Elliptic curves over finite fields

① More on isogenies

Prop (Sil. Chap II). Let C_1, C_2 be curves$/K$ and $\phi: C_1 \to C_2$ a morphism
$\Rightarrow \exists C$, curve; φ_s, separable morphism and φ_i, totally inseparable (or $=$ id).
morphism s.t.

$$\begin{tikzcd} \varphi: C_1 \arrow[rr] \arrow[dr, "\varphi_i"'] & & C_2 \\ & C \arrow[ur, "\varphi_s"'] & \end{tikzcd}$$

$\deg_s \varphi = \deg_s(\varphi_s)$
$\deg_i \varphi = \deg(\varphi_i)$
$\Rightarrow \deg(\varphi) = \deg_i(\varphi)\deg_s(\varphi)$

Obs: If φ separable $\Rightarrow \varphi = \varphi_s$
if φ is totally inseparable $\Rightarrow \varphi = \varphi_i$.

ϕ unramified $\Leftrightarrow \# \phi^{-1}(Q) = \deg(\phi)$

Prop (2.7, Sil II) $\phi: C_1 \to C_2$, $\# \phi^{-1}(Q) = \deg_s(\phi)$.
Moreover, for all but finitely many $Q \in C_2$,

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

Prop (Silv. III, 5.5) $E/\mathbb{F}_q$, $\phi: E \to E$ q-Frobenius, $n, m \in \mathbb{Z}$.
Then, $m + n\phi : E \to E$ is separable $\Leftrightarrow p \nmid m$.
In particular, $\phi - 1$ is separable.

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

$E/\mathbb{F}_q$: $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$, $a_i \in \mathbb{F}_q$.

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

$\Rightarrow \# E(\mathbb{F}_q) \leq 2q + 1$.
$\uparrow$ 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 $\phi: C_1 \to C_2$ a morphism
$\Rightarrow \exists\, C$, curve; φ_s, separable morphism and φ_i, totally inseparable (or $=$ id) morphism s.t.

$$\begin{tikzcd} \varphi: C_1 \arrow[r] \arrow[dr, "\varphi_i"'] & C_2 \\ & C \arrow[u, "\varphi_s"'] \end{tikzcd}$$

$\deg_s \varphi = \deg_s(\varphi_s)$

$\deg_i \varphi = \deg(\varphi_i)$

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

Obs: If φ separable $\Rightarrow \varphi = \varphi_s$

if φ is totally inseparable $\Rightarrow \varphi = \varphi_i$.

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

$\# \phi^{-1}(Q) = \deg_s(\phi)$.

Moreover, for all but finitely many $Q \in C_2$,

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

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

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

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

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

$E/\mathbb{F}_q : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$, $a_i \in \mathbb{F}_q$.

$(x,y) \in \mathbb{F}_q^2$, 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, ~~$\#E(\mathbb{F}_q)$~~.

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

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

Thm: $E/\mathbb{F}_q$ elliptic curve. Let $\phi: E \to E$ 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) $\underbrace{\phi^2 - a\phi + q}_{=0}$ in $\mathrm{End}(E)$

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

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

$1-aT+qT = (1-\alpha T)(1-\beta T)$, $|\alpha| = |\beta| = \sqrt{q}$.

Moreover, $Z_E(1/qT) = Z_E(T)$ and

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).

$\underline{\text{Set}}$ $T = q^{-s} \Rightarrow \zeta_E(s) = Z_E(q^{-s}) = \dfrac{1 - a q^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$

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

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

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

- $\underline{\text{Supersingular elliptic curves}}$

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

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

This works for any field K.

Now, what about $m = p$?

$\underline{\text{Prop}}$: one of the following is true:

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

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

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

$\Rightarrow |E[p^e]| = \deg_s[p^e] = \deg_s(\phi \circ \phi^*)^e = \deg_s(\phi^*)^e$ since $\deg_s \phi = 1$.

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

if not, $\deg_s(\phi^*) \Rightarrow |E[p^e]| = p^e$.

$\qquad \| $

$\deg_i(\phi^*)$

$\qquad \|$

$\deg(\phi^*) = p$

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

$\to$ Sil V.3.

Thm: Let E/K be an elliptic curve K field of charact. p. Then, TFSAE.

a) E is supersingular

b) $j(E) \in \mathbb{F}_{p^2}$

c) End(E) is non-commutative

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

Thm (Sil. V.4.1). $E/\mathbb{F}_p$ 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?

$$(x^3+x)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} \cdot (x^2+1)^{\frac{p-1}{2}} \Rightarrow \text{look at coeff of } x^{\frac{p-1}{2}} \text{ in}$$

$$(x^2+1)^{\frac{p-1}{2}} = \sum_{j=0}^{\frac{p-1}{2}} (x^2)^j \binom{\frac{p-1}{2}}{j} \qquad 2j = \frac{p-1}{2} \Leftrightarrow 4j = p-1$$

$\Leftrightarrow p \equiv 1 \bmod 4$.

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

($p \geq 5$)

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

$$\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & p \equiv 1 \ (12) \\ 1 & p \equiv 5 \ (12) \\ 1 & p \equiv 7 \ (12) \\ 2 & p \equiv 11 \ (12). \end{cases}$$

ej: $\binom{6}{3}$

$p =$