01 03 . 2022.

Aim: the paper of Ben Smith on Easy Scalar decompositions for efficient scalar multiplicatio on elliptic curves.

Scalar multiplication in Schnorr:

$\boxed{\text{Group structure}}$ $E(\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $m \mid n$ and $m \mid p-1$.
$m \mid \gcd(n, p-1)$.

Endomorphism ring structure.

<u>Theorem</u> for every ϕ in $\mathrm{End}(\mathcal{E})$ (endomorphism) there is a trace t_ϕ in $\mathbb{Z}$ with $t_\phi^2 < 4 \deg \phi$ such that

$$\phi^2 - t_\phi \cdot \phi + [\deg \phi] = 0 \text{ in } \mathrm{End}(\mathcal{E});$$

every endomorphism satisfies a quadratic integer equation.

ϕ is a "root" of the characteristic polynomial

$$\chi_\phi(X) = X^2 - t_\phi X + \deg(\phi)$$

the other root $\hat{\phi}$ is $[t_\phi] - \phi$.

Deuring's theorem showed that $\mathrm{End}(\mathcal{E})$ has one of these three forms:

- $\mathrm{End}(\mathcal{E}) \cong \mathbb{Z}$
- $\mathrm{End}(\mathcal{E}) \cong$ an order in a quadratic imaginary field (Complex Multiplication)
  → an order in $\mathbb{Q}[\sqrt{-d}]$ for $d > 1$.
- $\mathrm{End}(\mathcal{E}) \cong$ an order in a quaternion algebra: $1, i, j, k$ are quaternions, non-commutative.

Proposition 3.16: $\deg(a\alpha + b\beta) = a^2 \deg\alpha + b^2 \deg\beta + ab(\deg(\alpha+\beta) - \deg\alpha - \deg\beta)$.
α, β endomorphisms,
$a, b \in \mathbb{Z}$.

Frobenius endomorphism: characteristic polynomial

$\phi_q = \pi_q$, $\chi_q = X^2 - tX + q$

discriminant: $t^2 - 4q < 0$ by Hasse's theorem,

$t^2 - 4q = -Dy^2$ where D is square-free.

the roots are: $\dfrac{t + y\sqrt{-D}}{2}$, $\dfrac{t - y\sqrt{-D}}{2}$ $(D > 0)$.

Order of a number field. (of the ring of integers of a (quadratic) number field).

$\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}(i)$ is a number field. (quadratic)

$\mathbb{Q}[X]/(X^2+X+1) \cong \mathbb{Q}(\omega)$ is a quadratic number field.

$\mathbb{Z}[i]$ is the ring of integers (Gaussian integers) of $\mathbb{Q}(i)$, that is

$\{a+ib : a, b \in \mathbb{Z},\ i^2 = -1\}$.

$\mathrm{Norm}(a+ib) = a^2+b^2$.

$\mathbb{Z}[\omega]$, $\omega = \dfrac{-1+i\sqrt{3}}{2}$ is the ring of integers (Eisenstein integers) of $\mathbb{Q}(\omega)$,

$\{a + \omega b,\ a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\}$.

$\mathrm{Norm}(a+b\omega) = a^2 - ab + b^2$

there is a denominator 2 for ω, but it is algebraic because it is a root of a monic polynomial of integer coefficients.

For $d > 0$, square-free, $d \equiv 3 \bmod 4$, $X^2 + X + \underbrace{\frac{1+d}{4}}_{\in \mathbb{Z}}$ has roots $\dfrac{-1 \pm \sqrt{-d}}{2}$.

in the other cases, $X^2 + d$ has roots $\pm\sqrt{-d}$.

An ORDER is a subring $\mathcal{O}$ of a ring A,

- A is a finite-dimensional algebra (vector space with multiplication) over the field $\mathbb{Q}$
- $\mathcal{O}$ spans A over $\mathbb{Q}$ ($\mathcal{O}$ engendre A sur $\mathbb{Q}$ → si on passe des coefs entiers à rationels, on obtient tout A)
- $\mathcal{O}$ is a $\mathbb{Z}$-lattice in A.

multiplication is: $(a+ib)(a'+ib') = aa' - bb' + (ab' + a'b)i$.

subring of $\mathbb{Z}[i]$: can be with even coefficients a, b.

→ $(2a+2bi) + (2a'+2b'i) = 2(a+a') + 2(b+b')i \in (2\mathbb{Z} + 2i\mathbb{Z})$.

$(2a+2bi)(2a'+2b'i) = 4(aa'-bb' + (ab'+a'b)i)$.

$2i$: $(x-2i)(x+2i) = x^2+4$. $\Delta' = -16$ $\Delta(x^2+1) = -4$.

conductor 2. $\Delta'/\Delta = -16/-4 = 4 = 2^2$. conductor is 2.

LEMMA 1.

Let ϕ, ψ be endomorphisms of $\mathcal{E}$ defined over $\mathbb{F}_q$ such that
$\mathbb{Z}[\phi]$ and $\mathbb{Z}[\psi]$ are quadratic rings and $\mathbb{Z}[\phi] \subseteq \mathbb{Z}[\psi]$,
so $\phi = c\psi + b$ for some integers b and c.

Let $G \subset \mathcal{E}$ be a cyclic subgroup of order N such that
$\phi(G) \subseteq G$ and $\psi(G) \subseteq G$, and let λ and μ be the eigenvalues in $\mathbb{Z}/N\mathbb{Z}$ of ϕ and ψ on G, respectively. Then

$$\lambda - c\mu - b \equiv 0 \mod N \quad \text{and}$$

$$\lambda\mu - t_\psi \lambda - b\mu + c \cdot \deg(\psi) + b\, t_\psi \equiv 0 \mod N.$$

PROOF.

Let K be a quadratic field (real or imaginary) with maximal order $\mathcal{O}_K$ and discriminant Δ_K.
If ϕ is an element of $\mathcal{O}_K$ then we write t_ϕ for its trace, n_ϕ for its norm.
If ϕ is not in $\mathbb{Z}$, then it generates an order $\mathbb{Z}[\phi]$ in $\mathcal{O}_K$, we write $\Delta(\phi) = t_\phi^2 - 4n_\phi$ for the discriminant of $\mathbb{Z}[\phi]$, and $P_\phi(T) = T^2 - t_\phi T + n_\phi$ the minimal polynomial of ϕ.
The discriminants of $\mathcal{O}_K$ and $\mathbb{Z}[\phi]$ are related by $\Delta(\phi) = c_\phi^2 \Delta_K$ for some positive integer c_ϕ, the conductor of $\mathbb{Z}[\phi]$ in $\mathcal{O}_K$.

$\mathbb{Z}[\phi] \subset \mathbb{Z}[\psi]$ iff c_ϕ divides c_ψ.

if $\mathbb{Z}[\phi] \subset \mathbb{Z}[\psi]$ are orders in K, then neccessarily

$$(1) \qquad \phi = c\psi + b \qquad \text{for some integers b and c.}$$

it follows that (2) $\quad b = \frac{1}{2}(t_\phi - c\, t_\psi)$ and $c^2 = \dfrac{\Delta(\phi)}{\Delta(\psi)}$

c is (up to sign) the relative conductor of $\mathbb{Z}[\phi]$ in $\mathbb{Z}[\psi]$.

Multiply (1) by $t_\psi - \psi$, $\quad (\psi^2 - t_\psi\psi + \underbrace{n_\phi}_{\deg\phi} = 0 \iff (\psi - t_\phi)\psi = -n_\phi \iff t_\phi - \psi = \dfrac{n_\phi}{\psi}$

$$\phi(t_\psi - \psi) = (c\psi + b)(t_\phi - \psi)$$
$$= \phi t_\psi - \phi\psi = c\psi t_\phi - c\psi^2 + bt_\phi - b\psi$$
$$\iff \phi\psi - \phi t_\psi + \underline{c\psi t_\phi - c\psi^2} + bt_\phi - b\psi = 0$$
$$\iff \phi\psi - t_\psi\phi - b\psi + \underbrace{(c\, n_\phi + bt_\phi)}_{\text{integer}} = 0 \qquad (3)$$

$$\psi^2 - t_\phi\psi + n_\phi = 0$$
$$n_\phi = -\psi^2 + t_\phi\psi$$

replace ϕ by λ mod N and ψ by μ mod N in (1): $\lambda - c\mu - b = 0 \mod N$

in (3): $\lambda\mu - t_\psi\lambda - b\mu + c\deg\phi + bt_\phi = 0 \mod N$

Now, replace ϕ by the Frobenius endomorphism of eigenvalue $\lambda = 1$ over $\mathbb{F}_q$:

$$\phi_q(E(\mathbb{F}_q)) = E(\mathbb{F}_q), \quad \lambda_q = 1 \text{ over } E(\mathbb{F}_q).$$

$$t_\phi = t_q \text{ and } \deg(\phi_q) = q.$$

$$\lambda - c\mu - b \equiv 0 \bmod N \longrightarrow \underbrace{\lambda_q}_{=1} - c\mu - b \equiv 0 \bmod N \iff \boxed{(b-1) + c\mu \equiv 0 \bmod N.}$$

$$\lambda\mu - t_\psi\lambda - b\mu + c\deg(\psi) + b\,t_\psi \equiv 0 \bmod N$$

$$\to \lambda_q\mu - t_\psi\lambda_q - b\mu + c\deg(\psi) + b\,t_\psi \equiv 0 \bmod N$$

$$\mu(1-b) + t_\psi(b-1) + c\deg(\psi) \equiv 0 \bmod N$$

$$\boxed{((b-1)t_\psi + c\underbrace{\deg(\psi)}_{=n_\phi}) + (1-b)\mu \equiv 0 \bmod N.}$$

THEOREM 2.

Let ψ be a non-integer endomorphism of $\mathcal{E}$ such that $\mathbb{Z}[\phi_q] \subset \mathbb{Z}[\psi]$, (Frobenius end.)
so $\pi_q = \phi_q = c\,\psi + b$ for some integers c and b.
Suppose we are in the situation of a subgroup G, cyclic of order N, of $\mathcal{E}(\mathbb{F}_q)$, $\psi(G) \subseteq G$,
and ϕ_q is the identity on $E(\mathbb{F}_q)$. the vectors

$$\boxed{\vec{b_1} = (b-1, c) \text{ and } \vec{b_2} = (c\deg\psi + (b-1)t_\psi,\ 1-b)}$$

generate a sublattice of $\mathcal{L}$ of determinant $\# E(\mathbb{F}_q)$.
If $G = E(\mathbb{F}_q)$ (if $E(\mathbb{F}_q)$ is cyclic), then $\mathcal{L} = \langle \vec{b_1}, \vec{b_2} \rangle$

PROOF. $(b-1)\cdot 1 + c\mu \equiv 0 \bmod N$ $\qquad \vec{b_1} = (b-1, c)$

$((b-1)t_\psi + c\,n_\phi)\cdot 1 + (1-b)\mu \equiv 0 \bmod N.$ $\qquad \vec{b_2} = ((b-1)t_\psi + c\,n_\phi,\ 1-b)$

Then, we need to ensure that $\vec{b_1}$ and $\vec{b_2}$ are short.

Choosing b and c.

Consider the curve $E: y^2 = x^3 + ax$ defined over a prime field $\mathbb{F}_p$, $p \equiv 1 \bmod 4$.
($\sqrt{-1} \in \mathbb{F}_p$).

$\psi: (x, y) \mapsto (-x, A \cdot y)$ where $A^2 = -1$ in $\mathbb{F}_p$.

The Frobenius endomorphism satisfies the characteristic polynomial

$$X^2 - tX + q = 0$$

of discriminant $t^2 - 4q = -Dy^2$ where D is square-free.
The two roots are $\frac{t + y\sqrt{-D}}{2}$ and $\frac{t - y\sqrt{-D}}{2}$.

Take the second endomorphism ψ to be the complex multiplication by $\sqrt{-D}$. (or $\frac{-1+\sqrt{-D}}{2}$).

then $\phi_q = \underbrace{\frac{t}{2}}_{b} + \underbrace{\frac{y}{2}}_{c} \psi$.

$$\vec{b}_1 = \left\langle \frac{t}{2} - 1, \frac{y}{2} \right\rangle, \qquad \vec{b}_2 = \left\langle \frac{y}{2} \deg \psi + \left(\frac{t}{2} - 1\right) t_\psi, 1 - \frac{t}{2} \right\rangle$$

Example: $j = 1728$, $D = 1$, the characteristic polynomial of ψ is $\psi^2 + Id = 0$.
$X^2 + 1$ has discriminant -4, $t_\psi = 0$, $\deg(\psi) = 1$ (the point O is the only zero).

$\vec{b}_1 = \left\langle \frac{t}{2} - 1, \frac{y}{2} \right\rangle$ where t is even ($(0,0)$ has order 2) and y is even consequently.

$\vec{b}_2 = \left\langle \frac{y}{2}, 1 - \frac{t}{2} \right\rangle$

Example: $j = 0$, $D = 3$. the characteristic polynomial of $\psi: (x,y) \mapsto (\omega x, y)$ is $\psi^2 + \psi + 1 = 0$.
$X^2 + X + 1$ has discriminant -3, $t_\psi = -1$, $\deg(\psi) = 1$. $\psi = \frac{-1+\sqrt{-3}}{2}$

$\cancel{\vec{b}_1 =}$ $\phi_q = \frac{t + y\sqrt{-3}}{2} = \frac{t+y}{2} + \frac{-y + y\sqrt{-3}}{2} = \frac{t+y}{2} + y\psi$.

$\vec{b}_1 = \left(\frac{t+y}{2} - 1, y \right)$ and $\vec{b}_2 = \left(+y + \left(\frac{t+y}{2} - 1\right)(-1), 1 - \frac{t+y}{2} \right)$

$$\left(\frac{t+y}{2} + 1, 1 - \frac{t+y}{2} \right)$$

homework: find and check $\vec{b}_1$, $\vec{b}_2$ and the eigenvalue μ of ψ,
check that $\vec{b}_1 \cdot \begin{bmatrix} 1 \\ \mu \end{bmatrix} = 0$ and $\vec{b}_2 \cdot \begin{bmatrix} 1 \\ \mu \end{bmatrix} = 0 \bmod \#E(\mathbb{F}_p) = \frac{(t-2)^2 + Dy^2}{4}$

$D \equiv 3 \bmod 4$: $\psi \longleftrightarrow \dfrac{-1+\sqrt{-D}}{2}$ has characteristic polynomial

$$X^2 + X + \frac{D+1}{4} = \left(X - \frac{-1+\sqrt{-D}}{2}\right)\left(X - \frac{-1-\sqrt{-D}}{2}\right)$$

trace $(\psi) = -1$ and $\deg(\psi) = \dfrac{D+1}{4}$ (integer).

Frobenius: $\phi_q \longleftrightarrow \dfrac{t + y\sqrt{-D}}{2} = \dfrac{t+y}{2} + y\left(\dfrac{-1+\sqrt{-D}}{2}\right) = \dfrac{t+y}{2} + y\psi$.

$\phi_q = b + c\psi$ with $b = \dfrac{t+y}{2}$ and $c = y$.

$$\vec{b}_1 = \left(\frac{t+y}{2} - 1, y\right) \qquad \vec{b}_2 = \left(y\frac{D+1}{4} - \frac{t+y}{2}, 1 - \frac{t+y}{2}\right) = \left(\frac{y(D-1)-2t}{4}, 1 - \frac{t+y}{2}\right)$$

$$\mu_- = \frac{-1-(t-2)/y}{2} = -\frac{1}{2} - \frac{t-2}{2y}$$

$$\vec{b}_1 \cdot \begin{bmatrix} 1 \\ \mu_- \end{bmatrix} = \frac{t+y}{2} - 1 + y\left(\frac{-1}{2} - \frac{t-2}{2y}\right) = \frac{t+y-2}{2} + \frac{-y-t+2}{2} = 0.$$

$$\vec{b}_2 \cdot \begin{bmatrix} 1 \\ \mu_- \end{bmatrix} = \frac{y(D-1)-2t}{4} + \left(1 - \frac{t+y}{2}\right)\left(\frac{-y-t+2}{2y}\right)$$

$$= \frac{y^2(D-1)-2ty}{4y} + \frac{-2y-2t+4}{4y} - \frac{(t+y)(-y-t+2)}{4y}$$

$$= \left(y^2(D-1) - 2ty - 2y - 2t + 4 + t^2 + y^2 + 2ty - 2t - 2y\right)/4y$$

$$= \left(t^2 - 4t + 4 + y^2 D\right)/4y$$

$$= \frac{(t-2)^2 + Dy^2}{4y} \equiv 0 \bmod (t-2)^2 + Dy^2 \quad \square.$$

$D \not\equiv 3 \bmod 4$: $\psi \longleftrightarrow \sqrt{-D}$ has characteristic polynomial

$$X^2 + D = (X - \sqrt{-D})(X + \sqrt{-D}) \qquad \text{Trace}(\psi) = 0 \text{ and } \deg(\psi) = D.$$

Frobenius: $\phi_q \longleftrightarrow \dfrac{t + y\sqrt{-D}}{2} = \dfrac{t}{2} + \dfrac{y}{2}\sqrt{-D} = \underbrace{\dfrac{t}{2}}_{b} + \underbrace{\dfrac{y}{2}}_{c}\psi$.

$$\vec{b}_1 = \left(\frac{t}{2} - 1, \frac{y}{2}\right) \qquad \vec{b}_2 = \left(\frac{y}{2}D, 1 - \frac{t}{2}\right) \qquad \mu_- = -\frac{t-2}{y}$$

$$\vec{b}_1 \cdot \begin{bmatrix} 1 \\ \mu_- \end{bmatrix} = \frac{t-2}{2} + \frac{y}{2} \cdot \frac{-(t-2)}{y} = 0, \quad \vec{b}_2 \cdot \begin{bmatrix} 1 \\ \mu_- \end{bmatrix} = \frac{y}{2}D + \left(\frac{2-t}{2}\right)\left(\frac{-t+2}{y}\right) = \frac{Dy^2 + (t-2)^2}{2y} \equiv 0 \bmod r$$