Elliptic Curves II

Reinier Bröker
Fields Institute & University of Calgary

Summer School before ECC
September 2006

Elliptic curves

An *elliptic curve* E over a field K is given by a Weierstraß equation

$$Y^2 + h(X)Y = f(X)$$

with $h, f \in K[X]$.

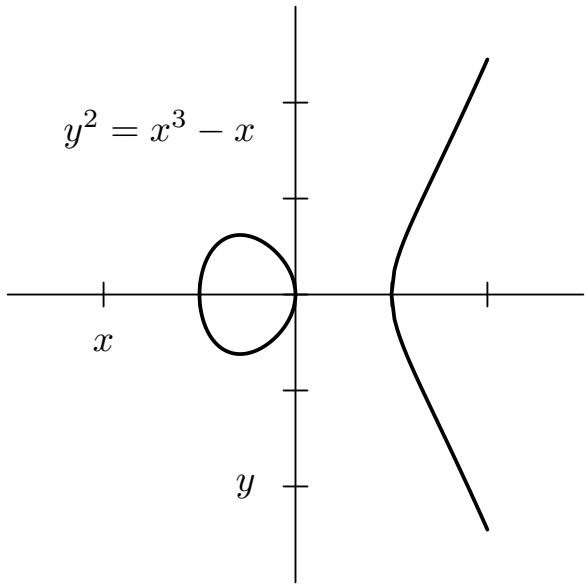
The set $E(K) = \{(x, y) \in K^2 | y^2 + h(x)y = f(x)\} \cup \{O_E\}$ has a natural group structure.

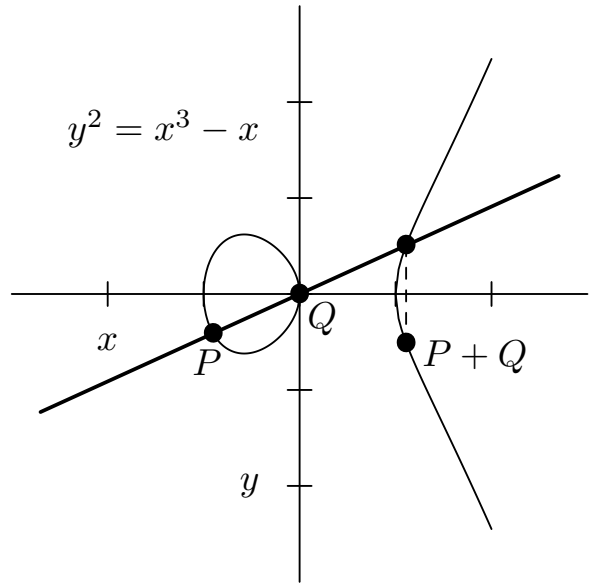
For simplicity restrict to $\mathrm{char}(K) \neq 2, 3$. The equation can then be put in the form

$$Y^2 = X^3 + aX + b$$

with $a, b \in K$.

Group operation





Maps between elliptic curves

A *morphism* $\varphi : E_1 \to E_2$ is given by rational functions, i.e., quotients of polynomials over $\overline{K}$.

With $\varphi = (f_1, f_2)$, we require $(f_1(x, y), f_2(x, y)) \in E_2(K)$.

Examples.

- $\varphi : E \to E$ given by $\varphi(x, y) = (x, -y)$.

- more generally: $\varphi : E \to E$ given by $\varphi(P) = nP$ for $n \in \mathbf{Z}_{\geq 1}$.

Multiplication by n

$\Psi_{-1}(X,Y) = -1$, $\Psi_0(X,Y) = 0$, $\Psi_1(X,Y) = 1$, $\Psi_2(X,Y) = 2Y$

$\Psi_3(X,Y) = 3X^4 + 6aX^2 + 12bX - a^2$, $\Psi_4(X,Y) = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3)$

$\Psi_{2n} = \Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)/2Y \ (n \in \mathbf{Z}_{\geq 1})$

$\Psi_{2n+1} = \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1} \ (n \in \mathbf{Z}_{\geq 1})$

Theorem. For $P = (x,y) \in E(\overline{K})$, $n \in \mathbf{Z}_{\geq 1}$ with $nP \neq 0$, we have

$$nP = \left(x - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4y\Psi_n^3} \right).$$

Don't remember the formulas! Just remember they exist…

More morphisms

Define $E/\mathbf{Q}$ by $Y^2 = X^3 + X$.

Define $\varphi : E \to E$ by $\varphi(x, y) = (-x, -iy)$.

Compute: $(-iy)^2 = -y^2$, and $(-x)^3 + (-x) = -x^3 - x$. We indeed have $\varphi(x, y) \in E(\mathbf{Q})$ for $(x, y) \in E(\mathbf{Q})$.

Note: $(\varphi \circ \varphi)(x, y) = (x, -y) = [-1]$. We write $\varphi = [i]$.

- $[i] \notin \mathbf{Z}$
- $[i]$ is not defined over $\mathbf{Q}$, but over $\mathbf{Q}(i)$ (or $\overline{\mathbf{Q}}$)

Generalities on morphisms

Morphisms between elliptic curves are automatically *group homomorphisms* on the point groups.

Morphisms are either constant or 'geometrically surjective': surjective over a finite extension of K.

Elliptic curves over finite fields

On $\mathbf{F}_q$ the map $x \mapsto x^q$ is a homomorphism.

This map induces a map on $E(\overline{\mathbf{F}}_q)$:

$$F_q : (x, y) \mapsto (x^q, y^q),$$

called *Frobenius*.

(Compute $(x^q)^3 + ax^q + b = (x^3)^q + a^q x^q + b^q = (x^3 + ax + b)^q$.)

We have $E(\mathbf{F}_q) = \mathrm{Ker}([1] - F_q)$.

Endomorphism ring

Let E/K be an elliptic curve.

The *endomorphisms* $E \to E$ have a natural ring structure.

Addition: pointwise. Multiplication: composition.

Write $\mathrm{End}(E) = \mathrm{End}_{\overline{K}}(E)$.

Involution on endomorphism ring

The ring $\mathrm{End}(E)$ has an involution $\bar{\cdot}$.

Properties:

- $\overline{\overline{\varphi}} = \varphi$
- $\overline{\varphi + \varphi'} = \overline{\varphi} + \overline{\varphi'}$
- $\overline{\varphi\varphi'} = \overline{\varphi}\,\overline{\varphi'}$
- $n \in \mathbf{Z} \Longrightarrow \overline{[n]} = [n]$
- for $\varphi \in \mathrm{End}(E)$, there is a unique $n \in \mathbf{Z}_{\geq 0}$ with $\varphi\overline{\varphi} = \overline{\varphi}\varphi = [n]$. It is called the *degree* of φ.
- for $\gcd(\deg(\varphi), \mathrm{char}(K)) = 1$ we have $\#\mathrm{Ker}(\varphi) = \deg(\varphi)$.

Using the involution on Frobenius

Let $E/\mathbf{F}_q$ be an elliptic curve. We have $E(\mathbf{F}_q) = \mathrm{Ker}([1] - F_q)$ with $F_q(x, y) = (x^q, y^q)$.

Compute $\#E(\mathbf{F}_q) = \#\mathrm{Ker}(1 - F_q) = \deg(1 - F_q) =$
$= (1 - F_q)(\overline{1 - F_q}) = (1 - F_q)(1 - \overline{F_q}) = F_q\overline{F_q} + 1 - (F_q + \overline{F_q}) =$
$= \deg(F_q) + 1 - (F_q + \overline{F_q}) = q + 1 - t.$

The integer t is called the *trace of Frobenius*.

Frobenius satisfies $F_q^2 - tF_q + q = 0 \in \mathrm{End}(E)$.

Hasse (1933): $|t| \leq 2\sqrt{q}$.

Structure of endomorphism ring

Three cases can arise:

(1) $\mathrm{End}(E) = \mathbf{Z}$

(2) $\mathrm{End}(E) = \mathbf{Z}[\alpha]$ with α imaginary quadratic

(3) $\mathrm{End}(E)$ is an order in a quaternion algebra

The rings in (1) and (2) are commutative, the ring in (3) is not.

For $\mathrm{char}(K) = 0$, we are in case (1) or (2). Reason: we can embed $\mathrm{End}(E)$ in $\overline{K}$.

For finite fields, we are in case (2) or (3).

Ordinary vs. supersingular curves

For $K = \mathbf{F}_q$ we have $\mathrm{End}(E) = \mathbf{Z}[\alpha]$ or $\mathrm{End}(E)$ is an order in a quaternion algebra. Proof: see exercises.

In the first case, E is called *ordinary*. Second case: *supersingular*.

Theorem. E is supersingular $\iff p \mid t \iff E[p] = \{O\}$.
Supersingular curves are 'rare': they have $j(E) \in \mathbf{F}_{p^2}$.

Crypto: usually uses ordinary curves.