Computing rational points on databases of genus 3 curves

Sachi Hashimoto
joint with María de Frutos Fernández and Travis Morrison

Boston University

Wesleyan Algebra/Number Theory Seminar
September 27, 2019
A *curve* $X$ is the solution to a polynomial in two variables $f(x, y) = 0$ with coefficients in $\mathbb{Q}$. Solutions $(x, y)$ with rational coordinates are *rational points* on the curve, $X(\mathbb{Q})$ is the set of all such points. Curves are classified by their genus:

Faltings’s theorem (1983) states that a curve $X$ of genus $g \geq 2$ has finitely many rational points, but it does not give an explicit recipe to compute $X(\mathbb{Q})$. 

Databases of rational points  

Sachi Hashimoto  

2
Motivating question

Problem (Motivating question)

Given a curve $X/\mathbb{Q}$ of genus $g \geq 2$, can we compute $X(\mathbb{Q})$?

Diophantus (3rd century AD) published over 100 equations and numerical solutions. A genus 2 equation in Diophantus’s books was not solved until 1998 by Wetherell.

The Cursed Curve, J. Balakrishnan, K. Carde, SH
We will focus on the Chabauty-Coleman method. Proves finiteness of $X(\mathbb{Q})$ for curves with Mordell-Weil rank $r$ strictly less than their genus $g$.

A curve $X$ embeds into its Jacobian $J$, an abelian variety. The Mordell-Weil theorem proves $J(\mathbb{Q})$ is a finitely generated abelian group, thus $J(\mathbb{Q}) \cong \mathbb{Z}^r \oplus J(\mathbb{Q})_{\text{tors}}$. We call $r$ the rank of the curve.
Example

Question (Hirakawa-Matsumura, 2018)

Does there exist a rational right triangle and a rational isosceles triangle that have the same area and same perimeter?

Reduces to solving for all rational points on the genus 2 rank 1 curve $X : y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16$.

- Coleman proved a bound, $\#X(\mathbb{Q}) \leq 10$.
- Can exhibit points
  \{$\pm \infty, (0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3)$\} and then rule out degenerate cases.

Unique pair of triangles $(377, 135, 352)$ and $(366, 366, 132)$ from the point $(12/11, 868/11^3)$. 
Big idea

• If $X(\mathbb{Q})$ is contained in a finite computable set $X(\mathbb{Q}_p)_1$ then we can compute $X(\mathbb{Q})$ plus an extra bit, and hope the extra bit is not too big.

• If we can bound the size of $X(\mathbb{Q})$ then with some luck the bound is equal to the number of known points.
We are interested in the embedding of our curve $X$ inside of its Jacobian $J$.

On $J(\mathbb{Q}_p)$ we will define functionals $f_i$ which are zero on $X(\mathbb{Q})$ but not identically zero, and have finitely many zeros.
In Search of a Functional

Fix $\infty \in X(\mathbb{Q})$. Suppose we had a $p$-adic integral $\int$, and could find $\omega$ a regular 1-form such that $\int_P^\infty \omega = 0$ for all $P \in X(\mathbb{Q})$.

Then we would have a functional $f : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ by sending $Q \mapsto \int_Q^\infty \omega$ and $X(\mathbb{Q})$ would be contained in the vanishing of $f$.

Letting $V$ be the vector space of all such “vanishing differentials” $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$. Then picking a basis for $V$, $X(\mathbb{Q}_p)_1$ will be the common vanishing locus of all the set of functionals defined by integrating against that basis.
Genus 2, rank 1 Chabauty-Coleman

Suppose $X$ is genus 2 and rank $J(\mathbb{Q}) = 1$, $\infty \in X(\mathbb{Q})$. Fix $p$ prime of good reduction.

- Fix a basis for the differentials on $X_{\mathbb{Q}_p}$, $dx/y, xdx/y$.
- Suppose we can find $P \in X(\mathbb{Q})$, $[P - \infty]$ of infinite order in $J(\mathbb{Q})$. Compute $p$-adic numbers

$$\int_{\infty}^{P} dx/y = A, \int_{\infty}^{P} xdx/y = B,$$

and solve

$$X(\mathbb{Q}_p)_1 = \left\{ z \in X(\mathbb{Q}_p) : \int_{\infty}^{z} (Bdx/y - Axdx/y) = 0 \right\}.$$

For any $Q \in X(\mathbb{Q})$, $[Q - \infty]$ is torsion or $n[P - \infty]$ and

$$n \int_{\infty}^{P} (Bdx/y - Axdx/y) = n(BA - AB) = 0.$$
Coleman integration

\(X/\mathbb{Q}_p\) a curve, \(P, Q, R \in X(\mathbb{Q}_p)\), \(\omega, \eta\) regular 1-forms, \(\alpha, \beta \in \mathbb{Q}_p\).

Coleman defined an integral \(\int_P^Q \omega\) satisfying the properties

1. **Linearity:** \(\int_P^Q (\alpha \omega + \beta \eta) = \alpha \int_P^Q \omega + \beta \int_P^Q \eta\).
2. **Additivity:** \(\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega\).
3. **Change of variables:** if \(X'\) is a curve and \(\phi : X \to X'\) a rigid analytic map between wide opens then \(\int_P^Q \phi^* \omega = \int_{\phi(P)}^{\phi(Q)} \omega\).
4. **Fundamental theorem of calculus:** \(\int_P^Q df = f(Q) - f(P)\).
5. **For** \(D \in J_{\mathbb{Q}_p}\) **a divisor of degree zero,** \(D = \sum_i [P_i - Q_i]\) **then** \(\int_D \omega := \sum_i \int_{P_i}^{Q_i} \omega\) **is well-defined,** and \(\int_D \omega = 0\) when \(D\) principal.
Coleman Integration

\[ X(\mathbb{Q}_p) = \bigsqcup \text{red}^{-1} X(\mathbb{F}_p) \]

\[ X(\mathbb{Q}_p) \] decomposes into residue discs (preimages of \( X(\mathbb{F}_p) \) under reduction):

\( P \in X(\mathbb{Q}_p), \ P = (a_0 + a_1p + O(p^2), b_0 + b_1p + O(p^2)). \) So \( \overline{P} = (a_0, b_0). \) If \( P' \in X(\mathbb{Q}_p) \) has \( \overline{P'} = (a_0, b_0) \) then they are in the same residue disc, \( p \)-adically close.

Within a disc, an integral \( \int_P^{P'} \omega = \int_{t(P')}^{t(P)} \omega(t)dt \) has a power series expansion in a uniformizer \( t \in \mathbb{Q}_p(X) \) (The uniformizer \( t \) gives an isomorphism of disc to \( p\mathbb{Z}_p \).)

Databases of rational points

Sachi Hashimoto
Coleman integration

- Power series has finite number of zeros (bound with the Newton polygon).
- Global bound: if \( p > 2g \), then \( \#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2) \).
- Integrating between discs happens by “analytic continuation along the Frobenius”.
- Can be made explicit: (Balakrishnan-Bradshaw-Kedlaya 2010), (Balakrishnan 2013) hyperelliptic, (Balakrishnan-Tuitman 2017) general curves.
Computing on genus 3 curves

Drew Sutherland has databases of genus 3 curves of bounded discriminant. Now $H^0(X_{\mathbb{Q}_p}, \Omega^1) = \langle \omega_0, \omega_1, \omega_2 \rangle$. We consider two cases:

1. Genus 3 rank 0 hyperelliptic curves. In this case all points are torsion, and the vanishing functionals $f_i$ are just $\int_{\infty}^{z} \omega_i$.

2. Genus 3 rank 1 Picard curves, $y^3 = f(x)$, $\deg(f) = 4$. Have two regular 1-forms $v_1, v_2$ such that $\int_{Q}^{Q} v_i = 0$ for all $Q \in X(\mathbb{Q})$. Let $f_i(z) := \int_{\infty}^{z} v_i$.

We compute Chabauty-Coleman set $X(\mathbb{Q}_p)_1 := \{ z \in X(\mathbb{Q}_p) | f_i(z) = 0 \}$.

We computed $X(\mathbb{Q})$ for 5870 rank 0 genus 3 curves, 1403 rank 1 Picard curves, but the code can be applied generally.

The case of genus 3, rank 1 hyperelliptic was explored by Balakrishnan–Bianchi–Cantoral–Farfán–Çiperiani–Etropolski.
Algorithm $r = 1$, $g = 3$, $\mathbb{Q}$-generator

On each curve in the database:

1. Compute the rank of $J(\mathbb{Q})$, decide whether to proceed.
2. Find $P \in X(\mathbb{Q})$ such that $[P - \infty]$ infinite order.
3. Compute the regular 1-forms $v_1, v_2$ such that $\int_{\infty}^{P} v_i = 0$.
4. Solve for $X(\mathbb{Q}_p)_1$ the $p$-adic points by computing $f_i(z) = \int_{\infty}^{z} v_i = 0$.
5. Compute a list of $X(\mathbb{Q})$ and compare to $X(\mathbb{Q}_p)_1$. Explain any extra points.

Problem (Motivating Question)

What does the Chabauty-Coleman method give us beyond rational points? i.e. What is $X(\mathbb{Q}_p)_1 - X(\mathbb{Q})$?
Genus 3, rank 0, hyperelliptic

\[ X : y^2 = x^7 - 37024x^6 + 3134464x^5 - 101220352x^4 + 1613758464x^3 - 13656653824x^2 + 59055800320x - 103079215104 \]

We write \( f_i(z) = \int_{\infty}^{z} \omega_i \) in local coordinates and find their zeros above each point of \( X(\mathbb{F}_7) \).

<table>
<thead>
<tr>
<th>disc</th>
<th>common roots of ( f_1(z) ), ( f_2(z) ) and ( f_3(z) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \infty )</td>
<td>( \infty )</td>
</tr>
<tr>
<td>( (0, \pm 4) )</td>
<td>no common roots</td>
</tr>
<tr>
<td>( (1, \pm 5) )</td>
<td>no common roots</td>
</tr>
<tr>
<td>( (2, \pm 6) )</td>
<td>no common roots</td>
</tr>
<tr>
<td>( (4, 0) )</td>
<td>( (32, 0) )</td>
</tr>
<tr>
<td>( (6, \pm 2) )</td>
<td>no common roots</td>
</tr>
</tbody>
</table>

Thus we prove \( X(\mathbb{Q}) = \{(32, 0), \infty\} \).
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 - 3x^2 + x + 1 \]

Applying the algorithm at \( p = 11 \), we find

\[ X(\mathbb{Q}_{11})_1 = X(\mathbb{Q}) = \{ (0, 1), (1, 0), \infty \}. \]

But if \( p = 5 \), \( X(\mathbb{Q}_5)_1 \) has an extra point: \( x = 2, y^3 = 7 \). It turns out

\[ 3(2, 7^{1/3}) - 3\infty \simeq 2(1, 0) - 2\infty \]

as divisors. Since \( (1, 0) - \infty \) is 3-torsion, the extra solution is a 9-torsion point.
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + x^3 - 3x^2 - 2x \]

We compute rational points \( \{(0, 0), (2, 2), (-2, 0), (-1, -1), \infty\} \).

<table>
<thead>
<tr>
<th>prime</th>
<th>( x )-coord</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>(-105237648 + O(7^{10}))</td>
</tr>
<tr>
<td>11</td>
<td>(-800588 + O(11^6))</td>
</tr>
<tr>
<td>13</td>
<td>(864 + O(13^3))</td>
</tr>
<tr>
<td>17</td>
<td>no extra point</td>
</tr>
</tbody>
</table>

The \( x \)-coordinates come from a global point of \( X, (\alpha, \alpha^2 + 2\alpha) \), where \( \alpha \) is a root of \( x^3 + 3x^2 + 1 \).

The field \( \mathbb{Q}(\alpha) \) has a prime of degree 1 above 7, 11, and 13 but not 17.

\( 3[ (\alpha, \alpha^2 + 2\alpha) - \infty ] = [(-1, -1) - \infty] \) is in \( J(\mathbb{Q}) \cap X(\mathbb{Q}) \).
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + 6x^3 - 48x - 64 \] has two extra global points over two different number fields!

In \( X(\mathbb{Q}_{17})_1 \), we find extra 17-adic points which Sage recognizes as
\[ T = (t, 1/2t^2 - 4) \] over \( \mathbb{Q}(t)/(t^3 - 24t - 48) \) and
\[ S = (s, s^2 + 6s + 8) \] over \( \mathbb{Q}(s)/(s^3 + 9s^2 + 24s + 24) \).

In the Jacobian, we have that\[ 18([T - \infty]) = 9([S - \infty]) \] so one point is twice the other (up to 9-torsion).

Also, \[ 18([T - \infty]) = 3[(-3, -1) - \infty] \], where we know \([(-3, -1) - \infty]\) is infinite order in \( J(\mathbb{Q}) \).
Genus 3, rank 2, Picard: not explained by Jacobian relations

\[ X : y^3 = x^4 - 2 \]

- \( P_1 = (1, -1), P_2 = (-1, -1) \) points so that \([P_1 - \infty], [P_2 - \infty]\) are non-torsion and linearly independent in \( J(\mathbb{Q}) \).
- \( X/\mathbb{Q}(i) \) has order 4 automorphism \( \phi : x \mapsto ix \).
- \( \phi^* v_{\text{van}} = iv_{\text{van}} \) where \( v_{\text{van}} \) is the vanishing differential defined to make \( \int_{\infty}^{P_j} v_{\text{van}} = 0 \) for \( j = 1, 2 \).
- We can find \( Q_1 = (i, -1), Q_2 = (-i, -1) \) in \( X(\mathbb{Q}(i)) \) so that \( \phi(P_1) = Q_1 \) and \( \phi(P_2) = Q_2 \).

Stitching it together we see \( Q_j \in X(\mathbb{Q}_p)_1 \), e.g.:

\[
\int_{\infty}^{Q_1} v_{\text{van}} = \int_{\phi(\infty)}^{\phi(P_1)} v_{\text{van}} = \int_{\infty}^{P_1} \phi^* v_{\text{van}} = i \int_{\infty}^{P_1} v_{\text{van}} = 0.
\]
• Any $\phi : X \to X$ acts linearly on the $\mathbb{Q}_p$-vector space $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ and subspace of vanishing differentials $V$ by $\phi^*$.

• Since $\phi^k = 1$, if eigenvalues defined over $\mathbb{Q}_p$, then $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ decomposes into eigenspaces with eigenvalues which are $k$th roots of unity.

**Question**

Does $V$ have a decomposition into $\phi^*$ eigenspaces? i.e. is $\phi^*V \subset V$?
Automorphisms

- $X/\mathbb{Q}$ be a curve with $\phi \in \text{Aut}(X_K)$ an automorphism for $K/\mathbb{Q}$ finite, $\phi^k = 1$
- $p$ be a prime of good reduction such that $\mathbb{Q}_p$ contains a primitive $k$th root of unity
- $P_1, \ldots, P_r \in X(\mathbb{Q})$ such that $[P_i - b]$ are of infinite order and linearly independent in $J(\mathbb{Q})$, and $\phi(b) = b$, $b \in X(\mathbb{Q})$

Proposition (H.-Morrison)

Suppose the eigenvalues of $\phi^*$ are $2^m$th of unity which are not all complex conjugates of each other. Then the space of vanishing differentials decomposes into $\phi^*$-eigenspaces.
Beyond rational points

What if we don’t have rational points \( P_1, \ldots, P_r \in X(\mathbb{Q}) \) so that \([P_i - \infty]\) are linearly independent and infinite order in \( J(\mathbb{Q}) \)?

Fixing a rational base point \( b \), there is a canonical map 
\[ \text{Sym}^g(X) \to J \] sending \((P_1, \ldots, P_g) \mapsto [P_1 + \cdots + P_g - gb]. \]

Generator for \( J(\mathbb{Q}) \) is a divisor defined over at most a degree \( g \) extension of \( \mathbb{Q} \).

For example \( X : y^3 - (x^4 + 7x^3 + 8x^2 - 15x + 4) \) has genus 3 and rank 1, with infinite order point 
\[ [(-2 + \sqrt{5}, 1) + (-2 - \sqrt{5}, 1) - 2\infty]. \] The \( x \)-coordinates here are roots of \( x^2 + 4x - 1 \), and \( p = 11 \) splits completely in 
\( L = \mathbb{Q}[x]/(x^2 + 4x - 1) \), so if \( p \mid p \), \( L_p \simeq \mathbb{Q}_p \).

Most of the time work locally in \( \mathbb{Q}_p \). Coming soon on GitHub: new code to integrate to number field points when \( p \) splits in the number field.
Genus 3, rank 1, Picard

\[ X : y^3 = x^4 + 7x^3 + 3x^2 - x \]

We compute \( D = \text{div}(x^3 + 6x^2 + 3x - 1) - 3\infty \) is an infinite order point in \( J(\mathbb{Q}) \).

The first split prime in the number field \( \mathbb{Q}(x)/(x^3 + 6x^2 + 3x - 1) \) is 17.

Chabauty at 17 gives three Weierstrass points and \((1, 10^{1/3})\) which is a 9-torsion point.
Data: genus 3, rank 0 hyperelliptic

With María de Frutos-Fernández, we computed rational points on 5,870 rank 0 genus 3 hyperelliptic curves, using a Sage script.

Most of the time, in 3083 curves, $X(\mathbb{Q}_p)_1 = X(\mathbb{Q})$ plus the Weierstrass points. In 16 cases we had torsion of higher order.
Data: genus 3, rank 1 Picard

With Travis Morrison, we have preliminary data of several test runs computing Chabauty-Coleman on 1403 rank 1 genus 3 curves.

- 6 curves with torsion over number fields (9-torsion and 4-torsion). Of the form \((a, b^{1/3})\) where \(a, b\) are integers.
- 4 curves with extra points that have relations with points in \(J(\mathbb{Q})\).

![Bar chart showing number of rank 1 Picard curves with \(n\) rational points.]