Criptografía con curvas elípticas

Llorenç Huguet Rotger
Josep Rifà Coma
Juan Gabriel Tena Ayuso

PID_00200952

UOC
Universitat Oberta de Catalunya

Índice

Introducción

La teoría de curvas elípticas sobre cuerpos finitos encuentra aplicaciones en diversas disciplinas, como por ejemplo la teoría de números o la criptografía. Resultan sorprendentes sus relaciones con problemas tan diversos como la realización de tests de primalidad, la factorización de números enteros o la demostración del último teorema de Fermat, entre otras.

Veamos unas pinceladas de estas relaciones para centrarnos después en la aplicación de las curvas elípticas a la criptografía. En un principio podemos pensar en una curva elíptica como el conjunto de soluciones de una ecuación de la forma:

$$y^2 = x^3 + ax + b.$$

Relacionadas con la teoría de números podemos destacar dos aplicaciones:

- **Números congruentes**. Un número racional N se dice que es congruente si existe un triángulo con aristas racionales cuya área es N. Durante mucho tiempo el problema ha permanecido sin que se conociese ningún algoritmo capaz de resolverlo, es decir, de comprobar si un número dado N era congruente o no. Actualmente, está demostrado que N es un número congruente si y solo si la curva elíptica $y^2 = x^3 - N^2x = x(x - N)(x + N)$ tiene algún punto racional diferente de $(0,0)$, $(\pm N,0)$ y del punto del infinito de la curva.

- **Teorema de Fermat**. En 1985 Gerhard Frey observó que si $A^n + B^n = C^n$ era un contraejemplo al último teorema de Fermat, entonces la curva elíptica $y^2 = x(x-A^n)(x+B^n)$ tenía por discriminante $-(A^nB^n(A^n+B^n))^2 = -(ABC)^{2n}$. Tal curva contradecía la denominada conjetura de Taniyama. Posteriormente, A. Wiles probó que ninguna curva podía contradecir esta conjetura y, por lo tanto, quedó probado que no existe ningún contraejemplo al último teorema de Fermat.

El problema de los números congruentes

Fue enunciado por primera vez por el matemático persa al-Karaji (hacia el siglo X a. C.). Actualmente, la solución del problema depende de la conjetura de Birch-Swinnerton-Dyer sobre curvas elípticas. El problema es uno de los siete problemas del milenio que el Clay Mathematics Institute dotó, en el año 2000, con un premio de un millón de dólares para quien aportara la solución de cualquiera de ellos.

Discriminante

El discriminante de una curva elíptica $y^2 = x^3 + ax + b$ viene dado por $\Delta = 4a^3 + 27b^2$ y es nulo si y solo si la curva tiene puntos singulares (puntos en los que las dos derivadas parciales se anulan).

En el campo de la criptografía, la aplicación de estas curvas la podemos encontrar en la descomposición de un número en factores, en los sistemas criptográficos y en los tests de primalidad, estos últimos desarrollados por Bosma, Goldwasser-Killian, Atkin y Lenstra entre otros.

H.W. Lenstra ha obtenido un nuevo método de factorización que es, en muchos aspectos, mejor que los conocidos anteriormente. La mejora y eficiencia

de este nuevo método todavía no es significativo en la práctica (el tiempo para factorizar continúa siendo el mismo) pero, aún así, el hecho de haber encontrado un mecanismo diferente hace que los sistemas criptográficos basados en el problema de la factorización no resulten, al fin y al cabo, tan seguros como parecían. El algoritmo de factorización con curvas elípticas de Lenstra es análogo al método clásico denominado $p - 1$ de Pollard.

Los avances en estos métodos así como en las prestaciones de los ordenadores exigen números cada vez mayores a fin de poder garantizar la seguridad de los sistemas criptográficos, lo que representa un grave inconveniente a la hora de implementar los procesos de generación y distribución de las claves secretas. Este problema se soluciona, en parte, usando sistemas de cifrado con curvas elípticas. Estos sistemas ofrecen un nivel de seguridad equivalente al de los métodos tradicionales (RSA, ELGamal,...) pero utilizando un número menor de dígitos. El resultado son claves más pequeñas, característica que resulta especialmente útil para la seguridad en aplicaciones basadas en circuitos integrados y tarjetas inteligentes.

Objetivos

En los materiales didácticos de este módulo el estudiante encontrará los contenidos necesarios para alcanzar los objetivos siguientes:

1. Conocer el concepto de curva en el espacio proyectivo y en el espacio afín.
2. Conocer el concepto de curva elíptica sobre un cuerpo finito y los parámetros que la definen.
3. Conocer el uso de las curvas elípticas en criptografía y los principales problemas que hay que tener en cuenta en su utilización.
4. Conocer los principales algoritmos y protocolos basados en curvas elípticas (Diffie-Helman, Shamir, ElGamal, firma digital).
5. Conocer los estándares y las aplicaciones más corrientes que utilizan las curvas elípticas.

1. Curvas y puntos racionales

1.1. Definiciones previas

Ver también

En el módulo "Cuerpos finitos"de esta asignatura encontraréis de forma detallada algunos de los conceptos que también usaremos en este módulo.

Ya hemos estudiado de forma detallada algunos de los conceptos que también usaremos en este módulo. Vamos a recordar solo algunos:

- La característica de un cuerpo K es el mínimo número p tal que para todo $x \in K$ se cumple que $\underbrace{1+1+\cdots+1}_{p} = 0$, donde 0 es el elemento neutro de la suma y 1 es el elemento neutro del producto en el cuerpo K. Escribiremos $char(K) = p$.

  Si para todo $n \in \mathbb{N}$, $\underbrace{1+1+\cdots+1}_{n} \neq 0$ decimos que $char(K) = 0$.

  Por ejemplo, si $K = \mathbb{F}_q$ donde $q = p^m$, p primo, entonces $char(K) = p$. Para los cuerpos $\mathbb{Q}$ de los números racionales, $\mathbb{R}$ de los números reales y $\mathbb{C}$ de los números complejos se tiene, $char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = 0$.

- Sea K un cuerpo y $x \in K^* = K - \{0\}$. El orden de x es el mínimo número $r > 0$ tal que $x^r = 1$.

- Sea K un cuerpo. La clausura algebraica de K es el cuerpo más pequeño que contiene a K y tal que cualquier polinomio con coeficientes en K tiene todas las raíces en este cuerpo.

1.2. Plano proyectivo

Definición 1.1 (Plano afín y plano proyectivo).

Sea K un cuerpo. El plano afín sobre K, que denominaremos $\mathbb{A}^2$ (o $\mathbb{A}^2(K)$) es el conjunto de puntos de K^2. El plano proyectivo sobre K, $\mathbb{P}^2$ (o $\mathbb{P}^2(K)$), es el conjunto de puntos $(x,y,z) \in K^3 - \{(0,0,0)\}$ con la relación de equivalencia $\sim$ tal que:

$(x,y,z) \sim (x',y',z')$ si, y solo si, $\exists \lambda \in K^* = K - \{0\}$ tal que $x = \lambda x'$, $y = \lambda y'$, $z = \lambda z'$.

Así definimos $\mathbb{P}^2 = K^3 - \{0\}/\sim$. Cada una de las clases de equivalencia se llama punto proyectivo y lo denotaremos por $(x : y : z)$. Para todo $\lambda \in K^*$, diremos que (x,y,z) y $(\lambda x,\lambda y,\lambda z)$ son dos representantes de la misma clase $(x : y : z)$.

Dado un punto proyectivo $(x_0 : x_1 : x_2)$ sabemos que para algún $i = 0,1,2$ $x_i \neq 0$. Definimos el conjunto abierto $U_i = \{(x_0 : x_1 : x_2) | x_i \neq 0\}$

Nota

Análogamente se define el espacio proyectivo n-dimensional $\mathbb{P}^n = K^{n+1} - \{0\}/\sim$, cuyas clases de equivalencia se denominan puntos y se denotan por $(x_0 : x_1 : \cdots : x_n)$.

Sea $(x : y : z) \in U_3$. Existe un único representante de este punto de la forma $(\frac{x}{z},\frac{y}{z},1)$. De este modo, dado que $z \neq 0$, podemos identificar puntos proyectivos con puntos afines:

Algoritmo 1.2.

$\mathbb{P}^2 \cap U_3 \longrightarrow K^2$
$(x : y : z) \longrightarrow (\frac{x}{z},\frac{y}{z})$

Los puntos proyectivos con $z = 0$ forman lo que se denomina recta del infinito.

Definición 1.3 (Polinomio homogéneo).

Un polinomio $F(z_0,\ldots,z_n) \in K[z_0,\ldots,z_n]$ diremos que es un polinomio homogéneo si todos sus monomios tienen el mismo grado. Denotaremos por $F[z_0,\ldots,z_n]$ un tal polinomio.

Observación

El paso del plano proyectivo al plano afín se podría hacer con cualquiera de las tres coordenadas. En general, lo haremos con la z o con la x_0 si escribimos los puntos con la notación $(x_0 : x_1 : \cdots : x_n)$.

Ejemplo 1.1.

- $z_0 z_3 - {z_2}^2$ es un polinomio homogéneo de grado 2.
- $z_1 - z_3$ es un polinomio homogéneo de grado 1.
- ${z_2}^3$ es un polinomio homogéneo de grado 3.

Dado $F[x,y,z]$, un polinomio homogéneo de grado r, no tiene sentido *dar valores* a F en el plano proyectivo. Por ejemplo, si $F[x,y,z] = x^3 + 3y^2z + z^3$, entonces $(1 : 1 : 1) = (2 : 2 : 2)$, pero $F[1,1,1] = 5 \neq 40 = F[2,2,2]$.

Ahora bien, sí que tiene sentido decir que $F[x,y,z]=0$ puesto que si $\lambda \neq 0$, $F[\lambda x,\lambda y,\lambda z] = \lambda^r F[x,y,z]$; en consecuencia, si F es un polinomio homogéneo de grado r, entonces $F[\lambda x,\lambda y,\lambda z] = 0$ si y solo si $F[x,y,z] = 0$.

Relación afín-proyectivo

Consideremos como antes el conjunto $U_i := \{(x_0 : \cdots : x_n) \in \mathbb{P}^n | x_i \neq 0\} \subset \mathbb{P}^n$.

Relación de coordenadas entre los puntos considerados en el espacio afín y en el espacio proyectivo.

Algoritmo 1.4.

$\mathbb{A}^n \longrightarrow U_i \subset \mathbb{P}^n$
$(a_1, \ldots, a_n) \longrightarrow (a_1;\ \ldots;\ a_{i-1};\ 1;\ a_{i+1};\ \ldots;\ a_n)$
$(\frac{z_0}{z_i}, \ldots, \frac{z_{i-1}}{z_i}, \frac{z_{i+1}}{z_i}, \ldots, \frac{z_n}{z_i}) \longleftarrow (z_0;\ \ldots;\ z_n)$

Relación de polinomios. Dado $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ en el espacio afín, se tiene $F[x_0, \ldots, x_n] \in K[x_0, \ldots, x_n]$, su homogeneizado en el espacio proyectivo, el cual se obtiene a partir de f multiplicando por potencias de x_0 cada monomio hasta conseguir un polinomio homogéneo de grado $gr(f)$. Recíprocamente, para pasar de un polinomio del espacio proyectivo a uno en el espacio afín, daremos valor 1 a la coordenada x_0 (o a la coordenada que previamente hayamos fijado).

Ejemplo 1.2.

- Coordenadas:

  $\mathbb{A}^2 \longrightarrow U_2 \subset \mathbb{P}^2$
  $(1,2) \longrightarrow (x : y : z) = (1 : 2 : 1)$
  $(2, \frac{1}{2}) \longleftarrow (x : y : z) = (4 : 1 : 2)$

- Polinomios:

  $K[x,y] \longrightarrow K[x,y,z]$
  $x^2 + x^3 + xy \longrightarrow x^2z + x^3 + xyz$
  $x + x^2y + 1 \longleftarrow xz^2 + x^2y + z^3$

1.3. Curvas afines y proyectivas

Definición 1.5 (Curva afín y curva proyectiva).

Sean $f(x,y) \in K[x,y]$ y $F[x,y,z] \in K[x,y,z]$ no constantes. Entonces el conjunto $C_f(K) = \{(x,y) | f(x,y) = 0\}$ se denomina curva afín y $C_F(K) = \{(x : y : z) | F[x,y,z] = 0\}$ curva proyectiva.

Recordar

Un cuerpo K' es la clausura algebraica de un cuerpo K si $K \subseteq K'$ y K' mínimo, con la propiedad de que cualquier polinomio de $K'[x]$ se descompone en factores de grado uno.

Definición 1.6 (Componentes irreducibles de una curva).

Sea $f \in K[x,y]$. Podemos descomponer f en producto de factores irreducibles $f = f_1^{e_1} \dots f_s^{e_s}$. (Del mismo modo para $F \in K[x,y,z]$).

Con esta descomposición, podemos escribir la curva como unión de sus componentes irreducibles: $C_f(K) = C_{f_1}(K) \cup \dots \cup C_{f_s}(K)$.

Definición 1.7 (Punto singular).

Sea $C = C_f(K) \subseteq \mathbb{A}^2$ una curva afín y $p = (a,b) \in C$. Decimos que p es un **punto múltiple** o **punto singular** de C si satisface las ecuaciones:

$$\begin{cases} \dfrac{\partial f}{\partial x}(p) = 0 \\ \dfrac{\partial f}{\partial y}(p) = 0 \end{cases}$$

Definición 1.8 (Curva no singular).

Una curva es no singular si todos sus puntos son simples (o sea, no singulares).

Recordar

La notación $\dfrac{\partial f}{\partial x}(p)$ significa calcular la derivada parcial de $f(x)$ respecto a la variable x y dar valores en el punto p.

Definición 1.9 (Recta tangente).

Sea $p = (a,b) \in C = C_f(K)$ un punto simple. Definimos la **recta tangente** a C en el punto p como la recta dada por la ecuación:

$$\frac{\partial f}{\partial x}(p)(x-a) + \frac{\partial f}{\partial y}(p)(y-b) = 0$$

Sea $C = C_f(K), p = (a,b)$. Podemos escribir f como suma de componentes homogéneas:

$$f(x-a,y-b) = f_0(x-a,y-b) + \dots + f_m(x-a,y-b),$$

donde $gr(f_i(x-a,y-b)) = i$.

Definición 1.10 (Multiplicidad en un punto).

Definimos la multiplicidad de C, en el punto $p = (a,b)$, como el mínimo k tal que $f_k(x-a,y-b) \neq 0$ (como polinomio) y la denotaremos por $m_p(C)$.

Observación

- $m_p(C) = 0 \iff p \notin C$.
- $m_p(C) = 1 \iff p$ es un punto simple de C.
- Si $m_p(C) = 2$, decimos que p es un punto doble.

Definición 1.11 (Nodos y cúspides).

Si $m_p(C) = 2$, entonces $f_2(x-a,y-b)$ se puede descomponer en producto de 2 factores: $f_2(x-a,y-b) = \alpha\beta$.

- Si $\alpha \neq \beta$, diremos que p es un nodo.
- Si $\alpha = \beta$, diremos que p es una cúspide.

Donde la anterior igualdad o desigualdad de α y β se entiende salvo un factor constante.

Observación

Nótese que los factores α y β en la Definición1.11 no tienen por qué tener los coeficientes en el cuerpo K, sino que pueden tenerlos en alguna extensión cuadrática de K.
En el caso de un nodo distinguiremos un *nodo racional* (si α y β tienen coeficientes en K), de un *nodo irracional* (en caso contrario).

Ejemplo 1.3.

Supongamos que $char(K) \neq 2,3$. Consideramos la curva $C: y^2 = x^3 + ax^2$. De otro modo, sea $f(x,y) = x^3 + ax^2 - y^2$, donde a es un valor constante $a \in K$.

La curva C, ¿tiene puntos singulares? Y, en caso afirmativo, ¿qué multiplicidad tienen?

- Para responder la primera cuestión, tal y como hemos dicho en la definición 1.7, calcularemos las derivadas parciales teniendo en cuenta que, además, el valor de la función $f(x,y)$ debe ser cero en todos los puntos de la curva:

$$\begin{cases} \dfrac{\partial f}{\partial x} = 3x^2 + 2ax = 0 \\ \dfrac{\partial f}{\partial y} = -2y = 0 \\ f = x^3 + ax^2 - y^2 = 0 \end{cases}$$

  Resolviendo este sistema encontramos $y = 0$, $x(3x + 2a) = 0$, $x^3 + ax^2 - y^2 = 0$. Finalmente, $y = 0, x = 0$. Por lo tanto, (0,0) es un punto singular.

- Para estudiar la multiplicidad del punto singular (0,0) utilizaremos la definición1.10, pero antes descompongamos $f(x,y)$ en suma de funciones homogéneas $f_0(x-0,y-0)$, $f_1(x-0,y-0)$, $f_2(x-0,y-0)$, $f_3(x-0,y-0)$, de grados 0,1,2,3, respectivamente.

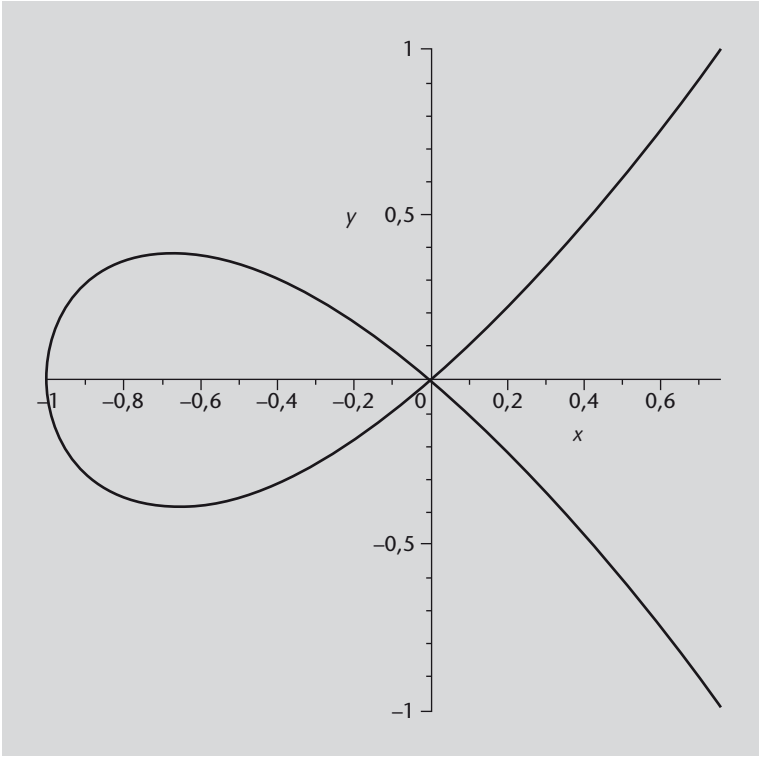
  Vemos que $f(x-0,y-0) = f(x,y) = 0 + 0 + (ax^2 - y^2) + x^3$.

  Por lo tanto, $f_0(x,y) = f_1(x,y) = 0$, $f_2(x,y) = ax^2 - y^2 = (\sqrt{a}x + y)(\sqrt{a}x - y)$, $f_3(x,y) = x^3$.

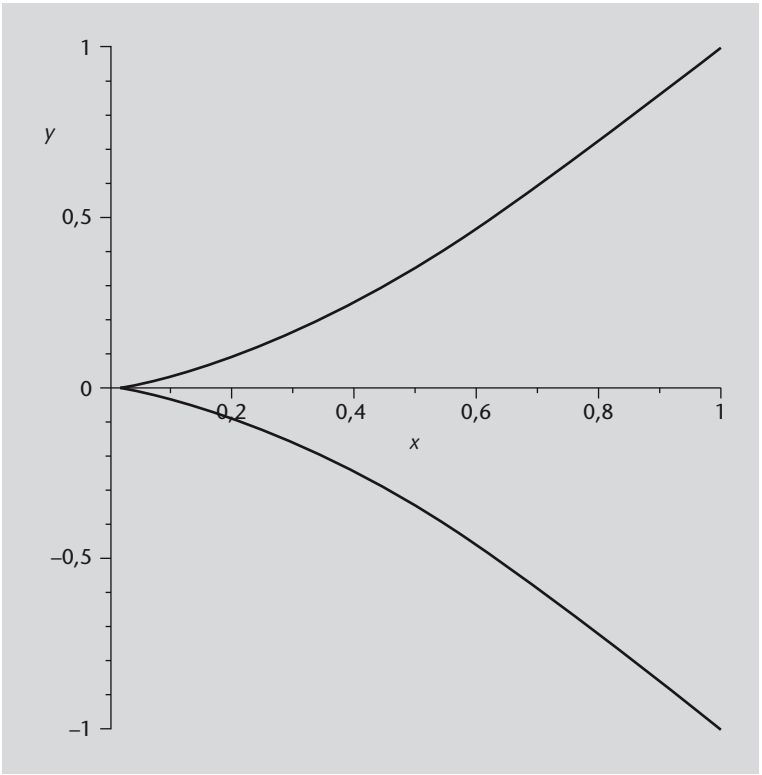
  Así, de acuerdo con la definición 1.10, vemos que $m_p(C) = 2$ y, por lo tanto, $p = (0,0)$ es un punto doble. Ahora, de acuerdo con la Definición 1.11 vemos que para $a = 0$ el punto $p = (0,0)$ es una cúspide y para todos los valores $a \neq 0$, el punto $p = (0,0)$ es un nodo. Dependiendo de si $\sqrt{a} \in K$ o no el nodo será racional o irracional.

  Las figuras siguientes corresponden a la curva $y^2 = x^3 + ax^2$ para $a = 1$ y $a = 0$, respectivamente.

Nodo racional en el punto $(0,0)$ de la curva $y^2 = x^3 + x^2$



Cúspide en el punto $(0,0)$ de la curva $y^2 = x^3$



Una pregunta que quizás nos hayamos hecho a estas alturas es: ¿por qué nos interesará mirar las curvas en el plano proyectivo?

Supongamos la misma curva que en el ejemplo anterior para el caso $a = 2$. La podemos ver como una curva proyectiva dada por un polinomio homogéneo,

$F[x,y,z] = x^3 + 2x^2z - y^2z = 0$. Podemos pasar la curva proyectiva al plano afín dando el valor $z = 1$; así, obtenemos la curva $f(x,y) = x^3 + 2x^2 - y^2 = 0$, que está dada por la misma ecuación que ya habíamos visto en el ejemplo anterior y de la que ya sabemos que el punto $(x = 0, y = 0)$ es un punto singular. Para evitar este punto singular podríamos pasar al afín usando otra coordenada; por ejemplo, $y = 1$, obteniendo una "nueva curva": $g(x,z) = x^3 + 2x^2z - z = 0$, en la que el punto $(x = 0, z = 0)$ pertenece a la curva y no es singular.

Estas dos curvas afines (las dadas por f y g) son curvas asociadas a la misma curva proyectiva. Así, aunque una de las curvas afines contenga un punto singular podríamos encontrar otra curva afín asociada a la misma curva proyectiva que no tenga ninguno.

Observación

El uso de coordenadas proyectivas también permite realizar cálculos en curvas elípticas sobre cuerpos finitos sin necesidad de hacer operaciones de división en el cuerpo. Esto es importante, puesto que las operaciones de dividir son computacionalmente costosas.

Teorema 1.12 (Teorema de Bezout).

Sean $C = \{(x : y : z) \in \mathbb{P}^2 | F[x,y,z] = 0\}$ y $D = \{(x : y : z) \in \mathbb{P}^2 | G[x,y,z] = 0\}$ dos curvas proyectivas de grados m y n respectivamente ($m = gr(F)$, $n = gr(G)$). Si C y D no tienen componentes irreducibles en común, entonces C y D tienen $\boldsymbol{mn}$ puntos en común contando sus multiplicidades.

Ejemplo 1.4.

- Dos rectas diferentes (curvas proyectivas de grado 1) se cortan siempre en un punto. En efecto, si las consideramos en el plano afín, sabemos que dos rectas diferentes o bien se cortan en un punto o bien son paralelas y, en este caso, se cortan en un punto de la recta del infinito del plano proyectivo.

- Dos cónicas diferentes (curvas proyectivas de grado 2) se cortan exactamente en 4 puntos.

Corolario 1.13.

Una cónica definida por un polinomio irreducible F de grado 2, no tiene puntos singulares.

Demostración: Una cónica es una curva proyectiva de grado 2. Suponemos que esta cónica tiene un punto singular. Tomemos otro punto de la cónica y consideramos la recta que pasa por estos dos puntos; esta recta es una curva proyectiva de grado 1.

Nuestra cónica es una curva proyectiva de grado 2; por lo tanto, por el teorema de Bezout, la recta y la cónica tienen 2 puntos en común, pero como el punto singular tiene multiplicidad más grande o igual que 2, el número de puntos en

común será de 3 o más. Ello contradice el teorema de Bezout, a menos que la recta y la cónica tengan una componente irreducible en común, componente que debería ser la propia recta. Pero dado que F es irreducible, la cónica solo tiene una componente irreducible ∎

1.4. Puntos racionales

El cuerpo de los números racionales lo representaremos por $\mathbb{Q}$.

Definición 1.14 (Sucesión fundamental).

Una sucesión de números a_n, con $a_i \in \mathbb{Q}$ decimos que es una sucesión fundamental si $\forall \epsilon > 0\ \exists n_\epsilon \in \mathbb{N}$ tal que $|a_n - a_m| < \epsilon$, $\forall m,n > n_\epsilon$, donde la norma es la norma euclídea.

Definición 1.15 (Cuerpo p-ádico).

Sea p primo. Todo número $a \in \mathbb{Q}$ se puede escribir de la forma $a = p^r \frac{m}{n}$, donde $mcd(m,p) = 1$ y $mcd(n,p) = 1$. Entonces, definimos la **norma p-ádica** de a como: $|a|_p = \frac{1}{p^r}$.

Definimos el cuerpo p-ádico $\mathbb{Q}_p$ como el conjunto de todas las sucesiones fundamentales con esta norma, módulo una cierta relación de equivalencia.

Observación

El cuerpo $\mathbb{R}$ de los números reales se puede definir como el conjunto de todas las sucesiones fundamentales, módulo una cierta relación de equivalencia.

Definición 1.16 (Puntos racionales de una curva).

Sea K un cuerpo, y $C = C_f(K)$ una curva. Decimos que $p = (p_1,p_2)$ es un punto racional de la curva si $f(p) = 0$ y $p \in K^2$.

Teorema 1.17 (Teorema de Legendre).

Una cónica (con coeficientes en $\mathbb{Q}$) tiene un punto racional si y solo si tiene un punto racional sobre $\mathbb{R}$ y sobre los cuerpos $\mathbb{Q}_p$ para todo primo p.

Observación

El Teorema1.17 es falso para curvas de grado mayor que 2. Para curvas de grado 2, es cierto para cualquier número de variables, es decir, curvas planas o no, definidas por una forma cuadrática (Hasse-Minkowski).

1.4.1. Puntos racionales de una curva de grado 1

Una curva de grado 1 es una recta. La ecuación de una tal recta se puede escribir como $Ax + By + C = 0$.

Consideremos una parametrización de la recta o sea, expresaremos los puntos de la recta en función de un parámetro. Una manera de hacerlo sería:

Algoritmo 1.18.

$t \longrightarrow (t, \frac{C-At}{B})$

Ahora, dando a t valores en el cuerpo obtenemos puntos racionales de nuestra recta. En particular si el cuerpo base es infinito, como $\mathbb{Q}$, $\mathbb{R}$,..., las rectas tienen infinitos puntos racionales.

1.4.2. Puntos racionales de una curva de grado 2

Una curva de grado 2 es una cónica. En el caso $K = \mathbb{Q},\mathbb{R},...,$ (cuerpos ordenados) la ecuación de una cónica, tras cambios apropiados de coordenadas, se puede escribir de una de las formas siguientes:

1) $x^2 + y^2 = c < 0 \Longrightarrow \emptyset$.

2) $x^2 + y^2 = 0 \Longrightarrow$ un punto.

3) $x^2 = 0 \Longrightarrow$ recta doble.

4) $xy = 0 \Longrightarrow$ dos rectas.

5) $y = x^2 \Longrightarrow$ parábola.

6) $xy = 1 \Longrightarrow$ hipérbole.

7) $x^2 + y^2 = c > 0 \Longrightarrow$ elipse.

Los casos 2, 3 y 4 son curvas degeneradas o no irreducibles y, por lo tanto, no las trataremos.

Los casos 5, 6, 7 son proyectivamente equivalentes; es decir, en el plano proyectivo, podemos pasar de unos a otros vía un cambio de variables.

Ejemplo 1.5. Cálculo de puntos racionales en una cónica

Consideremos, como ejemplo, la cónica afín $x^2 + y^2 = 1$ y calculemos sus puntos racionales. En primer lugar, se ve fácilmente que el punto $p = (0,1)$ es un punto racional de la curva. Ahora, vamos a ver si podemos calcular los restantes.

Los puntos de la cónica los podemos pensar como intersecciones de la cónica con rectas que pasan por este punto fijado $p = (0,1)$.

Consideramos las rectas $r : Ax + By + C = 0$, del haz de rectas que pasan por el punto p. Como $p = (0,1)$ pertenece a la recta, se tiene que $B + C = 0$, o sea $C = -B$.

Podemos, por tanto, escribir la ecuación de la recta r como $Ax + By - B = 0$ o, también, $\frac{A}{B}x + y - 1 = 0$.

Hagamos $A' = \dfrac{A}{B}$ y, entonces la recta será, $A'x + y - 1 = 0$.

Así, el haz de rectas que pasan por $p = (0,1)$ es $\{A'x + y - 1 = 0\}_{A'}$ (o sea, variando los valores del parámetro A', encontramos todas las rectas del haz).

Hagamos ahora la intersección de las rectas del haz con la cónica. O sea, resolvamos el sistema de ecuaciones:

$$\begin{cases} A'x + y - 1 = 0 \\ x^2 + y^2 = 1 \end{cases}$$

Haciendo operaciones, $y = 1 - A'x$

$x^2+(1-A'x)^2 = 1 \rightarrow\ x^2+1-2A'x+A'^2x^2 = 1\ \rightarrow x^2(1+A'^2)-2A'x = 0\ \rightarrow x(x(1+A'^2)-2A') = 0.$
Posibilidades:

$$\begin{cases} x = 0 \rightarrow \text{ punto } (0,1) \\ x(1 + A'^2) - 2A' = 0,\ x = \dfrac{2A'}{1 + A'^2} \rightarrow \text{ punto } \left(\dfrac{2A'}{1 + A'^2}, \dfrac{1 - A'^2}{1 + A'^2}\right) \end{cases}$$

Así, escogiendo como punto fijo $p = (0,1)$, parametrizamos la cónica inicial de la siguiente manera:

Algoritmo 1.19.

$t \longrightarrow \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$

Para cada t del cuerpo base, el punto de la curva $\left(\dfrac{2t}{1 + t^2}, \dfrac{1 - t^2}{1 + t^2}\right)$ también lo es; en particular si el cuerpo es infinito, la curva dada por $f(x,y) = x^2 + y^2 - 1$ tiene infinitos puntos racionales.

1.4.3. Puntos racionales de una curva de grado 3

Una curva de grado 3 es una cúbica.

Proposición 1.20.

Si $F[x,y,z] = 0$ es una curva proyectiva irreducible de grado 3 con un punto singular, entonces este es único. Además, este único punto singular tiene multiplicidad 2.

Observación

Hemos demostrado que, en el caso de un cuerpo infinito, si una cónica tiene un punto racional, posee infinitos. Con esto no podemos decir que toda cónica tiene infinitos puntos racionales porque existen curvas sin ningún punto racional; por ejemplo, $x^2 + y^2 = -1$ sobre $\mathbb{Q}$.

Demostración: Suponemos que tenemos una cúbica con dos puntos singulares. Consideramos la recta que pasa por estos dos puntos. La curva y la recta tienen, como mínimo, 4 puntos en común contando multiplicidades; pero, teniendo en cuenta el teorema de Bezout, solo podrían tener 3, a menos que tuviesen una componente irreducible en común, lo que como en el corolario 1.13 no puede ocurrir. Por tanto, la cúbica solo puede tener un punto singular a lo sumo.

Supongamos ahora que este punto singular tiene multiplicidad mayor que dos. Entonces una recta que pase por este punto y otro punto cualquiera de la cúbica tendría, al menos, 4 puntos en común con la curva y esto, por el teorema de Bezout, no puede ocurrir. ∎

Proposición 1.21.

Un punto singular es siempre racional.

Resumiendo, una curva de grado 3 o no tiene puntos singulares o tiene exactamente un punto singular que es un nodo o una cúspide y, además, es racional.

Si tenemos una curva de grado 3 no singular, sabemos que una recta que pasa por dos de sus puntos corta a la curva en un tercer punto. Además, si dos de estos punto son racionales, entonces el tercero también lo es. (Diofantes, siglo III a. C.).

Teorema 1.22 (Teorema de la base finita de Mordell. (1923)).

Si C es una cúbica no singular sobre $\mathbb{Q}$, existe un conjunto finito de puntos racionales sobre C tal que todos los otros puntos racionales de la curva se pueden encontrar haciendo construcciones de tangentes y secantes a partir de estos.

1.4.4. Puntos racionales de una curva de grado 4

Teorema 1.23 (Teorema de Faltings (1983)).

Las curvas irreducibles de grado ≥ 4 tienen un número finito de puntos racionales sobre el cuerpo $\mathbb{Q}$.

Resumimos lo que hemos dicho hasta ahora sobre los puntos racionales sobre $\mathbb{Q}$:

- Curvas de grado 1: hay infinitos puntos racionales.

- Curvas de grado 2: si hay un punto racional, hay infinitos. Hilbert y Hurwitz (1890) lo demuestran para las curvas de género cero (las de grado 1 y 2 lo son).

- Curvas de grado 3: hay un conjunto infinito de puntos racionales, conjunto que es finitamente generado. Mordell, 1923.

- Curvas de grado 4: hay un número finito de puntos racionales. Conjeturado por Mordell y demostrado por Faltings, 1983.

2. Geometría de las curvas elípticas

Comencemos dando una definición más formalizada de curva elíptica.

Definición 2.1 (Curva elíptica).

Una **curva elíptica** es una curva plana no singular de grado 3 junto con un punto racional prefijado, que denominaremos punto base.

2.1. Ecuación de Weierstrass

Cualquier curva elíptica puede ser escrita en $\mathbb{P}^2$ como una ecuación cúbica de la siguiente forma:

$$Ax^3 + Bx^2y + Cx^2z + Dxyz + Ey^2z + Fy^2x + Gy^3 + Hz^3 + Iz^2x + Jz^2y = 0$$

Tomando un sistema de referencia adecuado, tales curvas se pueden expresar en la **forma de Weierstrass**:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \quad (1)$$

con $a_1, \ldots, a_6 \in K$

O en el plano afín, curvas de grado 3 de la forma:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2)$$

Si $char(K) \neq 2$, entonces

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 = y^2 + a_1xy + a_3y + \frac{1}{4}a_1x^2 + \frac{1}{4}a_3^2 + \frac{1}{2}a_1a_3x$$

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 - (\frac{1}{4}a_1x^2 + \frac{1}{4}a_3^2 + \frac{1}{2}a_1a_3x) = x^3 + a_2x^2 + a_4x + a_6$$

Podemos pues simplificar la ecuación (1) haciendo el cambio

$$y := y + \frac{1}{2}a_1x + \frac{1}{2}a_3$$

y nos queda:

$$y^2 = x^3 + (a_2 + \frac{1}{4}a_1)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + (a_6 + \frac{1}{4}a_3^2)$$

Por tanto, si $char(K) \neq 2$, la ecuación de Weierstrass se puede escribir:

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \tag{3}$$

Suponemos ahora que además la característica del cuerpo es diferente de 3 ,

$$(x + \frac{b_2}{3 \cdot 4})^3 = x^3 + \frac{b_2}{4}x^2 + \frac{b_2^2}{4^2 \cdot 3}x + \frac{b_2^3}{(3 \cdot 4)^3}$$

$$y^2 = (x + \frac{b_2}{3 \cdot 4})^3 - 3x\frac{b_2^2}{(3 \cdot 4)^2} - (\frac{b_2}{3 \cdot 4})^3 + 2b_4x + b_6$$

Hagamos ahora el cambio,

$$x := x + \frac{b_2}{3 \cdot 4}$$

y nos queda la ecuación:

$$y^2 = x^3 + 27c_4x - 54c_6$$

Hemos simplificado más todavía la ecuación puesto que hemos eliminado el coeficiente de x^2.

Finalmente si $char(K) \neq 2,3$, la ecuación (1) se puede escribir de manera más simple cómo:

$$y^2 = x^3 + Ax + B \tag{4}$$

De manera similar, cuando tenemos un cuerpo de característica 2 o 3, también se puede simplificar la ecuación (1).

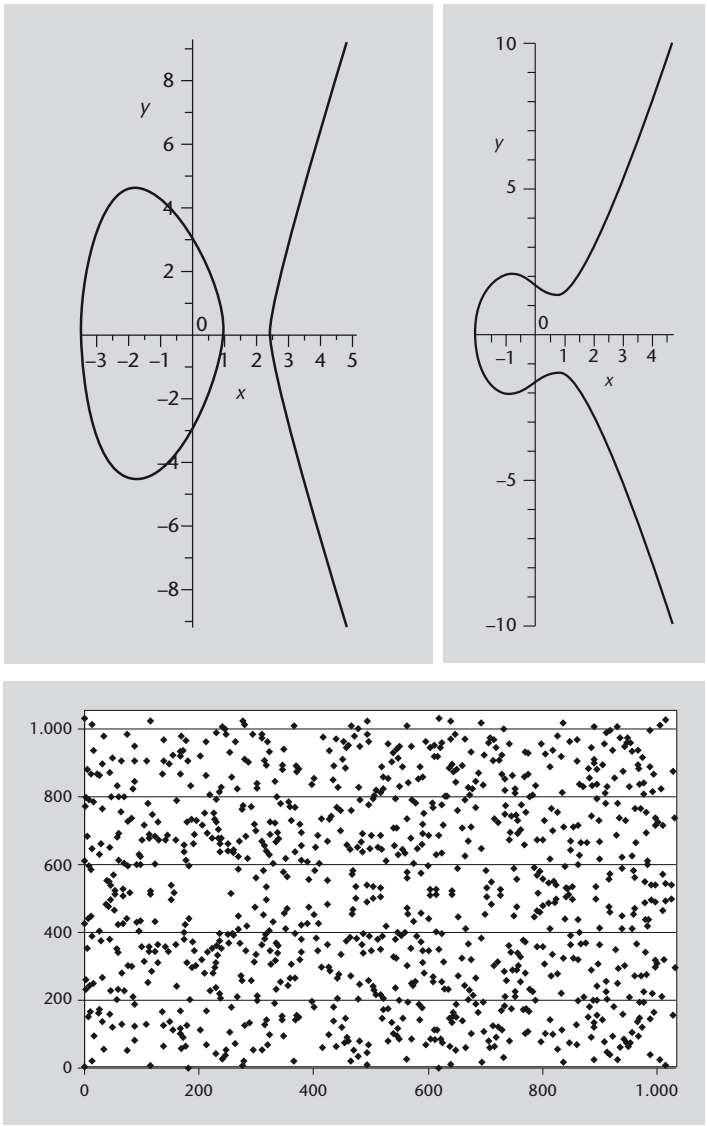
Si $char(K) = 2$, entonces la ecuación de la curva elíptica tiene una de las dos formas siguientes:

$$\begin{aligned} &\text{Si } a_1 \neq 0 \text{ en la ecuación (1) : } y^2 + xy = x^3 + b_2x^2 + b_6, \text{ donde } b_6 \neq 0 \\ &\text{Si } a_1 = 0 \text{ en la ecuación (1) : } y^2 + b_3y = x^3 + b_4x + b_6, \text{ donde } b_3 \neq 0 \end{aligned} \tag{5}$$

Si $char(K) = 3$, entonces tenemos:

$$y^2 = x^3 + a_2x^2 + a_6 \qquad (6)$$

Las dos primeras curvas $y^2 = x^3 - 10x + 9$ y $y^2 = x^3 - 2x + 3$ definidas sobre los números reales. La última, $y^2 = x^3 + 10x + 9$ sobre $\mathbb{F}_{1031}$



Proposición 2.2.

Sea K un cuerpo con $char(K) \neq 2,3$, sea C una curva sobre K, $C : y^2 = x^3+Ax+B$. Sea $\Delta = 4A^3+27B^2$ el discriminante de la curva. Entonces:

- $\Delta \neq 0 \Leftrightarrow C$ no tiene puntos singulares.
- $\Delta = 0$ y $A = 0 \Longrightarrow C$ tiene una cúspide.
- $\Delta = 0$ y $A \neq 0 \Longrightarrow C$ tiene un nodo.

Demostración: Sea $C : y^2 = x^3 + Ax + B$, $f(x,y) = x^3 + Ax + B - y^2$. C tiene puntos singulares si, y solo si, $\frac{\partial f}{\partial x}(p) = 0$, $\frac{\partial f}{\partial y}(p) = 0$.

$$\begin{cases} \frac{\partial f}{\partial x} = 3x^2 + A \\ \\ \frac{\partial f}{\partial y} = -2y \end{cases}$$

Puntos singulares:

$$\begin{cases} \frac{\partial f}{\partial x} = 0 \iff x = \pm\sqrt{\frac{-A}{3}}, \\ \\ \frac{\partial f}{\partial y} = 0 \iff y = 0 \end{cases}$$

$$x^3 + Ax + B - y^2 = 0 \to \frac{-A}{3}x + Ax + B = 0 \to x = \frac{3B}{2A}$$

entonces

$$x^2 = \frac{9B^2}{4A^2} = \frac{-A}{3} \to 4A^3 + 27B^2 = 0$$

1) C no tiene puntos singulares si, y solo si, $4A^3 + 27B^2 \neq 0$.

2) Sea $4A^3 + 27B^2 = 0$ y $A = 0$, entonces $B = 0$ y $f(x,y) = x^3 - y^2$. El punto (0,0) es un punto singular, además, según la definición1.11, sabemos que es una cúspide.

3) Sea $4A^3 + 27B^2 = 0$ y $A \neq 0$. El punto $\left(\frac{3B}{2A},0\right)$ es un punto singular. $f(x,y) = x^3 + Ax + B - y^2$ se puede escribir como $f(x,y) = \left(x - \frac{3B}{2A}\right)^3 + \frac{9B}{2A}\left(x - \frac{3B}{2A}\right)^2 - (y-0)^2$, entonces $f_2\left(x - \frac{3B}{2A}, y - 0\right) = \frac{9B}{2A}x^2 - y^2 = \left(\sqrt{\frac{9B}{2A}}x - y\right)\left(\sqrt{\frac{9B}{2A}}x + y\right)$. Así, el punto $\left(\frac{3B}{2A},0\right)$ es un punto doble y, según la definición1.11, sabemos que es un nodo.

∎

2.2. La ley de grupo de una curva elíptica

Sea $C \subset \mathbb{P}^2$ una curva elíptica dada por la ecuación de Weierstrass. Denotemos O al punto base de la curva. Sea $L \subset \mathbb{P}^2$ una recta. Como la ecuación de la curva tiene grado 3, L y C se intersecan en, exactamente, 3 puntos, digamos $L \cap C = \{P,Q,R\}$. Observemos, sin embargo, que si L es tangente a C, entonces P,Q,R no serán tres puntos diferentes; habrá uno doble (el punto de tangencia). El hecho de que $L \cap C$, contando multiplicidades, dé tres puntos se deduce del teorema de Bezout (teorema 1.12).

2.2.1. Ley de grupo en C

Sean $P,Q \in C$ y L la recta que pasa por estos dos puntos (la tangente en el caso $P = Q$), y R el tercer punto de intersección de L y C. Sea L' la recta que une R y O. Entonces $L' \cap C = \{R,O,P+Q\}$; es decir $P+Q$ es el tercer punto de intersección de la curva y la recta que pasa por R y O.

Definimos así una operación sobre los puntos de la curva elíptica de forma que $P + Q$ sea el punto calculado a partir de P y Q tal y como acabamos de describir en el párrafo anterior. La operación que hemos definido dota a C de estructura de grupo abeliano.

Proposición 2.3.

La ley de grupo en C tiene las siguientes propiedades:

- Si $L \cap C = \{P,Q,R\}$ (puntos no necesariamente diferentes), entonces $(P + Q) + R = O$.
- $P + O = P$, $\forall P \in C$.
- $P + Q = Q + P$, $\forall P,Q \in C$.
- $\forall P \in C \ \exists(-P) \in C$ tal que $P + (-P) = O$.
- $(P + Q) + R = P + (Q + R)$, $\forall P,Q,R \in C$

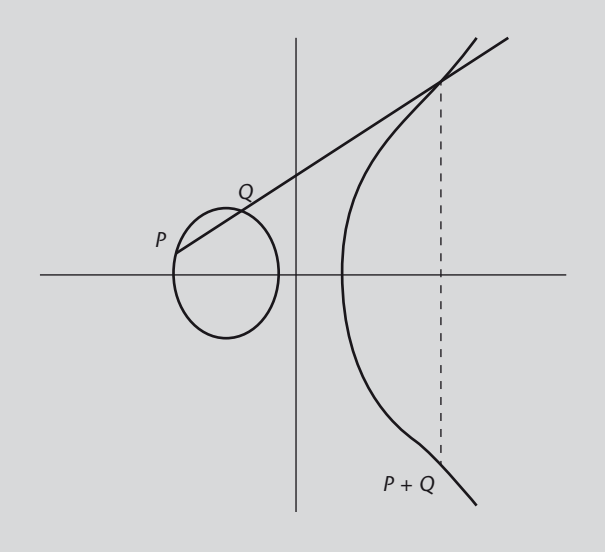
Para facilitar los cálculos, tomaremos como punto base el punto del infinito de la curva, $O = (0 : 1 : 0)$. Dados dos puntos de la curva, P y Q calculemos R (en la figura siguiente, R es el tercer punto donde la recta que pasa por P y Q corta a la curva). Si ahora queremos calcular la intersección de la recta que pasa por R y O con la curva elíptica, basta encontrar el simétrico de R respecto al eje de las x.

Notación

Para $n \in \mathbb{Z}$, $P \in C$ escribiremos:

- $nP = P + \cdots + P$ n veces, si $n > 0$.
- $nP = (-P) + \cdots + (-P)$ $|n|$ veces, si $n < 0$
- $0P = O$

Suma de dos puntos



Finalmente, detallamos un algoritmo, análogo al algoritmo de multiplicar y elevar al cuadrado, para calcular nP con el mínimo número posible de operaciones.

Antes que nada calcularemos la expansión binaria de n: $n \leftrightarrow b_1 b_2 \dots b_r$, $b_i \in \{0,1\}$ (b_r es el bit menos significativo, o sea, las unidades).

Algoritmo 2.4.

```
function Suma(n)
    begin
        for j ← 1 to n
            if b_j = 1 then parcial ← parcial + P endif
            if j < r then parcial ← 2·parcial endif
        endfor
        return(parcial)
end
```

Ejemplo 2.1.

Calcular $19P$.

El número 19 escrito en binario es 10011. Entonces, de acuerdo con el algoritmo anterior $19P = 2\Big(2\big(2(2(0+P))\big)+P\Big)+P$.

Ejemplo 2.2.

Sea $K = \mathbb{F}_{23}$, $C : y^2 = x^3 + x + 1$, $P_1 = (3,10)$, $P_2 = (9,7)$.

- Calcular $P_1 + P_2$.
- Calcular $10 \cdot P_1$

Empezaremos calculando la recta que pasa por P_1 y P_2, que denominaremos $L : y = \alpha x + \beta$

$$\alpha = \frac{7-10}{9-3} = -\frac{1}{2} = -12 = 11$$

$$10 = 11 \cdot 3 + \beta \Longrightarrow \beta = 10 - 10 = 0$$

Por lo tanto $L : y = 11x$.

Ahora calcularemos la intersección de esta recta con la curva, o sea $L \cap C$:

$$\begin{cases} y = 11x \\ y^2 = x^3 + x + 1 \end{cases}$$

Sustituyendo la y en la ecuación de la curva obtenemos

$$6x^2 = x^3 + x + 1$$

luego

$$0 = x^3 + 17x^2 + x + 1 = (x-3)(x-9)(x-x_3)$$

puesto que sabemos que pasa por los puntos P_1 y P_2.

Igualamos los coeficientes de grado 2:

$$17 = -3 - 9 - x_3 \Longrightarrow x_3 = -12 - 17 = 17$$

$$y_3 = 11 \cdot 17 = 3$$

El tercer punto de intersección es pues (17,3).

Finalmente, calcularemos el punto simétrico, sobre $\mathbb{F}_{23}$, respecto al eje de abscisas: $P_1 + P_2 = (17,20)$

Para calcular $10P_1$ empezaremos escribiendo en binario $10 \leftrightarrow 1010$. Aplicando el algoritmo análogo al de multiplicar y elevar, tenemos: $10P_1 = 2(2(2P_1) + P_1)$

Cálculo de la tangente que pasa por P_1:

La ecuación de la tangente por un punto P es:

$$\frac{\partial f}{\partial x}(P)(x - x_1) + \frac{\partial f}{\partial y}(P)(y - y_1) = 0$$

Tenemos $f(x,y) = y^2 - x^3 - x - 1$

$$\begin{cases} \frac{\partial f}{\partial x}(P_1) = -4 - 1 = 18 \\ \frac{\partial f}{\partial y}(P_1) = 20 \end{cases}$$

Por lo tanto $18(x-3) + 20(y-10) = 18x + 20y + 22 = 0 \rightarrow 10y = 14x + 12 \rightarrow 5y = 7x + 6 \rightarrow y = 6x + 15$, $(5^{-1} = 14)$.

$L_{P_1} : y = 6x + 15$ recta tangente por P_1.

Recordar

De acuerdo con el teorema de Bezout, una recta corta a una curva elíptica en tres puntos P,Q,R. Si dos de estos puntos son iguales, digamos $P = Q$, entonces la recta es tangente a la curva en el punto P.

Ahora calcularemos la intersección $L_{P_1} \cap C$

$$\begin{cases} y = 6x + 15 \\ y^2 = x^3 + x + 1 \end{cases}$$

Sustituyendo y en la ecuación de la curva tenemos

$$(6x + 15)^2 = x^3 + x + 1$$

entonces

$$0 = x^3 - 13x^2 + 5x + 6 = (x - 3)^2(x - x_3)$$

ya que el punto de tangencia $P_1 = (3,10)$ es una solución doble del sistema de ecuaciones.

Miramos el coeficiente de grado 2:

$$-13 = -3 - 3 - x_3 \Longrightarrow x_3 = -6 + 13 = 7$$

$$y_3 = 6 \cdot 7 + 15 = 11$$

El punto de intersección es pues (7,11) y su simétrico sobre $\mathbb{F}_{23}$ es (7,12).

Por lo tanto: $Q = 2P_1 = (7,12)$

Seguimos..., calculamos ahora la tangente a la curva que pasa por Q:

$$\begin{cases} \dfrac{\partial f}{\partial x}(Q) = 13 \\ \dfrac{\partial f}{\partial y}(Q) = 1 \end{cases}$$

Por lo tanto $13(x - 7) + (y - 12) = 13x + y + 11 = 0 \rightarrow y = 10x + 11$.

$L_Q : y = 10x + 11$ recta tangente por Q.

La intersección de esta tangente con la curva $L_Q \cap C$

$$\begin{cases} y = 10x + 11 \\ y^2 = x^3 + x + 1 \end{cases}$$

$$0 = x^3 - 8x^2 - 12x - 5 = (x - 7)^2(x - x_3)$$

Miramos el coeficiente de grado 2:

$$-8 = -7 - 7 - x_3 \Longrightarrow x_3 = 17$$

$$y_3 = 10 \cdot 17 + 11 = 20$$

El punto de intersección es (17,20) y, el simétrico sobre $\mathbb{F}_{23}$, es (17,3).

O sea: $R = 2Q = (17,3)$

Ahora, la recta que pasa por P_1 y R, $L_{P_1,R} : y = \alpha x + \beta$

$$\alpha = \frac{3-10}{17-3} = -\frac{8}{7} = 8 \cdot 10 = 11$$

$$10 = 11 \cdot 3 + \beta \Longrightarrow \beta = 10 - 10 = 0$$

Por lo tanto $L_{P_1,R} : y = 11x$.

Calculemos ahora la intersección con la curva: $L_{P_1,R} \cap C$:

$$\begin{cases} y = 11x \\ y^2 = x^3 + x + 1 \end{cases}$$

El punto de intersección es (9,7) y el simétrico sobre $\mathbb{F}_{23}$, es $S = R + P_1 = (9,16)$.

Calcularemos la tangente que pasa por S:

$$\begin{cases} \frac{\partial f}{\partial x}(Q) = 9 \\ \frac{\partial f}{\partial y}(Q) = 9 \end{cases}$$

Por lo tanto $9(x-9) + 9(y-16) = 0 \rightarrow x - 9 + y - 16 = 0 \rightarrow y = 22x + 2$.

$L_S : y = 22x + 2$ recta tangente por S.

Ahora corresponde calcular la intersección de esta recta L_S con la curva: $L_S \cap C$

$$\begin{cases} y = 22x + 2 \\ y^2 = x^3 + x + 1 \end{cases}$$

$$0 = x^3 - x^2 + 3x - 3 = (x-9)^2(x - x_3)$$

Miramos el coeficiente de grado 2:

$$-1 = -9 - 9 - x_3 \Longrightarrow x_3 = 6$$

$$y_3 = -6 \cdot +2 = 19$$

El punto de intersección es (6,19) y el simétrico a $\mathbb{F}_{23}$, es $2S = (6,4)$. Esta es la solución que buscábamos:

$$10P_1 = (6,4)$$

Ejemplo 2.3.

Sea $K = \mathbb{F}_{16}$, $C : y^2 + xy = x^3 + \alpha^4 x^2 + 1$, $P_1 = (\alpha^6, \alpha^8)$, $P_2 = (\alpha^3, \alpha^{13})$.

- Construir el cuerpo $\mathbb{F}_{16}$ (utilizando el polinomio primitivo $x^4 + x + 1$)
- Calcular $P_1 + P_2$
- Calcular $2 \cdot P_1$

En primer lugar construiremos el cuerpo finito $\mathbb{F}_{16} = \mathbb{Z}_2[x] \,/ x^4 + x + 1$.

Sea $\alpha = [x]$, la lista de los elementos en forma exponencial y su equivalente forma polinomial es entonces:

$\alpha = [x]$

$\alpha^2 = [x]^2 = [x^2]$

$\alpha^3 = [x]^3 = [x^3]$

$\alpha^4 = [x]^4 = [x^4] = [x + 1] = [x] + 1 = \alpha + 1$

$\alpha^5 = \alpha \cdot \alpha^4 = \alpha^2 + \alpha$

$\alpha^6 = \alpha^3 + \alpha^2$

$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$

$\alpha^8 = \alpha^2 + 1$

$\alpha^9 = \alpha^3 + \alpha$

$\alpha^{10} = \alpha^2 + \alpha + 1$

$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$

$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^{13} = \alpha^3 + \alpha^2 + 1$

$\alpha^{14} = \alpha^3 + 1$

$\alpha^{15} = 1$

Ahora calcularemos $P_1 + P_2 =$

- Recta que pasa por P_1 y P_2, $L_{P_1,P_2} : y = ax + b$

$$a = \frac{\alpha^{13} - \alpha^8}{\alpha^3 - \alpha^6} = \frac{\alpha^3 + \alpha^2 + 1 + \alpha^2 + 1}{\alpha^3 + \alpha^3 + \alpha^2} = \frac{\alpha^3}{\alpha^2} = \alpha$$

Por lo tanto, $y = \alpha x + b$. El punto P_1 pertenece a L_{P_1,P_2}:

$$\alpha^8 = \alpha \cdot \alpha^6 + b \Longrightarrow b = \alpha^8 + \alpha^7 = \alpha^{11}$$

$$L_{P_1,P_2} : y = \alpha x + \alpha^{11}$$

- $L_{P_1,P_2} \cap C$

$$\begin{cases} y = \alpha x + \alpha^{11} \\ y^2 + xy = x^3 + \alpha^4 x^2 + 1 \end{cases}$$

Sustituyendo el valor de y en la segunda ecuación, tenemos:

$$\alpha^2 x^2 + \alpha^{10} + \alpha x^2 + \alpha^{11} x = x^3 + \alpha^4 x^2 + 1$$

$$0 = x^3 + \alpha^8 x^2 + \alpha^{12} x + \alpha^{10} + 1 = (x - \alpha^6)(x - \alpha^3)(x - x_3)$$

Miramos el coeficiente de grado 2:

$$\alpha^8 = \alpha^6 + \alpha^3 + x_3 \Longrightarrow x_3 = \alpha^8 + \alpha^6 + \alpha^3 = \alpha^2 + 1 + \alpha^3 + \alpha^2 + \alpha^3 = 1$$

$$y_3 = \alpha + \alpha^{11} = \alpha^6$$

Sobre $\mathbb{F}_4$, el simétrico de un punto es él mismo.
Solución:

$$P_1 + P_2 = (1, \alpha^6)$$

En segundo lugar, vamos a calcular $2P_1$

– Tangente que pasa por P_1:

$$\begin{cases} \dfrac{\partial f}{\partial x}(P_1) = \alpha^9 \\ \dfrac{\partial f}{\partial y}(P_1) = \alpha^6 \end{cases}$$

$$\alpha^9(x - \alpha^6) + \alpha^6(y - \alpha^8) = 0 \rightarrow \alpha^3 x + \alpha^9 + y + \alpha^8 = 0$$

$L_{P_1} : y = \alpha^3 x + \alpha^{12}$

– $L_{P_1} \cap C$

$$\begin{cases} y = \alpha^3 x + \alpha^{12} \\ y^2 + xy = x^3 + \alpha^4 x^2 + 1 \end{cases}$$

Sustituyendo el valor de y en la segunda ecuación, tenemos:

$$\alpha^6 x^2 + \alpha^9 + \alpha^3 x^2 + \alpha^{12} x = x^3 + \alpha^4 x^2 + 1$$

$$0 = x^3 + \alpha^{10} x^2 + \alpha^{12} x + \alpha^7 = (x - \alpha^6)^2 (x - x_3)$$

Miramos el coeficiente de grado 2:

$$\alpha^{10} = \alpha^6 + \alpha^6 + x_3 = x_3$$

$$y_3 = \alpha^{13} + \alpha^{12} = \alpha$$

Solución:

$$2P_1 = (\alpha^{10}, \alpha)$$

2.2.2. Ecuación general de *P + Q*

Dada una curva elíptica, para calcular el resultado de hacer operaciones de acuerdo con la ley de grupo definida en el subapartado 2.2.1, podemos usar una fórmula que resume los cálculos que acabamos de hacer en los ejercicios anteriores.

Consideramos la curva elíptica C sobre K con $char(K) \neq 2,3$, con ecuación $C : y^2 = x^3 + Ax + B$. El punto base (en la recta del infinito) es $O = (0 : 1 : 0)$ de forma que el simétrico $-P$ de un punto $P = (x,y)$ se puede tomar como $-P = (x, -y)$. Sean $P = (x_1,y_1)$, $Q = (x_2,y_2)$, $P + Q = (x_3,y_3)$, con $P,Q \in C$, $-P = (x_1, -y_1)$. Suponemos que $Q \neq -P$. Entonces:

Observación

Verificar, si se desea, que el punto base $O = (0,1,0)$ pertenece a la curva $C : y^2 = x^3 + Ax + B$.

$$a) P \neq Q \begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \end{cases}$$

$$b) P = Q \begin{cases} x_3 = \left(\dfrac{3x_1^2 + A}{2y_1}\right)^2 - x_1 - x_1 \\ y_3 = \left(\dfrac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3) - y_1 \end{cases}$$

Si $Q = -P$, $P + Q = O$ (punto base de C).

Si $char(K) = 2$, tenemos dos casos (ver ecuación 5):

- $E : y^2 + cy = x^3 + ax + b,\ c \neq 0$
  $-P = (x_1, y_1 + c)$

$$\text{a) } P \neq Q \begin{cases} x_3 = \left(\dfrac{y_1 + y_2}{x1 + x_2}\right)^2 + x_1 + x_2 \\ \\ y_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + c \end{cases}$$

$$\text{b) } P = Q \begin{cases} x_3 = \dfrac{x_1^4 + a^2}{c^2} \\ \\ y_3 = \left(\dfrac{x_1^2 + a}{c}\right)(x_1 + x_3) + y_1 + c \end{cases}$$

- $E : y^2 + xy = x^3 + ax + b,\ b \neq 0$
  $-P = (x_1, y_1 + x_1)$

$$\text{a) } P \neq Q \begin{cases} x_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a \\ \\ y_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1 \end{cases}$$

$$\text{b) } P = Q \begin{cases} x_3 = x_1^2 + \dfrac{b}{x_1^2} \\ \\ y_3 = x_1^2 + \left(x_1 + \dfrac{y_1}{x_1}\right) x_3 + x_3 \end{cases}$$

Ejemplo 2.4.

Dada la curva $y^2 = x^3 + 10x + 13$ sobre $\mathbb{F}_{23}$ y los puntos de la misma $P = (7,9)$, $Q = (17,6)$, calcular $P + Q$.

Usando las fórmulas anteriores, si hacemos $P + Q = (x_3, y_3)$, resulta:

$$x_3 = \left(\frac{6-9}{17-7}\right)^2 - 7 - 17 = \frac{9}{8} - 1 = 3,$$

$$y_3 = \frac{6-9}{17-7}(7-3) - 9 = \frac{-3}{4}4 - 9 = 22.$$

Fijémonos en que hemos hecho sumas y multiplicaciones en el cuerpo finito $\mathbb{F}_{23}$ pero, también, divisiones. O, de otro modo, hemos tenido que calcular inversos en $\mathbb{F}_{23}$.

El cálculo de inversos en un cuerpo finito es una operación costosa que se puede obviar usando coordenadas proyectivas en lugar de coordenadas afines.

3. Curvas elípticas sobre cuerpos finitos

3.1. Número de puntos de una curva elíptica

En todo este apartado $K = \mathbb{F}_q$ representará un cuerpo finito, con $q = p^m$ elementos, para un cierto $m \in \mathbb{N}$ y p primo. Si E es una curva elíptica sobre K escribiremos E o $E(q)$ para designarla.

Recordar

$\mathbb{Z}_n$ representa el anillo de los enteros módulo n.

Notación

Escribiremos $N = \#E(q)$ para indicar el número de puntos racionales de E.

Teorema 3.1.

$(E(q), +)$, donde + representa la ley de grupo definida en el subapartado 2.2.1, es un grupo cíclico, que puede ser generado por un solo elemento, o bien se puede descomponer como suma directa de dos subgrupos cíclicos con órdenes n_1 y n_2, respectivamente, de forma que

$$E(q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

donde n_2 divide n_1 y $N = n_1 n_2$.

Definición 3.2 (Residuos cuadráticos).

Sea $x \in \mathbb{F}_q$. Si existe $z \in \mathbb{F}_q$ tal que $x = z^2$, diremos que x es un residuo cuadrático (QR). En caso contrario, diremos que x es un no-residuo cuadrático (QNR).

Definición 3.3 (Símbolo de Legendre).

Sea p un número primo y sea $n \in \mathbb{F}_p$. Definimos el símbolo de Legendre de n respecto p, y lo denotaremos por $\left(\frac{n}{p}\right)$, cómo:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ es QR} \pmod p \\ -1 & \text{si } n \text{ es QNR} \pmod p \end{cases}$$

Suponemos que $char(K) \neq 2,3$, $E : y^2 = x^3 + Ax + B$. La curva E contiene el punto del infinito $(0 : 1 : 0)$, por lo tanto, el número de puntos de la curva es $N \geq 1$. Tomemos ahora $x \in \mathbb{F}_q$ (x puede tomar q valores diferentes), si $\exists y \in \mathbb{F}_q$ tal que $y^2 = x^3 + Ax + B$, entonces $-y$ también cumple esta ecuación. Por lo tanto, podemos decir que $N \leq 1 + 2q$.

Definimos ahora el carácter cuadrático χ:

Algoritmo 3.4.

$\mathbb{F}_q^* \longrightarrow \{1, -1\}$
$x \longrightarrow 1$, si x es QR
$x \longrightarrow -1$, si x es QNR

Sea $f(x) = x^3 + Ax + B$. Fijado $x \in \mathbb{F}_q$, si $f(x)$ es QR, entonces tenemos 2 puntos de la curva; en cambio, si es QNR no tenemos ninguno. Así, podemos escribir N en función de $f(x)$:

$$N = 1 + \sum_{x \in \mathbb{F}_q} (\chi(f(x)) + 1) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

Vemos el caso particular $q = p$, $\mathbb{F}_q = \mathbb{Z}/p$.

$$\forall x \in \mathbb{Z}/p, \quad x^{p-1} = 1 \pmod{p} \Longrightarrow x^{\frac{p-1}{2}} = \begin{cases} +1, \text{ si } x \text{ es QR} \\ -1, \text{ si } x \text{ es QNR} \end{cases}$$

Recordar

Un carácter cuadrático χ es un homomorfismo del grupo multiplicativo del cuerpo finito $\mathbb{F}_q$ (que escribiremos $\mathbb{F}_q^*$) en el grupo multiplicativo $\{1, -1\}$.

Si q es un número primo, entonces $\chi(x) = \left(\frac{x}{q}\right)$.

Lema 3.5.

Sea p un número primo.

$$\sum_{x \in (\mathbb{Z}/p)^*} x^i = \begin{cases} p-1, \text{ si } i = 0 \text{ o } i = p-1 \\ 0, \text{ si } i \neq 0, p-1 \end{cases}$$

Demostración: Si $i = 0$, es claro que $\sum_{x \in (\mathbb{Z}/p)^*} x = p - 1$. Con $i = p - 1$ nos encontramos en la misma situación puesto que $x^{p-1} = 1 \pmod{p}$.

Consideramos el caso $i \neq 0, p-1$:

$\forall x \in (\mathbb{Z}/p)^*$ tenemos que $x^p - x = 0$. Por lo tanto, podemos escribir $x^p - x = (x-x_1)\cdots(x-x_p)$, donde $\mathbb{Z}/p = \{x_1, \ldots, x_p\}$.

Mirando el coeficiente de x^{p-1} en la ecuación $x^p - x = 0$, tenemos $0 = x_1 + \cdots + x_p$. También, mirando el coeficiente de x^{p-2} tenemos $\sum_{i,j} x_i x_j = 0$. Pero $\sum x_i^2 = (\sum x_i)^2 - 2\sum x_i x_j = 0$. Haciendo lo mismo para cada exponente i encontraríamos: $\sum_{x\in(\mathbb{Z}/p)^*} x^i = 0, \ \forall i \notin \{0, p-1\}$. ∎

Usaremos este lema para encontrar el valor de N:

$$N = 1 + p + \sum_{x\in\mathbb{F}_p} \chi(f(x)) = 1 + p + \sum_{x\in\mathbb{F}_p} (f(x))^{\frac{p-1}{2}}$$

$$= 1 + p + \sum_{x\in\mathbb{F}_p} (x^3 + Ax + B)^{\frac{p-1}{2}} = 1 + p + \sum_{x\in\mathbb{F}_p} \sum_{i=0}^{3\cdot\frac{p-1}{2}} f_i x^i$$

$$= 1 + p + \sum_{i=0}^{3\cdot\frac{p-1}{2}} f_i \sum_{x\in\mathbb{F}_p} x^i = 1 + p + \sum_{i=0}^{3\cdot\frac{p-1}{2}} f_i \sum_{x\in\mathbb{F}_p^*} x^i + f_0$$

$$= 1 + p + (p-1)f_0 + (p-1)f_{p-1} + f_0.$$

Por lo tanto, $N = 1 - f_{p-1} \pmod{p}$.

Casos especiales:

- Si $f_{p-1} = 0 \pmod{p}$ y, más concretamente, si $N = 1 + p$, E se denomina curva supersingular. Este tipo de curvas es importante, puesto que existe un algoritmo para romper el logaritmo elíptico definido sobre ellas.

- Si $f_{p-1} = 1 \pmod{p}$ y, concretamente, si $N = p$, E se denomina curva anómala. En este caso también es sencillo romper el logaritmo elíptico (Semaev-Smart-Satoh-Araki).

Definición 3.6 (Curvas supersingulares y anómalas).

Dado el cuerpo $K = \mathbb{F}_q$, con $q = p^m$, p primo, entonces:

- Si $N = 1 + q \pm t$, donde $p \mid t$, diremos que E es una curva supersingular.

- Si $N = 0 \pmod{p}$, diremos que E es una curva anómala.

Teorema 3.7 (Teorema de Hasse, 1930).

Consideramos la curva elíptica $E(q)$ y sea N el número de puntos racionales de $E(q)$. Se cumple:

$$|N-(1+q)| \leq 2\sqrt{q}$$

Observación

El teorema de Hasse nos da un intervalo bastante ajustado para el valor N: $1+q-2\sqrt{q} \leq N \leq 1+q+2\sqrt{q}$.

Para la demostración de este teorema, se necesita la hipótesis de Riemann.

Definición 3.8 (La función de Riemann).

La función de Riemann viene dada por:

$$\zeta(s) = \prod_{p \text{ primo}} \left(\frac{1}{1-\frac{1}{p^s}}\right) = \sum_{n\in\mathbb{N}} \frac{1}{n^s}$$

Para valores reales de s tenemos:

$$\zeta(s) = \begin{cases} 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots = \infty, \text{ si } s=1 \\ \text{tiene solución, si } s>1 \\ \text{diverge, si } s<1. \end{cases}$$

La hipótesis de Riemann dice que, sobre el cuerpo de los números complejos, los ceros no triviales de $\zeta(s)$ se encuentran todos sobre la recta $Re(s) = \frac{1}{2}$.

Hipótesis de Riemann

Es uno de los problemas abiertos más importantes y famosos de la matemática contemporánea. Es el cuarto problema del milenio que el Clay Mathematics Institute dotó con un premio de un millón de dólares para la primera persona que aporte una demostración correcta de la conjetura.

Ahora nos planteamos el problema inverso. Dado un valor N, ¿existe una curva elíptica que tenga este número de puntos?

Teorema 3.9.

Sobre el cuerpo finito $\mathbb{F}_q$, donde $q = p^m$ y p primo, si t es cualquier valor tal que:

$$\begin{cases} |t| \leq 2\sqrt{q} \\ si\ \ p|t \rightarrow p^n|t,\ \ donde\ \ n = \left\lfloor \frac{m+1}{2} \right\rfloor \end{cases}$$

entonces, podemos encontrar una curva elíptica con $N = 1+q+t$ puntos.

Ejemplo 3.1.

Las curvas elípticas sobre $\mathbb{Z}_2$ se pueden escribir cómo:

$$y^2 + xy = x^3 + b_2x^2 + b_6, \text{ si } \Delta = b_6 \neq 0$$

$$y^2 + b_3y = x^3 + b_4x + b_6, \text{ si } \Delta = b_3^4 \neq 0$$

Por el teorema de Hasse, $3 - 2\sqrt{2} \leq N \leq 3 + 2\sqrt{2} \rightarrow 1 \leq N \leq 5$.

- $E : y^2 + y = x^3 + x + 1$, $N = 1$ (solo tiene el punto del infinito).
- $E : y^2 + y = x^3 + x$, $N = 5$.
- $E : y^2 + xy = x^3 + x^2 + 1$, $N = 2$.
- $E : y^2 + xy = x^2 + 1$, $N = 4$.
- $E : y^2 + y = x^3 + 1$, $N = 3$.
- $E : y^2 + y = x^3$, $N = 3$.

Las dos últimas curvas son curvas supersingulares, puesto que $N = 1 + p$ y la tercera es una curva anómala.

¿Cómo podemos calcular el número de puntos N de una curva elíptica? Hay diferentes métodos:

1) Por fuerza bruta, probando toda pareja de puntos $(x,y) \in \mathbb{F}_q^2$.

2) A partir de $P = (x,y) \in E$, $y \neq 0$, calculamos $2P$, $3P, \cdots$ hasta obtener el subgrupo $\langle P \rangle \subset E$. Si E fuera cíclico ($n_1 = N, n_2 = 1$) y P fuera un generador de E, obtendríamos $\langle P \rangle = E$. En el supuesto de que N fuese un número primo, tendríamos que todos los $P \neq O$ son generadores.

3) Algoritmo de Schoof (1985). Calcula el número de puntos de una curva con una complejidad $O(log_2^8(q))$.

Hay casos particulares algo más sencillos; por ejemplo, curvas del tipo $y^2 = x^3 + Ax$ o $y^2 = x^3 + B$. En estos casos se usa el algoritmo de Munuera-Tena (1993) con complejidad del orden de $O(log_2^3(p))$.

3.2. Extensión de una curva sobre un cuerpo a una curva sobre un cuerpo extendido

Una curva elíptica definida sobre $\mathbb{F}_p$ puede considerarse también definida sobre $\mathbb{F}_q$ donde $q = p^m$. Denotemos $N = \#E(p) = p + 1 - t$ y $N_m = \#E(q)$.

Conjetura de Weil: (de hecho, es un teorema de Schmidt de 1925, previo a Weil). Sean $\alpha, \beta \in \mathbb{C}$ las raíces conjugadas de la ecuación $x^2 + tx + p = 0$. Entonces:

$$N_m = 1 + p^m - \alpha^m - \beta^m$$

Ejemplo 3.2.

Consideramos la curva $E : y^2 + y = x^3$. Sabemos que E tiene 3 puntos sobre $Z/2$. Vamos a calcular cuántos puntos tiene la curva definida por la misma función, sobre $\mathbb{F}_{2^m}$.

Calculamos α y β, haciendo $t = \left(N - (p+1)\right)$ en la ecuación anterior:

$$x^2 + (3-3)x + 2 = 0 \rightarrow \begin{cases} \alpha = \sqrt{2}y \\ \beta = -\sqrt{2}y \end{cases}$$

- Si $m = 0 \pmod 4$, entonces $N_m = 1 + 2^m - 2\sqrt{2^m}$
- Si $m = 2 \pmod 4$, entonces $N_m = 1 + 2^m + 2\sqrt{2^m}$
- Si $m = 1,3 \pmod 4$, entonces $N_m = 1 + 2^m$

4. El uso de las curvas elípticas en criptografía

En 1985, Koblitz y Miller propusieron, de manera independiente, la utilización del grupo de puntos de una curva elíptica definida sobre un cuerpo finito como base para criptosistemas basados en la dificultad de romper el logaritmo discreto.

4.1. El problema del logaritmo elíptico

Como hemos visto en el apartado anterior, los puntos de una curva elíptica forman un grupo respecto de la suma. Dado un punto P de una curva elíptica E, podemos calcular $Q = sP$, $s \in \mathbb{Z}$, donde Q vuelve a ser un punto de la curva E.

Definición 4.1 (Problema del logaritmo elíptico).

Sea E una curva elíptica sobre el cuerpo finito $\mathbb{F}_q$, con $q = p^m$, p primo, $m \in \mathbb{N}$, y sea $P \in E$ de orden n. El problema del logaritmo elíptico en E (respecto de la base P) dado $Q \in E$, se basa en encontrar $s \in \mathbb{Z}$ tal que $Q = sP$, en caso de que exista.

En este subapartado veremos algunos métodos y algoritmos conocidos para romper el logaritmo elíptico.

El algoritmo de Silver -Pohlig-Hellman para romper el logaritmo discreto en el cuerpo F_p tiene una complejidad de $\mathcal{O}(\sqrt{N_1})$, donde $p - 1 = N_1 \cdot \ldots \cdot N_r$ es la factorización de $(p - 1)$ en primos y N_1 es el más grande de estos primos. En el caso del logaritmo elíptico tenemos que $N = N_1 \cdot \ldots \cdot N_r$, es la factorización de N en primos y N_1 es el primo más grande y, del mismo modo,romper este logaritmo tiene una complejidad de $\mathcal{O}(\sqrt{N_1})$.

Observación

Si $K = \mathbb{Z}/p$, p primo grande y $N = p$, entonces tenemos que $N = N_1 (= p)$ es un primo grande y además, cualquier punto diferente del neutro es generador con orden N. Por otro lado, hemos visto que si $N = p$, entonces E es una curva anómala y el logaritmo es fácil de romper en estos casos. También es fácil de romper en el caso $N = p + 1$, que corresponde a las curvas supersingulares.

Supongamos que $K = \mathbb{F}_q$, donde $q = p^m$ y p primo pequeño. Sea $N = \#E(q)$ y $N_1 = \#E(p)$. Sabemos que los puntos que pertenecen a la curva sobre el cuerpo base, también son puntos de la curva en un cuerpo mayor y el grupo de puntos de la curva sobre el cuerpo base es un subgrupo del grupo de puntos de la curva sobre el cuerpo mayor. Así, $N_1 | N$ y existe un entero d tal que $N = N_1 \cdot d$. Querríamos $N = N_1 \cdot \ldots \cdot N_r$, con algún N_i primo grande; así, si N_1 es primo grande, ya hemos acabado. Si N_1 es pequeño, entonces d es grande, si además d es primo ya tenemos una buena descomposición. En el supuesto de que $N = N_1 \cdot d$ con d primo, se dice que que E es quasiprima.

Teorema 4.2 (Tena, 1994).

Sea $K = \mathbb{F}_q$, donde $q = p^m$ y p primo pequeño, E curva elíptica sobre K. Una condición necesaria para que E sea cuasiprima es que m sea primo.

El mejor algoritmo conocido para romper el logaritmo elíptico es el método ρ de Pollard, que necesita $\frac{\sqrt{\pi n}}{2}$ pasos (sumas de puntos en curvas elípticas). Este método se puede paralelizar con r procesadores y conseguir rebajar el número de pasos necesarios a $\frac{\sqrt{\pi n}}{2r}$.

Teorema 4.3 (MOV -Menezes, Okamoto y Vanstone-, 1993).

El cálculo del logaritmo elíptico sobre $\mathbb{Z}/p$ es equivalente al cálculo del logaritmo discreto sobre $\mathbb{F}_{p^k}$ para algún entero k.

Esta equivalencia se obtiene haciendo la inmersión del grupo de puntos de la curva definida sobre el cuerpo base dentro del grupo multiplicativo $\mathbb{F}^*_{p^k}$, lo que solo es posible si N divide $p^k - 1$. En $\mathbb{F}^*_{p^k}$ se puede usar el algoritmo index-calculus o el algoritmo *NFS* (*number field sieve*) para romper el logaritmo, lo que proporciona un algoritmo subexponancial del orden de

Para $k = 6$ cuando $p \simeq \mathcal{O}(160)$ bits, entonces $p^k \simeq \mathcal{O}(2000)$ bits.

$$exp\left[\left(c + o(s)\right) \cdot \left(log(p^k)\right)^{\frac{1}{3}} \cdot \left(log\left(log(p^k)\right)\right)^{\frac{2}{3}}\right]$$

El método xedni-calculus (Silverman) es la idea inversa del index-calculus. Dada $E(\mathbb{Z}/p)$ se proyectan r combinaciones lineales en el plano sobre el cuerpo $\mathbb{Q}$ y se considera la curva $E(\mathbb{Q})$ que contiene estos r puntos. En el supuesto de que estos r puntos obtenidos sean linealmente dependientes, se soluciona el problema elíptico. Actualmente se usa este método con $r \leq 9$ y la probabilidad de que los puntos obtenidos sean linealmente dependientes es muy pequeña. La importancia del xedni-calculus es que es fácilmente adaptable tanto al problema del logaritmo discreto como a la factorización, por tanto permitiría atacar todos los criptosistemas de clave pública en caso de que se encontrara algún algoritmo eficiente para resolverlo.

Observación

En la equivalencia dada por el algoritmo MOV, normalmente, el valor del parámetro k será muy grande y, por lo tanto, no ganaremos nada haciendo la conversión del logaritmo elíptico en logaritmo discreto clásico. Pero, en algunos casos, sí que podremos romper el logaritmo elíptico a través de los algoritmos para romper el logaritmo discreto (esto es el que pasa para las curvas supersingulares donde es conocido que $k \leq 6$).

4.2. Elección de la curva

La elección de la curva elíptica se debe hacer teniendo en cuenta los ataques comentados en el subapartado anterior:

- Para resistir el ataque por el método ρ de Pollard, el número de puntos de la curva debe ser divisible por un número primo lo suficientemente grande ($> 2^{160}$).

- Para resistir el ataque de Semaev-Smart-Araki, el número de puntos de la curva no debe ser múltiple de p.

- Para resistir la reducción MOV n (orden del punto escogido) no debe dividir $p^k - 1$, k pequeño.

- Para resistir los ataques contra curvas elípticas supersingulares, el número de puntos de la curva no debe ser igual a 1 módulo p.

Veamos ahora diferentes métodos conocidos para escoger una curva adecuada.

1) El **Teorema de Hasse** y la **Conjetura de Weil** nos proporcionan una técnica para elegir curvas sobre $\mathbb{F}_{2^m}$, donde m es divisible por un entero l pequeño. De hecho, como estos resultados son válidos para cualquier $\mathbb{F}_{p^m}$, podríamos extender esta técnica a todos estos cuerpos.

Recordemos que dada una curva elíptica E, definida sobre $\mathbb{F}_p$, podemos considerarla también como una curva elíptica sobre cualquier extensión $\mathbb{F}_{p^m}$ de $\mathbb{F}_p$. Además, sabemos calcular el número de puntos de la curva sobre el cuerpo extendido, a partir del número de puntos de la curva sobre el cuerpo base.

Para elegir una curva adecuada sobre $\mathbb{F}_{2^m}$, primero tomaremos una curva sobre $\mathbb{F}_{2^l}$, con l dividiendo m y calcularemos el número de puntos de la curva sobre $\mathbb{F}_{2^l}$ (que se puede hacer de forma exhaustiva puesto que hemos elegido l de forma que el cuerpo $\mathbb{F}_{2^l}$ sea pequeño). Entonces calcularemos el número de puntos de la curva sobre el cuerpo extendido y comprobaremos si es resistente a los ataques anteriores. En caso de que no resista alguno de los ataques anteriores repetimos el proceso hasta encontrar una curva adecuada.

El principal problema que presenta esta técnica es que el número de curvas sobre $\mathbb{F}_{2^l}$ será relativamente pequeño, y por lo tanto, es posible que dados m y l no consigamos encontrar ninguna curva adecuada usando este método.

2) Método global. Esta manera de elegir la curva está basada en tomar una curva sobre los racionales y reducirla módulo un primo para tener la curva sobre un cuerpo finito y comprobar si resiste los ataques anteriores.

Por ejemplo, si empezamos con $E : y^2 = x^3 + Ax + B$, donde A,B son números racionales podemos considerar la misma ecuación módulo un primo p. Entonces, tendremos la curva sobre $\mathbb{F}_p$ con N_p puntos. Hay resultados teóricos que aseguran que para p lo suficientemente grande N_p es múltiplo del número de puntos de orden finito de la curva original sobre los racionales. Así, conociendo el número de puntos de orden finito sobre el cuerpo inicial tendremos una cota inferior para el número de puntos de la curva sobre $\mathbb{F}_p$.

3) Método de la multiplicación compleja. Este método permite la elección del orden de la curva antes de construirla. Se debe comprobar que el orden que queremos supere los ataques mencionados. Este método es eficiente cuando el cardinal q del cuerpo y el valor t tal que $\#E = 1 + q - t$ son escogidos de forma que el cuerpo $\mathbb{Q}(\sqrt{t^2 - 4q})$ tiene un número pequeño de clases de ideales. Para

curvas elípticas sobre $\mathbb{F}_p$ este método se denomina método de Atkin-Morain y, sobre $\mathbb{F}_{2^m}$, método de Lay-Zimmerman.

4) Método de elección aleatoria. Como su nombre indica, en este método se elige la curva de manera aleatoria. Fijado un cuerpo finito $\mathbb{F}_q$, suponemos que $char(K) \neq 2,3$ y la curva $E : y^2 = x^3 + Ax + B$. Seleccionamos $A,B \in \mathbb{F}_q$ de forma aleatoria, pero satisfaciendo $4A^3 + 27B^2 \neq 0$. Calculamos entonces el número de puntos de la curva sobre $\mathbb{F}_q$ y lo factorizamos. Este proceso se repetirá hasta encontrar una curva que pueda resistir los ataques anteriores.

Este método es especialmente usado en el caso de trabajar con curvas elípticas sobre $\mathbb{F}_p$, puesto que resultados de Lenstra demuestran su funcionalidad. Para curvas elípticas sobre $\mathbb{F}_{2^m}$ hay resultados similares en los trabajos de Waterhouse y Schoof.

4.3. Asignación de mensajes a puntos

Uno de los problemas prácticos que se plantean a la hora de usar este tipo de criptografía es el de definir una correspondencia entre los mensajes que se quieren transmitir y los puntos de la curva. Existen diferentes procedimientos para hacerlo; veamos dos de ellos. Suponemos que $char(K) \neq 2,3$. $E : y^2 = f(x) = x^3 + Ax + B$.

4.3.1. Creación de una tabla

Sea m el mensaje que queremos transmitir, $0 < m < C$, donde C es una cota superior del número de mensajes diferentes. Tomamos k arbitrario (que llamaremos grado de fiabilidad), escogemos p primo tal que $p > Ck$, p con al menos 160 bits para asegurar la fortaleza del sistema. Podemos suponer los elementos $1,\ldots,Ck$ contenidos en $\mathbb{Z}/p$ usando la siguiente tabla:

$$\begin{bmatrix} & 1 & 2 & \ldots & k-1 \\ k & k+1 & k+2 & \ldots & 2k-1 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ mk & mk+1 & mk+2 & \ldots & (m+1)k-1 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ (C-1)k & \cdots & \cdots & \ldots & Ck-1 \end{bmatrix}$$

donde cada fila representa una clase.

Dado m, tomamos $x = mk$ y calculamos $y^2 = f(x)$. Si $f(x)$ no tiene raíz cuadrada, entonces necesitamos otro valor de x, tomamos $x = mk + 1$ y repetimos el

mismo proceso hasta encontrar x tal que $f(x)$ tiene raíz cuadrada, tomando entonces $y = \sqrt{f(x)}$.

Ahora nos podríamos preguntar: ¿este valor x se encuentra en la clase de m? Sabemos que la mitad de los elementos de $\mathbb{Z}/p$ tienen raíz cuadrada y están repartidos aleatoriamente. La probabilidad que en una fila no haya un cuadrado es pues $\frac{1}{2^k}$. Por lo tanto, la probabilidad de que en una fila no haya una x válida se puede hacer tan pequeña como queramos, aumentando el valor de k.

Así pues, dado m, existe un valor $j \in \{1,\ldots,k-1\}$ tal que el punto $P = (mk+j,y)$ pertenece a la curva. Tenemos entonces la correspondencia:

Algoritmo 4.4.

Curva $\longrightarrow \mathbb{Z}/p$
$m \longrightarrow (mk+j,y)$
$\left\lfloor \frac{\alpha}{k} \right\rfloor \longleftarrow (\alpha,\beta)$

4.3.2. Método de curvas entrelazadas

Definición 4.5 (Curvas entrelazadas).

Sea $E : y^2 = x^3 + Ax + B$ una curva elíptica sobre $\mathbb{Z}/p$, p primo. Sea $E' : y^2 = x^3 + A\beta^2 x + B\beta^3$, con $\beta \in \mathbb{Z}/p$, β NQR. Diremos que E y E' son curvas entrelazadas.

Teorema 4.6.

Sean E y E' curvas entrelazadas. Entonces

$$\#E + \#E' = 2(p+1)$$

Observación

Fijada una curva E, existe una gran cantidad de parejas (E,E') de curvas entrelazadas.

El concepto de par de curvas entrelazadas permite definir una aplicación biyectiva entre el conjunto de valores $\{0,1,\ldots,2p+1\}$ y el conjunto de puntos de las dos curvas. Así, a cada punto $P = (x,y)$ que puede pertenecer bien a E o bien a E', le asignamos un valor de $m \in \{0,1,\ldots,2(p+1)\}$ de la siguiente manera:

$$m = \begin{cases} 2x, & \text{si } P \in E,\ 0 \le y \le \dfrac{p-1}{2} \\ 2x+1, & \text{si } P \in E,\ \dfrac{p-1}{2} < y \le p \\ 2p, & \text{si } P = (\infty,\infty) \in E \\ \dfrac{2x}{\beta}, & \text{si } P \in E',\ 0 \le y \le \dfrac{p-1}{2} \\ \dfrac{2x}{\beta}+1, & \text{si } P \in E',\ \dfrac{p-1}{2} < y \le p \\ \dfrac{2x}{\beta}+1, & \text{si } P = (x,0) \in E' \\ 2p+1, & \text{si } P = (\infty,\infty) \in E' \end{cases}$$

donde $\dfrac{2x}{\beta}$ se ha de reducir módulo $2p$.

Supongamos ahora que tenemos el mensaje m. El punto asociado es:

$$P = \begin{cases} (\dfrac{m}{2}, \sqrt{\omega}) \in E, & \text{si } m \text{ es par y } \omega \neq 0 \text{ es QR} \pmod p \\ (\beta\dfrac{m}{2}, \sqrt{\beta^3\omega}) \in E', & \text{si } m \text{ es par y } \omega \neq 0 \text{ es NQR} \pmod p \\ (\dfrac{m}{2}, 0) \in E, & \text{si } m \text{ es par, } \dfrac{m}{2} \neq p \text{ y } \omega = 0 \\ (\infty,\infty) \in E, & \text{si } m \text{ es par, } \dfrac{m}{2} = p \\ (\dfrac{m-1}{2}, -\sqrt{\omega}) \in E, & \text{si } m \text{ es impar y } \omega \neq 0 \text{ es QR} \pmod p \\ (\beta\dfrac{m-1}{2}, -\sqrt{\beta^3\omega}) \in E', & \text{si } m \text{ es impar y } \omega \neq 0 \text{ es NQR} \pmod p \\ (\beta\dfrac{m-1}{2}, 0) \in E', & \text{si } m \text{ es impar, } \dfrac{(m-1)}{2} \neq p \text{ y } \omega = 0 \\ (\infty,\infty) \in E', & \text{si } m \text{ es impar, } \dfrac{(m-1)}{2} = p \end{cases}$$

donde $\omega \equiv x^3 + Ax + B \pmod p$ y $\sqrt{\alpha}, -\sqrt{\alpha}$ son las raíces cuadradas de un elemento α.

Ejemplo 4.1.

Sea $p = 31$ y la pareja de curvas entrelazadas (hemos escogido $\beta = 13$):

$$E : y^2 = x^3 + 3x + 1$$

$$E' : y^2 = x^3 + 3 \cdot 13^2 + 1 \cdot 13^3 = x^3 + 11x + 27$$

E tiene 39 puntos y E' tiene 25:

Puntos de E:

(0,1)	(0,30)	(1,6)	(1,25)	(6,7)	(6,24)
(8,14)	(8,17)	(10,15)	(10,16)	(11,1)	(11,30)
(13,6)	(13,25)	(14,11)	(14,20)	(17,6)	(17,25)
(18,11)	(18,20)	(19,2)	(19,29)	(20,1)	(20,30)
(21,5)	(21,26)	(22,12)	(22,19)	(24,3)	(24,28)
(26,4)	(26,27)	(27,7)	(27,24)	(29,7)	(29,24)
(30,11)	(30,20)	(∞,∞)			

$$\text{Puntos de } E'\text{:} \begin{cases} (1,15) & (1,16) & (3,5) & (3,26) & (8,10) & (8,21) \\ (9,7) & (9,24) & (15,8) & (15,23) & (20,1) & (20,30) \\ (21,8) & (21,23) & (22,6) & (22,25) & (23,4) & (23,27) \\ (24,14) & (24,17) & (26,8) & (26,23) & (29,11) & (29,20) \\ (\infty,\infty) \end{cases}$$

Entre las dos curvas tenemos pues 64 puntos. La correspondencia entre mensajes y puntos viene dada por la tabla siguiente.

punto de E	mensaje	punto de E'	mensaje
(0,1)	0	(1,15)	24
(0,30)	1	(1,16)	25
(1,6)	2	(3,5)	10
(1,25)	3	(3,26)	11
(6,7)	12	(8,10)	6
(6,24)	13	(8,21)	7
(8,14)	16	(9,7)	30
(8,17)	17	(9,24)	31
(10,15)	20	(15,8)	50
(10,16)	21	(15,23)	51
(11,1)	22	(20,1)	46
(11,30)	23	(20,30)	47
(13,6)	26	(21,8)	8
(13,25)	27	(21,23)	9
(14,11)	28	(22,6)	32
(14,20)	29	(22,25)	33
(17,6)	34	(23,4)	56
(15,25)	35	(23,27)	57
(18,11)	36	(24,14)	18
(18,20)	37	(24,17)	19
(19,2)	38	(26,8)	4
(19,29)	39	(26,23)	5
(20,1)	40	(29,11)	14
(20,30)	41	(29,30)	15
(21,5)	42	(∞,∞)	63
(21,26)	43	-	-
(22,12)	44	-	-
(22,19)	45	-	-
(24,3)	48	-	-
(24,28)	49	-	-
(26,4)	52	-	-
(26,27)	53	-	-
(27,7)	54	-	-
(27,24)	55	-	-
(29,7)	58	-	-
(29,24)	59	-	-
(30,10)	60	-	-
(30,20)	61	-	-
(∞,∞)	62	-	-

5. Criptografía y protocolos criptográficos basados en curvas elípticas

5.1. Protocolos criptográficos

Escribiremos $E_U(m)$ cuando hablamos de cifrar el mensaje m usando la clave pública del usuario U y $D_U(c)$ cuando hablamos de descifrar el mensaje c.

5.1.1. Protocolo de Diffie-Helman

Versión clásica. Sea p un número primo, $\alpha \in \mathbb{Z}_p$ un elemento primitivo. Cada usuario U elige al azar un número secreto $n_U \in \mathbb{Z}_p^*$ y hace público el valor α^{n_U}. Los usuarios A y B desean compartir una clave secreta:

Algoritmo 5.1.

$A \xrightarrow{\alpha^{n_A}} B$
$A \xleftarrow{\alpha^{n_B}} B$

La clave secreta será $K = \alpha^{n_A \cdot n_B}$, que solo es conocida por A y B.

Versión con curvas elípticas. Sea E una curva elíptica sobre $\mathbb{F}_p$ y $P \in E$ punto públicamente conocido. Cada usuario U elige al azar un número secreto $n_U \in \mathbb{F}_p$ y hace público el valor $n_U P$. Para compartir una clave secreta, A y B deben hacer:

Algoritmo 5.2.

$A \xrightarrow{n_A P} B$
$A \xleftarrow{n_B P} B$

La clave secreta será $K = (n_A \cdot n_B)P$ que solo es conocida por A y B.

Ejemplo 5.1. Acuerdo de claves de *Diffie-Helman* usando curvas elípticas

En primer lugar, los usuarios A y B eligen una curva elíptica E sobre un cuerpo finito $\mathbb{Z}_p$. También eligen un punto P de la curva de forma que su orden sea un número primo grande.

Suponemos que la curva elíptica es $E : y^2 = x^3 + 5x + 7$ sobre $\mathbb{Z}_{113}$. El número de puntos racionales de esta curva es 127 que es un número primo y, por lo tanto, los puntos de la curva elíptica constituyen un grupo isomorfo a $\mathbb{Z}_{127}$.

Tomemos $P = (16,51)$ que tiene orden $ord(P) = 127$, o sea P es un generador de la curva E.

Protocolo

- $A \to B$. El usuario A elige un entero grande n_A, calcula $K_A = n_A \cdot P$ y envía K_A a B.

  Si A toma, por ejemplo, $n_A = 98$, entonces, $K_A = n_A \cdot P = (24,74)$.

- $B \to A$. El usuario B elige un entero grande n_B, calcula $K_B = n_B \cdot P$ y envía K_B a A.

  Si B toma, por ejemplo, $n_B = 101$; entonces, $K_B = n_B \cdot P = (3,7)$.

- $A \to B$. El usuario A calcula $K = n_A \cdot K_B = n_A \cdot n_B \cdot P = 98 \cdot (3,7) = (5,48)$.

- $B \to A$. El usuario B calcula $K = n_B \cdot K_A = n_B \cdot n_A \cdot P = 101 \cdot (24,74) = (5,48)$.

Al finalizar el algoritmo, tanto A como B disponen del mismo punto que tomarán como clave de sesión: $K = (5,48)$.

Utilización del software SAGE

Simulador de cálculos en curvas elípticas

Para comprobar los cálculos de este ejemplo podéis usar el programa SAGE, que encontraréis en la dirección http:www.sagemath.org/.

En este ejemplo podemos seguir los cálculos numéricos haciendo uso del software SAGE. Se puede utilizar instrucción a instrucción, pero también se puede utilizar un script que nos calcule directamente el resultado que queremos.

Antes que nada definiremos el cuerpo finito $\mathbb{F}_{113}$, que denominaremos F, con la orden:

```
sage: F = FiniteField(113)
```

A continuación definiremos la curva elíptica $y^2 = x^3 + 5 * x + 7$. En general, la curva definida por los parámetros $[a,b,c,d,e]$ es $y^2 + axy + cy = x^3 + bx^2 + dx + e$.

```
sage: E = EllipticCurve(F,[0,0,0,5,7])
Elliptic Curve defined by y^2 = x^3 + 5*x + 7 over Finite Field of size 113
```

Si queremos conocer el orden de la curva elíptica:

```
sage: print(E.cardinality())
127
```

A continuación, para indicarle el punto $P = (16,51)$ escribiremos lo siguientes (y calcularemos, también, su orden):

```
sage: P = E.point((16,51))
sage: P.order()
```

donde estamos explicando que se toma el punto $P = (16,51)$ dentro del dominio de puntos de la curva E.

El usuario A calcula $K_A := 98P$ y el usuario B $K_B := 101 * P$:

```
sage: K_A = 98*P
sage: K_B = 101*P
```

Finalmente, podemos comprobar que los dos usuarios pueden utilizar la misma clave común: $K = n_A * K_B = n_B * K_A$:

```
print 101*K_A,98*K_B
```

Tras esta última instrucción SAGE contesta con los dos valores que le hemos pedido imprimir:

```
(5 : 48 : 1) (5 : 48 : 1)
```

Observar que SAGE está realizando las operaciones en coordenadas proyectivas.

5.1.2. Protocolo de tres-pasos de Shamir

Versión clásica. Este protocolo pretende enviar el mensaje m de A a B.

Algoritmo 5.3.

$A \xrightarrow{E_A(m)} B$
$A \xleftarrow{E_B(E_A(m))} B$
$A \xrightarrow{E_B(m)} B$

Es fundamental suponer que la función criptográfica utilizada cumple, para cada pareja de usuarios, $E_A \cdot E_B = E_B \cdot E_A$. Un ejemplo de función criptográfica con esta característica es $E_A(x) = x^{n_A}$ en $\mathbb{Z}/p$, con p primo y n_A clave privada del usuario A. En este caso concreto, el protocolo se denomina protocolo de Massey-Omura:

Algoritmo 5.4.

$A \xrightarrow{m^{n_A}} B$
$A \xleftarrow{(m^{n_A})^{n_B}} B$
$A \xrightarrow{m^{n_B}} B$

Versión con curvas elípticas. Veamos la traducción del protocolo de Massey-Omura. Sea E una curva elíptica sobre $\mathbb{F}_q$, $N = \#E(q)$. Sea $P \in E$ el mensaje que el usuario A quiere enviar a B. Cada usuario U tiene una clave privada n_U tal que $\text{mcd}(n_U, N) = 1$.

Algoritmo 5.5.

$A \xrightarrow{n_A P} B$
$A \xleftarrow{n_B(n_A P)} B$
$A \xrightarrow{n_B P} B$

5.2. Criptosistema ElGamal

Versión clásica. Se basa en el problema del logaritmo discreto sobre un cuerpo finito $\mathbb{Z}/p$, con p primo. Sea $\alpha \in \mathbb{Z}/p$ un elemento primitivo el cual se hace público. Cada usuario U tiene una clave privada $n_U \in \mathbb{Z}/p - \{0,1,p-1\}$ y hace pública la clave pública $\alpha_U = \alpha^{n_U}$. Suponemos que el usuario A quiere enviar el mensaje m al usuario B. A debe seguir los siguientes pasos:

- A escoge un número $k \in \mathbb{Z}/p - \{0,1,p-1\}$ al azar y calcula α^k,
- cifra m como $c = E_B(m) = m \cdot (\alpha_B)^k$,
- envía a B el par (c,α^k).

B para descifrar el mensaje deberá hacer:

- calcula $\beta = (\alpha^k)^{n_B}$,
- $m = c \cdot \beta^{-1}$.

Versión con curvas elípticas. Sea E una curva elíptica sobre $\mathbb{Z}/p$, sea P un punto de la curva de orden grande N (sería deseable que $\langle P\rangle = E$), $N|\#E(p)$. Para cada usuario U, sea n_U su clave privada, $1 < n_U < N$; (bastaría tomar $n_U < p + 1 - 2\sqrt{p}$). La clave pública de U será $P_U = n_U P$. Suponemos que el usuario A quiere enviar el mensaje m cifrado al usuario B:

- A escoge al azar un número $k \in \mathbb{Z}/p$,
- calcula P_m el punto de la curva asociado al mensaje m,
- cifra P_m como $C = E_B(P_m) = P_m + k \cdot P_B$,
- envía a B (C,kP).

B para descifrar el mensaje deberá hacer:

- $P_m = C - n_B(kP)$,
- encuentra el mensaje m asociado con el punto P_m.

5.3. Criptosistema RSA

Versión clásica. Se basa en la función de una vía o unidireccional de la potenciación: $E_{(e,n)}(x) = x^e \pmod n$ donde $1 < x < n = pq$, $1 < e < \varphi(n)$ con $mcd(e,\varphi(n)) = 1$ y $d = e^{-1} \pmod{\varphi(n)}$. La fortaleza del criptosistema se basa en que p y q sean números primos grandes y, por lo tanto, n sea difícilmente factorizable, lo que imposibilita calcular $\varphi(n)$.

Recordar

La función de Euler $\varphi(n)$ proporciona el cardinal de los números entre 1 y n que son primos con n. En el supuesto de que n sea un número primo $n = p$, tenemos $\varphi(p) = p - 1$. En el supuesto de que $n = p \cdot q$ es el producto de dos primos tenemos $\varphi(n) = (p-1)\cdot(q-1)$.

Supongamos que un usuario A quiere enviar un mensaje m a B. Los parámetros públicos de B son (e,n), y los privados $(p,q,\varphi(n),d)$. A deberá seguir los siguientes pasos:

- El usuario A cifra m calculando $c = E_{(e,n)}(x) = x^e \pmod n$ (con el método de multiplicar y elevar al cuadrado, por ejemplo),
- El usuario A envía c a B.

Observación

Actualmente no se conoce ningún algoritmo de factorización de complejidad menor que la sub-exponencial.

El usuario B para descifrar el mensaje c deberá hacer:

- $m = D_{(d,n)}(c) = c^d \pmod n$

Versión con curvas elípticas (esquema de KMOV. 1991). En este esquema se representan los puntos de una curva elíptica de la forma $y^2 = x^3 + b$ sobre $\mathbb{Z}_n$ como $E_n(b)$. Para generar la clave pública el usuario B escogerá dos números primos grandes (p,q) tales que $p = q = 2 \pmod 3$ y, como en el esquema clásico, calculará y publicará (e,n), donde $n = p \cdot q$ y mantendrá en secreto las claves privadas $(p,q,\varphi(n),d)$.

Cada vez que A quiere enviar un mensaje m a B deberá seguir los siguientes pasos:

- El usuario A divide su mensaje m en dos partes $m = (m_1,m_2)$ donde $m_1,m_2 \in \mathbb{Z}_n$.
- El usuario A determina el valor b de la curva de forma que $m \in E_n(b)$. Específicamente, calcula $b = m_2^2 - m_1^3 \pmod n$.
- cifra el punto m calculando $c = E(m) = e \cdot m$ sobre $E_n(b)$,
- envía el texto cifrado $c = (c_1,c_2)$ a B.

El usuario B para descifrar el mensaje c deberá hacer:

- a partir del mensaje cifrado $c = (c_1,c_2)$ el usuario B puede determinar el valor de b puesto que este no cambia en el proceso de cifrado. Específicamente, calcula $b = c_2^2 - c_1^3 \pmod n$ y construye la curva $y^2 = x^3 + b$.
- a partir de la clave privada calcula $m = D(c) = d \cdot c$ sobre $E_n(0,b)$.

Observación

El esquema de KMOV (Koyama, Maurer, Okamoto, Vanstone) usa curvas elípticas definidas sobre $\mathbb{Z}_n$, donde $n = p \cdot q$ es el producto de dos números primos que se mantienen en secreto. La seguridad de KMOV es la misma que la del esquema RSA. No obstante, el cifrado en el esquema KMOV es más flexible que en el RSA, por ejemplo, la curva elíptica no se fija, sino que se construye para cada nuevo mensaje. Para solucionar este inconveniente hay otros esquemas como el de Demytko (1993), Meyer y Müller (1996), Paillier (1999), etc.

5.4. Firma digital

En 1991 el NIST (National Institute of Standards and Technology) propuso el DSS (*digital signature standard*), basado en el DSA (*digital signature algorithm*), como estándar de firma digital. El DSS se basa en el criptosistema ElGamal. Aun cuando podemos hacer la traducción de este sistema de firma a las curvas elípticas, el que veremos es la versión análoga al DSA denominada ECDSA (*elliptic curve digital signature algorithm*) puesto que este se ha convertido en el estándar de firma digital con curvas elípticas.

Versión clásica: DSS. Usaremos la misma nomenclatura que en el criptosistema ElGamal que ya hemos visto anteriormente.

Ver también

El criptosistema ElGamal se estudia en el módulo "Elementos de criptografía" de esta asignatura.

El usuario A quiere firmar un mensaje m:

- A escoge un número $k \in \mathbb{Z}/p - \{0,1,p-1\}$ al azar, tal que $mcd(k,p-1) = 1$ y calcula α^k,
- calcula $h(m)$, donde $h(.)$ es una función hash,
- calcula $s \in \mathbb{Z}/(p-1)$ verificando,

$$h(m) = n_A \cdot \alpha^k + k \cdot s \pmod{(p-1)}.$$

- La firma de m es la pareja (α^k, s).

Un usuario que quiera verificar la firma del mensaje m deberá hacer:

- calcular el hash de m, $h(m)$,
- obtener del directorio público la clave pública de A: α^{n_A},
- validar la firma comprobando la siguiente igualdad:

$$\alpha^{h(m)} = (\alpha^{n_A})^{\alpha^k} \cdot (\alpha^k)^s \pmod{p}.$$

Versión clásica: DSA. Sea q un número primo de unos 160 bits y p otro número primo de unos 500 bits tal que $p = 1 \pmod{q}$. Sea α un generador del subgrupo cíclico de orden q de $(\mathbb{Z}/p)^*$. Para cada usuario U, su clave privada es n_U, un número escogido al azar, $0 < n_U < q$ y la clave pública es $\alpha_U = \alpha^{n_U}$.
El usuario A quiere firmar un mensaje m:

- A escoge un número $0 < k < q$ al azar y calcula $r = (\alpha^k \pmod{p}) \pmod{q}$
- calcula el hash de m, $0 < h(m) < q$,
- calcula s que verifica

$$h(m) + n_A \cdot r = k \cdot s \pmod{q},$$

- La firma de m es la pareja (r,s).

Un usuario que quiera verificar la firma del mensaje m deberá hacer:

- calcular el hash de m, $h(m)$,
- obtener del directorio público la clave pública de A: $\alpha_A = \alpha^{n_A}$,
- calcular $u_1 = s^{-1}h(m)$, $u_2 = s^{-1}r \pmod{q}$,
- validar la firma si, y solo si, $r = \alpha^{u_1} \cdot \alpha_A^{u_2} \pmod{p}$.

Versión con curvas elípticas: ECDSA. Sea E una curva elíptica sobre $\mathbb{Z}/p$, sea P un punto de la curva de orden primo n. Cada usuario U toma al azar un número $n_U \in [1, n-1]$ que será su clave privada, la clave pública de U será $P_U = n_U P$. El usuario A quiere firmar un mensaje m:

- A escoge un número $k \in [1, n-1]$ al azar,
- calcula $h(m)$, donde $h(.)$ es el algoritmo SHA-1 (*secure hash algorithm*),
- calcula $kP = (x_1, y_1)$ y $r = x_1 \pmod{n}$. Si $r = 0$, entonces volvemos a escoger otro k y repetimos el mismo proceso.
- calcula $k^{-1} \pmod{n}$
- calcula $s = k^{-1}\{h(m) + n_A r\} \pmod{n}$. Si $s = 0$, volvemos a escoger otro k y repetimos el mismo proceso.
- La firma de m es la pareja (r,s).

Un usuario que quiera verificar la firma del mensaje m deberá hacer:

- obtener del directorio público la clave pública de A: $P_A = n_A P$,
- verificar que $r,s \in [1,n-1]$,
- calcular $w = s^{-1} \pmod{n}$ y el hash de m: $h(m)$,
- calcular $u_1 = h(m) \cdot w \pmod{n}$ y $u_2 = r \cdot w \pmod{n}$,
- calcular $(x_0,y_0) = u_1 P + u_2 P_A$ y $v = x_0 \pmod{n}$,
- validar la firma si, y solo si, $v = r$.

Siguiendo las recomendaciones del NIST (National Institute of Standards and Technology, Digital Signature Standard, FIPS, PUB 186-2. 2000) se debería verificar que el orden de la curva elíptica sobre $\mathbb{F}_p$ sea de la forma $a \cdot q$ donde q es primo y a es un entero pequeño, de esta forma la curva no es vulnerable al ataque de Pohlig-Hellman. También es conveniente que la curva no sea supersingular ni anómala.

Dada una curva elíptica, deberemos calcular su cardinal y ver si satisface las condiciones anteriores. Aunque hay un algoritmo polinomial (Schoof 1985) para hacer este cálculo, su complejidad es del orden de $\log^8(p)$, que para valores demasiado grandes de p no es práctico.

5.5. Comparación de los sistemas de clave pública

5.5.1. Seguridad

Para llegar a un grado aceptable de seguridad el RSA y el DSA deberían usar claves de 1024 bits, mientras que para la ECC sería suficiente con 160.

A medida que la clave crece, aumenta la distancia entre la seguridad de cada propuesta. Por ejemplo, el ECC con 380 bits es mucho más seguro que el RSA o el DSA con 2000 bits (de hecho, para esta longitud de clave, el ECC es comparable al RSA de 7600 bits).

5.5.2. Eficiencia

Para comparar los niveles de eficiencia, deberemos tener en cuenta:

1) Costes computacionales, o sea la cantidad de computación requerida para cifrar y descifrar.

Cada uno de los tres sistemas, ECC, RSA, DSA, exige un gran esfuerzo computacional. En el RSA se puede usar un exponente público pequeño (aun cuando se deberían discutir los riesgos en los que se puede incurrir) para mejorar la rapidez en la verificación de firmas y en el cifrado, pero no en la generación

de la firma y el descifrado. Tanto en el DSA como en el ECC se pueden precalcular varias tablas para mejorar el rendimiento. También se pueden utilizar bases normales y óptimas para trabajar en cuerpos finitos de la forma $\mathbb{F}_{2^m}$.

Ver también

Las bases normales se estudian en el módulo "Cuerpos finitos".

Teniendo en cuenta el estado actual del arte en las implementaciones resulta que la ECC es un orden de magnitud más rápido que el RSA y, también, que el DSA.

2) Tamaño de la clave, o sea, la cantidad de bits necesarios para guardar la pareja de claves y los otros parámetros del sistema.

La tabla siguiente compara la medida de los parámetros del sistema y de las claves (pública y privada) para los diferentes sistemas.

Medida de los parámetros y claves

	Sistema de parámetros (bits)	Clave pública (bits)	Clave privada (bits)
RSA	2208	1088	2048
DSA	2208	1024	160
ECC	481	161	160

3) Anchura de banda, o sea, la cantidad de bits que se deben transmitir para comunicar un mensaje cifrado o una firma digital.

Los tres tipos de criptosistemas requieren la misma anchura de banda cuando se usan para cifrar o firmar mensajes largos. De todos modos cuando los mensajes no son largos se ha de observar con más atención (y, de hecho, este tipo de mensajes son los que usualmente son utilizados en la criptografía de clave pública).

Por poder hacer comparaciones, suponemos que queremos firmar un mensaje de 2000 bits o cifrar un mensaje de 100 bits. Las dos siguientes tablas comparan las longitudes de las firmas y de los mensajes cifrados, respectivamente.

Medida de las firmas en mensajes de 2000 bits

	Tamaño de la firma (bits)
RSA	1024
DSA	320
ECC	320

Medida de los mensajes de 100 bits, cifrados

	Mensaje cifrado (bits)
RSA	1024
ElGamal	2048
ECC	321

En resumen, el sistema ECC tiene una gran eficiencia y, en las implementaciones, esto significa rapidez, bajo consumo y reducción de la medida del código transmitido.

6. ECC estándares y aplicaciones

6.1. ECC estándares

Los progresos realizados en la criptografía con curvas elípticas desde su aparición en la década de los ochenta, hasta la actualidad, lo han transformado en algo más práctico que los esquemas propuestos inicialmente. Las mejoras introducidas han permitido la creación de implementaciones que ofrecen la posibilidad de comenzar a extender el uso de este tipo de criptografía.

Para promover la difusión de las mejores técnicas conocidas así como la interoperatibidad entre aplicaciones, han ido surgiendo esfuerzos por estandarizar la criptografía elíptica. Este esfuerzo ha sido liderado por la corporación Certicom*, haciendo las mayores aportaciones en materia de criptografía con curvas elípticas a los principales estándares de clave pública existentes.

* http://www.certicom.com

A continuación detallamos algunos de los estándares más importantes, así como otros más específicos, basados en aquellos.

6.1.1. Estándares principales

Los primeros frutos importantes del esfuerzo por estandarizar la criptografía elíptica se traducen en la adopción de sus principales algoritmos dentro de algunos de los estándares más importantes de criptografía de clave pública.

ANSI X9.62, X9.63

El American National Standards Institute's ha sido una de las organizaciones de más peso al adoptar las curvas elípticas dentro de sus estándares de criptografía. Los estándares de esta organización son referencia directa para servicios financieros y la industria en general.

La primera aparición de la criptografía con curvas elípticas fue en el estándar X9.62, con la adopción del esquema de firma digital ECDSA (*elliptic curve digital signature algorithm*) en enero de 1999 Algunas de las características iniciales que se adoptaron fueron una longitud mínima para las claves de 80 bits, y el uso de bases normales y polinomiales sobre F_{2^m}.

Posteriormente (2000) se amplió este estándar con el X9.63. El núcleo de este estándar está basado en el anterior, pero se adoptan algunos esquemas

para el intercambio de claves como la ECDH (*elliptic curve Diffie-Hellman*), ECMQV (*elliptic curve Menezes-Qu-Vastone*) o ECUM (*elliptic curve unified model Key Agreement*). Aparte de estos también se introduce el esquema de cifrado ECAES (Bellare-Rogaway).

IEEE P1363 y P1363A

La IEEE incluyó la criptografía con curvas elípticas en su estándar de criptografía de clave pública P1363 en febrero del 2000. El estándar es muy general y fue desarrollado principalmente por investigadores de Certicom (Vanstone y Menezes). En él se describen algoritmos típicos de criptografía de clave pública sobre curvas elípticas. Algunas de las características de este estándar son las siguientes:

- Soporta curvas elípticas sobre F_p y F_{2^m}
- Apoyo para esquemas de firmado ECDSA (*elliptic curve digital signature algorithm*) y ECNR (*Elliptic Curve Nyberg-Rueppel*) signature scheme.
- Apoyo para algoritmos de intercambio de claves ECDH (*elliptic curve Diffie-Hellman*) key agreement y ECMQV (*elliptic curve Menezes-Qu-Vastone*) key agreement.

Posteriormente, en un draft que complementa este estándar llamado P1363A (*standard specifications for public key cryptography: additional techniques*) se introduce la posibilidad de utilizar el esquema de cifrado ECIES. También, en el draft P1363.3, se introducen los esquemas basados en la identidad usando *pairings*.

Ver también

Los *pairings* se estudian en el módulo "*Pairings* y sus aplicaciones" .

ISO 14888, 9796-4, 15946

La International Organization for Standarizatcion (ISO) fue otra de las principales organizaciones para la estandarización que apuesta por añadir la criptografía con curvas elípticas en sus estándares criptograficos. La descripción principal del uso de estas técnicas se hace en el estándar 15946 (*cryptographic techniques based on elliptic curves*). Mientras que la primera parte del estándar hace una descripción general de los métodos basados en curvas elípticas, la segunda y tercera parte ya introducen el uso del esquema ECDSA para las firmas digitales, y algunos algoritmos de intercambio de claves (ECDH, ECMQV).

Esta no es la única repercusión de la criptografía de curva elíptica sobre los estándares de la ISO. También podemos encontrar modificaciones a otros estándares de firma digital, concretamente al 14888 (*digital signature with appendix part 3: certificate-based mechanisms*) y al 9796-4 (*digital signature with message recovery, discrete logarithm-based mechanisms*).

FIPS 186-2

Uno de los primeros éxitos de la estandarización de los algoritmos criptográficos basados en curvas elípticas fue la adopción de esta tecnología por el National Institute of Standards and Technology (NIST). El estándar FIPS (*federal information processing standard*) 186-2 fue extendido en febrero del 2000 ampliando el apartado dedicado al DSS (*digital signature standard*) para incluir la versión del ECDSA especificada en el estándar de ANSI X9.62.

Este estándar es un punto de referencia para la comercialización de productos que contengan criptografía de curva elíptica, puesto que desde su creación, las agencias gubernamentales americanas pueden comprar productos basados en este tipo de criptografía sin pedir permisos especiales. El NIST ha incluido también especificaciones para algoritmos de criptografía de curva elíptica en su documento MISPC (minimum interoperability specification).

SEC 1, SEC 2, SEC 3 y SEC 4

El SECG (*standards for efficient cryptography group*) fue creado por la empresa Certicom, para promover estándares de curva elíptica así como la difusión de los mejores métodos para implementar este tipo de criptografía. Su principal objetivo es crear un estándar, basado en los principales que existen, pero haciendo restricciones sobre los parámetros que estos exigen sobre cada uno de los esquemas de firmado, cifrado o intercambio de claves que usan. El objetivo de estas restricciones es hacer posible la interoperatividad de las aplicaciones basadas en este estándar, con las basadas en cualquiera de los otros estándares principales.

Los frutos de esta organización quedan reflejados en dos estándares. El primero de ellos, recogido en el 2009 en el documento SET 1 (*elliptic curve cryptography*) hace una descripción de los esquemas permitidos (ECDSA, ECDH, ECMQV y ECIES). Además, se describen todas las primitivas criptográficas que se usan en estos esquemas y la notación ASN1 (*abstract syntax notation one*) para representar las estructuras necesarias (claves, certificados, contenidos cifrados, etc) que se utilizan.

El esquema de cifrado ECIES tiene una larga historia en su nomenclatura y ha ido sufriendo a la vez pequeñas modificaciones. Lo podemos encontrar en la literatura como ECAES (*elliptic curve augmented encryption scheme*) o simplemente como ECES (*elliptic curve encryption scheme*). La versión definida en el documento SET 1 es la más extensa y actualizada. Este esquema se basa en utilizar criptografía simétrica para cifrar el mensaje deseado a partir de una clave generada en el proceso de inicialización del método. Una vez se ha cifrado el mensaje se transmite el contenido cifrado y se envia la clave generada utilizando el esquema ECDH.

El segundo documento, SET 2 (*recommended elliptic curve domain parameters*), hace una propuesta sobre los parámetros a utilizar sobre los esquemas definidos en SET 1, así como en otros estándares como el ANSI X9.63 o el IEEE P1363. El uso de estas recomendaciones aumentan en gran medida la interoperatividad de las aplicaciones que los usen.

SET 3 trata sobre esquemas de firma basados en curvas elípticas con reconstrucción parcial del mensaje (ECPVS y ECAOS).

SET 4 incorpora el esquema de certificación de Qu-Vanstone.

RSA

Laboratorios RSA publica dos documentos PKCS11 y PKCS13 para la estandarización del uso de las curvas elípticas (generación de claves, firmas digitales, cifrado con clave pública, etc.). El objetivo de ambos documentos era crear un nuevo estándar criptográfico al estilo de otras PKCS (*public key cryptography standard*) desarrollados por los Laboratorios RSA. La línea de la propuesta inicial realizada en enero de 1998 tenía los mismos objetivos que los del grupo SECG creado por Certicom. Hasta hoy no se ha adelantado más allá de la propuesta inicial de 1998 y aparentemente el desarrollo de este estándar está congelado.

NSA

NSA (National Security Agency) de USA anuncia, en el 2005, la *suite B Cryptography* la cual incluye la criptografía basada en curvas elípticas en la seguridad de los sistemas de datos USA. Esta suite B incorpora la colección de algoritmos: SHA256 y SHA384 (FIPS 180-3); AES128 y AES256 (FIPS 197); ECDH (ANSI X9.63) y ECDSA (ANSI X9.62, SET 1).

Posteriormente se ha propuesto la suite E para sistemas restringidos (con códigos de tamaño pequeño y requerimientos particulares de hardware, potencia y ancho de banda).

6.1.2. Estándares de aplicación

Los estándares descritos en el subapartado anterior han sido los principales promotores del esfuerzo por estandarizar la criptografía con curvas elípticas. Aun así existen otros más específicos que se basan en el trabajo aportado por los anteriores. La mayoría de estas iniciativas suelen definir protocolos criptográficos basados en la criptografía de clave pública, pero están expresados de forma que el algoritmo de cifrado a utilizar pueda ser cambiado siempre que cumpla ciertas propiedades. Muchos de estos trabajos han incluido los esquemas de criptografía con curvas elípticas propuestos en el apartado ante-

rior como nuevas soluciones para optimizar estos protocolos, sobre todo en entornos donde el tamaño de la clave no puede ser demasiado grande. A continuación enumeraremos algunos.

IETF (IPSec, TLS, S/MIME, SSH, DNSSEC)

El Working Group de la IETF (Internet Engineering Task Force) ha adoptado también la criptografía con curvas elípticas en sus estándares. Las especificaciones más importantes hacen referencia a los protocolos IPSec, TLS, S/MIME, SSH, DNSSEC.

El protocolo de intercambio de claves OAKLEY (RFC 2412), basado en el algoritmo de Diffie-Hellman, ha sido modificado para soportar la variante ECDH sobre curvas elípticas. Las curvas por defecto que se utilizan en este protocolo están definidas sobre $F_{2^{155}}$ y $F_{2^{185}}$.

WAP WTLS

WTLS (*wireless transporte security layer*) es la capa de seguridad para WAP (*wireless application protocol*). Esta especificación se ha convertido en el estándar *de facto* para proveer seguridad, integridad y autenticidad para aplicaciones de teléfonos móviles y otros dispositivos pequeños. Los esquemas de firma (DSA) y de intercambio de claves (DH) descritos en esta especificación han sido ampliados para soportar ECDSA para las firmas y ECDH para el intercambio de claves. Los parámetros utilizados para estos dos algoritmos siguen los del estándar del IEEE P1363 descrito en el apartado anterior. Esta especificación, junto con el estándar FIPS del NIST demuestran la voluntad por parte de la industria de adoptar este tipo de criptografía

ATM

El Security specification draft para redes ATM (*asyncronous transfer Mode*) es el documento que especifica los mecanismos de seguridad que pueden ser aplicados sobre este tipo de redes. Entre estos mecanismos hay sistemas para garantizar la confidencialidad, la autenticidad, la integridad o el control de acceso. Algunos de los mecanismos se basan en criptografía de clave pública y, en ellos, se ha incluido la criptografía con curvas elípticas como posible candidata a utilizar.

6.2. Aplicaciones de la ECC. Tarjetas inteligentes

Actualmente donde más se utilizan las nuevas tecnologías basadas en curvas elípticas es en:

1) Aplicaciones que requieren operaciones de clave pública de tipo intensivo. Por ejemplo, el comercio electrónico basado en Internet, etc.

2) Aplicaciones que requieren la utilización de canales con restricciones. Por ejemplo, redes *wireless*, etc.

3) Aplicaciones que requieren el uso de tarjetas inteligentes.

Todas estas aplicaciones comparten un escenario implicando unas restricciones más severas en el uso del procesador. Comentaremos, básicamente, las aplicaciones basadas en tarjetas inteligentes, aun cuando son fácilmente extrapolables a las otras aplicaciones mencionadas.

En el 2001, Europay, Mastercard y VISA dan a conocer un informe técnico sobre curvas elípticas, el EMV40. En él se introduce el uso de curvas elípticas como sustituto del RSA para la autentificación y el cifrado.

La implementación de aplicaciones seguras para tarjetas inteligentes presenta una serie de inconvenientes debido a las restricciones existentes en estos dispositivos. Estas limitaciones son debidas principalmente a sus disponibilidades de memoria, de ancho de banda y de potencia de cálculo.

Las tarjetas inteligentes son pequeños dispositivos portátiles, que ofrecen al usuario integridad de la información almacenada en su interior y capacidad de procesamiento. Esta capacidad de procesamiento hace que las tarjetas inteligentes sean de gran utilidad para la implementación de un gran número de aplicaciones relacionadas con el comercio electrónico, la identificación de personas...

Para la mayor parte de estas aplicaciones, es necesario el uso de servicios criptográficos que no encarezcan el producto final. Tales servicios criptográficos son necesarios por varias razones. En primer lugar, la tarjeta requiere una serie de características de seguridad que permitan la protección de la información sensible almacenada a su interior. En segundo lugar, deben proporcionar un entorno de procesamiento.

La generación de una clave pública y privada en el interior de una tarjeta inteligente, así como la protección de la clave privada en su interior, es crítica. Para poder proporcionar servicios criptográficos, la clave almacenada en la tarjeta nunca ha de ser revelada. Por este motivo, la propia tarjeta deberá autoprotegerse haciendo uso de sus servicios criptográficos.

6.2.1. Restricciones de las tarjetas inteligentes

Implementar criptografía de clave pública en aplicaciones basadas en tarjetas inteligentes representa un gran reto, en parte por las restricciones de imple-

mentación que estos dispositivos requieren (memoria muy reducida y capacidad de cálculo muy limitada).

La mayor parte de tarjetas inteligentes disponibles hoy en día en el mercado disponen de una memoria RAM de alrededor de 1.024 bytes, de unos 16 kilobytes de memoria EPROM y de unos 24 kilobytes de memoria ROM. Su capacidad de procesamiento es también muy reducida. Normalmente, tienen CPU de 32 bits a una frecuencia de unos 5 megaherzios.

Por último, la velocidad de transmisión de estas tarjetas es también muy limitada. Para conseguir velocidades de aplicación aceptables, la información transmitida por la tarjeta habría de ser la mínima necesaria.

6.2.2. Ventajas de la ECC

Las ventajas de la utilización de la ECC para la construcción de los servicios criptográficos necesarios para tarjetas inteligentes son básicamente los siguientes:

- **Mínimos requerimientos de memoria y de tasa de transmisión**. La utilización de la ECC permite reducir el tamaño de las claves y los certificados. Esto se traduce en una reducción de la memoria necesaria por parte de la tarjeta inteligentes. Por otro parte, también permite una reducción de los datos a transmitir entre tarjeta y aplicación. Por este motivo, la tasa de transmisión necesaria se reduce considerablemente.

- **Escalabilidad**. Las aplicaciones basadas en tarjetas inteligentes requieren un nivel de seguridad bastante elevado (con lo cual, la longitud de las claves aumenta considerablemente). La criptografía de curvas elípticas puede proporcionar el nivel de seguridad parecido destinando menos recursos para conseguirlo. Esto significa que con el uso de la ECC, las tarjetas inteligentes pueden proporcionar un nivel de seguridad muy elevado sin necesidad de incrementar su coste de producción.

- **No requiere coprocesador**. La mayor parte de dispositivos que ofrecen criptografía de clave pública requieren un componente *hardware* conocido como *cripto coprocesador* para apoyar los intensos cálculos que el sistema debe realizar. Este componente *hardware* adicional no solo reduce el espacio disponible en la tarjeta sino que incrementará su coste de un 20 a un 30 por ciento.

  La naturaleza de los cálculos necesarios para implementar la ECC, con unos tiempos de procesamiento bastante reducidos, no requieren este coprocesador. Por lo tanto, los algoritmos necesarios pueden ser implementados en la ROM de la tarjeta, sin necesidad de *hardware adicional*.

- **Generación interna de claves**. La clave privada asociada a una clave pública debe permanecer almacenada de forma secreta. Además, para garantizar el no repudio, la clave privada habría de ser completamente inaccesible por terceras partes.

  Con la utilización de otros algoritmos, la introducción de claves dentro de la tarjeta se debe hacer de forma personalizada en un entorno seguro. Debido a la complejidad de los cálculos necesarios, la generación de claves dentro de la propia tarjeta es ineficiente y generalmente impracticable.

  Utilizando ECC se consigue que el tiempo necesario para generar una pareja de claves sea tan reducido que incluso dispositivos de características de cálculo tan modestas como las tarjetas inteligentes pueden generar tal pareja. Esto significa que el proceso de personalización puede ser evitado en aquellas aplicaciones donde la no repudiación sea realmente importante.

6.2.3. Conclusiones

Las tarjetas inteligentes tienen unas restricciones de implementación muy rígidas debido a sus limitaciones de cálculo, parámetros de almacenamiento y tasas de transferencia. Como resultado de estas restricciones, implementar un sistema de clave pública con tarjetas inteligentes requiere el uso de tarjetas de más alto nivel, con mayor capacidad de almacenamiento y con coprocesador criptográfico.

La reducción del tamaño de las clave y los certificados que permite la ECC para construir sistemas de clave pública, ofrece unas ventajas incuestionables para la implementación de aplicaciones seguras en tarjetas inteligentes.

Ejercicios de autoevaluación

1. Dada la cónica $x^2 + xy + y^2$ sobre $\mathbb{F}_2$, calcular sus puntos racionales.

2. Dada la cónica $x^2 + xy + y^2$ sobre $\mathbb{F}_8$, calcular sus puntos racionales.

3. Dada la curva $y^2 = x^3 + 3x + 2$ sobre $\mathbb{F}_{23}$ y los dos puntos de la misma $P = (16,11), Q = (8,20)$, calcular $P + Q$, $2P$, $4P$.

4. Dada la curva $y^2 + xy = x^3 + \alpha x^2 + 1$ sobre $\mathbb{F}_4$.
a) Comprobar que no tiene puntos singulares.

b) Dar un punto P de la curva. Por ejemplo, fijar un valor de x (por ejemplo $x = 0$) y resolver la ecuación cuadrática resultante para ver si encontramos un valor válido para y (en nuestro ejemplo, $y^2 = 1$).

5. Dada la curva $y^2 + xy = x^3 + \alpha x^2 + \alpha$ sobre $\mathbb{F}_4$.
a) Comprobar que no tiene puntos singulares.

b) Dar un punto P de la curva.

c) Calcular el orden del punto P. Es decir, calcular el mínimo a, tal que $aP = 0$, donde 0 es el punto del infinito.

d) ¿Podemos saber cuántos puntos tiene la curva, utilizando los teoremas conocidos?

6. Implementar usando SAGE el sistema criptográfico ElGamal sobre curvas elípticas. Usar un número primo de más de 10 cifras y cifrar el texto

'Cifrar con ElGamal elíptico hace difícil el descifrado.'

Mostrar el texto en claro y el texto cifrado.

El método de codificación será una variante, debida a *Menezes y Vanstone* conocida como MV-ElGamal. Un punto P de orden grande y la curva E son información pública. La clave privada es un entero n_U más pequeño que el orden de P y la clave pública es $P_U = n_U P$. El mensaje m lo dividiremos en dos bloques módulo p, o sea $(m_1,m_2) \in \mathbb{F}_p \times \mathbb{F}_p$. La función de cifrado viene dada por

$$E_U(m) = (rP, c_1, c_2) \in E \times P \times P$$

donde r es un número aleatorio, $(x,y) = rP_U$ y $c_1 = xm_1 \pmod p$, $c_2 = ym_2 \pmod p$. Supondremos que $x,y \neq 0$, de lo contrario buscaremos otro valor de r.
La correspondiente función de descifrado es:

$$D_U(C,c_1,c_2) = (c_1 x^{-1}, c_2 y^{-1}), \text{ donde } (x,y) = n_U C.$$

Soluciones

1. Los únicos puntos posible de la curva son (0,0),(0,1),(1,0),(1,1). Solo hace falta probar qué valores satisfacen la ecuación y ver que los puntos racionales son (0,1),(1,0),(1,1).

2. El problema, ahora, no es tan sencillo como el anterior. Si en el cuerpo hay muchos elementos no podemos irlos probando todos de uno en uno. Podemos hacer como en el ejemplo 1.5.

Supongamos que el cuerpo finito lo hemos construido utilizando el polinomio primitivo $x^3 + x + 1$. Ya sabemos por el ejercicio anterior que (0,1) es un punto de la curva. El haz de rectas que pasan por este punto es $Ax+By+C = 0$. Dando valores en el punto (0,1) obtenemos $B+C = 0$, o sea $B = C \neq 0$ (si B y C fueran cero la recta sería $x = 0$ y no pasaría por otros puntos que ya conocemos (los (1,0) y (1,1)). Si cortamos esta recta con la curva inicial obtenemos los puntos que buscamos, o sea, las soluciones del sistema de ecuaciones:

$$\begin{cases} Dx + y + 1 &= 0 \\ x^2 + xy + y^2 + 1 &= 0 \end{cases}$$

Resolviendo este sistema obtenemos: $x = \frac{1}{D^2+D+1}$; $y = \frac{D^2+1}{D^2+D+1}$ y, al ir dando valores a $D \in \mathbb{F}_8$ obtenemos las ocho soluciones (1,0); (1,1); (α^2,α); (α,α^2); (α^4,α); (α,α^4); (α^2,α^4); (α^4,α^2) que, junto con la solución inicial (0,1), da los nueve puntos racionales que buscábamos.

3. $2P = (20,14)$, $4P = (19,15)$, $P + Q = (15,8)$.

4.

a) Efectivamente, el único punto singular sería (0,0) que no pertenece a la curva.

b) Fijamos $x = \alpha$. Entonces obtenemos $y^2 + \alpha y + 1 = 0$ que no tiene solución. Esto quiere decir que no hay ningún punto de la curva del tipo $P = (\alpha,?)$.

Si vamos buscando otros posibles puntos, llegaremos a la conclusión de que solo hay soluciones cuando $x = 0$, valor que tiene dos soluciones. En el plano proyectivo escribiríamos las soluciones como (0,1,0) y (0,1,1).

5.

a) Efectivamente, el único punto singular sería (0,0) el cual no pertenece a la curva.

b) Fijamos $x = \alpha^2$ y obtenemos $y^2 + \alpha^2 y = 0$, que proporciona dos soluciones $(\alpha^2,0)$ y (α^2,α^2).

c) Empezamos con el punto $P = (\alpha^2,0)$ y calculamos $2P = (\alpha^2,\alpha^2)$, $3P = 0$. El orden del punto P es 3 .

d) Según el teorema de Hasse el número de puntos de la curva es $1 \leq N \leq 9$. Por el teorema 3.1, como el orden del punto P es 3, $3|N$. O sea que N puede ser 3, 6 o 9. Pero conocemos más puntos aparte de P, $2P$, $3P$ (por ejemplo (α^2,α^2)). Es decir que $N \in \{6,9\}$. Para terminar de precisar el valor de N necesitariamos calcular algún otro punto.

6. Empezaremos por buscar un número primo de más de 10 dígitos y definir una curva elíptica sobre el cuerpo finito $\mathbb{F}_p$. También escogeremos un punto P (fácil de calcular) sobre esta curva.

```
sage: p= nextprime(10^10+10^8+10^5+1)
sage: E = EllipticCurve(GF(p),[1975,4])
sage: P = E([0,2])
sage: print p
sage: print(E.cardinality())
sage: print P.additiveorder()
10100100007
10100137808
1262517226
```

La curva es $E : y^2 = x^3 + 1975x + 4$ y el orden del punto P es lo suficientemente grande.

Las funciones de cifrado y descifrado las podríamos definir cómo:

```
def cipher(PU ,m1 ,m2):
    x=0,y=0
    while ((x==0) oro (y==0)):
        r = floor(p*random())
        x = (r* Kpub)[0]
        y = (r* Kpub)[1]
    return r*P, m1*x, m2*y

def uncipher(NU ,ciph):
    x = (NU*ciph[0])[0]
    y = (NU*ciph[0])[1]
    return ciph[1]*x^(-1), ciph[2]*y^(-1)
```

Para ver su funcionamiento tomemos por ejemplo, como clave privada $n_U = 10000$:

```
sage: privatekey = 10000
sage: publickey = privatekey*P
sage: cipher(publickey,999,1999)
((5871087149 : 8478284639 : 1), 571107865, 7072444218)

sage: uncipher(privatekey,cipher(publickey,999,1999))
(999,1999)
```

Podemos convertir un texto de caracteres en enteros:

```
def codificar(texto):
    valornumerico = 0
    for c in texto:
        valornumerico = 256*valornumerico + ord(c)
    return valornumerico
```

Y, a la inversa, para convertir un número en un texto alfabético:

```
def descodificar(numero):
    numero = Integer(numero)
    texto = ''
    for y  in numero.digits(256):
        texto = chr(y) + texto
    return texto
```

Finalmente, como estamos codificando/descodificando utilizando el código ASCII, para la tabla que nos piden, debemos hacer bloques en el texto que no superen $log_{256}p$ caracteres.

```
texto = 'Cifrar con ElGamal eliptico hace dificil el descifrado'
L=len(texto)
k = floor(log(p,256))
NU = 10000
for y  in range(0,L,2*k):
    t1 = texto[y:y+k]
    m1 = codificar(t1)
    t2 = texto[y+k:y+2*k]
    m2 = codificar(t2)
    textciph = cipher(NU*P,m1,m2)
    d1 = descodificar(uncipher(NU,textciph)[0])
    d2 = descodificar(uncipher(NU,textciph)[1])
    print d1+d2 , m1 ,m2, textciph, t1+t2
```

Este es el resultado. La primera columna es el texto a cifrar. La segunda y tercera columnas el texto codificado (m_1,m_2). La cuarta columna los valores cifrados. Y la quinta columna el resultado de descifrar.

Cifrar c	1130980978	1634869347	((3670548167 : 8041465163 : 1),6186249921, 6388942806)	Cifrar c
on ElGam	1869488197	1816617325	((9491602649 : 7910460644 : 1),8350385062, 7689324084)	on ElGam
al elipt	1634476133	1818849396	((1257214778 : 421866546 : 1), 524846611,5065905920)	al elipt
ico hace	1768124192	1751212901	((2068088083 : 6284606394 : 1),4999183562, 850702920)	ico hace
dificil	543451494	1768122732	((6466692567 : 5666762513 : 1),3325032242, 7746857338)	dificil
el desc	543517728	1684370275	((5844556383 : 4258913833 : 1),6783579288, 8248646216)	el desc
ifrado	1768321633	25711	((3083653805 : 3609902653 : 1), 4465267786,7374582335)	ifrado

Bibliografía

Blake, I.; Seroussi, G.; Smart, N. (2000). "Elliptic Curves in Cryptography". *London Mathematical Society Lecture Note Series* (núm. 265). Cambridge: Cambridge U. Press.

Fulton, W. (1969). *Algebraic Curves. An Introduction to Algebraic Geometry*. Nueva York: Benjamin Inc. (Versión en castellano: *Curvas algebraicas* (1972). Barcelona: Ed. Reverte.)

Hankerson, D.; Menezes, A.; Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Nueva York: Springer-Verlag.

Koblitz, N. (2004). "Algebraic Aspects of Cryptography". *Algorithms and computations in Mathematics* (vol. 3). Berlín, Heidelberg, Nueva York: Springer-Verlag.

Menezes, A. (1993). *Elliptic Curve Public Key Cryptosystems*. Massachusetts: Kluwer Academic Publishers, Norwell.

Silverman, J. H. (1986). "The Arithmetic of Elliptic Curves". *Graduate Texts in Mathematics* (núm. 106). Nueva York: Springer-Verlag.

Washington, L. C. (2008). "Elliptic Curves: Number Theory and Cryptography". *Discrete Mathematics and its Applications*. Nueva York: Chapman & Hall/CRC.