Entonces para calcular $e_m(P,Q)$ podemos escribir

$$P = a_P P_1 + b_P P_2$$
$$Q = a_Q P_1 + b_Q P_2$$

y usar esta fórmula para calcular $e_m(P,Q)$.

Pero, encontrar a_P, b_P, a_Q, b_Q debería ser más difícil que el DCDLP.

Entonces presentamos un algoritmo

Thm: (Miller) E, $P=(x_P,y_P)$ $Q=(x_Q,y_Q)$ puntos en E no cero.

(a) Sea λ la pendiente de la recta entre P y Q (puede ser $\lambda=\infty$, y si $P=Q$ es el recta de la tangente)

Definimos
$$g_{P,Q} = \begin{cases} \dfrac{y - y_P = \lambda(x-x_P)}{x + x_P + x_Q - \lambda^2} & \lambda \neq \infty \quad (\star) \\ x - x_P & \lambda = \infty \end{cases}$$

Entonces $\operatorname{div}(g_{P,Q}) = [P] + [Q] - [P+Q] - [O]$

(b) $1 \leq m = m_0 + m_1 2 + \cdots + m_{n-1}2^{n-1}$ Este algoritmo devuelve una función f_P Verificando $\operatorname{div}(f_P) = m[P] - [mP] - (m-1)[O]$ (suma de los coefs = 0)

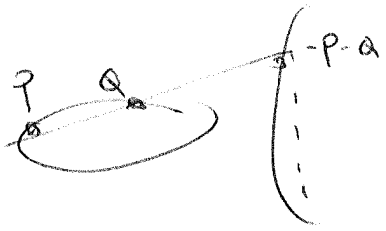
(1) $T=P$, $f=1$
(2) for $i = n-2$ to 0
  $f \leftarrow f^2 \cdot g_{T,T}$
  $T \leftarrow 2T$
  si $m_i = 1$
  $f \leftarrow f \, g_{T,P}$
return f

En particular
$P \in E[m] \Rightarrow$
$\operatorname{div}(f_P) = m[P] - m[O]$

Rem:

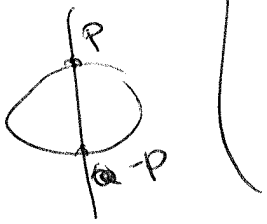
(a)(i) $\lambda \neq \infty$, sea $y = \lambda x + \nu$ la recta entre P y Q.

o la tangente si $P = Q$. Cruza la curva E entres puntos. Entonces



$$\operatorname{div}(y - \lambda x - \nu) = [P] + [Q] + [-P-Q] - 3[O]$$

Rectas verticales cruzan E en todos los puntos, cada uno el opuesto del otro.



$$\Rightarrow \operatorname{div}(x - x_{P+Q}) = [P+Q] + [-P-Q] - 2[O]$$

Entonces si $g_{P,Q} = \dfrac{y - \lambda x - \nu}{x - x_{P+Q}}$

$$= [P] + [Q] - [P+Q] - [O] - 3[O] - ([P+Q] + [-P-Q] - 2[O])$$

y además como $x_{P+Q} = \lambda^2 - x_P - x_Q$ y como

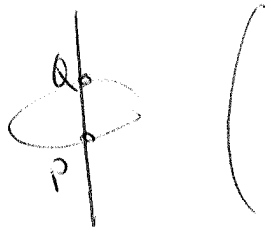
$$\nu = \lambda x_P - y_P$$

$$y = \lambda x + \nu \Leftrightarrow (y - y_P) = \lambda(x - x_P)$$

tenemos

$$g_{P,Q} = \frac{y - y_P - \lambda(x - x_P)}{x - \lambda^2 + x_P + x_Q}.$$

Ahora si $\lambda = +\infty$, $\nexists\ P+Q=O$.



Como queremos que

$$\mathrm{div}_{P,Q}(g_{P,Q}) = [P]+[-P]-2[O]$$

se ve que la función $X - X_P$

cumple esto.

(5) Intuición. ~~Obs~~ La observación clave es:

$$\mathrm{div}(g_{T,T}) = 2[T]-[2T]-O \quad \text{y} \quad \mathrm{div}(g_{T,P}) = [T]+[P]-[T+P]-[O]$$

y $\mathrm{div}(f^2) = 2\mathrm{div}(f)$ o sea es como un shift.]

Este teorema se puede usar para calcular el weil pairing

Idea: Sea $P \in E[m]$. Algoritmo $\Rightarrow$ f_P con divisor $m[P]-m[O]$

Además, R cualquier punto en E $\Rightarrow$ en cada paso iteración del loop se puede calcular $g_{T,T}(R)$ y $g_{T,P}(R)$. Estamos de la función f_P en la definición ~~dos~~.

$$e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)}$$

para algún $S \notin \{O, P, Q, P-Q\}$

G] $y^2 = x^3 + 30x + 34$ \ $\mathbb{F}_{631}$.

La curva tiene $\#E(\mathbb{F}_{631}) = 650 = 2 \cdot 5^2 \cdot 13$ puntos y tiene un 25 de orden 5 ($\cong \mathbb{Z}/52 \times \mathbb{Z}/52$) generado por $P = (36, 60)$ y $Q = (121, 387)$.

Queremos ver si $\{$ subgrupo generado por P y $Q\}$.

~~$5 = \#\langle P \rangle = \#\langle Q \rangle$~~ P tiene orden 5 y Q también

Entonces el algoritmo $\Rightarrow f_P + f_Q \operatorname{div}(f_P) = 5[P] - 5[O]$

El f_P se calcula así: $m = 101$

$T = (36, 60)$ $f = 1$

$y^2 = x^3 + 30x + 34$

$2y \frac{dy}{dx} = 3x^2 + 30$

$\lambda = \frac{653}{20}$

$i = 0 \rightarrow f = 1^2 \cdot g_{T,T}$

$= \dfrac{y - 60 - \lambda(x - 36)}{x + 36 + 36 - \left(\frac{653}{20}\right)^2}$

$n_0 = 1$

$\Rightarrow f_P = f \cdot g_{T,P} = \dots$

Al final, $\dfrac{f_P(Q+S)}{f_P(S)}$ calculamos la suma de varios (x_3, y_3) y después evaluamos $f_P(x_3, y_3)$.

$= 437 \in \mathbb{F}_{631}$

$\dfrac{f_Q(P-S)}{f_Q(-S)} = \dfrac{176}{2} = 88 \in \mathbb{F}_{631}$

$e_5(P, Q) = \dfrac{437}{88} = 242 \in \mathbb{F}_{631}$

Obs: $(242)^5 = 1$

Reducción de ECDLP en $E(\mathbb{F}_p)$ a DLP en $\mathbb{F}_{p^k}^{\times}$

Def. E una curva elíptica sobre $\mathbb{F}_p$ y $m \geq 1$ con $p \nmid m$.

El grado de inmersión de E con respecto a m es el k más chico que cumple

$$E[(\mathbb{F}_{p^k})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

En general nos interesa este grado cuando m es un primo grande.

Prop: $E/\mathbb{F}_p$ $\ell \neq p$ primo. Supongamos que $E(\mathbb{F}_p)$ contiene un punto de orden ℓ. Entonces el grado de inmersión desde p es

(1) grado de inmersión puede ser 1 (pero no puede ser 1 si $\ell > \sqrt{p}+1$)

(2) $p \equiv 1 \pmod{\ell}$ $\Rightarrow$ grado es ℓ

(3) $p \not\equiv 1 \pmod{\ell}$ $\Rightarrow$ grado es el k mínimo que cumple $p^k \equiv 1 \pmod{\ell}$

Idea: $E/\mathbb{F}_p$, $P \in E(\mathbb{F}_p)[\ell]$ para $\ell > \sqrt{p}+1$ Sea k el grado de inmersión y supongamos que sabemos resolver DLP en $\mathbb{F}_{p^k}$. Sea $Q \in E(\mathbb{F}_p)$ un multiplo de P

Entonces el algoritmo de Menezes, Okamoto y Vanstone (MOV) resuelve el ECDLP.

1) Calcular $N = \#E(\mathbb{F}_{p^k})$. Obs: $\ell \mid N$ para que $E(\mathbb{F}_p)$ tiene un punto de orden ℓ.
(algoritmo SEA)

2) Elegir un punto al azar hq $T \in E(\mathbb{F}_{p^k})$ pero $T \notin E(\mathbb{F}_p)$:
(¿cómo se hace? Elegir una coordenada x_T al azar y ver si es un cuadrado usando Tonelli-Shanks)

3) Calcular $T' = \left(\frac{N}{\ell}\right) T$ Si $T' = \mathcal{O}$ elegir otro T (paso 2)
$\in \mathbb{Z}$
sumar y doblar o sumar y fallar

4) Calcular
$\alpha = e_\ell(P, T') \in \mathbb{F}_{p^k}^\times$ $\beta = e_\ell(Q, T') \in \mathbb{F}_{p^k}^\times$
el $\mathbb{F}_{p^k}^\times$ es porque sabemos que es una raíz de 1

Si $\alpha = 1$ elegir otro T (paso 2)

5) Resolver nDLP para α y β en $\mathbb{F}_{p^k}^\times$. O sea, hallar
n t.q $\beta = \alpha^n$
(si p^k no es demasiado grande se puede hacer con cálculo de índices).

6) Entonces $Q = nP$.