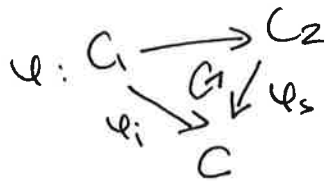


Elliptic curves over finite fields

① More on isogenies

Prop (sil. Chap II). Let C_1, C_2 be curves/ K and $\phi: C_1 \rightarrow C_2$ a morphism
 $\Rightarrow \exists C$, where ψ_s separable morphism and ψ_i totally inseparable (or = id).

morphism s.t.



$$\deg_s \phi = \deg_s(\psi_s)$$

$$\deg_i \phi = \deg(\psi_i)$$

$$\Rightarrow \deg(\phi) = \deg_i(\phi) \deg_s(\phi)$$

Obs: If ϕ separable $\Rightarrow \phi = \psi_s$

if ϕ is totally inseparable $\Rightarrow \phi = \psi_i$.

Prop (2.7, sil II) $\phi: C_1 \rightarrow C_2$ unramified $\Leftrightarrow \# \phi^{-1}(Q) = \deg(\phi)$

Moreover, for all but finitely many $Q \in C_2$, $\# \phi^{-1}(Q) = \deg_s(\phi)$.

So, if ϕ is a separable isogeny $\Rightarrow \phi$ unramified $\Rightarrow \# \text{Ker}(\phi) = \deg_s(\phi) = \deg(\phi)$.

Prop (sil. III, 5.5) E/\mathbb{F}_q , $\phi: E \rightarrow E$ q -Frobenius, $n, m \in \mathbb{Z}$.
 Then, $m+n\phi: E \rightarrow E$ is separable $\Leftrightarrow p \nmid m$.

In particular, $\phi - 1$ is separable.

② Number of \mathbb{F}_q -rational points

$$E/\mathbb{F}_q: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{F}_q.$$

$(x, y) \in \mathbb{F}_q^2$, then there are ≤ 2 values $y \in \mathbb{F}_q$ s.t. $y^2 = x$

$$\Rightarrow \# E(\mathbb{F}_q) \leq 2q + 1.$$

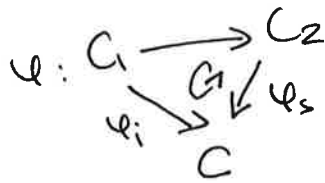
↑ the $(0:1:0)$

Elliptic curves over finite fields

① More on isogenies

Prop (sil. Chap II). Let C_1, C_2 be curves/ K and $\phi: C_1 \rightarrow C_2$ a morphism
 $\Rightarrow \exists C$, where ψ_s separable morphism and ψ_i totally inseparable (or = id).

morphism s.t.



$$\deg_s \phi = \deg_s(\psi_s)$$

$$\deg_i \phi = \deg(\psi_i)$$

$$\Rightarrow \deg(\phi) = \deg_i(\phi) \deg_s(\phi)$$

Obs: If ϕ separable $\Rightarrow \phi = \psi_s$

if ϕ is totally inseparable $\Rightarrow \phi = \psi_i$.

Prop (2.7, sil II) $\phi: C_1 \rightarrow C_2$ unramified $\Leftrightarrow \# \phi^{-1}(Q) = \deg(\phi)$

Moreover, for all but finitely many $Q \in C_2$, $\# \phi^{-1}(Q) = \deg_s(\phi)$.

So, if ϕ is a separable isogeny $\Rightarrow \phi$ unramified $\Rightarrow \# \text{Ker}(\phi) = \deg_s(\phi) = \deg(\phi)$.

Prop (sil. III, 5.5) E/\mathbb{F}_q , $\phi: E \rightarrow E$ q -Frobenius, $n, m \in \mathbb{Z}$.

Then, $m+n\phi: E \rightarrow E$ is separable $\Leftrightarrow p \nmid m$.

In particular, $\phi - 1$ is separable.

② Number of \mathbb{F}_q -rational points

$$E/\mathbb{F}_q: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{F}_q.$$

$(x, y) \in \mathbb{F}_q^2$, then there are ≤ 2 values $y \in \mathbb{F}_q$ s.t. $y^2 = x$

$$\Rightarrow \# E(\mathbb{F}_q) \leq 2q + 1.$$

↑ the $(0:1:0)$

The zeta function

Let C/\mathbb{F}_q be a curve, ~~Let E/\mathbb{F}_q be an elliptic curve~~

define
$$Z(C/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n}) \frac{T^n}{n}\right)$$

Notice:
$$\frac{1}{(n-1)!} \frac{d^n}{dT^n} \log Z(C/\mathbb{F}_q; T) \Big|_{T=0} = \#C(\mathbb{F}_{q^n})$$

Thm: E/\mathbb{F}_q elliptic curve. Let $\phi: E \rightarrow E$ be the q -Frobenius.

$a := q + 1 - \#E(\mathbb{F}_q)$.

- a) Let α, β roots of $T^2 - aT + q \Rightarrow \#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$
- b) $\phi^2 = a\phi + q$ in $\text{End}(E)$

Thm: Let E/\mathbb{F}_q be an elliptic curve $\Rightarrow \exists a \in \mathbb{Z}$ s.t.

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

Moreover, $Z_E(1/qT) = Z_E(T)$ and $1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$, $|\alpha| = |\beta| = \sqrt{q}$.

Proof:
$$\log Z_E(T) = \sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n} = \sum_{n=1}^{\infty} \frac{(1 - \alpha^n - \beta^n + q^n) T^n}{n} =$$

$$= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT)$$

$a = \alpha + \beta = q + 1 - \#E(\mathbb{F}_q) \in \mathbb{Z}$

α, β are complex conjugates $\Rightarrow |\alpha| = |\beta| = \sqrt{q}$. $\#$

Moreover: That's true for every curve C/\mathbb{F}_q and even for every variety

V/\mathbb{F}_q . (Weil conjectures, proved by Deligne).

Set $T = \bar{q}^s \Rightarrow \zeta_E(s) = \sum_F (\bar{q}^s) = \frac{1 - a\bar{q}^s + q^{1-2s}}{(1-\bar{q}^s)(1-\bar{q}^{1-s})}$

$\Rightarrow \zeta_E(s) = \zeta_E(1-s)$

$\zeta_E(s) = 0 \Rightarrow 1 - a\bar{q}^s + q^{1-2s} = 0 \Rightarrow q^{2s} - aq^s + q = 0 \Rightarrow$

q^s root of $T^2 - aT + q \Rightarrow |q^s| = \sqrt{q} \Rightarrow \text{Re}(s) = \frac{1}{2} \neq$

Supersingular elliptic curves

$E/\mathbb{F}_q, m \neq 0 (m \neq q) = 1 \Rightarrow \text{deg}[m] = m^2$ i.e. $|\text{Ker}[m]| =$

$= |E[m](\bar{\mathbb{F}}_q)| = m^2.$

Moreover, since $\forall P \in \text{Ker}[m], [m]P = 0 \Rightarrow E[m](\bar{\mathbb{F}}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$

This works for any field K .

Now, what about $m=p$?

Prop: one of the following is true:

a) $E[p^e] = \{0\} \quad \forall e \geq 1$

b) $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \quad \forall e \geq 1.$

Proof: ϕ Frobenius, $\text{deg}(\phi) = \text{deg}(\phi^*) = p$ and ϕ is totally inseparable.

$\Rightarrow |E[p^e]| = \text{deg}_s [p^e] = \text{deg}_s (\phi \circ \phi^*)^e = \text{deg}_s (\phi^*)^e$ since $\text{deg}_s \phi = 1.$

So, if ϕ^* is separable $\Rightarrow |E[p^e]| = 1$

if not, $\text{deg}_s(\phi^*) \Rightarrow |E[p^e]| = p^e.$

" $\text{deg}_s(\phi^*)$

" $\text{deg}(\phi^*) = p$

Def: E/\mathbb{F}_p . If $|E[p^e]| = 1 \forall e \geq 1$ we say that E is supersingular. Otherwise E is ordinary.

→ sil V.3.
Thm: Let E/K be an elliptic curve K field of charact. p . Then,

TFAE.

- a) E is supersingular
- b) $j(E) \in \mathbb{F}_{p^2}$
- c) $\text{End}(E)$ is non-commutative

Def: If a), b) c) holds we say that E has Hasse-invariant 0, otherwise Hasse invariant 1.

Thm (V.4.1). sil. E/\mathbb{F}_p elliptic curve, $p \geq 3$ $E: y^2 = f(x)$.

$\Rightarrow E$ is supersingular \Leftrightarrow the coeff of x^{p-1} in $f(x)^{\frac{p-1}{2}}$ is 0.

e.g. For which $p \geq 3$, $E: y^2 = x^3 + x$ is ss?

$$(x^3 + x)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} \cdot (x^2 + 1)^{\frac{p-1}{2}}$$

$$(x^3 + 1)^{\frac{p-1}{2}} = \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{2j}$$

\Rightarrow look at coeff of $x^{\frac{p-1}{2}}$ in $2j = \frac{p-1}{2} \Leftrightarrow 4j = p-1$
 $\Leftrightarrow p \equiv 1 \pmod{4}$.

in which case is $j = \frac{p-1}{4}$, $\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \not\equiv 0 \pmod{p}$.

($p \geq 5$)

Cor: # ss curves in \mathbb{F}_q up to \mathbb{F}_q -iso:

$$\lfloor \frac{p}{12} \rfloor + \begin{cases} 0 & p \equiv 1 \pmod{12} \\ 1 & p \equiv 5 \pmod{12} \\ 1 & p \equiv 7 \pmod{12} \\ 2 & p \equiv 11 \pmod{12} \end{cases}$$

e.g. $\begin{pmatrix} 6 \\ 3 \end{pmatrix}$

$p =$

3