Teoría de Números y Criptografía

F. J. Lobillo

2021/2022

Parte II

Criptografía y Curvas Elípticas

Índice general

Capítulo 5

Curvas elípticas

5.1 Concepto de curva elíptica.

Antes de proceder a definir el concepto de curva elíptica, vamos a dedicar unas secciones a estudiar las ecuaciones que las van a definir. Comenzamos con la ecuación más general.

Definición 5.1. Una ecuación de Weierstrass afín sobre un cuerpo K es una ecuación de la forma

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \qquad (5.1)$$

con $a_1, a_3, a_2, a_4, a_6 \in K$. Las siguientes cantidades están relaciona-

das con E y serán de importancia más adelante:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2\\
b_4 &= 2a_4 + a_1a_3\\
b_6 &= a_3^2 + 4a_6\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\\
c_4 &= b_2^2 - 24b_4\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\\
j &= \frac{c_4^3}{\Delta} \text{ para } \Delta \neq 0.
\end{aligned}$$

Δ recibe el nombre de discriminante, y j es el j-invariante.

Para la siguiente demostración necesitamos recordar cómo se extiende el concepto de grado a funciones racionales. Concretamente, si $r = \frac{f}{g} \in K(X)$ con f, g primos relativos, se define

$$\deg(r) = \deg(f) - \deg(g).$$

Lema 5.2. *Dados* $r, s \in K(X)$,

$$\begin{aligned}
\deg(rs) &= \deg(r) + \deg(s),\\
\deg(r+s) &\leq \max\{\deg(r), \deg(s)\}.
\end{aligned}$$

Si $\deg(r) \neq \deg(s)$*, la última desigualdad es una igualdad.*

Demostración. Ejercicio. □

Proposición 5.3. *El polinomio* $E = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in K[X, Y]$ *es irreducible.*

Demostración. Por el Lema de Gauss es suficiente con ver que E es irreducible en $K(X)[Y]$. Si fuese reducible, tendríamos que $E = (Y - r)(Y - s)$ con $r, s \in K(X)$. Comparando coeficientes tenemos que $r + s = a_1X + a_3$ y $rs = -X^3 - a_2X^2 - a_4X - a_6$. En consecuencia $\deg(r+s) \leq 1$ y $\deg(rs) = 3$. Como 3 es impar tenemos que $\deg(r) \neq \deg(s)$, lo que implica

$$1 \geq \deg(r+s) = \max\{\deg(r), \deg(s)\} \geq \frac{1}{2}(\deg(r) + \deg(s)) = \frac{3}{2},$$

una contradicción. □

Tenemos por tanto que $K[E] = \frac{K[X,Y]}{\langle E \rangle}$ es un dominio de integridad, cuyo anillo de fracciones se denota $K(E)$.

Consideremos dos ecuaciones de Weierstrass.

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$
$$E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'$$

¿Qué posibles cambios de variable pueden transformar E en E'? Supongamos por el momento que K es algebraicamente cerrado y tengamos en cuenta que a cada ecuación vamos a asociar las soluciones dentro del espacio afín $\mathbb{A}^2(K) = K^2$. Para que las transformaciones respeten las propiedades deben ser inversibles, por lo que es razonable limitarnos a transformaciones afines

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix}$$

que transformen E en un múltiplo $E(\alpha X + \beta Y + r, \gamma X + \delta Y + s)$ de E'. Como el grado de X es 3 y el de Y es 2, necesariamente $\beta = 0$. Los

coeficientes de X^3 e Y^2 en la ecuación resultante deben ser idénticos y no nulos, por lo tanto $\alpha^3 = \delta^2 \neq 0$. Dado que K es algebraicamente cerrado, existe $u \in K \setminus \{0\}$ tal que $\alpha = u^2$ y $\delta = u^3$. Si llamamos $t = \frac{\gamma}{u^2}$ podemos concluir que la transformación afín debe ser de la forma

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} u^2 & 0 \\ u^2 t & u^3 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix} \tag{5.2}$$

Definición 5.4. Las curvas E y E' se dicen isomorfas si E' se obtiene a partir de E mediante el cambio de variable (5.2) y dividiendo la ecuación resultante por u^6, donde $u \in K \setminus \{0\}$ y $r, s, t \in K$.

Proposición 5.5. *Ser isomorfas es una relación de equivalencia.*

Demostración. Ejercicio. □

Proposición 5.6. *Sea* $p = \mathrm{char}(K)$ *y sea* E *una ecuación de Weierstrass dada en* (5.8)*.*

1. *Si* $p \neq 2$*, la ecuación* E *es isomorfa a una ecuación de la forma*

$$Y^2 = X^3 + aX^2 + bX + c. \tag{5.3}$$

2. *Si* $p \neq 2, 3$*, la ecuación* E *es isomorfa a una ecuación de la forma*

$$Y^2 = X^3 + aX + b, \tag{5.4}$$

   que recibe el nombre de forma de Weierstrass simplificada.

3. *Si* $p = 3$*, la ecuación* E *es isomorfa a alguna de las ecuaciones de la forma* (5.4) *o*

$$Y^2 = X^3 + aX^2 + c. \tag{5.5}$$

4. *Si* $p = 2$*, la ecuación* E *es isomorfa a*

$$Y^2 + XY = X^3 + aX^2 + b \text{ si } a_1 \neq 0, \tag{5.6}$$

$$Y^2 + aY = X^3 + bX + c \quad \text{si } a_1 = 0, \tag{5.7}$$

denominadas también forma de Weierstrass simplifcada.

Demostración. Si $p \neq 2$, el cambio de variable

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ -2^{-1}a_1 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} 0 \\ -2^{-1}a_3 \end{pmatrix}$$

transforma (5.8) en (5.3). Si $p > 3$, el cambio de variable

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} -3^{-1}a \\ 0 \end{pmatrix}$$

transforma (5.3) en (5.4). Para el caso $p = 3$, si $a = 0$ en (5.3), la ecuación ya satisface (5.4), luego necesitamos analizar el caso $a \neq 0$. El cambio de variable

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} ba^{-1} \\ 0 \end{pmatrix}$$

transforma (5.3) en (5.5). Finalmente, si $p = 2$, los cambios de variable

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} a_1^2 & 0 \\ 0 & a_1^3 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} a_3 a_1^{-1} \\ (a_1^2 a_4 + a_3^2) a_1^{-3} \end{pmatrix}$$

cuando $a_1 \neq 0$, y

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} a_2 \\ 0 \end{pmatrix}$$

cuando $a_1 = 0$, son admisibles y transforman (5.8) en (5.6) y (5.7) respectivamente. □

A cada ecuación E podemos asociar el conjunto de puntos del plano afín $\mathbb{A}^2 = \mathbb{A}^2(K) = K^2$ que satisfacen la ecuación. Identificando la ecuación con el polinomio correspondiente el conjunto asociado es

$$E = \left\{(x, y) \in \mathbb{A}^2 \mid E(x, y) = 0\right\}.$$

Un punto $(x, y) \in E$ se dice singular si

$$\frac{\partial E}{\partial X}(x, y) = \frac{\partial E}{\partial Y}(x, y) = 0.^1$$

La ecuación E se dice singular si tiene al menos un punto singular.

Teorema 5.7. *E es singular si y sólo si $\Delta = 0$.*

Demostración. Dado que los cambios de variable afines cambian el discriminante en una constante no nula (ver el Ejercicio 5.4), y que preservan singularidades (son transformaciones afines), basta demostrar el Teorema para ecuaciones de la forma (5.3), (5.6) y (5.7).

Veamos primero el caso $\mathrm{char}(K) \neq 2$, es decir (5.3). Sea $f(X) = X^3 + aX^2 + bX + c$, es decir, $E = Y^2 - f(X)$. Por tanto

$$\frac{\partial E}{\partial Y} = 2Y, \quad \frac{\partial E}{\partial X} = f'(X).$$

Como consecuencia, $(x, y) \in E$ es un punto singular si y sólo si $y = 0$ y $f(x) = f'(x) = 0$. Es decir, E es singular si y sólo si $f(X)$ tiene una

[1] El concepto de derivada de un polinomio es algebraico.

raíz doble. Un polinomio de grado 3 tiene una raíz doble si y sólo si su discriminante es cero[2], siendo el discriminante de f

$$-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3.$$

Como

$$\Delta = 16(-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3),$$

tenemos que $\Delta = 0$ si y sólo si $f(X)$ tiene una raíz doble, lo que demuestra el resultado en el caso característica impar. Para la característica 2, analicemos cada ecuación por separado.

Consideremos en primer lugar (5.6), es decir, $E = Y^2 + XY + X^3 + aX^2 + b$. Dado que

$$\frac{\partial E}{\partial X} = Y + X^2, \quad \frac{\partial E}{\partial Y} = X,$$

un punto $(x, y) \in E$ es singular si y solo si $x = y = 0$, pero para que $(0, 0) \in E$ necesariamente $b = 0$. Como $\Delta = b$, tenemos que E es singular si y sólo si $\Delta = 0$.

Consideremos finalmente la ecuación (5.7), es decir, $E = Y^2 + aY + X^3 + bX + c$. En este caso,

$$\frac{\partial E}{\partial X} = X^2 + b, \quad \frac{\partial E}{\partial Y} = a,$$

por lo que si E es singular entonces $a = 0$. Dado que $\Delta = a$ tenemos una implicación. Por otra parte, si $a = 0$, el punto $(\sqrt{b}, \sqrt{c}) \in E$ y es singular, lo que termina la demostración. □

[2] Álgebra III, o [5, páginas 258 y 259]

Definición 5.8. Una curva elíptica (afín) es el conjunto de puntos en $\mathbb{A}^2(K)$ asociado a una ecuación de Weierstrass no singular junto con un punto adicional $\mathcal{O}$ sin coordenadas.

Por la Proposición 5.6, toda curva elíptica es isomorfa a alguna de las formas simplificadas allí descritas.

5.2 Curvas elípticas proyectivas

Recordemos que el plano proyectivo se define como el conjunto cociente

$$\mathbb{P}^2 = \mathbb{P}^2(K) = \frac{K^3 \setminus \{(0,0,0)\}}{\sim}$$

donde $(x_0, y_0, z_0) \sim (x_1, y_1, z_1)$ si y solo si existe $\lambda \in K \setminus \{0\}$ tal que $(x_0, y_0, z_0) = \lambda(x_1, y_1, z_1)$. Hay una inclusión canónica

$$\begin{aligned} \mathbb{A}^2(K) &\to \mathbb{P}^2(K) \\ (x, y) &\mapsto (x, y, 1) \end{aligned}$$

cuya "inversa" es

$$(x, y, z) \mapsto \left(\frac{x}{z}, \frac{y}{z}\right).$$

Los elementos no afines son una recta proyectiva que recibe el nombre de recta del infinito. La denotamos

$$L^\infty = \mathbb{P}^2 \setminus \mathbb{A}^2 = \left\{(x, y, z) \in \mathbb{P}^2 \mid z = 0\right\}.$$

Denotamos por $K[X,Y,Z]_{\text{hom}}$ al conjunto de los polinomios homogéneos en esas variables, es decir, aquellos polinomios cuyos monomios tienen todos el mismo grado total. Las aplicaciones

$$\begin{aligned} K[X,Y] &\to K[X,Y,Z]_{\text{hom}} \\ f(X,Y) &\mapsto f^*(X,Y,Z) = Z^{\deg(f)} f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \end{aligned}$$

y

$$\begin{aligned} K[X,Y,Z]_{\text{hom}} &\to K[X,Y] \\ F(X,Y,Z) &\mapsto F_*(X,Y) = F(X,Y,1) \end{aligned}$$

se llaman homogeneización y deshomogeneización con respecto de Z.

Proposición 5.9. *Sean* $f, g \in K[X,Y]$, $F, G \in K[X,Y,Z]_{\text{hom}}$. *Entonces*

1. $(fg)^* = f^* g^*$.
2. $(FG)_* = F_* G_*$.
3. $(f^*)_* = f$.
4. *Si* Z *no divide a* F, $(F_*)^* = F$.

Demostración. Ejercicio. □

Definición 5.10. Una ecuación de Weierstrass proyectiva sobre K es una ecuación de la forma

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (5.8)$$

con $a_1, a_3, a_2, a_4, a_6 \in K$. Dos ecuaciones de Weierstrass proyectivas

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$
$$E' : Y^2Z + a_1'XYZ + a_3'YZ^2 = X^3 + a_2'X^2Z + a_4'XZ^2 + a_6'Z^3$$

son isomorfas si E' puede obtenerse a partir de E mediante el cambio de variable

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto u^{-6} \begin{pmatrix} u^2 & 0 & r \\ u^2t & u^3 & s \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \tag{5.9}$$

con $u \in K \setminus \{0\}$, $r, s, t \in K$.

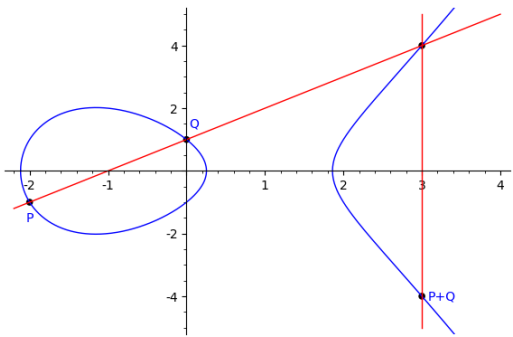
5.3 Aritmética de una curva elíptica

Las curvas elípticas han demostrado su utilidad en Teoría de Números en general y en Criptografía en particular por tener una estructura de grupo en sus puntos. Dicha estructura de grupo puede presentarse de diversas maneras. En este curso vamos a dar un ejemplo geométrico que nos sirva de introducción a la aritmética que presentaremos de manera formal de forma algebraica.

Ejemplo 5.11. La suma de los puntos $P = (-2, -1)$ y $Q = (0, 1)$ en la curva $y^2 = x^3 - 4x + 1$ es $P + Q = (3, -4)$ tal y como se presenta en la Figura 5.11.

Para trasladar este ejemplo a una definición general de la aritmética, necesitamos introducir algunas ideas. Fijemos una curva E con ecuación

Figura 5.1: Suma en la curva $y^2 = x^3 - 4x + 1$.



de Weierstrass general (5.8). Dado $P = (x_0, y_0) \in K^2$, denotamos $-P = (x_0, -y_0 - a_1x_0 - a_3)$. Observemos que

$$-(-P) = (x_0, -(-y_0 - a_1x_0 - a_3) - a_1x_0 - a_3) = (x_0, y_0) = P. \tag{5.10}$$

Lema 5.12. *Si* $P = (x_0, y_0) \in E$ *y* L *es la recta de ecuación* $X - x_0$*, entonces* $E \cap L = \{P, -P\}$.

Demostración. Observemos que $(x_0, y_1) \in E \cap L$ si y sólo si y_1 es solución de la ecuación de segundo grado

$$Y^2 + (a_1x_0 + a_3)Y - (x_0^3 + a_2x_0^2 + a_4x + a_6) = 0.$$

Como y_0 es raíz de dicha ecuación, otra solución y_1 debe verificar[3] $y_0 + y_1 = -(a_1 x_0 + a_3)$, de donde se obtiene el resultado. □

Observación 5.13. El Lema 5.12 incluye el caso $P = -P$.

Lema 5.14. *Para cualesquiera* $\lambda, \mu \in K$,

$$E(X, \lambda X + \mu) = -X^3 + \left(\lambda^2 + a_1\lambda - a_2\right) X^2 + \left(2\lambda\mu + a_1\mu + a_3\lambda - a_4\right) X + \left(\mu^2 + a_3\mu - a_6\right).$$

Demostración. El resultado es un cálculo directo. Puede obtenerse también con el código

```
sage: A.<la,mu,a1,a3,a2,a4,a6> = PolynomialRing(RationalField())
sage: Rels = A.ideal(0)
sage: B = QuotientRing(A,Rels)
sage: Q = FractionField(B)
sage: R.<x> = PolynomialRing(Q)
sage: y = R(la*x+mu)
sage: f = R(y^2 + a1*x*y + a3*y - x^3 - a2*x^2 - a4*x - a6)
sage: f
```

en SageMath. □

Dado $P = (x_0, y_0) \in E$, se define la recta tangente a E en P como aquella de ecuación

$$\frac{\partial E}{\partial X}(x_0, y_0)\,(X - x_0) + \frac{\partial E}{\partial Y}(x_0, y_0)\,(Y - y_0) = 0.$$

Observemos que, al ser las curvas elípticas no singulares, la ecuación no es trivial. Es inmediato comprobar que si llamamos T a dicha recta

[3] Consecuencia de que la suma de las dos soluciones de una ecuación de segundo grado $az^2 + bz + c = 0$ es $-\frac{b}{a}$.

tangente, tenemos que $P \in E \cap T$. Los siguientes resultados nos permiten calcular esa intersección.

Lema 5.15. $\frac{\partial E}{\partial Y}(x_0, y_0) = 0$ *si y sólo si* $P = -P$, *en cuyo caso* $E \cap T = \{P\}$.

Demostración. Como $\frac{\partial E}{\partial Y} = 2Y + a_1X + a_3$, tenemos que

$$\frac{\partial E}{\partial Y}(x_0, y_0) = 0 \iff 2y_0 + a_1x_0 + a_3 = 0,$$

lo que equivale a que $y_0 = -y_0 - a_1x_0 - a_3$. El resultado final se deduce, por tanto, del Lema 5.12. □

Lema 5.16. *Sea* E *una curva elíptica y* L *una recta de ecuación* $Y - \lambda X - \mu$. *Un punto* $(x_0, y_0) \in E \cap L$ *si y sólo si* $y_0 = \lambda x_0 + \mu$ *y* $x_0 \in K$ *es raíz del polinomio* $E(X, \lambda X + \mu)$.

Demostración. Dado que $(x_0, y_0) \in L$ si y sólo si $y_0 = \lambda x_0 + \mu$, bajo esta condición $E(x_0, y_0) = E(x_0, \lambda x_0 + \mu)$, por lo que $(x_0, y_0) \in E$ si y sólo si $E(x_0, \lambda x_0 + \mu) = 0$. □

Lema 5.17. *Supongamos que* $P = (x_1, y_1), \in E \cap L$ *donde la ecuación de* L *es* $Y - \lambda X - \mu$. *Si* L *es la recta tangente a* E *en* P, *entonces* $(X - x_1)^2 \mid E(X, \lambda X + \mu)$.

Demostración. Si L es la tangente a E en P, tenemos que $\frac{\partial E}{\partial Y}(x_1, y_1) \neq 0$, pues en otro caso la ecuación de L no podría ser la indicada. La ecuación de L puede reescribirse como

$$Y + \frac{\frac{\partial E}{\partial X}(x_1, y_1)}{\frac{\partial E}{\partial Y}(x_1, y_1)}(X - x_1) - y_1.$$

de donde

$$\lambda = \frac{-\frac{\partial E}{\partial X}(x_1, y_1)}{\frac{\partial E}{\partial Y}(x_1, y_1)} = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{a_1x_1 + a_3 + 2y_1}$$
$$\mu = -\lambda x_1 + y_1$$

Por el Lema 5.16, $f(x_1) = 0$, donde $f(X) = E(X, \lambda X + \mu)$. Un cálculo directo, aunque bastante engorroso, permite comprobar que $(X - x_1)^2 \mid f(X)$. Dicha comprobación puede hacerse también con el siguiente código de `SageMath`:

```
sage: A.<a1,a3,a2,a4,a6,x1,y1> = PolynomialRing(RationalField())
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1
- x1^3 - a2*x1^2 - a4*x1 - a6)
sage: B = QuotientRing(A,Rels)
sage: Q = FractionField(B)
sage: R.<x> = PolynomialRing(Q)
sage: la = Q((3*x1^2 + 2*a2*x1 + a4 - a1*y1)/(a1*x1 + a3 + 2*y1))
sage: mu = Q(-la * x1 + y1)
sage: y = R(la*x + mu)
sage: f = R(y^2 + a1*x*y + a3*y - x^3 - a2*x^2 - a4*x - a6)
sage: f.list()[2] == la^2 + a1*la - a2
sage: f.mod((x-x1)^2)
```

Por tanto $(X - x_1)^2 \mid E(X, \lambda X + \mu)$. □

Lema 5.18. *Supongamos que* $P = (x_1, y_1), \in E$ *con* $P \neq -P$ *y sea* T *la recta tangente a* E *en* P. *Entonces*

$$E \cap T = \{(x_1, y_1), (x_3, y_3)\}$$

donde

$$\begin{aligned}\lambda &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{a_1x_1 + a_3 + 2y_1},\\ x_3 &= \lambda^2 + a_1\lambda - a_2 - 2x_1,\\ y_3 &= \lambda(x_3 - x_1) + y_1.\end{aligned}$$

Demostración. Por el Lema 5.15 $\frac{\partial E}{\partial Y}(x_1, y_1) \neq 0$, de donde la ecuación de T puede reescribirse como

$$Y + \frac{\frac{\partial E}{\partial X}(x_1, y_1)}{\frac{\partial E}{\partial Y}(x_1, y_1)}(X - x_1) + y_1.$$

Si llamamos

$$\begin{aligned}\lambda &= \frac{-\frac{\partial E}{\partial X}(x_1, y_1)}{\frac{\partial E}{\partial Y}(x_1, y_1)} = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{a_1x_1 + a_3 + 2y_1}\\ \mu &= -\lambda x_1 + y_1\end{aligned}$$

la ecuación se representa de forma simplificada como $Y - \lambda X - \mu$. Por el Lema 5.17, $(X - x_1)^2 \mid f(X)$. Dado que además el coeficiente líder de $f(X)$ es -1 por el Lema 5.14, tenemos que existe un único $x_3 \in K$ tal que $f(X) = -(X - x_1)^2(X - x_3)$. De nuevo por el Lema 5.14 y desarrollando $-(X-x_1)^2(X-x_3)$, tenemos que el coeficiente de grado 2 de $f(X)$ es

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

de donde $x_3 = \lambda^2 + a_1\lambda - a_2 - 2x_1$. Por último el valor de y_3 se obtiene directamente de la ecuación de T. □

Lema 5.19. *Supongamos que* $(x_1, y_1), (x_2, y_2) \in E$ *con* $x_1 \neq x_2$ *y sea* L *la recta que pasa por ambos puntos. Entonces*

$$E \cap L = \{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$$

donde

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, \\ x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= \lambda(x_3 - x_1) + y_1. \end{aligned}$$

Demostración. La recta L tiene por ecuación

$$Y - \frac{y_2 - y_1}{x_2 - x_1}(X - x_1) - y_1.$$

Llamando $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ y $\mu = -\lambda x_1 + y_1$, la ecuación de L puede escribirse como $Y - \lambda X + \mu$. Sea $f(X) = E(X, \lambda X + \mu)$. Por el Lema 5.14, f tiene por coeficientes de grados 3 y 2 a -1 y $\lambda^2 - a_1\lambda - a_2$ respectivamente. Por el Lema 5.16, $f(X)$ tiene al menos dos raíces, $x_1 \neq x_2$, por lo que existe un único $x_3 \in K$ tal que

$$f(X) = -(X - x_1)(X - x_2)(X - x_3).$$

Utilizando la expresión derecha, el coeficiente de grado 2 de $f(X)$ es $x_1 + x_2 + x_3$, por lo que

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

de donde

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

El valor de y_3 se obtiene directamente de la ecuación de la recta. □

Observación 5.20. El punto de coordenadas (x_3, y_3) obtenido en el Lema 5.19 no depende del orden en el que coloquemos a los puntos (x_1, y_1) y (x_2, y_2): por observación directa x_3 no depende del orden, e y_3 depende de la recta, cuya ecuación tampoco depende del orden de los puntos. Además, dicho punto no tiene por qué ser diferente de los otros dos. De hecho el siguiente resultado aclara dicha situación.

Lema 5.21. *Sean* $(x_1, y_1), (x_2, y_2) \in E$ *dos puntos tales que* $x_1 \neq x_2$, *y sea* $(x_3, y_3) \in E$ *tal que el punto dado por el Lema 5.19. Si* $(x_3, y_3) = (x_1, y_1)$, *entonces la recta que pasa por* (x_1, y_1) *y* (x_2, y_2) *es tangente a* E *en* (x_1, y_1).

Demostración. Como se observa en las demostraciones de los Lemas 5.19 y 5.18, la recta que pasa por (x_1, y_1) y (x_2, y_2) tiene por ecuación $Y - \lambda_0 X - \mu_0$ donde $\lambda_0 = \frac{y_2 - y_1}{x_2 - x_1}$ y $\mu_0 = -\lambda_0 x_1 + y_1$, y la tangente a E en (x_1, y_1) tiene por ecuación $Y - \lambda_1 X - \mu_1$ con $\lambda_1 = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{a_1 x_1 + a_3 + 2y_1}$ y $\mu_1 = -\lambda_1 x_1 + y_1$. Es suficiente con verificar que $\lambda_0 = \lambda_1$ para demostrar el Lema. Como $x_3 = x_1$, tenemos que $x_1 = \lambda_0^2 + a_1\lambda_0 - a_2 - x_1 - x_2$, de dónde

$$x_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1 \frac{y_2 - y_1}{x_2 - x_1} - a_2 - x_1 - x_2.$$

Quitando denominadores tenemos que

$$\begin{aligned} x_1(x_2 - x_1)^2 = & \\ & (y_2 - y_1)^2 + a_1(y_2 - y_1)(x_2 - x_1) \\ & - a_2(x_2 - x_1)^2 - (x_2 + x_1)(x_2 - x_1)^2, \end{aligned}$$

que al desarrollar proporciona la identidad

$$\begin{aligned} x_1x_2^2 - 2x_1^2x_2 + x_1^3 = \\ y_2^2 - 2y_1y_2 + y_1^2 + a_1x_2y_2 - a_1x_2y_1 - a_1x_1y_2 + a_1x_1y_1 \\ - a_2x_2^2 + 2a_2x_1x_2 - a_2x_1^2 - x_2^3 + x_1x_2^2 + x_1^2x_2 - x_1^3. \end{aligned}$$

Reordenamos la identidad y simplificamos algunos términos,

$$\begin{aligned} y_2^2 - 2y_1y_2 + y_1^2 + a_1x_2y_2 - a_1x_2y_1 - a_1x_1y_2 + a_1x_1y_1 = \\ x_2^3 - 3x_1^2x_2 + 2x_1^3 + a_2x_2^2 - 2a_2x_1x_2 + a_2x_1^2. \end{aligned} \quad (5.11)$$

Como $(x_2, y_2) \in E$ se verifica la identidad $y_2^2 + a_1x_2y_2 + a_3y_2 = x_2^3 + a_2x_2^2 + a_4y_2 + a_6$, restándola de (5.11) tenemos

$$\begin{aligned} - 2y_1y_2 + y_1^2 - a_1x_2y_1 - a_1x_1y_2 + a_1x_1y_1 - a_3y_2 = \\ - 3x_1^2x_2 + 2x_1^3 - 2a_2x_1x_2 + a_2x_1^2 - a_4x_2 - a_6. \end{aligned} \quad (5.12)$$

Análogamente, $(x_1, y_1) \in E$, por lo que $y_1^2 + a_1x_1y_1 + a_3y_1 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6$. Sumando esta identidad a (5.12) y reordenando obtenemos

$$\begin{aligned} 2y_1^2 - 2y_1y_2 - a_1x_2y_1 - a_1x_1y_2 + 2a_1x_1y_1 - a_3y_2 + a_3y_1 = \\ 3x_1^3 - 3x_1^2x_2 - 2a_2x_1x_2 + 2a_2x_1^2 - a_4x_2 + a_4x_1. \end{aligned}$$

Reordenamos nuevamente la identidad anterior para obtener

$$\begin{aligned} a_1x_1y_2 + a_3y_2 + 2y_1y_2 - a_1x_1y_1 - a_3y_1 - 2y_1^2 = \\ 3x_1^2x_2 + 2a_2x_1x_2 + a_4x_2 - a_1x_2y_1 \\ - 3x_1^3 - 2a_2x_1^2 - a_4x_1 + a_1x_1y_1. \end{aligned}$$

Empleando la propiedad distributiva, tenemos en consecuencia que

$$(y_2-y_1)(a_1x_1+a_3+2y_1) = (x_2-x_1)(3x_1^2+2a_2x_1+a_4-a_1y_1),$$

de donde

$$\frac{y_2-y_1}{x_2-x_1} = \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{a_1x_1+a_3+2y_1},$$

es decir, $\lambda_0 = \lambda_1$, lo que termina la demostración. □

Hemos introducido todos los resultados necesarios para definir la estructura de grupo en los puntos de una curva elíptica.

Definición 5.22. Dados $P, Q \in E$ se define $P+Q$ de la siguiente forma:

1. $\mathcal{O}$ es elemento neutro, es decir, $\mathcal{O}+P = P+\mathcal{O} = P$.
2. $P + -P = \mathcal{O}$.
3. Si $Q = P$ y R es el punto obtenido por el Lema 5.18, entonces $P+P = 2P = -R$.
4. Si $Q \neq P, -P$ y R el punto obtenido por el Lema 5.19, entonces $P+Q = -R$.

Teorema 5.23. *Si* $P, Q \in E \setminus \{\mathcal{O}\}$ *con* $P = (x_1, y_1)$, $Q = (x_2, y_2)$ *y* $Q \neq -P$, *entonces* $P+Q = (x_3, y_3)$ *donde*

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{si } P \neq Q \\ \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{a_1x_1+a_3+2y_1} & \text{si } P = Q \end{cases}$$

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

$$y_3 = -\lambda(x_3-x_1) - y_1 - a_1x_3 - a_3.$$

Demostración. Consecuencia directa de las definiciones de suma y punto simétrico, y de los Lemas 5.19 y 5.18. □

Proposición 5.24. *La operación* $+ : E \times E \to E$ *es conmutativa.*

Demostración. La propiedad conmutativa es consecuencia directa de la Observación 5.20. También puede obtenerse como consecuencia del siguiente código:

```
sage: # P = (x1,y1), Q = (x2,y2)
sage: A.<a1,a3,a2,a4,a6,x1,y1,x2,y2> = PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: lambda0 = F((y2-y1)/(x2-x1))
sage: # P + Q = (x1,y1) + (x2,y2) = (x3,y3)
sage: x3 = lambda0^2 + a1*lambda0 - a2 - x1 - x2
sage: y3 = -lambda0*(x3-x1) - y1 - a1*x3 - a3
sage: # Q + P = (x2,y2) + (x1,y1) = (x4,y4)
sage: lambda0 = F((y1-y2)/(x1-x2))
sage: x4 = lambda0^2 + a1*lambda0 - a2 - x2 - x1
sage: y4 = -lambda0*(x4-x2) - y2 - a1*x4 - a3
sage: # (x3,y3) == (x4,y4)
sage: A(x3.numerator()*x4.denominator()
- x3.denominator()*x4.numerator()),
A(y3.numerator()*y4.denominator()
- y3.denominator()*y4.numerator())
```

□

Lema 5.25. *Para cualesquiera* $P, Q \in E$, $-(P+Q) = -P + -Q$.

Demostración. El único caso no inmediato es $Q \neq P, -P, \mathcal{O}$. El caso restante puede deducirse del siguiente código

```
sage: # P = (x1,y1), Q = (x2,y2)
sage: A.<a1,a3,a2,a4,a6,x1,y1,x2,y2> = PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1
- x1^3 - a2*x1^2 - a4*x1 - a6,
y2^2 + a1*x2*y2 + a3*y2 - x2^3 - a2*x2^2 - a4*x2 - a6)
sage: # P + Q = (x1,y1) + (x2,y2) = (x3,y3)
```

```
sage: lambda0 = F((y2-y1)/(x2-x1))
sage: x3 = lambda0^2 + a1*lambda0 - a2 - x1 - x2
sage: y3 = -lambda0*(x3-x1) - y1 - a1*x3 - a3
sage: # -(P+Q) = -(x3,y3) = (x4,y4)
sage: x4 = x3
sage: y4 = -y3 - a1*x3 - a3
sage: # -P = -(x1,y1) = (x5,y5)
sage: x5 = x1
sage: y5 = -y1 - a1*x1 - a3
sage: # -Q = -(x2,y2) = (x6,y6)
sage: x6 = x2
sage: y6 = -y2 - a1*x2 - a3
sage: # -P + -Q = (x5,y5) + (x6,y6) = (x7,y7)
sage: lambda0 = F((y6-y5)/(x6-x5))
sage: x7 = lambda0^2 + a1*lambda0 - a2 - x5 - x6
sage: y7 = -lambda0*(x7-x5) - y5 - a1*x7 - a3
sage: # (x4,y4) == (x7,y7)
sage: A(x4.numerator()*x7.denominator()
- x4.denominator()*x7.numerator()),
A(y4.numerator()*y7.denominator()
- y4.denominator()*y7.numerator())
```

□

Lema 5.26. *Para cualesquiera* $P, Q \in E$, $P + (-P + Q) = Q$.

Demostración. Si P o Q son $\mathcal{O}$, el resultado es inmediato. Supondremos por tanto $P, Q \neq \mathcal{O}$.

Si $Q = P$, el resultado también es inmediato. Si $Q = -P$, debemos comprobar que $P + (-P + -P) = -P$. Para realizar la suma debemos analizar cuatro casos: si $-P + -P = \mathcal{O}$, tenemos que $P = -P$, de donde la identidad es cierta; si $-P + -P = -P$, tenemos que $P = -P = \mathcal{O}$; si $-P + -P = P$, tenemos que $P + P = -P$ por el Lema 5.25, de donde

$$-P = P + P = P + (-P + -P);$$

falta, el caso $-P + -P \neq P, -P, \mathcal{O}$, caso que sale del código

```
sage: # P + (-P + -P) = -P, P = (x1,y1)
sage: A.<a1,a3,a2,a4,a6,x1,y1> = PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1 - x1^3 - a2*x1^2 - a4*x1 - a6)
sage: # -P = (x2,y2)
sage: x2 = x1
sage: y2 = -y1-a1*x1-a3
sage: # -P + -P = 2(x2,y2) = (x3,y3)
sage: lambda0 = F((3*x2^2 + 2*a2*x2 + a4 - a1*y2)/(a1*x2 + a3 + 2*y2))
sage: x3 = lambda0^2 + a1*lambda0 - a2 - x2 - x2
sage: y3 = -lambda0*(x3-x2) - y2 - a1*x3 - a3
sage: # P + (-P + -P) = (x1,y1) + (x3,y3) = (x4,y4)
sage: sage: lambda0 = F((y3-y1)/(x3-x1))
sage: x4 = lambda0^2 + a1*lambda0 - a2 - x1 - x3
sage: y4 = -lambda0*(x4-x1) - y1 - a1*x4 - a3
sage: # (x4,y4) == (x2,y2)
sage: A(x4.numerator()*x2.denominator()
- x4.denominator()*x2.numerator()),
A(y4.numerator()*y2.denominator()
- y4.denominator()*y2.numerator())
```

Supongamos finalmente $Q \neq P, -P, \mathcal{O}$. Para comprobar la identidad $P + (-P + Q) = Q$ debemos, nuevamente, considerar cuatro casos: si $-P + Q = \mathcal{O}$, tenemos que $P = Q$, ya tratado; si $-P + Q = -P$, tenemos que la recta que pasa por $-P$ y Q corta a la curva en P, lo que es imposible pues la curva que pasa por $Py - P$ no corta en ningún otro punto; si $-P + Q = P$, el tercer punto en el que la recta que pasa por $-P$ y Q corta E es $-P$, de donde esa recta es tangente a $-P$, deducimos que $-P + -P = -Q$, o $P + P = Q$, lo que implica la identidad ya que $P + (-P + Q) = P + P = Q$; el caso restante es consecuencia del código

```
sage: # P + (-P + Q) = Q, P = (x1,y1), Q = (x2,y2)
sage: A.<a1,a3,a2,a4,a6,x1,y1,x2,y2> = PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1
- x1^3 - a2*x1^2 - a4*x1 - a6,
y2^2 + a1*x2*y2 + a3*y2 - x2^3 - a2*x2^2 - a4*x2 - a6)
sage: # -P = -(x1,y1) = (x3,y3)
sage: x3 = x1
```

```
sage: y3 = -y1 - a1*x1 - a3
sage: # -P + Q = (x3,y3) + (x2,y2) = (x4,y4)
sage: lambda0 = F((y2-y3)/(x2-x3))
sage: x4 = lambda0^2 + a1*lambda0 - a2 - x3 - x2
sage: y4 = -lambda0*(x4-x3) -y3 - a1*x4 - a3
sage: # P + (-P + Q) = (x1,y1) + (x4,y4) = (x5,y5)
sage: lambda0 = F((y4-y1)/(x4-x1))
sage: x5 = lambda0^2 + a1*lambda0 - a2 - x1 - x4
sage: y5 = -lambda0*(x5-x1) -y1 - a1*x5 - a3
sage: # (x5,y5) == (x2,y2)
sage: A(x5.numerator()*x2.denominator()
- x5.denominator()*x2.numerator()),
A(y5.numerator()*y2.denominator()
- y5.denominator()*y2.numerator())
```

□

Lema 5.27. *Para cualesquiera* $P, Q \in E$, $P + (P + Q) = (P + P) + Q$.

Demostración. Si P o Q son $\mathcal{O}$, el resultado es inmediato. Supondremos por tanto $P, Q \neq \mathcal{O}$. Si $P = Q$ entonces

$$P + (P + P) = (P + P) + P$$

por la conmutatividad (Proposición 5.24).

Si $Q = -P$,

$$P+(P+-P) = P+(-P+P) = P = -P+(-(-P)+P) = (P+P)+-P$$

donde hemos usado la conmutatividad, Proposición 5.24, la identidad (5.10) y el Lema 5.26.

Si $Q = -(P + P)$,

$$P + (P + -(P + P)) = P + (P + (-P + -P)) = \\ = P + (-P) = \mathcal{O} = (P + P) + -(P + P),$$

donde hemos usado los Lemas 5.25 y 5.26.

Si $Q = (P + P)$, debemos comprobar que

$$P + (P + (P + P)) = (P + P) + (P + P),$$

lo que se deduce del código

```
sage: # P = (x1,y1)
sage: A.<a1,a3,a2,a4,a6,x1,y1> = PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1
- x1^3 - a2*x1^2 - a4*x1 - a6)
sage: # P + P = 2(x1,y1) = (x2,y2)
sage: lambda0 = F((3*x1^2 + 2*a2*x1 + a4 - a1*y1)/(a1*x1 + a3 + 2*y1))
sage: x2 = lambda0^2 + a1*lambda0 - a2 - x1 - x1
sage: y2 = -lambda0*(x2-x1) - y1 - a1*x2 - a3
sage: # (P + P) + (P + P) = 2(x2,y2) = (x4,y4)
sage: lambda0 = F((3*x2^2 + 2*a2*x2 + a4 - a1*y2)/(a1*x2 + a3 + 2*y2))
sage: x4 = lambda0^2 + a1*lambda0 - a2 - x2 - x2
sage: y4 = -lambda0*(x4-x2) - y2 - a1*x4 - a3
sage: # P + (P + P) = (x1,y1) + (x2,y2) = (x3,y3)
sage: lambda0 = F((y2-y1)/(x2-x1))
sage: x3 = lambda0^2 + a1*lambda0 - a2 - x1 - x2
sage: y3 = -lambda0*(x3-x1) - y1 - a1*x3 - a3
sage: # P + (P + (P + P)) = (x1,y1) + (x3,y3) = (x5,y5)
sage: lambda0 = F((y3-y1)/(x3-x1))
sage: x5 = lambda0^2 + a1*lambda0 - a2 - x1 - x3
sage: y5 = -lambda0*(x5-x1) - y1 - a1*x5 - a3
sage: # (x4,y4) == (x5,y5)
sage: A(x4.numerator()*x5.denominator()
- x4.denominator()*x5.numerator()),
A(y4.numerator()*y5.denominator()
- y4.denominator()*y5.numerator())
```

En los casos restantes, $Q \neq P, -P, P + P$. La identidad buscada es consecuencia del código

```
sage: # P = (x1,y1), Q = (x2,y2)
sage: A.<a1,a3,a2,a4,a6,x1,y1,x2,y2> = PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1
```

```
- x1^3 - a2*x1^2 - a4*x1 - a6,
y2^2 + a1*x2*y2 + a3*y2 - x2^3 - a2*x2^2 - a4*x2 - a6)
sage: # P + P = 2(x1,y1) = (x3,y3)
sage: lambda0 = F((3*x1^2 + 2*a2*x1 + a4 - a1*y1)/(a1*x1 + a3 + 2*y1))
sage: x3 = lambda0^2 + a1*lambda0 - a2 - x1 - x1
sage: y3 = -lambda0*(x2-x1) - y1 - a1*x3 - a3
sage: # (P + P) + Q = (x3,y3) + (x2,y2) = (x4,y4)
sage: lambda0 = F((y2-y3)/(x2-x3))
sage: x4 = lambda0^2 + a1*lambda0 - a2 - x3 - x2
sage: y4 = -lambda0*(x4-x3) - y3 - a1*x4 - a3
sage: # P + Q = (x1,y1) + (x2,y2) = (x5,y5)
sage: lambda0 = F((y2-y1)/(x2-x1))
sage: x5 = lambda0^2 + a1*lambda0 - a2 - x1 - x2
sage: y5 = -lambda0*(x5-x1) - y1 - a1*x5 - a3
sage: # P + (P + Q) = (x1,y1) + (x5,y5) = (x6,y6)
sage: lambda0 = F((y5-y1)/(x5-x1))
sage: x6 = lambda0^2 + a1*lambda0 - a2 - x1 - x5
sage: y6 = -lambda0*(x6-x1) - y1 - a1*x6 - a3
sage: # (x4,y4) == (x6,y6)
sage: A(x4.numerator()*x6.denominator()
- x4.denominator()*x6.numerator()).reduce(Rels),
A(y4.numerator()*y6.denominator()
- y4.denominator()*y6.numerator()).reduce(Rels)
```

□

Teorema 5.28. *La suma de puntos de una curva elíptica es asociativa.*

Demostración. Hay que demostrar que para cualesquiera $P, Q, R \in E$,

$$P + (Q + R) = (P + Q) + R.$$

Es inmediato observar que el resultado es cierto si alguno de los puntos es $\mathcal{O}$. Como consecuencia de (5.10), los Lemas 5.26 y 5.27 y la Proposición 5.24, la asociatividad también es cierta si dos de los puntos son iguales u opuestos. Concretamente,

$$P + (-P + Q) = Q = \mathcal{O} + Q = (P + -P) + Q,$$

$$\begin{aligned} -P + (P + Q) &= -P + (-(-P) + Q) \\ &= (-P + -(-P)) + Q = (-P + P) + Q, \end{aligned}$$

$$\begin{aligned} P + (Q + -P) = P + (-P + Q) = Q &= -P + (-(-P) + Q) \\ &= -P + (P + Q) = (P + Q) + -P, \end{aligned}$$

$$\begin{aligned} -P + (Q + P) &= -P + (Q + -(-P)) \\ &= (-P + Q) + -(-P) = (-P + Q) + P, \end{aligned}$$

$$\begin{aligned} Q + (P + -P) = (P + -P) + Q &= (-P + P) + Q \\ &= -P + (P + Q) = (P + Q) + -P = (Q + P) + -P, \end{aligned}$$

$$\begin{aligned} Q + (-P + P) &= Q + (-P + -(-P)) \\ &= (Q + -P) + -(-P) = (Q + -P) + P, \end{aligned}$$

$$P + (Q + P) = (Q + P) + P = (P + Q) + P,$$

$$\begin{aligned} Q + (P + P) = (P + P) + Q &= P + (P + Q) \\ &= (P + Q) + P = (Q + P) + P. \end{aligned}$$

Queda estudiar aquellos casos en los que P, Q, R son todos distintos y no opuestos entre ellos. Para realizar las cuatro sumas tenemos que considerar varios casos.

Caso $P = -(Q + R)$. Tenemos que $P = -(Q + R)$ si y sólo si $Q + R = -P$ por (5.10). Por la definición y el Lema 5.19

$$Q + R = -P \iff L \cap E = \{P, Q, R\}$$

donde L es la recta que une Q y R. Como todos los puntos son distintos y no opuestos, tenemos que L es también la recta que une P y Q, por lo que de nuevo por el Lema 5.19 $P + Q = -R$. En consecuencia

$$P + (Q + R) = P + -P = \mathcal{O} = -R + R = (P + Q) + R.$$

Caso $P = Q + R$. Por el Lema 5.27 y la Proposición 5.24,

$$((Q + R) + Q) + R = ((Q + Q) + R) + R = (Q + Q) + (R + R),$$

por lo que la asociatividad se deduce de comprobar la identidad

$$(Q + R) + (Q + R) = (Q + Q) + (R + R).$$

Las sumas de la izquierda pueden hacerse de una única forma por las condiciones que estamos arrastrando, pero las de la derecha necesitan considerar tres casos. En el primero de ellos si $R + R = -(Q + Q) = -Q + -Q$, por los Lemas 5.27 y 5.26,

$$R = R + (R + -R) = (R + R) + -R = \\ (-Q + -Q) + -R = (-R + -Q) + -Q,$$

de donde se deduce que $R + Q = -R + -Q = -(R + Q)$, por tanto

$$(Q + R) + (Q + R) = \mathcal{O} = (Q + Q) + (R + R).$$

Si $R+R = Q+Q$, por el Lema 5.18 $T_R \cap E = T_Q \cap E$, de donde $T_R = T_Q$. Por el Lema 5.17, las primeras coordenadas de Q y R son ambas raíces dobles del polinomio de grado 3 $E(x, \lambda x + \mu$ donde $y = \lambda x + \mu$ es la ecuación de $T_Q = T_R$. Por tanto Q y R tienen la misma primera coordenada y $R = Q$ o $R = -Q$, lo que va en contra de la hipótesis que estamos considerando. Queda el caso $(R + R) \neq -(Q + Q), (Q + Q)$, caso que se deduce del código

```
sage: # (Q + Q) + (R + R) = (Q + R) + (Q + R), Q = (x1,y1), R = (x2,y2)
sage: A.<a1,a3,a2,a4,a6,x1,y1,x2,y2> = PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1 - x1^3 - a2*x1^2 - a4*x1
- a6, y2^2 + a1*x2*y2 + a3*y2 - x2^3 - a2*x2^2 - a4*x2 - a6)
sage: # (Q + Q) = 2(x1,y1) = (x3,y3)
sage: lambda0 = F((3*x1^2 + 2*a2*x1 + a4 - a1*y1)/(a1*x1 + a3 + 2*y1))
sage: x3 = lambda0^2 + a1*lambda0 - a2 - x1 - x1
sage: y3 = -lambda0*(x3-x1) - y1 - a1*x3 - a3
sage: # (R + R) = 2(x2,y2) = (x4,y4)
sage: lambda0 = F((3*x2^2 + 2*a2*x2 + a4 - a1*y2)/(a1*x2 + a3 + 2*y2))
sage: x4 = lambda0^2 + a1*lambda0 - a2 - x2 - x2
sage: y4 = -lambda0*(x4-x2) - y2 - a1*x4 - a3
sage: # (Q + Q) + (R + R) = (x3,y3) + (x4,y4) = (x5,y5)
sage: lambda0 = F((y4-y3)/(x4-x3))
sage: x5 = lambda0^2 + a1*lambda0 - a2 - x3 - x4
sage: y5 = -lambda0*(x5-x3) - y3 - a1*x5 - a3
sage: # Q + R = (x1,y1) + (x2,y2) = (x6,y6)
sage: lambda0 = F((y2-y1)/(x2-x1))
sage: x6 = lambda0^2 + a1*lambda0 - a2 - x1 - x2
sage: y6 = -lambda0*(x6-x1) - y1 - a1*x6 - a3
sage: # (Q + R) + (Q + R) = 2(x6,y6) = (x7,y7)
sage: lambda0 = F((3*x6^2 + 2*a2*x6 + a4 - a1*y6)/(a1*x6 + a3 + 2*y6))
sage: x7 = lambda0^2 + a1*lambda0 - a2 - x6 - x6
sage: y7 = -lambda0*(x7-x6) - y6 - a1*x7 - a3
sage: # x5 == x7
sage: A(x5.numerator()*x7.denominator()
- x5.denominator()*x7.numerator()).reduce(Rels)
sage: # y5 == y7 # Este calculo tarda bastante
sage: A(y5.numerator()*y7.denominator()
- y5.denominator()*y7.numerator()).reduce(Rels)
```

El último caso que nos queda por cubrir es $P \neq (Q+R), -(Q+R)$, es decir, todas la sumas se particularizan a sumar puntos distintos no opuestos. La ejecución del código

```
sage: # P + (Q + R) = (P + Q) + R, P = (x1,y1), Q = (x2,y2), R = (x3,y3)
sage: A.<a1,a3,a2,a4,a6,x1,y1,x2,y2,x3,y3> =
PolynomialRing(RationalField())
sage: F = FractionField(A)
sage: Rels = A.ideal(y1^2 + a1*x1*y1 + a3*y1 - x1^3 - a2*x1^2 - a4*x1
- a6, y2^2 + a1*x2*y2 + a3*y2 - x2^3 - a2*x2^2 - a4*x2 - a6,
y3^2 + a1*x3*y3 + a3*y3 - x3^3 - a2*x3^2 - a4*x3 - a6)
sage: # P + Q, (x1,y1) + (x2,y2) = (x4,y4)
sage: lambda0 = F((y2-y1)/(x2-x1))
sage: x4 = lambda0^2 + a1*lambda0 - a2 - x1 - x2
sage: y4 = -lambda0*(x4-x1) - y1 - a1*x4 - a3
sage: # (P + Q) + R, (x4,y4) + (x3,y3) = (x5,y5)
sage: lambda0 = F((y3-y4)/(x3-x4))
sage: x5 = lambda0^2 + a1*lambda0 - a2 - x4 - x3
sage: y5 = -lambda0*(x5-x4) - y4 - a1*x5 - a3
sage: # Q + R, (x2,y2) + (x3,y3) = (x6,y6)
sage: lambda0 = F((y3-y2)/(x3-x2))
sage: x6 = lambda0^2 + a1*lambda0 - a2 - x2 - x3
sage: y6 = -lambda0*(x6-x2) - y2 - a1*x6 - a3
sage: # P + (Q + R), (x1,y1) + (x6,y6) = (x7,y7)
sage: lambda0 = F((y6-y1)/(x6-x1))
sage: x7 = lambda0^2 + a1*lambda0 - a2 - x1 - x6
sage: y7 = -lambda0*(x7-x1) - y1 - a1*x7 - a3
v# x5 == x7
sage: A(x5.numerator()*x7.denominator()
- x5.denominator()*x7.numerator()).reduce(Rels)
sage: # y5 == y7 # Tarda bastante
sage: A(y5.numerator()*y7.denominator()
- y5.denominator()*y7.numerator()).reduce(Rels)
```

nos demuestra la última identidad necesaria. □

Corolario 5.29. $(E, +)$ *es un grupo conmutativo.*

Demostración. Consecuencia directa de la definición, la Proposición 5.24 y el Teorema 5.28. □

Ejemplo 5.30. Sea $\mathbb{F}_8 = \mathbb{F}_2[\xi]_{\xi^3+\xi+1}$. Sea $E = E(\xi+1, \xi)$, es decir, dada por la ecuación

$$Y^2 + XY + X^3 + (\xi+1)X^2 + \xi.$$

Vamos a calcular $P + Q$ con $P = (\xi+1, \xi)$ y $Q = (\xi^2+\xi, \xi^2)$. El coeficiente λ es

$$\begin{aligned}\lambda = (\xi+\xi^2)(\xi+1+\xi^2+\xi)^{-1} &= (\xi+\xi^2)(1+\xi^2)^{-1} \\ &= \xi^4\xi^{-6} = \xi^5 = \xi^2+\xi+1.\end{aligned}$$

$P + Q = (x_3, y_3)$ donde

$$\begin{aligned}x_3 &= (\xi^2+\xi+1)^2 + \xi^2 + \xi + 1 + \xi + 1 + \xi + 1 + \xi^2 + \xi \\ &= \xi + 1 + 1 = \xi\end{aligned}$$

e

$$y_3 = (\xi^2+\xi+1)(\xi+1+\xi) + \xi + \xi = \xi^2+\xi+1,$$

luego $P + Q = (\xi, \xi^2+\xi+1)$.

Para calcular $2P = P + P$,

$$\begin{aligned}\lambda &= \xi + 1 + \xi(\xi+1)^{-1} = \xi + 1 + \xi(\xi^2+\xi) = \xi^2, \\ x_3 &= (\xi^2)^2 + \xi^2 + (\xi+1) + (\xi+1) + (\xi+1) \\ &= \xi^2 + \xi + \xi^2 + \xi + 1 = 1 \\ y_3 &= \xi^2(\xi+1+1) + 1 + \xi \\ &= (\xi+1) + 1 + \xi = 0,\end{aligned}$$

luego $2P = (1, 0)$.

5.4

Teoremas de Hasse y Rück

Dada una curva elíptica $(E, +)$ con su estructura de grupo, cada entero $n \in \mathbb{Z}$ define un homomorfismo de grupos

$$[n] : E \to E, [P \mapsto nP]\,.$$

Por otra parte, sea E es una curva elíptica definida por una ecuación de Weierstrass (5.8) sobre un cuerpo finito $\mathbb{F}_q$. Sea $K \supseteq \mathbb{F}_q$ y supongamos que $(x, y) \in E(K)$. Entonces

$$\begin{aligned}(y^q)^2 + a_1 x^q y^q + a_3 y^q - (x^q)^3 - a_2 (x^q)^2 - a_4 (x^q) - a_6 = \\ (y^q)^2 + a_1^q x^q y^q + a_3^q y^q - (x^q)^3 - a_2^q (x^q)^2 - a_4^q (x^q) - a_6^q = \\ (y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6)^q = 0^q = 0,\end{aligned}$$

por lo que $(x^q, y^q) \in E(K)$. Como las ecuaciones definidas en el Teorema 5.23 también conmutan con elevar a la potencia q, tenemos que el automorfismo de Frobenius

$$\phi : K \to K, [x \mapsto x^q]$$

se extiende a un homomorfismo de grupos

$$\phi : E(K) \to E(K), [(x, y) \mapsto (x^q, y^q)]$$

también denominado automorfismo de Frobenius. Con estos ingredientes podemos enunciar el teorema de Hasse.

Teorema 5.31 (Hasse)**.** *Sea* E *una curva elíptica sobre un cuerpo finito* $\mathbb{F}_q$ *y sea* $t = q + 1 - |E|$*. Entonces*

1. $\phi \circ \phi - [t] \circ \phi + [q] = [0]$ *en cualquier extensión* $\mathbb{F}_q \subseteq K$.
2. $|t| \leq 2\sqrt{q}$.

Demostración. Ver [3, Theorem 3.61]. □

Otro resultado que debemos destacar por su incidencia posterior es el siguiente

Teorema 5.32 (Rück)**.** *Sea* E *una curva elíptica definida sobre* $\mathbb{F}_q$*. Entonces*

$$E \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

con $n_1 \mid (n_2, q-1)$.

Demostración. Véase [3, Theorem 3.76]. □

5.5 Orden de puntos y curvas

En esta última sección vamos a dar un algoritmo para calcular el orden de una curva elíptica. Dicho algoritmo está basado en el algoritmo de Shank's Baby Step Giant Step presentado como Algoritmo 3.

El procedimiento pasa por varias etapas que vamos a describir.

5.5.1 *Puntos de la curva*

El primer algoritmo, Algoritmo 5, devuelve un punto aleatorio de una curva elíptica.

Algorithm 5 Selección de puntos de una CE

Input: La ecuación de Weierstrass (5.8) de una Curva Elíptica E sobre un cuerpo finito $\mathbb{F}_q$.

Output: Un punto $P \in E$.

1. Selecciona aleatoriamente $x \in \mathbb{F}_q$.
2. Si $E(x, Y) = Y^2 + a_1xY + a_3Y - x^3 - a_2x^2 - a_4x - a_6 = 0$ tiene solución y, devuelve (x, y) o $(x, -y - a_1x - a_3)$. En caso contrario, vuelve al inicio.

Para que el Algoritmo 5 funcione necesitamos poder resolver ecuaciones cuadráticas en $\mathbb{F}_q$. En realidad dicho problema sólo afecta al grupo multiplicativo de las unidades de $\mathbb{F}_q$. Vamos a dividir el problema en dos casos, q impar o $q = 2^\ell$.

Caso $\mathbb{F}_q$ con q impar. No perdemos generalidad en suponer que la curva viene dada por la ecuación (5.3) o por alguna de las ecuaciones (5.4) y (5.5), debemos buscar valores $x_0 \in \mathbb{F}_q$ tales que $x_0^3 + ax_0^2 + bx_0 + c$ es un cuadrado perfecto y calcular dicha raíz cuadrada. El algoritmo es idéntico al Algoritmo 1 presentado en el Capítulo 3. Como $\mathbb{F}_q \setminus \{0\}$ es un grupo cíclico de orden par, es en este marco donde vamos a presentar el algoritmo.

Lema 5.33. *Sea G un grupo cíclico de orden par n. Dado $\beta \in G$, existe γ tal que $\beta = \gamma^2$ si y solo si $\beta^{n/2} = 1$.*

Demostración. Si $\beta = \gamma^2$, entonces $\beta^{n/2} = \gamma^n = 1$ por el Teorema de Lagrange.

Recíprocamente, supongamos que $\beta^{n/2} = 1$. Sea g un generador de G. Existe, por tanto $j < n$ tal que $\beta = g^j$. Si j es impar, $d = (jn/2, n)$ es un divisor propio de n, y como

$$1 = (g^j)^{n/2} = g^{jn/2},$$

tenemos que $g^d = 1$, lo que es imposible por ser n el orden de g . Por tanto j es par y $\beta = \gamma^2$ con $\gamma = g^{j/2}$. □

Las raíces cuadradas pueden calcularse con un algoritmo análogo al Algoritmo 1 para grupos cíclicos de orden par, que presentamos como Algoritmo 6.

Para comprobar la corrección del Algoritmo 6, observemos en primer lugar que sólo existen dos raíces cuadradas de la unidad, es decir, dos elementos cuyo cuadrado es 1. Uno de ellos es 1, y el otro $g^{n/2}$ donde g es cualquier generador de G. Por otra parte, si $\beta^{n/2} \neq 1$, necesariamente $\beta^{n/2} = g^{n/2}$, ya que es una raíz cuadrada de 1. Además, como consecuencia del Lema 5.33, al menos los generadores de G no pueden tener raíces cuadradas, por lo que hay al menos $\varphi(n)$ elementos sin raíz cuadrada.

Como n es par puede ocurrir que $n \equiv 0 \mod 4$ o $n \equiv 2 \mod 4$. Supongamos este segundo caso, es decir, $n + 2 \equiv 0 \mod 4$, entonces $\left(\beta^{\frac{n+2}{4}}\right)^2 = \beta^{\frac{n+2}{2}} = \beta\beta^{\frac{n}{2}} = \beta$, por lo que $\beta^{(n+2)/4}$ es una raíz cuadrada de β.

Nos queda el caso $n \equiv 0 \mod 4$, en el que $\frac{n}{2}$ es par. Sea $\gamma \in G$ un elemento sin raíz cuadrada, es decir, satisface $\gamma^{n/2} = g^{n/2}$, que puede

Algorithm 6 Raíces cuadradas en grupos cíclicos de orden par

Input: G grupo cíclico generado por g de orden par n, y $\beta \in G$
Output: Una raíz cuadrada de β, si existe.

if $\beta^{\frac{n}{2}} = 1$ **then**
  if $n \equiv 2 \mod 4$ **then**
    return $\beta^{\frac{n+2}{4}}$
  else
    $\{n \equiv 0 \mod 4\}$
    Sea γ un elemento sin raíces cuadradas. {Búsqueda aleatoria.}
    Descomponemos $\frac{n}{2} = 2^l r$ con r impar.
    Sea $s_0 = 0$.
    for $1 \leq i \leq l$ **do**
      $y_i = \beta^{2^{l-i}} \gamma^{\frac{s_{i-1}}{2}}$
      if $y_i = 1$ **then**
        $s_i = \frac{s_{i-1}}{2}$
      else
        $s_i = \frac{s_{i-1}}{2} + \frac{n}{2}$
    return $\beta^{\frac{r+1}{2}} \gamma^{\frac{s_l}{2}}$
else
  return β no tiene raíces cuadradas.

ser encontrado por una búsqueda aleatoria. Sean r impar y $l \geq 1$ tales que $\frac{n}{2} = 2^l r$. Sea, además, $s_0 = 0$. Tenemos que

$$\beta^{2^l r}\gamma^{s_0} = \beta^{n/2}\gamma^0 = 1.$$

Supongamos que hemos calculado s_{i-1} tal que $2^{l-i+2} \mid s_{i-1}$ y

$$\beta^{2^{l-i+1}r}\gamma^{s_{i-1}} = 1.$$

Sea $y_i = \beta^{2^{l-i}r}\gamma^{s_{i-1}/2}$. Por nuestra hipótesis $y_i^2 = 1$, por lo que $y_i = 1$ o $y_i = g^{n/2}$. Si $y_i = 1$, llamamos $s_i = \frac{s_{i-1}}{2}$, por lo que $2^{l-i+1} \mid s_i$ y

$$\beta^{2^{l-i}r}\gamma^{s_i} = \beta^{2^{l-i}r}\gamma^{s_{i-1}/2} = y_i = 1.$$

Si $y_i = g^{n/2}$, llamamos $s_i = \frac{s_{i-1}}{2} + \frac{n}{2}$. Dado que $2^l \mid \frac{n}{2}$ tenemos que $2^{l-i+1} \mid s_i$. Además

$$\beta^{2^{l-i}r}\gamma^{s_i} = \beta^{2^{l-i}r}\gamma^{s_{i-1}/2}\gamma^{n/2} = y_i\gamma^{n/2} = g^{n/2}g^{n/2} = 1.$$

En ambos casos, hemos encontrado s_i tal que $2^{l-i+1} \mid s_i$ y

$$\beta^{2^{l-i}r}\gamma^{s_i} = 1.$$

Después de l pasos, llegamos a $s = s_l$ tal que $2 = 2^{l-l+1} \mid s_l$ y

$$\beta^r\gamma^s = \beta^{2^{l-l}r}\gamma^{s_l}01.$$

Por tanto,

$$\left(\beta^{\frac{r+1}{2}}\gamma^{\frac{s}{2}}\right)^2 = \beta^{r+1}\gamma^s = \beta,$$

lo que nos da una raíz cuadrada de β.

El cálculo de raíces cuadradas nos permite encontrar puntos de la curva en el caso $\mathbb{F}_q$ con q impar, ya que en dicho caso $\mathbb{F}_q^*$ es un grupo cíclico de orden par.

Ejemplo 5.34. Vamos a calcular los puntos de la curva $E = E(1,7)$ sobre $\mathbb{F}_{17}$, cuya ecuación es

$$Y^2 = X^3 + X + 7.$$

Para cada $\alpha \in \mathbb{F}_{17}$ comprobamos si $\alpha^3 + \alpha + 7$ es residuo cuadrático, lo que podemos ver en el cuadro 5.1 Por tanto tenemos tres puntos, $(2,0), (7,0), (8,0) \in E$ junto con otros cuatro valores $1, 5, 6, 12$ que pueden proporcionar puntos de la curva. Por ejemplo, para $\alpha = 6$ debemos calcular las dos raíces cuadradas de $\beta = 8$. Como $17 \equiv 1 \mod 4$, nos encontramos en el segundo caso. Buscamos un elemento de $\mathbb{F}_{17}$ que no sea residuo cuadrático, por ejemplo $\gamma = 12$. Como $\frac{17-1}{2} = 2^3$, tenemos que dar tres pasos empezando en la identidad $\beta^{2^3}\gamma^0 = 1$

$$\begin{aligned}
\beta^{2^3}\gamma^0 &\equiv 1 \mod 17,\\
y_1 = \beta^{2^2}\gamma^0 &\equiv -1 \mod 17,\\
\beta^{2^2}\gamma^8 &\equiv 1 \mod 17,\\
y_2 = \beta^2\gamma^4 &\equiv -1 \mod 17,\\
\beta^2\gamma^{4+8} = \beta^2\gamma^{12} &\equiv 1 \mod 17,\\
y_3 = \beta\gamma^6 &\equiv -1 \mod 17,\\
\beta\gamma^{6+8} = \beta\gamma^{14} &\equiv 1 \mod 17,
\end{aligned}$$

Cuadro 5.1: Residuos cuadráticos en $E(1,7)$

α	$\beta = \alpha^3 + \alpha + 7$	β^8
0	7	16
1	9	1
2	0	0
3	3	16
4	7	16
5	1	1
6	8	1
7	0	0
8	0	0
9	14	16
10	14	16
11	6	16
12	13	1
13	7	16
14	11	16
15	14	16
16	5	16

de donde

$$\beta^2\gamma^{14} \equiv \beta \mod 17$$

y

$$\sqrt{\beta} = \pm\beta\gamma^7 \equiv \pm 5 \mod 17.$$

Esta identidad nos da dos nuevos puntos $(6,5),(6,12) \in E$. Los demás puntos se calculan de forma análoga.

Caso $\mathbb{F}_{2^\ell}$. Vamos a centrarnos en las curvas elípticas $E = E(a,b)$ dadas por la ecuación (5.6). Si $(x_0,y_0) \in E$, y_0 es solución de la ecuación cuadrática

$$Y^2 + x_0 Y = x_0^3 + a x_0^2 + b.$$

Para ello necesitamos algunos resultados relativos a la resolución de ecuaciones cuadráticas en característica 2. Recordemos, que para todo $\alpha \in \mathbb{F}_{2^\ell}$, se define la traza como

$$\mathrm{Tr}(\alpha) = \textstyle\sum_{j=0}^{\ell-1} \alpha^{2^j}.$$

La raíz cuadrada en $\mathbb{F}_{2^\ell}$ siempre existe y es única, ya que la aplicación $\tau : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ definida por $\tau(\alpha) = \alpha^2$ es un automorfismo de álgebras, el automorfismo de Frobenius. De hecho τ es automorfismo de álgebras porque $(\alpha+\beta)^2 = \alpha^2 + \beta^2$ en característica 2. En particular

$$\mathrm{Tr}(\alpha) = \textstyle\sum_{j=0}^{\ell-1} \tau^j(\alpha),$$

lo que implica

$$\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta).$$

Además,

$$(\alpha^{2^{\ell-1}})^2 = \alpha^{2^\ell} = \alpha\alpha^{2^\ell - 1} = \alpha,$$

de donde

$$\tau^{-1}(\alpha) = \alpha^{2^{\ell-1}} = \tau^{\ell-1}(\alpha),$$

es decir, $\sqrt{\alpha} = \alpha^{2^{\ell-1}}$ en $\mathbb{F}_{2^\ell}$. La identidad

$$\begin{aligned}\left(\sum_{j=0}^{\ell-1} \alpha^{2^j}\right)^2 &= \sum_{j=0}^{\ell-1} \left(\alpha^{2^j}\right)^2 \\ &= \sum_{j=0}^{\ell-1} \alpha^{2^{j+1}} = \sum_{i=1}^{\ell} \alpha^{2^i} = \sum_{i=0}^{\ell-1} \alpha^{2^i}\end{aligned}$$

implica

$$\mathrm{Tr}(\alpha)^2 = \mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha),$$

de donde $\mathrm{Tr}(\alpha)$ es raíz del polonomio $z^2 - z \in \mathbb{F}_{2^\ell}[z]$, es decir, $\mathrm{Tr}(\alpha) \in \mathbb{F}_2$.

Proposición 5.35. *Los conjuntos*

$$\{\alpha \in \mathbb{F}_{2^\ell} \mid \mathrm{Tr}(\alpha) = 0\}, \quad \{\alpha \in \mathbb{F}_{2^\ell} \mid \mathrm{Tr}(\alpha) = 1\}$$

tienen el mismo cardinal.

Demostración. El polinomio $\sum_{j=0}^{\ell-1} z^{2^j} \in \mathbb{F}_{2^\ell}[z]$ tiene grado $2^{\ell-1}$, luego hay elementos en $\mathbb{F}_{2^\ell}$ que no son raíces del mismo, lo que implica que existe $\alpha_0 \in \mathbb{F}_{2^\ell}$ tal que $\mathrm{Tr}(\alpha_0) = 1$. Dado que

$$\alpha_0 + \{\alpha \in \mathbb{F}_{2^\ell} \mid \mathrm{Tr}(\alpha) = 0\} \subseteq \{\alpha \in \mathbb{F}_{2^\ell} \mid \mathrm{Tr}(\alpha) = 1\}$$

y

$$\alpha_0 + \{\alpha \in \mathbb{F}_{2^\ell} \mid \mathrm{Tr}(\alpha) = 1\} \subseteq \{\alpha \in \mathbb{F}_{2^\ell} \mid \mathrm{Tr}(\alpha) = 0\},$$

tenemos el resultado. □

Dado que

$$Z^2 + \beta = \left(Z + \tau^{-1}(\beta)\right)^2 \in \mathbb{F}_{2^\ell}[Z],$$

las ecuaciones cuadráticas de tipo $z^2 + \beta$ tienen solución siempre. Si $\alpha \neq 0$, el polinomio

$$Z^2 + \alpha Z + \beta \in \mathbb{F}_{2^\ell}[z]$$

se transforma en

$$\alpha^2 T^2 + \alpha^2 T + \alpha^2 \beta \alpha^{-2} \in \mathbb{F}_{2^\ell}[T]$$

mediante el cambio de variable $z = \alpha t$, por lo que es suficiente con saber buscar las raíces de un polinomio de la forma

$$T^2 + T + \beta \in \mathbb{F}_{2^\ell}[T].$$

Proposición 5.36. *La ecuación*

$$T^2 + T + \beta = 0$$

tiene solución si y sólo si $\mathrm{Tr}(\beta) = 0$*, en cuyo caso, si* t_0 *es una solución entonces* $t_0 + 1$ *es la otra solución.*

Demostración. Si $t_0^2 + t_0 + \beta = 0$, entonces

$$\begin{aligned} 0 = \mathrm{Tr}(t_0^2 + t_0 + \beta) &= \mathrm{Tr}(t_0^2) + \mathrm{Tr}(t_0) + \mathrm{Tr}(\beta) \\ &= 2\,\mathrm{Tr}(t_0) + \mathrm{Tr}(\beta) = \mathrm{Tr}(\beta). \end{aligned}$$

Además

$$(t_0+1)^2+(t_0+1)+\beta = t_0^2+1^2+t_0+1+\beta = t_0^2+t_0+\beta = 0,$$

por tanto sólo nos queda demostrar la existencia de solución si $\mathrm{Tr}(\beta) = 0$.

Supongamos que ℓ es impar. Sea

$$f(\alpha) = \sum_{j=0}^{\frac{\ell-1}{2}} \alpha^{2^{2j}}.$$

Dado que

$$f(\alpha)^2+f(\alpha) = \sum_{j=0}^{\frac{\ell-1}{2}} \alpha^{2^{2j+1}} + \sum_{j=0}^{\frac{\ell-1}{2}} \alpha^{2^{2j}} = \mathrm{Tr}(\alpha)+\alpha,$$

para cualquier $\alpha \in \mathbb{F}_{2^\ell}$, tenemos que

$$f(\beta)^2+f(\beta)+\beta = \mathrm{Tr}(\beta) = 0,$$

por lo que $t_0 = f(\beta)$ es una de las dos soluciones. Finalmente, si ℓ es par, sea $\delta \in \mathbb{F}_{2^\ell}$ tal que $\mathrm{Tr}(\delta) = 1$ (que puede ser fácilmente encontrado mediante una búsqueda aleatoria) y sea

$$t_0 = \sum_{i=0}^{\ell-2} \left(\sum_{j=i+1}^{\ell-1} \delta^{2^j} \right) \beta^{2^i}.$$

Tenemos que

$$\begin{aligned}
t_0^2 + t_0 &= \sum_{i=0}^{\ell-2} \left(\sum_{j=i+1}^{\ell-1} \delta^{2^{j+1}} \right) \beta^{2^{i+1}} \\
&\quad + \sum_{i=0}^{\ell-2} \left(\sum_{j=i+1}^{\ell-1} \delta^{2^j} \right) \beta^{2^i} \\
&= \sum_{i=1}^{\ell-1} \left(\sum_{j=i}^{\ell-1} \delta^{2^{j+1}} \right) \beta^{2^i} \\
&\quad + \sum_{i=0}^{\ell-2} \left(\sum_{j=i+1}^{\ell-1} \delta^{2^j} \right) \beta^{2^i} \\
&= \sum_{i=1}^{\ell-1} \left(\sum_{j=i+1}^{\ell} \delta^{2^j} \right) \beta^{2^i} \\
&\quad + \sum_{i=0}^{\ell-2} \left(\sum_{j=i+1}^{\ell-1} \delta^{2^j} \right) \beta^{2^i} \\
&\overset{\dagger}{=} \sum_{i=1}^{\ell-2} \left(\sum_{j=i+1}^{\ell-1} \delta^{2^j} \right) \beta^{2^i} + \delta \sum_{i=1}^{\ell-1} \beta^{2^i} \\
&\quad + \sum_{i=0}^{\ell-2} \left(\sum_{j=i+1}^{\ell-1} \delta^{2^j} \right) \beta^{2^i} \\
&= \delta \sum_{i=1}^{\ell-1} \beta^{2^i} + \left(\sum_{j=1}^{\ell-1} \delta^{2^j} \right) \beta \\
&= \delta(\mathrm{Tr}(\beta) + \beta) + (\mathrm{Tr}(\delta) + \delta)\beta \\
&= \delta\,\mathrm{Tr}(\beta) + \beta,
\end{aligned}$$

donde † se obtiene extrayendo de la primera suma todos los sumandos con $j = \ell$, por lo que $t_0^2 + t_0 + \beta = 0$ ya que $\mathrm{Tr}(\beta) = 0$. □

La demostración de la Proposición 5.36, junto con la observación previa, nos da, de hecho, un algoritmo para dicho cálculo, que presentamos como Algoritmo 7.

Ejemplo 5.37. Sean de nuevo $\mathbb{F}_8 = \mathbb{F}_2[\xi]_{\xi^3+\xi+1}$ y la curva $E = E(\xi, +$

Algorithm 7 Ecuaciones cuadráticas en característica 2

Input: Una ecuación $Z^2 + \alpha Z + \beta$ en $\mathbb{F}_{2^\ell}$.
Output: Las dos soluciones de dicha ecuación, si existen.

```
if Tr(βα^{-2}) = 0 then
    if ℓ es impar then
        t_0 = Σ_{j=0}^{(ℓ-1)/2} (βα^{-2})^{2^{2j}}
    else
        Calcula δ ∈ F_{2^ℓ} tal que Tr(δ) = 1 {Búsqueda aleatoria}
        t_0 = Σ_{i=0}^{ℓ-2} Σ_{j=i+1}^{ℓ-1} δ^{2^j} (βα^{-2})^{2^i}
    return αt_0, αt_0 + α
else
    return No hay solución
```

$1, \xi)$ dada por la ecuación

$$Y^2 + XY + X^3 + (\xi + 1)X^2 + \xi.$$

Los primeros dos puntos de E son $\mathcal{O} \in E$ y $(0, \sqrt{\xi}) = (0, \xi^4) = (0, \xi^2+\xi) \in E$. Para los demás necesitamos conocer, para cada $\alpha \in \mathbb{F}_8$, $\mathrm{Tr}(\alpha^3+(\xi+1)\alpha^2+\xi)$. El cuadro 5.2 contiene dichos valores. Los valores $\xi, \xi+1, \xi^2+\xi, 1$ deben dar nuevos puntos de la curva. Por ejemplo, para $x_0 = \xi^2 + \xi$, transformamos la ecuación

$$Y^2 + x_0 Y = x_0^3 + (\xi + 1)x_0^2 + \xi$$

en la ecuación

$$t^2 + t = x_0 + (\xi + 1) + \xi x_0^{-2} = \xi^2 + \xi + \xi + 1 + \xi(\xi^2 + 1) = \xi^2$$

Cuadro 5.2: Trazas en $E(\xi+1,\xi)$

α	$\beta=\alpha+(\xi+1)+\xi\alpha^{-2}$	$\mathrm{Tr}(\beta)$
ξ	ξ^2	0
ξ^2	1	1
$\xi+1$	ξ^2	0
$\xi^2+\xi$	ξ^2	0
$\xi^2+\xi+1$	$\xi+1$	1
ξ^2+1	ξ^2+1	1
1	0	0

mediante el cambio $t=yx_0^{-1}$. Como $\ell=3$ es impar, las raíces vienen dadas por

$$f(\xi^2)=\sum_{j=0}^{1}(\xi^2)^{2^{2j}}=(\xi^2)^{2^0}+(\xi^2)^{2^2}=\xi^2+\xi,$$

luego $y_0=f(\xi^2)x_0=(\xi^2+\xi)(\xi^2+\xi)=\xi$ nos da los puntos $(\xi^2+\xi,\xi),(\xi^2+\xi,\xi^2)\in E$.

Ejemplo 5.38. Os dejo como ejercicio calcular puntos de la curva $E(\xi,\xi+1)$ sobre $\mathbb{F}_4$.

Como consecuencia de la resolución de ecuaciones cuadráticas en característica 2, observemos que para cualquier $x_0\in\mathbb{F}_{2^\ell}^*$ la ecuación

$$Y^2+x_0Y=x_0^3+ax_0^2+b$$

tiene solución si y solo si $\mathrm{Tr}(x_0 + a + bx_0^{-2}) = 0$, en cuyo caso, si y_0 es solución, $y_0 + x_0$ también lo es. Como $\mathcal{O} \in E(a,b)$ y $(0, \sqrt{\beta}) \in E(a,b)$, tenemos que $|E(a,b)|$ es par. Si asumimos que los elementos de la forma $x_0 + a + bx_0^{-2}$ están uniformemente distribuidos entre aquellos con traza 0 y traza 1, podemos concluir que $|E| \approx 2^{\ell}$.

5.5.2 *Orden de puntos*

El cálculo del orden de un punto se divide en varias partes partes. Todas ellas vamos a presentarlas en el ambiente de un grupo cuyas características incluyen al grupo aditivo de los puntos de una curva elíptica. La primera de ellas es una observación sencilla sobre el orden de un elemento de cuyo orden se conoce un múltiplo.

Algorithm 8 Orden de un punto con torsión conocida

Input: Un grupo G con notación aditiva y elemento neutro $\mathcal{O}$, $P \in G$ y $n > 0$ tal que $nP = \mathcal{O}$.

Output: El orden de P.

$l \leftarrow$ un divisor primo de n
while $\frac{n}{l}P = \mathcal{O}$ **do**
  $n \leftarrow \frac{n}{l}$.
  $l \leftarrow$ un divisor primo de n
return n

El segundo algoritmo calcula el orden de un punto arbitrario

Proposición 5.39. *El Algoritmo 9 es correcto.*

Algorithm 9 Orden de un punto

Input: Un grupo G con notación aditiva y elemento neutro $\mathcal{O}$. Enteros $1 \leq C < B, 0 \leq l_1 < L$

Output: El menor $l \in [C, B]$ tal que $lP = \mathcal{O}$ y $l \equiv l_1 \mod L$, si existe. Si, además, el orden de LP no es mayor que $\frac{B-C+2}{L} - 2$, también se proporciona el orden de LP

1: $A = \{c \in [C, B] \mid c \equiv l_1 \mod L\}$
2: **if** $A = \varnothing$ **then**
3: **return** 'No existe solución'
4: **else**
5: $C_1 \leftarrow \min A$, $B_1 \leftarrow \max A$
6: **if** $C_1 = B_1$ y $C_1P \neq \mathcal{O}$ **then**
7: **return** 'No existe solución'
8: **else if** $C_1 = B_1$ y $C_1P = \mathcal{O}$ **then**
9: **return** C_1
10: **else**
11: $P_1 \leftarrow LP$, $s \leftarrow \left\lceil \sqrt{\frac{B_1 - C_1}{L} + 1} \right\rceil$, $T \leftarrow []$
12: **for** $0 \leq i < s$ **do**
13: $T \leftarrow T + [(i, iP_1)]$
14: $M = []$
15: **for** $0 \leq j < s$ **do**
16: $H_j \leftarrow -C_1P - jsP_1 = H_{j-1} - sP_1$
17: **if** $(i, H_j) \in T$ y $C_1 + (js + i)L \leq B_1$ **then**
18: $M \leftarrow M + [(j, i)]$
19: **if** $M = []$ **then**
20: **return** 'No existe solución'
21: **else**
22: $(j, i) \leftarrow \min_{lex} M$
23: **if** $(j_1, i_1) \in M - [(i, j)]$ **then**
24: **return** $C_1 + (js + i)L, (j_1 - j)s + (i_1 - i)$ {Orden de LP}
25: **else**
26: **return** $C_1 + (js + i)L, 0$

Demostración. Observemos que el algoritmo busca el menor elemento del conjunto

$$\{l \in [C, B] \mid lP = \mathcal{O}, l \equiv l_1 \mod L\} =$$
$$\left\{C_1 + kL \mid k \in \left[0, \tfrac{B_1 - C_1}{L}\right], (C_1 + KL)P = C_1P + kP_1 = \mathcal{O}\right\}.$$

Tenemos que $(j, i) \in M$ significa

$$-C_1P - jsP_1 = iP_1 \iff C_1P + (js + i)P_1 = \mathcal{O}.$$

Dado que cualquier elemento del intervalo $\left[0, \frac{B_1 - C_1}{L}\right]$ tiene una representación de la forma $i + js$ con $0 \leq i, j < s$, podemos asegurar que encontramos todas las parejas de M, y por lo tanto el menor elemento en el conjunto anterior. Es inmediato observar que si encontramos dos elementos distintos en M el algoritmo determina correctamente el orden de P_1. Este caso ocurre exactamente si $|\langle P_1\rangle| \leq \frac{B_1 - C_1}{L}$. Como $C_1 \leq C + (L-1)$ y $B_1 \geq B - (L-1)$, tenemos que $\frac{B_1 - C_1}{L} \geq \frac{B - C + 2}{L} - 2$. Por tanto se calcula $|\langle P_1\rangle|$ si este valor está acotado por $\frac{B - C + 2}{L} - 2$. □

El siguiente paso es un algoritmo que calcule el orden de un elemento en un grupo cociente. Dicho algoritmo se presenta como Algoritmo 10.

Su corrección se basa en el siguiente Lema.

Lema 5.40. *$\exists Q \in \mathcal{G} \mid \frac{h}{p'}P' - Q \in \mathcal{B}$ si y sólo si $\frac{h}{p'}P' \in H$.*

Demostración. Por construcción

$$\begin{aligned}\mathcal{B} + \mathcal{G} &= \{(i + js)P \mid 0 \leq i, j < s\} \\ &= \left\{iP \mid 0 \leq i < \left\lceil \sqrt{l} \right\rceil^2\right\} \\ &= \langle P\rangle = H,\end{aligned}$$

Algorithm 10 Orden de un punto en el grupo cociente

Input: Un grupo G, un subgrupo cíclico normal $H = \langle P \rangle$, $P' \in G$, $l = |H|$ y $l' = |\langle P' \rangle|$

Output: $|\langle P' + H \rangle|$

1: $h \leftarrow l'$, $s \leftarrow \left\lceil \sqrt{l} \right\rceil$
2: $\mathcal{B} \leftarrow \{iP \mid 0 \leq i < s\}$, $\mathcal{G} \leftarrow \{jsP \mid 0 \leq j < s\}$
3: $l' = p_1^{e_1} \cdots p_t^{e_t}$
4: **for all** Divisor primo p' de h **do**
5: **if** $\exists Q \in \mathcal{G} \mid \frac{h}{p'} P' - Q \in \mathcal{B}$ **then**
6: $h \leftarrow \frac{h}{p'}$
7: **return** h

de donde se deduce inmediatamente el resultado. □

Proposición 5.41. *El Algoritmo 10 es correcto.*

Demostración. El algoritmo combina las ideas de los Algoritmos 8 y 9. Dado que $l'P = \mathcal{O} \in H$, el resultado se deduce del Lema anterior. □

5.5.3 *Cardinal de la curva*

Teorema 5.42. *El Algoritmo 11 es correcto.*

Demostración. Veamos que si el algoritmo termina, produce el resultado correcto. Por el Teorema de Hasse, la salida debe estar en el intervalo $[C, B]$, además, el valor de l, fijado P es un divisor de $|E|$. Observemos que $r = 0$ si y sólo si hay un único elemento en el intervalo $[C, B]$, satisfaciendo las condiciones del Algoritmo 9, y como tanto $|E|$ satisface

Algorithm 11 Orden de una curva elíptica E

Input: Una curva elíptica E sobre $\mathbb{F}_q$
Output: $|E|$

1: $C \leftarrow q + 1 - \lfloor 2\sqrt{q} \rfloor$, $B \leftarrow q + 1 + \lfloor 2\sqrt{q} \rfloor$
2: Selecciona un punto aleatorio $P \in E \setminus \{\mathcal{O}\}$ mediante el Algoritmo 5
3: Llamamos al Algoritmo 9 con los parámetros C, B, $L \leftarrow 1$ y $l_1 \leftarrow 0$, siendo la salida l, r
4: **if** $r = 0$ **then**
5: **return** l
6: **else**
7: $\{r = |\langle P \rangle|\}$
8: **repeat**
9: Selecciona un punto aleatorio $P' \in E \setminus \{\mathcal{O}\}$ mediante el Algoritmo 5
10: Llamamos al Algoritmo 9 con los parámetros C, B, $L \leftarrow r$ y $l_1 \leftarrow 0$, siendo la salida l', r'
11: **if** $r' = 0$ **then**
12: **return** l'
13: **else**
14: $\{r'$ es el orden de lP', por lo que $r'lP' = \mathcal{O}\}$
15: Calcula, mediante el Algoritmo 8, y reasigna $r' \leftarrow |\langle P' \rangle|$
16: Intercambia, si es necesario, P y P' para que $R \geq r'$
17: $t \leftarrow |\langle P' + \langle P \rangle \rangle|$ mediante el Algoritmo 10
18: **until** $rt > 2\lfloor 2\sqrt{q} \rfloor$
19: **return** El único elemento en $[C, B]$ que es divisible por r

esas condiciones, necesariamente $l = |E|$ y la salida es correcta. Por otra parte, $r = 0$ si y sólo si $|\langle P\rangle| > \frac{B-C+2}{L} - 2 = 2\left\lfloor 2\sqrt{q}\right\rfloor$, por lo que si $r \neq 0$ tenemos que $|\langle P\rangle| = r \leq 2\left\lfloor 2\sqrt{q}\right\rfloor$.

Elegimos un segundo punto y comprobamos cuantos elementos en el intervalo $[C, B]$ son simultáneamente múltiplos de r y l'. Como $|E|$ satisface esta propiedad, si dicho elemento es único, es decir $r' = 0$, tenemos que $l' = |E|$. En caso contrario, $rt = |\langle P, P'\rangle|$, que divide a $|E|$. El algoritmo terminará cuando $E = \langle P, P'\rangle$. Por el Teorema de Rück, existen P, P' con dicha propiedad, por lo que la probabilidad de terminar en no nula. □

Ejercicio 5.1. Demuestra el Lema 5.2

Ejercicio 5.2. Demuestra la Proposición 5.5.

Ejercicio 5.3. Completa la demostración de la Proposición 5.6. Es decir, comprueba que los cambios de variable indicados transforman la ecuación (5.8) en las ecuaciones (5.4), (5.5), (5.6) y (5.7).

Ejercicio 5.4. Dada la ecuación de Weierstrass

$$E : Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$$

y el cambio de variable admisible

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} u^2 & 0 \\ u^2t & u^3 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix}$$

que transforma E en otra ecuación de Weierstrass E', comprueba que

$$\Delta' = u^{-12}\Delta$$

donde Δ y Δ' son los discriminantes de E y E' respectivamente.

Ejercicio 5.5. Calcula el discriminante y el j-invariante para las ecuaciones (5.3), (5.4), (5.5), (5.6) y (5.7).

Ejercicio 5.6. Sea $G = \langle g \rangle$ de orden par n. Demuestra que 1 y $g^{n/2}$ son los únicos elementos cuyo cuadrado es 1.

Ejercicio 5.7. Calcula todos los puntos de la curva $E(\xi, \xi + 1)$ sobre $\mathbb{F}_4$.

Ejercicio 5.8. Sea $\mathbb{F}_8 = \mathbb{F}_2[\xi]_{\xi^3+\xi+1}$. Sea $E = E(\xi + 1, \xi)$, es decir, la curva dada por la ecuación

$$y^2 + xy = x^3 + (\xi + 1)x^2 + \xi.$$

1. Encuentra todos los $\alpha \in \mathbb{F}_8^*$ tales que
$$\mathrm{Tr}(\alpha + \xi + 1 + \xi\alpha^{-2}) = 0.$$
2. Usa los valores anteriores para calcular todos los puntos de E.
3. Demuestra, usando el Teorema de Rück, que E es un grupo cíclico.
4. Calcula un generador P de E.
5. Calcula $2P, 3P, 4P$, este último de las dos formas posibles, es decir, $3P + P$ y $2(2P)$.

Ejercicio 5.9. Sea $\mathbb{F}_{16} = \mathbb{F}_2[\xi]_{\xi^4+\xi+1}$. Sea $E = E(\xi^3, \xi^2)$, es decir, la curva dada por la ecuación

$$y^2 + xy = x^3 + \xi^3x^2 + \xi^2.$$

1. Encuentra todos los $\alpha \in \mathbb{F}_{16}^*$ tales que
$$\mathrm{Tr}(\alpha + \xi^3 + \xi^2\alpha^{-2}) = 0.$$
2. Usa los valores anteriores para calcular $|E|$.

3. Usa el Teorema de Rück para obtener las posibles estructuras de E como grupo abeliano.

4. Sea $P = (\xi^2, \xi^3 + \xi + 1)$. Comprueba que $P \in E$.

5. Calcula $6P, 9P$. Deduce que E es un grupo cíclico.

Ejercicio 5.10. Sea $\mathbb{F}_{16} = \mathbb{F}_2[\xi]_{\xi^4+\xi+1}$. Sea $E = E(\xi+1, \xi^2+\xi)$, es decir, la curva dada por la ecuación

$$Y^2 + XY + X^3 + (\xi+1)X^2 + (\xi^2+\xi).$$

Toma elementos aleatorios $Q \in E$ y calcula, con el algoritmo de Shanks, $\log_Q \mathcal{O}$, es decir, encuentra n tal que $nQ = \mathcal{O}$. Calcula $|E|$ usando el Algoritmo 11.

Capítulo 6

Criptosistemas basados en curvas elípticas

Para su uso en criptografía, vamos a considerar curvas elípticas sobre $\mathbb{F}_p$ con $p > 3$ o $\mathbb{F}_{2^\ell}$, cuyas ecuaciones simplificadas son (5.4) y (5.6)

6.1 Aritmética en característica $p > 3$

La estructura de grupo de los puntos de una curva elíptica sobre $\mathbb{F}_p$ con $p > 3$ se describe mediante las ecuaciones de la suma simplificada.

Lema 6.1. *Sea* $E(a, b)$ *una curva elíptica sobre* $\mathbb{F}_p$ *con* $p > 3$ *definida por la ecuación* (5.4)*. Si* $(x_0, y_0), (x_0, y_1) \in E$*, entonces* $y_1 = y_0$ *o* $y_1 = -y_0$*.*

Demostración. Inmediato, ya que es este caso $y_0^2 = y_1^2$. □

Proposición 6.2. *Sea* $E(a, b)$ *una curva elíptica sobre* $\mathbb{F}_p$ *con* $p > 3$ *satisfaciendo* (5.4)*. Sean* $P = (x_0, y_0)$*,* $P_1 = (x_1, y_1)$ *y* $P_2 = (x_2, y_2)$ *puntos de* $E(a, b)$*. Entonces,*

(1) $-P = (x_0, -y_0)$.

(2) Si $P_2 = -P_1$, $P_1 + P_2 = \mathcal{O}$.

(3) Si $P_2 \neq -P_1$, $P_1 + P_2 = P_3$, *viene dado por*

$$\begin{aligned} P_3 &= (x_3, y_3) \\ &= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1), \end{aligned}$$

donde

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{si } x_1 \neq x_2, \\ (3x_1^2 + a)(2y_1)^{-1} & \text{si } x_1 = x_2 \text{ e } y_1 = y_2. \end{cases}$$

6.2 Aritmética en característica 2

Proposición 6.3. *Una curva* $E(a, b)$ *sobre* $\mathbb{F}_{2^l}$ *satisfaciendo* (5.6) *tiene un punto singular si y solo si* $b = 0$.

Demostración. Sea $F(x, y) = y^2 + xy + x^3 + ax^2 + b$. E es singular en $(x_0, y_0) \in E$ si y solo si

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0.$$

Dado que

$$\frac{\partial F}{\partial x} = y + 3x^2 + 2ax = y + x^2$$

y

$$\frac{\partial F}{\partial y} = 2y + x = x,$$

el único punto donde puede haber una singularidad es $(0, 0)$ que pertenece a la curva si y solo si $b = 0$. □

Lema 6.4. *Sea* $E = E(a, b)$ *una curva sobre* $\mathbb{F}_{2^l}$ *definida por la ecuación* (5.6). *Si* $(x_0, y_0), (x_0, y_1) \in E$, *entonces* $y_1 = y_0$ *o* $y_1 = x_0 + y_0$.

Demostración. Dado que

$$y_0^2 + x_0 y_0 = x_0^3 + a x_0^2 + b = y_1^2 + x_0 y_1,$$

tenemos que

$$(y_1 + y_0)^2 = y_1^2 + y_0^2 = (y_1 + y_0) x_0.$$

Si $y_0 \neq y_1$, tenemos que $y_0 + y_1 \neq 0$ y en consecuencia $x_0 = y_1 + y_0$, por tanto $y_1 = y_0$ o $y_1 = y_0 + x_0$. □

Proposición 6.5. *Sea* $E(a, b)$ *una curva elíptica sobre* $\mathbb{F}_{2^l}$ *satisfaciendo* (5.6). *Sean* $P = (x_0, y_0)$, $P_1 = (x_1, y_1)$ *y* $P_2 = (x_2, y_2)$ *puntos de* $E(a, b)$. *Entonces,*

(1) $-P = (x_0, x_0 + y_0)$.

(2) Si $P_2 = -P_1$, $P_1 + P_2 = \mathcal{O}$.

(3) Si $P_2 \neq -P_1$, $P_1 + P_2 = P_3$, *viene dado por*

$$\begin{aligned} P_3 &= (x_3, y_3) \\ &= (\lambda^2 + \lambda + a + x_1 + x_2, \lambda(x_1 + x_3) + x_3 + y_1), \end{aligned}$$

donde

$$\lambda = \begin{cases} (y_2 + y_1)(x_2 + x_1)^{-1} & \text{si } x_1 \neq x_2, \\ x_1 + y_1 x_1^{-1} & \text{si } x_1 = x_2. \end{cases}$$

Demostración. La ecuación (5.8) particulariza a (5.6) tomando $a_1 = 1, a_3 = 0, a_2 = a, a_4 = 0, a_6 = b$. Por tanto la aritmética es consecuencia de la aritmética definida para una curva elíptica genérica, observando que, por el Lema 6.4, $x_1 = x_2$ y $P_2 \neq -P_1$ implica $P_2 = P_1$ y por tanto $P_1 + P_2 = 2P_1$. □

6.3 Complejidad de la aritmética en EC

Proposición 6.6. *Sea* E *una curva elíptica dada por* (5.4) *o* (5.6) *en función de la característica del cuerpo base* $\mathbb{F}_q$. *Dados* $P, Q \in E$ *el cálculo* $P + Q$ *es* $\mathcal{O}\left((\log q)^3\right)$.

Demostración. Por la Proposición 6.5 en característica 2, si $P \neq Q$ hay que realizar 9 sumas, 3 multiplicaciones y 1 inverso, y si $P = Q$ una suma menos, por lo que la complejidad está dominada por el cálculo del inverso que es $\mathcal{O}\left((\log q)^3\right)$ por el análogo polinomial de la Proposición 1.7. En característica $p > 3$ el resultado es equivalente. □

Proposición 6.7. *Sea* E *una curva elíptica dada por* (5.4) *o* (5.6) *en función de la característica del cuerpo base* $\mathbb{F}_q$. *Dados* $P \in E$ *y* $m \in \mathbb{N}$, *el cálculo* mP *es* $\mathcal{O}\left((\log q)^3 (\log m)\right)$.

Demostración. Empleando el equivalente a los cuadrados iterados pero en notación aditiva (duplicados iterados) tenemos que

$$mP = 2\left(2\left(\cdots 2\left(2\left(m_t P\right) + m_{t-1} P\right)\cdots\right) + m_1 P\right) + m_0 P$$

donde $m_t m_{t-1} \cdots m_1 m_0$ es la expresión binaria de m. Hay que realizar un máximo de $3 \log_2 m$ sumas para calcular mP. El resultado se deduce de la Proposición 6.6. □

Estas dos proposiciones nos indican que la aritmética en una curva elíptica es una operación eficiente. El problema del logaritmo discreto en una curva elíptica E sobre un cuerpo finito consiste en dado $P \in E$ y $Q \in \langle P \rangle$, calcular $\log_P(Q)$, donde

$$\log_P(Q) = m \iff Q = mP.$$

Para el cálculo del logaritmo en curvas elípticas podemos emplear cualquiera de los dos algoritmos genéricos conocidos, el Algoritmo 3 de Shanks y el Algoritmo 4 de Silver-Pohlig-Hellman. Para aplicar el primero necesitamos una cota superior del orden de E, y para el segundo necesitamos conocer explícitamente dicho orden y que se descomponga como producto de primos pequeños. En cualquier caso ninguno de estos algoritmos es polinomial.

6.4 Parámetros para uso criptográfico

Para su uso en criptografía, necesitamos los siguientes parámetros:

- El cuerpo base $\mathbb{F}_q$
- Los parámetros $a, b \in \mathbb{F}_q$ que definen la curva E mediante las ecuaciones (5.4) o (5.6).
- Un punto base $Q \in E$ cuyo orden n es un primo grande.
- El cofactor h tal que $|E| = hn$.

Lema 6.8. *Sea* E *una curva elíptica tal que* $|E| = hn$ *con* n *primo y* $h < n$. *Entonces* E *tiene un único subgrupo* E_n *de orden* n *que es cíclico y generado por cualquiera de sus elementos distintos de* $\mathcal{O}$.

Demostración. Por el Teorema de Rück, $E \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$, con $d_1 \mid d_2$. Como $h < n$ tenemos que $n \mid d_2$ pero $n \nmid d_1$. Por tanto E_n se corresponde con el subgrupo $\{0\} \times \left\langle \frac{d_2}{n} \right\rangle \leq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$. □

Las curvas elípticas que satisfacen que $|E| = hn$ con n primo y h pequeño se llaman *curvas de orden próximo a primo*, y E_n es el *subgrupo de orden primo*.

Selección de la curva. Como el grupo que vamos a emplear para las claves es en realidad E_n, necesitamos que el problema del logaritmo discreto sea difícil en E_n. Para seleccionar la curva debemos evitar los siguientes casos

- Curvas supersingulares (por ejemplo las definidas por (5.7)). En estas curvas $E_n \cong \mathbb{F}_{q^l}^*$ con l pequeño. Este hecho fue demostrado por Menezes-Okamoto-Vanstone empleando el llamado par de Weil. En realidad basta con comprobar que $n \nmid q^l - 1$ para valores pequeños de l.
- Curvas sobre $\mathbb{F}_p$ tales que $|E| = p$. En este caso, Semaev, Smart y Satoh-Araki construyen un isomorfismo $E \cong \mathbb{F}_p$ mediante un algoritmo en tiempo polinomial, lo que reduce el logaritmo discreto al uso del algoritmo de Euclides extendido en $\mathbb{F}_p$.

La curva debería elegirse mediante una búsqueda aleatoria para evitar sesgos en familias que hipotéticamente pudieran ser comprobadas

como inseguras en el futuro[1]. Se eligen los parámetros $a, b \in \mathbb{F}_q$. Se calcula $|E(a,b)|$ y se observa si $|E(a,b)| = hn$ para h pequeño con n primo. Se comprueba que no son vulnerables a los ataques anteriores.

Existen suficientes curvas con orden próximo a primo para que una búsqueda aleatoria sea efectiva en la práctica. Si el cuerpo base es primo, existen muchas curvas de orden primo. En característica 2 el orden es par, por lo que se buscan curvas con cofactor $h = 2$.

Selección del punto base. Sea $E = E(a,b)$ una curva elíptica tal que $|E| = hn$ con n primo y h pequeño. Para encontrar un punto de orden n seleccionamos aleatoriamente $P \in E$, calculamos $Q = hP$ y comprobamos si $Q \neq \mathcal{O}$. Como n es primo y $nQ = \mathcal{O}$, Q será un generador de E_n. Si $Q = \mathcal{O}$ tomamos empezamos con un nuevo P.

6.5 Protocolo ECDH

Fijamos una curva elíptica $E = E(a,b)$ tal que $|E| = hn$ con n primo y h pequeño. Fijamos también Q un elemento de orden n. La estructura de grupo de una curva elíptica permite establecer un protocolo de intercambio de claves análogo al protocolo de Diffie-Hellman. La conjetura de Diffie y Hellman para curvas elípticas puede presentarse como sigue

Conjetura 6.9 (Diffie-Hellman)**.** *Conocidos* $P_A = aQ$ *y* $P_B = bQ$

[1] Sin embargo, en la actualidad se procede justo al revés, las implementaciones de algoritmos criptográficos sobre curvas elípticas se limitan a algunas decenas de curvas conocidas.

para ciertos $1 \leq a, b \leq n$*, calcular* abQ *es computacionamente equivalente a calcular* $a = \log_Q(P_A)$ *o* $b = \log_Q(P_B)$.

El protocolo es el siguiente:

- Alice y Bob se ponen de acuerdo en la curva elíptica E y el punto $Q \in E$.
- Alice elige aleatoriamente $2 \leq a \leq n-1$ y envía a Bob $P_A = aQ$.
- Bob elige aleatoriamente $2 \leq b \leq n-1$, envía a Alice $P_B = bQ$ y calcula $b(P_A)$.
- Alice calcula $a(P_B)$.
- La clave compartida es $(ab)Q = a(P_B) = b(P_A)$.

6.6

Criptosistema ElGamal en EC

Parámetros y clave pública. Alicia elige una curva elíptica E de orden hn próximo a primo sobre un cuerpo finito y un punto $Q \in E$ de orden primo n. A continuación elige $2 \leq a \leq n-1$ y hace público (E, Q, aQ), manteniendo en privado el valor de a.

Cifrado. Para enviar un mensaje cifrado a Alice, Bob codifica dicho mensaje como $M \in E$, elige aleatoriamente $2 \leq k \leq n-1$, y transmite a Alic3 $E(M) = (kQ, M + k(aQ))$.

Descifrado. Alice calcula $D(C_1, C_2) = C_2 - aC_1$. Efectivamente,

$$D(kQ, M + k(aQ)) = M + k(aQ) - a(kQ) = M.$$

En esta construcción hemos dejado de lado el problema de convertir un mensaje en un punto de la curva. Si empleamos este criptosistema como parte de un criptosistema híbrido, podemos transmitir una clave de sesión como $K = lQ$ para cierto $1 \leq l \leq n$ aleatorio. En cualquier caso, nuestro mensaje puede siempre identificarse con un número dentro de un cierto rango, ¿cómo asociamos unívocamente un número con un punto de nuestra curva?.

6.7 ECDSA

De manera análoga a los protocolos basados en el problema del logaritmo discreto en $\mathbb{Z}_p^*$, las curvas elípticas son la base de un estándar de firma digital basado en la dificultad de resolver el logaritmo discreto en ellas.

Parámetros. Una curva elíptica $E = E(a, b)$ sobre un cuerpo finito $\mathbb{F}_q$, de la que conocemos su orden hn y en la que hemos seleccionado un punto $Q \in E$ de orden primo n.

Generación de claves. Alice genera de forma aleatoria $1 \leq d_A \leq n - 1$, que mantiene como clave secreta. Calcula $P_A = d_A Q$, que distribuye como clave pública.

Algoritmo de firma. Los mensajes son elementos $m \in \mathbb{Z}_n$, normalmente obtenido como el hash de un mensaje de tamaño arbitrario.

1. Genera aleatoriamente un valor $1 \leq k \leq n-1$.
2. Calcula $kQ = (x, y)$, convierte la coordenada x a un entero[2], y calcula $r = x \bmod n$. Si $r = 0$ volvemos al paso 1.
3. Calcula $s = k^{-1}(m + rd_A) \bmod n$. Si $s = 0$, se vuelve al paso 1.
4. (r, s) es la firma del mensaje m.

Algoritmo de verificación El mensaje firmado es una tripleta (m, r, s) de elementos en $\mathbb{Z}_n$. Disponemos de P_A, además de los parámetros de la curva, para verificar la firma.

1. Se comprueba que $(r, s) \in \mathbb{Z}_n^* \times \mathbb{Z}_n^*$, rechazando la firma en caso contrario.
2. Se calcula $v = s^{-1} \bmod n$, $w_1 = mv \bmod n$, $w_2 = rv \bmod n$, y $R = w_1 Q + w_2 P_A \in E$. Si $R = \mathcal{O}$, se rechaza la firma.
3. Si $R = (x', y')$, convertimos x' a entero. Si $x' \equiv r \mod n$, la firma se acepta, en caso contrario se rechaza

Proposición 6.10. *Si* (r, s) *es la firma generada para el mensaje* m*, entonces* $x' \equiv r \mod n$.

[2]Si $\mathbb{F}_q = \mathbb{Z}_p$, nuestra coordenada ya es un número entero, si $\mathbb{F}_q = \mathbb{F}_{2^\ell}$, identificamos sus elementos con números en binario.

Demostración. Dado que

$$k \equiv s^{-1}(m + rd_A) \equiv s^{-1}m + s^{-1}rd_A \equiv w_1 + w_2 d_A \mod n,$$

tenemos que

$$kQ = w_1 Q + w_2 d_A Q = w_1 Q + w_2 P_A = R,$$

luego $r \equiv x' \mod n$. □

Seguridad

- Si permitiésemos $r = 0$, la firma no dependería de la clave privada d_A.
- Dados m y r, encontrar s tal que $R = s^{-1}(mQ + rP_A)$ es equivalente a calcular un logaritmo discreto.
- Dado m, encontrar (r, s) tales que r es la primera coordenada de $R = s^{-1}(mQ+rP_A)$ no se sabe que sea equivalente a calcular un logaritmo discreto, sin embargo no hay evidencias de que pueda hacerse de forma eficiente.

6.8 Codificación de mensajes

Sea E una curva elíptica con orden próximo a primo sobre un cuerpo $\mathbb{F}_q$. Es natural que nuestros mensajes puedan verse como elementos $m \in \mathbb{F}_q$. Una forma de codificar en un punto de la curva sería la siguiente:

1. Elegimos aleatoriamente $r \in \mathbb{F}_q^*$ y llamamos $x_0 = rm$.
2. Si existe $y_0 \in \mathbb{F}_q$ tal que $(x_0, y_0) \in E$, asociamos a m el punto $M = (x_0, y_0)$. En caso contrario volvemos al paso anterior.

Como ya hemos analizado, sobre la mitad de los elementos de $\mathbb{F}_q$ aparecen como primera coordenada de un punto en E, por lo que un par de intentos deberían bastar para encontrar un punto. Podemos tratar de que $(x_0, y_0) \in E_n$, lo que baja la probabilidad a $\frac{1}{2h}$. El valor r debe ser transmitido para que el receptor pueda recuperar m a partir de r y x_0.

6.9

Criptosistema de Menezes-Vanstone

La generación de claves es idéntica a ECDH y a ElGamal sobre EC. Los mensajes van a ser parejas $(m_1, m_2) \in \mathbb{F}_q^2$. Para cifrar un mensaje, seleccionamos aleatoriamente $2 \leq k \leq n-1$, calculamos kQ y $(x_0, y_0) = k(aQ)$. Si $x_0 y_0 = 0$ tomamos un nuevo k. El criptograma es

$$E(m_1, m_2) = (kQ, x_0 m_1, y_0 m_2).$$

Para descifrar un criptograma (C_1, c_2, c_3), Alicia calcula $a(C_1) = a(kQ) = k(aQ) = (x_0, y_0)$ y

$$D(C_1, c_2, c_3) = (x_0^{-1} c_2, y_0^{-1} c_3).$$

Los valores x_0, y_0 no son independientes, satisfacen la ecuación de la curva elíptica. Un atacante que averigüe cualquiera de las dos mitades del mensaje, puede calcular la otra mitad. Por este motivo, se suele tomar m_1 como el mensaje y m_2 como valor aleatorio.

6.10

Curvas en OpenSSL

OpenSSL es un proyecto de código abierto que proporciona un conjunto de herramientas robustas, completas y de nivel comercial para los protocolos TLS y SSL. Incluye una biblioteca criptográfica de propósito general. La mejor fuente de información sobre **OpenSSL** podéis encontrarla en `https://www.openssl.org/`.

OpenSSL dispone de varias curvas elípticas implementadas. Podemos acceder al listado de aquellas disponibles en nuestra implementación mediante la orden

```
openssl ecparam -list_curves
```

En mi implementación, la salida a la orden anterior es

```
secp112r1 : SECG/WTLS curve over a 112 bit prime field
secp112r2 : SECG curve over a 112 bit prime field
secp128r1 : SECG curve over a 128 bit prime field
secp128r2 : SECG curve over a 128 bit prime field
secp160k1 : SECG curve over a 160 bit prime field
secp160r1 : SECG curve over a 160 bit prime field
secp160r2 : SECG/WTLS curve over a 160 bit prime field
secp192k1 : SECG curve over a 192 bit prime field
secp224k1 : SECG curve over a 224 bit prime field
secp224r1 : NIST/SECG curve over a 224 bit prime field
secp256k1 : SECG curve over a 256 bit prime field
secp384r1 : NIST/SECG curve over a 384 bit prime field
secp521r1 : NIST/SECG curve over a 521 bit prime field
prime192v1: NIST/X9.62/SECG curve over a 192 bit prime field
prime192v2: X9.62 curve over a 192 bit prime field
prime192v3: X9.62 curve over a 192 bit prime field
prime239v1: X9.62 curve over a 239 bit prime field
prime239v2: X9.62 curve over a 239 bit prime field
prime239v3: X9.62 curve over a 239 bit prime field
prime256v1: X9.62/SECG curve over a 256 bit prime field
sect113r1 : SECG curve over a 113 bit binary field
sect113r2 : SECG curve over a 113 bit binary field
sect131r1 : SECG/WTLS curve over a 131 bit binary field
sect131r2 : SECG curve over a 131 bit binary field
sect163k1 : NIST/SECG/WTLS curve over a 163 bit binary field
sect163r1 : SECG curve over a 163 bit binary field
```

```
  sect163r2 : NIST/SECG curve over a 163 bit binary field
  sect193r1 : SECG curve over a 193 bit binary field
  sect193r2 : SECG curve over a 193 bit binary field
  sect233k1 : NIST/SECG/WTLS curve over a 233 bit binary field
  sect233r1 : NIST/SECG/WTLS curve over a 233 bit binary field
  sect239k1 : SECG curve over a 239 bit binary field
  sect283k1 : NIST/SECG curve over a 283 bit binary field
  sect283r1 : NIST/SECG curve over a 283 bit binary field
  sect409k1 : NIST/SECG curve over a 409 bit binary field
  sect409r1 : NIST/SECG curve over a 409 bit binary field
  sect571k1 : NIST/SECG curve over a 571 bit binary field
  sect571r1 : NIST/SECG curve over a 571 bit binary field
  c2pnb163v1: X9.62 curve over a 163 bit binary field
  c2pnb163v2: X9.62 curve over a 163 bit binary field
  c2pnb163v3: X9.62 curve over a 163 bit binary field
  c2pnb176v1: X9.62 curve over a 176 bit binary field
  c2tnb191v1: X9.62 curve over a 191 bit binary field
  c2tnb191v2: X9.62 curve over a 191 bit binary field
  c2tnb191v3: X9.62 curve over a 191 bit binary field
  c2pnb208w1: X9.62 curve over a 208 bit binary field
  c2tnb239v1: X9.62 curve over a 239 bit binary field
  c2tnb239v2: X9.62 curve over a 239 bit binary field
  c2tnb239v3: X9.62 curve over a 239 bit binary field
  c2pnb272w1: X9.62 curve over a 272 bit binary field
  c2pnb304w1: X9.62 curve over a 304 bit binary field
  c2tnb359v1: X9.62 curve over a 359 bit binary field
  c2pnb368w1: X9.62 curve over a 368 bit binary field
  c2tnb431r1: X9.62 curve over a 431 bit binary field
  wap-wsg-idm-ecid-wtls1: WTLS curve over a 113 bit binary field
  wap-wsg-idm-ecid-wtls3: NIST/SECG/WTLS curve over a 163 bit binary field
  wap-wsg-idm-ecid-wtls4: SECG curve over a 113 bit binary field
  wap-wsg-idm-ecid-wtls5: X9.62 curve over a 163 bit binary field
  wap-wsg-idm-ecid-wtls6: SECG/WTLS curve over a 112 bit prime field
  wap-wsg-idm-ecid-wtls7: SECG/WTLS curve over a 160 bit prime field
  wap-wsg-idm-ecid-wtls8: WTLS curve over a 112 bit prime field
  wap-wsg-idm-ecid-wtls9: WTLS curve over a 160 bit prime field
  wap-wsg-idm-ecid-wtls10: NIST/SECG/WTLS curve over a 233 bit binary field
  wap-wsg-idm-ecid-wtls11: NIST/SECG/WTLS curve over a 233 bit binary field
  wap-wsg-idm-ecid-wtls12: WTLS curve over a 224 bit prime field
  Oakley-EC2N-3:
IPSec/IKE/Oakley curve #3 over a 155 bit binary field.
Not suitable for ECDSA.
Questionable extension field!
  Oakley-EC2N-4:
IPSec/IKE/Oakley curve #4 over a 185 bit binary field.
Not suitable for ECDSA.
Questionable extension field!
  brainpoolP160r1: RFC 5639 curve over a 160 bit prime field
  brainpoolP160t1: RFC 5639 curve over a 160 bit prime field
  brainpoolP192r1: RFC 5639 curve over a 192 bit prime field
  brainpoolP192t1: RFC 5639 curve over a 192 bit prime field
  brainpoolP224r1: RFC 5639 curve over a 224 bit prime field
  brainpoolP224t1: RFC 5639 curve over a 224 bit prime field
  brainpoolP256r1: RFC 5639 curve over a 256 bit prime field
  brainpoolP256t1: RFC 5639 curve over a 256 bit prime field
  brainpoolP320r1: RFC 5639 curve over a 320 bit prime field
```

```
  brainpoolP320t1: RFC 5639 curve over a 320 bit prime field
  brainpoolP384r1: RFC 5639 curve over a 384 bit prime field
  brainpoolP384t1: RFC 5639 curve over a 384 bit prime field
  brainpoolP512r1: RFC 5639 curve over a 512 bit prime field
  brainpoolP512t1: RFC 5639 curve over a 512 bit prime field
  FRP256v1  : FRP256v1
  id-GostR3410-2001-TestParamSet: GOST R 34.10-2001 Test Curve
  id-GostR3410-2001-CryptoPro-A-ParamSet: GOST R 34.10-2001 CryptoPro-A
  id-GostR3410-2001-CryptoPro-B-ParamSet: GOST R 34.10-2001 CryptoPro-B
  id-GostR3410-2001-CryptoPro-C-ParamSet: GOST R 34.10-2001 CryptoPro-C
  id-GostR3410-2001-CryptoPro-XchA-ParamSet: GOST R 34.10-2001 CryptoPro-XchA
  id-GostR3410-2001-CryptoPro-XchB-ParamSet: GOST R 34.10-2001 CryptoPro-XchB
  id-tc26-gost-3410-2012-512-paramSetA: GOST R 34.10-2012 TC26-A
  id-tc26-gost-3410-2012-512-paramSetB: GOST R 34.10-2012 TC26-B
```

Podemos acceder a los parámetros de cada una de dichas curvas. Por ejemplo, la orden

```
openssl ecparam -name sect233r1 -param_enc
explicit -text -noout
```

da como salida

```
Field Type: characteristic-two-field
Basis Type: tpBasis
Polynomial:
    02:00:00:00:00:00:00:00:00:00:00:00:00:00:
    00:00:00:00:00:04:00:00:00:00:00:00:00:01
A:    1 (0x1)
B:
    66:64:7e:de:6c:33:2c:7f:8c:09:23:bb:58:21:3b:
    33:3b:20:e9:ce:42:81:fe:11:5f:7d:8f:90:ad
Generator (uncompressed):
    04:00:fa:c9:df:cb:ac:83:13:bb:21:39:f1:bb:75:
    5f:ef:65:bc:39:1f:8b:36:f8:f8:eb:73:71:fd:55:
    8b:01:00:6a:08:a4:19:03:35:06:78:e5:85:28:be:
    bf:8a:0b:ef:f8:67:a7:ca:36:71:6f:7e:01:f8:10:
    52
Order:
    01:00:00:00:00:00:00:00:00:00:00:00:00:00:
    13:e9:74:e7:2f:8a:69:22:03:1d:26:03:cf:e0:d7
Cofactor:  2 (0x2)
Seed:
    74:d5:9f:f0:7f:6b:41:3d:0e:a1:4b:34:4b:20:a2:
    db:04:9b:50:c3
```

Esta salida se interpreta de la siguiente forma:

- La descripción de la curva nos indica que el polinomio con respecto al que hacemos reducción modular tiene coeficiente 1 en los grados 233, 74 y 0, luego el cuerpo es $\mathbb{F}_{2^{233}} = \mathbb{F}_2[\xi]_{\xi^{233}+\xi^{74}+1}$.

- La curva es $y^2 + xy = x^3 + ax^2 + b$, donde $a = 1$ y b es el polinomio cuyos coeficientes escritos como lista binaria (escrita en hexadecimal) son

```
b = 0x66647ede6c332c7f8c0923bb58213b333b20e9ce4281fe115f7d8f90ad,
```

es decir

$$\begin{aligned} b = {} & \xi^{230} + \xi^{229} + \xi^{226} + \xi^{225} + \xi^{222} + \xi^{221} + \xi^{218} \\ & + \xi^{214} + \xi^{213} + \xi^{212} + \xi^{211} + \xi^{210} + \xi^{209} + \xi^{207} \\ & + \xi^{206} + \xi^{204} + \xi^{203} + \xi^{202} + \xi^{201} + \xi^{198} + \xi^{197} \\ & + \xi^{195} + \xi^{194} + \xi^{189} + \xi^{188} + \xi^{185} + \xi^{184} + \xi^{181} \\ & + \xi^{179} + \xi^{178} + \xi^{174} + \xi^{173} + \xi^{172} + \xi^{171} + \xi^{170} \\ & + \xi^{169} + \xi^{168} + \xi^{167} + \xi^{163} + \xi^{162} + \xi^{155} + \xi^{152} \\ & + \xi^{149} + \xi^{145} + \xi^{144} + \xi^{143} + \xi^{141} + \xi^{140} + \xi^{139} \\ & + \xi^{137} + \xi^{136} + \xi^{134} + \xi^{132} + \xi^{131} + \xi^{125} + \xi^{120} \\ & + \xi^{117} + \xi^{116} + \xi^{115} + \xi^{113} + \xi^{112} + \xi^{109} + \xi^{108} \\ & + \xi^{105} + \xi^{104} + \xi^{101} + \xi^{100} + \xi^{99} + \xi^{97} + \xi^{96} \\ & + \xi^{93} + \xi^{87} + \xi^{86} + \xi^{85} + \xi^{83} + \xi^{80} + \xi^{79} \\ & + \xi^{78} + \xi^{75} + \xi^{74} + \xi^{73} + \xi^{70} + \xi^{65} + \xi^{63} \\ & + \xi^{56} + \xi^{55} + \xi^{54} + \xi^{53} + \xi^{52} + \xi^{51} + \xi^{50} \\ & + \xi^{49} + \xi^{44} + \xi^{40} + \xi^{38} + \xi^{36} + \xi^{35} + \xi^{34} \\ & + \xi^{33} + \xi^{32} + \xi^{30} + \xi^{29} + \xi^{28} + \xi^{27} + \xi^{26} \\ & + \xi^{24} + \xi^{23} + \xi^{19} + \xi^{18} + \xi^{17} + \xi^{16} + \xi^{15} \\ & + \xi^{12} + \xi^{7} + \xi^{5} + \xi^{3} + \xi^{2} + 1. \end{aligned}$$

- El punto base tiene por coordenadas los polinomios correspondientes a las listas de bits que en hexadecimal se representan co-

mo

$$Q = (0x00fac9dfcbac8313bb2139f1bb755fef65bc391f8b36f8f8eb7371fd558b,\ 0x01006a08a41903350678e58528bebf8a0beff867a7ca36716f7e01f81052)$$

- El orden de Q es

$$n = 0x0100000000000000000000000013e974e72f8a6922031d2603cfe0d7$$

- El cofactor es $h = 2$.

La orden

```
openssl ecparam -name prime239v3 -param_enc
explicit -text -noout
```

da como salida

```
Field Type: prime-field
Prime:
    7f:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:7f:ff:ff:
    ff:ff:ff:80:00:00:00:00:00:7f:ff:ff:ff:ff:ff
A:
    7f:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:7f:ff:ff:
    ff:ff:ff:80:00:00:00:00:00:7f:ff:ff:ff:ff:fc
B:
    25:57:05:fa:2a:30:66:54:b1:f4:cb:03:d6:a7:50:
    a3:0c:25:01:02:d4:98:87:17:d9:ba:15:ab:6d:3e
Generator (uncompressed):
    04:67:68:ae:8e:18:bb:92:cf:cf:00:5c:94:9a:a2:
    c6:d9:48:53:d0:e6:60:bb:f8:54:b1:c9:50:5f:e9:
    5a:16:07:e6:89:8f:39:0c:06:bc:1d:55:2b:ad:22:
    6f:3b:6f:cf:e4:8b:6e:81:84:99:af:18:e3:ed:6c:
    f3
Order:
    7f:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:7f:ff:ff:
    97:5d:eb:41:b3:a6:05:7c:3c:43:21:46:52:65:51
Cofactor:  1 (0x1)
Seed:
    7d:73:74:16:8f:fe:34:71:b6:0a:85:76:86:a1:94:
    75:d3:bf:a2:ff
```

Esta salida es más fácil de interpretar pues los valores son enteros escritos en hexadecimal.

- El cuerpo es

$$\mathbb{F}_{0x7fffffffffffffffffffffff7fffffffff8000000000007fffffffff}.$$

- La curva es $y^2 = x^3 + ax + b$, donde

$$a = 0x7fffffffffffffffffffffff7fffffffff8000000000007fffffffffc$$
$$b = 0x255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e,$$

- El punto base tiene por coordenadas

$$Q = (0x6768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a,$$
$$0x1607e6898f390c06bc1d552bad226f3b6fcfe48b6e818499af18e3ed6cf3)$$

- El orden de Q es

$$n = 0x7fffffffffffffffffffffff7fffff975deb41b3a6057c3c432146526551$$

- El cofactor es $h = 1$

UNIVERSITAS GRANATENSIS
PLUS ULTRA
1531

Ejercicios de evaluación de criptosistemas basados en curvas elípticas

Ejercicio. Sea $\mathbb{F}_{32} = \mathbb{F}_2[\xi]_{\xi^5+\xi^2+1}$. Cada uno de vosotros, de acuerdo a su número de DNI o similar, dispone de una curva elíptica sobre $\mathbb{F}_{32}$ y un punto base dados en el Cuadro 6.1.

1. Calcula, mediante el algoritmo de Shank o mediante el Algoritmo 9, $\log_Q \mathcal{O}$.
2. Para tu curva y tu punto base, genera un par de claves pública/privada para un protocolo ECDH.
3. Cifra el mensaje $(\xi^3 + \xi^2 + 1, \xi^4 + \xi^2) \in \mathbb{F}_{32}^2$ mediante el criptosistema de Menezes-Vanstone
4. Descifra el mensaje anterior.

Cuadro 6.1: Curvas elípticas

dni mod 32	$E(A, B)$	Q
0	$E(\xi^3, \xi)$	$(\xi^4+\xi+1, \xi^4+\xi^2+\xi)$
1	$E(\xi^4+\xi^3+\xi^2+\xi, \xi)$	$(\xi^4+\xi^2+1, \xi^4+\xi^3+\xi^2+\xi+1)$
2	$E(\xi^4+1, \xi)$	$(\xi^3+\xi^2, \xi^3+\xi^2+1)$
3	$E(\xi^3+\xi^2+\xi, \xi^4)$	$(\xi^4+\xi^2+\xi+1, \xi)$
4	$E(\xi^4+\xi^2+\xi+1, \xi^4)$	$(\xi^4+1, \xi^2+\xi)$
5	$E(\xi^2+1, \xi^4+\xi^3+\xi+1)$	$(\xi^3+\xi^2+\xi, \xi+1)$
6	$E(\xi^2+\xi+1, \xi^2)$	$(\xi^4+\xi+1, \xi^4)$
7	$E(\xi+1, \xi^4+\xi^3+\xi+1)$	$(\xi^3+\xi^2+\xi, \xi^4+\xi^3+\xi^2+\xi+1)$
8	$E(\xi^2+\xi+1, \xi^4+\xi^3+\xi+1)$	$(\xi^4+1, \xi^3+\xi^2)$
9	$E(\xi^4+\xi+1, \xi)$	$(1, \xi^3+\xi^2+\xi+1)$
10	$E(\xi+1, \xi^3+\xi^2+1)$	$(\xi^3+\xi, \xi^4)$
11	$E(\xi^2+\xi+1, \xi^4)$	(ξ^2+1, ξ^4)
12	$E(\xi^4+\xi^2+1, \xi^4)$	$(\xi+1, \xi^4+\xi^3+\xi^2+\xi)$
13	$E(\xi^4+1, \xi^3+\xi^2+1)$	$(\xi^3, \xi^4+\xi^3+\xi^2)$
14	$E(\xi^2+1, \xi^4)$	$(1, \xi^2+1)$
15	$E(\xi^3+\xi^2+\xi, \xi^2)$	(ξ^2+1, ξ)
16	$E(\xi^4+\xi^2+\xi+1, \xi^4+\xi^3+\xi+1)$	$(1, \xi^4+\xi^3+\xi^2+\xi+1)$
17	$E(\xi^3+\xi^2, \xi^3+\xi^2+1)$	$(\xi^4+1, \xi^4+\xi^3+\xi)$
18	$E(\xi^3+\xi^2, \xi^4+\xi^3+\xi+1)$	$(1, \xi^3+\xi^2+1)$
19	$E(\xi^3+\xi^2+\xi, \xi)$	$(\xi^3+\xi^2, \xi^4)$
20	$E(\xi^3+\xi^2, \xi^4)$	$(\xi^4+\xi^2+\xi+1, \xi^3+\xi+1)$
21	$E(\xi^4+1, \xi^2)$	$(\xi^4+\xi^3+\xi^2+\xi, \xi^3+1)$
22	$E(\xi^4+\xi^2+\xi+1, \xi^2)$	$(\xi^4+\xi+1, \xi^3+\xi)$
23	$E(\xi^3+\xi^2, \xi)$	$(\xi^3+\xi^2+\xi, \xi^4+\xi^3+\xi)$
24	$E(\xi^4+\xi^3, \xi^4)$	$(\xi^3+\xi, \xi^4+\xi^3+\xi+1)$
25	$E(\xi^3, \xi^4+\xi^3+\xi+1)$	$(\xi^4+\xi^3+\xi, \xi^3+\xi^2+1)$
26	$E(\xi^3+\xi, \xi^4)$	$(\xi^2+1, \xi^4+\xi^3+1)$
27	$E(\xi^4+\xi^3, \xi)$	$(\xi^3+\xi^2, \xi^2+\xi)$
28	$E(\xi+1, \xi^4)$	(ξ^4+1, ξ^3)
29	$E(\xi^4+\xi^3+\xi^2, \xi)$	$(\xi^4+\xi^3+\xi^2+\xi, \xi^4+\xi^2+\xi)$
30	$E(\xi^4+\xi^3+\xi, \xi^2)$	$(\xi^4+\xi+1, \xi^4+\xi^3+\xi+1)$
31	$E(\xi^4+\xi^3+\xi^2+\xi, \xi^4+\xi^3+\xi+1)$	$(\xi^3+\xi, \xi^2)$

Bibliografía

[1] Gregory V. Bard. *Algebraic Cryptanalysis*. Springer Science and Business Media, 2009.

[2] Hans Delfs and Helmut Knebl. *Introduction to Cryptography*. Information Security and Cryptography. Springer-Verlag Berlin Heidelberg, 2015.

[3] Andreas Enge. *Elliptic curves and their applications to cryptography. An Introduction.* Kluwer Academic Publishers, 1999.

[4] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, fourth edition, 1960.

[5] Nathan Jacobson. *Basic Algebra: I*. W.H. Freeman & Company, second edition, 1985.

[6] Neal Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2 edition, 1994.

[7] National Institute of Standards and Technology (NIST). *Digital Signature Standard (DSS)*, July 2013.

[8] Harald Niederreiter and Arne Winterhof. *Applied Number Theory*. Springer International Publishing, 2015.

[9] Nigel P. Smart. *Cryptography Made Simple*. Information Security and Cryptography. Springer International Publishing, 2016.

[10] Joachim von zur Gathen. *CryptoSchool*. Springer-Verlag Berlin Heidelberg, 2015.