24.02.2022.

- Endomorphisms: Frobenius endomorphism.
- Supersingular and ordinary curves
- Computing a short basis of the eigenvalue for GLV with Ben Smith technique
- Implementing GLV in Sage Math.

Supersingular and ordinary curves.

Let $E: y^2 = x^3 + Ax + B$ be an elliptic curve defined over a field $\mathbb{F}_q$.

Hasse's theorem says that

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

Definition. Let the TRACE be

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

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

Definition. A SUPERSINGULAR CURVE is such that

$\#E(\mathbb{F}_q) \equiv 0 \mod p$, where p is the characteristic of q: $q = p^n$.

Theorem 4.3 p 98 (Waterhouse 1969) tells us what are the possibilities for t.

- either $\gcd(t, p) = 1$ and the curve is ORDINARY
- or p divides t and only few cases can happen:
  - $t = 0$ for odd n : $\#E(\mathbb{F}_p) = p+1$ for $y^2 = x^3 + x / \mathbb{F}_p$, $p \equiv 3 \mod 4$, $p \geq 5$.
  - $t = 0$ for even n and $p \not\equiv 1 \mod 4$
  - n is even, $p \not\equiv 1 \mod 3$, and $t = \pm\sqrt{q}$
  - n is even and $t = \pm 2\sqrt{q}$: $(p+1)^2 = p^2+1+2p$ for example, $= \#E(\mathbb{F}_{p^2})$ for $y^2 = x^3 + x$
  - small char: $p = 2$, $p = 3$.

$\rightsquigarrow$ "Is the curve supersingular" in the hardware: is the trace $0 \mod p$?

Frobenius map 4.2.

Endomorphism of the curve. $E: y^2 = x^3 + Ax + B \,/\, \mathbb{F}_q$, $A, B \in \mathbb{F}_q$, $q = p^n$.

(also noted ϕ_q) $\pi_q : E \longrightarrow E$

$(x,y) \longmapsto (x^q, y^q)$

non-separable endomorphism of degree q. (lemma 4.6).

lemma 4.5 p99

1) $\phi_q(x,y) \in E(\overline{\mathbb{F}}_q)$ relies on the fact that $(x_1+x_2)^q = x_1^q + x_2^q$ in $\mathbb{F}_q$

2) $(x,y) \in E(\mathbb{F}_q)$ iff $\pi_q(x,y) = (x,y)$.

→ $x \in \mathbb{F}_q \iff x^q = x$ (for any finite field $\mathbb{F}_q$)

then $(x,y) \in E(\mathbb{F}_q)$ for $(x,y) \in E(\overline{\mathbb{F}}_q)$

$\iff x \in \mathbb{F}_q$ and $y \in \mathbb{F}_q$

so we need $\phi_q(x) = x$ and $\phi_q(y) = y$ ($x^q = x$ and $y^q = y$)

$\iff \phi_q(x,y) = (x,y)$.

PROPOSITION 4.7.

$E / \mathbb{F}_q$, $n \geq 1$. apply ϕ_q n-times: $\underbrace{\phi_q \circ \phi_q \circ \dots \circ \phi_q}_{n \text{ times}}$

1. $\mathrm{Ker}(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$
2. $\phi_q^n - 1$ is a separable endomorphism, so $\# E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$

PROOF of HASSE theorem uses:

$$t = q + 1 - \# E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1) \qquad (4.1)$$

shows that $|t| \leq 2\sqrt{q}$.

THEOREM 4.10.

$E / \mathbb{F}_q$, t in (4.1)

$$\phi_q^2 - t\,\phi_q + q = 0.$$

as endomorphisms of E, and t is the unique integer a' such that

$$\phi_q^2 - a'\phi_q + q = 0.$$

$$(x^{q^2}, y^{q^2}) - \underbrace{a'}_{t \text{ is the only one}} (x^q, y^q) + [q](x,y) = 0$$

$t \equiv \mathrm{Trace}((\phi_q)_m) \bmod m$ for all m with $\gcd(m,q) = 1$.