Chabauty and the Mordell–Weil Sieve
Episode 1

Samir Siksek

University of Warwick

1 September 2014

Warning

- Warning: some of the mathematics will be only approximately correct.

Warning

- Warning: some of the mathematics will be only approximately correct.

> *"In mathematics you don't understand things. You just get used to them."*
>
> John von Neumann

Graduate Texts in Mathematics

Joseph H. Silverman

The Arithmetic of Elliptic Curves

Basic Philosophy

A Basic Philosophy of Arithmetic Geometry: The geometry of an algebraic variety governs its arithmetic.

A Central Question of Arithmetic Geometry: How does the geometry govern the arithmetic?

Think of varieties as defined by systems of polynomial equations in affine or projective space. An **affine variety** $V \subset \mathbb{A}^n$ defined over a field k is given by a system of polynomial equations

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \qquad \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases} \qquad f_i \in k[x_1, \ldots, x_n].$$

For $L \supseteq k$, the set of L-points of V is

$$V(L) = \{(a_1, \ldots, a_n) \in L^n : f_i(a_1, \ldots, a_n) = 0 \text{ for } i = 1, \ldots, m\}.$$

A **projective variety** $V \subseteq \mathbb{P}^n$ defined over k is given by a system of polynomial equations

$$V : \begin{cases} f_1(x_0, \ldots, x_n) = 0, \\ \quad \vdots \\ f_m(x_0, \ldots, x_n) = 0, \end{cases} \qquad f_i \in k[x_0, \ldots, x_n] \text{ are homogeneous.}$$

For $L \supseteq k$, the set of L-points of V is

$$V(L) = \{(a_0, \ldots, a_n) \in L^{n+1} \setminus \{0\} : f_i(a_0, \ldots, a_n) = 0 \text{ for } i = 1, \ldots, m\} / \sim,$$

where $(a_0, \ldots, a_n) \sim (b_0, \ldots, a_n)$ if there is some $\lambda \in L^*$ such that $\lambda a_i = b_i$ for $i = 0, \ldots, n$.

A variety $V \subset \mathbb{P}^n$ is covered by $n+1$ **affine patches**:

$$V \cap \{x_i = 1\} \qquad i = 0, 1, \ldots, n.$$

Dimension

We classify varieties by **dimension**, a non-negative integer: $0, 1, 2, \ldots$.

Fact

A variety $V \subset \mathbb{A}^n$ or $\mathbb{P}^n$, defined by a single polynomial equation $V : f = 0$, where f is a non-constant polynomial, has dimension $n - 1$.

Example

$V_1 \subset \mathbb{A}^1$, $V_1 : x^3 + x + 1 = 0$ has dimension 0.

$V_2 \subset \mathbb{A}^2$, $V_2 : y^2 = x^6 + 1$, has dimension 1.

$V_3 \subset \mathbb{P}^2$, $V_3 : x^3 + y^3 + z^3 = 0$, has dimension 1.

$V_4 \subset \mathbb{P}^3$, $V_4 : x^3 + y^3 + z^3 + w^3 = 0$, has dimension 2.

Varieties of dimension $1, 2, 3, \ldots$ are called **curves, surfaces, threefolds,** etc.

Smooth

Let V be an affine variety $V \subset \mathbb{A}^n$ of dimension d, defined over a field k, and given by a system of polynomial equations

$$V : \begin{cases} f_1(x_1,\ldots,x_n) = 0, \\ \qquad \vdots \\ f_m(x_1,\ldots,x_n) = 0, \end{cases} \qquad f_i \in k[x_1,\ldots,x_n].$$

We say that $P \in V(\overline{k})$ is smooth if the matrix

$$\operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i=1,\ldots,m,\, j=1,\ldots,n} = n-d.$$

We say that V is **smooth** or **non-singular** if it is smooth at all points $P \in V(\overline{k})$.

If $V \subset \mathbb{P}^n$, we say that V is **smooth** if all the affine patches $V \cap \{x_i = 1\}$ are smooth.

Example

Let

$$C : y^2 = f(x) \qquad \textbf{(hyperelliptic curve)}$$

where f is a non-constant polynomial. Then $P = (a, b) \in C$ is singular iff

$$(2a \qquad -f'(b)) = (0\,0).$$

So

$$2a = 0, \qquad a^2 = f(b), \qquad f'(b) = 0.$$

If $\mathrm{char}(k) \neq 2$, then $f(b) = f'(b) = 0$. So C has a singular point if and only if $\mathrm{Disc}(f) = 0$. So C is smooth iff $\mathrm{Disc}(f) \neq 0$.

Example

Let $V \subset \mathbb{P}^n$ (defined over k) be given by

$$V : f(x_0, \ldots, x_n) = 0,$$

where $f \neq 0$ is homogeneous. Then V is **singular** if and only if there is $P \in V(\overline{k})$ such that

$$\frac{\partial f}{\partial x_1}(P) = \cdots = \frac{\partial f}{\partial x_n}(P) = 0.$$

Curves

We will restrict to **c**urves.

Definition

By a curve C over a field k, we mean a smooth, projective, absolutely irreducible (or geometrically irreducible), 1-dimensional k-variety.

Rational Points: Given $C/\mathbb{Q}$, we want to understand $C(\mathbb{Q})$.

Example: Reducibility

Example

Consider the variety $V \subset \mathbb{A}^2$ given by the equation

$$V : x^6 - 1 = y^2 + 2y.$$

Can rewrite as

$$V : (y + 1 - x^3)(y + 1 + x^3) = 0.$$

So

$$V = V_1 \cup V_2$$

where

$$V_1 : y + 1 - x^3 = 0, \qquad V_2 : y + 1 + x^3 = 0.$$

Note V is *reducible*, but V_1 and V_2 are *irreducible*. To understand $V(\mathbb{Q})$ enough to understand $V_1(\mathbb{Q})$ and $V_2(\mathbb{Q})$.

Example: Absolute Reducibility

Example

$$V : 2x^6 - 1 = y^2 + 2y.$$

V is irreducible, but *absolutely reducible* since

$$V_{\overline{\mathbb{Q}}} = \{y + 1 + \sqrt{2}x^3 = 0\} \cup \{y + 1 - \sqrt{2}x^3 = 0\}.$$

If $(x, y) \in V(\mathbb{Q})$ then

$$y + 1 + \sqrt{2}x^3 = y + 1 - \sqrt{2}x^3 = 0.$$

In other words

$$y = -1, \qquad x = 0.$$

So $V(\mathbb{Q}) = \{(0, -1)\}$.

Moral: To understand rational points on varieties, it is enough to understand rational on absolutely irreducible varieties.

Function Fields

Let $V \subset \mathbb{A}^n$ be an absolutely irreducible affine variety defined over k by the equations

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \quad \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases} \qquad f_i \in k[x_1, \ldots, x_n].$$

The **affine coordinate ring** of V is given by

$$k[V] = k[x_1, \ldots, x_n]/(f_1, \ldots, f_m).$$

The **function field** $k(V)$ of V is the field of fractions of $k[V]$.

If $V \subset \mathbb{P}^n$ then its function field is the function field of any affine patch.

Example

$$k[\mathbb{A}^n] = k[x_1, \ldots, x_n], \qquad k(\mathbb{A}^n) = k(x_1, \ldots, x_n),$$

$$k(\mathbb{P}^n) = k(\mathbb{P}^n \cap \{x_0 = 1\}) = k(x_1, \ldots, x_n).$$

Function Fields

Let $V \subset \mathbb{A}^n$ be an absolutely irreducible affine variety defined over k by the equations

$$V : \begin{cases} f_1(x_1,\ldots,x_n) = 0, \\ \vdots \\ f_m(x_1,\ldots,x_n) = 0, \end{cases} \qquad f_i \in k[x_1,\ldots,x_n].$$

The **affine coordinate ring** of V is given by

$$k[V] = k[x_1,\ldots,x_n]/(f_1,\ldots,f_m).$$

The **function field** $k(V)$ of V is the field of fractions of $k[V]$.

If $V \subset \mathbb{P}^n$ then its function field is the function field of any affine patch.

Example

$$C : y^2 = f(x) \qquad f \in k[x]\backslash k, \qquad \operatorname{disc}(f) \neq 0.$$

$$k[C] = k[x,y]/(y^2 - f(x)), \qquad k(C) = k(x)(\sqrt{f(x)}).$$

Function Fields

Let $V \subset \mathbb{A}^n$ be an absolutely irreducible affine variety defined over k by the equations

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0, \end{cases} \qquad f_i \in k[x_1, \ldots, x_n].$$

The **affine coordinate ring** of V is given by

$$k[V] = k[x_1, \ldots, x_n]/(f_1, \ldots, f_m).$$

The **function field** $k(V)$ of V is the field of fractions of $k[V]$.

If $V \subset \mathbb{P}^n$ then its function field is the function field of any affine patch.

Example (Why do we want irreducibility?)

$$V \subset \mathbb{A}^2, \qquad V : x_1 x_2 = 0, \qquad k[V] = k[x_1, x_2]/(x_1 x_2).$$

x_1, x_2 are zero divisors in $k[V]$ so it isn't an integral domain.

Genus

We classify curves by **genus**. This is a non-negative integer: $0, 1, 2, \ldots$.

Example

If

$$C/k : F(x,y,z) = 0, \qquad C \subset \mathbb{P}^2$$

is smooth, where $F \in k[x,y,z]$ is homogeneous of degree n, then C has genus $(n-1)(n-2)/2$.

Example

Let

$$C/k : y^2 = f(x), \qquad C \subset \mathbb{A}^2 \qquad (f \in k[x] \text{ non-constant}).$$

If C is smooth and $\deg(f) = n$ then

$$\text{genus}(C) = \begin{cases} (d-1)/2 & d \text{ odd} \\ (d-2)/2 & d \text{ even.} \end{cases}$$

Curves of Genus 0

Theorem

Let C be a curve of genus 0 defined over k. Then C is isomorphic (over k) to a smooth plane curve of degree 2 (i.e. a conic). Moreover, if $C(k) \neq \emptyset$ then C is isomorphic over k to $\mathbb{P}^1$.

Theorem

(The Hasse Principle) Let $C/\mathbb{Q}$ be a curve of genus 0. The following are equivalent:

1. $C(\mathbb{Q}) \neq \emptyset$;
2. $C(\mathbb{R}) \neq \emptyset$ *and* $C(\mathbb{Q}_p) \neq \emptyset$ *for all primes* p.

Theorem

(The Hasse Principle) Let $C/\mathbb{Q}$ be a curve of genus 0. The following are equivalent:

1. $C(\mathbb{Q}) \neq \emptyset$;
2. $C(\mathbb{R}) \neq \emptyset$ *and* $C(\mathbb{Q}_p) \neq \emptyset$ *for all primes* p.

Theorem (Legendre, Hasse)

Let

$$C : ax^2 + by^2 + cz^2 = 0, \qquad a,\ b,\ c \text{ non-zero, squarefree integers.}$$

The following are equivalent:

1. $C(\mathbb{Q}) \neq \emptyset$;
2. $C(\mathbb{R}) \neq \emptyset$ *and* $C(\mathbb{Q}_p) \neq \emptyset$ *for all primes* p.
3. $C(\mathbb{R}) \neq \emptyset$ *and* $C(\mathbb{Q}_p) \neq \emptyset$ *for all primes* $p \mid 2abc$.

Genus 1

Theorem

If C is a curve of genus 1 over a field k and $P_0 \in C(k)$, then C is isomorphic over k to a Weierstrass elliptic curve

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad \subset \mathbb{P}^2,$$

where the isomorphism sends P_0 to $(0:1:0)$.
(Mordell–Weil) Moreover, if $k = \mathbb{Q}$ or a number field, then $C(k)$ is a finitely generated abelian group with P_0 as the zero element.

1. There is no known algorithm for deciding if $C(\mathbb{Q}) \neq \emptyset$.
2. There is no known algorithm for computing a Mordell–Weil basis for $C(\mathbb{Q})$ if it is non-empty.

But there is a descent strategy that usually works **(Steffen's lectures)**.

Genus ≥ 2

Theorem (Faltings)

Let C be a curve of genus ≥ 2 over a number field k. Then $C(k)$ is finite.

1. There is no known algorithm for computing $C(k)$.
2. There is no known algorithm for deciding if $C(k) \neq \emptyset$.

But there is a bag of tricks that can be used to show that $C(k)$ is empty, or determine $C(k)$ 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 in some example.

Divisors

Let C be a curve over k. A divisor D on C is a formal linear combination

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

We define the degree of D to be $\sum a_i$.

Example

Let

$$C \,:\, y^2 = x(x^2+1)(x^3+1).$$

Let

$$D_1 = 2\cdot(0,0)+(1,2), \quad D_2 = (i,0)-(-i,0), \quad D_3 = (i,0)+(-i,0)-2\cdot(1,2).$$

Then

$$\deg(D_1) = 3, \qquad \deg(D_2) = 0, \qquad \deg(D_3) = 0.$$

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

Example

Let

$$C/\mathbb{Q} : y^2 = x(x^2+1)(x^3+1).$$

Let

$$D_1 = 2\cdot(0,0)+(1,2), \quad D_2 = (i,0)-(-i,0), \quad D_3 = (i,0)+(-i,0)-2\cdot(1,2).$$

Then D_1 is rational, D_3 is rational, D_2 is **not** rational.

Definition

Let

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

This is an abelian group.

In the example $D_3 \in \mathrm{Div}^0(C/k)$, but D_1, $D_2 \notin \mathrm{Div}^0(C/k)$.

Principal Divisors

Let $k(C)$ be the function field of C, and let $f \in k(C)$. If $P \in C(\overline{k})$ then there is $v_P(f) \in \mathbb{Z}$ which measures the **order of vanishing** of f at P. Define

$$\operatorname{div}(f) = \sum_{P \in C(\overline{k})} v_P(f) \cdot P.$$

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

Example

Let $f = \frac{x^2-7}{x^3}$ on $\mathbb{P}^1$. Then

$$\operatorname{div}(f) = -3 \cdot (0) + (\sqrt{7}) + (-\sqrt{7})$$

Principal Divisors

Let $k(C)$ be the function field of C, and let $f \in k(C)$. If $P \in C(\overline{k})$ then there is $v_P(f) \in \mathbb{Z}$ which measures the **order of vanishing** of f at P. Define

$$\operatorname{div}(f) = \sum_{P \in C(\overline{k})} v_P(f) \cdot P.$$

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

Example

Let $f = \frac{x^2-7}{x^3}$ on $\mathbb{P}^1$. Then

$$\operatorname{div}(f) = -3 \cdot (0) + (\sqrt{7}) + (-\sqrt{7}) + \infty.$$

Picard Group

Define

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

This is an abelian group (note $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$). Also $\mathrm{Princ}(C/k) \subset \mathrm{Div}^0(C/k)$. We define the Picard group of C/k as

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

Example

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

Define

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

This is an abelian group (note $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$). Also $\mathrm{Princ}(C/k) \subset \mathrm{Div}^0(C/k)$. We define the Picard group of C/k as

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

Example

Let

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in k, \quad 4A^3 + 27B^2 \neq 0.$$

be an elliptic curve over k. Then (consequence of Riemann-Roch)

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

If C is a curve that isn't an elliptic curve, what is the right object to replace $E(k)$ in this isomorphism?

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 $J_C(k)$.

Example

Let

$$C\,:\,y^2 = x(x^2+1)(x^2+3).$$

The curve C has genus 2. Using descent it is possible to show that

$$J_C(\mathbb{Q}) = \frac{\mathbb{Z}}{2\mathbb{Z}}\cdot[(0,0)-\infty] \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}\cdot[(i,0)+(-i,0)-2\infty].$$

Note

$$[(0,0)-\infty]+[(i,0)+(-i,0)-2\infty] = [(\sqrt{-3},0)+(-\sqrt{-3},0)-2\infty].$$

Definition

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

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

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

Definition

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

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

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 $C(k)$.

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 $C(k)$.

Example

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

$$J_C(\mathbb{Q}) = \{0, [(0,0)-\infty], [(i,0)+(-i,0)-2\infty], [(\sqrt{-3},0)+(-\sqrt{-3},0)-2\infty]\}. \quad (1)$$

We can take $\iota : C \hookrightarrow J_C$, $P \mapsto [P-\infty]$, and using this we find that

$$C(\mathbb{Q}) = \{\infty, (0,0)\}.$$

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

Definition

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

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

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

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

Definition

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

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

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

Suppose C is defined over $\mathbb{Q}$. If $J_C(\mathbb{Q})$ is infinite, can we still use it to recover $C(\mathbb{Q})$?

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

Definition

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

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

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

Suppose C is defined over $\mathbb{Q}$. If $J_C(\mathbb{Q})$ is infinite, can we still use it to recover $C(\mathbb{Q})$?

Find out on Wednesday!

Pleeeeeeeeeease tell me now!