Diophantine and $p$-adic geometry

David Zureick-Brown
joint with Eric Katz (Waterloo) and Joe Rabinoff (Georgia Tech)

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

Spring Lecture Series, Fayetteville, AR
April 6, 2018
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); Theorem (Faltings, Bombieri, Vojta)**

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

This can be used to provably compute $X(\mathbb{Q})$. 
Example (Gordon, Grant)

\[ y^2 = x(x - 1)(x - 2)(x - 5)(x - 6) \]

Analysis

1. \( \text{rank}_{\mathbb{Z}} \text{Jac}_X(\mathbb{Q}) = 1, \ g = 2 \)
2. \( X(\mathbb{Q}) \) contains
   \[ \{ \infty, (0,0), (1,0), (2,0), (5,0), (6,0), (3, \pm 6), (10, \pm 120) \}. \]
3. \( \#X(\mathbb{F}_7) = 8 \)
4. \( 10 \leq \#X(\mathbb{Q}) \leq \#X(\mathbb{F}_7) + 2g - 2 = 10 \)

This determines \( X(\mathbb{Q}) \).
**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
Chabauty’s method

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

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

\((p\text{-adic Rolle’s (Coleman), via Newton Polygons})\)
Number of zeroes in a residue disc \(D_P\) is \(\leq 1 + n_P\), where

\[n_P = \#(\text{div} \omega \cap D_P)\]

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

\((\text{Coleman’s bound})\) \(\sum_{P \in X(F_p)} (1 + n_P) = \#X(F_p) + 2g - 2\).
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 \( \widetilde{Q} = (0, 1) \) are given by

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

\[
y = \sqrt{x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1} = 1 + x^2 + \cdots
\]

2. \[
\int_{(0,1)}^{P_t} \frac{x \, dx}{y} = \int_0^t (x - x^3 + \cdots) \, dx
\]
Chabauty’s method

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

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

(*$p$*-adic Rolle’s (Coleman), via Newton Polygons)
Number of zeroes in a residue disc $D_P$ is $\leq 1 + n_P$, where

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

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

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

Theorem (Lorenzini-Tucker, McCallum-Poonen)

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. Suppose $r < g$.

Let $\mathcal{X}$ be a regular proper model of $X$. Then

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

Remark (Still doesn’t prove uniformity)

$\#\mathcal{X}^{\text{sm}}(\mathbb{F}_p)$ can contain an $n$-gon, for $n$ arbitrarily large.

Tools

$p$-adic integration and arithmetic Riemann–Roch ($\mathcal{K} \cdot \mathcal{X}_p = 2g - 2$)
Models – semistable example

\[ y^2 = (x(x - 1)(x - 2))^3 - 5 \]
\[ = (x(x - 1)(x - 2))^3 \mod 5. \]

Note: no point can reduce to \((0, 0)\). Local equation looks like \(xy = 5\).
Models – semistable example (not regular)

\[ y^2 = (x(x - 1)(x - 2))^3 - 5^4 \]
\[ = (x(x - 1)(x - 2))^3 \mod 5 \]

Now: \((0, 5^2)\) reduces to \((0, 0)\). Local equation looks like \(xy = 5^4\)
Models – semistable example

\[ y^2 = (x(x - 1)(x - 2))^3 - 5^4 \]

\[ = (x(x - 1)(x - 2))^3 \quad \text{mod} \; 5 \]

Blow up. Local equation looks like \( xy = 5^3 \)
Models – semistable example (regular at (0,0))

\[ y^2 = (x(x - 1)(x - 2))^3 - 5^4 \]

\[ = (x(x - 1)(x - 2))^3 \mod 5 \]

Blow up. Local equation looks like \( xy = 5 \)
**Theorem (Lorenzini-Tucker, McCallum-Poonen)**

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. Suppose $r < g$.

Let $\mathcal{X}$ be a regular proper model of $X$. Then

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

**Remark (Still doesn’t prove uniformity)**

$\#\mathcal{X}^{\text{sm}}(\mathbb{F}_p)$ can contain an $n$-gon, for $n$ arbitrarily large.

**Tools**

$p$-adic integration and arithmetic Riemann–Roch ($\mathcal{K} \cdot \mathcal{X}_p = 2g - 2$)
Stoll’s hyperelliptic uniformity theorem

Theorem (Stoll)

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

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
- \( p \)-adic Rolle’s on hyperelliptic annuli
Analytic continuation of integrals

(Residue Discs.)
\[ P \in \mathcal{X}^{\text{sm}}(\mathbb{F}_p), \ t: D_P \cong p\mathbb{Z}_p, \ \omega|_{D_P} = f(t)dt \]

(Integrals on a disc.)
\[ Q, R \in D_P, \ \int_{Q}^{R} \omega := \int_{t(Q)}^{t(R)} f(t)dt. \]

(Integrals between discs.)
\[ Q \in D_{P_1}, \ R \in D_{P_2}, \ \int_{Q}^{R} \omega := ? \]
Analytic continuation of integrals via Abelian varieties

(Integrals between discs.)

\[ Q \in D_{P_1}, \ R \in D_{P_2}, \ \int_Q^R \omega := ? \]

(Albanese map.)

\[ \iota : X \hookrightarrow \text{Jac}_X, \ Q \mapsto [Q - \infty] \]

(Abelian integrals via functorality and additivity.)

\[
\int_Q^R \iota^* \omega = \int_{\iota(Q)}^{\iota(R)} \omega = \int_{[Q-\infty]}^{[R-\infty]} \omega = \int_0^{[R-Q]} \omega = \frac{1}{n} \int_0^{n[R-Q]} \omega
\]
(Integrals between discs.)

\[ Q \in D_{P_1}, \ R \in D_{P_2}, \int_Q^R \omega := ? \]

(Integrals via functorality and Frobenius.)

\[ \int_Q^R \omega = \int_Q^\phi(Q) \omega + \int_{\phi(Q)}^\phi(R) \omega + \int_{\phi(R)}^R \omega \]

(Very clever trick (Coleman))

\[ \int_{\phi(Q)}^{\phi(R)} \omega_i = \int_Q^R \phi^* \omega_i = df_i + \sum_j \int_Q^R a_{ij} \omega_j \]
Comparison of integrals

Facts

1. For $X$ with good reduction, the **Abelian** and **Coleman** integrals agree.
2. A mystery. The associated Berkovich curve is contractable.
3. For $X$ with bad reduction they differ.

Theorem (Stoll; Katz–Rabinoff–Zureick-Brown)

There exist linear functions $a(\omega), c(\omega)$ such that

$$\oint_R \omega - \int_Q \omega = a(\omega) [\log(t(R)) - \log(t(Q))] + c(\omega) [t(R) - t(Q)]$$
Assumption

Assume $\mathcal{X}/\mathbb{Z}_p$ is **stable**, but not regular.

(Residue Discs.)

\[
P \in \mathcal{X}^{\text{sm}}(\overline{\mathbb{F}}_p), \ t: D_P \cong p\mathbb{Z}_p, \ \omega|_{D_P} = f(t)dt
\]

(Residue Annuli.)

\[
P \in \mathcal{X}^{\text{sing}}(\overline{\mathbb{F}}_p), \ t: D_P \cong p\mathbb{Z}_p - p^r\mathbb{Z}_p, \ \omega|_{D_P} = f(t, t^{-1})dt
\]

(Integrals on an annulus are multivalued.)

\[
\int_{Q}^{R} \omega := \int_{t(Q)}^{t(R)} f(t, t^{-1})dt = \cdots + a(\omega) \log t(R) + \cdots
\]

(Cover the annulus with discs)

Each analytic continuation implicitly chooses a branch of log.
(Abelian integrals.) Analytically continue via Albanese.
\[ \oint_Q \omega = 0 \text{ if } R, Q \in X(\mathbb{Q}), \omega \in V \]

(Berkovich-Coleman integrals.) Analytically continue via Frobenius.
\[ \int_Q \omega := \int_{t(Q)}^{t(R)} f(t, t^{-1})dt = \cdots + a(\omega) \log_{\text{Col}} t(R) + \cdots \]

(Stoll’s theorem.)
\[ \oint_Q \omega - \int_Q \omega = a(\omega) (\log_{ab}(r(R)) - \log_{ab}(t(Q))) + c(\omega) (t(Q) - t(R)) \]
Berkovich picture

\[ X^{an} \]
Theorem (Katz, Rabinoff, ZB)

The difference $\log_{\text{Col}} - \log_{\text{ab}}$ is the unique homomorphism that takes the value

$$\int_{\gamma} \omega$$

on $\text{Trop}(\gamma)$, where $\text{Trop}: G(\mathbb{K}) \rightarrow T(\mathbb{K})/T(\mathcal{O})$.

$T = \text{torus}, \Lambda = \text{discrete}, \text{and } B = \text{Abelian with good reduction.}$
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 Rolle’s on annuli for arbitrary curves
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) $\tau : X^{an} \to \Gamma$.

(Combinatorial harmonic analysis/potential theory)

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

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

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

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