Diophantine and tropical geometry

David Zureick-Brown

Slides available at http://www.mathcs.emory.edu/~dzb/slides/

UW-Madison Colloquium
February 20, 2015

\[ a^2 + b^2 = c^2 \]
Basic Problem (Solving Diophantine Equations)

Analysis

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

Problem

Describe the set

$$\{(a_1, \ldots, a_n) \in R^n : \forall i, f_i(a_1, \ldots, a_n) = 0\}.$$
Basic Problem (Solving Diophantine Equations)

Analysis

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

Problem

*Describe the set*

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

Fact

*Solving diophantine equations is hard.*
The ring $R = \mathbb{Z}$ is especially hard.
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:** $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$;
- **output:** YES / NO according to whether the set

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

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:** $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$;
- **output:** YES / NO according to whether the set

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

is non-empty.

This is *still open* for many other rings (e.g., $R = \mathbb{Q}$).
The only solutions to the equation

\[ x^n + y^n = z^n, \ n \geq 3 \]

are multiples of the triples

\((0, 0, 0), (\pm 1, \mp 1, 0), \pm (1, 0, 1), (0, \pm 1, \pm 1)\).
Fermat’s Last Theorem

**Theorem (Wiles et. al)**

*The only solutions to the equation*

\[ x^n + y^n = z^n, \quad n \geq 3 \]

*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!
The only solutions to the equation

\[ x^n + y^n = z^n, \quad n \geq 3 \]

are multiples of the triples

(0, 0, 0), \ (±1, ±1, 0), \ ±(1, 0, 1), \ (0, ±1, ±1).

This took 300 years to prove!
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).
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?)
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

Lemma

The equation

\[ x^2 + y^2 = z^2 \]

has infinitely many non-zero coprime solutions.
Pythagorean triples

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

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

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

The solutions to

\[ a^2 + b^2 = c^2 \]

are all multiples of the triples

\[
\begin{align*}
  a &= 1 - t^2 \\
  b &= 2t \\
  c &= 1 + t^2
\end{align*}
\]
The Mordell Conjecture

Example
The equation $y^2 + x^2 = 1$ has infinitely many solutions.
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)
**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.
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.
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

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

\[ 3^2 + 4^2 = 5^2, \ 3 \cdot 4 = 2 \cdot 6 \]
$x^2 + y^2 = z^2, \ xy = 2 \cdot 157$
The pair of equations

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

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?
Congruent number problem

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

has \textbf{infinitely many} solutions. \textbf{How large} is the smallest solution? \textbf{How many digits} does the smallest solution have?

\[
\begin{align*}
x &= \frac{157841 \cdot 4947203 \cdot 52677109576}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441} \\
y &= \frac{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 52677109576} \\
z &= \frac{20085078913 \cdot 1185369214457 \cdot 942545825502442041907480}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 52677109576}
\end{align*}
\]
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?

\[
\begin{align*}
x & = \frac{157841 \cdot 4947203 \cdot 52677109576}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441} \\
y & = \frac{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 52677109576} \\
z & = \frac{20085078913 \cdot 1185369214457 \cdot 942545825502442041907480}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 52677109576}
\end{align*}
\]

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

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

- \( \text{Num, den}(x, y, z) \leq 10 \sim 10^6 \) many, \textbf{1 min} on Emory’s computers.
Back of the envelope calculation

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

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

\[ \frac{\text{many}}{\text{minutes}} = \frac{\text{many}}{\text{years}} \]
Back of the envelope calculation

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

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

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

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

\[
\]
The only solutions to the equation

\[ x^n + y^n = z^n + w^n, \quad n \geq 5 \]

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

Conjecture
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

1. \(10^{16}\) years to find via brute force.
2. Age of the universe – \(13.75 \pm 0.11\) billion years (roughly \(10^{10}\)).
Theorem (Poonen, Schaefer, Stoll)

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

\[
(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm (0, 1, 1),
\]
The coprime integer solutions to $x^2 + y^3 = z^7$ are the 16 triples

$(\pm 1, -1, 0), \ (\pm 1, 0, 1), \ \pm(0, 1, 1), \ (\pm 3, -2, 1), \ \ldots$
Fermat-like equations

Theorem (Poonen, Schaefer, Stoll)

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

\[(\pm 1, -1, 0), \ (\pm 1, 0, 1), \ \pm (0, 1, 1), \ (\pm 3, -2, 1), \ (\pm 71, -17, 2),\]
Fermat-like equations

Theorem (Poonen, Schaefer, Stoll)

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

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

What are the solutions to the equation $x^a + y^b = z^c$?
**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* $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 < 0$. 
Conjecture (Beal, Granville, Tijdeman-Zagier)

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

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

\[
\frac{1}{2} + \frac{1}{3} + \frac{1}{7} - 1 = -\frac{1}{42} < 0
\]
Examples of Generalized Fermat Equations

**Theorem (Poonen, Schaefer, Stoll)**

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

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

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

\[
\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0
\]
Examples of Generalized Fermat Equations

Theorem (Darmon, Merel)

Any pairwise coprime solution to the equation

\[ x^n + y^n = z^2, \; n > 4 \]

satisfies \( xyz = 0 \).

\[ \frac{1}{n} + \frac{1}{n} + \frac{1}{2} - 1 = \frac{2}{n} - \frac{1}{2} < 0 \]
The ideas behind the proof of FLT now permeate the study of diophantine problems.
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*

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

\[ x^2 + y^3 = z^5 \]

\[ \frac{1}{2} + \frac{1}{3} + \frac{1}{5} - 1 = \frac{1}{30} > 0 \]
Theorem (Klein, Zagier, Beukers, Edwards, others)

The equation

\[ x^2 + y^3 = z^5 \]

has infinitely many coprime solutions

\[ \frac{1}{2} + \frac{1}{3} + \frac{1}{5} - 1 = \frac{1}{30} > 0 \]
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.

<table>
<thead>
<tr>
<th>Set</th>
<th>Authors/Contributions</th>
</tr>
</thead>
<tbody>
<tr>
<td>${n, n, n}$</td>
<td>Wiles, Taylor-Wiles, building on work of many others</td>
</tr>
<tr>
<td>${2, n, n}$</td>
<td>Darmon-Merel, others for small $n$</td>
</tr>
<tr>
<td>${3, n, n}$</td>
<td>Darmon-Merel, others for small $n$</td>
</tr>
<tr>
<td>${5, 2n, 2n}$</td>
<td>Bennett</td>
</tr>
<tr>
<td>${(2, 4, n)}$</td>
<td>Ellenberg, Bruin, Ghioca $n \geq 4$</td>
</tr>
<tr>
<td>${(2, n, 4)}$</td>
<td>Bennett-Skinner; $n \geq 4$</td>
</tr>
<tr>
<td>${2, 3, n}$</td>
<td>Poonen-Shaefer-Stoll, Bruin. $6 \leq n \leq 9$</td>
</tr>
<tr>
<td>${2, 2\ell, 3}$</td>
<td>Chen, Dahmen, Siksek; primes $7 &lt; \ell &lt; 1000$ with $\ell \neq 31$</td>
</tr>
<tr>
<td>${3, 3, n}$</td>
<td>Bruin; $n = 4, 5$</td>
</tr>
<tr>
<td>${3, 3, \ell}$</td>
<td>Kraus; primes $17 \leq \ell \leq 10000$</td>
</tr>
<tr>
<td>${(2, 2n, 5)}$</td>
<td>Chen $n \geq 3^*$</td>
</tr>
<tr>
<td>${(4, 2n, 3)}$</td>
<td>Bennett-Chen $n \geq 3$</td>
</tr>
<tr>
<td>${(6, 2n, 2)}$</td>
<td>Bennett-Chen $n \geq 3$</td>
</tr>
<tr>
<td>${(2, 6, n)}$</td>
<td>Bennett-Chen $n \geq 3$</td>
</tr>
</tbody>
</table>
$(p, q, r)$ 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 $n \geq 3$ |
| $(2, 3, 10)$  | ZB |
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.
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.
Coleman’s bound

**Theorem (Coleman)**

Let $X$ be a curve of genus $g$ and let $r = \text{rank}_\mathbb{Z} \text{Jac}_X(\mathbb{Q})$. 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. Note: this does not prove uniformity (since the first good $p$ might be large).

**Tools**

$p$-adic integration and Riemann–Roch
(\textit{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,

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

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

\textbf{(Riemann-Roch)} $\sum n_P = 2g - 2$.

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

---

\text\text{David Zureick-Brown} (Emory University) \hspace{1cm} \text{Diophantine and tropical geometry} \hspace{1cm} \text{February 20, 2015} \hspace{1cm} \text{36 / 42}
Example (from McCallum-Poonen’s survey paper)

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

\[
\begin{align*}
x &= p \cdot t, \text{ where } t \in \mathbb{Z}_p \\
y &= \sqrt{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1} = 1 + x^2 + \cdots
\end{align*}
\]

2. \[
\int_{P_{(0,1)}}^{P_t} \frac{xdx}{y} = \int_{0}^{t} (x - x^3 + \cdots)dx
\]
Chabauty’s method

\textbf{\((p\text{-adic integration})\) There exists} \( V \subset H^0(X_{Q_p}, \Omega^1_X) \) \text{ with} 
\[ \dim_{Q_p} V \geq g - r \] 
\text{such that,} 
\[ \int_P^Q \omega = 0 \quad \forall P, Q \in X(Q), \omega \in V \]

\textbf{(Coleman, via Newton Polygons) Number of zeroes in a residue} 
\text{disc} \( D_P \) \text{ is} \( \leq 1 + n_P \), \text{ where} 
\[ n_P = \# (\text{div} \omega \cap D_P) \]

\textbf{(Riemann-Roch)} \[ \sum n_P = 2g - 2. \]

\textbf{(Coleman’s bound)} \[ \sum_{P \in X(F_p)} (1 + n_P) = \#X(F_p) + 2g - 2. \]
Theorem (Stoll)

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

Let $\mathcal{X}$ be a stable proper model of $X$. 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 (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 \( r \leq g - 2 \). Let \( e = 3(g+1)^2(4g-4) \). Then

\[
\#X(\mathbb{Q}) \leq (2g - 2)6 + 2g\sqrt{2}) \ N_2(1/e, 2g - 2)
\]

where

\[
N_p(A, B) := \min \left\{ N \text{ s.t. } p^N \geq N^{1/A} p^B \right\}.
\]

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
### Corollary ((Partially) effective Manin-Mumford)

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

$$\#(X \cap \text{Jac}_{X,tors})(\mathbb{Q}) \leq N(g)$$

### 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

$$\#(X \cap \text{Jac}_{X,tors})(\mathbb{C}) \leq N'(g)$$

### 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.
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 $X^\text{an}$

$F := (−\log |f|)|_\Gamma$ associated tropical, piecewise linear function

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

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