Ahora, si $n = v_0 + v_1 \tau + \cdots + v_\ell \tau^\ell$ con $v_i \in \{0, \pm 1\}$

$$\Rightarrow nP = (v_0 + v_1\tau + \cdots + v_\ell \tau^\ell)(P)$$
$$= v_0 P + v_1 \tau(P) + \cdots v_\ell \tau^\ell(P).$$

Thm: Tal expresión para n tiene $\ell \approx 2\log n$ y a lo más $\frac{1}{3}$ de los v_i distinto que cero.

Dem: Cuentas: escribimos $n = 2c + b$ y cambiamos el 2 por $-\tau - \tau^2$.

Pairing bilineales pre curvas elípticas:

Pairing bilineales

funciones $\beta : \hat{\mathbb{R}} \times \hat{\mathbb{R}} \to \mathbb{R}$ lineal en cada coordenada:

ej $\beta : \hat{\mathbb{R}}^n \times \hat{\mathbb{R}}^n \to \mathbb{R}$

$u, v \mapsto u \cdot v = \sum u_i v_i$

$\beta(\alpha_1 v_1 + \alpha_2 v_2, w) = \alpha_1 \beta(v_1, w) + \alpha_2 \beta(v_2, w)$

y $\beta(\cdot, b_1 w_1 + b_2 w_2) = \cdots$

$\beta : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$

$u, v \mapsto \det \begin{pmatrix} -u- \\ -v- \end{pmatrix}$

se puede probar que es bilineal

Para estos β, $\beta(u, v) = -\beta(v, u)$

$\Rightarrow \beta(v, v) = 0$

Vamos a mirar pairings

$$E(\mathbb{F}_{p^k}) \times E(\mathbb{F}_{p^k}) \to \mathbb{F}_{p^k}.$$

Def. Sea $m \geq 1$. Un punto $P \in E$ t.q. $mP = \mathcal{O}$ se llama un punto de orden m. El conjunto $E[m]$ de todos los puntos de orden m se denota

$$E[m] = \{P \in E : mP = \mathcal{O}\}.$$

Obs: $P, Q \in E[m]$

$\Rightarrow mP = mQ = \mathcal{O}$

Entonces $m(P+Q) = mP + mQ = \mathcal{O} + \mathcal{O} = \mathcal{O}$

$P \in E[m] \Rightarrow mP = \mathcal{O}$

Entonces $m(-P) = -mP$
$= -\mathcal{O}$
$= \mathcal{O}$

Entonces $E[m]$ es un subgrupo de E.

Notación Para K un cuerpo $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_{p^k})$, se escribe $E(K)[m]$

Prop $m \geq 1$

(a) E una curva elíptica sobre $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Entonces

$$E(\mathbb{C})[m] \cong \underbrace{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}}_{= \{(a,b) : a, b \in \mathbb{Z}/m\mathbb{Z}\}}$$

con $(a,b) + (c,d)$ componentes

(b) $E \setminus \mathbb{F}_p$. $p \nmid m \Rightarrow \exists k$ t.q. $\forall j \geq 1$

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

Obs: ℓ primo, y K t.q. $E(K)[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ (28)

entonces $E(K)[\ell]$ es un espacio vectorial de dimensión 2 sobre $\mathbb{Z}/\ell\mathbb{Z}$.

Más compuesto: t.q. $E(K)[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ se sigue teniendo una base aunque no es un espacio vectorial. O sea $\forall P \in E[m]$, $\exists a, b$ t.q.

$$P = aP_1 + bP_2$$

Encontrar tal a y b para m grande es "$\Leftrightarrow$" ECDLP.

Vamos a definir dos pairings en particular, el de Weil y el de Tate.

Antes de hacer eso tenemos que hablar de funciones racionales

$$f(X) = \frac{a_0 + a_1 X + \cdots + a_n X^n}{b_0 + b_1 X + \cdots + b_n X^n}$$

$$= \frac{a(X-\alpha_1)^{e_1} \cdots (X-\alpha_r)^{e_r}}{b(X-\beta_1)^{d_1} \cdots (X-\beta_s)^{d_s}}$$

Supongamos que se haya simplificado todo lo que se puede simplificar

Los α_i son los ceros de f

Los β_i son los polos de f.

Los e_i, d_i son las multiplicidades.

Se define el divisor como la suma formal

$$\operatorname{div}(f(X)) = \sum e_i[\alpha_i] - \sum d_i[\beta_i]$$

En nuestro caso, tenemos $f(X,Y)$ racional $= \frac{P(X,Y)}{Q(X,Y)}$ y hay puntos de E donde $P(X,Y)=0$ y otros donde $Q(X,Y)=0$

Se puede entonces definir

$$\mathrm{div}(f) = \sum_{P \in E} n_P [P]$$

n_P multiplicidad de cero o de polo ($n_P<0$ para polos)

Ej: $y^2 = X^3 + AX + B$

$$X^3 + AX + B = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$$

$P_1 = (\alpha_1, 0)$

$P_2 = (\alpha_2, 0)$

$P_3 = (\alpha_3, 0)$ son de orden 0.

$\mathrm{div}(Y)$

$f(X,Y) = Y$: tiene div : $[P_1] + [P_2] + [P_3]$

polos $\infty [\mathcal{O}]$

Def: Un divisor de E es cualquier suma formal

$$D = \sum_{P \in E} n_P [P] \quad \text{con } n_P \in \mathbb{Z} \text{ y } n_P = 0 \text{ para todo } P \text{ menos una cantidad fin.}$$

El grado de un divisor

$$\deg(D) = \deg\left(\sum_{P \in E} n_P [P]\right) = \sum n_P$$

La suma de un divisor $\mathrm{Sum}(D) = \mathrm{Sum}\left(\sum n_P [P]\right) = \sum n_P P$

Tma: E una CE

(1) f, f' funciones racionales en E.
Si $div(f) = div(f')$, entonces $f = cf'$ para una constante no cero.

(2) $D = \sum_{P \in E} n_P [P]$ un divisor. Entonces

D un divisor de una función racional f $\iff$ $\deg(D) = 0$ y $\sum(D) = \mathcal{O}$

En particular si $f(X,Y) = \frac{P(X,Y)}{Q(X,Y)}$ es una función racional sobre E, no tiene polos ni ceros, es constante.

Obs $div(f) = 0$, $f' = k \Rightarrow div(f') = 0$ (a) $\Rightarrow f = ck$ constante
f sin polos ni ceros

Ej: $[P_1] + [P_2] + [P_3] - n\mathcal{O}$
$\Rightarrow$ Como $div(Y)$ tiene que tener grado 0 $\Rightarrow n = 3$

Ej: $P \in E[m]$ $\Rightarrow$ $m[P] - m[\mathcal{O}]$ tiene que corresponder a una función racional.

$div(f_P) = m[P] - m[\mathcal{O}]$

m=2 $P \in E[2] \iff y_P = 0$. Si $P = (\alpha, 0) \in E[2]$
$f_P = X - \alpha$.

El pairing de Weil

denotado em

$e_m: E[m] \times E[m] \Rightarrow$ m-ésima raíz de 1 (→ raíz de 1)

$P, Q \mapsto$ | se encuentran $z^m = 1$ tiene m raíces $e^{2\pi i k/m}$ para $k = 0, 1, 2, \ldots, m-1$

en el plano forman un polígono regular con m lados

Bilineal)

$e_m(P_1 + P_2, Q) = e_m(P_1, Q)\, e_m(P_2, Q)$

porque raíces de uno 1 son multiplicativas

$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)\, e_m(P, Q_2)$

Def. $P, Q \in E[m]$ f_P, f_Q funciones racionales en E que verifican

$\operatorname{div}(f_P) = m[P] - m[\mathcal{O}]$

$\operatorname{div}(f_Q) = m[Q] - m[\mathcal{O}]$

Se define el pairing de Weil como:

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

donde $S \in E \setminus \{\mathcal{O}, P, -Q, P-Q\}$

↳ ⇒ que todo $f_P(*) \neq 0$.

Prop. Se puede probar que es

- bien definido: eg. si $\operatorname{div} f_P = \operatorname{div} f_P' \Rightarrow f_P = c f_P'$ y se cancelan

  e.j. es independiente de la elección de S.

- es ~~bilineal~~

Tma. (a) $e_m(P,Q)^m = 1 \quad \forall P,Q \in E[m]$

(b) e_m bilineal

(c) $e_m(P,P) = 1 \quad \forall P \in E[m]$

Ej: Calculemos e_2

E: $Y^2 = X^3 + AX + B = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$

Obs: $\alpha_1 + \alpha_2 + \alpha_3 = 0$ ~~para el~~ X^2 porque el coeficiente de X^2 es 0

Los puntos $P_1(\alpha_1, 0)$, $P_2(\alpha_2, 0)$, $P_3(\alpha_3, 0)$ son de orden 2

y como vimos recién $\operatorname{div}(X-\alpha_i) = 2[P_i] - 2[\mathcal{O}]$.

Ahora para calcular e_2, elegimos $S = (x,y)$ ct

La primera coordenada de $P_1 - S$ es $\dfrac{\alpha_1 x + \alpha_2\alpha_3 + \alpha_1^2}{x - \alpha_1}$

y para $(P_2 + S)$ es $\dfrac{\alpha_2 x + \alpha_1\alpha_3 + \alpha_2^2}{x - \alpha_2}$

Ahora

$$e_2(P_1,P_2) = \frac{f_{P_1}(P_2+S)}{f_{P_1}(S)} \Big/ \frac{f_{P_2}(P_1-S)}{f_{P_2}(-S)}$$

$$f_{P_1} = X - \alpha_1 = \frac{X(P_2+S) - \alpha_1}{X(S) - \alpha_1} \Big/ \frac{X(P_1-S) - \alpha_2}{X(-S) - \alpha_2}$$

$$= \frac{\dfrac{\alpha_2 x + \alpha_1\alpha_3 + \alpha_2^2}{x-\alpha_2} - \alpha_1}{x - \alpha_1} \Big/ \frac{\dfrac{\alpha_1 x + \alpha_2\alpha_3 + \alpha_1^2}{x-\alpha_1} - \alpha_1}{x - \alpha_2}$$

$$= -1$$ usando en algún momento que $\alpha_1 + \alpha_2 + \alpha_3 = 0$

Obs: $E[m]$ es un "espacio vectorial" de dimensión 2 sobre un "cuerpo" $\mathbb{Z}/m\mathbb{Z}$.

Sabemos que siempre hay un primo ℓ distinto de la característica.

Sea P_1, P_2 una base de $E[m]$. Entonces cada P se puede escribir como una combinación lineal de $a_P P_1 + a_P P_2$

~~Por tanto~~

Pero ojo si $\zeta = e_m(P_1, P_2)$,

$$e_m(P+P, Q) = e_m(P,Q)^2$$

$$e_m(P,P) = 1$$

~~$e_m(P,Q) = e_m(a_P P_1 + b_P P_2,\ a_Q P_1 + b_Q P_2)$~~

~~$= e_m(a_P P_1$~~

$= a_P\, e_m(P_1) \cdot$ ~~$e_m(a_Q P_1 + b_Q P_2)$~~

$\cdot e_m(b_P P_2,\ a_Q P + b_Q P_2)$

$= a_P\, e_m(P_1)\, b_P\, e_m(b_P P_2)\, a_Q$

$e_m(P,Q) = e_m(a_P P_1 + b_P P_2, Q)$

$= e_m(a_P P_1, Q) \cdot e_m(b_P P_2, Q)$

$= a_P b_P\, e_m(P_1,Q)^{a_P} e_m(P_2,Q)^{b_P}$

$= a_P b_P\, e_m(a_Q P_1,\ a_Q P_1 + b_Q P_2)^{a_P} e_m(P_2,\ a_Q P_1 + b_Q P_2)^{b_P}$

$= a_P b_P\, e_m(P_1,\ a_Q P_1)^{a_P} e_m(P_1, b_Q P_2)^{a_P}$

$e_m(P_2,\ a_Q P_1)^{b_P} e_m(P_2, b_Q P_2)$

$= e_m(P_1,P_1)^{a_P a_Q}\, e_m(P_1,P_2)^{b_Q a_P}$

$e_m(P_2,P_1)^{a_Q b_P}\, e_m(P_2,P_2)^{b_P b_Q}$

$= 1 \cdot \zeta^{b_Q a_P} \cdot \zeta^{-a_Q b_P} \cdot 1$

$= \zeta^{\det \begin{pmatrix} a_P & a_Q \\ b_P & b_Q \end{pmatrix}}$.