Computing integral points on hyperelliptic curves

Steffen Müller
Carl von Ossietzky Universität Oldenburg
joint with Jennifer Balakrishnan and Amnon Besser

Mathematics Colloquium
Jacobs University Bremen

Monday, October 6, 2014

Diophantine equations

Definition. A diophantine equation is an equation of the form

$$h = 0\,,$$

where $h \in \mathbb{Z}[x_1, \ldots, x_n]$ is not constant.

- Named for Diophantus of Alexandria (3rd century A.D.), author of the *Arithmetica*
- We're usually interested in integral or rational solutions.
- In this talk, we're going to concentrate on integral solutions.

Fermat and Pythagoras

Theorem (Wiles, 1994). If $n > 2$ is an integer, then the diophantine equation

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

has no integral solutions (x, y, z) such that $xyz \neq 0$.

- "conjectured" by Fermat around 1637

Fermat and Pythagoras

Theorem (Wiles, 1994). If $n > 2$ is an integer, then the diophantine equation

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

has no integral solutions (x, y, z) such that $xyz \neq 0$.

- "conjectured" by Fermat around 1637

For $n = 2$, there are infinitely many solutions, including Pythagorean triples.

- Dehomogenizing gives an equation for the unit circle.
- Nontrivial integral solutions correspond to rational points on the unit cicle.
- We can find all such points using projection onto a rational line.

So geometry is useful to study diophantine equations.

Main problems

Given a diophantine equation, we usually ask the following questions:

(I) Is there at least one integral solution?
(II) Are there finitely many integral solutions?
(III) Can we list or parametrize all integral solutions?

We can ask the same questions for rational solutions.

Hilbert's tenth problem

Problem (Hilbert, 1900).
Find an algorithm that, given a diophantine equation, decides whether there is an integral solution or not.

Hilbert's tenth problem

Problem (Hilbert, 1900).
Find an algorithm that, given a diophantine equation, decides whether there is an integral solution or not.

Theorem (Matiyasevich, 1970).
Such an algorithm cannot exist.

The proof

- uses techniques from mathematical logic;
- builds on earlier work of Robinson, Davis and Putnam.

Nobody knows if such an algorithm can exist for rational solutions!

Pell's equation

Let D be a positive integer and consider

$$y^2 = Dx^2 + 1.$$

Pell's equation

Let D be a positive integer and consider

$$y^2 = Dx^2 + 1.$$

If $D = N^2$ is a square, then

$$y^2 - Dx^2 = (y - Nx)(y + Nx) = 1$$

only has the integral solutions $(0, \pm 1)$.

Pell's equation

Let D be a positive integer and consider

$$y^2 = Dx^2 + 1.$$

If $D = N^2$ is a square, then

$$y^2 - Dx^2 = (y - Nx)(y + Nx) = 1$$

only has the integral solutions $(0, \pm 1)$.

If D is not a square, then the integral solutions form an infinite group, isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Pell's equation

Let D be a positive integer and consider

$$y^2 = Dx^2 + 1.$$

If $D = N^2$ is a square, then

$$y^2 - Dx^2 = (y - Nx)(y + Nx) = 1$$

only has the integral solutions $(0, \pm 1)$.

If D is not a square, then the integral solutions form an infinite group, isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example. For $D = 61$, the smallest integral solution is

$$(226153980, 1766319049).$$

Siegel's theorem

We now restrict to diophantine equations of the form

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

where $f \in \mathbb{Z}[x]$ has degree $d > 2$ and is separable.

Siegel's theorem

We now restrict to diophantine equations of the form

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

where $f \in \mathbb{Z}[x]$ has degree $d > 2$ and is separable.

Theorem (Siegel, 1929).
There are only finitely many integral solutions.

Siegel's theorem

We now restrict to diophantine equations of the form

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

where $f \in \mathbb{Z}[x]$ has degree $d > 2$ and is separable.

Theorem (Siegel, 1929).
There are only finitely many integral solutions.

Unfortunately, the proof is completely ineffective, so we can't use it to

- decide whether there is at least one integral solution;
- list all integral solutions.

In the remainder of this talk, we discuss how to tackle these problems in practice.

Baker's theorem

Theorem (Baker, 1970).
There is an explicitly computable constant c_f such that we have

$$|x| \leq c_f$$

for every pair $(x, y) \in \mathbb{Z}^2$ satisfying $y^2 = f(x)$.

Baker's theorem

Theorem (Baker, 1970).
There is an explicitly computable constant c_f such that we have

$$|x| \le c_f$$

for every pair $(x, y) \in \mathbb{Z}^2$ satisfying $y^2 = f(x)$.

So there's an obvious algorithm for listing all integral solutions:

- Compute c_f.
- Test for all $x \in \mathbb{Z}$ such that $|x| \le c_f$ whether $f(x)$ is a square.

An Example

Unfortunately c_f is usually too large for practical purposes.

An Example

Unfortunately c_f is usually too large for practical purposes.

Example. For $f(x) = x^5 - 16x + 8$, Baker's original papers give

$$c_f \approx 10^{10^{10^{600}}}.$$

An Example

Unfortunately c_f is usually too large for practical purposes.

Example. For $f(x) = x^5 - 16x + 8$, Baker's original papers give

$$c_f \approx 10^{10^{10^{600}}}.$$

Improving Baker's bounds is still an active field of research.

For $f = x^5 - 16x + 8$, improvements due to Matveev, Györy and Bugeaud give

$$c_f \approx 10^{600}$$

Still much too large for the naive algorithm above!

Hyperelliptic curves

Idea. Use a geometric approach.

Suppose that $f \in \mathbb{Z}[x]$

- is separable and
- has odd degree $2g + 1 > 2$.

Then the equation $y^2 = f(x)$ defines a smooth affine curve.

Its smooth projective model C is a hyperelliptic curve of genus $g > 0$.

The points on C are of the form

- (x, y), where $y^2 = f(x)$ or
- the unique point $O \in C$ at infinity.

Elliptic curves

If $g = 1$, the curve C is an elliptic curve.

For every extension field K of $\mathbb{Q}$, the set of K-rational points

$$C(K) = \{(x, y) \in K^2 : y^2 = f(x)\} \cup \{O\}$$

forms a group.

Elliptic curves

If $g = 1$, the curve C is an elliptic curve.

For every extension field K of $\mathbb{Q}$, the set of K-rational points

$$C(K) = \{(x, y) \in K^2 : y^2 = f(x)\} \cup \{O\}$$

forms a group.

The group law can be defined geometrically and the group operations are regular functions on C.
Hence C is a one-dimensional abelian variety: a projective variety with compatible group structure.

The group structure is extremely helpful in analyzing rational and integral points on C.

Divisors

If $g > 1$, then C is not an abelian variety, but we can embed C into an abelian variety.

A divisor on C is a finite formal sum $D = \sum_{P \in C} n_P \cdot P$, where all $n_p \in \mathbb{Z}$.

- The degree of $\sum_P n_P \cdot P$ is $\sum_P n_P$.
- Divisors on C carry an obvious group structure.
- Let Div_C^0 denote the subgroup of degree 0 divisors.

Divisors

If $g > 1$, then C is not an abelian variety, but we can embed C into an abelian variety.

A divisor on C is a finite formal sum $D = \sum_{P \in C} n_P \cdot P$, where all $n_p \in \mathbb{Z}$.

- The degree of $\sum_P n_P \cdot P$ is $\sum_P n_P$.
- Divisors on C carry an obvious group structure.
- Let Div_C^0 denote the subgroup of degree 0 divisors.

A rational function $\varphi \in \mathbb{Q}(C)^\times$ defines a divisor

$$\text{div}(\varphi) = \sum_{P \in C} \mathrm{ord}_P(\varphi) \cdot P,$$

where ord_P is the order of vanishing in P.

- Such divisors are called principal.
- They form a subgroup Prin_C of Div_C^0.

Jacobians

We define

$$\mathrm{Pic}^0_C := \mathsf{Div}^0_C / \mathrm{Prin}_C.$$

The absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the divisors. This induces an action on Pic^0_C and we define

$$\mathrm{Pic}^0_C(\mathbb{Q}) := (\mathrm{Pic}^0_C)^{G_{\mathbb{Q}}}.$$

Jacobians

We define

$$\mathrm{Pic}^0_C := \mathsf{Div}^0_C / \mathrm{Prin}_C.$$

The absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the divisors.
This induces an action on Pic^0_C and we define

$$\mathrm{Pic}^0_C(\mathbb{Q}) := (\mathrm{Pic}^0_C)^{G_{\mathbb{Q}}}.$$

Theorem (Weil, 1948)

There is an abelian variety J of dimension g such that

$$J(\mathbb{Q}) = \mathrm{Pic}^0_C(\mathbb{Q}),$$

where $J(\mathbb{Q})$ denotes the $\mathbb{Q}$-rational points on J.

Jacobians

We define

$$\mathrm{Pic}^0_C := \mathrm{Div}^0_C / \mathrm{Prin}_C.$$

The absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the divisors.
This induces an action on Pic^0_C and we define

$$\mathrm{Pic}^0_C(\mathbb{Q}) := (\mathrm{Pic}^0_C)^{G_{\mathbb{Q}}}.$$

Theorem (Weil, 1948)

There is an abelian variety J of dimension g such that

$$J(K) = \mathrm{Pic}^0_C(K)$$

for every extension field K of $\mathbb{Q}$, where $J(K)$ denotes the K-rational points on J.

Properties of Jacobians

We call J the Jacobian of C.

- If $g = 1$, then J is isomorphic to C.
- We can embed C into J via $\iota(P) = [P - O]$.
  - Since O is $\mathbb{Q}$-rational, this embeds $C(\mathbb{Q})$ into $J(\mathbb{Q})$.
  - So we can use information on $J(\mathbb{Q})$ to get information on $C(\mathbb{Q})$.
- The group $J(\mathbb{Q})$ is called the Mordell-Weil group of $J/\mathbb{Q}$.

Mordell-Weil

Theorem (Mordell-Weil, 1920's).
The group $J(\mathbb{Q})$ is finitely generated. In other words, we have

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \times J(\mathbb{Q})_{\mathrm{tors}}$$

where

- the rank r is a nonnegative integer and
- the torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}} \subset J(\mathbb{Q})$ is finite.

Mordell-Weil

Theorem (Mordell-Weil, 1920's).
The group $J(\mathbb{Q})$ is finitely generated. In other words, we have

$$J(\mathbb{Q}) \cong \mathbb{Z}^r \times J(\mathbb{Q})_{\mathrm{tors}}$$

where

- the rank r is a nonnegative integer and
- the torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}} \subset J(\mathbb{Q})$ is finite.

In practice, we can

- always compute $J(\mathbb{Q})_{\mathrm{tors}}$;
- often compute r, though no general algorithm is known;
- sometimes compute generators of $J(\mathbb{Q})$ when $g \leq 3$ and the coefficients of f are reasonably small.

BMSST

Bugeaud-Mignotte-Siksek-Stoll-Tengely have an algorithm that can compute all integral points $(x, y) \in C(\mathbb{Q})$ such that $|x| \leq c'_f \approx 10^{2000}$ provided we have generators for $J(\mathbb{Q})$.

Combined with the upper bound c_f obtained using Baker's method, can list all integral points.

BMSST

Bugeaud-Mignotte-Siksek-Stoll-Tengely have an algorithm that can compute all integral points $(x, y) \in C(\mathbb{Q})$ such that $|x| \leq c'_f \approx 10^{2000}$ provided we have generators for $J(\mathbb{Q})$.

Combined with the upper bound c_f obtained using Baker's method, can list all integral points.

- Currently this is only applicable for $g \leq 3$.
- Even then, computing generators for $J(\mathbb{Q})$ is usually quite difficult (and often impossible).

Most other approaches rely on p-adic analysis.

Reduction and p-adics

- p: prime of good reductioan for C, i.e. $p \nmid 2 \cdot \mathrm{disc}(f)$
- $\tilde{f} := f \bmod p \in \mathbb{F}_p[x]$

Then $y^2 = \tilde{f}(x)$ defines a hyperelliptic curve $\widetilde{C}$.

Reduction and p-adics

- p: prime of good reductioan for C, i.e. $p \nmid 2 \cdot \mathrm{disc}(f)$
- $\tilde{f} := f \bmod p \in \mathbb{F}_p[x]$

Then $y^2 = \tilde{f}(x)$ defines a hyperelliptic curve $\widetilde{C}$.

Let $\mathbb{Q}_p$ denote the field of p-adic numbers, the completion of $\mathbb{Q}$ wrt. the absolute value

$$\left|p^n \frac{a}{b}\right|_p = p^{-n}, \quad p \nmid ab.$$

- Can define the reduction $\tilde{P} \in \widetilde{C}(\mathbb{F}_p)$ of a point $P \in C(\mathbb{Q}_p)$.
- We want to do analysis on $C(\mathbb{Q}_p)$.
- In particular, we want a well-behaved integration theory on $C(\mathbb{Q}_p)$.

Residue disks

Problem: Topologically, $C(\mathbb{Q}_p)$ is totally disconnected.

We can write $C(\mathbb{Q}_p)$ as a disjoint union of residue disks

$$C(\mathbb{Q}_p) = \bigcup_{Q \in \widetilde{C}(\mathbb{F}_p)} \mathcal{D}_Q,$$

where

$$\mathcal{D}_Q = \{P \in C(\mathbb{Q}_p) \,:\, P \text{ reduces to } Q \bmod p\}.$$

It's easy to define p-adic integrals (e.g. of holomorphic differentials) inside residue disks, but how can we integrate from one disk to another?

Coleman integration

Coleman constructed path-independent p-adic integrals $\int_P^Q \omega$ for $P, Q \in C(\mathbb{Q}_p)$ and a meromorphic 1-form ω on $C(\mathbb{Q}_p)$, regular at P and Q.

Coleman integration

Coleman constructed path-independent p-adic integrals $\int_P^Q \omega$ for $P, Q \in C(\mathbb{Q}_p)$ and a meromorphic 1-form ω on $C(\mathbb{Q}_p)$, regular at P and Q.

Properties.

- Linearity: $\int_P^Q (\alpha\omega_1 + \beta\omega_2) = \alpha \int_P^Q \omega_1 + \beta \int_P^Q \omega_2$.
- Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$.
- Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$.
- $\int_D \omega = 0$ if $D \in \mathrm{Div}^0(C)$ represents a torsion point on J.
- Coleman integrals can be computed in practice (Balakrishnan, 2010).

More generally, we can define and compute iterated Coleman integrals, e.g. double integrals:

$$\int_P^Q \eta \cdot \omega := \int_P^Q \eta(R) \int_P^R \omega.$$

Differentials

The holomorphic differentials on $C(\mathbb{Q}_p)$ are generated by $\omega_0, \ldots, \omega_{g-1}$, where

$$\omega_i = \frac{x^i dx}{2y}.$$

We define

$$f_i(P) := \int_O^P \omega_i$$

on $C(\mathbb{Q}_p)$.

- By properties of the Coleman integral, can extend these to $J(\mathbb{Q}_p)$.
- By restriction, get $\mathbb{Q}_p$-valued functionals $f_0, \ldots, f_{g-1}$ on $J(\mathbb{Q})$.

Chabauty's theorem

Theorem (Chabauty, 1941).
Suppose that $g \geq 2$ and $r < g$. Then there exist $\alpha_0, \ldots, \alpha_{g-1} \in \mathbb{Q}_p$, not all equal to 0, such that

$$\sum_{i=0}^{g-1} \alpha_i f_i(P)$$

vanishes on $J(\mathbb{Q})$.

Chabauty's theorem

Theorem (Chabauty, 1941).
Suppose that $g \geq 2$ and $r < g$. Then there exist $\alpha_0, \ldots, \alpha_{g-1} \in \mathbb{Q}_p$, not all equal to 0, such that

$$\sum_{i=0}^{g-1} \alpha_i f_i(P)$$

vanishes on $J(\mathbb{Q})$.

Proof. The p-adic closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ has dimension at most $r < g$.

Chabauty's theorem

Theorem (Chabauty, 1941).
Suppose that $g \geq 2$ and $r < g$. Then there exist $\alpha_0, \ldots, \alpha_{g-1} \in \mathbb{Q}_p$, not all equal to 0, such that

$$\sum_{i=0}^{g-1} \alpha_i f_i(P)$$

vanishes on $J(\mathbb{Q})$.

Proof. The p-adic closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ has dimension at most $r < g$.

Corollary.

$$\rho(P) := \sum_{i=0}^{g-1} \alpha_i f_i(\iota(P))$$

vanishes on $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$.

Chabauty's Theorem II

- On a residue disk $\mathcal{D}$ of $C(\mathbb{Q}_p)$, can write $\rho|_{\mathcal{D}}$ as a convergent p-adic power series.
- Such power series only have finitely many zeroes which we can compute in practice to finite precision p^N.

Corollary. If $g \geq 2$ and $r < g$, then there are only finitely many rational points on C.

Chabauty's Theorem II

- On a residue disk $\mathcal{D}$ of $C(\mathbb{Q}_p)$, can write $\rho|_{\mathcal{D}}$ as a convergent p-adic power series.
- Such power series only have finitely many zeroes which we can compute in practice to finite precision p^N.

Corollary. If $g \geq 2$ and $r < g$, then there are only finitely many rational points on C.

This is superseded by Faltings' theorem: If $g \geq 2$, then $C(\mathbb{Q})$ is finite.

But, in contrast to Faltings' proof, Chabauty's proof can often be used in practice to actually find $C(\mathbb{Q})$ (and hence the integral points on C)!

- originally due to Coleman (1985)
- improved and applied by Flynn, Bruin, Stoll, Poonen, Schaefer
- can be combined with other methods, e.g. the Mordell-Weil sieve

Kim's program

What if $r \geq g$?

- In this case Chabauty fails completely, unless $\dim \overline{J(\mathbb{Q})} < g$.
- **Conjecture.** $r = g$ and J simple $\Rightarrow \dim \overline{J(\mathbb{Q})} = g$.
- Kim has a program to develop a "non-abelian" Chabauty method.
    - replace single Coleman-integrals by iterated Coleman integrals
    - replace the Jacobian by a higher-dimensional "Selmer variety"
- First step: Make this practical for $r = g$ and integral points!

$r = g$: strategy

Recall Chabauty's idea:

- We have $\mathbb{Q}_p$-valued functionals $f_0, \ldots, f_{g-1}$ on $J(\mathbb{Q})$.
- So if $r < g$, then some linear combination of the f_i must vanish on $J(\mathbb{Q})$.
- Compose with $\iota : C(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$ to get a function that
  - vanishes on $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$,
  - can be written as a convergent power series on every residue disk.

$r = g$: strategy

Recall Chabauty's idea:

- We have $\mathbb{Q}_p$-valued functionals $f_0, \ldots, f_{g-1}$ on $J(\mathbb{Q})$.
- So if $r < g$, then some linear combination of the f_i must vanish on $J(\mathbb{Q})$.
- Compose with $\iota : C(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$ to get a function that
  - vanishes on $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$,
  - can be written as a convergent power series on every residue disk.

Idea for $r = g$. Construct a $\mathbb{Q}_p$-valued quadratic form h on $J(\mathbb{Q})$ such that $h \circ \iota = \tau - \rho$ on $C(\mathbb{Q}_p)$, where

- ρ takes values on integral points in an explicitely computable finite set T;
- τ can be written as a convergent power series on every residue disk.

$r = g$: strategy

Recall Chabauty's idea:

- We have $\mathbb{Q}_p$-valued functionals $f_0, \ldots, f_{g-1}$ on $J(\mathbb{Q})$.
- So if $r < g$, then some linear combination of the f_i must vanish on $J(\mathbb{Q})$.
- Compose with $\iota : C(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$ to get a function that
  - vanishes on $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$,
  - can be written as a convergent power series on every residue disk.

Idea for $r = g$. Construct a $\mathbb{Q}_p$-valued quadratic form h on $J(\mathbb{Q})$ such that $h \circ \iota = \tau - \rho$ on $C(\mathbb{Q}_p)$, where

- ρ takes values on integral points in an explicitely computable finite set T;
- τ can be written as a convergent power series on every residue disk.

Then we can write $h = \sum_{1 \le i \le j \le g} \alpha_{ij} f_i f_j$, so ρ can be written as a convergent power series on every residue disk.

p-adic heights

The p-adic height

$$h : J(\mathbb{Q}) \to \mathbb{Q}_p$$

- is a quadratic form;
- was defined by several authors (Bernardi, Schneider, Perrin-Riou, Mazur-Tate, Coleman-Gross);
- has properties analogous to the canonical (or Néron-Tate) height;
- decomposes as a finite sum $h = \sum_q h_q$ over the prime numbers;
- is a linear combination

$$h = \sum_{1 \leq i \leq j \leq g} \alpha_{ij} f_i f_j$$

if $r = g$, since then the products $f_i f_j$, $1 \leq i \leq j \leq g$ form a basis of the $\mathbb{Q}_p$-valued quadratic forms on $J(\mathbb{Q})$.

Local heights at p

The local height h_p is given in terms of Coleman integration.

Theorem 1 (Balakrishnan-Besser-M., 2013) If $P \in C(\mathbb{Q}_p)$, then $h_p(\iota(P))$ is equal to a double Coleman integral

$$\tau(P) := h_p(\iota(P)) = \sum_{i=0}^{g-1} \int_O^P \omega_i \cdot \bar{\omega}_i,$$

where $\{\bar{\omega}_0, \cdots, \bar{\omega}_{g-1}\}$ are certain explicitly computable differentials on C.

Local heights at p

The local height h_p is given in terms of Coleman integration.

Theorem 1 (Balakrishnan-Besser-M., 2013) If $P \in C(\mathbb{Q}_p)$, then $h_p(\iota(P))$ is equal to a double Coleman integral

$$\tau(P) := h_p(\iota(P)) = \sum_{i=0}^{g-1} \int_O^P \omega_i \cdot \bar{\omega}_i,$$

where $\{\bar{\omega}_0, \cdots, \bar{\omega}_{g-1}\}$ are certain explicitly computable differentials on C.

In particular, $h_p = \tau$

- can be written as a convergent power series on every residue disk;
- can be computed in practice (Balakrishnan, 2011).

Local heights away from p

If $q \neq p$, then h_q is defined in terms of arithmetic intersection theory on a regular model of C over $\mathrm{Spec}(\mathbb{Z})$.

Local heights away from p

If $q \neq p$, then h_q is defined in terms of arithmetic intersection theory on a regular model of C over $\mathrm{Spec}(\mathbb{Z})$.

Theorem 2 (Balakrishnan-Besser-M., 2013) If $r = g$, then there is an explicitly computable finite set $T \subset \mathbb{Q}_p$ such that

$$\rho(P) := -\sum_{q \neq p} h_q(\iota(P)) = \tau(P) - h(\iota(P))$$

only takes values in T on integral points.

Local heights away from p

If $q \neq p$, then h_q is defined in terms of arithmetic intersection theory on a regular model of C over $\mathrm{Spec}(\mathbb{Z})$.

Theorem 2 (Balakrishnan-Besser-M., 2013) If $r = g$, then there is an explicitly computable finite set $T \subset \mathbb{Q}_p$ such that

$$\rho(P) := -\sum_{q \neq p} h_q(\iota(P)) = \tau(P) - h(\iota(P))$$

only takes values in T on integral points.

In practice, we can use Gröbner bases and linear algebra to compute

- $\rho(P)$ for given $P \in C(\mathbb{Q})$ (M., 2010);
- the set T.

Quadratic Chabauty

Theorem 1 and Theorem 2 can be used for the following algorithm, where $r = g$:

- Find representatives $D_1, \dots, D_g$ of nontorsion points in $J(\mathbb{Q})$, independent mod torsion.
- Compute
  - the global p-adic heights $h(D_j)$ and
  - the single Coleman integrals $\int_{D_j} \omega_i$
- Deduce α_{ij} such that $h = \sum_{1 \leq i \leq j \leq g} \alpha_{ij} f_i f_j$.
- Find power series expansions for τ and for the $f_i f_j$ in every residue disk,
- Compute the set T such that $\rho(P) \in T$ for all integral $P \in C(\mathbb{Q})$.
- Compute all solutions to $\rho(P) \in T$ across the various residue disks.

The integral points in $C(\mathbb{Q})$ will be contained in this solution set.

Example 1. Consider $C : y^2 = x^3(x-1)^2 + 1$

- C has genus $g = 2$.
- $J(\mathbb{Q})$ has rank 2 and trivial torsion.
- $Q_1 = (2, -3), Q_2 = (1, -1), Q_3 = (0, 1) \in C(\mathbb{Q})$ are integral points on C.

- Set $D_1 = Q_1 - O$, $D_2 = Q_2 - Q_3$, then
- the classes $[D_1]$ and $[D_2]$ in $J(\mathbb{Q})$ are independent.
- $p = 11$ is a prime of good reduction.

Example 1 continued

- Compute the height pairings $h(D_i, D_j)$ and the Coleman integrals $\int_{D_i}\omega_k \int_{D_j}\omega_l$ and deduce the α_{ij} from $(\alpha_{00}, \alpha_{01}, \alpha_{11})^t =$

$$\begin{pmatrix} \int_{D_1}\omega_0 \int_{D_1}\omega_0 & \int_{D_1}\omega_0 \int_{D_1}\omega_1 & \int_{D_1}\omega_1 \int_{D_1}\omega_1 \\ \int_{D_1}\omega_0 \int_{D_2}\omega_0 & \int_{D_1}\omega_0 \int_{D_2}\omega_1 & \int_{D_1}\omega_1 \int_{D_2}\omega_1 \\ \int_{D_2}\omega_0 \int_{D_2}\omega_0 & \int_{D_2}\omega_0 \int_{D_2}\omega_1 & \int_{D_2}\omega_1 \int_{D_2}\omega_1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} h(D_1, D_1) \\ h(D_1, D_2) \\ h(D_2, D_2) \end{pmatrix}$$

- Use power series expansions of τ and of the Coleman integrals f_i to give a convergent power series describing ρ in each residue disk.

- Compute

$$T = \{0,\ 1/2 \cdot \log_{11}(2),\ 2/3 \cdot \log_{11}(2)\}.$$

For example, on the residue disk containing $(0, 1)$, the only solutions to $\rho(P) \in T$ modulo 11^{11} have x-coordinate 0 or

$$4 \cdot 11 + 7 \cdot 11^2 + 9 \cdot 11^3 + 7 \cdot 11^4 + 9 \cdot 11^6 + 8 \cdot 11^7 + 11^8 + 4 \cdot 11^9 + 10 \cdot 11^{10}$$

Example 1 continued

For example, on the residue disk containing $(0,1)$, the only solutions to $\rho(P) \in T$ modulo 11^{11} have x-coordinate 0 or

$$4 \cdot 11 + 7 \cdot 11^2 + 9 \cdot 11^3 + 7 \cdot 11^4 + 9 \cdot 11^6 + 8 \cdot 11^7 + 11^8 + 4 \cdot 11^9 + 10 \cdot 11^{10}$$

Here are the recovered integral points and their corresponding ρ-values:

P	$\rho(P)$
$(2, \pm 3)$	$\frac{2}{3}\log(2)$
$(1, \pm 1)$	$\frac{1}{2}\log(2)$
$(0, \pm 1)$	$\frac{2}{3}\log(2)$

Additional solutions

- Recall that can find the (finitely many) $P \in C(\mathbb{Q}_p)$ such that $\rho(P) \in T$, up to some finite precision p^N.
- In general, some of these correspond to integral points $P \in C(\mathbb{Q})$, some don't.

Suppose that $P \in C(\mathbb{Q}_p)$ is a solution and we want to show that P does not correspond to a $\mathbb{Q}$-rational point.

Additional solutions

- Recall that can find the (finitely many) $P \in C(\mathbb{Q}_p)$ such that $\rho(P) \in T$, up to some finite precision p^N.
- In general, some of these correspond to integral points $P \in C(\mathbb{Q})$, some don't.

Suppose that $P \in C(\mathbb{Q}_p)$ is a solution and we want to show that P does not correspond to a $\mathbb{Q}$-rational point.

Simplifying assumptions:

- $g > 1$ (different methods exist for $g = 1$)
- $J(\mathbb{Q}) \cong \mathbb{Z}^g$ is free.
- We know generators $[D_1], \ldots, [D_g]$ of $J(\mathbb{Q})$.

Suppose P is $\mathbb{Q}$-rational. Then there are $a_1, \ldots, a_g \in \mathbb{Z}$ such that

$$\iota(z) = a_1[D_1] + \ldots + a_g[D_g].$$

Additional solutions II

Suppose P is $\mathbb{Q}$-rational. Then there are $a_1, \ldots, a_g \in \mathbb{Z}$ such that

$$\iota(P) = a_1[D_1] + \ldots + a_g[D_g].$$

Hence

$$f_i(\iota(P)) = \int_O^P \omega_i = a_1 \int_{D_1} \omega_i + \ldots + a_g \int_{D_g} \omega_i \text{ for all } i \in \{0, \ldots, g-1\}.$$

Additional solutions II

Suppose P is $\mathbb{Q}$-rational. Then there are $a_1, \ldots, a_g \in \mathbb{Z}$ such that

$$\iota(P) = a_1[D_1] + \ldots + a_g[D_g].$$

Hence

$$f_i(\iota(P)) = \int_O^P \omega_i = a_1 \int_{D_1} \omega_i + \ldots + a_g \int_{D_g} \omega_i \text{ for all } i \in \{0, \ldots, g-1\}.$$

Working modulo p^N, we can compute $a_1 \bmod p^N, \ldots, a_n \bmod p^N$ as

$$\begin{pmatrix} a_1 \bmod p^N \\ \vdots \\ a_g \bmod p^N \end{pmatrix} = \begin{pmatrix} \int_{D_1} \omega_0 & \cdots & \int_{D_g} \omega_0 \\ \vdots & \ddots & \vdots \\ \int_{D_1} \omega_{g-1} & \cdots & \int_{D_g} \omega_{g-1} \end{pmatrix}^{-1} \cdot \begin{pmatrix} \int_O^P \omega_0 \\ \vdots \\ \int_O^P \omega_{g-1} \end{pmatrix}.$$

The Mordell-Weil sieve

Hence it suffices to show that the residue class $c \in J(\mathbb{Q})/p^N J(\mathbb{Q})$ corresponding to $(a_1 \bmod p^N, \ldots, a_g \bmod p^N)$ does not contain the image of a rational point on C.

Hence it suffices to show that the residue class $c \in J(\mathbb{Q})/p^N J(\mathbb{Q})$ corresponding to $(a_1 \bmod p^N, \ldots, a_g \bmod p^N)$ does not contain the image of a rational point on C.

This is a job for the Mordell-Weil sieve (Sharashkin, Flynn, Bruin-Stoll):

- v: prime of good reduction
- The following diagram commutes:

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\alpha_v"] \\ \tilde{C}(\mathbb{F}_v) \arrow[r, "\iota_v"'] & \tilde{J}(\mathbb{F}_v) \end{tikzcd}$$

The Mordell-Weil sieve

Hence it suffices to show that the residue class $c \in J(\mathbb{Q})/p^N J(\mathbb{Q})$ corresponding to $(a_1 \bmod p^N, \ldots, a_g \bmod p^N)$ does not contain the image of a rational point on C.

This is a job for the Mordell-Weil sieve (Sharashkin, Flynn, Bruin-Stoll):

- v: prime of good reduction
- The following diagram commutes:

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q})/p^N J(\mathbb{Q}) \arrow[d, "\alpha_v"] \\ \tilde{C}(\mathbb{F}_v) \arrow[r, "\beta_v"'] & \tilde{J}(\mathbb{F}_v)/p^N \tilde{J}(\mathbb{F}_v) \end{tikzcd}$$

- If $\alpha_v(c) \notin \beta_v(\tilde{C}(\mathbb{F}_v))$, then we're done.

The Mordell-Weil sieve

Hence it suffices to show that the residue class $c \in J(\mathbb{Q})/p^N J(\mathbb{Q})$ corresponding to $(a_1 \bmod p^N, \ldots, a_g \bmod p^N)$ does not contain the image of a rational point on C.

This is a job for the Mordell-Weil sieve (Sharashkin, Flynn, Bruin-Stoll):

- S: finite set of primes of good reduction
- The following diagram commutes:

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q})/p^N J(\mathbb{Q}) \arrow[d, "\alpha_S"] \\
\prod_{v\in S} \tilde{C}(\mathbb{F}_v) \arrow[r, "\beta_S"'] & \prod_{v\in S} J(\mathbb{F}_v)/p^N J(\mathbb{F}_v)
\end{tikzcd}$$

- If $\alpha_S(c) \notin \beta_S\left(\prod_{v\in S} \tilde{C}(\mathbb{F}_v)\right)$, then we're done.

Example 1, continued

Now use the Mordell-Weil sieve to show that the list

$$(2, \pm 3), (1, \pm 1), (0, \pm 1) \in C(\mathbb{Q})$$

of integral points on $C : y^2 = x^3(x-1)^2 + 1$ is complete.

First attempt:

- Use $p = 11,\ N = 6$.
- After taking out residue classes containing integral points, we are left with 12 residue classes in $J(\mathbb{Q})/11^6 J(\mathbb{Q})$.
- Applying the Mordell-Weil sieve using $S = \{7, 17, 5903\}$, can eliminate 10 of these.
- No prime $5903 \leq v \leq 10^7$ seems to help with the remaining classes.

Example 1, continued

Second attempt: Apply quadratic Chabauty to C with

- $p_1 = 5, N_1 = 4$,
- $p_2 = 11, N_2 = 6$.

Example 1, continued

Second attempt: Apply quadratic Chabauty to C with

- $p_1 = 5, N_1 = 4$,
- $p_2 = 11, N_2 = 6$.

After taking out residue classes containing integral points, we are left with 209 residue classes in $J(\mathbb{Q})/MJ(\mathbb{Q})$, where $M = 5^4 \cdot 11^6$.

- We use the set of primes $S = \{17, 863, 7193\}$.
- This Mordell-Weil sieve computation shows that none of the 209 residue classes contains the image of a rational point on the curve.
- So we've found all integral points on C.

Example 2

Let C be the genus 4 hyperelliptic curve

$$y^2 = x^4(x-2)^2(x-1)(x+1)(x+2)+4.$$

Since $r = 4 = g > 3$, the previously available methods are not applicable.

We use

- quadratic Chabauty for $p = 5, 7, 11$,
- the Mordell-Weil sieve for $v = 7, 13, 29, 53, 73, 103, 109, 181, 317$.

This shows that

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

are the only integral points on C.

What else/next?

- Extension to number fields: work in progress
  - works quite well for $g = 1$, real quadratic fields
  - imaginary quadratic fields especially interesting
- Other types of curves: superelliptic, smooth plane quartics.
- $r > g$?