El algoritmo de Schoof para curvas elípticas

Virginia Villacampa Casalod

Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Directores del trabajo: Carlos de Vera Piquero y
Miguel Ángel Marco Buzunáriz
12 de junio de 2024

Abstract

Elliptic curves are algebraic structures with a wide range of applications in number theory and cryptography. These curves have gained significant importance over the last few years, specially during the 1980s, when they began to be used in cryptographic applications, leading to the development of elliptic curve techniques for factorization, among others. In recent decades, elliptic curve cryptography has become widely established in public key cryptography algorithms and it has been integrated into security products since the late 1990s.

The security of this type of cryptography relies on the difficulty of solving the discrete logarithm problem within the group structure of the points on elliptic curves defined over finite fields.

However, some algorithms can reduce the discrete logarithm problem on elliptic curves to groups where the solution to this problem is easier to find.

To ensure the cryptographic security of a curve, it is crucial to know the order of the underlying group that comprises the set of points of an elliptic curve over its defining field.

Schoof's algorithm, which employs Hasse's Theorem, the Frobenius endomorphism, and the Chinese Remainder Theorem, is currently the most efficient method for calculating this order.

The goal of the present project is to develop the theory of Schoof's algorithm, providing a comprehensive overview of the mathematical concepts and practical applications associated with elliptic curves and their use in cryptographic systems, with examples of how the theory can be used.

The first chapter of this work introduces basic concepts necessary to understand elliptic curves. Both affine space and the projective plane are defined to illustrate the notion of an elliptic curve from different points of view, including their definition via the Weierstrass equation. It will be assumed that an elliptic curve is given in its Weierstrass equation when there is no specification about it. A special point belonging to the curve appears during this process. It will be the neutral point for the operation constructed over elliptic curves.

The second chapter covers endomorphisms and key results about them, such as the reduction of the general expression to a more practical way of presenting the rational functions that define the endomorphism. Some easy and short examples are added to showcase the ideas explained in this chapter. The torsion subgroup is also included here. The next topic is endomorphism rings. A theorem is stated without proof to facilitate the discussion in the next section.

The focus then shifts to Frobenius endomorphism. After proving some of its fundamental properties, everything is ready to show Hasse's Theorem. It is important because it will provide a prediction for the order of the group formed by the points on the elliptic curve. Furthermore, the Frobenius endomorphism satisfies an important equation called the characteristic equation. This equation is used during Schoof's algorithm, and both its formula and proof are provided at the end of this section.

A brief description of division polynomials is included to express the addition of a point to itself using rational functions. These functions satisfy recursive relations between them.

The third chapter is the core of the project: the detailed presentation of Schoof's algorithm. This includes the computation of the Frobenius trace modulo small primes and the combination of these results using the Chinese Remainder Theorem to determine the exact number of points on the elliptic curve. This chapter finishes with an example of the algorithm applied to an elementary curve. All computations needed to solve each step have been done in Sage.

The fourth chapter is the last one of the work. It highlights the applications of elliptic curves in cryptography, emphasizing their importance in creating secure communication systems. The work de-

monstrates not only the theoretical underpinnings of the algorithm but also its practical implications in modern cryptographic practices. The Elliptic Curves Discrete Logarithm Problem is presented at the beginning of the chapter. Some public key schemes rely on the hardship of solving this problem.

If the order of the curve is not taken into account when choosing the cryptographic system based on it, it is possible to attack these curves because there are orders which make them insecure. Three examples of these attacks are explained at the end of this work.

The greatest part of the project has been done with the help of the texts from [5], [6] and [9], in addition to those explicitly cited in the text.

Índice general

Capítulo 1

Preliminares

En este primer capítulo, se darán las definiciones básicas para poder desarrollar el resto del trabajo. Las curvas elípticas son una familia de curvas algebraicas. Existen varias definiciones alternativas, pero equivalentes, de lo que es una curva elíptica. Según el contexto, se puede utilizar una u otra. En este caso, la primera que se dará requiere algunos conceptos previos.

1.1. Ecuación de Weierstrass

Definición. Sea $\mathbb{F}$ un cuerpo. El *espacio afín* tridimensional sobre $\mathbb{F}$, habitualmente denotado por $\mathbb{A}^3_{\mathbb{F}}$, es el conjunto de puntos tales que

$$\mathbb{A}^3_{\mathbb{F}} = \{(x,y,z) \mid x,y,z \in \mathbb{F}\}$$

Se define $\sim$ como la relación de equivalencia dada por

$$(x,y,z) \sim (\lambda x, \lambda y, \lambda z), \quad \forall \lambda \in (\mathbb{F} \setminus \{0\})$$

Notar que la relación de equivalencia se toma fuera del origen. La clase de equivalencia de (x,y,z) se escribe como $(x:y:z)$.

Definición. El *plano proyectivo* es el cociente entre el espacio afín y la relación de equivalencia $\sim$

$$\mathbb{P}^2_{\mathbb{F}} = (\mathbb{A}^3_{\mathbb{F}} \setminus \{(0,0,0)\})/\sim$$

Llegados a este punto, se puede dar una primera pincelada acerca de lo que es una curva elíptica:

Una curva elíptica es una curva lisa $E \subset \mathbb{P}^2_{\mathbb{F}}$ de grado 3.

Esta afirmación se puede visualizar de manera más concisa si se escribe una curva elíptica como el conjunto de puntos que satisfacen la ecuación general de una cúbica en $\mathbb{P}^2_{\mathbb{F}}$

$$Ax^3 + Bx^2y + Cx^2z + Dxyz + Ey^2z + Fxy^2 + Gy^3 + Hz^3 + Ixz^2 + Jyz^2 = 0$$

Si $char(\mathbb{F}) \neq 2,3$, se puede realizar un cambio de variables, y deshomogeneizando (es decir, evaluando $z = 1$), queda que una curva elíptica E se puede definir mediante una ecuación más sencilla.

Definición. Sea $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \neq 2,3$. Una *curva elíptica* E definida sobre $\mathbb{F}$ es una curva proyectiva cuya ecuación afín asociada es de la forma

$$y^2 = x^3 + Ax + B, \quad A,B \in \mathbb{F}, \quad 4A^3 + 27B^2 \neq 0$$

El algoritmo de Schoof se puede utilizar también en características 2 y 3 pero las ecuaciones obtenidas para ello son distintas y no serán tenidas en cuenta en este trabajo.

Se denotará con $E(\mathbb{F})$ al conjunto de puntos de la curva elíptica. Este conjunto está formado por los puntos $(x,y) \in \mathbb{F} \times \mathbb{F}$ que son solución a la ecuación mencionada E junto con **un punto extra**, denotado como $\mathcal{O}$ y cuya procedencia será detallada más adelante. Esta ecuación se conoce como *la ecuación simplificada de Weierstrass* para una curva elíptica E.

La condición de que el discriminante no sea nulo en el cuerpo, $4A^3+27B^2\neq 0$, se exige para que el polinomio x^3+Ax+B no tenga raíces múltiples. En este caso, se dice que la curva es *lisa* o *no singular*.

Una vez fijada la ecuación, se pueden definir tantos conjuntos de puntos que la cumplan como extensiones tenga $\mathbb{F}$. La misma definición de curva elíptica se puede usar para cada una de estas extensiones del cuerpo. Cuando pueda haber confusión sobre el cuerpo en el que están las coordenadas de un punto (x,y), se dice que el punto es **$\mathbb{F}$-racional** si sus coordenadas están en $\mathbb{F}$.

El punto extra, $\mathscr{O}$, procede del proceso de homogeneización de la ecuación simplificada de Weierstrass. Esto se realiza estableciendo que $x=\dfrac{X}{Z},\ y=\dfrac{Y}{Z}$, así se obtiene la ecuación en el plano proyectivo correspondiente. Se hace una distinción: las minúsculas x e y son las coordenadas en el plano afín y las mayúsculas X,Y y Z son las coordenadas en el plano proyectivo. Por lo tanto, la ecuación de Weierstrass homogeneizada es la siguiente

$$Y^2Z=X^3+AXZ^2+BZ^3$$

- Si $Z\neq 0$, entonces $(X:Y:Z)=\left(\dfrac{X}{Z}:\dfrac{Y}{Z}:1\right)=(x:y:1)$, recuperando la ecuación afín original $y^2=x^3+Ax+B$. Estos son los puntos 'finitos' del plano proyectivo.
- Si $Z=0$, se puede pensar que esta recta es la del infinito y por tanto los puntos de la forma $(X:Y:0)$ se llaman puntos del infinito. Sustituyendo $Z=0$ en la ecuación proyectiva, se obtiene que $X^3=0$. Por tanto, $X=0$ y entonces $Y\neq 0$ porque en la definición de la relación de equivalencia se excluye la posibilidad de que las tres coordenadas del plano proyectivo sean cero. Por lo que queda $(0:Y:0)$. La ecuación proyectiva correspondiente a la ecuación de Weierstrass posee **solo una solución** en la recta del infinito $Z=0$, que al reescalar se convierte en el punto $(0:1:0)$. Esta solución es el **punto extra** que se añade y se escribe como $\mathscr{O}=(0:1:0)$. Todo ello es coherente con el teorema de Bézout, que dice que la intersección entre una recta y una cúbica se debe producir en tres puntos, contando con la multiplicidad de cada uno de ellos.

Este punto es muy importante ya que se tomará como elemento neutro a la hora de construir una operación $\oplus$ sobre $E(\mathbb{F})$ que proporcionará una estructura de grupo a las curvas elípticas. A continuación, se describe el proceso que define esta operación.

1. Se toman dos puntos $P_1=(x_1,y_1)$ y $P_2=(x_2,y_2)$ en una curva elíptica $E(\mathbb{F})$ dada por la ecuación simplificada de Weierstrass $y^2=x^3+Ax+B$.
2. Se traza la recta L que pasa por P_1 y P_2. Esta recta corta a E en un tercer punto, que se considera distinto de $\mathscr{O}$, denotado por $P_3'=(x_3',y_3')$.
3. Se une este tercer punto P_3' con el punto del infinito $\mathscr{O}$ a través de la recta L' con la que se obtiene $P_3=(x_3,y_3)$. Notar que, si $P_3'\neq\mathscr{O}$, la recta L' es la vertical que pasa por P_3'. Debido a la simetría de la ecuación, se tiene entonces que $P_3=(x_3',-y_3')$. Por tanto, este último paso es equivalente a reflejar el punto P_3' respecto del eje x.
4. Se define precisamente el resultado de esta nueva operación como $P_1\oplus P_2=P_3$.

En esta explicación, se ha omitido en varias ocasiones el caso en el que dos puntos de la curva elíptica sean el mismo, puesto que para definir una recta geométricamente se necesita que estos sean distintos. Cada vez que aparezca este problema de considerar la recta que pase por dos puntos y que estos dos sean iguales, la solución será tomar la recta tangente a la curva en dicho punto, lo que es equivalente a pensar que la tangente corta dos veces a la curva en el mismo punto (en este caso, se dice que la curva tiene multiplicidad de intersección 2 con la recta en el punto). La recta tangente a un punto será entendida como la única recta que pasa por un punto con multiplicidad mayor estrictamente que uno.

En el segundo paso, se ha supuesto que $P_3'\neq\mathscr{O}$. Si por el contrario se tiene que $P_3'=\mathscr{O}$, la recta L' corta a la curva en $\mathscr{O}$ con multiplicidad al menos 2 y por definición, esta debe ser la recta tangente. Por otro lado, ya se ha visto que $Z=0$ corta a la curva en $\mathscr{O}$ con multiplicidad 3. La unicidad de la recta tangente demuestra que estas dos son en realidad la misma recta, y que $Z=0$ es la única tangente a la curva en $\mathscr{O}$.

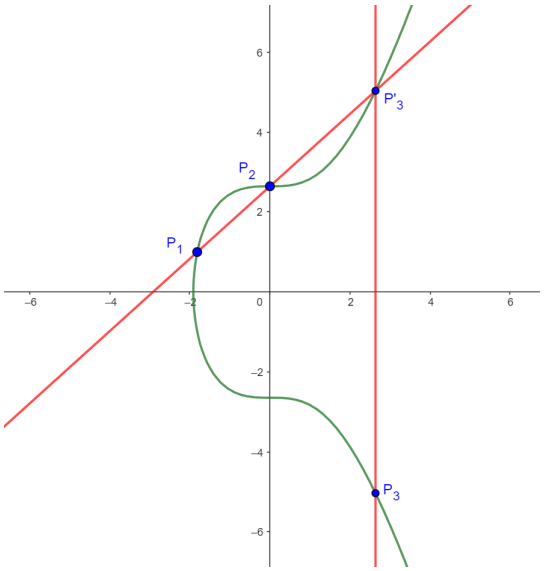

Figura 1.1: Ilustración geométrica de la construcción $\oplus$ (con la curva elíptica $y^2 = x^3 + 7$ sobre $\mathbb{R}$)

1.2. Estructura de grupo de las curvas elípticas

Si se utiliza la suma habitual $+$, entendida coordenada a coordenada, con dos puntos, el resultado no tiene que estar necesariamente en la curva, y por tanto, no da una suma en ese conjunto. Por este motivo, se hace esta distinción en cuanto a la notación para no confundir a esta con la nueva operación cuando estas dos aparezcan simultáneamente en una discusión o argumento. La suma que hasta ahora se venía conociendo se denotará por $+$ mientras que para la nueva operación de puntos en la curva elíptica se reservará el símbolo $\oplus$. También se llamará suma, ya que satisface las mismas propiedades que la anterior pero en el grupo de la curva elíptica.

Proposición. *La curva elíptica $E(\mathbb{F})$ con la operación $\oplus$ forman un grupo abeliano, es decir, se satisfacen las siguientes propiedades $\forall P,Q,R \in E(\mathbb{F})$:*

1. *Conmutatividad: $P \oplus Q = Q \oplus P$.*
2. *Existencia del elemento neutro, $\mathscr{O}$: $P \oplus \mathscr{O} = P$.*
3. *Existencia del elemento opuesto, $-P$: $P \oplus (-P) = \mathscr{O}$.*
4. *Asociatividad: $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.*

Demostración. Se realizará la demostración siguiendo los mismos puntos ya establecidos.

1. Proporcionados dos puntos distintos, existe una única recta que pase por ambos.
2. La recta L que une a P y $\mathscr{O}$ corta a E en un tercer punto R por el teorema de Bézout. La recta L' que pasa por $\mathscr{O}$ y R, siguiendo el mismo argumento que en 1, es de hecho igual a L, y por tanto el tercer punto de intersección con E vuelve a ser de nuevo P.
3. Dado un punto $P = (x,y)$, su elemento opuesto es $-P = (x,-y)$. Para probar esto, se suma P al punto $-P$. La recta L que pasa a través de P y $-P$ es vertical, así que el tercer punto de intersección es $\mathscr{O}$. Ahora se une $\mathscr{O}$ con $\mathscr{O}$, lo que resulta en la recta del infinito, y el tercer punto de intersección vuelve a ser $\mathscr{O}$ porque esta recta corta a la curva en $\mathscr{O}$ con multiplicidad de intersección 3.
4. Una demostración completa de esta propiedad puede encontrarse en el capítulo 2 sección 4 de [10].

□

Dados $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ se plantea ahora la siguiente cuestión: calcular $P_1 \oplus P_2 = P_3$ eficientemente, con $P_3 = (x_3, y_3)$.

El primer caso que se va a estudiar es $P_1 \neq P_2$ y ninguno de ellos $\mathscr{O}$. La recta L que junta P_1 y P_2 tiene pendiente

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Si $x_1 = x_2$ entonces L es vertical. Este caso será tratado más tarde, así que por el momento se puede asumir que $x_1 \neq x_2$. La ecuación de L es entonces

$$y = m(x - x_1) + y_1$$

Sin más que sustituir en la ecuación de la curva E para encontrar la intersección se obtiene la igualdad

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

Se reorganiza escribiendo todos los términos en un mismo lado de la igualdad de forma queda lo siguiente

$$0 = x^3 - m^2x^2 + (A + 2m(y_1 - x_1))x + B + m^2x_1^2 + y_1^2 - 2mx_1y_1$$

Esto es una ecuación cúbica en x, y sus tres raíces r, s, t dan las coordenadas de la x de los tres puntos de intersección de L con E. Generalmente, resolver una cúbica no es fácil, pero en este caso dos de las raíces ya son conocidas, x_1 y x_2, ya que P_1 y P_2 son puntos que están tanto en L como en E. Por lo tanto, se podría factorizar la cúbica para obtener el tercer valor de x. Pero hay una forma más sencilla. Si se tiene un polinomio de grado 3, $x^3 + ax^3 + bx + c$, con raíces r, s, t entonces

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + (rs + st + rt)x - srt$$

Igualando los coeficientes del término x^2 a ambos lados

$$r + s + t = -a$$

Si se conocen dos de las raíces, r, s, se puede recuperar la tercera como $t = -a - r - s$. En este caso particular

$$x = m^2 - x_1 - x_2, \qquad y = m(x - x_1) + y_1,$$

Ahora, reflejando respecto del eje x para obtener el punto $P_3 = (x_3, y_3)$

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1,$$

En el caso en el que $x_1 = x_2$ pero $y_1 \neq y_2$, la simetría de la ecuación $y^2 = x^3 + Ax + B$ conduce a deducir que lo que ocurre en este supuesto es que $y_2 = -y_1$. Entonces, la recta a través de P_1 y P_2 es una recta vertical, que, por lo tanto, interseca a E en $\mathscr{O}$, y ya se ha visto que entonces $P_3 = \mathscr{O}$.

Ahora se analiza el caso en el que $P_1 = P_2 = (x_0, y_0)$. Para este caso, se debe considerar la recta tangente a E en dicho punto. De la relación $y^2 = f(x)$ se deduce, por diferenciación implícita, que la pendiente m de la recta tangente L es

$$2y\frac{dy}{dx} = f'(x) = 3x^2 + A \Longrightarrow m = \frac{dy}{dx} = \frac{f'(x)}{2y} = \frac{3x_0^2 + A}{2y_0}$$

Si $y_0 \neq 0$, esta es la fórmula de la pendiente utilizada cuando se quiere duplicar un punto. En este caso, solamente una raíz es conocida, x_0, pero es una raíz doble ya que L es la tangente a E en (x_0, y_0). Una vez obtenido el valor para m, simplemente se sustituye en las fórmulas de arriba.

Si $y_0 = 0$, entonces la recta tangente es vertical y se obtiene $P_1 \oplus P_2 = \mathscr{O}$ al igual que antes.

Capítulo 2

Número de puntos en la curva elíptica

El propósito principal de este capítulo es preparar todos los requisitos necesarios para hacer un esquema de la demostración del Teorema de Hasse. Este teorema proporciona una cota del número de puntos en la curva elíptica. Para ello, se demostrarán algunos resultados técnicos sobre endomorfismos separables.

Notar que E es la ecuación de la curva elíptica mientras que $E(\mathbb{F})$ son las soluciones de dicha ecuación con coordenadas en $\mathbb{F}$. Por tanto, $E(\overline{\mathbb{F}})$ son las soluciones de la ecuación consideradas en la clausura algebraica del cuerpo anterior. Entonces, el cardinal del grupo que forma el conjunto de puntos de la curva elíptica dependerá del cuerpo en el que sean consideradas las soluciones de la ecuación. Además, se tiene que $E(\mathbb{F}) \subseteq E(\overline{\mathbb{F}})$ ya que $\mathbb{F} \subseteq \overline{\mathbb{F}}$.

2.1. Endomorfismos

Definición. Un *endomorfismo* de una curva E definida sobre un cuerpo $\mathbb{F}$ es un homomorfismo de grupos $\alpha : E(\overline{\mathbb{F}}) \to E(\overline{\mathbb{F}})$ dado por funciones racionales (cocientes de polinomios con coeficientes en $\overline{\mathbb{F}}$).

Si los coeficientes de las funciones racionales están en el cuerpo $\mathbb{F}$, entonces α induce un endomorfismo $\overline{\alpha} : E(\mathbb{F}) \to E(\mathbb{F})$ del grupo de puntos $\mathbb{F}$-racionales de E.

Por ser endomorfismo de grupos, en particular, $\forall P_1, P_2 \in E(\overline{\mathbb{F}})$ se cumple que $\alpha(P_1 \oplus P_2) = \alpha(P_1) \oplus \alpha(P_2)$ y $\alpha(\mathscr{O}) = \mathscr{O}$. El endomorfismo trivial que lleva cada punto a $\mathscr{O}$ se denotará por 0. En este trabajo se asumirá que α es no trivial; es decir, que existe algún punto $P = (x, y)$ tal que $\alpha(P) \neq \mathscr{O}$.

Los endomorfismos distintos del trivial son sobreyectivos. Intuitivamente, trabajar con la clausura algebraica de un cuerpo permite resolver las ecuaciones definidas para encontrar la imagen inversa de un punto.

Ejemplo. *Sea E dada por $y^2 = x^3 + Ax + B$ y sea $\alpha(P) = 2P$. Entonces α es un homomorfismo y,*

$$\alpha(P) = \left(\left(\frac{3x^2 + A}{2y} \right)^2 - 2x, \frac{3x^2 + A}{2y} \left(3x - \left(\frac{3x^2 + A}{2y} \right)^2 \right) - y \right)$$

donde $P = (x, y)$. Como α está dado por funciones racionales, es un endomorfismo de E. Se denota $[2]$:

$$\begin{array}{ccc} [2] : E(\overline{\mathbb{F}}) & \longrightarrow & E(\overline{\mathbb{F}}) \\ P & \longmapsto & 2P = P \oplus P. \end{array}$$

Ejemplo. *El ejemplo anterior se puede generalizar tomando $\alpha(P) = mP$ con $m \in \mathbb{Z}$ arbitrario, dando lugar a un endomorfismo que siguiendo con la misma notación que antes, se escribirá $[m]$:*

$$\begin{array}{ccc} [m] : E(\overline{\mathbb{F}}) & \longrightarrow & E(\overline{\mathbb{F}}) \\ P & \longmapsto & mP = \underbrace{P \oplus \ldots \oplus P}_{m}. \end{array}$$

Las expresiones concretas para las coordenadas de $[m]$ en términos de los coeficientes A y B de la ecuación simplificada de Weierstrass para E se pueden obtener utilizando las fórmulas de la duplicación de un punto sucesivamente, todas las veces que sean necesarias. Incluso las fórmulas para la suma de dos puntos distintos, en el caso en el que m sea un número impar. Esto resultará de gran utilidad a la hora de averiguar los puntos de $E(\mathbb{F})$ que satisfacen que $mP = \mathcal{O}$.

A continuación, se argumentará que la expresión general de un endomorfismo puede simplificarse. Partiendo de la definición, se tiene en consideración que tanto el punto de partida como su respectiva imagen, deben estar en la curva elíptica. Esto quiere decir que ambas coordenadas deben ser soluciones de la ecuación de la curva elíptica. Se asume que la curva elíptica viene dada en su forma de Weierstrass simplificada.

Por lo tanto, se puede reemplazar cualquier potencia par de y por un polinomio en x, y cualquier potencia impar de y por un polinomio en x multiplicado por y. Este argumento de sustitución de las potencias pares de y por la correspondiente ecuación en x se repite siempre. Entonces si $R(x,y)$ es una función racional, tenemos que se puede escribir de la siguiente manera

$$R(x,y) = \frac{f_1(x) + f_2(x)y}{q_1(x) + q_2(x)y}$$

A continuación, se racionaliza y se vuelve a utilizar que se debe cumplir la ecuación de Weierstrass. El resultado de realizar estos cambios es

$$R(x,y) = \frac{f_3(x) + f_4(x)y}{q_3(x)}$$

Considerando un endomorfismo tal que $\alpha(x,y) = (R_1(x,y), R_2(x,y))$, se sabe que $\alpha(x,-y) = \alpha(-(x,y))$ y utilizando las propiedades de los endomorfismos, esto último es $\alpha(-(x,y)) = -\alpha(x,y)$. Reescribiendo esto con R_1 y R_2 es equivalente a $R_1(x,-y) = R_1(x,y)$ y $R_2(x,-y) = -R_2(x,y)$. De aquí se deduce que en R_1 el polinomio $f_4(x) = 0$ y en R_2 el polinomio $f_3(x) = 0$.

La conclusión extraída del argumento desarrollado en los párrafos precedentes se halla enunciada en la siguiente proposición.

Proposición. *Un endomorfismo $\alpha : E(\overline{\mathbb{F}}) \to E(\overline{\mathbb{F}})$ viene dado por $\alpha(x,y) = (r_1(x), r_2(x) \cdot y)$ donde $r_1(x)$ y $r_2(x)$ son funciones racionales.*

Ejemplo. *Al realizar el cambio sugerido en la explicación de la sustitución de las potencias pares de y por la ecuación de Weierstrass en el ejemplo anterior, donde $\alpha(P) = 2P$, se obtiene el siguiente resultado*

$$\alpha(P) = \left(\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}, y \cdot \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8(x^3 + Ax + B)^2} \right)$$

Obsérvese que la primera coordenada es una función racional en x mientras que en la segunda aparece el factor y con exponente uno, tal y como se ha descrito con anterioridad.

Observación. *Los siguientes aspectos se deducen de lo visto hasta el momento.*

- *Se puede escribir $r_1(x) = \frac{g(x)}{q(x)}$, con $g(x)$ y $q(x)$ polinomios sin factores comunes.*
- *Si $q(x) = 0$ para algún punto (x,y), entonces $\alpha(x,y) = \mathcal{O}$.*
- *Si $q(x) \neq 0$, entonces $r_1(x)$ está bien definida y $r_2(x)$ también ya que $(yr_2(x))^2 = f(r_1(x))$. Se puede decir que el endomorfismo está bien definido por estarlo ambas funciones racionales.*

El núcleo de un endomorfismo no trivial es finito porque $\alpha(x,y) = \mathcal{O}$ en los puntos (x,y) para los que $q(x) = 0$. Habrá tantos puntos de estos como raíces tenga el polinomio $q(x)$, cuyo número viene determinado por su grado, y por tanto, existen solamente una cantidad finita de ellas.

Definición. Sea α un endomorfismo no trivial.

- El *grado* de α es
$$gr(\alpha) = \max\{gr(g(x)), gr(q(x))\}$$
Si $\alpha = 0$, entonces $gr(0) = 0$. Por lo tanto, el grado de un endomorfismo siempre es un número mayor o igual que cero.
- Se dice que el endomorfismo es *separable* si $r_1'(x) \neq 0$, o equivalentemente, si $g'(x) \neq 0$ ó $q'(x) \neq 0$.

Ejemplo. *Regresando de nuevo al ejemplo del endomorfismo* [2]*, su grado es* $gr(\alpha) = 4$ *y, además, es separable ya que* $3x^2 + A \neq 0$.

2.2. Anillos de endomorfismos

Definición. Sea E una curva elíptica definida sobre un cuerpo $\mathbb{F}$. El anillo de endomorfismos $End(E)$ de $E(\overline{\mathbb{F}}_q)$ en $E(\overline{\mathbb{F}}_q)$ está formado por el grupo abeliano bajo la suma, donde la suma $\alpha + \beta$ está definida por

$$(\alpha + \beta)(P) = \alpha(P) \oplus \beta(P)$$

y el endomorfismo cero es la identidad aditiva, con la multiplicación definida por composición ($\alpha\beta = \alpha \circ \beta$). Así pues, para cualquier $\alpha \in End(E)$ se tiene

$$n\alpha := \underbrace{\alpha + \ldots + \alpha}_{n} = [n] \circ \alpha,$$

donde se recuerda que $[n]$ es el endomorfismo multiplicación por n en $E(\overline{\mathbb{F}}_q)$.

Notar que $[1] = 1$ es la identidad multiplicativa (el endomorfismo identidad). Cuando el contexto lo deje suficientemente claro, se identificarán los endomorfismos de los enteros $[n]$ con n. El ejemplo anterior generalizado junto con la multiplicación por un entero motiva la siguiente definición.

Definición. Sea n un entero positivo. El núcleo del endomorfismo de la multiplicación por un $n \in \mathbb{Z}$ es el *subgrupo de n-torsión*.

$$E[n] = \{P \in E(\overline{\mathbb{F}}) \mid nP = \mathcal{O}\}$$

Sea E una curva elíptica definida sobre un cuerpo de característica p (incluyendo la posibilidad de que sea $p = 0$). Para cualquier $\alpha \in End(E)$, se considera la restricción α_n de α al subgrupo de n-torsión $E[n]$. Como α es un homomorfismo de grupos, conserva los puntos de n-torsión, así que α_n es un endomorfismo del grupo abeliano $E[n]$.

Cuando n es un entero positivo no divisible por p, los subgrupos de n-torsión tienen rango 2. En otro caso, tienen rango 0 ó 1. La prueba se da en el primer teorema de la séptima sección de [8]. Por lo tanto, suponiendo la primera situación, que es la que resulta interesante para lo que viene después, se puede elegir $\{\beta_1, \beta_2\}$ una base que genere $E[n]$ como un grupo abeliano. Todos sus elementos se pueden expresar como una combinación lineal de β_1 y β_2, es decir, de la forma $m_1\beta_1 + m_2\beta_2$ con $m_1, m_2 \in \mathbb{Z}$, únicamente determinados módulo n. Se puede representar α_n como una matriz 2×2

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ tales que

$$\alpha(\beta_1) = a\beta_1 + c\beta_2, \quad \alpha(\beta_2) = b\beta_1 + d\beta_2.$$

Notar que la representación de esta matriz depende solamente de la elección de la base, pero los invariantes de la matriz, como la traza o el determinante, son independientes de esta elección.

La composición de homomorfismos se corresponde con la multiplicación de matrices. En particular, los endomorfismos son homomorfismos, y por lo tanto esto también se cumple para ellos.

Teorema 2.1. *Sea $\alpha, \beta \in End(E)$. Entonces:*

- $\exists!\ \hat{\alpha} : E(\overline{\mathbb{F}}) \to E(\overline{\mathbb{F}})$ *tal que* $\alpha\hat{\alpha} = \hat{\alpha}\alpha = [n]$, *donde* $n = gr(\alpha) = gr(\hat{\alpha})$.
- $\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}$.
- $\widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}$
- *Si* $n \in \mathbb{Z}$, *entonces* $\hat{[n]} = [n]$ *y su grado es* n^2.

Observación. *Si* $gr(\alpha) = 1$, *entonces* α *es un isomorfismo y* $\hat{\alpha}$ *el endomorfismo inverso de* α.

Lema. *Para cualquier endomorfismo* α *se tiene que* $\alpha + \hat{\alpha} = [a]$, *donde* $a = 1 + gr(\alpha) - gr(\alpha - 1)$.

Demostración. Para cualquier $\alpha \in End(E)$, incluyendo $\alpha = 0$

$$gr(\alpha - 1) = (\widehat{\alpha - 1})(\alpha - 1) = (\hat{\alpha} - \hat{1})(\alpha - 1) = (\hat{\alpha} - 1)(\alpha - 1) = 1 - (\alpha + \hat{\alpha}) + gr(\alpha),$$

y por lo tanto, $\alpha + \hat{\alpha} = 1 + gr(\alpha) - gr(\alpha - 1)$ □

Definición. El entero *a* verificando el lema anterior se denomina *traza* del endomorfismo α, y se denotará $tr(\alpha)$. Es decir, $tr(\alpha)$ es el entero determinado por la condición

$$[tr(\alpha)] = \alpha + \hat{\alpha}.$$

Teorema 2.2. *Sea* $\alpha \in End(E)$ *un endomorfismo no trivial. Ambas* α *y* $\hat{\alpha}$ *son raíces del polinomio característico*

$$x^2 - tr(\alpha)x + gr(\alpha)$$

Demostración. Sustituyendo directamente en la ecuación

- $\alpha^2 - tr(\alpha)\alpha + gr(\alpha) = \alpha^2 - (\alpha + \hat{\alpha})\alpha + \alpha\hat{\alpha} = 0$
- $\hat{\alpha}^2 - tr(\alpha)\hat{\alpha} + gr(\alpha) = \hat{\alpha}^2 - (\alpha + \hat{\alpha})\hat{\alpha} + \alpha\hat{\alpha} = 0$

□

2.3. El endomorfismo de Frobenius

Se introduce a continuación otro tipo de ejemplo de endomorfismo, algo más concreto, distinto de la multiplicación por un entero, que juega un papel crucial en la teoría de curvas elípticas sobre un cuerpo finito, $\mathbb{F}_q$. Aquí, q, es una potencia de primo, es decir, $q = p^k$ para $k \in \mathbb{N}$, con p un número primo cualquiera, que será la característica del cuerpo.

Proposición. *Sea E una curva elíptica definida sobre* $\mathbb{F}_q$. *La aplicación siguiente es un automorfismo.*

$$\begin{array}{ccc} \phi_q : E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_q) \\ (x,y) & \longmapsto & (x^q, y^q) \\ \mathcal{O} & \longmapsto & \mathcal{O} \end{array}$$

Demostración. La inyectividad y la sobreyectividad de ϕ_q son evidentes por definición (para la sobreyectividad notar de nuevo que se trabaja sobre la clausura algebraica). Por lo tanto, es suficiente comprobar que ϕ_q es un endomorfismo. Se tiene que probar que $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ es un homomorfismo de grupos dado por funciones racionales. Esto último se ve directamente, ya que la función está dada por polinomios. El siguiente paso es ver que en efecto se trata de un homomorfismo.

Considerando la curva elíptica en su forma de Weierstrass, sean $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\overline{\mathbb{F}}_q)$ con $x_1 \neq x_2$. Utilizando las fórmulas ya desarrolladas en secciones anteriores para la suma, el punto $P_3 = (x_3, y_3) = P_1 \oplus P_2$ vendrá dado por

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad m = \frac{y_2 - y_1}{x_2 - x_1}$$

Elevando todo a la q-ésima potencia se obtiene que

$$x_3^q = m'^2 - x_1^q - x_2^q, \qquad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \qquad m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}$$

Lo que demuestra que $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) \oplus \phi_q(x_2, y_2)$.

En el caso en el que $x_1 = x_2$ pero $y_1 \neq y_2$, ya es sabido que $P_3 = \mathcal{O}$. Entonces $x_1^q = x_2^q$ e $y_1^q \neq y_2^q$, por lo que $\phi_q(x_1, y_1) \oplus \phi_q(x_2, y_2) = \mathcal{O}$, como se quería probar.

Se supone ahora que $P_2 = \mathcal{O}$, entonces $P_1 \oplus \mathcal{O} = P_1, \forall P_1 \in E(\overline{\mathbb{F}}_q)$. Además, se tiene que $\phi_q(x_2, y_2) = \mathcal{O}$ y trivialmente $\phi_q(x_1, y_1) \oplus \mathcal{O} = \phi_q(x_1, y_1)$.

Finalmente, se aborda este problema en el caso en el que se esté sumando un punto consigo mismo. Las fórmulas para las coordenadas de $2P_1 = P_3$ son iguales que anteriormente pero la pendiente cambia transformándose en $m = \dfrac{3x_1^2 + A}{2y_1}$ y cuando se produce el paso de elevar a la q-ésima potencia se obtiene $m' = \dfrac{3^q (x_1^q)^2 + A^q}{2^q y_1^q}$. Como $2, 3, A \in \mathbb{F}_q$, se tiene $2^q = 2, 3^q = 3, A^q = A$. Esto significa que el resultado cumple lo esperado $2(x_1^q, y_1^q) = (x_3^q, y_3^q)$. □

Definición. El endomorfismo anterior es lo que se conoce como el *endomorfismo de Frobenius*.

Lema. *El endomorfismo de Frobenius tiene grado q y no es separable.*

Demostración. El grado de los polinomios que definen el endomorfismo de Frobenius es q. Además, como q es múltiplo de la característica, cumple que $q \cdot 1 = 0$ en $\mathbb{F}_q$, y las derivadas tanto de x^q como de y^q son idénticamente cero. Por lo tanto, ϕ_q no es separable. □

Proposición. *El endomorfismo de Frobenius satisface estas dos propiedades.*

1. $Ker(\phi_q - 1) = E(\mathbb{F}_q)$.
2. $\phi_q - 1$ *es un endomorfismo separable y además, se puede deducir que* $\#E(\mathbb{F}_q) = gr(\phi_q - 1)$.

Demostración. El primer punto es más sencillo de probar que el segundo.

1. $(x, y) \in E(\mathbb{F}_q) \iff (x, y) \in \mathbb{F}_q \iff x^q = x,\ y^q = y \iff \phi_q(x, y) = (x, y) \iff (x, y) \in Ker(\phi_q - 1)$
2. La definición del endomorfismo $\phi_q - 1$ actuando sobre un punto (x, y) es

$$(\phi_q - 1)(x, y) = \phi_q(x, y) - (x, y) = (x^q, y^q) + (x, -y)$$

El cálculo de la expresión para la primera coordenada es

$$\left(\frac{-y - y^q}{x - x^q}\right)^2 - x^q - x = \left(\frac{-y(1 + y^{q-1})}{x - x^q}\right)^2 - x^q - x = \frac{(-y)^2 (1 + y^{q-1})^2}{(x - x^q)^2} - x^q - x$$

Utilizando el cambio habitual $y^2 = f(x)$ para que todo dependa únicamente de la variable x y teniendo en cuenta que $q - 1$ es par por ser q impar

$$\frac{f(x)(1 + f(x)^{\frac{q-1}{2}})^2}{(x - x^q)^2} - x^q - x$$

La derivada del denominador no es el polinomio nulo

$$2(x-x^q)(1-qx^{q-1}) = 2(x-x^q) \neq 0$$

Se concluye que efectivamente $\phi_q - 1$ es un endomorfismo separable.

Llevar a cabo la demostración de la segunda parte de esta afirmación, mencionada en el enunciado como una deducción de la primera, requiere de un detalle riguroso, por lo que se trata de una tarea costosa que excede en cuanto a su longitud para las características de este trabajo. Sin embargo, una demostración completa de esta propiedad puede encontrarse en la novena sección del segundo capítulo de [10].

□

Lema. *Sean $r,s \in \mathbb{Z}$. Entonces $gr(r\phi_q - s) = r^2q + s^2 - rst$, donde t es la traza del endomorfismo de Frobenius ϕ_q.*

Demostración. Se resuelve este apartado usando técnicas similares a la sección anterior

$$gr(r\phi_q - s) = \widehat{(r\phi_q - s)}(r\phi_q - s) = (\hat{r}\hat{\phi}_q - \hat{s})(r\phi_q - s) = r^2\hat{\phi}_q\phi_q + s^2 - rs\hat{\phi}_q - rs\phi_q = r^2q + s^2 - rst.$$

□

Teorema 2.3 (Teorema de Hasse)**.** *Sea E una curva elíptica definida sobre el cuerpo finito $\mathbb{F}_q$. Entonces, el orden de $E(\mathbb{F}_q)$ viene dado por la siguiente igualdad*

$$\#E(\mathbb{F}_q) = q + 1 - t, \quad |t| \leq 2\sqrt{q}$$

donde t vuelve a ser la traza del endomorfismo de Frobenius.

Demostración. Sea $\phi_q(x,y) = (x^q, y^q)$ el endomorfismo de Frobenius en la curva. Entonces, $E(\mathbb{F}_q)$ es el subgrupo de $E(\overline{\mathbb{F}}_q)$ fijado por ϕ_q, así que $E(\mathbb{F}_q) = ker(\phi_q - 1)$. El endomorfismo $\phi_q - 1$ es separable y por lo tanto, se tiene

$$\#Ker(\phi_q - 1) = \#E(\mathbb{F}_q) = gr(\phi_q - 1) = \widehat{(\phi_q - 1)}(\phi_q - 1) = \hat{\phi}_q\phi_q + 1 - (\hat{\phi}_q + \phi_q) = q + 1 - t.$$

Solo queda probar que efectivamente se cumple que $|t| \leq 2\sqrt{q}$. Para ello, se utiliza el lema anterior.

$$gr(r\phi_q - s) \geq 0 \iff r^2q + s^2 - rst \geq 0 \iff \frac{r^2q}{s^2} + \frac{s^2}{s^2} - \frac{rst}{s^2} \geq 0 \iff q\left(\frac{r}{s}\right)^2 - t\left(\frac{r}{s}\right) + 1 \geq 0$$

Esto es cierto para todos los números racionales distintos de cero de la forma r/s.

El conjunto de los números racionales r/s tales que $mcd(s,q) = 1$ es **denso** en $\mathbb{R}$.

Por lo tanto, $qx^2 - tx + 1 \geq 0, \forall x \in \mathbb{R}$. Se sigue que el discriminante de este polinomio, $t^2 - 4q$ no puede ser positivo, lo que se puede escribir como $t^2 - 4q \leq 0$ y esto da la cota deseada $|t| \leq 2\sqrt{q}$. □

Teorema 2.4 (Ecuación característica de Frobenius)**.** *Se tiene $\phi_q^2 - t\phi_q + q = 0$ como endomorfismo de E, donde t es la traza del endomorfismo de Frobenius. En otras palabras, $\forall (x,y) \in E(\overline{\mathbb{F}}_q)$ se cumple que*

$$(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x,y) = \mathcal{O}$$

Más aún, t es el único entero que satisface esta relación.

Demostración. Si $\phi_q^2 - t\phi_q + q$ no es el endomorfismo trivial, entonces su núcleo es finito ya que los elementos del núcleo se pueden calcular encontrando soluciones a una ecuación polinómica.

Se probará que el núcleo es infinito, por tanto es el endomorfismo cero.

Sea $m \geq 1$ un entero primo distinto de la característica del cuerpo. Recordar que ϕ_q induce una matriz $(\phi_q)_m$ que describe la acción de ϕ_q sobre el subgrupo de m-torsión $E[m]$. Sea esta matriz la siguiente

$$(\phi_q)_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Se tiene que $X^2 - tX + q \pmod m$ es el polinomio característico de ϕ_q como endomorfismo de $E[m]$. En particular, el polinomio característico se anula al evaluarlo en $X = \phi_q$. Es decir, el endomorfismo $(\phi_q)^2 - t\phi_q + q$ coincide con el endomorfismo 0 en $E[m]$. Esto es lo que se prueba a continuación.

Utilizando que $\phi_q - 1$ es separable y la equivalencia $det((\phi_q)_m) \equiv gr(\phi_q) \pmod m$[1], se puede escribir la siguiente cadena de igualdades

$$\#Ker(\phi_q - 1) = gr(\phi_q - 1) \equiv det((\phi_q)_m - I) = ad - bc - (a+d) + 1 \pmod m$$

Observar que volviendo a usar la misma equivalencia se obtiene que $ad - bc = det((\phi_q)_m) \equiv q \pmod m$. Y gracias al teorema de Hasse $\#Ker(\phi_q - 1) = q + 1 - t$. Por lo tanto, $Traza((\phi_q)_m) = a + d \equiv t \pmod m$.

Esto significa que el endomorfismo $\phi_q^2 - t\phi_q + q$ es idénticamente 0 en $E[m]$. Como hay infinitas elecciones para m, el núcleo del endomorfismo es infinito, como se quería demostrar.

Para probar la unicidad, se supone que $u \neq t$ también satisface $\phi_q^2 - u\phi_q + q = 0$. Para cualquier m primo y cualquier $P \in E[m]$ no trivial, se tiene

$$(t-u)\phi_q(P) = (\phi_q^2(P) - t\phi_q(P) + q(P)) - (\phi_q^2(P) - u\phi_q(P) + q(P)) = 0.$$

Como $\phi_q(P) \neq 0$ en $E[m]$ y m es primo, el punto $\phi_q(P)$ tiene orden m. De la ecuación anterior se deduce que m debe dividir a $t - u$, por lo que $u \equiv t \pmod m$. Por lo tanto, t es único módulo m. Y otra vez, como hay infinitas elecciones para m, el entero t es único. □

2.4. Polinomios de división

Para estudiar los subgrupos de torsión, es necesario describir los endomorfismos dados por la multiplicación por un entero. El objetivo de este apartado es desarrollar las fórmulas para la suma de un punto genérico consigo mismo n veces. Este punto P se encuentra en la curva E definida por $y^2 = x^3 + Ax + B$. El punto nP tiene la forma $\left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right)$ donde $\phi_n, \omega_n, \psi_n \in \mathbb{Z}[x, y, A, B]$ son polinomios que se reducen módulo la ecuación de la curva para que el grado de y sea como mucho 1.

Una observación será que ϕ_n y ψ_n^2 no dependen de y, y exactamente uno de ω_n y ψ_n^3 depende de una potencia impar de y, así que esto dará el endomorfismo $[n]$ de forma estándar, con funciones racionales.

El polinomio ψ_n se conoce como el n-ésimo polinomio de división, que se define de forma recursiva, empezando con las variables A y B:

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2) \\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \ \textit{para } n \geq 2 \\
\psi_{2n} &= (2y)^{-1}\psi_m(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \ \textit{para } n \geq 2
\end{aligned}$$

[1] La demostración de esta equivalencia utiliza un concepto introducido en el último capítulo de este trabajo, el pairing de Weil. Para más detalles, se ruega consultar la tercera sección del tercer capítulo [10].

donde se reduce el resultado módulo la ecuación de la curva para que ψ_n sea como mucho lineal en y.

Se puede probar que $\psi_m(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$ siempre es divisible por $(2y)^{-1}$, por lo que ψ_{2n} es, de hecho, un polinomio. Si se define $\psi_{-n} := -\psi_n$, se puede probar que estas recurrencias se cumplen $\forall n \in \mathbb{Z}$. Entonces, los siguientes se definen como

$$\phi_n := x\psi_n^2 - \psi_{n+1}\psi_{n-1},\ \forall n \in \mathbb{Z}$$
$$\omega_n := (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2),\ \forall n \in \mathbb{Z}$$

Se puede demostrar que $\phi_{-n} = \phi_n$ y $\omega_{-n} = \omega_n$. Al igual que antes, se reducen estos polinomios módulo la ecuación de la curva para que sean como mucho lineales en y.

Lema. *Para todo entero n:*

$$\psi_n \text{ pertenece a } \begin{cases} \mathbb{Z}[x,A,B], & \text{si n impar} \\ 2y\mathbb{Z}[x,A,B], & \text{si n par} \end{cases} \qquad \omega_n \text{ pertenece a } \begin{cases} \mathbb{Z}[x,A,B], & \text{si n par} \\ y\mathbb{Z}[x,A,B], & \text{si n impar} \end{cases}$$

$$\phi_n \text{ pertenece a } \mathbb{Z}[x,A,B]$$

Demostración. Se pueden realizar fácilmente por inducción; consultar el tercer y cuarto lemas de la segunda sección del tercer capítulo [10]. □

Se sigue del lema que, después de reemplazar y^2 por $x^3 + Ax + B$ si es necesario, ψ_n^2 pertenece a $\mathbb{Z}[x,A,B]$ para todo n positivo, así que se puede pensar en ϕ_n y ψ_n^2 como polinomios en x solamente, mientras que exactamente uno de ω_n y ψ_n^3 dependen de y. En este último caso, se puede multiplicar el numerador y el denominador de ω_n/ψ_n^3 por y, para después reemplazar y^2 en el denominador con $x^3 + Ax + B$. Notar que ψ_n no es necesariamente un polinomio en x.

Se finaliza el capítulo con el siguiente resultado, que no es del todo trivial.

Teorema 2.5. *Sea $E(\mathbb{F}_q)$ una curva elíptica definida por la ecuación $y^2 = x^3 + Ax + B$ y sea $n \in \mathbb{Z}$ distinto de cero. La función racional*

$$[n](x,y) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x)}{\psi_n^3(x,y)}\right)$$

envía cada punto $P \in E(\overline{\mathbb{F}}_q)$ a nP, y es separable si y solo si n no es divisible por la característica de $\mathbb{F}_q$.

Demostración. Un esquema de la prueba se puede encontrar en la sexta sección de [8]. □

Capítulo 3

Algoritmo de Schoof

En 1985, René Schoof introdujo el primer algoritmo para calcular $\#E(\mathbb{F}_q)$ en un periodo de tiempo razonable, mucho más rápido que los algoritmos que existían hasta entonces. Posteriormente, se desarrollaron extensiones del algoritmo que refinaron y mejoraron el original y que siguen siendo en la actualidad el método elegido para contar puntos cuándo la característica de $\mathbb{F}_q$ tiene varios cientos de dígitos decimales. La estrategia básica de Schoof es muy simple: calcular la traza del endomorfismo de Frobenius t módulo muchos primos pequeños ℓ (excluyendo la característica del cuerpo por simplicidad) para después utilizar el Teorema Chino de los Restos y obtener t; esto determinará $\#E(\mathbb{F}_q) = q+1-t$.

El algoritmo se repite hasta que el producto de todos los primos ℓ es mayor que $4\sqrt{q}$ porque se tiene que determinar la traza, que se sabe que está entre $-2\sqrt{q}$ y $2\sqrt{q}$ gracias al teorema de Hasse. Si se conoce módulo un número más grande que la amplitud de ese intervalo, ya está. Incluso si q es muy grande, no hacen falta muchos primos ya que el producto de ellos crece muy rápidamente.

3.1. La traza de Frobenius módulo 2

Se considera primero el caso $\ell = 2$. Si q es impar (de hecho, lo es, ya que q debe ser potencia de primo, siendo este mayor estricto que 3), entonces

$$t = q+1-\#E(\mathbb{F}_q) \text{ es divisible por } 2 \iff \#E(\mathbb{F}_q) \text{ es divisible por } 2 \iff \exists P \in E(\mathbb{F}_q) \text{ tal que } 2P = \mathcal{O}$$

Si E tiene ecuación de Weierstrass $y^2 = f(x)$, los puntos de orden 2 en $E(\mathbb{F}_q)$ son aquellos de la forma $(x_0, 0)$, donde $x_0 \in \mathbb{F}_q$ es una raíz de $f(x)$. Así que,

$$\mathrm{t} \equiv \begin{cases} 0 \pmod 2, & \text{si } f(x) \text{ tiene una raíz en } \mathbb{F}_q \\ 1 \pmod 2, & \text{en otro caso} \end{cases}$$

No es necesario encontrar las raíces de $f(x)$ en $\mathbb{F}_q$, solo se necesita determinar si existen. Para ello, simplemente se debe calcular $g = mcd(x^q - x, f(x))$. El grado de g es el número de raíces distintas de f, así que $t \equiv 0 \pmod 2$ si y solo si $gr(g) > 0$.

Esto acaba el caso $\ell = 2$, a partir de ahora se puede asumir que ℓ es impar.

3.2. La ecuación característica de Frobenius módulo ℓ

Recordar que el endomorfismo de Frobenius $\phi_q(x,y) = (x^q, y^q)$ cumple la ecuación característica $\phi_q^2 - t\phi_q + q = 0$ en el anillo de endomorfismos $End(E)$, donde $t = q+1-\#E(\mathbb{F}_q)$ y $q = gr(\phi_q)$.

Si se restringe ϕ_q al grupo de ℓ-torsión, entonces la ecuación $(\phi_q^2)_\ell - t_\ell(\phi_q)_\ell + q_\ell = 0$ es cierta en $End(E[\ell])$, donde $t_\ell \equiv t \pmod \ell$ y $q_\ell \equiv q \pmod \ell$ se pueden tomar como escalares en $\mathbb{Z}/\ell\mathbb{Z}$ multiplicados por la restricción al grupo de ℓ-torsión, $E[\ell]$, del endomorfismo identidad, $[1]_\ell$. Considerando $q_\ell[1]_\ell$ como la suma de q_ℓ copias de $[1]_\ell$, entonces se puede calcular dicha expresión utilizando las fórmulas para la suma, una vez sean conocidos tanto $End(E[\ell])$ como la suma explícita sus elementos.

Definición. Se denota por $End(E[\ell])$ al anillo de los endomorfismos del grupo $E[\ell]$. Estos endomorfismos se obtienen por la restricción de endomorfismos de E a su subgrupo de ℓ-torsión.

Sea $h = \psi_\ell$ el ℓ-ésimo polinomio de división de E; como ℓ es primo, sabemos que ψ_ℓ no depende de la coordenada y, así que $h \in \mathbb{F}_q[x]$. Un punto $(x_0, y_0) \in E(\overline{\mathbb{F}}_q)$ pertenece a $E[\ell]$ si y solo si $h(x_0) = 0$. Por lo tanto, cuando se escriben los elementos de $End(E[\ell])$ como funciones racionales, se pueden tratar los polinomios que aparecen en estas funciones como elementos del anillo $\mathbb{F}_q[x,y]/(h(x), y^2 - f(x))$ donde $f(x)$ es la ecuación de Weierstrass de E.

En el caso del endomorfismo de Frobenius, se tiene

$$(\phi_q)_\ell = (x^q \text{ mód } h(x), y^q \text{ mód } (h(x), y^2 - f(x)) = (x^q \text{ mód } h(x), y(f(x)^{\frac{q-1}{2}} \text{ mód } h(x)))$$

igualmente,

$$(\phi_q^2)_\ell = (x^{q^2} \text{ mód } h(x), y(f(x)^{\frac{q^2-1}{2}} \text{ mód } h(x)))$$

Notar también que

$$[1]_\ell = (x \text{ mód } h(x), y(1 \text{ mód } h(x)))$$

Por lo tanto, se pueden representar todos los endomorfismos que aparecen en la ecuación característica de Frobenius módulo ℓ de la forma $(a(x), b(x)y)$, donde a y b son polinomios del anillo $\mathbb{F}_q[x]/(h(x))$.

A continuación, se analiza como sumar y multiplicar los elementos de $End(E[\ell])$ que se encuentran representados de esta manera.

3.3. Estructura de $End(E[\ell])$

Se toman $\alpha_1 = (a_1(x), b_1(x)y), \alpha_2 = (a_2(x), b_2(x)y) \in End(E[\ell])$.

Recordar que el producto en $End(E[\ell])$ se define por composición

$$\alpha_1 \circ \alpha_2 = (a_1(a_2(x)), b_1(b_2(x))y)$$

donde cada una de las componentes se reduce módulo $h(x)$.

La suma de endomorfismos, como ya se sabe, se define en términos de la suma en la curva elíptica. Para calcular $\alpha_3 = \alpha_1 + \alpha_2$ simplemente se utilizan las fórmulas para la suma de puntos. Recordar que la fórmula general para calcular una suma distinta de cero $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ en la curva elíptica $E : y^2 = x^3 + Ax + B$ es

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1,$$

donde

$$\mathrm{m} = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2}, & \text{si } x_1 \neq x_2 \\ \dfrac{3x_1^2 + A}{2y_1}, & \text{si } x_1 = x_2 \end{cases}$$

Utilizando estas mismas con $x_1 = a_1(x), x_2 = a_2(x), y_1 = b_1(x)y, y_2 = b_2(x)y$, cuando $x_1 \neq x_2$ se tiene

$$m(x,y) = \frac{b_1(x) - b_2(x)}{a_1(x) - a_2(x)} y = r(x)y$$

donde $r = \dfrac{b_1 - b_2}{a_1 - a_2}$, y cuando $x_1 = x_2$ se tiene

$$m(x,y) = \frac{3a_1(x)^2 + A}{2b_1(x)y} = \frac{3a_1(x)^2 + A}{2b_1(x)f(x)} y = r(x)y$$

donde ahora $r = \dfrac{3a_1^2 + A}{2b_1 f}$. Notar que $m(x,y)^2 = (r(x)y)^2 = r(x)^2 f(x)$, entonces la suma $\alpha_1 + \alpha_2 = \alpha_3 = (a_3(x), b_3(x)y)$ está dada por

$$a_3 = r^2 f - a_1 - a_2$$
$$b_3 = r(a_1 - a_3) - b_1$$

En ambos casos, suponiendo que el denominador de r es invertible en el anillo $\mathbb{F}_q[x]/(h(x))$, se puede reducir r a un polinomio módulo h y obtener $\alpha_3 = (a_3(x), b_3(x)y)$, con $a_3, b_3 \in \mathbb{F}_q[x]/(h(x))$.

Esto no siempre es posible, porque cabe la opción de que el polinomio de división $h = \psi_\ell$ no sea irreducible (de hecho, si $E[\ell] \subseteq E(\mathbb{F}_q)$ se factorizará en polinomios lineales), así que el anillo $\mathbb{F}_q[x]/(h(x))$ no es necesariamente un cuerpo y puede contener elementos distintos de cero que no sean invertibles. Esto afecta cuando el denominador d de r no es invertible módulo h. En este caso, se tomará $mcd(d,h) = g \neq 1$ tal que $gr(g) < gr(h)$. Esto es claro cuando el denominador es $d = a_1 - a_2$, ya que tanto a_1 como a_2 están reducidos módulo h y por lo tanto $gr(d) < gr(h)$.

Una vez g ha sido hallado, la estrategia es simplemente sustituir h por g y volver a empezar el cálculo de la traza de Frobenius módulo ℓ. Las raíces de g corresponden a las primeras componentes de las coordenadas de un subconjunto no vacío de puntos afines en $E[\ell]$, y se sigue del teorema 2.4 que se puede centrar la atención a la acción del endomorfismo de Frobenius módulo ℓ en este subconjunto. Esto permite representar los elementos $End(E[\ell])$ usando coordenadas en el anillo $\mathbb{F}_q[x]/(g(x))$ en lugar de en el anillo $\mathbb{F}_q[x]/(h(x))$.

3.4. La traza de Frobenius módulo ℓ

Durante el algoritmo, los elementos de $End(E[\ell])$ están representados en la forma $(a(x), b(x)y)$ con $a, b \in \mathbb{F}_q[x]/(h(x))$ y todas las operaciones polinomiales tienen lugar en este anillo. Este algoritmo da un método para calcular t_ℓ, la traza de Frobenius módluo ℓ. Dada una curva elíptica $E : y^2 = f(x)$ sobre $\mathbb{F}_q$ y un primo impar ℓ, se calcula t_ℓ como sigue:

1. Calcular el ℓ-ésimo polinomio de división $h = \psi_\ell \in \mathbb{F}_q[x]$ en E.
2. Calcular $\phi_\ell = (x^q \text{ mód } h, (f^{\frac{q-1}{2}} \text{ mód } h)y)$.
3. Calcular $\phi_\ell^2 = \phi_\ell \circ \phi_\ell$.
4. Calcular la multiplicación escalar $q_\ell = q_\ell[1]_\ell$.
5. Calcular $\phi_\ell^2 + q_\ell$.
6. Hallar $x \in [0, \ldots, \ell - 1]$ tal que $x\phi_\ell = \phi_\ell^2 + q_\ell$.
7. Devolver $x = t_\ell$.

Si en cualquiera de los pasos surge algún denominador d no invertible, reemplazar h por $g = mcd(h,d)$ y volver al paso 2.

Ejemplo. *Sea E la curva elíptica $y^2 = x^3 + x + 1 \pmod 7$. Entonces*

$$\#E(\mathbb{F}_q) = 7 + 1 - t$$

Se quiere determinar t. Son necesarios los siguientes primos

$$2 \cdot 3 \cdot 5 = 30 > 11 \approx 4\sqrt{7}$$

El primero es $\ell = 2$. Se calcula

$$x^7 \equiv 2x^2 + 6 \text{ mód } x^3 + x + 1$$

entonces, el máximo común divisor a calcular es

$$mcd(x^7 - x, x^3 + x + 1) = mcd(2x^2 - x + 6, x^3 + x + 1) = 1$$

Se sigue que $x^3 + x + 1$ *no tiene raíces en* $\mathbb{F}_q$*. Por tanto, no hay 2-torsión en* $E(\mathbb{F}_q)$*, así que* $t \equiv 1 \pmod 2$.

Para $\ell = 3$*, el tercer polinomio de división es*

$$h = \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 = 3x^4 + 6x^2 + 12x - 1^2 = 3x^4 + 6x^2 + 5x + 6$$

Se calcula la coordenada x de ϕ_3

$$x^7 \equiv 2x^3 + 2x^2 + 6x + 1 \text{ mód } 3x^4 + 6x^2 + 5x + 6$$

Se calcula la coordenada y de ϕ_3

$$(x^3 + x + 1)^{\frac{7-1}{2}} = (x^3 + x + 1)^3 \equiv x^3 + x^2 + 3x \text{ mód } 3x^4 + 6x^2 + 5x + 6$$

Obteniendo pues que

$$\phi_3 = (2x^3 + 2x^2 + 6x + 1, (x^3 + x^2 + 3x)y)$$

Se calcula la coordenada x de ϕ_3^2

$$x^{49} \equiv x \text{ mód } 3x^4 + 6x^2 + 5x + 6$$

Se calcula la coordenada y de ϕ_3^2

$$(x^3 + x + 1)^{24} \equiv 6 \text{ mód } 3x^4 + 6x^2 + 5x + 6 \equiv -1 \pmod 7$$

Obteniendo pues que

$$\phi_3^2 = -1$$

Se tiene que $q \equiv 1 \pmod 3$*. Por lo tanto,* $q_3 = 1$*, y es necesario calcular*

$$\phi_3^2 + q_3 = 0$$

La traza de Frobenius es $t \equiv 0 \pmod 3$.

Se repite el mismo proceso para $\ell = 5$*. El quinto polinomio de división es*

$$h = \psi_5 = 5x^{12} + 6x^{10} + 2x^9 + 2x^7 + 6x^6 + 4x^5 + 6x^4 + 4x^2 + 2x$$

Se calcula la coordenada x de ϕ_5

$$x^7 \equiv x^7 \text{ mód } h(x)$$

Se calcula la coordenada y de ϕ_5

$$(x^3 + x + 1)^{\frac{7-1}{2}} = (x^3 + x + 1)^3 \equiv x^9 + 3x^7 + 3x^6 + 3x^5 + 6x^4 + 4x^3 + 3x^2 + 3x + 1 \text{ mód } h(x)$$

Obteniendo pues que

$$\phi_5 = (x^7, (x^9 + 3x^7 + 3x^6 + 3x^5 + 6x^4 + 4x^3 + 3x^2 + 3x + 1)y)$$

Se calcula la coordenada x de ϕ_5^2

$$x^{49} \equiv 6x^{11} + 4x^{10} + 2x^9 + 2x^8 + 5x^7 + x^6 + 5x^5 + 4x^4 + x^3 + x^2 \text{ mód } h(x)$$

Se calcula la coordenada y de ϕ_5^2

$$(x^3 + x + 1)^{24} \equiv 2x^{11} + 6x^{10} + x^8 + 4x^7 + 5x^6 + 4x^5 + x^4 + 5x^3 + 3x^2 + 6x + 1 \text{ mód } h(x)$$

Se tiene que $q \equiv 2 \pmod 5$. *Por lo tanto,* $q_5 = 2$, *y realizando los cálculos pertinentes,*

$$\phi_5^2 + q_5 = 3\phi_5$$

La traza de Frobenius es $t \equiv 3 \pmod 5$.

La información de $\ell = 2,3,5$ *es suficiente para determinar* t.

$$\mathrm{t} \equiv \begin{cases} 1 \pmod 2 \\ 0 \pmod 3 \\ 3 \pmod 5 \end{cases}$$

La solución del sistema está expresada en módulo $N = 2 \cdot 3 \cdot 5 = 30$. *Hay que encontrar encontrar los valores (enteros) de* x_1, y_1 *y* z_1 *tales que*

$$x_1 = \frac{30}{2} = 15, \quad y_1 = \frac{30}{3} = 10, \quad z_1 = \frac{30}{5} = 6$$

Con los valores de x_1, y_1 *y* z_1 *se debe determinar* x_2, y_2 *y* z_2

$$15x_2 \equiv 1 \pmod 2, \quad 10y_2 \equiv 1 \pmod 3, \quad 6z_2 \equiv 1 \pmod 5$$

$$\Downarrow$$

$$x_2 \equiv 1 \pmod 2, \quad y_2 \equiv 1 \pmod 3, \quad z_2 \equiv 1 \pmod 5$$

De esta manera, la solución final al sistema de congruencias (por el Teorema Chino del Resto) está dada por

$$t \equiv 1 \cdot 15 \cdot 1 + 0 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 = 33 \equiv 3 \pmod{30}$$

Como $|t| < 2\sqrt{7} < 5$, *debe ser* $t = 3$. *Regresando de nuevo al inicio,* $\#E(\mathbb{F}_q) = 5$.

Capítulo 4

Aplicaciones

Ciertas elecciones de algunas de las propiedades de las curvas elípticas y/o el cuerpo sobre el que están definidas, reducen la dificultad de resolución del problema del logaritmo discreto en esa curva y, como consecuencia, se produce una disminución de la seguridad de los esquemas criptográficos implementados en esas curvas elípticas, convirtiéndolas en criptográficamente inseguras. Es necesario que el orden cumpla una serie de requisitos para que la curva sea segura. En este último capítulo se describirán tres ataques que se aprovechan de varias características dependientes del orden que debilitan el poder de una curva. Los artículos originales del ataques que se van a explicar a continuación se encuentran en [2], [4] y [7]. Para facilitar la comprensión de los dos primeros se ha utilizado [3] y para el último [1].

4.1. El problema del logaritmo discreto

Sea G cualquier grupo, se mantiene la notación multiplicativa por el momento. Sean $a, b \in G$. Se supone conocido que $a^k = b$ para algún $k \in \mathbb{Z}$. El problema del logaritmo discreto es encontrar k dados a y b. Por ejemplo, G podría ser el grupo multiplicativo $\mathbb{F}_q^\times$ de un cuerpo finito. También, G podría ser el grupo formado por los puntos que satisfacen la ecuación de una curva elíptica $E(\mathbb{F}_q)$, en cuyo caso a y b son puntos de la curva y por tanto, se trata de encontrar $k \in \mathbb{Z}$ con $ka = b$. Con esta notación, en la que se considera $E(\mathbb{F}_q)$ como un grupo aditivo, se puede establecer el siguiente isomorfismo:

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \langle Q \rangle \\ [k] & \longmapsto & kQ. \end{array}$$

Aquí $[k]$ se refiere a la clase de equivalencia de k módulo n con $n \in \mathbb{Z}$ el orden de Q en $E(\mathbb{F}_q)$.

Por lo que el problema del logaritmo discreto también se puede enunciar de tal forma que el procedimiento para resolverlo sea encontrar una inversa a dicha aplicación.

La seguridad de los sistemas criptográficos subyace en la dificultad de la resolución del problema del logaritmo discreto. El enunciado del problema del logaritmo discreto en curvas elípticas (ECDLP, por sus iniciales en inglés 'Elliptic Curves Discrete Logarithm Problem') es el siguiente.

Definición. Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$. Dado un punto $Q \in E(\mathbb{F}_q)$ de orden $n \in \mathbb{Z}$ y un punto $P \in \langle Q \rangle$ (subgrupo generado por Q), calcular el entero $k \in [0, n-1]$ tal que $P = kQ$. El entero k se conoce como *el logaritmo discreto de P respecto de la base Q* y en algunas ocasiones se escribe como $k = \log_Q(P)$.

Una forma de atacar el ECDLP es, simplemente, fuerza bruta: probar todos los posibles valores de k hasta hallar uno que funcione. Esto es poco práctico, especialmente cuando la respuesta k puede ser un entero de varios cientos de dígitos, lo que es un tamaño típico usado en criptografía. Por lo tanto, se necesitan mejores técnicas.

4.2. Ataque de Pohlig-Hellman

Una posibilidad de curvas elípticas débiles son aquellas para las que $E(\mathbb{F}_q)$ no tiene subgrupos primos lo suficientemente grandes. Este ataque simplifica el proceso de resolver ECDLP en $E(\mathbb{F}_q)$ a resolver el mismo problema pero en los subgrupos primos de $\langle Q \rangle$.

Sea n el orden del subgrupo generado por Q, es decir, $\#\langle Q \rangle = n$. Ahora, se toma la factorización en primos de $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ (única salvo reordenación de los factores). El objetivo es hallar $k_i \equiv k \pmod{p_i^{e_i}}, \forall i = 1, \ldots, r$ y para ello se representa $k_i = z_0^i + z_1^i p_i + z_2^i p_i^2 + \ldots + z_{e_i-1}^i p^{e_i-1}$ y se calcula $z_j^i, \forall i = 1, \ldots, r$ y $\forall j = 1, \ldots, e_i - 1$.

Esto se hace escribiendo $Q_0^i = \dfrac{n}{p_i} Q$ y $P_0^i = \dfrac{n}{p_i} P$. De aquí se puede deducir que Q_0^i tiene orden p_i, ya que $p_i Q_0^i = \dfrac{p_i n}{p_i} Q = nQ$. Además, $k_i \equiv z_0^i \pmod{p_i}$. Teniendo en cuenta que z_0^i es el dígito menos significativo de la representación de k_i en la base p_i y manipulando la ecuación un poco, se obtiene que

$$P_0^i = \frac{n}{p_i} P = \frac{n}{p_i}(kQ) = \frac{n}{p_i}(z_0^i Q) = z_0^i \left(\frac{n}{p_i} Q\right) = z_0^i Q_0^i$$

Por lo tanto, encontrar z_0^i requiere calcular ECDLP en $\langle Q_0^i \rangle$. Repitiendo el mismo argumento, se puede hallar cada z_j^i resolviendo $P_j^i = z_j^i Q_0^i$ donde

$$P_j^i = \frac{n}{p_i^{j+1}} (P - z_0^i Q - z_1^i p_i Q - z_2^i p_i^2 Q - \ldots - z_{j-1}^i p_i^{j-1} Q)$$

todo este desarrollo se realiza para conseguir un sistema de ecuaciones como a este

$$\mathrm{k} \equiv \begin{cases} k_1 & (\text{mód } p_1^{e_1}) \\ k_2 & (\text{mód } p_2^{e_2}) \\ \vdots & \\ k_r & (\text{mód } p_r^{e_r}) \end{cases}$$

Se sabe que se puede resolver este sistema utilizando el Teorema Chino de los Restos, ya que todos los factores primos son ciertamente coprimos dos a dos, y por lo tanto, el proceso recupera k, la solución al ECDLP.

4.3. Ataque de MOV

El nombre del ataque proviene de los apellidos Menezes, Okamoto y Vanstone [2]. La idea es reducir el problema del logaritmo discreto en el grupo de puntos de una curva elíptica sobre un cuerpo finito al mismo problema pero en el grupo multiplicativo de otro cuerpo finito (quizás más grande). Para ello, se utiliza el pairing de Weil, que es una función que relaciona dos puntos en un subgrupo de torsión en una curva elíptica E con un elemento de $\mathbb{F}_{q^d}$, para un cierto d que se definirá más adelante. El problema del logaritmo discreto en $\mathbb{F}_{q^d}$ puede ser atacado por algunos métodos que son más rápidos que resolver el problema del logaritmo discreto sobre curvas elípticas, siempre que $\mathbb{F}_{q^d}$ no sea mucho más grande que $\mathbb{F}_q$. Para que una curva sea segura este d tiene que ser lo suficientemente grande.

Sea una curva elíptica definida sobre un cuerpo finito $E(\mathbb{F}_q)$ y sea $n \in \mathbb{Z}$ tal que no es divisible por la característica de $\mathbb{F}_q$. Sea

$$\mu_n = \left\{ x \in \overline{\mathbb{F}}_q \mid x^n = 1 \right\}$$

el grupo de las raíces n-ésimas de la unidad en $\overline{\mathbb{F}}_q$. Como la característica de $\mathbb{F}_q$ no divide a n, la ecuación $x^n = 1$ no tiene raíces múltiples y entonces tiene n raíces distintas en $\overline{\mathbb{F}}_q$. Por lo tanto, μ_n es un grupo cíclico de orden n. Cualquier generador ζ de μ_n se llama **raíz n-ésima primitiva de la unidad**. Esto es equivalente a decir que $\zeta^m = 1$ si y solo si n divide a m.

Teorema 4.1 (Pairing de Weil)**.** *Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$ y sea $n \in \mathbb{Z}$ positivo. Asumimos que la característica de $\mathbb{F}_q$ no divide a n. Entonces existe un* ***pairing***

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

que satisface las siguientes propiedades:

1. *e_n es bilineal en cada variable:*

$$\begin{aligned} e_n(S_1+S_2,T) &= e_n(S_1,T)e_n(S_2,T), && \forall S_1,S_2,T \in E[n] \\ e_n(S,T_1+T_2) &= e_n(S,T_1)e_n(S,T_2), && \forall T_1,T_2,S \in E[n] \end{aligned}$$

2. *e_n es no degenerado en cada variable:*

$$\begin{aligned} &si \quad e_n(S,T)=1 \quad \forall T \in E[n], \quad entonces \quad S=\mathcal{O} \\ &si \quad e_n(S,T)=1 \quad \forall S \in E[n], \quad entonces \quad T=\mathcal{O} \end{aligned}$$

3. $e_n(S,S) = 1,\ \forall S \in E[n]$.
4. $e_n(T,S) = e_n(S,T)^{-1},\ \forall S,T \in E[n]$.
5. *$e_n(\sigma(S),\sigma(T)) = \sigma(e_n(S,T))$ para todos los automorfismos σ de $\overline{\mathbb{F}}_q$ tales que σ es la función identidad en los coeficientes de la curva elíptica (si está en la forma de Weierstrass esto significa que $\sigma(A) = A$ y $\sigma(B) = B$).*
6. *$e_n(\alpha(S),\alpha(T)) = e_n(S,T)^{gr(\alpha)}$ para todos los endomorfismos α (incluido el de Frobenius).*

Observación. *Notar que de la bilinealidad de e_n se deduce en particular que*

$$e_n(aS,bT) = e_n(aS,T)^b = e_n(baS,T) = e_n(S,T)^{ba} = e_n(S,T)^{ab}$$

El pairing de Weil se puede describir a través de una función bilineal que asocia una raíz n-ésima de la unidad dados dos puntos de n-torsión.

Corolario. *Sea $\{T_1,T_2\}$ una base de $E[n]$. Entonces $e_n(T_1,T_2)$ es una raíz n-ésima primitiva de la unidad.*

Demostración. Supongamos que $e_n(T_1,T_2) = \zeta$ con $\zeta^d = 1$. Entonces $e_n(T_1,dT_2) = 1$. También se tiene $e_n(dT_1,T_2) = 1$ (por la observación anterior). Sea $S \in E[n]$. Entonces $S = aT_1 + bT_2$ para algunos $a,b \in \mathbb{Z}$. Por lo tanto,

$$e_n(S,dT_2) = e_n(T_1,dT_2)^a e_n(T_2,dT_2)^b = 1$$

Como esto se cumple para todo S, 2 implica que $dT_2 = \mathcal{O}$, y como esto ocurre si y solo si $n|d$, se sigue que ζ es una raíz n-ésima primitiva de la unidad. □

El grado de inmersión de un entero en un cuerpo finito es un pilar fundamental de este ataque.

Lema. *Sea n un divisor primo del cardinal $m = \#E(\mathbb{F}_q)$ y tal que $mcd(n,q) = 1$. Existe un $d \in \mathbb{Z}$ positivo que verifica las condiciones equivalentes:*

1. $n|(q^d-1)$
2. $\mathbb{F}_{q^d}^{\times}$ *contiene un subgrupo cíclico de orden n.*

Demostración. El grupo $\mathbb{F}_{q^d}^{\times}$ es cíclico, con cardinal q^d-1. Tal grupo contiene a un subgrupo de cardinal n si, y solamente si, $n|(q^d-1)$, es decir, $q^d \equiv 1 \pmod{n}$. Ahora bien, por hipótesis, $mcd(n,q) = 1$, y por tanto, $q \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. El orden d de q en tal grupo es una solución al problema. □

Definición. El mínimo d verificando el lema anterior se denomina *grado de inmersión* de $E(\mathbb{F}_q)$ respecto a n. Si n es el mayor divisor primo de m, entonces se dice simplemente que d es el grado de inmersión de $E(\mathbb{F}_q)$.

Ejemplo. *Sea $E : y^2 = x^3 + 2$ una curva elíptica definida sobre $\mathbb{F}_{89}$, y tal que $\#E(\mathbb{F}_{89}) = 90$. El punto $P = (20,9)$ pertenece a la curva y tiene orden 5. Para calcular el grado de inmersión de $E(\mathbb{F}_{89})$ respecto a 5, hay que encontrar el mínimo d tal que $5|89^d - 1$. No se verifica para $d = 1$, pero para $d = 2$, $89^2 - 1 = 5 \cdot 1584$. Luego $E(\mathbb{F}_{89})$ tiene grado de inmersión 2 respecto a 5. Además, 5 es el mayor divisor primo de 90, entonces se puede decir que 2 es el grado de inmersión de la curva.*

Lema. *Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$ y se asume que $mcd(n,q) = 1$. Sea d el grado de inmersión del entero n en $E(\mathbb{F}_q)$. Suponiendo que $d > 1$, entonces $E[n] \subset E(\mathbb{F}_{q^d})$.*

Demostración. Es suficiente con probar que una base de $E[n]$ está contenida en $E(\mathbb{F}_{q^d})$.

Sea $P \in E(\mathbb{F}_q)$ un punto de orden n (se sabe que existe tal punto porque n es un factor primo del cardinal de la curva) y se elige un $T \in E[n]$ tal que $\{P,T\}$ forme una base para $E[n]$. Como es habitual, ϕ_q denotará al endomorfismo de Frobenius. El objetivo es probar que $\phi_{q^d}(T) = T$, porque esto implicaría que $T \in E(\mathbb{F}_{q^d})$. Ya se sabe por lo visto anteriormente que para el endomorfismo de Frobenius se cumple que $\phi_q(P) = P$ ya que $P \in E(\mathbb{F}_q)$ y $\phi_q(T) = a \cdot P + b \cdot T$ para ciertos $a, b \in \mathbb{Z}/n\mathbb{Z}$.

Como $\{P,T\}$ forma una base para $E[n]$, el pairing de Weil $e_n(P,T)$ es una raíz n-ésima primitiva de la unidad, como en el corolario anterior. Por las propiedades del pairing de Weil, se satisface que

$$e_n(P,T)^q = \phi_q(e_n(P,T)) = e_n(\phi_q(P), \phi_q(T)) = e_n(P, a \cdot P + b \cdot T) = e_n(P,P)^a e_n(P,T)^b = e_n(P,T)^b$$

El hecho de que $e_n(P,T)$ sea una raíz n-ésima primitiva de la unidad implica que $b \equiv q \pmod{n}$. Por lo tanto,

$$\begin{aligned} \phi_q(T) &= a \cdot P + q \cdot T \\ \phi_q(\phi_q(T)) &= a \cdot P + q(a \cdot P + q \cdot T) \\ &= a \cdot P + qa \cdot P + q^2 \cdot T \\ \underbrace{(\phi_q \circ \ldots \circ \phi_q)}_{d}(T) &= (a(1 + q + \ldots + q^{d-1})) \cdot P + q^d \cdot T \end{aligned}$$

pero d es el grado de inmersión n en $E(\mathbb{F}_q)$, así que $q^d \equiv 1 \pmod{n}$ y además también se tiene que $1 + q + q^2 + \ldots + q^{d-1} \equiv 0 \pmod{n}$.

Esta última congruencia se debe a que $q^d - 1 = (q-1)(1 + q + q^2 + \ldots + q^{d-1})$ y n primo no divide a $q - 1$ pero sí a $q^q - 1$. El razonamiento anterior implica que $\phi_{q^d}(T) = T$.

Por lo tanto, la base de $E[n]$ dada por $\{P,T\}$ está contenida en $E(\mathbb{F}_{q^d})$ y entonces $E[n] \subset E(\mathbb{F}_{q^d})$. □

Algoritmo del ataque de MOV

1. Se elige un punto aleatorio $T \in E(\mathbb{F}_{q^d})$ donde d es el grado de inmersión de n en $E(\mathbb{F}_q)$.
2. Se calcula el orden m de T.
3. Se calcula $\frac{m}{n}$. Si $n \nmid m$, se vuelve al paso 1.
4. Se calcula $T_1 = (m/n)T$. Entonces T_1 tiene orden n. Como n es primo esto significa que $T_1 \in E[n]$.
5. Se calcula $\zeta_1 = e_n(Q, T_1)$ y $\zeta_2 = e_n(P, T_1)$. Entonces, ambas $\zeta_1, \zeta_2 \in \mu_n \subseteq \mathbb{F}_{q^d}^{\times}$.
6. Se resuelve el problema del logaritmo discreto $\zeta_2 = \zeta_1^k$ en $\mathbb{F}_{q^d}^{\times}$. Esto da una solución $k \pmod{n}$.

Observación. *El elemento $e_n(P,T)$ tiene orden n.*

El grado de inmersión d de n en $E(\mathbb{F}_q)$ determina la complejidad del ataque de MOV. Entonces, si este es razonablemente pequeño, el ataque produce una ventaja computacional para resolver ECDLP.

4.4. Ataque de Smart

Otra posibilidad de curvas elípticas débiles son aquellas tales que $\#E(\mathbb{F}_p) = p$, con p un número primo, o lo que es lo mismo, aquellas para las que la traza de Frobenius es 1. Sin embargo, describir este ataque requiere un contexto adicional. Se pueden definir curvas elípticas sobre los siguientes cuerpos definidos a continuación. Esto permitirá reducir ECDLP al grupo $\mathbb{Z}/p\mathbb{Z}$, donde se calcula fácilmente.

Definición. Un *número p-ádico* se puede representar como una serie infinita de la siguiente forma

$$c_{-n}p^{-n} + \ldots + c_0 + c_1 p + \ldots + c_m p^m + \ldots \quad c_i \in \mathbb{F}_p, \forall i$$

El cuerpo de los números p-ádicos se escribe como $\mathbb{Q}_p$ y aquellos que no tienen potencias negativas de p (i.e. $c_i = 0, \forall i < 0$) se conocen como los enteros p-ádicos y se denotan por $\mathbb{Z}_p$.

El siguiente lema se usará para 'levantar' elementos de $\mathbb{F}_p$ a $\mathbb{Q}_p$.

Lema (Lema de Hensel)**.** *Para $f(X) \in \mathbb{Z}[X]$, sea x tal que $f(x) \equiv 0 \pmod{p^s}$ y sea f' invertible módulo p. Entonces, se puede construir un x' que cumpla que $x' \equiv x \pmod{p^s}$ y $f(x') \equiv 0 \pmod{p^{s+1}}$.*

Otra componente importante de este ataque es la reducción de una curva elíptica módulo p. Esto se basa principalmente en tomar los coeficientes y puntos de la curva y trabajar con sus congruencias módulo el primo p.

Sea $E(\mathbb{Q}_p)$ una curva elíptica definida sobre el cuerpo p-ádico. Se establece una nueva curva sobre $\mathbb{F}_p$ reduciendo los coeficientes de $E(\mathbb{Q}_p)$ módulo p. Previamente, se puede suponer que los puntos de la curva elíptica se encuentran en $E(\mathbb{Z}_p)$, ya que al realizar común denominador sobre las coordenadas proyectivas, los denominadores 'desaparecen'. La única restricción impuesta es que al menos una de las coordenadas no debe ser múltiplo de p.

Se debería comprobar que esta nueva curva no es singular calculando el discriminante y viendo que no es cero, pero simplemente va a ser asumido.

Se sigue un proceso muy similar para los puntos de la curva elíptica, donde cada una de sus coordenadas se reduce módulo p.

Así se establece un homomorfismo de grupos de $E(\mathbb{Q}_p)$ a $E(\mathbb{F}_p)$. Si se denota $E_1(\mathbb{Q}_p)$ al núcleo de este homomorfismo, se tiene que $E_1(\mathbb{Q}_p)$ contiene todos los puntos de $E(\mathbb{Q}_p)$ que se reducen al punto del infinito en $E(\mathbb{F}_p)$.

$$\begin{array}{ccc} E(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{F}_p) \\ Q & \longmapsto & \overline{Q} \\ pQ & \longmapsto & p\overline{Q} = \mathscr{O} \end{array}$$

esto último se debe a la hipótesis de que $\#E(\mathbb{F}_p) = p$ por lo que $pQ \in E_1(\mathbb{Q}_p)$.

De forma similar, se construye otro grupo al que se le llamará $E_2(\mathbb{Q}_p)$ de tal manera que al hacer el cociente entre ambos se obtiene un isomorfismo $E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p) \cong \mathbb{Z}/p\mathbb{Z}$.

Definición. El *logaritmo elíptico p-ádico* ψ_p es un morfismo de $E_1(\mathbb{Q}_p)$ a $\mathbb{Z}/p\mathbb{Z}$ cuyo núcleo es $E_2(\mathbb{Q}_p)$ que se calcula como

$$\psi_p(S) = -\frac{x(S)}{y(S)}$$

para $S \in E_1(\mathbb{Q}_p)$ donde $x(S)$ e $y(S)$ denotan la primera y segunda coordenada del punto S, respectivamente.

Hay que recordar que se está tratando de encontrar k tal que $P = kQ$ donde $P, Q \in E(\mathbb{F}_p)$ y $\#E(\mathbb{F}_p) = p$. El primer paso es hallar $P', Q' \in E(\mathbb{Q}_p)$. Esto se hace estableciendo la coordenada x de Q' igual a la coordenada x de Q. Ahora, se utiliza el lema de Hensel descrito arriba para calcular la segunda coordenada en $\mathbb{Q}_p$ teniendo en cuenta la ecuación de la curva elíptica donde x está fijo. Se sabe que

$P' - kQ' \in E(\mathbb{Q}_p)$ se reduce módulo p al punto del infinito y por tanto está en $E_1(\mathbb{Q}_p)$. Si se multiplica por p, se obtiene que $pP' - k(pQ') \in E_1(\mathbb{Q}_p)$. Por lo tanto,

$$\psi_p(pP') - k\psi_p(pQ') \in \mathbb{Z}/p\mathbb{Z}, \quad k = \frac{\psi_p(pP')}{\psi_p(pQ')}$$

Por último, se reduce k módulo p para volver a $\mathbb{F}_p$, resolviendo ECDLP.

Bibliografía

[1] S. CHAND & M. KUMAR, *Pairing-Friendly Elliptic Curves: Revisited Taxonomy, Attacks and Security Concern*, Jawaharlal Nehru University, https://arxiv.org/pdf/2212.01855

[2] A. J. MENEZES, T. OKAMOTO & S. A. VANSTONE, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory, vol. 39, no. 5, 1993, pp. 1639-1646, https://doi.org/10.1109/18.259647

[3] P. NOVOTNEY, *Weak Curves in Elliptic Curve Cryptography*, 2010, https://wstein.org/edu/2010/414/projects/novotney.pdf

[4] S. POHLIG & M. HELLMAN, *An improved algorithm for computing logarithms over GF*(p) *and its cryptographic significance (Corresp.)*, IEEE Transactions on Information Theory, vol. 24, no. 1, 1978, pp. 106-110, https://doi.org/10.1109/TIT.1978.1055817

[5] R. SCHOOF, *Elliptic Curves Over Finite Fields and the Computation of Square Roots* mod$P$, Mathematics of Computation, vol. 44, no. 170, 1985, pp. 483–94. JSTOR, https://doi.org/10.2307/2007968

[6] J. H. SILVERMAN & J. TATE, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, Second Printing, 1994.

[7] N. SMART, *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, Cryptology, vol. 12, no. 3, 1999, pp. 193–6. https://doi.org/10.1007/s001459900052

[8] A. SUTHERLAND, *Elliptic Curves*, 2015, https://math.mit.edu/classes/18.783/2015/lectures.html

[9] P. VICIOSO, *Curvas elípticas y aplicaciones a la criptografía*, Trabajo de fin de grado en Matemáticas, Universidad de Zaragoza, 2021, https://zaguan.unizar.es/record/110321/files/TAZ-TFG-2021-3043.pdf

[10] L. C. WASHINGTON, *Elliptic Curves: Number Theory and Cryptography*, Discrete Mathematics and its applications, Series Editor: K. H. Rosen, Chapman & Hall/CRC, Second Edition, University of Maryland, 2008.