Rational Points on Curves

Samir Siksek

Assumptions

Prerequisites:

Assumptions

Prerequisites:

- Galois Theory.
- Algebraic Number Theory.
- p-adic Numbers.
- Algebraic Curves/Algebraic Geometry.
- Elliptic Curves.

Assumptions

Prerequisites:

- Galois Theory.
- Algebraic Number Theory.
- p-adic Numbers.
- Algebraic Curves/Algebraic Geometry.
- Elliptic Curves.

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

Assumptions

Prerequisites:

- Galois Theory.
- Algebraic Number Theory.
- p-adic Numbers.
- Algebraic Curves/Algebraic Geometry.
- Elliptic Curves.

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*

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

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

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

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

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

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

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**:

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

Local Methods

We're interested in understanding $V(\mathbb{Q})$ for varieties defined over $\mathbb{Q}$. More generally, if k is a number field, we're interested in $V(k)$ for varieties defined over k.
In particular, $\mathbb{Q} \subset \mathbb{R}$, and $\mathbb{Q} \subset \mathbb{Q}_p$ for all primes p. Think of $\mathbb{R} = \mathbb{Q}_\infty$.
Note $V(\mathbb{Q}) \subseteq V(\mathbb{Q}_p)$ for all p (including ∞). So,

$$V(\mathbb{Q}_p) = \emptyset \implies V(\mathbb{Q}) = \emptyset.$$

Example

$$V \ : \ x^2 + y^2 + z^2 = 0, \qquad V \subset \mathbb{P}^2.$$

Note $V(\mathbb{R}) = \emptyset$, so $V(\mathbb{Q}) = \emptyset$. But also, $V(\mathbb{Q}_2) = \emptyset$.

Local Methods

Definition

Let V be a variety defined over $\mathbb{Q}$. We say that V **has points everywhere locally** if $V(\mathbb{Q}_p) \neq \emptyset$ for all p (including ∞).

Trivial observation: $V(\mathbb{Q}) \neq \emptyset \implies V$ has points everywhere locally.

Theorem (Hasse–Minkowski)

Let $V \subset \mathbb{P}^n$ be a quadric ($n \geq 3$), defined over $\mathbb{Q}$. Then the following are equivalent:

- *V has points everywhere locally;*
- *$V(\mathbb{Q}) \neq \emptyset$ (V has global points).*

We say, quadrics **satisfy the Hasse principle**.

Fact

For varieties V defined over $\mathbb{Q}$ (or a number field), there is an algorithm to decide if V has points everywhere locally.

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

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

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

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

$$V_4 \subset \mathbb{P}^3, \qquad V_4 \; : \; x^3 + y^3 + z^3 + w^4 = 0, \quad \text{has dimension } 2.$$

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

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

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

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

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

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

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.

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

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

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

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3 \qquad \subset \mathbb{P}^2,$$

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.

Failure of the Hasse Principle in Genus 1

Example

Let

$$C \;:\; 3x^3 + 4y^3 + 5z^3 = 0. \qquad (C \text{ is a curve of genus 1 in } \mathbb{P}^2)$$

Then

1. $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ (C has points everywhere locally);
2. $C(\mathbb{Q}) = \emptyset$ (C has no global points).

In other words, C is a counterexample to the Hasse principle.

Exercise

Show that $X^4 - 17 = 2Y^2$ (also a curve of genus 1) is a counterexample to the Hasse principle.

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. Quotients;
2. Descent;
3. Chabauty;
4. 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.

Quotients

Let C be a curve over a field k. A quotient is curve D/k with a non-constant morphism

$$\phi : C \to D$$

also defined over k.

Lemma (Trivial Observation)

$\phi(C(k)) \subseteq D(k)$. *If we know* $D(k)$, *we can compute* $C(k)$.

Quotients

Example

Let

$$C \ : \ Y^2 = AX^6 + BX^4 + CX^2 + D, \qquad A, B, C, D \in \mathbb{Z},$$

and suppose $\mathrm{disc}(AX^6 + BX^4 + CX^2 + D) \neq 0$. So C has genus 2. Let

$$E_1 \ : \ y^2 = Ax^3 + Bx^2 + Cx + D, \qquad E_2 \ : \ y^2 = Dx^3 + Cx^2 + Bx + A.$$

Then E_1, E_2 are elliptic curves over $\mathbb{Q}$. We have non-constant morphisms

$$\phi_1 : C \to E_1, \qquad (X, Y) \mapsto (X^2, Y),$$

and

$$\phi_2 : C \to E_2, \qquad (X, Y) \mapsto \left(\frac{1}{X^2}, \frac{Y}{X^3} \right).$$

If the ranks of either E_i is 0 we can determine $E_i(\mathbb{Q})$ (which is finite) and so $C(\mathbb{Q})$.

Example

$$C \;:\; Y^2 = 13X^6 - 1.$$

Exercise: C has points everywhere locally.
Take $E : y^2 = x^3 + 13$ and $\phi : C \to E$ to be given by $(X, Y) \mapsto (-1/X^2, Y/X^3)$. Now $E(\mathbb{Q}) = \{\infty\}$. So $C(\mathbb{Q}) \subseteq \phi^{-1}(\infty) = \{(0, i),\ (0, -i)\}$. So $C(\mathbb{Q}) = \emptyset$.

Example

$$C \;:\; Y^2 = 11X^6 - 19.$$

Here:

- C has points everywhere locally.
- $E_1(\mathbb{Q}) \cong \mathbb{Z}$ and $E_2(\mathbb{Q}) \cong \mathbb{Z}$.

Example

$$C \ : \ Y^2 = 11X^6 - 19.$$

Here:

- C has points everywhere locally.
- $E_1(\mathbb{Q}) \cong \mathbb{Z}$ and $E_2(\mathbb{Q}) \cong \mathbb{Z}$.

Let p be a prime of good reduction. Note the commutative diagram:

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\phi"] \arrow[d, "\mathrm{red}"] & E_1(\mathbb{Q}) \times E_2(\mathbb{Q}) \arrow[d, "\mathrm{red}"] & \mathbb{Z} \times \mathbb{Z} \arrow[l, "\eta"'] \arrow[dl, "\mu"] \\
C(\mathbb{F}_p) \arrow[r, "\phi"] & E_1(\mathbb{F}_p) \times E_2(\mathbb{F}_p) &
\end{tikzcd}$$

- $\phi = (\phi_1, \phi_2)$; red denotes reduction modulo p;
- fix generators P_1, P_2 for $E_1(\mathbb{Q})$, $E_2(\mathbb{Q})$ respectively and let $\eta(m, n) = (mP_1, nP_2)$;
- $\mu = \text{red} \circ \eta$.

Let p be a prime of good reduction. Note the commutative diagram:

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\phi"] \arrow[d, "\mathrm{red}"] & E_1(\mathbb{Q}) \times E_2(\mathbb{Q}) \arrow[d, "\mathrm{red}"] & \mathbb{Z} \times \mathbb{Z} \arrow[l, "\eta"'] \arrow[dl, "\mu"] \\
C(\mathbb{F}_p) \arrow[r, "\phi"] & E_1(\mathbb{F}_p) \times E_2(\mathbb{F}_p) &
\end{tikzcd}$$

Lemma

$$(\mathrm{red} \circ \phi)(C(\mathbb{Q})) \subset \phi(C(\mathbb{F}_p)) \cap \mu(\mathbb{Z} \times \mathbb{Z}).$$

Exercise: Use this with $p = 7$ to show that $C(\mathbb{Q}) = \emptyset$.