Chabauty and the Mordell–Weil Sieve
Episode 2

Samir Siksek

University of Warwick

3 September 2014

Recap

Recall: **given a curve C over $\mathbb{Q}$, we want a complete description of $C(\mathbb{Q})$.**
For genus ≥ 1, **there is no algorithm for giving this!** But there is a bag of tricks that can be used to show that $C(\mathbb{Q})$ is empty, or determine $C(\mathbb{Q})$ if it is non-empty. These include:

1. Local methods (Michael's lectures);
2. Quotients (Michael's lectures);
3. Descent (Michael's lectures);
4. Chabauty;
5. Mordell–Weil sieve.

The purpose of these lectures is to get a feel for each of these methods and see it applied to a particular example.

Divisors

Let C be a curve over k.

- A **divisor** D on C is a finite formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in C(\overline{k}).$$

Divisors

Let C be a curve over k.

- A **divisor** D on C is a finite formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in C(\overline{k}).$$

- $\deg(D) = \sum a_i$.

Divisors

Let C be a curve over k.

- A **divisor** D on C is a finite formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in C(\overline{k}).$$

- $\deg(D) = \sum a_i$.
- We say that D is **rational** if it is invariant under $\mathrm{Gal}(\overline{k}/k)$.

Divisors

Let C be a curve over k.

- A **divisor** D on C is a finite formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in C(\overline{k}).$$

- $\deg(D) = \sum a_i$.
- We say that D is **rational** if it is invariant under $\mathrm{Gal}(\overline{k}/k)$.
- Let

$$\mathrm{Div}^0(C/k) := \{\text{rational degree 0 divisors}\}.$$

Divisors

Let C be a curve over k.

- A **divisor** D on C is a finite formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in C(\overline{k}).$$

- $\deg(D) = \sum a_i$.
- We say that D is **rational** if it is invariant under $\mathrm{Gal}(\overline{k}/k)$.
- Let

$$\mathrm{Div}^0(C/k) := \{\text{rational degree 0 divisors}\}.$$

- Let $f \in k(C)^*$. Define

$$\mathrm{div}(f) = \sum_{P \in C(\overline{k})} \upsilon_P(f) \cdot P \qquad \textbf{(principal divisor)}$$

Divisors

Let C be a curve over k.

- A **divisor** D on C is a finite formal linear combination

$$D = \sum_{i=1}^{n} a_i P_i, \qquad a_i \in \mathbb{Z}, \quad P_i \in C(\overline{k}).$$

- $\deg(D) = \sum a_i$.
- We say that D is **rational** if it is invariant under $\mathrm{Gal}(\overline{k}/k)$.
- Let

$$\mathrm{Div}^0(C/k) := \{\text{rational degree 0 divisors}\}.$$

- Let $f \in k(C)^*$. Define

$$\mathrm{div}(f) = \sum_{P \in C(\overline{k})} \upsilon_P(f) \cdot P \qquad \textbf{(principal divisor)}$$

- $\mathrm{div}(f) \in \mathrm{Div}^0(C/k)$.

Picard Group

- Define the **subgroup of principal divisors**

$$\mathrm{Princ}(C/k) := \{\mathrm{div}(f) : f \in k(C)^*\}.$$

Picard Group

- Define the **subgroup of principal divisors**

$$\mathrm{Princ}(C/k) := \{\mathrm{div}(f) : f \in k(C)^*\}.$$

- $\mathrm{Princ}(C/k) \subset \mathrm{Div}^0(C/k)$.

Picard Group

- Define the **subgroup of principal divisors**

$$\mathrm{Princ}(C/k) := \{\mathrm{div}(f) : f \in k(C)^*\}.$$

- $\mathrm{Princ}(C/k) \subset \mathrm{Div}^0(C/k)$.
- The **Picard group** of C/k is

$$\mathrm{Pic}^0(C/k) := \frac{\mathrm{Div}^0(C/k)}{\mathrm{Princ}(C/k)}.$$

Picard Group

- Define the **subgroup of principal divisors**

$$\mathrm{Princ}(C/k) := \{\mathrm{div}(f) : f \in k(C)^*\}.$$

- $\mathrm{Princ}(C/k) \subset \mathrm{Div}^0(C/k)$.
- The **Picard group** of C/k is

$$\mathrm{Pic}^0(C/k) := \frac{\mathrm{Div}^0(C/k)}{\mathrm{Princ}(C/k)}.$$

- $\mathrm{Pic}^0(\mathbb{P}^1/k) = 0$.

Picard Group

- Define the **subgroup of principal divisors**

$$\mathrm{Princ}(C/k) := \{\mathrm{div}(f) : f \in k(C)^*\}.$$

- $\mathrm{Princ}(C/k) \subset \mathrm{Div}^0(C/k)$.
- The **Picard group** of C/k is

$$\mathrm{Pic}^0(C/k) := \frac{\mathrm{Div}^0(C/k)}{\mathrm{Princ}(C/k)}.$$

- $\mathrm{Pic}^0(\mathbb{P}^1/k) = 0$.
- For an elliptic curve E/k,

$$E(k) \cong \mathrm{Pic}^0(E/k), \qquad P \mapsto [P - \infty].$$

Jacobians

Let C/k be a curve of genus g. The **Jacobian** J_C of C is a g-dimensional abelian variety defined over k. An elliptic curve E is its own Jacobian $J_E = E$.

Theorem

(Mordell–Weil Theorem) If k is a number field then $J_C(k)$ is a finitely generated abelian group.

Proof uses descent. Can often compute $J_C(k)$ in practice, but there is no algorithm guaranteed to work.

Theorem

Let C be a curve with $C(k) \neq \emptyset$. Then

$$J_C(k) \cong \mathrm{Pic}^0(C/k).$$

We usually use elements of $\mathrm{Pic}^0(C/k)$ to represent elements of $J_C(k)$.

Abel–Jacobi map

Definition

Let C/k be a curve of genus ≥ 1. Let $P_0 \in C(k)$. Associated to P_0 is an embedding

$$\iota \ : \ C \hookrightarrow J_C, \qquad P \mapsto [P - P_0]$$

called the **Abel–Jacobi** map associated to P_0.

Abel–Jacobi map

Definition

Let C/k be a curve of genus ≥ 1. Let $P_0 \in C(k)$. Associated to P_0 is an embedding

$$\iota \ : \ C \hookrightarrow J_C, \qquad P \mapsto [P - P_0]$$

called the **Abel–Jacobi** map associated to P_0.

Lemma

If C has genus ≥ 1, $P_0 \in C(k)$. Then $\iota(C(k)) \subseteq J_C(k)$. If $J_C(k)$ is finite (and we know it) we can compute $C(k)$.

Abel–Jacobi map

Definition

Let C/k be a curve of genus ≥ 1. Let $P_0 \in C(k)$. Associated to P_0 is an embedding

$$\iota \; : \; C \hookrightarrow J_C, \qquad P \mapsto [P - P_0]$$

called the **Abel–Jacobi** map associated to P_0.

Lemma

If C has genus ≥ 1, $P_0 \in C(k)$. Then $\iota(C(k)) \subseteq J_C(k)$. If $J_C(k)$ is finite (and we know it) we can compute $C(k)$.

What is $J_C(\mathbb{Q})$ is infinite?

Chabauty's Theorem

Let $C/\mathbb{Q}$ be a curve of genus ≥ 2. Write

$$g = \text{genus}(C), \qquad r = \text{rank}(J_C(\mathbb{Q})).$$

Theorem (Chabauty 1941)

If $r \leq g - 1$ then $C(\mathbb{Q})$ is finite.

Chabauty's Theorem

Let $C/\mathbb{Q}$ be a curve of genus ≥ 2. Write

$$g = \text{genus}(C), \qquad r = \text{rank}(J_C(\mathbb{Q})).$$

Theorem (Chabauty 1941)

If $r \leq g - 1$ then $C(\mathbb{Q})$ is finite.

Theorem (Coleman 1995)

Let p be a prime of good reduction for C and suppose $p > 2g$. If $r \leq g - 1$ then

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

Chabauty's Theorem

Let $C/\mathbb{Q}$ be a curve of genus ≥ 2. Write

$$g = \text{genus}(C), \qquad r = \text{rank}(J_C(\mathbb{Q})).$$

Theorem (Chabauty 1941)

If $r \leq g - 1$ then $C(\mathbb{Q})$ is finite.

Theorem (Coleman 1995)

Let p be a prime of good reduction for C and suppose $p > 2g$. If $r \leq g - 1$ then

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

The idea behind Coleman's proof can sometimes be used to compute $C(\mathbb{Q})$ provided $r \leq g - 1$. This is known as the **method of Chabauty** or **Chabauty–Coleman**.

Differentials

Let C be a curve of a field k with $g = \text{genus}(C)$. Write Ω_C for the space of **regular differentials**. This is a k-vector space of dimension g.

Example (Regular Differentials of a Hyperelliptic Curve)

Let $f \in k[x]$ satisfy $\text{disc}(f) \neq 0$. Suppose $\text{char}(k) \neq 2$. Let

$$C \; : \; y^2 = f(x).$$

We know

$$g = \begin{cases} (d-2)/2 & d \text{ even} \\ (d-1)/2 & d \text{ odd} \end{cases} \qquad d = \deg(f).$$

Then a k-basis for Ω_C is

$$\frac{dx}{y}, \; \frac{xdx}{y}, \ldots, \; \frac{x^{g-1}dx}{y}.$$

A Pairing

Let C be a curve over $\mathbb{Q}_p$ (p is a finite prime). Then there is a pairing

$$\langle\, , \,\rangle \;:\; \Omega_C \times J_C(\mathbb{Q}_p) \to \mathbb{Q}_p,$$

which is defined by

$$\langle \omega, [\sum P_i - Q_i] \rangle = \sum \int_{Q_i}^{P_i} \omega.$$

The pairing has the following properties:

1. it is $\mathbb{Q}_p$-linear on the left;
2. it is $\mathbb{Z}$-linear on the right;
3. the kernel on the right is $J(\mathbb{Q}_p)_{\mathrm{tors}}$ (the torsion subgroup of $J(\mathbb{Q}_p)$).

Example (McCallum and Poonen, "The Method of Chabauty and Coleman")

$$C\ :\ y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

Work over $\mathbb{Q}_3$.

$$\begin{aligned}
\int_{(0,1)}^{(-3,1)} \frac{dx}{y} &= \int_{(0,1)}^{(-3,1)} (1 + 6x + 5x^2 + 22x^3 + 22x^4 + 8x^5 + x^6)^{-1/2} dx \\
&= \int_{(0,1)}^{(-3,1)} (1 - 3x + 11x^2 - 56x^3 + \cdots) dx \\
&= \int_{0}^{-3} (1 - 3x + 11x^2 - 56x^3 + \cdots) dx \\
&= \left[x - \frac{3x^2}{2} + \frac{11x^3}{3} - \frac{56x^4}{4} + \cdots \right]_{x=0}^{x=-3} \\
&= (-3) - \frac{3\cdot(-3)^2}{2} + \frac{11\cdot(-3)^3}{3} - \frac{56(-3)^4}{4} + \cdots \\
&\equiv 87 \pmod{3^5}.
\end{aligned}$$

The integral above is called **'a tiny integral'**, where the two end points are sufficiently p-adically close to ensure p-adic convergence when evaluating the p-power series.

The integral above is called **'a tiny integral'**, where the two end points are sufficiently p-adically close to ensure p-adic convergence when evaluating the p-power series.

If $D \in J_C(\mathbb{Q}_p)$ then there exists a computable $n > 0$ such that

$$nD = \sum [P_i' - Q_i']$$

where P_i' are p-adically close to the Q_i'.

The integral above is called **'a tiny integral'**, where the two end points are sufficiently p-adically close to ensure p-adic convergence when evaluating the p-power series.

If $D \in J_C(\mathbb{Q}_p)$ then there exists a computable $n > 0$ such that

$$nD = \sum [P_i' - Q_i']$$

where P_i' are p-adically close to the Q_i'.

If $\omega \in \Omega_C$ then

$$\langle \omega, D \rangle = \frac{1}{n} \langle \omega, nD \rangle = \frac{1}{n} \sum \int_{Q_i'}^{P_i'} \omega.$$

The integrals are all tiny and so can be evaluated as in the above example.

Example (McCallum and Poonen, continued)

$$C \;:\; y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

Work over $\mathbb{Q}_3$. Want to approximate $\int_{\infty_-}^{\infty_+} dx/y$. Now

$$9[\infty_+ - \infty_-] = [(-3,1) - (0,1)].$$

So

$$\int_{\infty_-}^{\infty_+} \frac{dx}{y} = \frac{1}{9}\int_{(0,1)}^{(-3,1)} \frac{dx}{y} = \frac{1}{9}(87 + O(3^5)) = \frac{29}{3} + O(3^3).$$

Likewise

$$\begin{aligned}\int_{\infty_-}^{\infty_+} \frac{xdx}{y} &= \frac{1}{9}\int_{(0,1)}^{(-3,1)} \frac{xdx}{y} \\ &= \frac{1}{9}(72 + O(3^5)) \\ &= 8 + O(3^3).\end{aligned}$$

Reminder

Let C be a curve over $\mathbb{Q}_p$ (p is a finite prime). Then there is a pairing

$$\langle\, ,\, \rangle \; : \; \Omega_C \times J_C(\mathbb{Q}_p) \to \mathbb{Q}_p,$$

The pairing has the following properties:

1. it is $\mathbb{Q}_p$-linear on the left;
2. it is $\mathbb{Z}$-linear on the right;
3. the kernel on the right is $J(\mathbb{Q}_p)_{\mathrm{tors}}$ (the torsion subgroup of $J(\mathbb{Q}_p)$.

Lemma

Let C be a curve over $\mathbb{Q}$ of genus g. Write r for the rank of $J(\mathbb{Q})$. Suppose $r \le g-1$. Let p be a prime. Then there is some non-zero $\omega \in \Omega_{C/\mathbb{Q}_p}$ such that

$$\langle \omega, D \rangle = 0 \text{ for all } D \in J(\mathbb{Q}).$$

Proof.

$\dim(\Omega_{C/\mathbb{Q}_p}) = g$. Apply linear algebra. $\square$

We call such ω an **annihilating differential**.

Example (McCallum and Poonen, continued)

$$C \; : \; y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

Work over $\mathbb{Q}_3$. Basis for $\Omega_{C/\mathbb{Q}_3}$ is dx/y, xdx/y. Using descent,

$$J(\mathbb{Q}) \cong \mathbb{Z} \cdot [D], \qquad D = \infty_+ - \infty_-.$$

Want $\omega = \epsilon dx/y + \epsilon' xdx/y$ such that $\langle \omega, [\infty_+ - \infty_-] \rangle = 0$. But

$$\left\langle \frac{dx}{y}, [D] \right\rangle = \frac{29}{3} + O(3^3), \qquad \left\langle \frac{xdx}{y}, [D] \right\rangle = 8 + O(3^3).$$

Want $\langle \omega, [D] \rangle = 0$, or equivalently

$$\epsilon \cdot \left\langle \frac{dx}{y}, [D] \right\rangle + \epsilon' \cdot \left\langle \frac{xdx}{y}, [D] \right\rangle = 0.$$

Take

$$\epsilon' = 1, \qquad \epsilon = \frac{-8 + O(3^3)}{29/3 + O(3^3)} = 69 + O(3^4).$$

We focus on finding rational points $P \in C(\mathbb{Q})$ such that $P = (t,s) \equiv (0,1) \pmod 3$. Suppose P is such a point. Now

$$[P - (0,1)] \in J(\mathbb{Q}) \implies \int_{(0,1)}^{(t,s)} \omega = 0$$

where $\omega = \epsilon dx/y + x dx/y$ is the annihilating differential. Note that this is a tiny integral:

$$\begin{aligned}\int_{(0,1)}^{(t,s)} \omega &= \int_{(0,1)}^{(t,s)} (\epsilon + x)\frac{dx}{y} \\ &= \int_0^t (\epsilon + x)(1 - 3x + 11x^2 - 56x^3 + \cdots)dx \\ &= \epsilon t + \frac{-3\epsilon + 1}{2}t^2 + \frac{11\epsilon - 3}{3}t^3 + \cdots .\end{aligned}$$

Note $t \equiv 0 \pmod 3$. So $t = 3z$ where $z \in \mathbb{Z}_3$. So

$$(-4\cdot 3^2 + O(3^5))z + (-103\cdot 3^2 + O(3^7))z^2 + (3^5 + O(3^6))z^3 + \sum_{j\geq 4} O(3^4)z^j = 0.$$

Theorem (Strassmann)

Let $f = \sum_{i\geq 0} a_i z^i$ be a powerseries with $a_i \in \mathbb{Z}_p$, such that $\lim a_i = 0$. Let $k = \min \upsilon_p(a_i)$, and let

$$N = \max\{j : \upsilon_p(a_j) = k\}.$$

Then the number of zeros of f in $\mathbb{Z}_p$ is $\leq N$.

Back to the example. For the powerseries

$$(-4\cdot 3^2 + O(3^5))z + (-103\cdot 3^2 + O(3^7))z^2 + (3^5 + O(3^6))z^3 + \sum_{j\geq 4} O(3^4)z^j = 0.$$

we have $k = 2$, and

$$N = \max\{1, 2\} = 2.$$

So the equation in z has at most two solutions. There are at most two rational points $P \in C(\mathbb{Q})$ such that $P = (t, s) \equiv (0, 1) \pmod 3$. But we know two such points: $(0, 1)$ and $(-3, 1)$. So there are no others.

$$C(\mathbb{F}_3) = \{\overline{\infty_+},\ \overline{\infty_-},\ (\bar{0},\bar{1}),\ (\bar{0},\bar{2})\}.$$

By searching for rational points on C we find

$$\infty_+,\ \infty_-,\ (0,1),\ (0,-1),\ (-3,1),\ (-3,-1).$$

Are they all? From the points of $C(\mathbb{F}_3)$, we know that every $P \in C(\mathbb{Q})$ must satisfy $P \equiv P_0 \pmod 3$ where P_0 is one of the following **rational points**:

$$\infty_+,\ \infty_-,\ (0,1),\ (0,-1).$$

Using Chabauty (i.e. the strategy above) we obtain a bound on the number of points congruent to P_0 for each one of these four points:

P_0	bound on number of rational $P \equiv P_0 \pmod 3$	known rational $P \equiv P_0 \pmod 3$
∞_+	1	∞_+
∞_-	1	∞_-
$(0,1)$	2	$(0,1)$, $(-3,1)$
$(0,-1)$	2	$(0,-1)$, $(-3,-1)$

Conclusion

$$C(\mathbb{Q}) = \{\infty_+,\ \infty_-,\ (0,1),\ (0,-1),\ (-3,1),\ (-3,-1).\}.$$

Note for Chabauty to succeed in finding $C(\mathbb{Q})$:

1. we require $r \leq g - 1$;
2. we need explicit generators for $J(\mathbb{Q})$ (or some subgroup of $J(\mathbb{Q})$ of finite index);
3. we want some prime p of good reduction so that the known rational points surject onto the residue classes mod p;
4. in each residue class we want to find enough rational points to match the Chabauty bound!

Conclusion

$$C(\mathbb{Q}) = \{\infty_+,\ \infty_-,\ (0,1),\ (0,-1),\ (-3,1),\ (-3,-1).\}.$$

I need a proper meal

Note for Chabauty to succeed in finding $C(\mathbb{Q})$:

1. we require $r \leq g - 1$;
2. we need explicit generators for $J(\mathbb{Q})$ (or some subgroup of $J(\mathbb{Q})$ of finite index);
3. we want some prime p of good reduction so that the known rational points surject onto the residue classes mod p;
4. in each residue class we want to find enough rational points to match the Chabauty bound!

Even if we have (1) and (2), we find in most examples that (3) and (4) fail. The **Mordell–Weil** sieve often allows us to fix that!

Find out how on Friday!