Introducción a las curvas elípticas, hiperelípticas y libcurve

Eduardo Ruiz Duarte

Facultad de Ciencias UNAM

Octubre 28, 2009

Agenda

- Problema de logaritmo discreto en grupos cíclicos $\mathbb{Z}_p^*$
- Grupo aditivo en curvas elípticas
- Problema de logaritmo discreto en grupo $< E(\mathbb{K}), \oplus >$
- Divisores, grupo $Pic^0(\mathfrak{C})$ *y* $\mathbb{J}(\mathfrak{C})$
- Adición en divisores de curvas hiperelípticas g=2
- Software libre relacionado (OpenSSL, libcurve-beta)
- Conclusiones

Problema de logaritmo discreto

Definición del Problema de logaritmo discreto:
Sea $< G, * >$ cíclico , $|G| = n$, $b \in G$ y $< b >= G \Rightarrow \forall g \in G$
$g = b^k$, k entero y definimos el morfismo de grupos:

$$log_b : G \to \mathbb{Z}_n$$

$$g \mapsto [k]$$

de tal manera que $b^k = g \mod n$

Problema de logaritmo discreto

No existe hasta ahora un algoritmo para calcular esta k en tiempo polinomial dados g y b aunque existen cosas mas rápidas que "intentar todo" como $pollard - \rho$ o la criba de campo de funciones, criba numerica, etc.., también es muy rápido si usas tu computadora cuántica usando el algoritmo de Shor para el problema de logaritmo discreto y la transformada de fourier cuántica :p

Problema de logaritmo discreto

Una aplicación del problema de logaritmo discreto es intercambiar llaves a través de medios no seguros, Martin Hellman, Whitfield Diffie, Ralph Merkle pensaron en un algoritmo usando el problema de logaritmo discreto y no olvidemos a los que lo descubrieron antes pero por razones de secreto militar no podían publicarlo, Malcolm J. Williamson y James H. Ellis de Inglaterra en la GCHQ.

Protocolo Diffie-Hellman-Merkle-Ellis-Williamson

Alberto (A) quiere cifrar un mensaje a Berenice (B) pero necesitan un password en común, el problema es que no pueden comunicarse el password ya que podrían estar intervenidos, y Eulalio (E) podría estar capturando su tráfico
entonces:

- A y B se ponen de acuerdo en un $< \mathbb{Z}_p^*, * >$ y en un $g \in G$ tal que g es generador, (Nótese que E ya tiene esta información)
- A toma un $a \in \mathbb{Z}_p$, calcula $A_1 = g^a \mod p$ y manda A_1 a B
- B toma un $b \in \mathbb{Z}_p$, calcula $B_1 = g^b \mod p$ y manda B_1 a A
- A calcula $S_a = B_1^a \mod p$
- B calcula $S_b = A_1^b \mod p$
- $S_a = S_b$ ya que $S_a = (g^b)^a = S_b = (g^a)^b = g^{ab} = S$

Alberto y Berenice ya tienen un secreto S y no importa que Eulalio conozca A_1, B_1, p y g

Protocolo Diffie-Hellman-Merkle-Ellis-Williamson

Nótese que si usaramos DHMEW con el cíclico $< \mathbb{Z}_p, + >$ entonces el PLD sería trivial.
En $< \mathbb{Z}_p^*, * >$ la acción inducida es la exponenciación $(a * a * a = a^3)$ en cambio en $< \mathbb{Z}_p, + >$ es la multiplicación por un escalar, $(a + a + a = 3 \cdot a)$
Esto convierte al PLD en $< \mathbb{Z}_p, + >$ así:

$$log_b : G \to \mathbb{Z}_n$$

$$g \mapsto [k]$$

De tal manera que $b \cdot k = g$
E conoce b,g y p $\Rightarrow b^{-1} = b^{p-2} \mod p$ (Fermat $a^p \equiv a \mod p$)
lo cual hace que $k = g \cdot b^{-1} = g \cdot b^{p-2}$
Esto resuelve el problema de logaritmo discreto en este grupo aditivo :(

Curvas elípticas

Ahora, ¿Por qué no usar otros grupos ?

- Variedades abelianas en campos finitos
- Jacobianas de curvas hiperelípticas
- Jacobianas de otras curvas algebraicas

Curvas elípticas

Ahora definiremos el grupo abeliano aditivo de una curva elíptica,
Consideremos la curva $y^2 = x^3 + ax + b$ tal que la parte derecha no tiene raíces múltiples y $a, b \in \mathbb{K}$, $\mathbb{K} = \overline{\mathbb{K}}$
El conjunto:

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} \ / \ y^2 = x^3 + ax + b\} \cup \{\infty\}$$

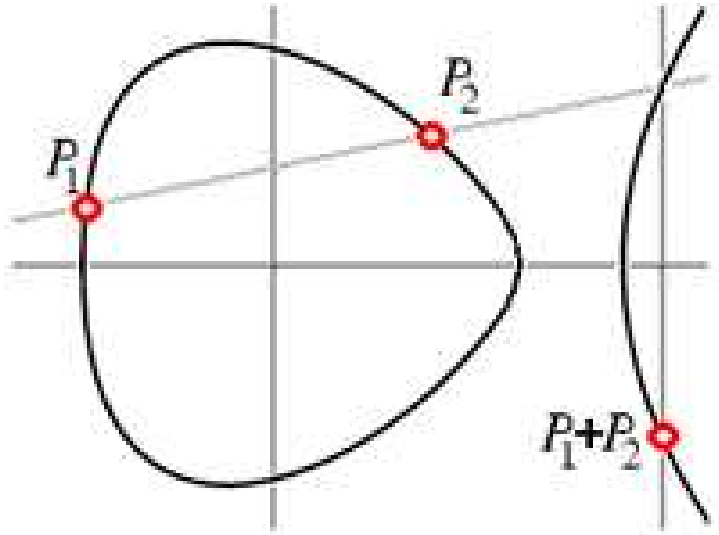
Forma un grupo abeliano, ∞ es un punto especial que nos hace ver la curva en su versión proyectiva
Ya que realmente este conjunto vive en $\mathbb{P}^2$

La adición $P \oplus Q$ y el inverso de P $(-P)$ con $P, Q \in E(\mathbb{K})$ cumplen lo siguiente:

- $P = \infty \Rightarrow -P = \infty$
- $P = (x, y) \Rightarrow -P = (x, -y)$
- P y Q con coordenada x distinta $\Rightarrow \exists\ \mathfrak{L}_{P,Q} \cap E(\mathbb{K}) \setminus \{P, Q\}$ (existe un tercer punto que intersecta la recta $\mathfrak{L}_{P,Q}$ con $E(\mathbb{K})$ que le llamaremos $-R$ (Bézout)) y entonces $P \oplus Q = R$
- $P = -Q \Rightarrow P \oplus Q = \infty$
- $P = Q$, nos tomamos $\mathfrak{L}_P$ tangente en P a la curva, esta línea interseca a la curva en otro punto $-R$, por lo tanto $P \oplus P = R$

Curvas elípticas

Ejemplo: $y^2 = x^3 - x$



Curvas elípticas

Si $y = \lambda x + b$ es la recta que pasa por P y Q, al intersectarla con $y^2 = x^3 + Ax + B$ obtenemos $P \oplus Q$, y si $P = Q$ obtenemos $P \oplus P$ derivando implícitamente la curva para así obtener:

Sean $P = (x_p, y_p),\ Q = (x_q, y_q)\ y\ R = (x_r, yr) \in E(\mathbb{K})$ tal que $car(\mathbb{K}) \neq 2$

- Si $P \neq Q$ (coordenada x distinta al menos) $P \oplus Q = R$ y
  $x_r = \lambda^2 - x_p - x_q$
  $y_r = \lambda(x_p - x_r) - y_p$
  $\lambda = \frac{y_q - y_p}{x_q - x_p}$
- Si $P = Q$
  $x_r = \lambda^2 - 2x_p$
  $y_r = \lambda(x_p - x_r) - y_p$
  $\lambda = \frac{3x_p^2 + A}{2y_p}$

PLD en curvas elípticas

Sea E una curva elíptica sobre $\mathbb{F}_q$ y $P \in E(\mathbb{F}_q)\backslash\{\infty\}$, computamos

$$Q = nP \text{ p.a n entero}$$

El problema de logaritmo discreto en curvas elípticas es que dado P y Q obtener n.

PLD en curvas elípticas

Regresemos a DHMEW pero ahora sobre curvas elípticas con el mismo contexto que tenian Alberto (A), Berenice (B) y Eulalio (E).

- A y B se ponen de acuerdo en un $E(\mathbb{F}_q)$ y un $G \in E(\mathbb{F}_q)$ tal que G es generador, asi como una n tal que $n < |E(\mathbb{F}_q)|$
- A toma un $z_a \in [1, n-1]$ y calcula $Q_a = z_a G$ y manda Q_a a B
- B toma un $z_b \in [1, n-1]$ y calcula $Q_b = z_b G$ y manda Q_b a A
- A calcula $S_a = z_a Q_b$
- B calcula $S_b = z_b Q_a$ Afirmamos que $S_a = S_b$ ya que

$$S_a = z_a Q_b = z_a(z_b G) = S_b = z_b Q_a = z_b(z_a G) = S$$

De esta manera los dos ya tienen S, en este caso pueden usar la coordenada x del punto S

PLD en curvas elípticas

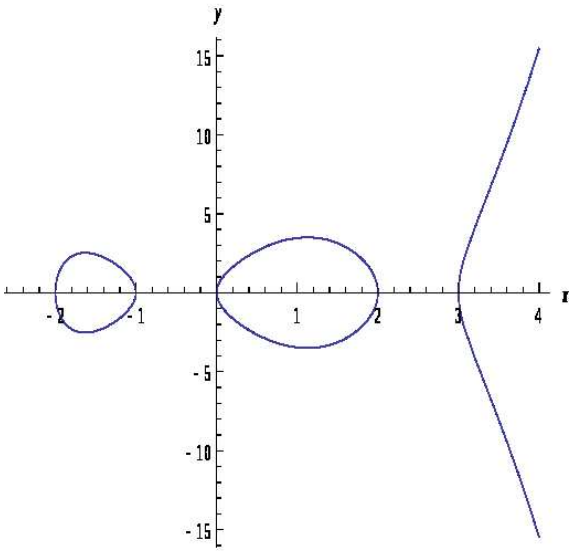
Existen muchas cosas a considerar para que esto sea seguro... solo mencionaré uno de los puntos mas importantes el cual es:
Si $|E(\mathbb{F}_q)| = q$ existe un morfismo de grupos

$$< E(\mathbb{F}_q), \oplus > \rightarrow < \mathbb{F}_q, + >$$

ya vimos que en el grupo aditivo, es trivial el problema de logaritmo discreto.
También hay una manera de dar el morfismo al grupo multiplicativo
Existen documentos del NIST que indican que curvas son las óptimas.

Divisores y grupo de Picard

Pero aquí, ¿Qué sucede utilizando la misma construcción geométrica? $y^2 = f(x)$ $Deg(f) = 5$



Aquí la linea que pasa por 2 puntos **no** necesariamente 'choca' con un único tercer punto viéndolo en $\mathbb{A}^2_{\mathbb{K}}$

Tendremos que definir una relación de equivalencia entre puntos y operar con las clases que nos permitan definir una operación binaria, para esto es lo que sigue.. divisores.

Divisores y grupo de Picard

Sea $\mathfrak{C}$ una curva suave y algebraica sobre $\mathbb{K}$.
Un divisor de $\mathfrak{C}$ es una suma formal finita:

$$D = \sum_{P \in \mathfrak{C}} n_P(P) \quad n_p \in \mathbb{Z}$$

Llamaremos $Div(\mathfrak{C})$ al conjunto de estos divisores.

Ejemplo:
$D_1 = 1(P) - 3(Q) + 2(R) + 3(S)$

Donde un número finito de coeficientes es no-cero

Divisores y grupo de Picard

La suma de divisores es así:
$D_1 = \sum_{P \in \mathfrak{C}} n_P(P)$
$D_2 = \sum_{P \in \mathfrak{C}} m_P(P)$

$$D_1 + D_2 = \sum_{P \in \mathfrak{C}} (n_P + m_P)(P)$$

Entonces $(Div(\mathfrak{C}), +)$ es un grupo con elemento neutro:

$$\mathcal{O} = \sum_{P \in \mathfrak{C}} 0(P)$$

El grado de un divisor es:
$\partial(D) = \sum_{P \in \mathfrak{C}} n_P$
Un subgrupo de $Div(\mathfrak{C})$ son los $X \in Div(\mathfrak{C})$ tal que $\partial(X) = 0$ el cual denotaremos como $Div^0(\mathfrak{C})$

Divisores y grupo de Picard

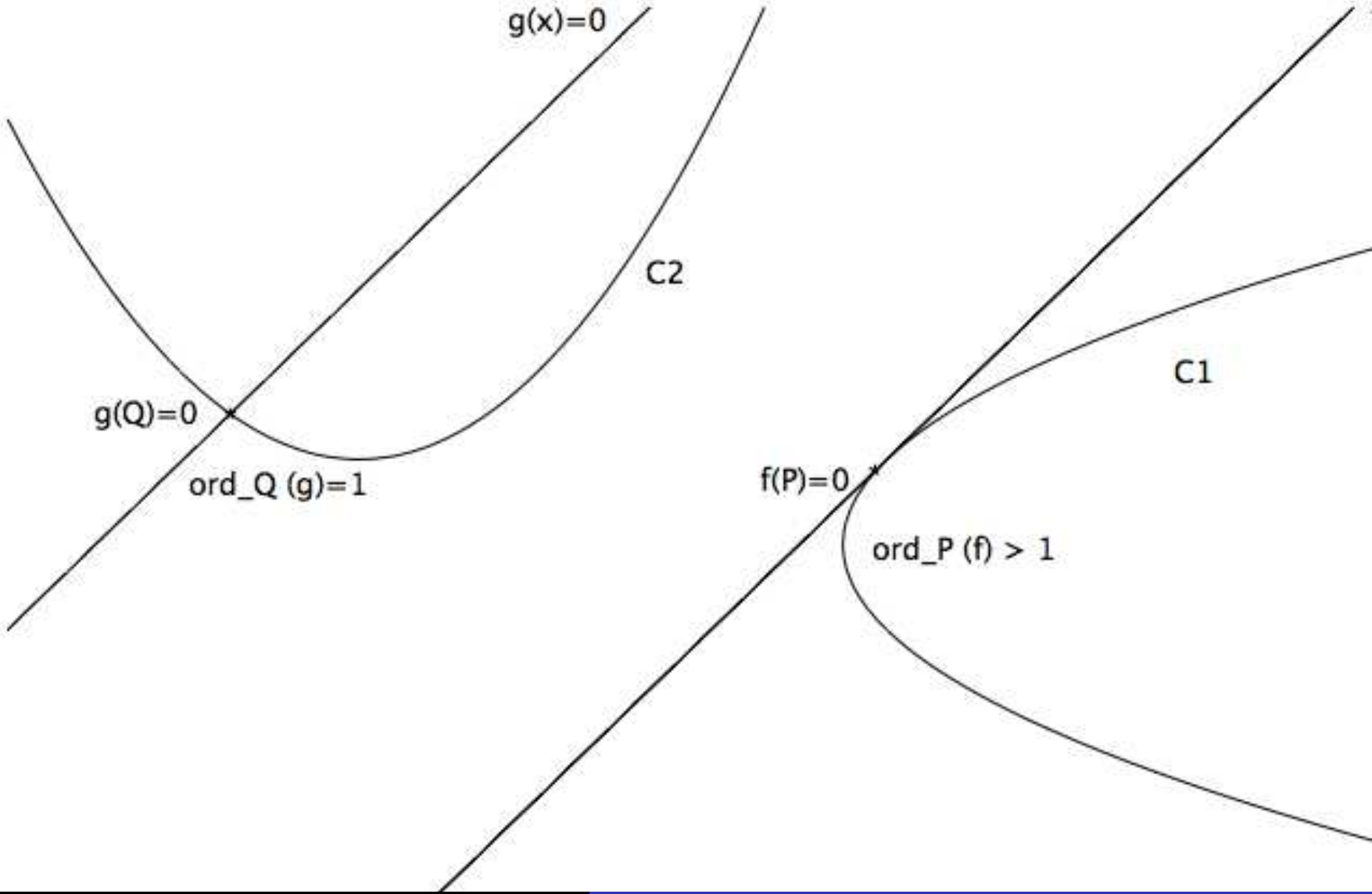
El divisor de una función $f \in \overline{\mathbb{K}}(\mathfrak{C})^*$ (campo de funciones racionales sobre $\mathfrak{C}$) es:

$Div(f) = \sum_{P \in \mathfrak{C}} ord_P(f)(P)$

Intuitivamente $ord_P(f)$ es una medida de la multiplicidad del cero de f, o sea la multiplicidad de la intersección de la curva $\mathfrak{C}$ con f=0
A estos divisores les llamamos divisores principales y los denotamos por $Princ(\mathfrak{C})$

Divisores y grupo de Picard

Intuitivamente así se define el orden en estos dos casos:



Divisores y grupo de Picard

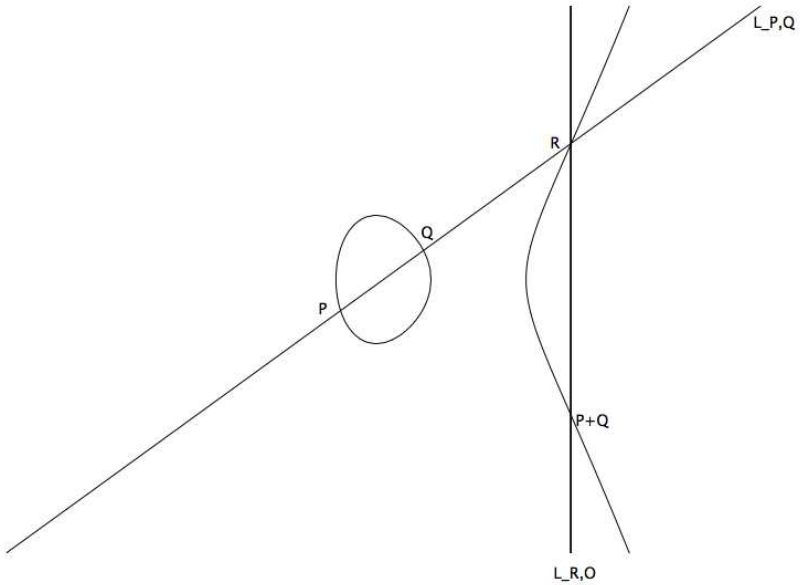
Estos divisores realmente lo que nos indican en sus coeficientes es que si bajo una una $f \in \overline{\mathbb{K}}(\mathfrak{C})^*$, P es un polo ($ord_P(f) < 0$) o P es un cero ($ord_P(f) > 0$)

Algunas propiedades de divisores principales sobre $\mathfrak{C}$ una curva suave algebraica sobre $\mathbb{K}$ y con $f, g \in \overline{\mathbb{K}}(\mathfrak{C})^*$

- $Div(f) = \mathcal{O} \Leftrightarrow f \in \overline{\mathbb{K}}^*$
- $\partial(Div(f)) = 0$
- $Div(f * g) = Div(f) + Div(g)$
- $Div(f/g) = Div(f) - Div(g)$
- $Div(f^n) = n \cdot Div(f) \quad \forall n \geq 1$
- $Div(f) = Div(g) \Leftrightarrow f = cg, c \in \overline{\mathbb{K}}^*$

Divisores y grupo de Picard

Ejemplo de divisores principales en $y^2 = x^3 - x$
(Con cuentas salen los $ord_{P_i}(\mathfrak{L})$ visto como el homogeneizado de $\mathfrak{L}$ en $\mathbb{P}^2$, esto es algebraicamente lo que vimos antes con geometría)
$Div(L_{P,Q}/Z) = (P) + (Q) + (R) - 3(\infty)$
$Div(L_{P\oplus Q,\infty}/Z) = (P \oplus Q) + (R) - 2(\infty)$
$Div(\frac{L_{P,Q}}{L_{P\oplus Q,\infty}}) = Div(L_{P,Q}) - Div(L_{P\oplus Q,\infty})$
$= (P) + (Q) - (P \oplus Q) - (\infty)$



Divisores y grupo de Picard

Vamos a dar una relación de equivalencia entre divisores para definir algo que nos pueda servir en criptografía

Sean $D_1, D_2 \in Div(\mathfrak{C})$
Si $D_1 - D_2 \in Princ(\mathfrak{C}) \Rightarrow D_1, D_2$ son linealmente equivalentes y $D_1 \sim D_2$
Ahora.. la relación de equivalencia en $Div^0(\mathfrak{C})$ forma el grupo $Pic^0(\mathfrak{C})$ (divisores módulo la equivalencia lineal) , en otras palabras:

$$Pic^0(\mathfrak{C}) = Div^0(\mathfrak{C})/Princ(\mathfrak{C})$$

Divisores y grupo de Picard

En curvas elípticas
$E(\mathbb{F}_q) \leftrightarrow Div^0(E)$
$P \mapsto (P) - (\infty)$
$\infty \mapsto \mathcal{O} = (\infty) - (\infty)$

Esto nos dice que $E \leftrightarrow Pic^0(E)$ y $P \rightarrow ((P) - (\infty))$ por lo tanto $((P) - (\infty))$ representa a P,
Esto nos dice que con las curvas elípticas se construye el grupo 'tal cual', los divisores principales son las rectas que pasan por los representantes de (P) y (Q) que definen un único punto
$R \rightarrow (R) - (\infty)$

Divisores y grupo de Picard

Teorema: Sea $\mathfrak{C}$ una curva algebraica de género g suave sobre un campo algebraicamente cerrado $\Rightarrow \exists$ una variedad abeliana $\mathbb{J}(\mathfrak{C}) \cong Pic^0(\mathfrak{C})$, donde $\mathbb{J}(\mathfrak{C})$ es la jacobiana de $\mathfrak{C}$

Adición en curvas hiperelípticas

Rápidamente con el siguiente teorema clasificamos a los divisores de una curva de género g:
Def: Una curva hiperelíptica de género g es de la forma
$y^2 + h(x)y = f(x), h, f \in \mathbb{K}[x], \quad Deg(f) = 2g + 1, \quad Deg(h) \leq g$
y f mónico

En este caso nos interesa que no tenga puntos singulares, o sea que no se anule el gradiente y la curva en algún punto.

Teorema: Sea $\mathfrak{C}$ una curva hiperelíptica de género g sobre $\mathbb{K}$ entonces cada clase de divisores se puede representar de manera única como:

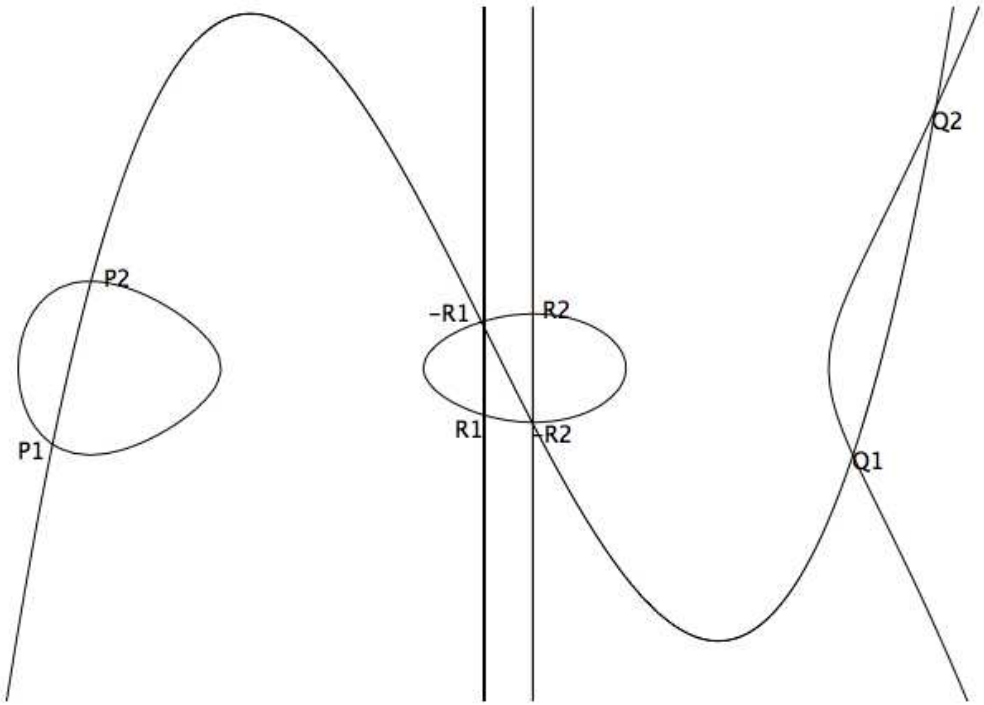
$$\sum_{1 \leq i \leq r} (P_i) - r(\infty)$$

donde $r \leq g, P_i \neq \infty$

Adición en curvas hiperelípticas

Veámoslo geométricamente con un ejemplo: Por geometría sabemos que en esta curva con $g = 2$ dados P_1, P_2, Q_1, Q_2 podemos encontrar una cúbica que pasa por esos 4 puntos que al sustituir en la curva $\mathfrak{C}$ nos darán 6 puntos De los cuales ya conocemos 4, los otros dos los proyectamos con ∞ y obtenemos a los representantes del nuevo divisor .

$$(P_1) + (P_2) - 2(\infty) + (Q_1) + (Q_2) - 2(\infty) = (R_1) + (R_2) - 2(\infty)$$



Divisores y grupo de Picard

En resumen para construir el grupo de Picard hacemos:

- Escoges una curva suave $\mathfrak{C}$ algebraica
- Buscas los divisores de orden cero $Div^0(\mathfrak{C})$
- Consideras relación de equivalencia lineal entre divisores
- Defines el representante de cada clase de divisores

Software libre para curvas elípticas

OpenSSL (www.openssl.org):

Listar curvas:
openssl ecparam -list_curves

Crear una llave privada:
openssl ecparam -out eckey.pem -name prime192v1 -genkey

Calcular la coordenada 'y' del punto de una llave de manera comprimida (Legendre)
openssl ecparam -in ecin.pem -out ecout.pem -conv_form compressed

Software libre para curvas elípticas

libcurve (http://math.co.ro/coloquio)
Rutinas en C para libcurve listas para usarse:
typedef struct point {
bint *x,*y;
int infinity; } point_t;
void lecc_initialize_parameters (void)
void lecc_point_normalize(point_t *)
void *lecc_point_alloc (void)
void lecc_point_print (point_t *, char *)
void lecc_point_free (point_t *)
void lecc_point_copy (point_t *, point_t *)
void lecc_point_clean (point_t *)
void lecc_point_double (point_t * , point_t *)
void lecc_point_add (point_t *, point_t *, point_t *)
void lecc_point_scalar_mul (bint * k, point_t * a, point_t * dst)
void lecc_point_scalar_mul_long (long k, point_t * a, point_t * dst)
void lecc_message_to_point (bint * x, point_t * Q) (Neal Koblitz)

Conclusiones

- Curvas elípticas son interesantes pero hay que investigar más curvas y estudiar el problema de logaritmo discreto en ellas
- Las curvas elípticas son una importante herramienta en matemáticas, las formas modulares de éstas probaron uno de los teoremas más importantes de la historia
- La criptografía con curvas hiperelípticas bien implementada es muy rápida
- Las curvas elípticas/hiperelípticas bien escogidas generan grupos donde los ataques al problema de logaritmo discreto son exponenciales, por lo tanto las llaves seguras se alcanzan con tan solo 160 bits

¡Gracias! Eduardo Ruiz Duarte

beck@math.co.ro

http://math.co.ro

Referencias y mas información en:

- Elliptic curves in cryptography - Ian Blake, Gadiel Seroussi, Nigel Smart
- Elliptic and hyperelliptic curve cryptography - Henri Cohen, Grehard Frey, Tanja Lange
- The arithmetic of elliptic curves - Joseph H. Silverman
- Software and hardware implementation of hyperelliptic curve cryptosystems - Thomas Wollinger
- Generalized Jacobians in cryptography - Isabelle Déchenè
- Guide to Elliptic curve cryptography - Alfred Menezes, Scott Vanstone, Darrel Hankerson
- A Course in number theory and cryptography - Neal Koblitz
- Elementary algebraic geometry - Klaus Hulek
- Algebraic Aspects of cryptography - Neal Koblitz, Alfred Menezes (Appendix, Hyperelliptic curves)