GLV endomorphism and multi-scalar multiplication.

def multi-scalar:
  inputs P, Q, a_1, a_2 scalars.
  output: $a_1 P + a_2 Q$

Write a_1 in bits: $a_1 = \sum_{i=0}^{n} b_i 2^i$, $a_2 = \sum_{i=0}^{n'} b_i' 2^i$

$\begin{array}{ccccc} 4&3&2&1&0 \\ 1&0&0&1&1 \end{array}$ $\begin{array}{cccccc} 5&4&3&2&1&0 \\ 1&0&0&0&1&1 \end{array}$

Precompute $R = P + Q$.

if $n > n'$:
  $S \leftarrow P$
elif $n < n'$:
  $S \leftarrow Q$
else:
  $S \leftarrow R$

For $i = \max(n, n') - 1$ downto 0 do
  $S \leftarrow 2S$
  if $b_i = 1$ and $b_i' = 1$
    $S \leftarrow S + R$
  elif $b_i = 1$
    $S \leftarrow S + P$
  elif $b_i' = 1$
    $S \leftarrow S + Q$
return S

example: $19P + 35Q$

$i=5$ $S \leftarrow Q$
$i=4$ $S \leftarrow 2S + P$ $= 2Q + P$
$i=3$ $S \leftarrow 2S$ $= 4Q + 2P$
$i=2$ $S \leftarrow 2S$ $= 8Q + 4P$
$i=1$ $S \leftarrow 2S + R$ $= 16Q + 8P + P + Q$
$= 17Q + 9P$
$i=0$ $S \leftarrow 2S + P$ $= 34Q + 18P + P =$
$34Q + 19P$

Complexity: in terms of $n = \log_2 a_1$ and $n' = \log_2 a_2$, what does it cost in terms of doublings and additions:

- what is the length of the for loop?
- in average, if the bits b_i, b_i' are random, with wich proportion does the alg do an addition?

(a) $\max(\log_2 n, \log_2 n')$

(b) $p = 3/4$. there is no addition if $b_i = b_i' = 0$.
  if $p(b_i = 1) = p(b_i = 0) = 1/2$ and $p(b_i' = 0) = p(b_i' = 1) = 1/2$,

$p(b_i = 0 \ \& \ b_i' = 0) = \frac{1}{2} \cdot \frac{1}{2}$ because of independence
$p(b_i = 1 \ \& \ b_i' = 0) = 1/4$
$p(b_i = 0 \ \& \ b_i' = 1) = 1/4$
$p(b_i = 1 \ \& \ b_i' = 1) = 1/4$.

$3/4$ addition, $1/4$ no addition.

Exercice: compute $\overset{100100}{36}P + \overset{10101}{21}Q$ with multi-scalar mult. How many doublings and add?

$p = 2^{255} - 19$, $p \equiv 1 \bmod 4$, then $(-1)^{\frac{p-1}{2}} = (-1)^2 = 1$ and -1 is a square mod p.

Let $i \in \mathbb{F}_p$ s.t. $i^2 = -1 \bmod p$.

We know that $p = \frac{t^2 + Dy^2}{4} = \left(\frac{t}{2}\right)^2 + \left(\frac{y}{2}\right)^2$ here, so $u = \frac{t}{2}$ and $v = \frac{y}{2}$

and $p = u^2 + v^2$.

a square root of -1 is $\frac{u}{v}$ mod p.

Modulo r: let r be a <u>prime</u> divisor of $p+1-t$.

$p+1-t = \frac{(t-2)^2 + Dy^2}{4} = \left(\frac{t-2}{2}\right)^2 + \left(\frac{y}{2}\right)^2 \to u = \frac{t-2}{2}$, $v = \frac{y}{2}$

$u^2 + v^2 = 0 \bmod r_0$

We have k random, λ eigenvalue mod r_0 prime, $\lambda = \pm\frac{u}{v}$ mod r_0 and u, v short.

Decompose $k = k_0 + k_1 \lambda \bmod r_0$, and k_1, k_2 are short.

Let $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(i, j) \longmapsto i + \lambda j$.

$f(-u, v) = -u + \lambda v = 0$. $\qquad \lambda = \frac{u}{v} \iff v\lambda - u = 0$

$f(v, u) = v + \lambda u = v\left(1 + \lambda \frac{u}{v}\right) = v(1 + \lambda^2) = v \cdot 0 = 0$.

$\to (-u, v)$ and (v, u) is a basis. $\quad (u_0, u_1)$, (v_0, v_1) in general.

Decompose $(k_1, 0)$ over (u_0, u_1), (v_0, v_1).

$$\beta_1 (u_0, u_1) + \delta_2 (v_0, v_1) = (\beta_1 u_0 + \delta_2 v_0, \beta_1 u_1 + \delta_2 v_1) = (k, 0)$$

$\beta_1, \delta_2 \in \mathbb{Q}$.

Now, round β_1, δ_2: $\underbrace{\lfloor \beta_1 \rceil}_{b_1} (u_0, u_1) + \underbrace{\lfloor \delta_2 \rceil}_{b_2} (v_0, v_1)$ is "close to" $(k, 0)$

the error term $\vec{e} = b_1 (u_0, u_1) + b_2 (v_0, v_1)$ will be short.

by construction, $f(\vec{e}) = 0$ because it is a linear combination of $\vec{u}, \vec{v}$ t.q. $f(\vec{u}) = 0$, $f(\vec{v}) = 0$.

so $f(\vec{e}) = 0$.

Find b_1, b_2. $\begin{cases} \beta_1 u_0 + \delta_2 v_0 = k \\ \beta_1 u_1 + \delta_2 v_1 = 0 \end{cases}$ $\quad \beta_1 u_0 + (-\beta_1) u_1 / v_1 \; v_0 = k$. (*)

$\to \delta_2 = -\beta_1 u_1 / v_1$

(*) $\beta_1 \left(u_0 - u_1 \frac{v_0}{v_1}\right) = k$. $\quad \beta_1 = k \frac{v_1}{u_0 v_1 - u_1 v_0}$ $\qquad b_1 = \left\lfloor k \frac{v_1}{u_0 v_1 - u_1 v_0} \right\rceil$

$\delta_2 = -\beta_1 \frac{u_1}{v_1} = -k \cdot \frac{\cancel{v_1}}{u_0 v_1 - u_1 v_0} \frac{u_1}{\cancel{v_1}} = \frac{-k u_1}{u_0 v_1 - u_1 v_0}$

$b_2 = \left\lfloor \frac{-k u_1}{u_0 v_1 - u_1 v_0} \right\rceil$ $\qquad \vec{v} = b_1 (u_0, u_1) + b_2 (v_0, v_1)$

$$\vec{V} = (\underbrace{b_1 u_0 + b_2 v_0}_{v'_0}, \underbrace{b_1 u_1 + b_2 v_1}_{v'_1})$$

and

$$v'_0 + \lambda v'_1 = 0 \mod r_0 .$$

$$(k, 0) - \vec{v} = (k - v'_0, - v'_1) = (k_0, k_1) \text{ and } k_0 + k_1 \lambda = 0 \mod r_0 .$$

Finally, it costs:

- a precomputation of a basis of short vectors (with short coefficients)

$$u_0 + \lambda u_1 = 0 \mod r$$
$$v_0 + \lambda v_1 = 0 \mod r.$$

then, $b_1 = \left\lfloor \dfrac{k v_1}{u_0 v_1 - u_1 v_0} \right\rceil$, $b_2 = \left\lfloor \dfrac{-k u_1}{u_0 v_1 - u_1 v_0} \right\rceil$

$$(k_1, k_2) = (k - (b_1 u_0 + b_2 v_0), -(b_1 u_1 + b_2 v_1)) .$$

Exercices.

2.13. (a). Legendre form: $y^2 = x(x-1)(x-\lambda)$ into Weierstraß form: $(\lambda \neq 0, 1)$

$$y^2 = (x^2-x)(x-\lambda) = x^3 - x^2 - \lambda x^2 + x\lambda = x^3 - (1+\lambda)x^2 + \lambda x$$

$$x \mapsto x - \frac{1+\lambda}{3} : \quad \left(x - \frac{1+\lambda}{3}\right)^3 = x^3 - (1+\lambda)x^2 + \frac{(1+\lambda)^2}{3}x - \frac{(1+\lambda)^3}{27}$$

$$y^2 = \left(x - \frac{1+\lambda}{3}\right)^3 + \left(\lambda - \frac{(1+\lambda)^2}{3}\right)x + \frac{(1+\lambda)^3}{27}$$

$$= \left(x - \frac{1+\lambda}{3}\right)^3 + \left(\lambda - \frac{(1+\lambda)^2}{3}\right)\left(x - \frac{1+\lambda}{3}\right) + \frac{(1+\lambda)^3}{27} + \lambda\frac{1+\lambda}{3} - \frac{(1+\lambda)^3}{9}$$

$$= \left(x - \frac{1+\lambda}{3}\right)^3 + \underbrace{\left(\lambda - \frac{(1+\lambda)^2}{3}\right)}_{A}\left(x - \frac{1+\lambda}{3}\right) + \underbrace{\frac{-2l^3+3l^2+3l-2}{27}}_{= -\frac{(l-2)(2l-1)(l+1)}{3^3}}$$

$$\underbrace{-\frac{(l-2)(2l-1)(l+1)}{3^3}}_{B}$$

With SageMath one checks that:

$$j = 1728\frac{4A^3}{4A^3+27B^2} = 256 \cdot \frac{(l^2-l+1)^3}{(l(l-1))^2}$$

(b) $j = 256\dfrac{(l^2-l+1)^3}{l^2(l-1)^2}$ ~~$\Leftrightarrow$~~, $S = 256(l^2-l+1)^3 - j(l^2)(l-1)^2 = 0$.

if j is a parameter, what are the roots?

$$\text{Resultant}(S_j(l), S_j'(l)) = \underbrace{d}_{\text{some integer}} \cdot (j-1728)^3 j^4$$

$\Rightarrow$ when $j \neq 0, 1728$, the roots are distinct.

We can then check with sageMath that replacing l by $1/l$, $1-l$, etc satisfies j.

(c) $j = 1728$: $\quad 256(l^2-l+1)^3 - 1728\, l^2(l-1)^2 = 0$

roots are $l = 2$ with multiplicity 2,
$l = 1/2$ ——————— 2,
$l = -1$ ——————— 2.

$j = 0$: $\quad 256(l^2-l+1)^3 = 0 \Rightarrow l^2 - l + 1 = 0$ if $\frac{+1+i\sqrt{3}}{2} \in K$, then the solutions are $l = \frac{1 \pm i\sqrt{3}}{2}$.

Exercices.

2.19. $\alpha(x,y) = \left(\dfrac{p(x)}{q(x)}, \; y\dfrac{s(x)}{t(x)}\right)$ endomorphism on $\mathcal{E}$: $y^2 = x^3+ax+b$.

p, q have no common root, s, t have no common roots. p, q, s, t polynomials

(a) $\alpha(x,y) \in \mathcal{E}$: $y^2 \dfrac{s^2(x)}{t^2(x)} = \left(\dfrac{p(x)}{q(x)}\right)^3 + a\dfrac{p(x)}{q(x)} + b$

replace y^2 by x^3+Ax+b:

$$(x^3+ax+b)\frac{s^2(x)}{t^2(x)} = \frac{\overbrace{p^3(x) + a\,p(x)\cdot q^2(x) + b\,q^3(x)}^{\text{this is } u(x)}}{q^3(x)}$$

(*) $u(x) \mod q(x) = p^3(x)$ hence a common root of $q(x)$ and $u(x)$ is also a root of $p(x)$,
in other words,
Let x_0 a root of $q(x)$, then $u(x_0) = p^3(x_0) + a\,p(x_0)\underbrace{q^2(x_0)}_{=0} + b\underbrace{q^3(x_0)}_{=0}$
$= p^3(x_0)$

but we assumed that p and q do not share a common root,
hence $u(x)$ and $q(x)$ do not share a common root.

(b) $t(x_0) = 0$. t and s do not share a root so $s^2(x_0) \neq 0$.

$$\frac{t(x_0)^2}{(x^3+Ax+B)\,s(x_0)^2} = \frac{q^3(x_0)}{u(x_0)}$$

17.02.2022

exercice 2.23. $\mathcal{E}: y^2 = x^3 + \overset{A}{a}x + \overset{B}{b}$, $\mathcal{E}^d : y^2 = x^3 + Ad^2x + Bd^3$.

(a) $j(\mathcal{E}^d) = 1728 \dfrac{4(Ad^2)^3}{4(Ad^2)^3 + 27(Bd^3)^2} = 1728 \dfrac{4\ A^3 \cdot d^6}{4A^3d^6 + 27B^2d^6} = 1728 \dfrac{4a^3}{4a^3+27b^2} = j(\mathcal{E}$

$j(\mathcal{E}^d) = j(\mathcal{E})$

(b) let $\sqrt{d}$ be a square root of d, either in K or in a quadratic extension.

then $\mathcal{E}$ multiplied by $d^3 = (\sqrt{d})^6$ gives

$$d^3y^2 = d^3x^3 + Ad^2\,dx + bd^3$$

$$\Leftrightarrow \quad (d\sqrt{d}\,y)^2 = (dx) + Ad^2(dx) + bd^3 \quad : \mathcal{E}^{(d)}$$

$(x,y) \longmapsto (dx, d\sqrt{d}\,y) \in \mathcal{E}^d$ is defined in $K(\sqrt{d})$.

(c) $\mathcal{E}^d : y^2 = x^3 + Ad^2x + Bd^3$

divides by d^3: $\quad \dfrac{dy^2}{d^4} = \left(\dfrac{x}{d}\right)^3 + A\,\dfrac{x}{d} + B$

$(x,y) \in \mathcal{E}^d \longmapsto (x/d,\ y/d^2) \in \quad dy^2 = x^3 + Ax + B.$

07.02.2022.

Morphisms: $\mathcal{E}_1 : y_1^2 = x_1^3 + a_1 x_1 + b_1$, $\mathcal{E}_2 : y_2^2 = x_2^3 + a_2 x_2 + b_2$

are two elliptic curves defined over a field K.

A morphism $\phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ is a mapping

$$\phi : (x_1, y_1) \longmapsto (\phi_x(x_1, y_1), \ \phi_y(x_1, y_1))$$

where ϕ_x and ϕ_y satisfy the equation of $\mathcal{E}_2$:

$$\phi_y^2 = (\phi_x)^3 + a_2 \phi_x + b_2$$

and ϕ_x, ϕ_y are in the function field of $\mathcal{E}_1$: $\overline{K}(\mathcal{E}_1)$

where $\overline{K}$ denotes the algebraic closure: it means for us that while $\mathcal{E}_1$ and $\mathcal{E}_2$ are defined over K, ϕ_x and ϕ_y can have coefficients in an extension of K.

K-morphisms, L-morphisms : morphisms ϕ with $\phi_x, \phi_y \in K(\mathcal{E}_1)$, resp. morphisms ϕ with $\phi_x, \phi_y \in L(\mathcal{E}_1)$ where L is an extension of K, for example $\mathbb{F}_{q^2}$ is an extension of $\mathbb{F}_q$, $\mathbb{Q}(i)$ is an extension of $\mathbb{Q}$ with $i^2 = -1$.

Homomorphisms : morphisms respecting the group law

Isomorphisms : invertible homomorphisms

Endomorphisms : homomorphisms from a curve to itself

Automorphisms : invertible endomorphisms.

there is also:

Epimorphism: surjective homomorphism, $\forall Q \in \mathcal{E}_2, \ \exists P \in \mathcal{E}_1, \ \phi(P) = Q$ i.e. there is always a preimage.

Monomorphism: injective homomorphism: $\phi(P_1) = \phi(P_2) \Rightarrow P_1 = P_2$
i.e. an injection maps distinct points to distinct images.

The degree of an K-morphism $\phi : \mathcal{E}_1 \to \mathcal{E}_2$ can be expressed in terms of the degree of extension of the corresponding function fields:

$$\phi : (x_1, y_1) \in \mathcal{E}_1(K) \longmapsto (\phi_x(x_1, y_1), \ \phi_y(x_1, y_1)) \in \mathcal{E}_2(K)$$

induces an extension of function fields:

a function in $K(\mathcal{E}_2)$ is of the form $f(x_2, y_2)$, then we can express it in $K(\mathcal{E}_1)$ thanks to $(x_2, y_2) = (\phi_x(x_1, y_1), \ \phi_y(x_1, y_1))$: this becomes

$$f(\phi_x(x_1, y_1), \phi_y(x_1, y_1)) \in K(\mathcal{E}_1).$$

and $\deg \phi$ = degree of the induced extension of fields:

$$\deg \phi = [K(\mathcal{E}_1) : K(\mathcal{E}_2)].$$

Operations on morphisms:

- one can compose homomorphisms $\phi_1 : \mathcal{E}_1 \to \mathcal{E}_2$ and $\phi_2 : \mathcal{E}_2 \to \mathcal{E}_3$
- we can also add homomorphisms $\phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ and $\psi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$

$$(\phi +_1 \psi)(P) = \phi(P) +_2 \psi(P)$$

addition on $\mathcal{E}_1$ ↗ ↖ addition on $\mathcal{E}_2$

- Automorphisms of $\mathcal{E}$ form a group $\mathrm{Aut}(\mathcal{E})$ under composition $\circ$
- Homomorphisms $\mathcal{E}_1 \longrightarrow \mathcal{E}_2$ form a $\mathbb{Z}$-module $\mathrm{Hom}(\mathcal{E}_1, \mathcal{E}_2)$ under addition $+$
- Endomorphisms of $\mathcal{E}$ form a ring $\mathrm{End}(\mathcal{E})$ under addition and composition $(+, \circ)$

Over a finite field $\mathbb{F}_q$, we always have scalar multiplication $\underset{m \in \mathbb{Z}}{[m]}$ and Frobenius π_q,

$$\mathbb{Z}[\pi_q] \subseteq \mathrm{End}(\mathcal{E})$$

this is a ring, like
$\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$ are rings of integers of $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$.

Chapter 3.

- What are the points of order 2 on a curve $y^2 = x^3 + a_2 x^2 + a_4 x + a_6$?
- What are the points of order 3?

The points of order 2 are the $(x_0, 0)$ points, where x_0 are three distinct roots of $x^3 + a_2 x^2 + a_4 x + a_6$.

if x_0 is such a root, then translate it to 0. $(x - x_0)(x^2 + a' x + b')$

with $(x-x_0)\left((x-x_0)^2 + \underbrace{(a_2 + 3x_0)}_{a'}(x-x_0) + \underbrace{3x_0^2 + 2a_2 x_0 + a_4}_{b'}\right)$

The other points of order 2 are: $(x_1, 0)$ and $(x_2, 0)$ where x_1, x_2 are two distinct roots of $x^2 + a'x + b'$.

These are in K if $a'^2 - 4b'$ is a square.

The points of order 3 are inflexion points (flex points).

$(u(v(x)))' = u'(v(x))v'(x)$

$(\sqrt{x})' = \frac{1}{2\sqrt{x}}$

$y^2 = x^3 + ax + b$ (or $x^3 + a_2 x^2 + a_4 x + a_6$).

let's look at $f = \sqrt{x^3 + a_2 x^2 + a_4 x + a_6}$ roots of the 2nd derivative:

$$g(x) = f''(x) f - \tfrac{1}{2} f'^2 = \tfrac{1}{2}\left(3x^4 + 4a_2 x^3 + 6a_4 x^2 + 12 a_6 x + (4a_2 a_6 - a_4^2)\right)$$

assume $4a_2 a_6 - a_4^2 = 0 \to (0, \sqrt{a_6})$ is a point of order 3.

the 8 points are $(x_0, \pm y_0)$ where x_0 is a root of $g(x)$, and (x_0, y_0) satisfies the equation.

the ninth point is $\mathcal{O}$.