Diophantine and tropical geometry

David Zureick-Brown

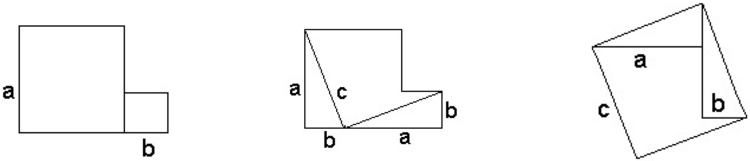
joint with Eric Katz (Waterloo) and Joe Rabinoff (Georgia Tech)

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

SERMON

March 28-29, 2015

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



Basic Problem (Solving Diophantine Equations)

Analysis

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

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)

Analysis

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

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

$$(0,0,0), \quad (\pm1,\mp1,0), \quad \pm(1,0,1), \quad (0,\pm1,\pm1).$$

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

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

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

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

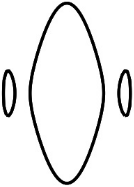
Why is Fermat's last theorem believable?

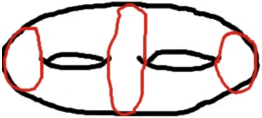
1. $x^n + y^n - z^n = 0$ looks like a surface (3 variables)
2. $x^n + y^n - 1 = 0$ looks like a curve (2 variables)

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 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.

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.

Coleman's bound

Theorem (Coleman)

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

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

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

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

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 $n_P = \#(\operatorname{div}\omega \cap D_P)$

(**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)

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 (partial uniformity for curves)

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 $r \leq g - 2$. Then

$$\#X(\mathbb{Q}) \leq 84g^2 - 123g + 48$$

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

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

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

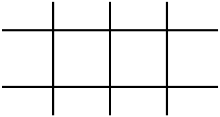
$$\#\left(X \cap \mathrm{Jac}_{X,tors}\right)(\mathbb{C}) \leq N'(g)$$

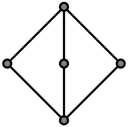
The second corollary is a big improvement

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.

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}
$F := (-\log\|f\|)\big\|_\Gamma$	associated tropical, piecewise linear function
$\operatorname{div} F$	combinatorial record of the slopes of F

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