Introduction to Explicit Chabauty Methods

William McCallum

Department of Mathematics
University Arizona

BIRS workshop on explicit methods for rational points on curves

Given a curve X of genus g over $\mathbb{Q}$, find $X(\mathbb{Q})$

- E.g., $y^2 = x(x-1)(x-2)(x-5)(x-6)$
- There are two parts to the problem
  - generating points
  - knowing when to stop.
- Knowing when to stop includes knowing when not to bother starting, i.e., deciding if $X(\mathbb{Q})$ is non-empty.
- From now on we assume we are given a point $O \in X(\mathbb{Q})$.
- If $g = 0$, we can find an explicit algebraic parameterization of $X(\mathbb{Q})$ by $\mathbb{Q}$.
- If $g = 1$ we have pretty good methods for finding explicit generators for $X(\mathbb{Q}) \simeq \mathbb{Z}^r \times$ (finite group).
- If $g \geq 2$, there are only finitely many points (Faltings). Generating points is easy in practice but knowing when to stop is hard.

Strange idea: identify $X(\mathbb{Q})$ as a subset of $J(\mathbb{Q})$

- J, the jacobian of X, is a proper g-dimensional group variety: why should it be easier to work with?
- Good cohomological machinery for bounding $J(\mathbb{Q}) \simeq \mathbb{Z}^r \times$ (finite group) without knowing equations for J.
- Use the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant isomorphism

$$J(\overline{\mathbb{Q}}) \simeq \frac{\{\text{Divisors on } \overline{X}\}}{\{\text{Divisors of functions}\}}$$

- $$\iota : X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q}), \quad P \mapsto [P - O],$$
- Given $[D] \in J(\mathbb{Q})$, look for non-zero functions f with $(f) \geq -D - O$, then $P = D + O + (f)$ is rational.
- What if $J(\mathbb{Q})$ is not finite?

If $J(\mathbb{Q})$ is infinite, we seek analytic functions that vanish on the rational points

$$\begin{tikzcd} X(\mathbb{Q}_p) \arrow[r, hook] & J(\mathbb{Q}_p) \\ & \overline{J(\mathbb{Q})} \arrow[u, hook] \end{tikzcd}$$

- Chabauty: if $\dim \overline{J(\mathbb{Q})} < g$, then $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ should be finite.
- Two approaches to finding the elements of this set explicitly:
  - look for analytic functions on $J(\mathbb{Q}_p)$ that vanish on $\overline{J(\mathbb{Q})}$ and find their zeroes $X(\mathbb{Q}_p)$ (Coleman)
  - look for analytic functions on $J(\mathbb{Q}_p)$ that vanish on $X(\mathbb{Q}_p)$ and find their zeroes on $\overline{J(\mathbb{Q})}$ (Flynn).

Digression: why not use real points?

$$\begin{tikzcd} X(\mathbb{R}) \arrow[r, hook] & J(\mathbb{R}) \\ & \overline{J(\mathbb{Q})} \arrow[u, hook] \end{tikzcd}$$

- Mazur conjectures that $\overline{J(\mathbb{Q})}$ is open in the Zariski closure of $J(\mathbb{Q})$.
- Thus, if $\dim \overline{J(\mathbb{Q})} < g$, then there is a non-trivial quotient A of J such that $A(\mathbb{Q})$ is finite.
- Could work with $X \to A$.

Find analytic functions using p-adic integration on $J(\mathbb{Q}_p)$

- For $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$, we have

$$\eta_J \colon J(\mathbb{Q}_p) \to \mathbb{Q}_p, \quad Q \mapsto \int_0^Q \omega_J$$

  characterized uniquely by the following two properties:
  1. It is a homomorphism.
  2. It is calculated by formal integration on some open $U \subset J(\mathbb{Q}_p)$.
- Translation invariance of ω gives homomorphism property:

$$\eta_J(P+Q) = \eta_J(P) + C.$$

- Putting all these together we get the logarithm

$$\log : J(\mathbb{Q}_p) \to T,$$

  where $T = \mathrm{Hom}(H^0(J_{\mathbb{Q}_p}, \Omega^1), \mathbb{Q}_p)$, the tangent space.
- There is a one-to-one correspondence between linear functionals λ on T and differentials ω_J such that $\lambda \circ \log = \eta_J$.

Structure of the closure of the rational points

Lemma

Define $r' := \dim \overline{J(\mathbb{Q})}$ *and* $r := \operatorname{rank} J(\mathbb{Q})$. *Then* $r' \leq r$.

Proof:

$$r' = \dim \overline{J(\mathbb{Q})} = \dim \log \left(\overline{J(\mathbb{Q})}\right), \quad \text{and} \quad \log \left(\overline{J(\mathbb{Q})}\right) = \overline{\log J(\mathbb{Q})}$$

$$r' = \operatorname{rank}_{\mathbb{Z}_p} (\mathbb{Z}_p \log J(\mathbb{Q})) \leq \operatorname{rank}_{\mathbb{Z}} \log J(\mathbb{Q}) \leq \operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) = r.$$

Theorem (Chabauty)

Suppose $g \geq 2$ *and that there is a prime* p *such that* $r' < g$. *Then* $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ *is finite (and hence so is* $X(\mathbb{Q})$*).*

- The hypothesis yields η_J on $J(\mathbb{Q}_p)$ that vanishes on $\overline{J(\mathbb{Q})}$.
- Restricting this to $X(\mathbb{Q}_p)$ gives us a locally-analytic function that vanishes on $X(\mathbb{Q})$.
- Why only finitely many zeros? How to count them?

p-adic integration on the curve X

- Suppose $X_{\mathbb{Q}_p}$ has good reduction, with model X over $\mathbb{Z}_p$.
- Then $J_{\mathbb{Q}_p}$ has a Néron model J, and $J_{\mathbb{F}_p}$ is the jacobian of $X_{\mathbb{F}_p}$.
- Restriction from $J_{\mathbb{Q}_p}$ to $X_{\mathbb{Q}_p}$ induces an isomorphism

$$H^0(J_{\mathbb{Q}_p}, \Omega^1) \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1).$$

- If ω is the restriction of ω_J to $X_{\mathbb{Q}_p}$, define

$$\int_Q^{Q'} \omega := \int_0^{[Q'-Q]} \omega_J.$$

- If $\sum(Q_i' - Q_i)$ is the divisor of a function, then $\sum \int_{Q_i}^{Q_i'} \omega = 0$.
- If Q and Q' are in the same residue class, then

$$\int_Q^{Q'} \omega = F(Q') - F(Q)$$

for a power series F in a local parameter t on X with $dF = \omega$.

Integration on residue classes

- A residue class is the preimage of a point under the reduction map $X(\mathbb{Q}_p) \twoheadrightarrow X(\mathbb{F}_p)$.
- A parameter t is a regular function on an open neighborhood of $\tilde{Q}$ in $X_{\mathbb{F}_p}$, whose restriction to the special fiber is a uniformizer at $\tilde{Q}$.
- The function t maps the residue class bijectively to $p\mathbb{Z}_p$.
- If ω is scaled so that it reduces to a nonzero $\tilde{\omega} \in H^0(X_{\mathbb{F}_p}, \Omega^1)$, then $\omega = w(t)\,dt$ on the residue class for some power series $w(t) \in \mathbb{Z}_p[[t]]$ such that $w(t) \not\equiv 0 \pmod{p}$.
- The function η on the residue class is represented by a series $I(t) \in \mathbb{Q}_p[[t]]$ (possibly no longer in $\mathbb{Z}_p[[t]]$) whose derivative is $w(t)$.

Counting zeros of power series on $p\mathbb{Z}_p$

Lemma (Baby Newton)

Suppose $f(t) \in \mathbb{Q}_p[[t]]$ is such that $f'(t) \in \mathbb{Z}_p[[t]]$. Let

$$m = \operatorname{ord}_{t=0}(f'(t) \bmod p)$$

If $m < p - 2$, then f has at most $m + 1$ zeros in $p\mathbb{Z}_p$.

Proof.

Write $f(t) = \sum a_i t^i$. We have

$$v_p(a_{m+1}) = 0, \quad v_p(a_i) \geq -v_p(i), \quad i > m + 1.$$

So the Newton polygon of f has slopes greater than -1 to the right of $(m + 1, 0)$. □

- Coleman gives an estimate for an arbitrary p-adic field.
- If the coefficient of t^{p-1} in $f'(t)$ is in $p\mathbb{Z}_p$, then one need assume only $m < 2p - 2$ to obtain the same conclusion.

In summary: an integral vanishing on rational points

If $r' < g$, we have ω such that

(i) If $Q_i, Q_i' \in X(\mathbb{Q}_p)$ are such that $\sum(Q_i' - Q_i)$ is the divisor of a rational function, or more generally $[\sum(Q_i' - Q_i)]$ is a torsion element of $J(\mathbb{Q}_p)$, then $\sum \int_{Q_i}^{Q_i'} \omega = 0$.

(ii) If $Q, Q' \in X(\mathbb{Q}_p)$ have the same reduction in $X(\mathbb{F}_p)$, then $\int_Q^{Q'} \omega$ can be calculated by expanding in power series in a local parameter t on the curve X.

(iii) If $Q_i, Q_i' \in X(\mathbb{Q}_p)$ are such that $[\sum(Q_i' - Q_i)] \in \overline{J(\mathbb{Q})}$, then $\sum \int_{Q_i}^{Q_i'} \omega = 0$.

Theorem (Coleman)

Let X, J, p, r' be as in Chabauty's theorem, suppose p is a prime of good reduction.

1. *Let ω satisfy (i)-(iii), and scale so $\tilde{\omega} \neq 0$. Suppose $\tilde{Q} \in X(\mathbb{F}_p)$. Let $m = \operatorname{ord}_{\tilde{Q}} \tilde{\omega}$. If $m < p - 2$, then the number of points in $X(\mathbb{Q})$ reducing to $\tilde{Q}$ is at most $m + 1$.*
2. *If $p > 2g$, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2)$.*

Proof.

1. Fix $Q \in X(\mathbb{Q})$ reducing to $\tilde{Q}$. Then $\int_Q^{Q'} \omega = 0$ for any $Q' \in X(\mathbb{Q})$ reducing to $\tilde{Q}$. As a function of Q', $\int_Q^{Q'} \omega$ can be expressed as a power series $I(t)$. The Lemma applied to $I(t)$ shows that $I(t)$ has at most $m + 1$ zeros, so there are at most $m + 1$ rational points Q' in the residue class.
2. By the Riemann-Roch theorem, the total number of zeros of $\tilde{\omega}$ in $X(\overline{\mathbb{F}}_p)$ is $2g - 2$. In particular, $m \leq 2g - 2 < p - 2$. Sum (1) over all $\tilde{Q} \in X(\mathbb{F}_p)$.

$\square$

Computational effectiveness

- Can have $r \geq g$, which makes $r' \leq g$ unlikely.
- Could be computationally difficult to bound r, and hence r'.
- The zero set of the integral of ω may be strictly larger than $\overline{J(\mathbb{Q})}$, even if one uses enough independent integrals.
- If the p-adic submanifolds $X(\mathbb{Q}_p)$ and $\overline{J(\mathbb{Q})}$ in $J(\mathbb{Q}_p)$ are tangent, it may be impossible to prove that they intersect.
- Even if $\#\left(X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}\right)$ is computed exactly, the true value of $\#X(\mathbb{Q})$ could be smaller; in other words, some of the intersection points could be irrational points in $X(\mathbb{Q}_p)$.

Example: $y^2 = x(x-1)(x-2)(x-5)(x-6)$

- This curve has good reduction at $p = 7$, and

  $$X(\mathbb{F}_7) = \{\infty, (0,0), (1,0), (2,0), (5,0), (6,0), (3,6), (3,-6)\}.$$

- A descent calculation by Gordon and Grant shows that $J(\mathbb{Q})$ has rank 1. Coleman's theorem says $\#X(\mathbb{Q}) \leq 10$.
-

  $$X(\mathbb{Q}) = \{\infty, (0,0), (1,0), (2,0), (5,0), (6,0), (3,\pm 6), (10,\pm 120)\}.$$

Example: $y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$

Theorem (Flynn-Poonen-Schaefer)

$$X(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 1), (-3, \pm 1)\}.$$

Out of the box, Coleman's Theorem needs $p = 5$, which gives $\#X(\mathbb{Q}) \leq 9$. However X has good reduction at 3, and

$$X(\mathbb{F}_3) = \{\infty^+, \infty^-, (0, \pm 1)\}.$$

$$\tilde{\omega} = a\frac{dx}{y} + b\frac{x\,dx}{y}.$$

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

$$\tilde{\omega} = \frac{x\,dx}{y} = (x - x^3 + \cdots)dx$$

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_3) + (2g - 2) = 4 + (2 \cdot 2 - 2) = 6.$$

Calculating integrals explicitly

$$\begin{aligned}
\int_{(0,1)}^{(-3,1)} \frac{dx}{y} &= \int_0^{-3} (1 + 6x + 5x^2 + 22x^3 + 22x^4 + 8x^5 + x^6)^{-1/2}\, dx \\
&= \int_0^{-3} (1 - 3x + 11x^2 - 56x^3 + \cdots)\, dx \\
&= \left(x - 3\frac{x^2}{2} + 11\frac{x^3}{3} - 56\frac{x^4}{4} + \cdots \right) \Big|_0^{-3} \\
&= (-3) - \frac{3}{2}(-3)^2 + \frac{11}{3}(-3)^3 - \frac{56}{4}(-3)^4 + \cdots \\
&\equiv 2 \cdot 3 + 3^4 \pmod{3^5}
\end{aligned}$$

and similarly

$$\begin{aligned}
\int_{(0,1)}^{(-3,1)} \frac{x\, dx}{y} &= \left(\frac{x^2}{2} - 3\frac{x^3}{3} + 11\frac{x^4}{4} - 56\frac{x^5}{5} + \cdots \right) \Big|_0^{-3} \\
&\equiv 2 \cdot 3^2 + 2 \cdot 3^3 \pmod{3^3}.
\end{aligned}$$

(Continued)

$$\omega = \epsilon \frac{dx}{y} + \frac{x\,dx}{y}, \quad \int_{(0,1)}^{(-3,1)} \omega = 0$$

$$(2 \cdot 3 + 3^4 + \cdots)\epsilon + (2 \cdot 3^2 + 2 \cdot 3^3 + \cdots) = 0,$$

$$\epsilon \equiv 2 \cdot 3 + 3^2 + 2 \cdot 3^3 \pmod{3^4}.$$

$$\begin{aligned}
I(t) &:= \int_{(0,1)}^{Q_t} \omega, \quad Q_t := (t, (1 + 6t + 5t^2 + 22t^3 + 22t^4 + 8t^5 + t^6)^{1/2}) \\
&= \int_{(0,1)}^{Q_t} \left(\epsilon \frac{dx}{y} + \frac{x\,dx}{y} \right) \\
&= \int_0^t (\epsilon + x)(1 + 6x + 5x^2 + 22x^3 + 22x^4 + 8x^5 + x^6)^{-1/2}\,dx \\
&= \epsilon t + (-3\epsilon + 1)\frac{t^2}{2} + (11\epsilon - 3)\frac{t^3}{3} + \cdots .
\end{aligned}$$

Computing integrals between residue classes

1. Restrict from $J(\mathbb{Q}_p)$:
   - Inside each residue class of J there is torsion point T, which can be used to set the constant of integration since $\int_0^T \omega_J = 0$.
   - Can be chosen to be rational over $\mathbb{Q}_p$ if it has order prime to p.
2. Set the constant directly on $X(\mathbb{Q}_p)$ using Coleman's theory of p-adic integration and the idea of a Teichmüller point.
3. Ultimately we care only about the residue classes in $J(\mathbb{Q}_p)$ containing a point of $J(\mathbb{Q})$. For each of these residue classes, we compute an explicit divisor representing a point in $J(\mathbb{Q})$ in the residue class, and use it to set the constant of integration. This idea is due to Wetherell.

Elliptic Chabauty

- Can replace $X \hookrightarrow J$ by any morphism to an abelian variety $X \to A$.
- Factors through $J \to A$; Chabauty's argument applies if $\operatorname{rank} A(\mathbb{Q}) < \dim A$.
- Special case: $X_k \twoheadrightarrow E$ for an elliptic curve E over some finite extension k of $\mathbb{Q}$
- We get a map from X to $A := \operatorname{Res}_{k/\mathbb{Q}} E$, an abelian variety of dimension $[k : \mathbb{Q}]$ such that $A(\mathbb{Q}) \simeq E(k)$.
- Typically the induced map $J \to A$ will be surjective; in this case one needs $\operatorname{rank} E(k) < [k : \mathbb{Q}]$ to apply Chabauty's argument.

Example: $y^2 = x^6 + x^2 + 1$ (Diophantus)

- J is isogenous over $\mathbb{Q}$ to a product of elliptic curves, each of rank 1, so $r' = r = 2$.
- Wetherell used descent to replace the problem with the problem for finite étale covers of higher genus to which the method could be applied.
- He succeeded in proving that

$$X(\mathbb{Q}) = \{(\pm 1/2, \pm 9/8), (0, \pm 1), \infty^+, \infty^-\}.$$

Stoll's improvement

Coleman's theorem requires $r' < g$, but if $r' < g - 1$, then one can improve the bound. For instance, if $p > 2g$, one can prove

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

Bad reduction

Theorem

Let X, p, r' be as in Chabauty's theorem, let $\mathcal{X}$ over $\mathbb{Z}_p$ be a minimal regular model for $X_{\mathbb{Q}_p}$, and let $\mathcal{X}_s$ over $\mathbb{F}_p$ be its special fiber.

1. *Let ω be a nonzero 1-form in $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ satisfying conditions (i)–(iii). Let C be a component of multiplicity 1 in $\mathcal{X}_s$, and define $C^{\text{smooth}} := C \cap \mathcal{X}^{\text{smooth}}$. Scale ω by a power of p so that it reduces to a nonzero 1-form $\tilde{\omega} \in H^0(C^{\text{smooth}}, \Omega^1)$. Let $\tilde{Q} \in C^{\text{smooth}}(\mathbb{F}_p)$. Let $m = \operatorname{ord}_{\tilde{Q}} \tilde{\omega}$. If $m < p - 2$, then the number of points in $X(\mathbb{Q})$ reducing to $\tilde{Q}$ is at most $m + 1$.*
2. *If $p > 2g$, then*

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