Rational Points on Curves

Main Question: Given $f(x,y) \in \mathbb{Q}[x,y]$, or more generally an algebraic curve C over $\mathbb{Q}$, understand its rational solutions

$$C_f(\mathbb{Q}) = \{(a,b) \in \mathbb{Q}^2 \mid f(a,b) = 0\}$$

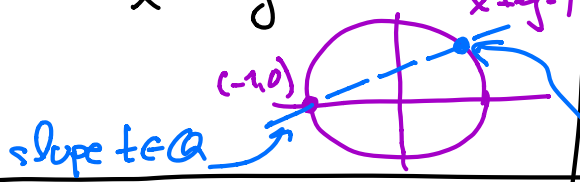
(or $C(\mathbb{Q})$ more generally).

- Is $C_f(\mathbb{Q}) \neq \emptyset$?
- If so, is $C_f(\mathbb{Q})$ finite? infinite? Other "structure" on $C_f(\mathbb{Q})$?

Approach: (1) Understand mod p, mod p^n, ---, p-adic solutions for all primes p.

(2) Understand the extent to which (1) controls the existence and structure of the rational solutions.

Examples

$f(x,y)$	$C_f(\mathbb{Q})$
$x+y$	Infinite and easy to parametrize $\{(t,-t) \mid t \in \mathbb{Q}\}$.
x^2+y^2+1	$\emptyset$. $C_f(\mathbb{R})=\emptyset$, and $C_f(\mathbb{Q}_p)=\emptyset$.
x^2+y^2-1 	Infinite, parametrized by $\left\{\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \mid t \in \mathbb{Q}\right\}$.
x^3-2-y^2 (in contrast, the set of $\mathbb{Z}$-solutions is finite!)	Infinite, but much harder to parametrize ("$\mathbb{Z}$") $\left(\frac{164323}{29241}, -\frac{66234835}{5000211}\right)$, for example
x^3+1-y^2	Finite. $\{(-1,0),(0,\pm 1),(2,\pm 3)\}$
$x^{691}+y^{691}-1$	Finite. $\{(1,0),(0,1)\}$ (FLT).

Degree of $f(x,y)$ is the first organizing feature of our study (more generally, the genus of the curve C).

Our target results

Degree 2 (warm-up)

(genus 0)

(Legendre)

Curve case of Hasse-Minkowski theorem over $\mathbb{Q}$:

Fix $a_1, a_2, a_3 \in \mathbb{Q} \setminus \{0\}$.

The homogeneous degree 2 polynomial equation

$$a_1 X^2 + a_2 Y^2 + a_3 Z^2 = 0$$

has a solution $(x, y, z) \in \mathbb{Q}^3 \setminus \{(0,0,0)\}$

if and only if

it has a non-zero solution in $\mathbb{R}^3$

and in $\mathbb{Q}_p^3$ for every prime p.

- Here $\mathbb{Q}_p$ = the field of p-adic numbers.

Degree 3

(genus 1)

- Example where the local-global principle of the H-M theorem fails for higher degree equations.

- Basics of elliptic curves, with a view toward an efficient proof of the Mordell-Weil Theorem.

Let $C \hookrightarrow \mathbb{P}^2$ be the projective curve defined by a homogeneous equation (deg 3) $y^2z = x^3 + axz^2 + bz^3$ for $a, b \in \mathbb{Q}$ satisfying $4a^3 + 27b^2 \neq 0$. Then in a natural way $C(\mathbb{Q})$ can be given the structure of an abelian group and:

Theorem (Mordell-[Weil]) The abelian group $C(\mathbb{Q})$ is finitely-generated,

i.e. $C(\mathbb{Q}) \cong \mathbb{Z}^r \times$ (finite abelian group)
for some $r \in \mathbb{Z}$.

- Both Mordell-Weil and Hasse-Minkowski hold with $\mathbb{Q}$ replaced by any number field.
- Both have "higher-dimensional" generalizations as well (M-W for abelian varieties, H-M for quadratic forms in any number of variables)

General degree (or genus)

Theorem: (Faltings — proof of Mordell's conjecture) Any non-singular plane curve C_f over $\mathbb{Q}$ of degree > 3 has $|C_f(\mathbb{Q})| < \infty$.

More generally, any non-singular curve C over a number field K with genus$(C) \geq 2$ has $|C(K)| < \infty$.

Too hard for us.

Any remaining time (there won't be any) we will devote to defining and studying

- the zeta function of an algebraic curve over $\mathbb{F}_p$ or $\mathbb{Q}$ (including statements of some fundamental theorems and conjectures: Weil conjectures, BSD conjecture, ---).

Prerequisites

- a 1st course in algebra, including Galois theory
- basic algebraic number theory: number fields, their rings of algebraic integers, the fundamental finiteness theorems (finiteness of the class group, Dirichlet unit theorem, Hermite-Minkowski theorem)
  - to some extent these can be black boxed, but by week 3 or 4 you should know the basic language (see e.g. Marcus, Number Fields)
- "local" algebraic number theory: the p-adics ($\mathbb{Z}_p, \mathbb{Q}_p$) — construction and basics — and eventually (~week 4) their generalizations (completions of a number field at its primes)
  - see Serre, A Course in Arithmetic (Chpt 2) ASAP for an intro. We'll discuss Hensel's Lemma in class.
  For a fuller (and more general) treatment, see Neukirch, Algebraic Number Theory Chpt 2 §1-5.

- a little language of algebraic geometry (only need the case of curves): affine and projective space over a field, affine and projective varieties, what it means for a variety to be non-singular at a point. maybe more later (it will depend on your backgrounds)

- see Silverman-Tate, Rational Points on Elliptic Curves, Appendix A, for an elementary treatment of the minimum we will use.
see Fulton, Algebraic Curves, for an accessible systematic study
see Milne, Elliptic Curves, Chpt. 1, for a useful introduction (with some proofs)

Other references for following the course

- For Hasse-Minkowski / $\mathbb{Q}$: Serre Chpt. 4
- For elliptic curves and the Mordell-Weil theorem: Silverman-Tate Chpt. 1 and 3
or Milne Chpt. 2 and 4
or Silverman, The Arithmetic of Elliptic Curves, Chpt. 3, 7, 8.
- For an introduction to the arithmetic of

curves of higher genus, see
Lorenzini, An Invitation to Arithmetic Geometry

Other remarks:

- I'll post a problem set each week.
  The course assistants will run problem sessions / review of background sessions.
- please ask questions in class.
- feel free to email me (patrikis.1@osu.edu) with other questions.

(notes + psets posted on my osu website.)

Topic 1: Hasse-Minkowski theorem for plane curves of degree 2 over $\mathbb{Q}$

(see Serre, Chpt. 4)

Quadratic forms. Let k be a field, and let V be a vector space over k of finite dimension $n = \dim_k(V)$. A function $f: V \longrightarrow k$ is a quadratic form if

1) $f(ax) = a^2 f(x) \quad \forall a \in k, x \in V$

2) $V \times V \longrightarrow k$

$(x, y) \longmapsto f(x+y) - f(x) - f(y)$

is a bilinear form.

definition of $\langle \cdot, \cdot \rangle : V \times V \to k$

We'll always assume $\mathrm{char}(k) \neq 2$

Then $\langle x, y \rangle := \frac{1}{2}\left(f(x+y) - f(x) - f(y)\right)$

is a symmetric bilinear form such that

$\langle x, x \rangle = \frac{1}{2}\left[f(2x) - f(x) - f(x)\right] = f(x)$

(can recover f from $\langle \cdot, \cdot \rangle$).

Therefore (for $\mathrm{char}(k) \neq 2$)

$$\left\{\begin{array}{l}\text{quadratic}\\ \text{forms over } k\end{array}\right\} \longrightarrow \left\{\begin{array}{l}\text{symmetric bilinear}\\ \text{forms over } k\end{array}\right\}$$

$$f: V \to k \longmapsto \langle\ ,\ \rangle : V \times V \to k$$

$$\langle x, y\rangle = \tfrac{1}{2}\left(f(x+y) - f(x) - f(y)\right)$$

is a bijection with inverse

$$f(x) = \langle x, x\rangle \longleftarrow \langle\ ,\ \rangle : V \times V \to k$$

(check these are inverses)

Matrix of the quadratic form f:

Choose a basis $e_1, \dots, e_n$ of V. Then

$$f\left(\sum_{i=1}^{n} x_i e_i\right) = \left\langle \sum_i x_i e_i, \sum_j x_j e_j \right\rangle = \sum_{i,j=1}^{n} \langle e_i, e_j\rangle x_i x_j$$

($x_i \in k$)

Write $a_{ij} = \langle e_i, e_j\rangle$ $\left(= \langle e_j, e_i\rangle = a_{ji}\right)$

The matrix of f in the basis $\{e_i\}$ is

$$A = (a_{ij})$$

$$\left\langle \sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j \right\rangle = (x_1 \cdots x_n) A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

$$\boxed{{}^t A = A}$$

Change-of-basis: replacing $\{e_i\}$ with the basis $e_i' = \sum_j c_{ij} e_j$

$$\langle e_i', e_k' \rangle = \left\langle \sum_{j=1}^{n} c_{ij} e_j, \sum_{\ell=1}^{n} c_{k\ell} e_\ell \right\rangle$$

$$= \sum_{j,\ell} c_{ij} a_{j\ell} c_{k\ell}$$

$$= (i,k)\text{-entry of } C \cdot A \cdot {}^tC.$$

(check!).

- The discriminant of f is the element $\det(A) \in k/\sim$ where $a \sim a\lambda^2$ $\forall \lambda \in k^\times$.

(well-defined since $\det(C \cdot A \cdot {}^tC) = \det(A) \cdot \det(C)^2$.)

- f is non-degenerate if one of the following equivalent conditions holds:
  - $\operatorname{disc}(f) \neq 0$
  - the symmetric bilinear form $\langle , \rangle$ is non-degenerate.

Diagonalizing quadratic forms

Lemma: There exists a basis $\{e_i\}$ of V in which f is diagonal:

$$f\left(\sum_i x_i e_i\right) = \sum_i a_i x_i^2$$

(ie $\exists$ orthogonal basis of V: $\langle e_i, e_j \rangle = 0$ for $i \neq j$).

- exercise

Conics associated to quadratic forms in 3 variables.

k : a field of characteristic $\neq 2$.

$$f(X_0, X_1, X_2) = \sum_{i,j=0}^{2} a_{ij} X_i X_j \quad \text{with } a_{ij} \in k$$

a quadratic form in 3 variables.

- we may and do assume that $a_{ij} = a_{ji}$ $\forall\, i,j$.

The solutions to $f = 0$ in k and fields containing k define an algebraic variety.

More precisely, we could:

(A) consider solutions to $f(X_0, X_1, X_2) = 0$ in $K \times K \times K$ for any field containing $K \supset k$, defining an affine surface in $\mathbb{A}^3$

— this is not what we'll do.

(B) alternatively, consider solutions in

$$\mathbb{P}^2(K) = \frac{K^3 - \{(0,0,0)\}}{\sim} \text{ where}$$

$(a_0, a_1, a_2) \sim (\lambda a_0, \lambda a_1, \lambda a_2)$ for any $\lambda \in K^\times$.

($\mathbb{P}^2(K) \longleftrightarrow$ set of lines through 0 in K^3).

Write $[a_0, a_1, a_2]$ for the equivalence class in $\mathbb{P}^2(K)$ of $(a_0, a_1, a_2) \in K^3 \setminus 0$.

(*) It makes sense to ask whether $[a_0, a_1, a_2] \in \mathbb{P}^2(K)$ satisfies $f(a_0, a_1, a_2) = 0$

because $f(a_0, a_1, a_2) = 0 \iff f(\lambda a_0, \lambda a_1, \lambda a_2)\ \forall \lambda \in K^\times$

f is a homogeneous polynomial $\qquad \lambda^{??} f(a_0, a_1, a_2) = 0$

Notation: $C_f(K) \subset \mathbb{P}^2(K)$ is the set of $[a_0, a_1, a_2] \in \mathbb{P}^2(K)$: $f(a_0, a_1, a_2) = 0$.

We just write C_f for $C_f(\bar{k})$, $\bar{k}$ a fixed algebraic closure of k. C_f is a projective variety (a conic).