Number Theory & Cryptography - Weekly meetings

Curso en Zacatecas [Q1 2015]

Luis J. Dominguez Perez

CIMAT-Zac, Mayo 06 de 2015

Contenido, sección 1

Divisores

Emparejamiento de Weil

Funciones racionales de la curva

Dada una curva elíptica E definida sobre un campo finito $\mathbb{F}_q$, donde $q = p^n$, y $n \in \mathbb{Z}^+$, con $\bar{\mathbb{F}}_q$ como la cerradura de $\mathbb{F}_q$, se dice que $f(x, y)$ es una función racional en $E/\mathbb{F}_q$, si existe un punto $P = (x_P, y_P) \in E(\bar{\mathbb{F}}_q)$, tal que $f(x_P, y_P) \neq \infty$

El conjunto de funciones racionales en $E/\mathbb{F}_q$ está denotado por $\bar{\mathbb{F}}_q(E)$, y para todo $f \in \bar{\mathbb{F}}_q(E)$ se cumple que $f(P)$ es un elemento en el conjunto $\{\bar{\mathbb{F}}_q \cup \infty\}$

funciones racionales de la curva

Sean P y Q puntos en la curva elíptica $E/\mathbb{F}$, una función racional $f \in \bar{\mathbb{F}}_q(E)$ tiene un **cero** en P, y un **polo** en Q, si y sólo sí $f(P) = 0$, y $f(Q) = \infty$, respectivamente. En general, la evaluación de f en un punto P puede ser representada a partir de la siguiente igualdad:

$$f(P) = (u(P))^m \cdot g(P)$$

donde $m \in \mathbb{Z}$, $u(P) = 0$, y $g(P) \neq 0, \infty$. Si $m > 0$, entonces f tiene un cero en P, y si $m < 0$, entonces f tiene un polo (en P). cabe mencionar que $u(P)$ es llamada la función "*uniformadora*", y el número m es el **orden** de f en P, denotado como:

$$\text{ord}_P(f) = m.$$

Divisores

Sea $E/\mathbb{F}_q$ una curva elíptica, a cada punto $P \in E(\bar{\mathbb{F}}_q)$ se le asigna el símbolo formal $[P]$. Un divisor $\mathcal{D}$ sobre $E/\mathbb{F}_q$ es una combinación lineal finita de dichos símbolos con coeficientes en $\mathbb{Z}$

$$\mathcal{D} = \sum_j a_j [P_j], \quad a_j \in \mathbb{Z}.$$

divisores

Los operadores que definen a un divisor son:

- El grado

$$\deg\left(\sum_j a_j[P_j]\right) = \sum_j a_j \in \mathbb{Z}$$

- La suma

$$\text{sum}\left(\sum_j a_j[P_j]\right) = \sum_j a_j P_j \in E$$

- El soporte

$$\text{supp}\left(\sum_j a_j[P_j]\right) = \{P_j \in E | a_j \neq 0\}$$

Divisores principales

Un divisor $\mathcal{D}$ sobre la curva elíptica $E/\mathbb{F}_q$ con $\deg(\mathcal{D}) = 0$, y $\text{sum}(\mathcal{D}) = \mathcal{O}$, es llamado **"principal"** si existe una función racional $f \in \bar{\mathbb{F}}_q(E)$, tal que $\mathcal{D} = \text{div}(f)$, donde

$$\text{div}(f) = \sum_{P_j \in E} \text{ord}_{P_j}(f)[P_j].$$

ejemplos

Las funciones racionales $\ell_{P,P}$, y $\ell_{P,Q}$

- $\mathbf{div}(\ell_{P,P}) = 2[P] + [-2P] - 3[\mathcal{O}]$
- $\mathbf{div}(\ell_{P,Q}) = [P] + [Q] + [-(P+Q)] - 3[\mathcal{O}]$

Propiedades

En general, dadas las funciones f y $g \in \bar{\mathbb{F}}_q(E)$, los divisores principales cumplen con las siguientes propiedades:

- $\mathsf{div}(f \cdot g) = \mathsf{div}(f) + \mathsf{div}(g)$
- $\mathsf{div}(f/g) = \mathsf{div}(f) - \mathsf{div}(g)$
- La función f es una constante, sí y sólo si $\mathsf{div}(f) = 0$

propiedades

Una función racional f puede ser evaluada en un divisor $\mathcal{D} = \sum_j a_j[P_j]$, a través de la siguiente fórmula:

$$f(\mathcal{D}) = \prod_{P_j \in \text{supp}(\mathcal{D})} f(P_j)^{a_j},$$

de tal manera que, para todo $n \in \mathbb{Z}$,

$$f(\mathcal{D})^n = f(n\mathcal{D}),$$

donde $n\mathcal{D} = \sum_j n \cdot a_j[P_j]$.

Definiciones varias

Reciprocidad de Weil

Sea $E/\mathbb{F}_q$ una curva elíptica, y $f, g \neq 0$ funciones racionales en $\bar{\mathbb{F}}_q(E)$ con soportes disjuntos, entonces:

$$f(\mathsf{div}(g)) = g(\mathsf{div}(f))$$

definiciones varias

Relación de equivalencia

Dos divisores $\mathcal{D}_1$, y $\mathcal{D}_2$ son linealmente equivalentes, $\mathcal{D}_1 \sim \mathcal{D}_2$, sí y sólo si $\mathcal{D}_1 - \mathcal{D}_2$ es un divisor principal, esto es,

$$\mathcal{D}_1 - \mathcal{D}_2 = \mathsf{div}(f), \quad \text{o bien} \mathcal{D}_1 = \mathcal{D}_2 + \mathsf{div}(f)$$

Miller

Función de Miller

Una función de Miller de longitud $s \in \mathbb{Z}$ denotada por $f_{s,R}$, es una función racional en $\bar{\mathbb{F}}_q(E)$ con divisor
$\text{div}(f_{s,R}) = s[R] - [sR] - (s-1)[\mathcal{O}]$.

Lemma

Sea $f_{s,R}$ una función de Miller, y sea v_R la función vertical que corta a la curva elíptica E en el punto R, para todo $a, b \in \mathbb{Z}$ se cumple que:

- $f_{a+b,R} = f_{a,R} \cdot f_{b,R} \cdot \ell_{aR,bR}/v_{(a+b)R}$
- $f_{ab,R} = f_{b,R}^{a} \cdot f_{a,bR}$
- $f_{1,R} = c$, donde c es una constante

Contenido, sección 2

Divisores

Emparejamiento de Weil

Emparejamiento de Weil

Emparejamiento de Weil

Sea $r > 1$ un número entero, y sean $\mathcal{D}_1$, y $\mathcal{D}_2$ divisores en una curva elíptica E con soportes disjuntos, es decir,

$$\text{supp}(\mathcal{D}_1) \cap \text{supp}(\mathcal{D}_2) = \emptyset,$$

existen dos funciones racionales f_1, y f_2 en E, tales que $\text{div}(f_1) = r\mathcal{D}_1$, y $\text{div}(f_2) = r\mathcal{D}_2$. El emparejamiento de Weil definido como

$$e_W(\mathcal{D}_1, \mathcal{D}_2) = \frac{f_1(\mathcal{D}_2)}{f_2(\mathcal{D}_1)},$$

es un emparejamiento bilineal no degenerado . . .

emparejamiento de Weil

Específicamente, dados los puntos $P \in \mathbb{G}_1$, y $Q \in \mathbb{G}_2$, f_1, y f_2 son funciones racionales en $\mathbb{F}_{p^k}(E)$ con divisores $\text{div}(f_1) = r[P] - r[\mathcal{O}]$, y $\text{div}(f_2) = r[Q] - r[\mathcal{O}]$, respectivamente, tal que $\mathcal{D}_1 \sim [P] - [\mathcal{O}]$, y $\mathcal{D}_2 \sim [Q] - [\mathcal{O}]$. Por lo tanto, el cálculo de $f_i(\mathcal{D}_i)$ toma valores en el grupo multiplicativo $\mathbb{F}^*_{p^k}$, y además, a través de la reciprocidad de Weil, se cumple que

$$\left(\frac{f_1(\mathcal{D}_2)}{f_2(\mathcal{D}_1)}\right)^r = \frac{f_1(r\mathcal{D}_2)}{f_2(r\mathcal{D}_1)} = \frac{f_1(\text{div}(f_2))}{f_2(\text{div}(f_1))} = 1,$$

es decir, $g = e_W(\mathcal{D}_1, \mathcal{D}_2)$ es un elemento en el subgrupo de las r-ésimas raíces primitivas de la unidad en $\mathbb{F}^*_{p^k}$.

emparejamiento de Weil

En los últimos años se han hecho distintas mejoras a los emparejamientos bilineales, por un lado, se ha demostrado que el cálculo de $f_1(\mathcal{D}_2)$ puede ser reemplazado por $f_1(Q)$, y del mismo modo $f_2(\mathcal{D}_1)$ por $f_2(P)$. Por otro lado, si p, y Q son puntos de torsión r, entonces:

$$\text{div}(f_1) = r[P] - r[\mathcal{O}] = r[P] - [rP] - (r-1)[\mathcal{O}]$$

y

$$\text{div}(f_2) = r[Q] - r[\mathcal{O}] = r[Q] - [rQ] - (r-1)[\mathcal{O}]$$

es decir, f_1, y f_2 se pueden expresar como las funciones de Miller $f_{r,P}$, y $f_{r,Q}$.

emparejamiento de Weil

Finalmente,

$$e_W : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T,$$

$$(Q, P) \mapsto \frac{f_{r,P}(Q)}{f_{r,Q}(P)}$$