according to whether the set of solutions*

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

is non-empty.

This is *known* to be true for many other cases (e.g., $\mathbb{C}, \mathbb{R}, \mathbb{F}_q, \mathbb{Q}_p, \mathbb{C}(t)$).

This is *still unknown* in many other cases (e.g., $\mathbb{Q}$).

Fermat's Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

For primes $p \geq 3$ the only integer solutions to the equation

$$x^p + y^p = z^p$$

are integer multiples of the triples

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

Fermat's Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

For primes $p \geq 3$ the only integer solutions to the equation

$$x^p + y^p = z^p$$

are integer multiples of the triples

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

This took 300 years to prove!

Fermat's Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

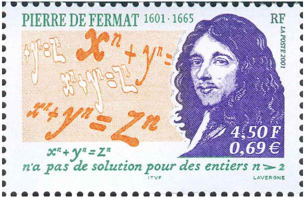
For primes $p \geq 3$ the only integer solutions to the equation

$$x^p + y^p = z^p$$

are integer multiples of the triples

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

This took 300 years to prove!



Fermat's Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

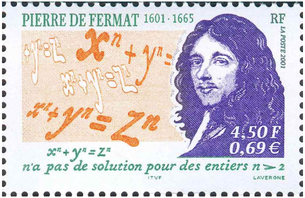
For primes $p \geq 3$ the only integer solutions to the equation

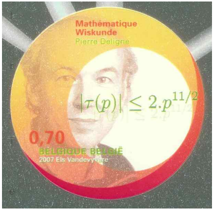
$$x^p + y^p = z^p$$

are integer multiples of the triples

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

This took 300 years to prove!





Fermat’s Last Theorem - A Marvelous Proof

Theorem (Wiles; Taylor)

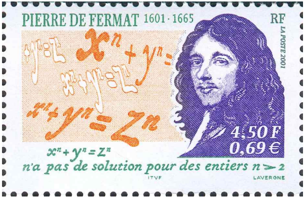
For primes $p \geq 3$ the only integer solutions to the equation

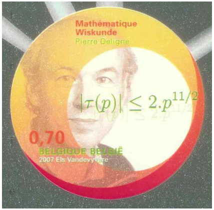
$$x^p + y^p = z^p$$

are integer multiples of the triples

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

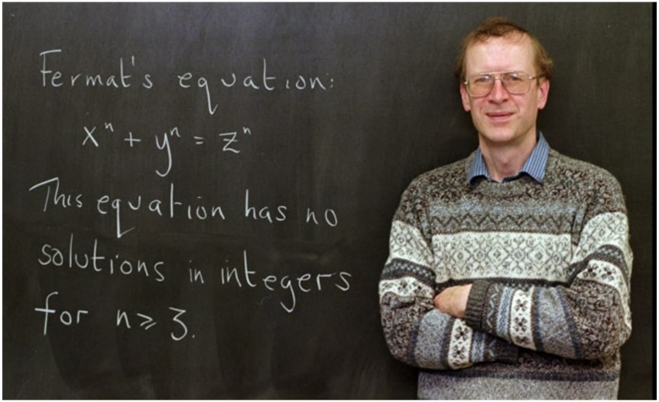
This took 300 years to prove!



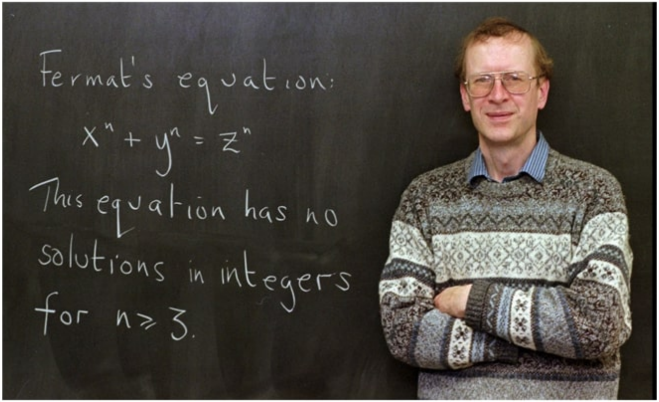


https://mathshistory.st-andrews.ac.uk/Miller/stamps/

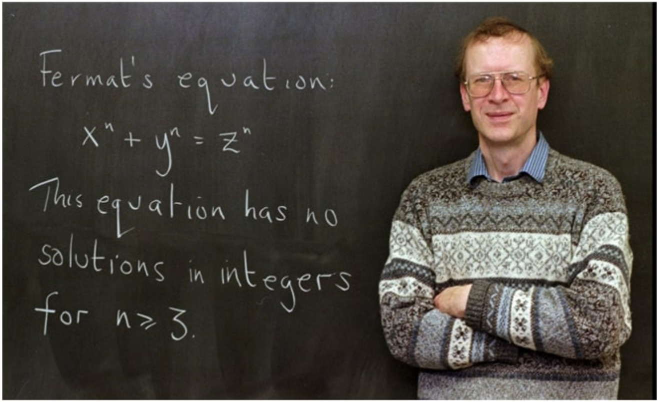
Fermat's Last Theorem - aftermath



Fermat’s Last Theorem - aftermath



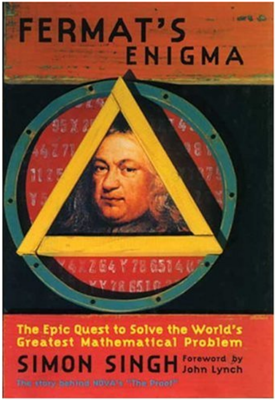
Fermat's Last Theorem - aftermath

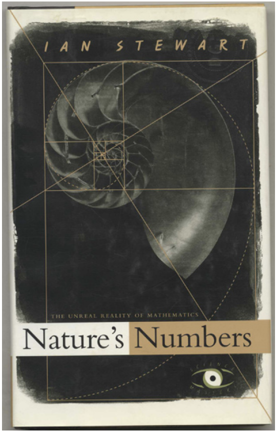


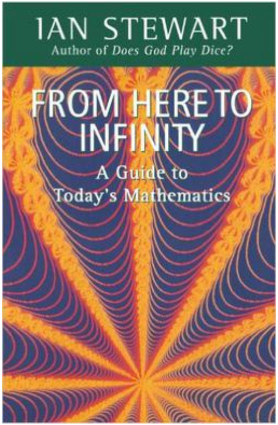
GAP

20/20

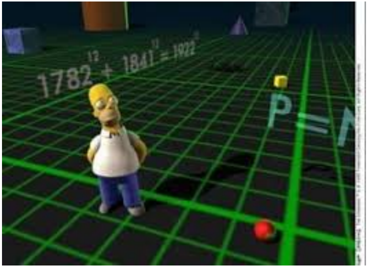
Books


FERMAT'S
ENIGMA
The Epic Quest to Solve the World's Greatest Mathematical Problem
SIMON SINGH
Foreword by John Lynch
The story behind NOVA's "The Proof"

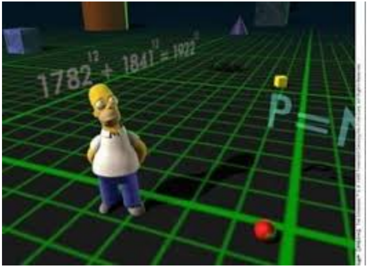

IAN STEWART
THE UNREAL REALITY OF MATHEMATICS
Nature's Numbers

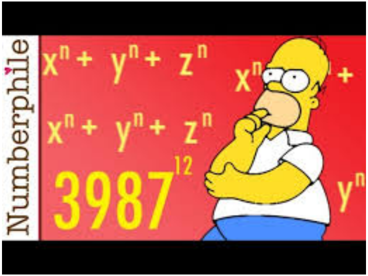

IAN STEWART
Author of Does God Play Dice?
FROM HERE TO INFINITY
A Guide to Today's Mathematics

Fermat trolling



Fermat trolling





See https://youtu.be/ReOQ300AcSU?si=--fAdsdPttt4HR3N

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 explicitly find all solutions? (With proof?)

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

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

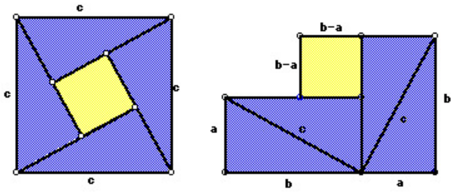
$$3^2+4^2=5^2$$
$$5^2+12^2=13^2$$
$$7^2+24^2=25^2$$

Lemma

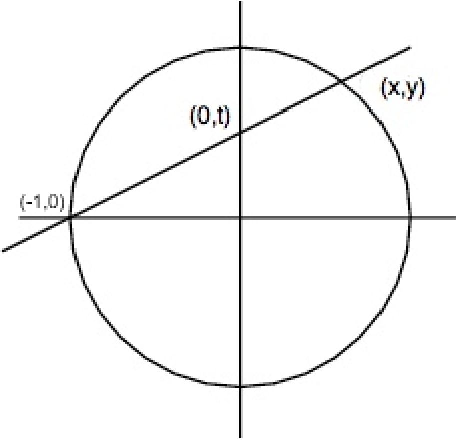
The equation

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

has infinitely many non-zero coprime solutions.



Pythagorean triples



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

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

(with $c \neq 0$) are all multiples of the triples

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

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.

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?

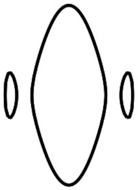
1. $x^n + y^n - z^n = 0$ looks like a surface (3 variables)
2. $x^n + y^n - 1 = 0$ looks like a curve (2 variables)

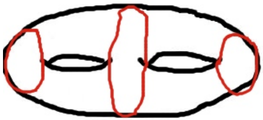
Mordell Conjecture

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, 1922)

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

Fermat Curves

Question

Why is Fermat's last theorem believable?

1. $x^n + y^n - z^n = 0$ looks like a surface (3 variables)
2. $x^n + y^n - 1 = 0$ looks like a curve (2 variables)
3. and has genus
$$(n-1)(n-2)/2$$
which is ≥ 2 iff $n \geq 4$.

Fermat Curves

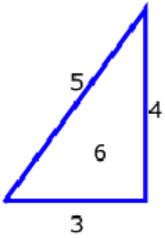
Question

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

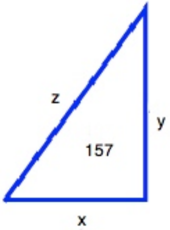
$$x^2 + y^2 = z^2,\ xy = 2 \cdot 6$$



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

Congruent number problem

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



Assume the Birch–Swinnerton-Dyer conjectures

If you assume $1,000,000 worth of conjectures, then the equations

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

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

Assume the Birch–Swinnerton-Dyer conjectures

If you assume $1,000,000 worth of conjectures, then the equations

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

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

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

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

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

Assume the Birch–Swinnerton-Dyer conjectures

If you assume $1,000,000 worth of conjectures, then the equations

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

have **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**!

Assume the Birch–Swinnerton-Dyer conjectures

If you assume $1,000,000 worth of conjectures, then the equations

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

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

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

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

$$z = \frac{20085078913 \cdot 1185369214457 \cdot 9425458255024420419 07480}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 52677109576}$$

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

Assume the Birch–Swinnerton-Dyer conjectures

If you assume \$1,000,000 worth of conjectures, then the equations

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

have **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?
(Heegner Points)

Assume the Birch–Swinnerton-Dyer conjectures

If you assume $1,000,000 worth of conjectures, then the equations

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

have **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?
(Heegner Points)
“Next” soluton has **176 digits**!

Back of the envelope calculation (as of 2011)

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

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

Back of the envelope calculation (as of 2011)

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

- 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 (as of 2011)

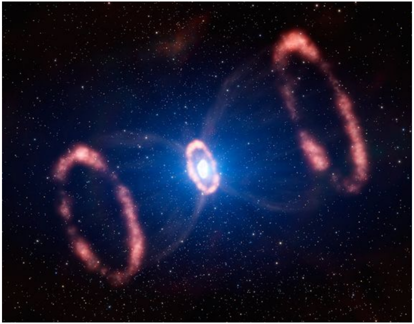
$$\boxed{x^2 + y^2 = z^2,\ xy = 2 \cdot 157}$$

- 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 (as of 2011)

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

- 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 until 'heat death' of universe – $\mathbf{10^{100}}$ **years.**



Fermat Surfaces

Conjecture

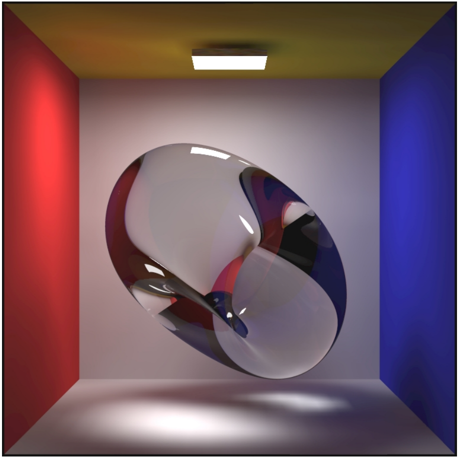
The only solutions to the equation

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

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

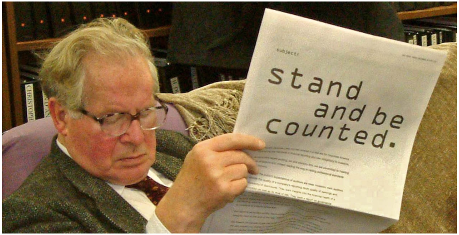
The Swinnerton-Dyer K3 surface

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



The Swinnerton-Dyer K3 surface

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



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

The Swinnerton-Dyer K3 surface

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

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

Problem

Find another solution. (Probably impossible.)

Back of envelope calcluation

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

Sums of cubes

$$1 = 1^3 + 0^3 + 0^3$$
$$2 = 1^3 + 1^3 + 0^3$$
$$3 = 1^3 + 1^3 + 1^3$$
$$3 = 4^3 + 4^3 + (-5)^3$$
$$4 \neq x^3 + y^3 + z^3$$
$$5 \neq x^3 + y^3 + z^3$$
$$6 = 1^3 + 1^3 + 2^3$$

Conjecture (Heath-Brown)

The equation

$$x^3 + y^3 + z^3 = n$$

has an integer solution if and only if n is not 4 or 5 mod 9.

Solved by Booker–Sutherland

$32 \neq x^3 + y^3 + z^3$

$33 =$

https://www.quantamagazine.org/why-the-sum-of-three-cubes-is-a-hard-math-problem-20191105/

Solved by Booker–Sutherland

$$32 \neq x^3 + y^3 + z^3$$

$$33 = 8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3$$

https://www.quantamagazine.org/why-the-sum-of-three-cubes-is-a-hard-math-problem-20191105/

Solved by Booker–Sutherland

$$32 \neq x^3 + y^3 + z^3$$

$$33 = 8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3$$

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3$$

https://www.quantamagazine.org/why-the-sum-of-three-cubes-is-a-hard-math-problem-20191105/

Solved by Booker–Sutherland

$32 \neq x^3 + y^3 + z^3$

$$33 = 8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3$$
$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3$$

https://www.quantamagazine.org/why-the-sum-of-three-cubes-is-a-hard-math-problem-20191105/

Solved by Booker–Sutherland

$$32 \neq x^3 + y^3 + z^3$$

$$33 = 8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3$$

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3$$

$$3 = 569936821221962380720^3 + (-569936821113563493509)^3 + (-472715493453327032)^3$$

https://www.quantamagazine.org/why-the-sum-of-three-cubes-is-a-hard-math-problem-20191105/

Solved by Booker–Sutherland

$$32 \neq x^3 + y^3 + z^3$$

$$33 = 8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3$$
$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3$$

$$3 = 569936821221962380720^3 + (-569936821113563493509)^3 + (-472715493453327032)^3$$

$$114 = x^3 + y^3 + z^3?$$

https://www.quantamagazine.org/why-the-sum-of-three-cubes-is-a-hard-math-problem-20191105/

“Generalized” Fermat equations

Theorem (Poonen, Schaefer, Stoll)

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

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

“Generalized” Fermat equations

Theorem (Poonen, Schaefer, Stoll)

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

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

“Generalized” Fermat equations

Theorem (Poonen, Schaefer, Stoll)

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

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

“Generalized” Fermat equations

Theorem (Poonen, Schaefer, Stoll)

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

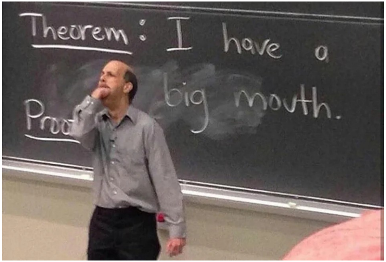
$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1),$$
$$(\pm 71, -17, 2), (\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113),$$
$$(\pm 21063928, -76271, 17).$$

“Generalized” Fermat equations

Theorem (Poonen, Schaefer, Stoll)

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

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

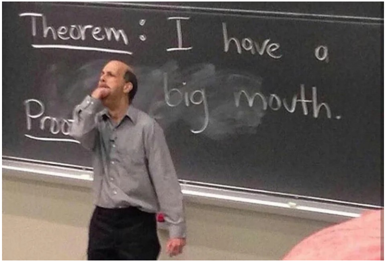


“Generalized” Fermat equations

Theorem (Poonen, Schaefer, Stoll)

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

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



Generalized Fermat Equations

Problem

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

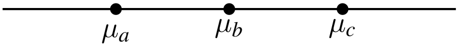
Generalized Fermat Equations

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 $x^a + y^b = z^c$ with $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$

$$1^p + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4$$

$$7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2$$

$$3^5 + 11^4 = 122^2$$

$$17^7 + 76271^3 = 21063928^2$$

$$1414^3 + 2213459^2 = 65^7$$

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

$$43^8 + 96222^3 = 30042907^2$$

$$33^8 + 1549034^2 = 15613^3$$

Known Solutions to $x^a + y^b = z^c$ with $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$

$$1^p + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4$$

$$7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2$$

$$3^5 + 11^4 = 122^2$$

$$17^7 + 76271^3 = 21063928^2$$

$$1414^3 + 2213459^2 = 65^7$$

$$9262^3 + 15312283^2 = 113^7$$

$$43^8 + 96222^3 = 30042907^2$$

$$33^8 + 1549034^2 = 15613^3$$

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 $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 < 0$.

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman–Zagier)

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

$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 $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 < 0$.

$1,000,000 prize for proof of conjecture...
...or even for a counterexample.

Generalized Fermat Equations – Known Solutions

Conjecture (Beal, Granville, Tijdeman–Zagier)

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

$1,000,000 prize for proof of conjecture...
...or even for a counterexample.

SETI@home

ABC@home

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 $xyz = 0$.

$$\frac{1}{n} + \frac{1}{n} + \frac{1}{2} - 1 = \frac{2}{n} - \frac{1}{2} < \frac{2}{4} - \frac{1}{2} = 0$$

Other applications of the modular method

Ideas behind the proof of FLT permeate the study of diophantine problems.

Other applications of the modular method

Ideas behind the proof of FLT permeate the study of diophantine problems.

Theorem (Bugeaud, Mignotte, Siksek; 2006)

The only Fibonacci numbers that are perfect powers are

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

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Other applications of the modular method

Ideas behind the proof of FLT permeate the study of diophantine problems.

Theorem (Bugeaud, Mignotte, Siksek; 2006)

The only Fibonacci numbers that are perfect powers are

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

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Theorem (Silliman–Vogt; 2013 REU)

0 and 1 are the only perfect powers in the Lucas sequence

$$L_1 = 0, L_2 = 1, \quad L_n = 3L_{n-1} - 2L_{n-2}.$$

$$0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, \ldots, 2^n - 1, \ldots$$

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.

(a,b,c) such that $\chi < 0$ and the solutions to $x^a + y^b = z^c$ 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 $n \geq 3$

(a,b,c) such that $\chi < 0$ and the solutions to $x^a + y^b = z^c$ 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 $n \geq 3$
$(2,3,10)$	**ZB**

Faltings' theorem / Mordell's conjecture

Theorem (Faltings, Vojta, Bombieri)

Let X be a smooth curve with genus at least 2. Then $\#X(\mathbb{Q}) < \infty$.

Example

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

Conjecture (Lang, Vojta)

Let X be a variety of general type. Then $X(\mathbb{Q})$ is not (Zariski) dense.

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	$16(g+1)$

Uniformity numerics

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

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

Uniformity numerics

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

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

$$x = -3898675687/2462651894$$

$$y = 414541623698393040986922116885/83905238898871602089890028$$

Uniformity numerics

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

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

$$x = -3898675687/2462651894$$
$$y = 414541623698393040986922116885/839052388988716020898890028$$

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 square.

Main Theorem (uniformity for curves of small rank)

Theorem (Katz–Rabinoff–ZB)

Let X *be any curve of genus* g *and let* $r = \mathrm{rank}_{\mathbb{Z}} \mathrm{Jac}_X(\mathbb{Q})$. *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

Coleman's bound

Theorem (Coleman, 1985)

Let X be a curve of genus g and let $r = \mathrm{rank}_{\mathbb{Z}} \mathrm{Jac}_X(\mathbb{Q})$. Suppose $p > 2g$ is a prime of good reduction. Suppose $r < g$. Then

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2g - 2.$$

Remark

1. *A modified statement holds for $p \leq 2g$ or for $K \neq \mathbb{Q}$.*
2. *This does not prove uniformity (since the first good p might be large).*

Tools

p-adic integration and Riemann–Roch

Example (from McCallum–Poonen's survey paper)

Example

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

1. Points P_t reducing mod 3 to $\widetilde{Q} = (0,1)$ are given by

$$\begin{aligned} x &= 3 \cdot t, \text{ where } t \in \mathbb{Z}_3 \\ y &= \sqrt{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1} = 1 + x^2 + \cdots \end{aligned}$$

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

p-adic integration

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

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

Example

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

1. Points reducing mod 3 to $\widetilde{Q} = (0, 1)$ are given by

$$\begin{aligned} x = & \quad 3 \cdot t, \text{ where } t \in \mathbb{Z}_3 \\ y = & \quad \sqrt{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1} = 1 + x^2 + \cdots \end{aligned}$$

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

Chabauty's method

(**p-adic integration**) There exists $V \subset H^0(X_{\mathbb{Q}_p}, \Omega^1_X)$ with $\dim_{\mathbb{Q}_p} V \geq g - r$ such that

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

(**Coleman, via Newton Polygons**) Number of zeroes in a residue disc D_P is $\leq 1 + n_P$, where $n_P = \#\left(\operatorname{div}\omega \cap D_P\right)$

(**Riemann–Roch**) $\sum n_P = 2g - 2$.

(**Coleman's bound**) $\sum_{P \in X(\mathbb{F}_p)} (1 + n_P) = \#X(\mathbb{F}_p) + 2g - 2$.

Stoll's hyperelliptic uniformity theorem

Theorem (Stoll, 2013)

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

Then

$$\#X(\mathbb{Q}) \leq 8(r+4)(g-1) + \max\{1, 4r\} \cdot g$$

Tools

p-adic integration on annuli

comparison of different analytic continuations of p-adic integration

Main Theorem (uniformity for curves of small rank)

Theorem (Katz–Rabinoff–ZB)

Let X be any curve of genus g and let $r = \operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}_X(\mathbb{Q})$. 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

Comments

Corollary ((Partially) effective Manin-Mumford)

There is an effective constant $N(g)$ such that if $g(X) = g$, then

$$\#\left(X \cap \mathrm{Jac}_{X,\mathit{tors}}\right)(\mathbb{Q}) \leq N(g)$$

Corollary

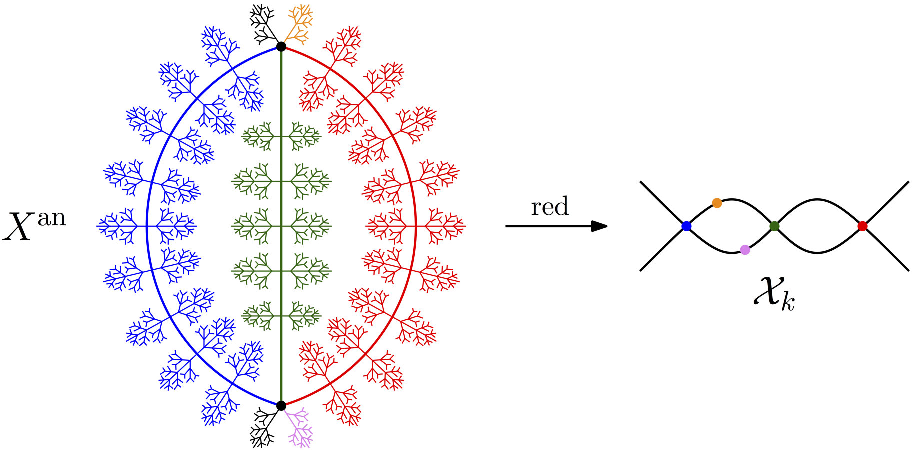
There is an effective constant $N'(g)$ such that if $g(X) = g > 3$ and $X/\mathbb{Q}$ has totally degenerate, trivalent reduction mod 2, then

$$\#\left(X \cap \mathrm{Jac}_{X,\mathit{tors}}\right)(\mathbb{C}) \leq N'(g)$$

The second corollary is a big improvement

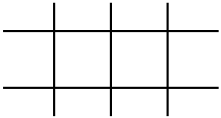
1. It requires working over a non-discretely valued field.
2. The bound only depends on the reduction type.
3. Integration over wide opens (c.f. Coleman) instead of discs and annuli.

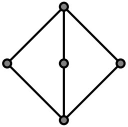
Berkovich picture



Baker–Payne–Rabinoff and the slope formula

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





(**Contraction Theorem**) $\tau\colon X^{\mathrm{an}} \to \Gamma$.

(**Combinatorial harmonic analysis/potential theory**)

f	a meromorphic function on X^{an}
$F := (-\log\lvert f\rvert)\big\rvert_\Gamma$	associated tropical, piecewise linear function
$\operatorname{div} F$	combinatorial record of the slopes of F

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

Berkovich picture