Rational Points on Curves

Samir Siksek

Recall: given a curve C over $\mathbb{Q}$, or over a number field k, we want a complete description of $C(k)$. For genus ≥ 1, there is no algorithm for giving this! But there is a bag of tricks that can be used to show that $C(k)$ 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* $D(k)$ *and it is finite, we can compute* $C(k)$.

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 $C(\mathbb{Q}) = \emptyset$.

Descent

Example

We will study the rational points on the genus 2 curve.

$$C \ : \ Y^2 = (X^2 + X + 1)(X^4 + 7). \tag{1}$$

(N.B. no obvious quotients.) Write

$$X = \frac{x}{z}, \qquad Y = \frac{y}{z^3}, \qquad x, y, z \in \mathbb{Z}, \qquad \gcd(x, z) = 1.$$

So

$$y^2 = (x^2 + xz + z^2)(x^4 + 7z^4). \tag{2}$$

Note we have 2 extra points on this model $(x : y : z) = (1 : \pm 1 : 0)$ which we think of as points are infinity on (1). We think of (2) as an equation for C in $\mathbb{P}(1, 3, 1)$.
Does C have any other rational points?

Lemma

If x, y are coprime non-zero integers and $xy = z^n$ where z is also an integer, $n \geq 1$, then there exists $x_1, y_1 \in \mathbb{Z}$ such that $x = \pm x_1^n$ and $y = \pm y_1^n$.

Lemma

Let S be a set of primes. If x, y are non-zero integers and $xy = z^n$ where z is also an integer, $n \geq 1$. If x, y are coprime outside S then there exists $x_1, y_1 \in \mathbb{Z}$ such that $x = a x_1^n$ and $y = b y_1^n$, where all the prime factors of a, b belong to S.

Resultants

Lemma

Let f, $g \in \mathbb{Z}[x]$, *coprime. Then there is a* $R = R(f,g) \in \mathbb{Z}$, $R \neq 0$ *(*R *is called the* **resultant***), and polynomials* a, $b \in \mathbb{Z}[x]$ *such that*

$$a(x)f(x) + b(x)g(x) = R.$$

In particular, if $\alpha \in \mathbb{Z}$, *then* $\gcd(f(\alpha), g(\alpha)) \mid R$.

Lemma

Let $F(x, y)$, $G(x, y)$ be coprime homogeneous polynomials $\in \mathbb{Z}[x, y]$. Let $f = F(x, 1)$ and $g = G(x, 1)$, and define $R = R(F, G) = R(f, g)$ (the resultant of F and G). If α, $\beta \in \mathbb{Z}$ are coprime, then

$$\gcd(F(\alpha, \beta), G(\alpha, \beta)) \mid R.$$

Proof.

We know that $a(x)f(x) + b(x)g(x) = R$. Substitute $x = \alpha/\beta$ and homogenize, to obtain

$$A(\alpha, \beta)F(\alpha, \beta) + B(\alpha, \beta)G(\alpha, \beta) = R\beta^m$$

for some m. It turns out that also,

$$A'(\alpha, \beta)F(\alpha, \beta) + B'(\alpha, \beta)G(\alpha, \beta) = R\alpha^n.$$

So

$$\gcd(F(\alpha, \beta), G(\alpha, \beta)) \mid \gcd(R\beta^m, R\alpha^n) = R.$$

Example

We will study the rational points on the genus 2 curve.

$$C \ : \ Y^2 = (X^2 + X + 1)(X^4 + 7).$$

Write

$$X = \frac{x}{z}, \qquad Y = \frac{y}{z^3}, \qquad x, y, z \in \mathbb{Z}, \qquad \gcd(x, z) = 1.$$

So

$$C \ : \ y^2 = (x^2 + xz + z^2)(x^4 + 7z^4).$$

The resultant of the two polynomials is 43, so

$$\gcd(x^2 + xz + z^2, x^4 + 7z^4) = 1 \text{ or } 43.$$

So the two factors are coprime outside $S = \{43\}$. Hence

$$x^2 + xz + z^2 = ay_1^2, \qquad x^4 + 7z^4 = ay_2^2 \qquad \text{where } a = \pm 1 \text{ or } a = \pm 43.$$

$$C \ : \ Y^2 = (X^2 + X + 1)(X^4 + 7).$$

$$x^2 + xz + z^2 = ay_1^2, \qquad x^4 + 7z^4 = ay_2^2 \qquad \text{where } a = \pm 1 \text{ or } a = \pm 43.$$

So we obtain four curves

$$D_a \ : \ \begin{cases} X^2 + X + 1 = aY_1^2, \\ X^4 + 7 = aY_2^2 \end{cases}$$

with $a = \pm 1, \pm 43$. Let $\phi_a : D_a \to C$ be given by $\phi_a(X, Y_1, Y_2) = (X, aY_1Y_2)$. From the above argument,

$$C(\mathbb{Q}) = \bigcup_a \phi_a\left(D_a(\mathbb{Q})\right).$$

Vague Definition Given a curve C over a number field k, a **descent** is some process which which yields a finite family $\phi_a : D_a \to C$ of **covers** such that

$$C(k) = \bigcup_a \phi_a\left(D_a(k)\right).$$

$$C \;:\; Y^2 = (X^2+X+1)(X^4+7).$$

$$x^2+xz+z^2 = ay_1^2, \qquad x^4+7z^4 = ay_2^2 \qquad \text{where } a=\pm 1 \text{ or } a=\pm 43.$$

So we obtain four curves

$$D_a \;:\; \begin{cases} X^2+X+1 = aY_1^2, \\ X^4+7 = aY_2^2 \end{cases}$$

with $a=\pm 1, \pm 43$. Let $\phi_a : D_a \to C$ be given by $\phi_a(X, Y_1, Y_2) = (X, aY_1Y_2)$. From the above argument,

$$C(\mathbb{Q}) = \bigcup_a \phi_a\left(D_a(\mathbb{Q})\right).$$

- $D_{-1}(\mathbb{R}) = \emptyset$, so $D_{-1}(\mathbb{Q}) = \emptyset$.
- $D_{-43}(\mathbb{R}) = \emptyset$, so $D_{-43}(\mathbb{Q}) = \emptyset$.
- $D_{43}(\mathbb{Q}_2) = \emptyset$, so $D_{43}(\mathbb{Q}) = \emptyset$.

$$C \ : \ Y^2 = (X^2 + X + 1)(X^4 + 7).$$

After descent and local solvability checking, we have

$$C(\mathbb{Q}) = \phi(D(\mathbb{Q}))$$

where

$$D = D_1 \ : \ \begin{cases} X^2 + X + 1 = Y_1^2, \\ X^4 + 7 = Y_2^2, \end{cases} \qquad \phi(X, Y_1, Y_2) = (X, Y_1 Y_2).$$

In fact D_1 has four rational points are infinity. So $D_1(\mathbb{Q}) \neq \emptyset$.

Reduced finding all rational points on C (which has genus 2) to finding all rational points on D (which has genus 3).

The curve

$$D \ : \ \begin{cases} X^2 + X + 1 = Y_1^2, \\ X^4 + 7 = Y_2^2, \end{cases}$$

has a genus 1 quotient: $X^4 + 7 = Y_2^2$. In fact, we have $\psi : D \to E$,

$$E \ : \ y^2 = x(x^2 + 7), \qquad (X, Y_1, Y_2) \mapsto (X^2, XY_2).$$

But

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

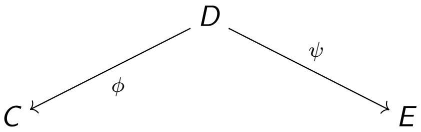
So

$$D(\mathbb{Q}) = \{(1 : \pm 1 : \pm 1 : 0)\}.$$

So

$$C(\mathbb{Q}) = \{(1 : \pm 1 : 0)\}.$$

Note the following diagram



To find the rational points on C we constructed a cover D and used its quotient E.

Example

The curve

$$C \ : \ X^4 - 17 = 2Y^2$$

has points everywhere locally. We will use descent to show that $C(\mathbb{Q}) = \emptyset$. Write

$$X = \frac{x}{z}, \qquad Y = \frac{y}{z^2}, \qquad x, y, z \in \mathbb{Z}, \qquad \gcd(x, z) = 1.$$

so

$$x^4 - 17z^4 = 2y^2.$$

Note y is even: write $y = 2y_1$. So

$$x^4 - 17z^4 = 8y_1^2.$$

Obtain

$$(x^2 + z^2\sqrt{17})(x^2 - z^2\sqrt{17}) = 8y_1^2.$$

$$x^4 - 17z^4 = 8y_1^2 \qquad \gcd(x,z) = 1.$$

Obtain

$$(x^2 + z^2\sqrt{17})(x^2 - z^2\sqrt{17}) = 8y_1^2.$$

Let $K = \mathbb{Q}(\sqrt{17})$, and $\mathcal{O}$ its ring of integers. So

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\frac{(1+\sqrt{17})}{2}, \qquad \mathcal{O}^\times = \{\pm(4+\sqrt{17})^n : n \in \mathbb{Z}\}.$$

Also $\mathcal{O}$ has class number 1 (i.e. it is a UFD)

$$\left(\frac{x^2 + z^2\sqrt{17}}{2}\right)\left(\frac{x^2 - z^2\sqrt{17}}{2}\right) = 2y_1^2.$$

The gcd of the two factors divides x^2 and $\sqrt{17}z^2$, so divides $\sqrt{17}$. But $17 \nmid y$. So gcd $= 1$.

$$\mathcal{O}^\times = \{\pm(4+\sqrt{17})^n : n \in \mathbb{Z}\}, \qquad 2 = \left(\frac{5+\sqrt{17}}{2}\right)\left(\frac{5-\sqrt{17}}{2}\right).$$

$$\left(\frac{x^2+z^2\sqrt{17}}{2}\right)\left(\frac{x^2-z^2\sqrt{17}}{2}\right) = 2y_1^2.$$

So

$$\frac{x^2+z^2\sqrt{17}}{2} = \alpha\mu^2, \qquad \frac{x^2-z^2\sqrt{17}}{2} = \bar{\alpha}\bar{\mu}^2, \qquad \mu \in \mathcal{O}$$

and

$$\alpha = \pm\left(\frac{5\pm\sqrt{17}}{2}\right), \qquad \pm\left(\frac{5\pm\sqrt{17}}{2}\right)(4+\sqrt{17})$$

Since $\alpha\bar{\alpha} = 2$, and $\alpha > 0$ we have

$$\alpha = \left(\frac{5\pm\sqrt{17}}{2}\right).$$

So

$$\frac{x^2+z^2\sqrt{17}}{2} = \left(\frac{5 \pm \sqrt{17}}{2}\right)(u+v\sqrt{17})^2 \qquad u, v \in \mathbb{Q}.$$

So

$$x^2+z^2\sqrt{17} = \left(5u^2+85v^2 \pm 34uv\right) + \left(\pm(u^2+17v^2)+10uv\right)\sqrt{17}.$$

So get

$$\begin{cases} 5u^2+85v^2 \pm 34uv = x^2 \\ \pm(u^2+17v^2)+10uv = z^2. \end{cases}$$

The important point is that these define curves over $\mathbb{Q}$, and $C(\mathbb{Q}) = \cup \phi_a(D_a(\mathbb{Q}))$, even though the descent argument works over an extension.

Finally $D_a(\mathbb{Q}_{17}) = \emptyset$. So $C(\mathbb{Q}) = \emptyset$.

A More General Example

Suppose that

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

where $f \in \mathbb{Z}[x]$ is irreducible with even degree n. Homogenizing we have

$$Y^2 = F(X, Z)$$

where F is homogeneous and $F(x, 1) = f(x)$. Let θ be a root of f and $K = \mathbb{Q}(\theta)$. Then we can factor

$$Y^2 = (X - \theta Z)G(X, Z)$$

Using algebraic number theory

$$X - \theta Z = \alpha \cdot \mu^2$$

where α belongs to a finite computable set, and $\mu \in K$. Write $\mu = u_0 + u_1\theta + \cdots + u_{n-1}\theta^{n-1}$. Then

$$X - \theta Z = Q_1^{\alpha}(u_0, \ldots, u_n) + Q_2^{\alpha}(u_0, \ldots, u_n)\theta + \cdots + Q_n^{\alpha}(u_0, \ldots, u_n)\theta^{n-1}.$$

$$Y^2 = (X - \theta Z) G(X, Z)$$

Using algebraic number theory

$$X - \theta Z = \alpha \cdot \mu^2$$

where α belongs to a finite computable set, and $\mu \in K$. Write $\mu = u_0 + u_1\theta + \cdots + u_{n-1}\theta^{n-1}$. Then

$$X - \theta Z = Q_1^\alpha(u_0, \ldots, u_n) + Q_2^\alpha(u_0, \ldots, u_n)\theta + \cdots + Q_n^\alpha(u_0, \ldots, u_n)\theta^{n-1},$$

where Q_i^α are homogeneous degree 2 polynomials. Comparing coefficients we have obtain covers

$$D_\alpha \; : \; \begin{cases} Q_3^\alpha(u_0, \ldots, u_n) = 0 \\ \vdots \\ Q_n^\alpha(u_0, \ldots, u_n) = 0, \end{cases}$$