Capítulo 6

Curvas elípticas

6.1. Introducción

En este capítulo presentaremos los aspectos de la teoria de las curvas elípticas que son los más relevantes para la criptografia. Para una exposición más detallada del tema ver [12],[64],[92],[93],[95], [100].

6.2. Ecuaciones de Weierstrass

Sea F un campo, $\bar{F}$ su cerradura algebraica y F^* su grupo multiplicativo. En general, una curva elíptica sobre un campo F es el conjunto de puntos en el plano proyectivo $\mathbb{P}^2(\bar{F})$ que satisfacen una ecuación de la forma:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{6.1}$$

incluyendo a $\mathcal{O} = [0, 1, 0]$, donde $a_1, \cdots, a_6 \in \bar{F}$ (ver [92, 93]).

Utilizando coordenadas no-homogeneas

$$\begin{aligned} x &= X/Z \\ y &= Y/Z, \end{aligned}$$

la ecuación anterior se transforma en:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6.2}$$

la cual es denominada *Forma Normal de Weierstrass (FNW)*[95].

El valor

$$\Delta = -4a_2^3a_6 + a_2^2a_4^2 + 18a_2a_4a_6 - 4a_4^3 - 27a_6^2 \tag{6.3}$$

es denominado el *discriminante* de la ecuación. Puede mostrarse [95] que si $\alpha_1, \alpha_2, \alpha_3$ son las raices del polinomio cúbico en el lado derecho de (6.2), entonces

$$\Delta = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

y por lo tanto, si las raices son diferentes, $\Delta \neq 0$. Por esta razón, si $\Delta \neq 0$ la curva elíptica es *no singular*.

A partir de la Forma Normal de Weierstrass es posible encontrar formas particulares para la ecuación de la curva dependiendo de la característica del campo subyacente, tal como se detalla en la siguiente proposición.

Teorema 6.1 *Sea E/F una curva sobre el campo F dada por la ecuación de Weierstrass. Entonces, bajo las hipótesis en los recuadros, existe una substitución:*

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

donde $u \in \bar{F}$ y $r, s, t \in F$, tal que E/F tiene una ecuación de Weierstrass de la forma indicada.

1. $\boxed{car\ F \neq 2, 3}$

$$\begin{aligned} y^2 &= x^3 + a_4x + a_6 \\ \Delta &= -16(4a_4^3 + 27a_6^2) \\ j &= 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2} \end{aligned}$$

2. $\boxed{car\ F = 3\ y\ j(E) \neq 0}$

$$\begin{aligned} y^2 &= x^3 + a_2x^2 + a_6 \\ \Delta &= -a_2^3a_6 \\ j &= -a_2^3/a_6 \end{aligned}$$

$\boxed{car\ F = 3\ y\ j(E) = 0}$

$$\begin{aligned} y^2 &= x^3 + a_4x + a_6 \\ \Delta &= -a_4^3 \\ j &= 0 \end{aligned}$$

3. $\boxed{car\ F = 2\ y\ j(E) \neq 0}$

$$\begin{aligned} y^2 + xy &= x^3 + a_2x^2 + a_6 \\ \Delta &= a_6 \\ j &= 1/a_6 \end{aligned}$$

$\boxed{car\ F = 2\ y\ j(E) = 0}$

$$\begin{aligned} y^2 + a_3y &= x^3 + a_4x + a_6 \\ \Delta &= a_3^4 \\ j &= 0 \end{aligned}$$

Demostración

1. Partiendo de la FNW

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Si $car(\bar{F}) \neq 2$, se puede completar el cuadrado substituyendo y por $\frac{1}{2}(y - a_1x - a_3)$, quedando la ecuación:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

donde

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \end{aligned}$$

Si $car(\bar{F}) \neq 2, 3$, sustituyendo (x, y) por $((x - 3b_2)/36, y/216)$ se tiene

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

2. Tomando la FNW y completando el cuadrado a la izquierda

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

Si $j = 0$ entonces $a_2 = 0$ y se tiene

$$y^2 = x^3 + a_4x + a_6$$

Si $j \neq 0$, entonces $a_2 \neq 0$, y substituyendo $x = x' + a_4/a_2$ eliminamos el término lineal.

3. Partiendo de la FNW

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

donde el j-invariante está dado por

$$j = a_1^{12}/\Delta$$

Si $j \neq 0$, entonces $a_1 \neq 0$ y por lo tanto

$$\begin{aligned} x &= a_1^2x' + a_3/a_1 \\ y &= a_1^3y' + (a_1^4a_4 + a_3^2)/a_1^3 \end{aligned}$$

nos da una ecuación de la forma deseada. Similarmente, si $j = a_1 = 0$ entonces

$$\begin{aligned} x &= x' + a_2 \\ y &= y' \end{aligned}$$

nos proporciona la ecuación deseada.

□

El j-invariante, $j(E)$, de la curva está estrechamente relacionado al *isomorfismo de curvas elípticas*. Dos curvas elípticas definidas por ecuaciones de Weierstrass E (con variables X, Y) y E' (con variables X', Y') son isomorfas sobre F sí y solamente si existen constantes $r, s, t \in F$ y $u \in F^*$, tales que el cambio de variables

$$\begin{aligned} X &= u^2X' + r \\ Y &= u^3Y' + su^2X' + t \end{aligned}$$

transforma E en E'. El isomorfismo de curvas es una relación de equivalencia, y el j-invariante caracteriza a las clases de equivalencia en esta relación. Esto es, dos curvas elípticas que son isomorfas sobre F tiene el mismo j-invariante y recíprocamente, dos curvas con el mismo j-invariante son isomorfas sobre F [92].

6.3. Estructura de grupo de una curva elíptica

Sea E una ecuación en la *forma normal de Weierstrass* definida sobre el campo F. Entonces $E \subset F^2$ es el conjunto de puntos $P = (x, y)$ que satisfacen la ecuación junto con el punto $\mathcal{O} = [0, 1, 0]$ al infinito. Sea $L \subset F^2$ una linea. Entonces dado que la ecuación tiene grado 3, L intersecta a E en exactamente 3 puntos, digamos P, Q, R.

Ley de composición. Sean $P, Q \in E$, L la linea que pasa por P y Q (linea tangente a E en el caso en que $P = Q$) y R el tercer punto de intersección de L con E. Sea L' la linea que conecta R y $\mathcal{O}$. Entonces $P \oplus Q$ es el punto tal que L' intersecta E en R,$\mathcal{O}$ y $P \oplus Q$.

Teorema 6.2 *La ley de composición tiene las siguientes propiedades:*

1. *Si una linea L intersecta a E en los puntos (no necesariamente distintos) P, Q y R, entonces*

$$(P \oplus Q) \oplus R = \mathcal{O}$$

2. *$P \oplus \mathcal{O} = P$ para toda $P \in E$.*

3. *$P \oplus Q = Q \oplus P$ para toda $P, Q \in E$.*

4. *Sea $P \in E$. Existe un punto de E, denotado $\ominus P$, tal que*

$$P \oplus (\ominus P) = \mathcal{O}$$

   .

5. *Sean $P, Q, R \in E$. Entonces*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$$

   En otras palabras, la ley de composición hace de E un grupo abeliano con elemento identidad $\mathcal{O}$.

6. *Supóngase que E está definida sobre F. Entonces*

   $$E(F) = \{(x, y) \in F^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

   es un subgrupo de E.

Para una demostración del teorema anterior, ver [92]. En la discusión posterior, dado que las propiedades de la operación $\oplus$ son similares a las de la adición, la denotaremos por simplicidad como $+$ y de igual forma, el inverso aditivo de P, $\ominus P$, se denotará como $-P$.

6.4. Cálculo de operaciones de grupo

Sea E una curva elíptica sobre el campo F dada por:

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad (6.4)$$

donde $a_i \in F$ y sea $P_0 = (x_0, y_0) \in E$. Tomemos la línea L que pasa a través de P_0 y $\mathcal{O}$,

$$L : x - x_0 = 0.$$

Substituyendo esta en la ecuación para E, podemos ver que el polinomio cuadrático $f(x_0, y)$ tiene raices y_0 y $y_0' \in F$, donde $-P_0 = (x_0, y_0')$. Escribiendo

$$f(x_0, y) = c(y - y_0)(y - y_0')$$

y comparando los coeficientes de y^2 tenemos que $c = 1$, y entonces comparando los coeficientes de y obtenemos $y_0' = -y_0 - a_1x_0 - a_3$. De donde

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ puntos de E. Si $x_1 = x_2$ y $y_1 + y_2 + a_1x + a_3 = 0$ entonces $P_1 + P_2 = \mathcal{O}$. De otro modo, la línea L que pasa a través de P_1 y P_2 (línea tangente a E si $P_1 = P_2$) tiene una ecuación de la forma

$$L : y = \lambda x + \nu.$$

Substituyendo en la ecuación para E, vemos que $f(x, \lambda x + \nu)$ tiene raices x_1, x_2, $x_3 \in F$, donde $P_3 = (x_3, y_3)$ es el tercer punto de $L \cap E$. Entonces

$$P_1 + P_2 + P_3 = \mathcal{O}$$

y por otro lado, escribiendo

$$f(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$$

e igualando coeficientes para x^3 y x^2 tenemos que $c = -1$ y

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

Esto nos dá una formula para x_3, y substituyendo en la ecuación para L tenemos $y_3 = \lambda x_3 + \nu$. Finalmente, para encontrar $P_1 + P_2 = -P_3$, aplicamos la fórmula de la negación arriba establecida a P_3.

Entonces, podemos resumir las fórmulas para las operaciones de grupo de la siguiente manera:

Cálculo de las operaciones de grupo. Sea E una curva elíptica dada por la ecuación de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

1. Sea $P_0 = (x_0, y_0) \in E$. Entonces

$$-P_0 = (x_0, -y_0 - a_1 x_0 - a_3).$$

Ahora, sea $P_1 + P_2 = P_3$ con $P_1, P_2, P_3 \in E$

2. Si $x_1 = x_2$ y $y_1 + y_2 + a_1 x_2 + a_3 = 0$, entonces

$$P_1 + P_2 = \mathcal{O}.$$

De otra forma, sean

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ \nu &= \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \end{aligned}$$

si $x_1 \neq x_2$, y si $x_1 = x_2$

$$\begin{aligned} \lambda &= \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \\ \nu &= \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3} \end{aligned}$$

3. $P_3 = P_1 + P_2$ está dado por

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3. \end{aligned}$$

En las secciones siguientes deduciremos formulas más simples tanto para la ecuación de la curva como de las operaciones de grupo en el caso de campos subyacentes particulares como son $GF(p)$ y $GF(2^m)$.

6.5. Curvas elípticas sobre $GF(p)$

Sea $GF(p)$ un campo finito de característica $p \neq 2, 3$, y sean $a, b \in GF(p)$ tales que satisfacen la desigualdad $4a^3 + 27b^2 \neq 0$. Una *curva elíptica* $E_{(a,b)}$ sobre $GF(p)$ se define como el conjunto de puntos $(x, y) \in GF(p) \times GF(p)$ que satisfacen la ecuación

$$y^2 = x^3 + ax + b \tag{6.5}$$

junto con un punto especial $\mathcal{O}$, denominado el *punto al infinito*. Los puntos de la curva forman un grupo abeliano bajo la operación aditiva definida de la siguiente forma.

Sea $E_{(a,b)}$ una curva elíptica sobre $GF(p)$ y sean P y Q dos puntos sobre $E_{(a,b)}$. Se tiene que $P + \mathcal{O} = \mathcal{O} + P = P$. Sean $P = (x_1, y_1)$ y $Q = (x_2, y_2)$. Entonces $-P = (x_1, -y_1)$ y $P + (-P) = \mathcal{O}$. Si $Q \neq -P$ entonces $P + Q = (x_3, y_3)$ donde

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$

y

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{si } P \neq Q \\ (3x_1^2 + a)/(2y_1) & \text{si } P = Q \end{cases}$$

Ejemplo 6.1 *Curva elíptica sobre* $GF(23)$. Sea $p = 23$ y considérese la curva elíptica $E : y^2 = x^3 + x + 1$ definida sobre $GF(23)$. Obsérvese que $4a^3 + 27b^2 = 4 + 27 = 31 \equiv 8 \pmod{23}$. Los puntos en E son $\mathcal{O}$ y los siguientes:

(0,1) (0,22) (1,7) (1,16) (3,10) (3,13) (4,0)
(5,4) (5,19) (6,4) (6,19) (7,11) (7,12) (9,7) (9,16)
(11,3) (11,20) (12,4) (12,19) (13,7) (13,16) (17,3) (17,20)
(18,3) (18,20) (19,5) (19,18).

El grupo E tiene 28 puntos (incluyendo al punto al infinito $\mathcal{O}$). Los siguientes son ejemplos de operaciones en el grupo:

1. Sean $P_1 = (x_1, y_1) = (3, 10)$, $P_2 = (x_2, y_2) = (9, 7)$, $P_1 + P_2 = (x_3, y_3)$. Tenemos que:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{7 - 10}{9 - 3} = \frac{-3}{6} = 11,$$

$$x_3 = \lambda^2 - x_1 - x_2 = 11^2 - 3 - 9 = 6 - 3 - 9 = -6 = 17,$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 11(3 - 17) - 10 = 11(9) - 10 = 89 = 20.$$

   Por lo tanto, $P_1 + P_2 = (17, 20)$.

2. Sea $P_1 = (x_1, y_1) = (3, 10)$, $2P_1 = (x_3, y_3)$. Entonces

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(3^2) + 1}{20} = \frac{5}{20} = \frac{1}{4} = 6,$$

$$x_3 = \lambda^2 - 2x_1 = 6^2 - 6 = 30 = 7,$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 6(3 - 7) - 10 = -24 - 10 = -11 = 12.$$

   Entonces $2P_1 = (7, 12)$.

6.6. Curvas elípticas sobre $GF(2^m)$

Ahora consideraremos a las curvas elípticas definidas sobre campos de característica 2. Sea $GF(2^m)$ tal campo finito para alguna $m \geq 1$.

Una *curva elíptica* $E_{(a,b)}$ sobre $GF(2^m)$ se define como el conjunto de puntos $(x, y) \in GF(2^m) \times GF(2^m)$ que son soluciones de la ecuación

$$y^2 + xy = x^3 + ax + b \tag{6.6}$$

donde $a, b \in GF(2^m)$ y $b \neq 0$, junto con el punto al infinito, $\mathcal{O}$.

Sea $E_{(a,b)}$ una curva elíptica sobre $GF(2^m)$. Sea $P = (x_1, y_1)$ un punto sobre $E_{(a,b)}$. Definimos $-P$ como $(x_1, x_1 + y_1)$, de modo que $P + (-P) = (-P)+P = \mathcal{O}$. Ahora supongamos que P y Q son diferentes de $\mathcal{O}$ y $Q \neq -P$. Sean $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ entonces $P + Q = (x_3, y_3)$ donde

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + x_1 + x_2 + a \\ y_3 &= \lambda(x_1 - x_3) + x_3 + y_1, \end{aligned}$$

y

$$\lambda = \begin{cases} (y_2 + y_1)/(x_2 + x_1) & \text{si } P \neq Q \\ (x_1^2 + y_1)/x_1 & \text{si } P = Q \end{cases}$$

Los puntos de la curva forman un grupo abeliano bajo la operación aditiva definida de esta forma.

Ejemplo 6.2 *Curva elíptica sobre* $GF(2^4)$. Considérese $GF(2^4)$ representado por el trinomio irreducible $f(x) = x^4+x+1$ (ver ejemplo 5.3). Considérese la curva elíptica $E : y^2 + xy = x^3 + \alpha^4 x^2 + 1$ sobre $GF(2^4)$. Los puntos en E son $\mathcal{O}$ y los siguientes:

$(0, 1)$	$(1, \alpha^6)$	$(1, \alpha^{13})$	(α^3, α^8)	(α^3, α^{13})
(α^5, α^3)	(α^5, α^{11})	(α^6, α^8)	(α^6, α^{14})	(α^9, α^{10})
(α^9, α^{13})	(α^{10}, α)	(α^{10}, α^8)	$(\alpha^{12}, 0)$	$(\alpha^{12}, \alpha^{12})$.

Si $P = (\alpha^6, \alpha^8)$ y $Q = (\alpha^3, \alpha^{13})$, entonces algunos ejemplos de operaciones aritméticas son los siguientes:

- $P + Q = (1, \alpha^{13})$.
- $2P = (\alpha^{10}, \alpha^8)$.

Ejemplo 6.3 *Curva elíptica sobre* $GF(2^{163})$. Considérese la representación de $GF(2^{163})$ en base polinomial dada en el ejemplo 5.4. Tomemos la curva sobre $GF(2^{163})$ definida por la ecuación

$$y^2 + xy = x^3 + x^2 + 1.$$

Esta curva es la denominada curva K-163 incluida en la relación de curvas elípticas recomendadas por el NIST para aplicaciones criptográficas [73]. Un punto sobre la curva es el punto de coordenadas:

$$G_x = 0x8eee49c5e5d6e4ed397d70aaca11cbb7350c31ef2$$

$$G_y = 0x9d3aadcc835d635008e2f12385ff83d50bf070982$$

cuyo orden es:

$$5846006549323611672814741753598448348329118574063.$$

El resultado de $P = 2G$ es:

$$0xbe14c5a8d828b77a24b00bfcaa003ef8372ac5bc$$
$$0xb6afefe515466696a3af5d3dca09f58ba9e97c922$$

El valor de $Q = P + G$ es:

$$0x02596f02bd330028f4208282f3e8fa2a9ccfcfca2$$
$$0x4efdceff9014085e41fd71c4b7cdab519f74c9275$$

El resultado de $P = -G$ es:

$$0x8eee49c5e5d6e4ed397d70aaca11cbb7350c31ef2$$
$$0x13d4e409668b87bd319f81894fee48623efc4177$$

Sea k_1 el entero aleatorio:

$$372897787406025110559828689773387838153511823425 8$$

y sea k_2 el entero aleatorio:

$$2211754861024375336142134678017244734940075421768$$

El resultado de $k2 * (k1 * P)$ es:

$$0xd9db11c518586ff98171617aa4530bf09af9ef304$$

$$0xde61eb1ea4a53fd536e4925fc62cd71094f163124$$

El resultado de $k1 * (k2 * P)$ es:

$$0xd9db11c518586ff98171617aa4530bf09af9ef304$$

$$0xde61eb1ea4a53fd536e4925fc62cd71094f163124$$

Todos los cálculos de esta sección han sido realizados utilizando la implementación de la aritmética de puntos de curvas elípticas cuyo código se presenta en el apéndice A.

Figura 6.1: Descripción geométrica de la suma $P + Q = R$

6.7. Interpretación gráfica de la aritmética de puntos sobre curvas elípticas

Las operaciones anteriormente definidas para los puntos sobre una curva elíptica tienen una interpretación gráfica directa.

Haciendo referencia a la figura 6.1, si P y Q son dos puntos sobre la curva, al trazar una recta que pase por P y Q, ésta se intersecta en la curva elíptica en un tercer punto. Si R es la reflexión de este último punto respecto al eje X, entonces $R = P + Q$.

De igual forma, si P es un punto sobre la curva, como se ilustra en la figura 6.2, la tangente a la curva que pasa por P se intersecta en la curva en un segundo punto. Si R es la reflexión de este punto respecto al eje X, entonces $R = 2P$.

6.8. Propiedades fundamentales

Orden del Grupo. Sea E una curva elíptica sobre un campo finito $GF(q)$. El teorema de Hasse (ver demostración en [92]) establece que el número de puntos sobre una curva elíptica (incluyendo el punto al infinito) es

$$|E| = q + 1 - t \tag{6.7}$$

donde $|t| \leq 2\sqrt{q}$; $|E|$ es llamado el *orden* de la curva y t es denominada la *traza* de E. En otras palabras, el orden de una curva elíptica es aproximada-

Figura 6.2: Descripción geométrica de la duplicación $2 \cdot P = R$

mente igual al tamaño q del campo subyacente. [1]

Sean E una curva elíptica y P un punto sobre la curva. Si n es un entero positivo, definimos a la *potencia n de P*, denotada por nP, como

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ veces}}.$$

Si P es un punto sobre E, definimos al *orden de P*, denotado por $ord(P)$, como al menor entero n tal que $nP = \mathcal{O}$. Puede observarse que si $n = ord(P)$ y $k_1 \equiv k_2 \pmod{n}$ entonces $k_1 P = k_2 P$.

Estructura del Grupo. Una curva elíptica E forma un grupo abeliano de rango 1 o 2. Esto es, E es isomorfo a $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, donde n_1 divide a n_2, y $\mathbb{Z}_n$ denota al grupo cíclico de orden n. Más aun, n_2 divide a $q - 1$. Si $n_2 = 1$, entonces se dice que E es *cíclica*. En este caso E es isomorfa a $\mathbb{Z}_{n_1}$, y existe un punto $P \in E$ tal que

$$E = \{kP \ : \ 0 \leq k \leq n_1 - 1\}.$$

Al punto P se le denomina *generador* de E.

Ejemplo 6.4 *Curva elíptica cíclica.* Considérese la curva elíptica E sobre $GF(23)$ definida por la ecuación

$$y^2 = x^3 + x + 4.$$

[1] Para una exposición más detallada, ver [64].

Dado que $|E| = 29$, el cual es primo, E es cíclico y cualquier punto diferente a $\mathcal{O}$ es un generador de E. Por ejemplo, $P = (0, 2)$ es un generador como se muestra a continuación:

$1P = (0, 2)$	$2P = (13, 12)$	$3P = (11, 9)$	$4P = (1, 12)$
$5P = (7, 20)$	$6P = (9, 11)$	$7P = (15, 6)$	$8P = (14, 5)$
$9P = (4, 7)$	$10P = (22, 5)$	$11P = (10, 5)$	$12P = (17, 9)$
$13P = (8, 15)$	$14P = (18, 9)$	$15P = (18, 14)$	$16P = (8, 8)$
$17P = (17, 14)$	$18P = (10, 18)$	$19P = (22, 18)$	$20P = (4, 16)$
$21P = (14, 18)$	$22P = (15, 17)$	$23P = (9, 12)$	$24P = (7, 3)$
$25P = (1, 11)$	$26P = (11, 14)$	$27P = (13, 11)$	$28P = (0, 21)$
$29P = \mathcal{O}$			

6.9. Logaritmo discreto sobre curvas elípticas

Sean E una curva elíptica sobre un campo finito $GF(q)$, un punto $P \in E$ de orden n y un punto $Q \in E$, el *problema del logaritmo discreto sobre curvas elípticas* consiste en encontrar un entero k, $0 \leq k \leq n - 1$, suponiendo que existe, tal que $Q = kP$.

Los algoritmos conocidos a la fecha para resolver el problema del logaritmo discreto sobre curvas elípticas (PLDCE) son los siguientes:

1. Busqueda Exhaustiva. Por este método, simplemente se calculan los múltiplos sucesivos de P: $P, 2P, 3P, \ldots$ hasta que se obtiene Q. Este método puede tomar hasta n pasos en el peor caso.

2. Algoritmo de Pohlig-Hellman. En el algoritmo propuesto por Pohlig y Hellman [79], se utiliza la factorización de n, el orden de P. El algoritmo reduce el problema de encontrar k al problema de encontrar k módulo los factores primos de n; el número k puede entonces determinarse usando el teorema chino del residuo.

   Por lo tanto, para construir la instancia más difícil del PLDCE, se debe seleccionar una curva elíptica cuyo orden sea divisible por un primo grande n. De preferencia, este orden debe ser un primo o casi un primo, es decir, un primo grande n por un entero pequeño h. En la discusión restante, supondremos que el orden n de P es primo.

3. Algoritmo de Paso-Enano Paso-Gigante. Este algoritmo representa un compromiso tiempo-espacio en el algoritmo de búsqueda exhaustiva [3]. Requiere del almacenamiento de aproximadamente $\sqrt{n}$ puntos, y su tiempo de ejecución es aproximadamente de $\sqrt{n}$ pasos en el peor caso.

4. Algoritmo Rho de Pollard. Este algoritmo, debido a Pollard [80], es una versión aleatorizada del algoritmo de paso-enano paso-gigante. Tiene aproximadamente el mismo tiempo esperado de ejecución ($\sqrt{\pi n/2}$ pasos) que dicho algoritmo, pero a diferencia de este no requiere de almacenamiento significativo.

   Se ha mostrado [31][105] que es posible acelerar al algoritmo rho de Pollard por un factor de $\sqrt{2}$; por lo tanto, el tiempo de ejecución del algoritmo es $O((\sqrt{\pi n})/2)$.

5. Algoritmo Rho Paralelizado. Van Oorschot y Wiener [103] han demostrado que el algoritmo rho de Pollard puede ser paralelizado de modo que cuando el algoritmo es ejecutado en paralelo en r procesadores, el tiempo esperado de ejecución es de $(\sqrt{\pi n})/(2r)$ pasos.

6. Algoritmo Lambda de Pollard. Este es otro algoritmo aleatorio propuesto por Pollard [80]. Al igual que el algoritmo rho, puede ser paralelizado con una aceleración lineal. El algoritmo lambda paralelizado es ligeramente más lento que el algoritmo rho paralelizado [103]. El algoritmo lambda es sin embargo más rápido en situaciones en las cuales se conoce de antemano que el logaritmo buscado se encuentra en el subintervalo $[0, b]$ de $[0, n-1]$, donde $b < 0{,}39n$ [103].

7. Logaritmos Múltiples. Se ha observado [96] que si una sola instancia del PLDCE, para una curva elíptica E dada y un punto base P, es resuelta utilizando el algoritmo rho de Pollard paralelizado, entonces el trabajo realizado para resolver esta instancia puede utilizarse para encontrar solución a otras instancias del PLDCE (con la misma curva E y punto base P) más rápidamente. De manera más precisa, si la primera instancia fue resuelta en un tiempo t, entonces la segunda instancia tendrá un tiempo esperado de $(\sqrt{2}-1)t \approx 0{,}41t$. Teniendo resueltas las dos primeras instancias, la tercera tomaría un tiempo estimado de $(\sqrt{3}-\sqrt{2})t \approx 0{,}32t$. En otras palabras, resolver k instancias del PLDCE, para una misma curva E y punto base P, requieren solamente de $\sqrt{k}$ veces las operaciones requeridas para resolver una sola instancia. Por lo tanto, en la práctica se debe asegurar que no puede resolverse fácilmente la primera instancia.

8. Curvas elípticas supersingulares. Se ha demostrado [65][29] que, bajo ciertas suposiciones, el PLDCE en una curva elíptica E definida sobre un campo finito $GF(q)$ puede reducirse al problema del logaritmo discreto en el grupo multiplicativo de un campo de extensión

$GF(q^k)$, para alguna $k \geq 1$, en donde puede aplicarse el algoritmo de criba numérica. Sin embargo, como han demostrado Balasubramanian y Koblitz [8], esta reducción es práctica solamente para k pequeñas, lo cual no se cumple para la mayoría de las curvas elípticas. Para asegurarse de que el algoritmo de reducción no puede aplicarse a una curva particular, solamente es necesario verificar que n, el orden del punto P, no divide a $q^k - 1$ para los valores de k en los cuales el problema del logaritmo discreto sobre $GF(q^k)$ es tratable; en la práctica, cuando $n > 2^{160}$ es suficiente con $1 \leq k \leq 20$ [4].

Se dice que una curva elíptica E sobre $GF(q)$ es *supersingular* si la traza t de E es divisible por la característica p de $GF(q)$. Para esta clase de curvas elípticas se sabe que $k \leq 6$ [65]. En consecuencia, el algoritmo de reducción permite una solución en tiempo sub-exponencial para el PLDCE en curvas supersingulares. Debido a esta razón, las curvas supersingulares son excluidas explícitamente de los estándares mediante la verificación de divisibilidad anteriormente mencionada.

9. Curvas anómalas de campo primo. Una curva E sobre $GF(p)$ se denomina *anómala de campo primo* si $|E| = p$. Semaev[89], Smart[97], así como Sato y Araki[84] demostraron como resolver eficientemente el PLDCE sobre estas curvas. Debido a que el método no puede extenderse a otro tipo de curvas basta con asegurarse que el número de puntos de una curva elíptica no es igual a la cardinalidad del campo subyacente. El número de puntos de una curva puede ser calculado eficientemente mediante el algoritmo de Schoof [87].

10. Curvas definidas sobre un campo pequeño. Supongamos que E está definida sobre el campo $GF(2^{ed})$. Gallant, Lambert y Vanstone [31], asi como Wiener y Zucherato [105], mostraron como el algoritmo rho de Pollard para el cálculo de logaritmos sobre E puede ser mejorado en velocidad por un factor de $\sqrt{d}$ reduciendo entonces el tiempo de ejecución de algoritmo rho de Pollard para estas curvas a $(\sqrt{\pi n/d})/2$ pasos.

11. Curvas sobre un campo compuesto. Galbraith y Smart [30] expusieron como resolver el PLDCE en curvas elípticas definidas sobre $GF(2^m)$ para m compuesto (tales campos son denominados *campos compuestos*). Más recientemente, Gaudry, Hess y Smart[37] probaron que cuando m tiene un divisor pequeño l, por ejemplo $l = 4$, el PLDCE para curvas elípticas definidas sobre $GF(2^m)$ puede ser resuelto

más rápidamente que con el algoritmo rho de Pollard. Debido a estas razones algunos estándares de CCE, incluyendo al ANSI X9.62 [4], excluyen explícitamente el uso de curvas elípticas sobre campos compuestos.

12. Criptoanálisis cuántico En 1994, Shor [90][91] mostró que es posible resolver la factorización de primos y el logaritmo discreto en tiempo polinomial utilizando una computadora cuántica. El algoritmo de Shor puede ser utilizado también para resolver el logaritmo discreto sobre curvas elípticas[34]. Sin embargo, a pesar de los esfuerzos realizados por varios grupos de investigación, no ha sido aún construida una computadora cuántica.

La seguridad de los sistemas criptográficos basados en curvas elípticas radica en la dificultad para resolver el problema del logaritmo discreto sobre curvas elípticas. A la fecha, no se conoce un algoritmo para resolver dicho problema que sea mejor que el algoritmo rho de Pollard [80], de modo que los tamaños de clave pueden ser menores que los de RSA o sistemas similares para tener el mismo nivel de seguridad [27]. El algoritmo de Pollard es de complejidad $O(\sqrt{\pi n/2})$. Este algoritmo puede ser paralelizado [103] de modo que si se utilizan r procesadores, entonces el número esperado de operaciones que realiza cada procesador para que alguno de ellos obtenga un logaritmo es de $O(\sqrt{\pi n/2}/r)$. A diferencia del problema de logaritmo discreto sobre campos finitos, se desconocen algoritmos del tipo de cálculo de índices para el problema de logaritmos sobre CE. Incluso se ha demostrado que algunos métodos de índices no funcionan en el caso de CE [68][94].

La inexistencia de ataques de complejidad subexponencial sobre CCE ofrece reducciones potenciales en capacidades de procesamiento, almacenamiento, tamaños de mensajes, etc. Si se elige adecuadamente, un CCE sobre campos con elementos de 160 bits pueden ser tan seguros como el RSA o sistemas de logaritmo discreto en campos finitos con elementos de 1024 bits [17].

6.10. Curvas de Koblitz

Una clase de curvas, denominadas *curvas binarias anómalas* o curvas ABC, también conocidas como *curvas de Koblitz*, fueron propuestas por primera vez para su uso criptográfico por Koblitz [50]. Las curvas ABC son curvas sobre $GF(2^m)$ con coeficientes a y b que son 0 o 1. Dado que se

requiere que $b \neq 0$, deben estar definidas por la ecuación

$$y^2 + xy = x^3 + 1$$

o la ecuación

$$y^2 + xy = x^3 + x^2 + 1.$$

Solinas [99] [100], basandose en trabajo previo de Meier y Staffelbach [62], mostró como puede calcularse kP eficientemente para una k arbitraria donde P es un punto de una curva de Koblitz. Sin embargo, la mayor estructura que presentan estas curvas también permite ataques más eficientes [25]. Para una curva de Koblitz definida sobre un campo $GF(2^m)$ es posible acelerar el algoritmo rho de Pollard por un factor de $\sqrt{m}$ [31] [105].

6.10.1. Propiedades básicas

A continuación haremos una revisión de las propiedades básicas de las curvas de Koblitz.

Ordenes de grupo Las curvas de Koblitz están dadas por la ecuación:

$$E_a : y^2 + xy = x^3 + ax^2 + 1 \tag{6.8}$$

donde $a = 0$ o $a = 1$. Como es usual, se denota por $E_a(GF(2^m))$ al grupo de puntos en $GF(2^m) \times GF(2^m)$ que satisfacen la ecuación E_a. El grupo debe elegirse de modo que sea computacionalmente difícil calcular logaritmos discretos sobre él. Debido a esto, por ejemplo, el orden $|E(GF(2^m))|$ debe ser divisible por un primo grande [65]. Idealmente, el orden debe ser un primo o el producto de un primo y un entero pequeño. Esto solo puede ocurrir cuando m es primo, pues de otra manera existen divisores grandes que surgen de los subgrupos $E_d(GF(2^m))$ donde d divide a m.

Cuando m es primo, el único de tales divisores es para $d = 1$. Las curvas de Koblitz sobre $GF(2)$ son:

$$\begin{aligned} E_1(GF(2)) &= \{\mathcal{O}, (0,1)\} \\ E_2(GF(2)) &= \{\mathcal{O}, (0,1), (1,0), (1,1)\}. \end{aligned}$$

Dado que $E_a(GF(2))$ es un subgrupo de $E_a(GF(2^m))$, tenemos que el orden $|E_a(GF(2^m))|$ es siempre divisible por:

$$f = |E_a(GF(2))| = \begin{cases} 2 & \text{para } a = 1 \\ 4 & \text{para } a = 0 \end{cases} \tag{6.9}$$

Definimos a un entero como *muy cercano a primo* si es de la forma $N = f \cdot r$, donde $f = 2$ o 4 y $r > 2$ es primo. Si bien los ordenes $|E_1(GF(2^m))|$ no son nunca primos para $m > 1$, frecuentemente son muy cercanos a primo. Los valores de $m \leq 512$ para los cuales $|E_1(GF(2^m))|$ es el doble de un primo son:

$$m = 3, 5, 7, 11, 17, 19, 23, 101, 107, 109, 113, 163, 283, 311, 331, 347, 359.$$

Los valores de $m \leq 512$ para los cuales $|E_0(GF(2^m))|$ es 4 veces un primo son:

$$m = 5, 7, 13, 19, 23, 41, 83, 97, 103, 107, 131, 233, 239, 277, 283, 349, 409.$$

Las curvas cuyo orden es muy cercano a primo son las de mayor interés criptográfico.

SUBGRUPO PRINCIPAL Supongamos que $|E_a(GF(2^m))| = f \cdot r$ es muy cercano a primo. Definimos al *subgrupo principal* como el subgrupo de orden r. Comúnmente, se realizan operaciones criptográficas sobre el subgrupo principal en lugar de sobre la curva entera.

Proposición 6.3 *Supóngase que $|E_a(GF(2^m))|$ es muy cercano a primo, y sea P un punto sobre $E_a(GF(2^m))$. Entonces P está en el subgrupo principal si y solo si $P = fQ$ para algún Q sobre $E_a(GF(2^m))$.*

Demostración
Las dos curvas $E_a(GF(2))$ son grupos cíclicos. Esto se puede verificar fácilmente observando que $2(1, 0) = (1, 1)$ sobre $E_1(GF(2))$. Por lo tanto la curva $E_a(GF(2^m))$ es cíclica cuando su orden es muy cercano a primo. El resultado se sigue de las propiedades de grupos finitos cíclicos. □

Como resultado de lo anterior, podemos determinar en una forma sencilla cuando un punto dado está en el subgrupo principal. Si $a = 1$, entonces un punto $P = (x, y)$ está en el subgrupo principal si y solo si $Tr(x) = 1$. Si $a = 0$ entonces $P = (x, y)$ está en el subgrupo principal si y solo si $Tr(x) = 0$ y $Tr(y) = Tr(\lambda, x)$, donde λ es un elemento tal que $\lambda^2 + \lambda = x$. Si se utiliza una representación en bases normales del campo, el cálculo tanto de la traza como de λ puede hacerse en forma muy eficiente.

MULTIPLICACIÓN COMPLEJA Dado que las curvas de Koblitz también están definidas sobre $GF(2)$, tienen la propiedad de que si $P = (x, y)$ es un punto sobre E_a entonces también lo es el punto (x^2, y^2). Más aún, uno puede verificar de (6.8) que

$$(x^4, y^4) + 2(x, y) = \mu \cdot (x^2, y^2) \tag{6.10}$$

para toda (x, y) sobre E_a, donde

$$\mu := (-1)^{1-a} \tag{6.11}$$

Esta relación puede escribirse más fácilmente en términos del mapeo de Frobenius sobre $GF(2)$:

$$\tau(x, y) := (x^2, y^2). \tag{6.12}$$

Utilizando esta notación, (6.10) queda como

$$\tau(\tau P) + 2P = \mu\tau P \tag{6.13}$$

para toda $P \in E_a$. Simbólicamente, esto puede ser escrito como

$$(\tau^2 + 2) = \mu\tau.$$

Explícitamente, este número es

$$\tau = \frac{\mu + \sqrt{-7}}{2}.$$

Mediante la combinación del mapeo de Frobenius con la multiplicación escalar ordinaria, podemos multiplicar puntos sobre E_a por cualquier elemento en el anillo $\mathbb{Z}[\tau]$. Decimos por lo tanto que E_a tiene *multiplicación compleja* por τ.