divisors again. 21/04/2022. 4

Miller Algorithm computes a function whose divisor is $\ell(P) - \ell(O)$ with the intermediate functions

$$f_{i,P} \quad \text{such that} \quad \operatorname{div}(f_{i,P}) = i(P) - (iP) - (i-1)(O)$$

of degree 0 and sum O.

Note that $f_{1,P}$ has divisor $\operatorname{div}(f_{1,P}) = 1(P) - (P) - 0(O) = 0$.

in other words, $f_{1,P}$ has no zero and no pole $\Rightarrow$ this is a constant of the field.

So we can just take 1.

$$f_{1,P} = 1.$$

(see also prop. 11.1 in Washington's book).

We aim at computing the function g s.t. $\operatorname{div}(g) = \ell(P) - \ell(O)$.

But there is no function of divisor $(P)-(O)$ on E: the most simple functions are lines and tangents but because of Bezout's theorem, there ~~are~~ are three points counted with multiplicity that intersect a line and the curve.

$$\operatorname{div}(\ell_{P,Q}) = (P) + (Q) + (-(P+Q)) - 3(O).$$

$$\operatorname{div}(\ell_{P,P}) = 2(P) + (-2P) - 3(O).$$

$$\operatorname{div}(v_P) = (P) + (-P) - 2(O).$$ (also valid if P has order 2: vertical tangent)

Miller step:

line through iP and jP
tangent if $i=j$.

$$f_{i+j,P} = f_{i,P} \cdot f_{j,P} \cdot \frac{\ell_{iP,jP}}{v_{(i+j)P}}$$

vertical at $(i+j)P$

(see lecture of Week 5 Thursday, March 3, and Washington's book chapter 11).

From (reduced) Tate pairing to ate pairing

see Galbraith's chapter IX on pairings (week 11 PDF).

Let E an elliptic curve defined over $\mathbb{F}_q$ with a subgroup of order ℓ, $\ell \mid \#E(\mathbb{F}_q)$ but $\ell \nmid q-1$ and $\ell^2 \nmid \#E(\mathbb{F}_q)$, $(E[\ell] \not\subset E(\mathbb{F}_q))$ and the embedding degree of ℓ with respect to q is n.

Th. IX.9 Let $P \in E(\mathbb{F}_q)[\ell]$ of order ℓ and $Q \subset E(\mathbb{F}_{q^n})$.

$$\left(e_{Tate,\ell}(P,Q)\right)^{\frac{p^n-1}{\ell}} = \left(e_{Tate,N}(P,Q)\right)^{\frac{p^n-1}{N}}$$

for N a multiple of ℓ, and $N \mid p^n-1$.

Proof. Write $N = h \cdot \ell$ for some cofactor h, and assume h is coprime to ℓ.

The Tate pairing is $\quad (g(Q))^{\frac{p^n-1}{\ell}} = (g(Q))^{h\frac{p^n-1}{N}} = (g^h(Q))^{\frac{p^n-1}{N}}$

What is g^h? a function whose divisor is $h(\ell(P) - \ell(\mathcal{O})) = N(P) - N(\mathcal{O})$

$\rightarrow$ this is $e_{Tate,N}(P,Q)^{\frac{p^n-1}{N}}$. It holds because $\ell P = \mathcal{O} \Rightarrow NP = \mathcal{O}$.

Now, let's consider $N = \gcd(T^n - 1, p^n-1)$ where $T = t-1$.

We have $\ell \mid N$ because 1) $\ell \mid p^n-1$ by assumption, and

2) $\ell \mid T^n - 1 = (t-1)^n - 1$ because actually $\ell \mid \Phi_n(t-1)$ and $\Phi_n(t-1) \mid (t-1)^n-$

$\rightarrow$ we can replace ℓ by N in the Tate pairing. Denote $T^n - 1 = c \cdot N$.

Let $f_{i,P}$ denote a Miller function $\operatorname{div}(f_{i,P}) = i(P) - (iP) - (i-1)(\mathcal{O})$.

$$\operatorname{div}(f_{T^n-1,Q}) = (T^n-1)(Q) - (\underbrace{(T^n-1)Q}_{=\mathcal{O}}) - (T^n-2)(\mathcal{O}) = (T^n-1)(Q) - (T^n-1)(\mathcal{O})$$
$$= c \cdot (N(Q) - N(\mathcal{O}))$$

$$f_{T^n-1,Q} = g_N^c \quad \text{where} \quad \operatorname{div}(g_N) = N(Q) - N(\mathcal{O}).$$

$$\left(f_{T^n-1,Q}(P)\right)^{\frac{p^n-1}{N}} = \left(f_{N,Q}(P)\right)^{\frac{p^n-1}{N}\cdot c} = \left(e_{Tate,N}(Q,P)\right)^{\frac{p^n-1}{N}\cdot c}$$

Finally, let's simplify $f_{T^n-1,Q}(P)$.

$$\mathrm{div}(f_{T^n,Q}(P)) = T^n(Q) - (T^nQ) - (T^n-1)(O)$$

where $(T^n-1)Q = O$, hence $T^nQ = Q$.

$$\mathrm{div}(f_{T^n,Q}(P)) = T^n(Q) - (Q) - (T^n-1)(O)$$
$$= (T^n-1)(Q) - (T^n-1)(O)$$
$$= \mathrm{div}(f_{T^n-1,Q})$$

We need: $f_{ab,Q} = f_{a,Q}^b \cdot f_{b,[a]Q}$ where f is a Miller function.

$$\mathrm{div}(f_{ab,Q}) = ab(Q) - (abQ) - (ab-1)(O)$$
$$= b(a(Q) - (aQ) - (a-1)(O))$$
$$+ \quad b(aQ) - (abQ) - (b-1)(O) = \mathrm{div}(f_{a,Q}^b) + \mathrm{div}(f_{b,aQ})$$

$$\mathrm{div}(f_{a,Q}^b) = b(a(Q) - (aQ) - (a-1)(O)) = ab(Q) - b(aQ) - (ab-b)(O)$$
$$\mathrm{div}(f_{b,aQ}) = b(aQ) - (abQ) - (b-1)(O)$$

Let's decompose $T^n = T\ T^{n-1} = T \cdot T \cdot T^{n-2} \ldots$

$$f_{T^n,Q} = f_{T,Q}^{T^{n-1}}\ f_{T^{n-1},[T]Q}$$
$$= f_{T,Q}^{T^{n-1}}\ f_{T,[T]Q}^{T^{n-2}}\ f_{T^{n-2},[T^2]Q}$$
$$= \cdots\ f_{T,Q}^{T^{n-1}}\ f_{T,[T]Q}^{T^{n-2}}\ f_{T,[T^2]Q}^{T^{n-3}} \cdots f_{T,[T^{n-1}Q]}$$

Note that $\ell \nmid T^{n-1}$ nor $T^{n-1}-1$.

Finally: we need a special property on $[T]Q$. : $[T]Q = [q]Q = \pi_q(Q)$.

and $f_{a,\pi_q(Q)} = f_{a,Q}^q$

$$\Rightarrow f_{T,[T]Q} = f_{T,Q}^p$$

and $$f_{T^n,Q} = f_{T,Q}^{T^{n-1}} \cdot f_{T,Q}^{T^{n-2}q} \cdot f_{T,Q}^{T^{n-3}q^2} \cdots f_{T,Q}^{q^{n-1}} = f_{T,Q}^{T^{n-1}+T^{n-2}q+T^{n-3}q^2+\cdots+q^{n-1}}$$
$$= f_{T,Q}^c \quad \text{for some constant } c.$$

Finally, we need $[T]\,Q = [q]\,Q = \pi_q(Q)$.

G_2 and the trace-0 subgroup.

Remember that there are $\ell+1$ distinct subgroups of order ℓ over $\mathbb{F}_{p^n}$.

G_1 is the only choice of $\mathbb{F}_q$-subgroup : $E(\mathbb{F}_q)[\ell] = G_1$.

We have many choices for G_2 and one of them will provide us with

$$\pi_q(Q) = [q]\,Q.$$

First: $Q \notin E(\mathbb{F}_q)$ hence π_q is not the identity on Q.

Then, writing $\pi_q(Q) = [q]\,Q$ means we want G_2 to be "orthogonal" to G_1 with respect to the Frobenius endomorphism, that is the matrix representing π_q will be diagonal over $\mathbb{Z}/\ell\mathbb{Z}$.

π_q is identity on G_1.

$$\pi_q \Leftrightarrow M = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \quad \text{in the basis } (G_1, G_2).$$

this would means $\pi_q(Q) = [q]\,Q$.

$\chi_q = X^2 - tX + q$ is the characteristic polynomial of π_q and M.

Let's factor it mod ℓ: $(X-1)(X-q) = X^2 - \underbrace{(1+q)}_{\equiv -t \bmod \ell}X + q$ indeed.

because $\ell \mid q+1-t \Leftrightarrow q+1 \equiv -t \bmod \ell$.

(in all generality: with $\ell \mid q+1-t$, $M = \begin{pmatrix} 1 & a \\ 0 & q \end{pmatrix}$).

So there exists one choice of G_2 such that $\pi_q(Q) = [q]\,Q \;\forall\, Q \in G_2$.

Finally, $f_{a,\pi_q(Q)}(P) = f^{\,q}_{a,Q}(P)$ as long as $P \in E(\mathbb{F}_q)$ is fixed by π_q.

Trace-0 subgroup. Galbraith's chapter IX, § IX.7.4.

$$\mathrm{Tr}(Q) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma(Q) = \sum_{i=0}^{n-1} (x^{q^i}, y^{q^i}).$$

$\mathrm{Tr}(Q) \in E(\mathbb{F}_q)$ even if $Q \in E(\mathbb{F}_{q^n})$.

$\forall Q' \in E(\mathbb{F}_{q^n})[\ell]$, define $Q = [n]\,Q - \mathrm{Tr}(Q)$ where n is the embedding degree.

$$\mathrm{Tr}(Q) = \mathrm{Tr}([n]\,Q) - \mathrm{Tr}(\mathrm{Tr}(Q)) = [n]\,\mathrm{Tr}(Q) - \sum_{i=0}^{n-1} \pi_q^i(\mathrm{Tr}(Q))$$
$$= [n]\,\mathrm{Tr}(Q) - [n]\,\mathrm{Tr}(Q) = 0.$$

G_2 as the Trace-zero subgroup of order ℓ of $E(\mathbb{F}_{p^n})[\ell]$.

Galbraith chapter IX, section IX.7.4.

Lemma IX.16. ℓ prime, embedding degree n, coprime to ℓ. $\ell \mid q+1-t$, $\ell \nmid n$, $\ell \nmid q-1$.

$$\mathcal{G} = \{ Q \in E(\mathbb{F}_{p^n})[\ell] : Tr(Q) = \mathcal{O} \}$$

$$= \{ Q \in E(\mathbb{F}_{p^n})[\ell] : \pi_q(Q) = [q]Q \}$$

and $e_{Tate,\ell}(P,Q) = 1 \ \forall P, Q \in \mathcal{G}$.

Proof.

i) if $Q \in E(\mathbb{F}_q)$ then $Tr(Q) = \sum_{i=1}^{n-1} \pi_q^i(Q) = \sum_{i=1}^{n-1} Q = nQ \neq \mathcal{O}$ $(\gcd(n,\ell)=1)$.

$\to \mathcal{G} \cap E(\mathbb{F}_q) = \{\mathcal{O}\}$.

ii) $\mathcal{G}$ is a subgroup of $E(\mathbb{F}_{q^n})[\ell]$.

Then $\mathcal{G}$ has order ℓ and $\mathcal{G}$ is cyclic.

Now consider the 2nd def of $\mathcal{G}$: $\{Q \in E(\mathbb{F}_{p^n})[\ell] : \pi_q(Q) = [q]Q\}$.

Let Q_2 a generator of the choice of the subgroup of order ℓ of $E(\mathbb{F}_{q^n})$ s.t. $\pi_q(Q) = [q]Q$.

$$Tr(Q_2) = \sum_{i=0}^{n-1} \pi_q^i(Q_2) = \sum_{i=0}^{n-1} [q^i] Q_2 = [1+q+q^2+\cdots+q^{n-1}] Q_2.$$

but note that $q^n - 1 = (q-1)(1+q+q^2+\cdots+q^{n-1})$

and $\ell \mid q^n-1$ but $\ell \nmid q-1$ hence $\ell \mid 1+q+q^2+\cdots+q^{n-1}$

and $Tr(Q_2) = \mathcal{O}$.

So $Q_2 \in \mathcal{G}$ (1st definition). $\square$.