UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE INGENIERÍA QUÍMICA

UNIDAD DE INVESTIGACIÓN

INFORME FINAL DEL PROYECTO DE INVESTIGACIÓN

"TEORIA DE LAS CURVAS ELÍPTICAS SOBRE CAMPOS FINITOS Y SU APLICACIÓN EN LA SOLUCIÓN DEL PROBLEMA DE LOGARITMO DISCRETO"

AUTOR: Santos Pantaleón Rodríguez Chuquimango

PERIODO DE EJECUCIÓN: Del 01 de Julio del 2016 al 30 de Junio del 2018

Resolución de aprobación N° 593-2016-R

Callao, 2018

INDICE

1.1. TABLA DE GRÁFICOS

II. RESUMEN

El propósito de este trabajo de investigación es la presentación de la teoría fundamental de las curvas elípticas sobre campos finitos y su aplicación en la solución del problema del logaritmo discreto.

En el marco teórico presentamos la definición de grupos, campos, campos finitos, curvas elípticas y sus principales propiedades especialmente las que son necesarias en la solución del problema del logaritmo discreto. Luego presentamos algunos apuntes sobre criptografía, disciplina que consiste en crear e implementar algoritmos para encriptar mensajes que sean muy difíciles o imposibles de descifrar por un interceptador de mensajes.

El problema del logaritmo discreto, al igual que el problema de factorización entera de números grandes es un problema difícil. Ambos problemas son útiles para sistemas criptográficos. En el marco teórico presentamos los diferentes algoritmos que existen para resolver el problema del logaritmo discreto sobre campos finitos tales como: Fuerza bruta, Index-Cálculus, el algoritmo the Baby-Giant step.

En el capítulo de resultados presentamos la solución del problema de logaritmo discreto sobre curvas elípticas haciendo uso del algoritmo de Pohlig-Hellman y el algoritmo rho de Pollard. Para aplicaciones criptográficas se establece que los parámetros de la curva elíptica deben ser escogidos muy grandes a fin de que la solución del problema de logaritmo discreto sea muy difícil y así garantizar la seguridad del algoritmo criptográfico.

ABSTRACT

The purpose of this research work is the presentation of the fundamental theory of elliptic curves on finite fields and its application in the solution of the discrete logarithm problem. In the theoretical framework we present the definition of groups, fields, finite fields, elliptic curves and their main properties, especially those that are necessary in the solution of the discrete logarithm problem. Then we present some notes on cryptography, a discipline that consists of creating and implementing algorithms to encrypt messages that are very difficult or impossible to decipher by a message interceptor.

The problem of the discrete logarithm, as well as the problem of the whole factorization of large numbers, is a difficult problem. Both problems are useful for cryptographic systems. In the theoretical framework we present the different algorithms that exist to solve the problem of the discrete logarithm over finite fields such as: Brute force, Index-Calculus, the algorithm the Baby-Giant step.

In the results chapter we present the solution of the discrete logarithm problem on elliptic curves using the Pohlig-Hellman algorithm and the Pollard rho algorithm. For cryptographic applications it is established that the parameters of the elliptic curve must be chosen very large so that the solution of the discrete logarithm problem is very difficult and thus guarantee the security of the cryptographic algorithm.

Key Word: Discrete logarithm.

III. INTRODUCCION

3.1. Planteamiento del problema de investigación

El estudio Ecuaciones Diofánticas, es decir ecuaciones cuyas soluciones están en el conjunto de números enteros, o alternativamente en los racionales ha fascinado a investigadores desde tiempos antiguos. Según J. W CASSELS, Lectures on Elliptic curves, pag. 1, una tabla babilónica que data entre los 1600 y 1900 D.C listó 15 soluciones de la ecuación Pitagórica

$$X^2 + Y^2 = Z^2$$

Las curvas elípticas son un caso especial de ecuaciones Diofánticas. 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 test de primalidad, la factorización de números enteros o la demostración del último teorema de Fermat, entre otras.

En criptografía de clave pública se hace uso de funciones unidireccionales, que son funciones $y = f(x)$ sencillas de evaluar, pero difíciles de calcular su inversa $x = f^{-1}(y)$. Una de las funciones unidireccionales más usadas y estudiadas es la exponencial discreta. Dado un grupo cíclico G de orden p y uno de sus elementos, g, podemos definir la operación exponencial $f_g(x) = g^x$ para todo $x = 0, \dots, p-1$. Existen algoritmos de exponenciación rápida que pueden hacer este cálculo (dados g, x) en tiempos aceptables para grupos de orden p muy grande. Ahora, si tenemos $h = g^x$ los cálculos necesarios para obtener x requieren un tiempo exponencial de ejecución. La operación, $x = f_g^{-1}(h)$, se llama logaritmo discreto en base g de h. Su dificultad radica en la naturaleza cíclica de la operación definida en G y es la base de muchos algoritmos criptográficos.

¿Se puede usar la teoría de curvas elípticas sobre campos finitos para resolver el problema de logaritmo discreto?

3.2. Objetivos

3.2.1. Objetivo general

Desarrollar la teoría de curvas elípticas sobre campos finitos para resolver el problema de logaritmo discreto.

3.2.2. Objetivos específicos

a) Desarrollar la teoría de curvas elípticas sobre campos finitos.
b) Resolver el problema de logaritmc discreto para curvas elípticas usando aritmética modular.

3.3. Importancia y justificación de la investigación

3.3.1. Importancia.

La investigación es importante porque se trata de la teoría de curvas elípticas que ha sido tema de investigación de grandes científicos e investigadores en todos los tiempos. Actualmente es un tema de gran interés en investigadores de teoría de números, geometría algebraica y Criptografía.

3.3.2. Justificación.

Existen algoritmos que usan la teoría modular para resolver el problema de logaritmo discreto en un tiempo sub exponencial de ejecución, pero la teoría de curvas elípticas lo hace en tiempo exponencial, lo cual hace más eficaz en la generación de algoritmos para criptografía.

IV. MARCO TEÓRICO

Comenzamos con un resumen de la teoría de grupos y campos presentada por DARREL HANKERSON, ALFRED MENESES, Guide to Elliptic Curve Cryptography, pag. 25-69, necesarios para el desarrollo de nuestra investigación.

4.1. Grupo Abeliano

4.1.1. Definición: (Grupo).

Sea el conjunto $S \neq \emptyset$, una operación binaria en S es una aplicación:

$$*: \begin{matrix} S \times S & \to S \\ (a,b) & \to a * b \end{matrix}$$

Un grupo es un conjunto $G \neq \emptyset$, dotado de una operación binaria $*: G \times G \to G$ que verifica las siguientes propiedades:

i) $a * (b * c) = (a * b) * c$ para todo $a, b, c \in G$

ii) Existe un $e \in G$ llamado elemento neutro, tal que $a * e = e * a = a$ para todo $a \in G$

iii) Dado $a \in G$, existe $a^{-1} \in G$ llamado elemento opuesto, tal que

$$a * a^{-1} = a^{-1}a = e$$

Decimos que G es Abeliano si se cumple que $a * b = b * a$, para todo $a, b \in G$

4.1.2. Propiedades básicas de los grupos:

Sea G un grupo, se tienen las siguientes propiedades:

1) El elemento neutro de G es único
2) El elemento opuesto es único
3) Para todo $a \in G, a^{-1} \in G$, y $(a^{-1})^{-1} = a$
4) Para todo $a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$
5) Dados $a, b \in G$, las ecuaciones $ax = b$, $ya = b$ tienen soluciones únicas para todo $x, y \in G$.
6) Se verifican las leyes de cancelación

$$au = aw \Rightarrow u = w$$

$$ua = wa \Rightarrow u = w$$

7) También se define

i) $a^0 = e$

ii) $a^n = a.a^{n-1}, n \in \mathbb{Z}^+$

iii) $a^{-n} = (a^{-1})^n, n \in \mathbb{Z}^+$

iv) $a^m a^n = a^{m+n} \quad m, n \in \mathbb{Z}$

v) $(a^m)^n = a^{mn} = (a^n)^m, \ m, n \in \mathbb{Z}$

8) Si G es Abeliano denotamos: $e \equiv 0, a^n \equiv na$. Con esta notación se tiene

i) $ma + na = (m + n)a$

ii) $n(ma) = (nm)a$

4.1.3. Sub grupos Cíclicos

Sea G un grupo y $a \in G$, el conjunto

$$\langle a \rangle = \{a^i / \ i \in \mathbb{Z}\}$$

$\langle a \rangle$ es llamado un sub grupo cíclico generado por a. Si existe un $a \in G$ tal que $\langle a \rangle = G$ decimos que G es cíclico.

4.1.4. Sub grupos generados

Sea G un grupo y sea $S \subset G, S \neq \emptyset$ el subgrupo generado por S es el subgrupo denotado y definido por

$$\langle S \rangle = \cap H, H \text{ sub grupo de } G$$

$\langle S \rangle$ es el subgrupo mas pequeño que contiene a S.

4.1.5. Congruencia módulo H

Sea G un grupo y H un subgrupo de G. Definimos la siguiente relación de equivalencia en G.

$$a \sim b \Leftrightarrow a.b^{-1} \in H$$

Esta es una relación de equivalencia, y se llama relación de congruencia módulo H y se denota por

$$a \sim b \Leftrightarrow a \equiv b (mod H)$$

Esta relación determina una partición en G. Es decir se determina un conjunto cociente

$$G/\sim = G/H = \{[a] / \ a \in G\}$$

4.2. Campos finitos

En esta sección presentamos algunos hechos básicos acerca de campos finitos. Otras propiedades serán dadas en el trabajo cuando sea necesario. Campos finitos son abstracciones de sistemas de números familiares (tales como los números

racionales, los números reales y los números complejos) y sus esenciales propiedades. ([1] DARREL HANKERSON, ALFRED MENESES, Guide to Elliptic Curve Cryptography, pag. 25-69).

4.2.1. Definición. (Campo)

Un campo es un conjunto F en el que se definen dos operaciones, de adición (denotado por +) y multiplicación (denotado por ".") que satisfacen las propiedades aritméticas usuales.

i) $(F, +)$ es un grupo abeliano con elemento neutro (aditivo) denotado por 0.
ii) $(F \setminus \{0\}, .)$ Es un grupo con elemento neutro (multiplicativo) denotado por 1.
iii) Se cumplen las propiedades de distribución

$$(a + b).c = a.c + b.c, \text{ para todo } a, b, c \in F$$

Si F es finito, entonces se dice que el campo F es finito.

4.2.2. Sustracción y división

Estas operaciones están definidos en términos de la adición y la multiplicación. La sustracción se define para todo $a, b \in F$, por

$$a - b = a + (-b)$$

donde $-b$ es el único elemento en F tal que $b + (-b) = 0$ ($-b$ es llamado el negativo de b).

Similarmente, la división de un par de elementos del campo está definido en términos de la multiplicación: para todo $a, b \in F$,

$$a/b = a.b^{-1}$$

donde b^{-1} es el único elemento en F tal que $b.b^{-1} = 1$ (b^{-1} es llamado el inverso de b).

4.2.3. Existencia y unicidad

El orden de un campo finito F es el número de elementos en el campo. Existe un campo finito F de orden q si y solamente si q es de potencia prima, es decir, $q = p^m$ donde p es un número primo llamado la característica de F, y m es un entero

positivo. Si $m = 1$, Entonces F es llamado un campo primo. Si $m \geq 2$, entonces F es llamado un campo de extensión. Para cualquier potencia prima q, hay esencialmente solo un campo finito de orden q; informalmente, esto significa que cualesquier dos campos de orden q son estructuralmente lo mismo excepto que la notación usada para representar los elementos del campo puede ser diferente. Se dice que dos campos de orden q son isomorfos y denotamos tales campos por F_q.

4.2.4. Campos primos

Sea p un número primo. Los enteros módulo p consistiendo de los enteros $\{0,1,2,3,\ldots,p-1\}$ con adición y multiplicación módulo p, es un campo finito de orden p. Denotamos este campo por F_p y es llamado los p módulos de F_p.

Para cualquier entero a, $a \bmod p$ denota el único entero residuo $r, 0 \leq r \leq p-1$ obtenido al dividir a por p; esta operación es llamada reducción módulo p.

Ejemplo 4.1.

En el campo primo F_{47} sus elementos son $\{0,1,2,3,\ldots,47\}$. Los siguientes son algunos ejemplos de operaciones aritméticas en F_{47}.

i) Adición: $27 + 20 = 0$, puesto que $47 \bmod 47 = 0$

ii) Sustracción: $27 - 20 = 7$, puesto que $7 \bmod 47 = 7$

iii) Multiplicación: $(27).(20) = 23$, puesto que $540 \bmod 47 = 23$

iv) Inversa: $(27)^{-1} = 7$, puesto que $(27).(7) \bmod 47 = 1$.

4.2.5. Campos finitos binarios

Campos finitos de orden 2^m son llamados campos binarios o campos finitos de característica 2. Una forma de construir F_{2^m} es usar una representación base polinomial. Aquí, los elementos de F_{2^m} son los polinomios binarios (polinomios cuyos coeficientes están en el campo $F_2 = \{0,1\}$) de grado menor o igual que $m-1$.

$$F_{2^m} = \{p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_{m-1} z^{m-1},\ a_i \in \{0,1\}\}$$

Un polinomio binario irreducible $f(z)$ de grado m es escogido (tal polinomio existe para cada m y puede ser hallado eficientemente). Irreducible significa que $f(z)$ no puede ser factorizado como un producto de polinomios binarios cada uno de grado menor que m. Las operaciones de adición y multiplicación de polinomios del campo son las usuales considerando reducción modulo. Para cualesquier polinomio binario $a(z), a(z) \bmod f(z)$ denotará el único polinomio residuo $r(z)$ de grado menor que m obtenido de la division de $a(z)$ por $f(z)$. Esta operación es llamada reducción modulo $f(z)$.

Ejemplo 4.2

Sobre el campo binario F_{2^4}, los elementos son los 16 polinomios binarios de grado a los más 3 son:

$$0, \quad z^2, \quad z^3, \quad z^3 + z^2$$

$$1, \quad z^2 + 1, z^3 + 1, z^3 + z^2 + 1$$

$$z, \quad z^2 + z, \quad z^3 + z, \quad z^3 + z^2 + z$$

$$z + 1, \quad z^2 + z + 1, \quad z^3 + z + 1, \quad z^3 + z^2 + z + 1$$

Los siguientes son algunos ejemplos de operaciones aritméticas en F_{2^4} con reducción polynomial $f(z) = z^4 + z + 1$.

Suma

$$(z^3 + z^2 + z + 1) + (z^3 + 1) = z^2 + z$$

Resta

$$z^3 + z^2 + z + 1) - (z^3 + 1) = z^2 + z$$

Nota: $-1 = 1$ en F_2, se tiene que $-a = a$ para todo $a \in F_{2^m}$

Multiplicación

$$(z^3 + z^2 + z + 1).(z^3 + 1) = z^6 + z^5 + z^4 + z^2 + z + 1 = z^3 + z^2 + z$$

Puesto que el resto de dividir $z^6 + z^5 + z^4 + z^2 + z + 1$ entre $z^4 + z + 1$ es $z^3 + z^2 + z$.

Inverso

$$(z^3 + z^2 + z + 1)^{-1} = z^3$$

puesto que

$$(z^3 + z^2 + z + 1).(z^3)\ mod\ (z^4 + z + 1) = 1$$

4.2.6. Campos isomorfos

Hay tres polinomios binarios irreducibles de grado 4, a saber,

$$f_1(z) = z^4 + z + 1, f_2(z) = z^4 + z^3 + 1, f_3(z) = z^4 + z^3 + z^2 + 1$$

cada uno de estos polinomios reducción pueden ser usados para construir el campo F_{2^4}. Llamamos a los campos resultantes K_1, K_2, K_3. Los elementos de estos campos son los mismos 16 polinomios binarios de grado menor o igual a 3. Superficialmente, estos campos aparecen siendo diferentes, por ejemplo:

$$z^3.z = z + 1, \text{en } K_1,$$

$$z^3.z = z^3 + 1 \text{ en } K_2$$

$$z^3.z = z^3 + z^2 + 1\ en\ K_3$$

Sin embargo, todos los campos de un orden dado son isomorfos, esto es, la diferencia es solamente la representación de los elementos. Un isomorfismo entre $K_1\ y\ K_2$ puede ser construido hallando un $c \in K_2$ tal que $f_1(c) \equiv 0(mod\ f_2)$ y entonces extendiendo $z \to c$ a un isomorfismo $\varphi: K_1 \to K_2$. Los valores para c son

$$z^2 + z,\ \ z^2 + z + 1,\ z^3 + z^2, \text{y } z^3 + z^2 + 1$$

4.2.7. Campos extensión

La representación base polinomial para campos binarios puede ser generalizada a todos los campos de extensión como sigue. Sea p un número primo y $m \geq 2$. Sea $F_p(z)$ denotando el conjunto de todos los polinomios en la variable z con

coeficientes en F_p. Sea $f(z)$, la reducción polinomial irreducible de grado m en $F_p(z)$, tal polinomio existe para cualquier $p.m$, y puede ser eficientemente hallado. Irreducible significa que $f(z)$ no puede ser factorizado como un producto de polinomios en $F_p(z)$ cada uno de grado menor que m. Los elementos de F_{p^m} son los polinomios en $F_p(z)$ de grado a lo mas $m-1$

$$F_{p^m} = \{a_{m-1}z^{m-1} + a_{m-2}z^{m-2} + \cdots + a_2z^2 + a_1z + a_0,\ \ a_i \in F_p\}$$

La suma de los elementos del campo es la suma usual de polinomios con coeficientes aritméticos operados en F_p. La multiplicación de los elementos del campo es calculado modulo el polinomio $f(z)$.

Ejemplo 4.3

Sea $p = 251$ y $m = 5$. El polinomio $f(z) = z^5 + z^4 + 12z^3 + 9z^2 + 7$ es irreducible en $F_{251}(z)$ y puede servir como reducción polinomial para la construcción de F_{251^5}, el campo finito de orden 251^5. Los elementos de F_{251^5} son los polinomios en $F_{251}(z)$ de grado a lo más 4. Los siguientes son algunos ejemplos de operaciones aritméticas en F_{251^5}.

Sea $p(z) = 123z^4 + 76z^2 + 7z + 4,\ q(z) = 196z^4 + 12z^3 + 225z^2 + 76.$

(i) Adición:

$$p(z) + q(z) = 68z^4 + 12z^3 + 50z^2 + 7z + 80$$

(ii) Sustracción:

$$p(z) - q(z) = 178z^4 + 239z^3 + 102z^2 + 7z + 179$$

(iii) Multiplicación:

$$p(z).q(z) = 117z^4 + 151z^3 + 117z^2 + 182z + 217$$

(iv) Inverso:

$$p(z)^{-1} = 109z^4 + 111z^3 + 250z^2 + 98z + 85$$

4.2.8. Sub campos de un campo finito

Un sub conjunto k de un campo K es un sub campo de K, si k es también un campo con las operaciones de K. En este caso se dice que K es una extensión del campo k. Los sub campos de un campo finito pueden ser caracterizados. Un campo finitoF_{p^m} tiene precisamente un sub campo de orden p^l para cada divisor positivo l de m. Los elementos de este sub campo son los elementos $a \in F_{p^m}$ satisfaciendo $a^{p^l} = a$. Recíprocamente, cada sub campo de F_{p^m} tiene orden p^lpara algún divisor positivo l de m.

4.2.9. Bases de un campo finito

El campo finito F_{q^n} puede ser visto como un espacio vectorial sobre su sub campo F_q. Aquí, vectores son los elementos de F_{q^m}; escalares son los elementos de F_q. Adición de vectores es la adición en F_{q^m} , y multiplicación escalar es la multiplicación en F_{q^m} de F_q elementos con elementos de F_{q^m}. El espacio vectorial tiene dimensión n y tiene muchas bases.

Si $B = \{b_1, b_2, \dots, b_n\}$ es una base, entonces $a \in F_{q^n}$ puede ser únicamente determinado por una n-upla $(a_1, a_2, \dots, a_n)$ de elementos de F_q, es decir

$$a = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

Por ejemplo, en la representación base polinomial del campo F_{p^m}, F_{p^m} es un espacio vectorial de dimensión m sobre F_p, y $\{z^{m-1}, z^{m-2}, \dots, z^2, z, 1\}$ es una base para F_{p^m} sobre F_p.

4.2.10. Grupo multiplicativo de un campo finito

Los elementos no nulos de un campo finito F_q, denotado por F_q^*, forman un grupo cíclico bajo la multiplicación. Entonces existen elementos $b \in F_q^*$ llamados generadores tales que $F_q^* = \{b^i : 0 \leq i \leq q-2\}$. El orden de $a \in F_q^*$ es el menor entero positivo t tal que $a^t = 1$. Puesto que F_q^* es un grupo cíclico, se tiene que t es un divisor de $q - 1$.

4.3. Apuntes sobre curvas elípticas

4.3.1. Definición.

Una curva elíptica E sobre un campo K está definida por una ecuación

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

donde $a_1, a_2, a_3, a_4, a_6 \in K$, $\Delta \neq 0$, Δ es el discriminante de E y se define por

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$$

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1a_3$$

$$d_6 = a_3^2 + 4a_6$$

$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

Si L es cualquier extensión del campo K, entonces el conjunto de L-puntos racionales sobre E es

$$E(L) = \{(x, y) \in L: y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$$

donde ∞ es el punto en el infinito.

Observaciones. (Comentarios de la definición)

i) La ecuación de la definición es llamada ecuación de Weierstrass

ii) Decimos que E está definida sobre K puesto que los coeficientes $a_1, a_2, a_3, a_4, a_6 \in K$. A veces se escribe $E/_K$ para indicar que E está definida sobre K. Y K es llamado el campo subyacente. Note que si E es definida sobre K, entonces E también está definida sobre cualquier extensión de K.

iii) La condición $\Delta \neq 0$ asegura que la curva elíptica es "suave", es decir, no existen puntos en los que la curva tiene dos o más distintas rectas tangentes.

iv) El punto ∞ es el único punto sobre la recta en el infinito que satisface la forma proyectiva de la ecuación de Weierstrass.

4.3.2. Simplificación de la ecuación de Weierstrass

Dos curvas elípticas E_1 y E_2 definidas sobre K dadas por las ecuaciones

$$E_1: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$E_2: y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

Se dice que son isomorfas sobre K si existen $u, r, s, t \in K, u \neq 0$, tales que el cambio de variables

$$(x, y) \rightarrow (u^2x + r, u^3y + u^2sx + t)$$

transforma la ecuación E_1 en la ecuación E_2. ([1] DARREL HANKERSON, ALFRED MENESES, Guide to Elliptic Curve Cryptography, pag. 78-79.)

1) Si la característica de K es diferente de 2 ó 3, entonces el cambio de variables

$$(x, y) \rightarrow \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right)$$

transforma E en la curva

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

Donde $a, b \in K$, el discriminante de la curva es $\Delta = -16(4a^3 + 27b^2)$

2) Si la característica de K es 2, hay dos casos a considerar. Si $a_1 \neq 0$, entonces el cambio de variables

$$(x, y) \rightarrow \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right)$$

transforma E en la curva

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

Donde $a, b \in K$, tal curva es no super singular y tiene como discriminante, $\Delta = b$.

Si $a = 0$, entonces el cambio de variables

$$(x, y) \rightarrow (x + a_2, y)$$

Transforma E en la curva

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

Donde $a, b, c \in K$, tal curva es super singular y tiene como discriminante $\Delta = c^4$

3) Si la característica de K es 3, entonces hay dos casos a considerar.

Si $a_1^2 \neq -a_2$, entonces el cambio de variable

$$(x, y) \to \left(x + \frac{d_4}{d_2}, y + a_1 x + a_1 \frac{d_4}{d_2} + a_3\right)$$

Donde $d_2 = a_1^2 + a_2$ y $d_4 = a_4 - a_1 a_3$, transforma E en la curva

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

Donde $a, b, \in K$, tal curva se dice que es no supersingular y tiene discriminante $\Delta = -a^3 b$.

Si $a_1^2 = -a_2$, entonces el cambio de variable

$$(x, y) \to (x, y + a_1 x + a_3)$$

transforma E en la curva

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

Donde $a, b, \in K$. Tal curva es llamada supersingular y tiene discriminante $\Delta = -a^3$.

4.3.3. Ecuación de Weierstrass reducida

Consideremos la ecuación de Weierstrass en forma reducida

$$y^2 = x^3 + Ax + B$$

O en coordenadas homogéneas

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

La ecuación en el lado derecho no tiene raíces con multiplicidad si

$$4A^3 + 27B^2 \neq 0$$

El punto racional especificado es $\mathcal{O} = (0,0,1)$ en el infinito. Puesto que la recta en el infinito en una tangente inflexional en $\mathcal{O}$. La ley de grupo sobre C es especialmente simple.

Si $P = (x, y) \in C$, el punto $-P = (x, -y)$.

Veremos que esta forma canónica es particularmente conveniente cuando el campo es $\mathbb{Q}$. Cuando el campo es característica 2 o 3, no podemos usar la forma canónica en su lugar usamos

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

Una curva elíptica es una curva que es también naturalmente un grupo. La ley de grupo es construida geométricamente.

Curvas elípticas no tienen nada que ver con elipses. Curvas elípticas aparecen en diversas áreas de matemáticas, teoría de números y análisis complejo, y criptografía.

4.3.4. Puntos sobre curvas elípticas

Curvas elípticas pueden tener puntos con coordenadas en cualquier campo, tales como $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}$ *o* $\mathbb{C}$. Curvas elípticas con puntos en $\mathbb{F}_p$ son grupos finitos.

Una curva elíptica en su forma simple es una curva dada por una ecuación de la forma

$$y^2 = x^3 + Ax + B$$

Donde se requiere que el discriminante $\triangle = 4A^3 + 27B^3$ sea diferente de cero. Equivalentemente, el polinomio $x^3 + Ax + B$ tiene raíces distintas. Además necesitamos un punto extra, $\mathcal{O}$, un punto en el infinito, así, E es el conjunto

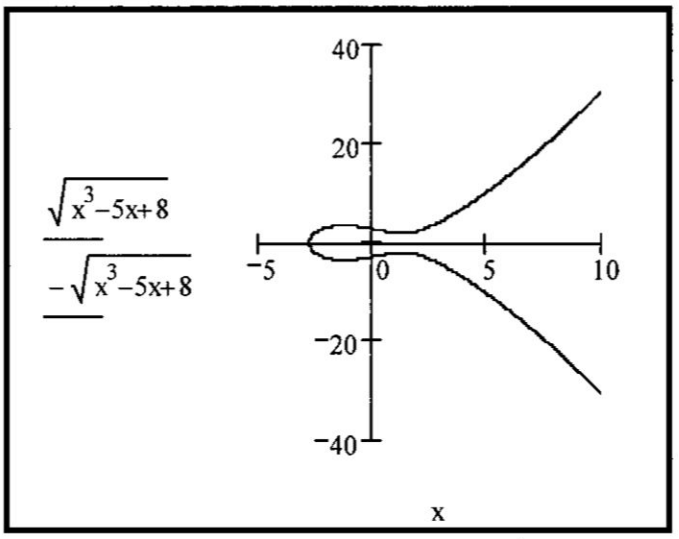
$$E = \{(x, y): y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

4.3.5. Geometría de curvas elípticas

La curva elíptica dada por $y^2 = x^3 + Ax + B$ es simétrica con respecto al eje X. Así por ejemplo la gráfica de $E: y^2 = x^3 - 5x + 8$ se presenta en el gráfico 4.1.

GRÁFICO 4.1.

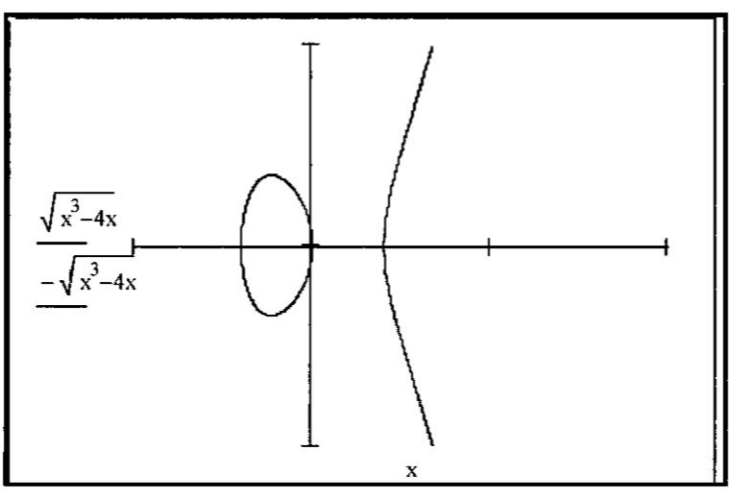
CURVA ELÍPTICA E: $y^2 = x^3 - 5x + 8$:



Fuente: elaboración propia con el software mathcad.

GRÁFICO 4.2.

CURVA ELÍPTICA: $y^2 = x^3 - 4x$



Fuente: elaboración propia con el software mathcad.

4.3.6. Algebra de curvas elípticas

La ley de adición sobre E tiene las siguientes propiedades:

a) $P + \mathcal{O} = \mathcal{O} + P = P$, para todo $P \in E$

b) $P + (-P) = \mathcal{O}$, para todo $P \in E$

c) $P + (Q + R) = (P + Q) + R$, para todo, $P, Q, R \in E$

d) $P + Q = Q + P$, para todo $P, Q \in E$

En otras palabras, la ley de adición +, con E forma un grupo conmutativo.

La prueba de todas las propiedades es fácil excepto la ley asociativa, la cual puede ser verificada usando métodos algebraicos o analíticos.

4.3.7. Fórmulas para la adición

Supongamos que deseamos sumar los puntos

$$P_1 = (x_1, y_1) \quad \text{y} \quad P_2 = (x_2, y_2)$$

Sobre la curva elíptica

$$E: y^2 = x^3 + Ax + B$$

La recta que pasa por los puntos dados es

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

Explícitamente, la pendiente y el intercepto con el eje y de L están dados por

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, \text{ si } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1}, \text{si } P_1 = P_2 \end{cases} \qquad y \qquad \nu = y_1 - \lambda x_1$$

Hallando la intersección de L con E se tiene

$$(\lambda x + \nu)^2 = x^3 + Ax + B$$

Conocemos que x_1 y x_2 son soluciones, podemos hallar la tercera solución x_3 comparando los dos lados de

$$x^3 + Ax + B - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3)$$

$$= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3$$

Igualando los coeficientes de x^2, tenemos

$$-\lambda^2 = -x_1 - x_2 - x_3$$

Es decir

$$x_3 = \lambda^2 - x_1 - x_2$$

Luego calculamos y_3, usando $y_3 = \lambda x_3 + v$. Finalmente

$$P_1 + P_2 = (x_3, -y_3).$$

4.3.8. Algoritmo para la adición sobre E

Algoritmo de adición para $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ sobre la curva elíptica

$$E: y^2 = x^3 + Ax + B$$

i) Si $P_1 \neq P_2$ y $x_1 = x_2$, entonces $P_1 + P_2 = \mathcal{O}$.

ii) Si $P_1 = P_2$ y $y_1 = 0$, entonces $P_1 + P_2 = 2P_1 = \mathcal{O}$.

iii) Si $P_1 \neq P_2$ $(x_1 \neq x_2)$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad y \quad v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

iv) Si $P_1 = P_2$ (donde $y_1 \neq 0$)

$$\lambda = \frac{3x_1^2 + A}{2y_1} \quad y \quad v = \frac{-x^3 + Ax + 2B}{2y}$$

Entonces

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - v)$$

Observaciones:

i) La coordenada x de $P_1 + P_2$ se denota y define por

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

ii) Similarmente, si $P = (x, y)$ entonces la coordenada x de $2P$ está dada por

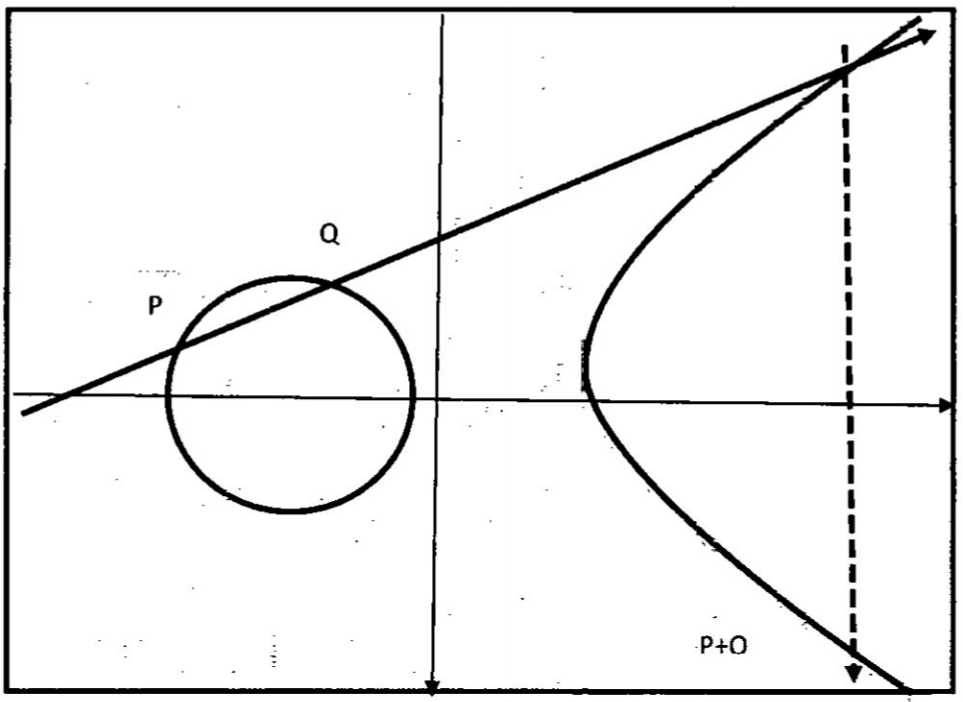
$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

iii) Si A y B están en el campo K y si P_1 y P_2 tienen coordenadas en K, entonces $P_1 + P_2$ y $2P_1$ también tienen coordenadas en K.

4.3.9. Representación gráfica de las operaciones

GRÁFICO 4.3.

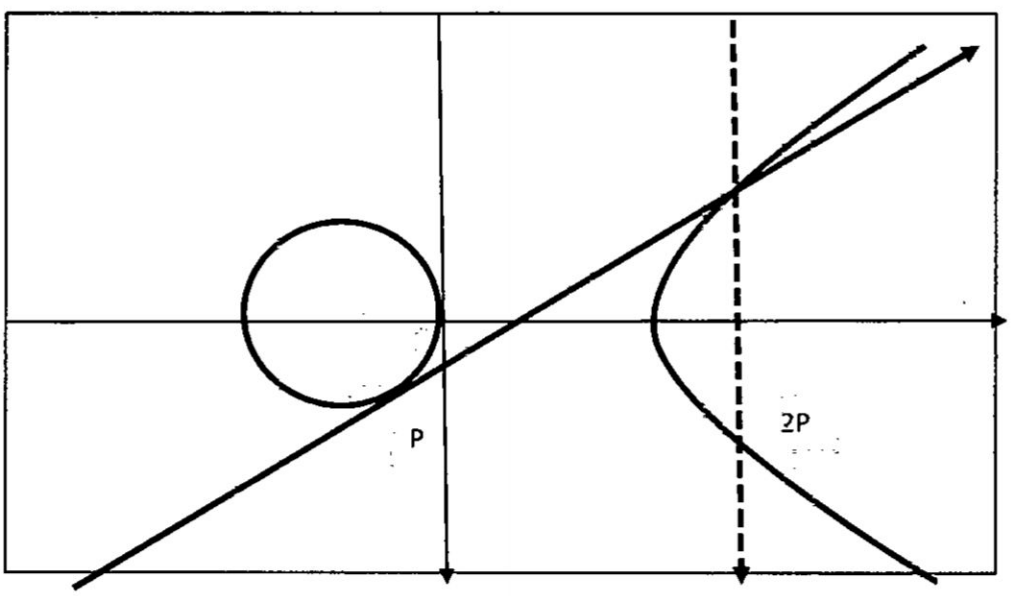
ADICIÓN DE PUNTOS SOBRE CURVAS ELÍPTICAS



Fuente: Elaboración propia.

GRÁFICO 4.4

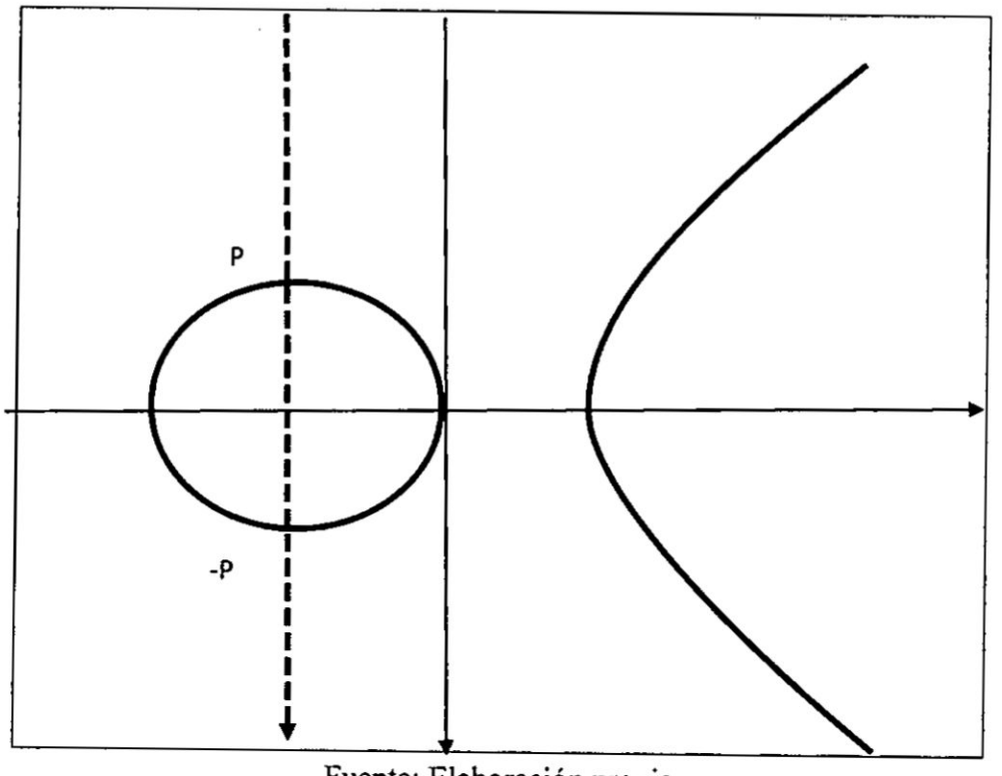
DUPLICACIÓN DE UN PUNTO



Fuente: Elaboración propia.

GRÁFICO 4.5

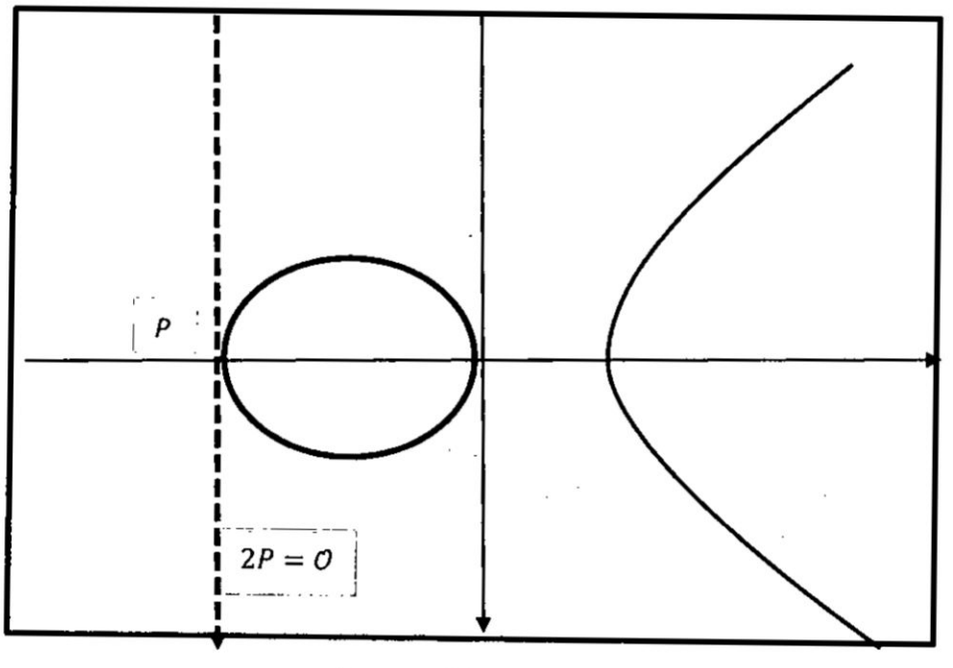
ELEMENTO OPUESTO



Fuente: Elaboración propia.

GRÁFICO 4.6

PUNTO DE ORDEN 2



Fuente: Elaboración propia.

La representación gráfica presentada está en el conjunto de los números Reales. Sin embargo, las aplicaciones criptográficas se trabajan en campos finitos, cuya gráfica no es como en $\mathbb{R}$.

4.3.10. Representación en un campo finito

Para ilustrar la representación de los puntos de una curva elíptica sobre un campo finito consideremos la curva dada por

$$E: y^2 = x^3 - 5x + 8 \pmod{37}$$

Considere los puntos

$$P = (6,3) \in E(\mathbb{F}_{37}) \; y \; Q = (9,10) \in E(\mathbb{F}_{37})$$

Usando las fórmulas para la adición en $E(\mathbb{F}_{37})$ se tiene

$$2P = (35,11), \; 3P = (34,25), \; P + Q = (11,10)$$

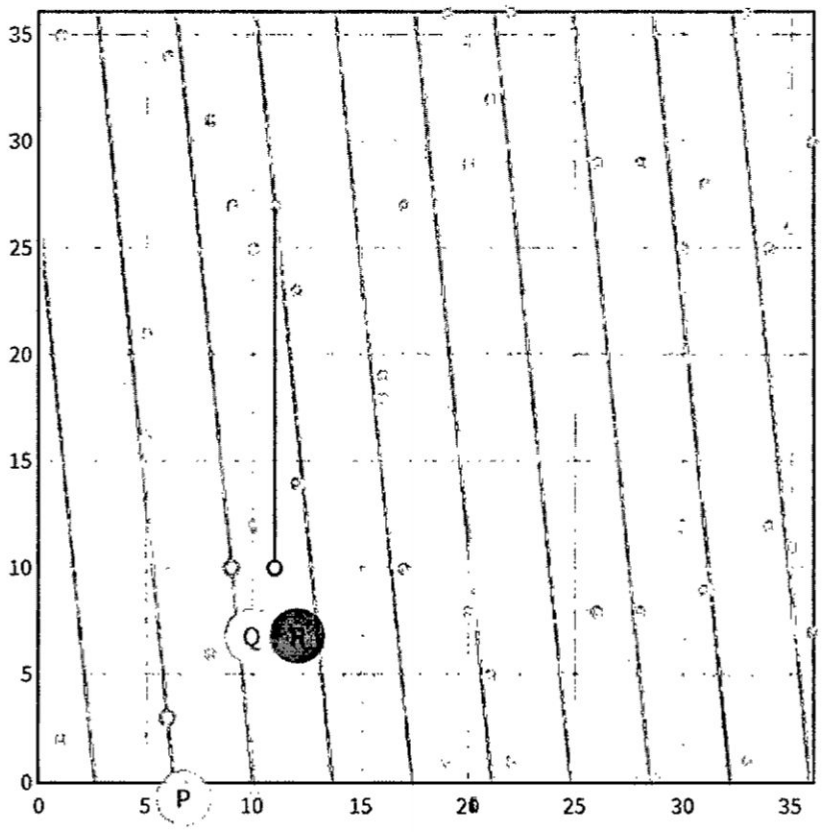
Número de puntos en $E(\mathbb{F}_{37})$: Sustituyendo cada valor de $x \in \{0,1,2,,3,\cdots,36\}$ y verificando que $x^3 - 5x + 8$ sea un cuadrado módulo 37, se tiene que $E(\mathbb{F}_{37})$ consiste de los siguientes 45 puntos.

$$(1, \pm 2), (5, \pm 21), (6, \pm 3), (8, \pm 6),$$
$$(9, \pm 27), (10, \pm 25), (11, \pm 27),$$
$$(12, \pm 23), (16, \pm 19), (17, \pm 27),$$
$$(19, \pm 1), (20, \pm 8), (21, \pm 5),$$
$$(22, \pm 1), (26, \pm 8), (28, \pm 8),$$
$$(30, \pm 25), (31, \pm 9), (33, \pm 1),$$
$$(34, \pm 25), (35, \pm 26), (36, \pm 7), O$$

En el gráfico 4.7 se muestra los puntos de la curva $y^2 = x^3 - 5x + 8 \pmod{37}$.

Gráfico 4.7.

GRÁFICA DE PUNTOS EN UN CAMPO FINITO



Fuente: Elaboración propia con la herramienta visual **HTML5/JavaScript visual tool**.

4.3.11. Cálculo del múltiplo de un punto

Para el uso del grupo finito $E(\mathbb{F}_p)$ por Diffie-Hellman, por ejemplo, se necesita que p sea muy grande ($p > 2^{160}$) y se necesita computar

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ veces}} \in E(\mathbb{F}_p)$$

para un valor grande de m.

Se puede computar mP en $O(\log m)$ pasos usando el método usual de duplicaciones y sumas. Podemos escribir

$$m = m_0 + m_1.2 + m_2 2^2 + \cdots + m_r 2^r, \quad \text{con } m_0, \cdots, m_r \in \{0,1\}$$

Entonces mP puede ser computado como

$$mP = m_0P + m_1.2P + m_2 2^2 P + \cdots + m_r 2^r P$$

Donde $2^k P = 2.2 \ldots 2P$ requiere solamente k duplicaciones.

Así en promedio, se necesita aproximadamente $\log_2(m)$ duplicaciones y $\frac{1}{2}\log_2(m)$ adiciones al computar mP.

Hay una forma simple de reducir el tiempo de cómputo aún más. Como se necesita la misma cantidad de tiempo para restar dos puntos cuando se suma, podemos en lugar de esto observar una expansión ternaria de m,

$$m = m_0 + m_1.2 + m_2 2^2 + \cdots + m_r 2^r, \quad \text{con } m_0, \cdots, m_p \in \{-1,0,1\}$$

En promedio, esto puede ser hecho aproximadamente con 2/3 los m_i igual a cero, que reduce el promedio del número de adiciones a $\frac{1}{3}\log_2(m)$.

Así por ejemplo, para $n = 151$ la representación binaria es

$$151 = 10010111_2 = 1.2^7 + 0.2^6 + 0.2^5 + 1.2^4 + 0.2^3 + 1.2^2 + 1.2^1 + 0.2^0$$

Luego

$$151P = 2^7P + 2^4P + 2^2P + 2^1P + P$$

Una forma para calcular 151P sería:

Tomar P

- Duplicar P para tener 2P
- Sumando se tiene $2^1P + P$
- Duplicar 2P para tener 2^2P
- Sumando el resultado anterior tenemos $2^2P + 2^1P + P$
- Duplicamos 2^2P y obtenemos 2^3P
- Duplicamos 2^3P y obtenemos 2^4P
- Añadimos el resultado anterior y tenemos $2^4P + 2^2P + 2^1P + P$
- Duplicamos 2^4P y obtenemos 2^5P
- Duplicamos 2^5P y obtenemos 2^6P
- Duplicamos 2^6P y obtenemos 2^7P

- Añadimos a la suma anterior y obtenemos

$$2^7P + 2^4P + 2^2P + 2^1P + P = 151P$$

4.3.12. Orden de un grupo

Sea E una curva elíptica definida sobre F_q. El número de puntos en $E(F_q)$, denotado por $\#\ E(F_q)$ es llamado el orden de E sobre F_q. El teorema de Hasse provee una cota para el $\#\ E(F_q)$.

La aplicación de Frobenius es la función

$$\tau_p: E(\overline{\mathbb{F}}_p) \to E(\overline{\mathbb{F}}_p), \quad \tau_P(x, y) = (x^p, y^p)$$

Se puede verificar que τ_P es un homomorfismo de grupo.

La cantidad

$$a_p = p + 1 - \#\ E(\mathbb{F}_p)$$

es llamada la traza de Frobenius, puesto que una forma de calcular esto es el uso de la aplicación de Frobenius para tener una transformación lineal sobre un cierto subespacio vectorial $V_\ell(E)$. Entonces a_p es la traza tal transformación lineal.

El teorema de Hasse dice que

$$|a_p| \leq 2\sqrt{p}$$

Para criptografía, se necesita que $E(\mathbb{F}_p)$ contenga un subgrupo que tenga como orden un primo grande. ¿Cómo varía $\#\ E(\mathbb{F}_p)$ para diferentes E?

Hay aproximadamente $2p$ diferentes curvas elípticas definidas sobre $\mathbb{F}_p$.

Si los valores $a_p(E)$ para diferentes E están uniformemente distribuidas en el intervalo $[-2\sqrt{p}, 2\sqrt{p}]$ entonces deberíamos suponer que cada valor aparece aproximadamente $\frac{1}{2}\sqrt{p}$ veces.

Esto no es completamente cierto, pero es verdad que los valores de a_p entre, digamos $-\sqrt{p}$ y $\sqrt{p}$ aparece con bastante frecuencia. La declaración precisa dice que los valores de a_p siguen la distribución de Sato-Tate.

La moderna teoría de ecuaciones Diofánticas, la solución de ecuaciones polinomiales usando números enteros o racionales, fue iniciado en 1922 cuando L.J. Mordell probó un resultado de referencia describiendo $E(\mathbb{Q})$.

4.3.13. Teorema. (Mordell, 1922)

Sea E una curva elíptica dada por la ecuación

$$E: y^2 = x^3 + Ax + B, \;\; A, B \in \mathbb{Q}$$

Entonces el grupo de puntos racionales $E(\mathbb{Q})$ es un grupo Abeliano finitamente generado. En otras palabras, existe un conjunto finito de puntos $P_1, \cdots, P_t \in E(\mathbb{Q})$ de modo que cada punto $P \in E(\mathbb{Q})$ puede ser escrito en la forma

$$P = n_1P_1 + n_2P_2 + \cdots + n_tP_t, \qquad \text{para algunos } n_1, \cdots, n_t \in \mathbb{Z}$$

Un teorema estándar acerca de grupos Abelianos finitamente generados nos dice que

$$E(\mathbb{Q}) \cong (\text{Grupo finito}) \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copias}}$$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copias}}$$

El grupo finito $E(\mathbb{Q})_{\text{tors}}$ es llamado el sub grupo torsión de $E(\mathbb{Q})$. El entero r es llamado el rango de $E(\mathbb{Q})$.

La descripción de todos los subgrupos de torsión para $E(\mathbb{Q})$ es fácil, a pesar que la prueba del teorema es extremadamente difícil.

4.4. Puntos de torsión

Los puntos de torsión son aquellos cuyo orden es finito, estos puntos juegan un rol importante en el estudio de curvas elípticas, especialmente para curvas elípticas sobre campos finitos, donde todos los puntos son puntos de torsión. Primeramente veremos los casos elementales, los puntos de 2-torsión y 3-torsión, luego determinamos el caso general, finalmente discutiremos la importante paridad de Weil- Tate.

4.4.1. Definición (Puntos de Torsión)

Sea E una curva elíptica sobre un campo K, sea n un entero positivo, los puntos de torsión están dados por el conjunto

$$E[n] = \{P \in E(\overline{K})/nP = \infty\}$$

(Recalcamos que $\overline{K}$ es la clausura algebraica de K). Enfatizamos que $E[n]$ contiene puntos con coordenadas en $\overline{K}$, no exactamente en K. En este caso también se dice que el punto P es de orden finito n.

4.4.2 Puntos de orden 2 (2-torsión)

Cuando la característica de $K \neq 2$, E está dado por una ecuación de la forma

$$y^2 = x^3 + ax^2 + bx + c$$

En este caso

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

Como un grupo abstracto, este es isomorfo a $Z_2 \oplus Z_2$, como lo muestra [7] JCSHEF H. SILVERMAN, JOHN TATE, Rational Point on Elliptic Curves, capítulo IV, pag. 121.

Si E tiene cualquiera de las dos formas:

(I) $y^2 + xy + x^3 + a_2x^2 + a_6 = 0$

(II) $y^2 + a_3y + x^3 + a_4x + a_6 = 0$

En la primera forma, $a_6 \neq 0$; en la segunda forma $a_3 \neq 0$ (de otro modo la curva seria singular)

Si $P(x, y)$ es un punto de orden 2, entonces la tangente en P debería ser vertical, lo que significa que la derivada parcial con respecto a y es cero.

En el caso (I) esto significa que $x = 0$, sustituyendo en (I) obtenemos

$$0 = y^2 + a_6 = \left(y + \sqrt{a_6}\right)^2$$

Por lo tanto $(0, \sqrt{a_6})$ es el único punto de orden 2. (las raíces cuadradas son únicas en característica 2), así

$$E[2] = \{\infty, (0, \sqrt{a_6})\ \}$$

Como un grupo abstracto es isomorfo a Z_2.

En el caso (II), la derivada parcial con respecto a y es $a_3 \neq 0$, por lo tanto no hay puntos de orden 2, así

$$E[2] = \{\infty\}$$

Resumiendo, sea E una curva elíptica sobre el cuerpo K, si la característica de K $\neq 2$ entonces,

$$E[2] \cong Z_2 \oplus Z_2$$

Si la característica de $K = 2$, entonces

$$E[2] = \{\infty\} \quad o \quad E[2] \cong Z_2$$

4.4.3. Puntos de orden 3 (3- torsión)

Ahora veamos los puntos de orden 3. Asumamos primero que la característica de $K \neq 2,3$ E se puede dar en la forma

$$y^2 = x^3 + Ax + B$$

Un punto P de orden 3 satisface, $2P = -P$, esto significa que la x-coordenada de $2P$ es igual a la x-coordenada de $-P$.

Usando las ecuaciones de la adición se tiene

$$\mathrm{m}^2 - 2\mathrm{x} = \mathrm{x}$$

Donde

$$\mathrm{m} = \frac{3\mathrm{x}^2 + \mathrm{A}}{2\mathrm{y}}$$

Usando el hecho que

$$y^2 = x^3 + Ax + B$$

Hallamos que

$$(3x^2 + A)^2 = 12x(x^3 + Ax + B)$$

Simplificando

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0$$

El discriminante de este polinomio es $-6912(4A^3 + 27B^2)^2 \neq 0$, por lo tanto el polinomio no tiene raíces múltiples. Hay cuatro diferentes valores de "x" (en $\overline{K}$), cada x da dos valores de y, luego tenemos ocho puntos de orden 3, luego hay nueve puntos de orden 3.

$$E[3] \cong Z_3 \oplus Z_3$$

Ahora asumamos que la característica es 3. Podemos asumir que E es de la forma

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

Procediendo como en el caso anterior, algunos términos desaparecen pues $3 = 0$,

$$\left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 3x = 0$$

Simplificando (observando que $4 = 1$)

$$a_2x^3 + a_2a_6 - a_4^2 = 0$$

Asumiendo que $a_2, a_4 \neq 0$. Si $a_2 = 0$, entonces $-a_4^2 = 0$, lo cual no puede ser, así que no hay valores para x. Por lo tanto

$$E[3] = \{\infty\}$$

Si $a_2 \neq 0$, obtenemos una ecuación de la forma

$$a_2(x^3 + a) = 0$$

Que tiene una única raíz triple en característica 3, Por lo tanto existe un valor de x, con dos valores correspondientes a y, esto da dos puntos de orden 3, por lo tanto

$$E[3] \cong Z_3$$

4.4.4. Teorema. (Puntos de orden n)

Sea E una curva elíptica sobre un cuerpo K, y sea n un entero positivo. Si la característica de K no divide a n, o es cero, entonces

$$E[n] \cong Z_n \oplus Z_n$$

Si la característica de K es $p > 0$, y $p \nmid n$, escribimos $n = p^r n'$ con $p \nmid n'$, entonces

$$E[n] \cong Z_{n'} \oplus Z_{n'} \quad o \quad E[n] \cong Z_n \oplus Z_{n'}$$

Para la prueba de este teorema necesitamos algunos resultados previos, como lo muestra [2] LAWRENCE C. WASHINGTON, Elliptic Curves, Number Theory and Cryptography, pag. 86.

4.4.5. La paridad de Weil

La paridad de Weil sobre el grupo n-torsión de una curva elíptica es la mayor herramienta en el estudio de una curva elíptica. Se usa para probar el teorema de Hasse que se refiere al número de puntos sobre una curva elíptica sobre un campo finito, también es usado para resolver el problema del logaritmo discreto para curvas elípticas. Sea E una curva elíptica sobre un cuerpo K, y sea n un entero no divisible por la característica de K. Entonces,

$$E[n] \cong Z_n \oplus Z_n$$

Sea el grupo de n raíces de unidad en $\overline{K}$

$$u_n = \{x \in \overline{K} : x^n = 1\}$$

4.4.6. Definición.

Sea E una curva elíptica definida sobre un campo K, y sea n un entero positivo. Asumiendo que la característica de K no divide a n, entonces existe una paridad llamada paridad de Weil

$$e_n : E[n] \times E[n] \rightarrow u_n$$

La paridad de Weil satisface las siguientes propiedades

1) e_n es bilineal en cada variable. Esto significa que

$$e_1(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

Y

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

Para todo $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2) e_n es no degenerada en cada variable. Esto significa que si $e_n(S, T) = 1$ para todo $T \in E[n]$ entonces $S = \infty$ y también que si $e_n(S, T) = 1$ para todo $S \in E[n]$ entonces $T = \infty$.
3) $e_n(T, T) = 1$ para todo $T \in E[n]$
4) $e_n(T, S) = e_n(S, T)^{-1}$ para todo $S, T \in E[n]$
5) $e_n(\sigma T, \sigma S) = \sigma(e_n(T, S))$ para todo automorfismo σ de $\overline{K}$ tal que σ es la aplicación identidad sobre los coeficientes de E (si E está en la forma de Weierstrass, $\sigma(A) = A$ y $\sigma(B) = B$)
6) $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\text{gra}(\alpha)}$ para algún endomorfismo separable α de E. Si los coeficientes de E están en el campo finito F_q, entonces la declaración también se cumple cuando α es el endomorfismo de Frobenius.

4.4.7. El Endomorfismo de Frobenius

Sea F_q un campo finito con clausura algebraica $\bar{F}_q$ y sea

$$\phi_q : \bar{F}_q \to \bar{F}_q$$
$$x \to x^q$$

la aplicación de Frobenius para F_q. Sea E una curva elíptica definida sobre F_q. Entonces ϕ_q actúa sobre las coordenadas de los puntos en $E(\bar{F}_q)$:

$$\phi_q(x, y) = (x^q, y^q), \qquad \phi_q(\infty) = \infty$$

Lema 1.

Sea E definida sobre F_q, y sea $(x, y) \in E(\bar{F}_q)$

1) $\phi_q(x, y) \in E(\bar{F}_q)$

2) $(x,y) \in E(F_q)$ si y solamente si $\phi_q(x,y) = (x,y)$

Prueba: Sabiendo que $(a+b)^q = a^q + b^q$ cuando q es una potencia de la característica del campo y sabiendo que $a^q = a$ para todo $a \in F_q$.

Tenemos que

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

Con $a_i \in F_q$. Elevando la ecuación a la q-ésima potencia obtenemos

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^2)^2 + a_4x^q + a_6$$

Esto significa que (x^q, y^q) está sobre E, lo cual prueba 1).

Para probar 2) recalquemos que $x \in F_q$ si y solamente si $\phi_q(x) = x$. Por lo tanto

$$(x,y) \in E(F_q) \Leftrightarrow x,y \in F_q \Leftrightarrow \phi_q(x) = x, \phi_q(y) = y \Leftrightarrow \phi_q(x,y) = (x,y).$$

El siguiente resultado es la clave para contar puntos sobre una curva elíptica definida sobre un campo finito. Como ϕ_q es un endomorfismo de E, también lo son $\phi_q^2 = \phi_q \circ \phi_q$, y también $\phi_q^n = \phi_q \circ \phi_q \ldots \phi_q$ para cada $n \geq 1$. Como la multiplicación por -1 es también un endomorfismo, la suma $\phi_q^n - 1$ es un endomorfismo de E.

Lema 2.

Sea E definida sobre F_q y sea $n \geq 1$.

1) $Ker(\phi_q^n - 1) = E(F_{q^n})$
2) $\phi_q^n - 1$ es un endomorfismo separable, tal que $\# E(F_q) = gra(\phi_q^n - 1)$

Prueba. Como ϕ_q^n es la aplicación de Frobenius para el campo F_{q^n} la parte 1) es una repetición del lema 1. El hecho de que $\phi_q^n - 1$ es separable está probado en [2] LAWRENCE C. WASHINGTON, Elliptic Curves, Number Theory and Cryptography, pag. pag 50-51.

Lema 3.

Sean r, s enteros con $MCD(s,q) = 1$. Entonces $gra(r\phi_q - s) = r^2q + s^2 - rsa$

Prueba:

Esto se sigue del hecho que si tenemos dos endomorfismos α, β de E, para a, b enteros, el endomorfismo $a\alpha + b\beta$ está definido por

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P)$$

$a\alpha + b\beta$ es un endomorfismo y verifica que

$$gra(a\alpha + b\beta) = a^2 gra(\alpha) + b^2 gra(\beta) + ab(grad(\alpha + \beta) - gra(\alpha) - gra(\beta))$$

Como el $gra(\phi_q) = q$ y el $gra(-1) = 1$ tenemos

$$gra(r\phi_q - s) = r^2 gra(\phi_q) + s^2 gra(-1) + rs(gra(\phi_q - 1) - gra(\phi_q) - gra(-1))$$

$$= r^2 q + s^2 + rs(gra(\phi_q - 1) - q - 1)$$

Si hacemos

$$a = q + 1 - gra(\phi_q - 1)$$

Se tiene la prueba del lema 3.

Ahora podemos finalizar la prueba del teorema de Hasse. Como $gra(r\phi_q - s) \geq 0$, el lema 3 implica que

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

Para todo r, s con $MCD(s, q) = 1$. El conjunto de los números r/s tales que $MCD(s, q) = 1$ es denso en $\mathbb{R}$. Por lo tanto,

$$qx^2 - ax + 1 \geq 0$$

Para todos los números reales x. Luego el discriminante es negativo o cero, lo cual significa que $a^2 + 4q \leq 0$, entonces, $|a| \leq 2\sqrt{q}$. Esto completa la prueba del teorema de Hasse.

¿Cómo es $E(\mathbb{F}_p)$? El grupo $E(\mathbb{F}_p)$ es obviamente un grupo finito, en efecto, este claramente no tiene más de $2p + 1$ puntos.

Para cada $x \in \mathbb{F}_p$ existe un 50% de probabilidad que el valor de $f(x) = x^3 + Ax + B$ sea un cuadrado en $\mathbb{F}_p^*$. Y si $y^2 = f(x)$ es un cuadrado, entonces (usualmente) tenemos dos puntos $(x, \pm y)$ en $E(\mathbb{F}_p)$. Además está un punto en el infinito $\mathcal{O}$.

Así podemos esperar que $E(\mathbb{F}_p)$ contenga aproximadamente

$$\# E(\mathbb{F}_p) \approx \frac{1}{2}.2.p + 1 = p + 1$$

4.4.8. Teorema. (Hasse, 1922) Sea E una curva elíptica dada por

$$y^2 = x^3 + Ax + B, \;\; A, B \in \mathbb{F}_p$$

Entonces

$$\left|\# E(\mathbb{F}_p) - (p + 1)\right| \leq 2\sqrt{p}.$$

4.4.9. Teorema.

Sea E una curva elíptica definida sobre F_q.

Sea

$$a = q + 1 - gra(\phi_q - 1)$$

entonces

$$\phi_q^2 - a\phi_q + q = 0$$

Como endomorfismo de E, y a es el único entero k tal que

$$\phi_q^2 - k\phi_q + q = 0$$

En otras palabras, si $(x, y) \in E(\bar{F}_q)$, entonces

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = \infty$$

Donde a es el único entero tal que esta relación se cumple para todo $(x, y) \in E(\bar{F}_q)$. Además, a es el único entero que satisface

$$a \equiv traz\left((\phi_q)_m\right) \; mod\, m$$

Para todo m tal que $MCD(m,q)=1$.

Prueba:

Si $\phi_q^2 - a\phi_q + q$ es un endomorfismo nulo, entonces su núcleo es finito, demostraremos que el núcleo es infinito, luego el endomorfismo es el nulo.

Sea $m \geq 1$ un entero tal que $MCD(m,q)=1$. Recalcando que ϕ_q induce una matriz $(\phi_q)_m$ que describe la acción de ϕ_q sobre $E[m]$.

Sea

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

Como $\phi_q - 1$ es separable y algunas otras propiedades de los endomorfismos se tiene

$$\#\, Ker(\phi_q - 1) = gra(\phi_q - 1) \equiv det\left((\phi_q)_m - I\right) = sv - tu - (s+v) + 1$$

Además, $sv - tu = det\left((\phi_q)_m\right) \equiv q \pmod m$ y $\#\, Ker(\phi_q - 1) = q + 1 - a$. Por lo tanto

$$Traz\left((\phi_q)_m\right) = s + v \equiv a \pmod m$$

Por el teorema de Cayley Hamilton del algebra lineal, tenemos

$$(\phi_q)_m^2 - a\,(\phi_q)_m + qI \equiv 0 \pmod m$$

Esto significa que el endomorfismo $\phi_q^2 - a\phi_q + q$ es idénticamente cero sobre $E[m]$. Como hay infinitas escogencias para m, el núcleo para $\phi_q^2 - a\phi_q + q$ es infinito, luego el endomorfismo es 0.

Ahora supongamos que existe un $a_1 \neq a$ y satisface $\phi_q^2 - a_1\phi_q + q = 0$, entonces

$$(a - a_1)\phi_q = (\phi_q^2 - a_1\phi_q + q) - (\phi_q^2 - a\phi_q + q) = 0$$

Además $\phi_q : E(\bar{F}_q) \to E(\bar{F}_q)$ es suryectivo, por lo tanto $(a - a_1)$ aniquila $E(\bar{F}_q)$, en particular aniquila $E[m]$ para cada $m \geq 1$. Puesto que hay puntos en $E[m]$ de

orden m cuando $MCD(m, q) = 1$, tenemos que $a - a_1 \equiv 0 \pmod{m}$. Luego $a - a_1 = 0$, así a es único.

4.5. Determinación del orden de un grupo

El teorema de Hasse da cotas para el grupo de puntos sobre una curva elíptica sobre un campo finito.

4.5.1. Curvas sub campos

Algunas veces tenemos una curva elíptica E definida sobre un campo pequeño finito F_q y deseamos conocer el orden de $E(F_{q^n})$ para algún n. Podemos determinar el orden de $E(F_{q^n})$ cuando $n = 1$ listando los puntos o por algún otro procedimiento elemental. Lo fabuloso de este hecho es que esto nos lleva a determinar el orden para todo n.

4.5.2. Teorema:

Sea $\# E(F_{q^n}) = q + 1 - a$. Haciendo

$$X^2 - aX + q = (X - \alpha)(X - \beta)$$

Entonces, para todo $n \geq 1$ se tiene

$$\# E(F_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

Prueba:

Primeramente, necesitamos el hecho que $\alpha^n + \beta^n$ es un entero. Esto podría ser probado remarcando que este es un entero algebraico y es también un número racional. Sin embargo, esto puede ser probado por medios más elementales.

Lema 4.

Sea $s_n = \alpha^n + \beta^n$, entonces $s_0 = 2$, $s_1 = a$ y $s_{n+1} = as_n - qs_{n-1}$ para todo $n \geq 1$.

Prueba

Multiplicando la relación $\alpha^2 - a\alpha + q = 0$ por α^{n-1} se obtiene $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$. Similarmente para β. Sumando las dos relaciones se obtiene el lema 4.

Se sigue inmediatamente del lema 4 que $\alpha^n + \beta^n$ es un entero para todo $n \geq 0$.

Sea

$$F(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n$$

Entonces $X^2 - aX + q = (X - \alpha)(X - \beta)$ divide $f(X)$. Esto se sigue inmediatamente de la división de polinomios que el cociente es un polinomio $Q(X)$ con coeficientes enteros, el punto principal de esto es que el coeficiente principal de $X^2 - aX + q$ es 1 y que el polinomio $f(X)$ tiene coeficientes enteros. Por lo tanto

$$\left(\phi_q^n\right)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0,$$

Como endomorfismo de E, por teorema 4.10. Note que $\phi_q^n = \phi_{q^n}$. Por el mismo teorema existe un entero k tal que $\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$ y tal k es determinado por $k = q^n + 1 - \#\, E(F_{q^n})$. Por lo tanto

$$\alpha^n + \beta^n = q^n + 1 - \#\, E(F_{q^n})$$

Lo que completa la prueba del teorema.

Así por ejemplo, la curva elíptica dada por $y^2 + xy = x^3 + 1$ sobre F_2 satisface que $\#\, E(F_2) = 4$, por lo tanto $a = 2 + 1 - 4 = -1$, y obtenemos el polinomio

$$X^2 + X + 2 = \left(X - \frac{-1 + \sqrt{-7}}{2}\right)\left(X - \frac{-1 - \sqrt{-7}}{2}\right)$$

Luego, el teorema dice que

$$\#\, E(F_4) = 4 + 1 - \left(\frac{-1 + \sqrt{-7}}{2}\right)^2 - \left(\frac{-1 - \sqrt{-7}}{2}\right)^2$$

Usando la recurrencia del lema se tiene

$$s_2 = as_1 - 2s_0 = -(-1) - 2(2) = -3$$

De esto se tiene que

$$\#\, E(F_4) = 4 + 1 - (-3) = 8$$

Similarmente

$$\left(\frac{-1+\sqrt{-7}}{2}\right)^{101}+\left(\frac{-1-\sqrt{-7}}{2}\right)^{101}=2969292210605269$$

Por lo tanto

$$\#\, E(F_{2^{101}})=2^{101}+1-2969292210605269=2535301200\ldots 84$$

4.5.3. Símbolo de Legendre

Para hacer una lista de los puntos de $y^2=x^3+Ax+B$ sobre un campo finito, evaluamos cada valor posible para x, entonces hallamos la raíz cuadrada y de x^3+Ax+B, si existe. Este procedimiento es la base para un algoritmo que contabiliza los puntos.

Recordemos el símbolo de Legendre $\left(\frac{x}{p}\right)$ para un primo p impar, que está definido como sigue

$$\left(\frac{x}{p}\right)=\begin{cases}+1, \text{ si } t^2\equiv x\ (mod\ p) \text{ tiene solución } t\not\equiv 0\ \ (mod\ p)\\ -1, \text{ si } t^2\equiv x\ (mod\ p) \text{ no tiene solución } t\\ 0, \ si\ x\equiv 0\ \ (mod\ p)\end{cases}.$$

Este puede ser generalizado para cualquier campo finito F_q, con q impar por definición, para $x\in F_q$,

$$\left(\frac{x}{F_q}\right)=\begin{cases}+1, \text{ si } t^2=x \text{ tiene una solución } t\in F_q^x\\ -1, \text{ si } t^2=x \text{ no tiene solución } t\in F_q\\ 0, \ si\ x\equiv 0\end{cases}.$$

4.5.4. Teorema

Sea E una curva elíptica definida por $y^2=x^3+Ax+B$ sobre F_q, entonces

$$\#\, E(F_q)=q+1+\sum_{x\in F_q}\left(\frac{x^3+Ax+B}{F_q}\right)$$

Prueba

Para un x_0 dado, existen dos puntos (x, y) con x-coordenada x_0 si $x_0^3 + Ax_0 + B$ es un cuadrado diferente de cero en F_q, uno si este es cero, y no hay puntos si este no es un cuadrado. Por lo tanto, el número de puntos con x- coordenada x_0 es igual a $1 + \left(\frac{x_0^3 + Ax_0 + B}{F_q}\right)$. Sumando sobre todo $x_0 \in F_q$, incluyendo 1 para el punto ∞, se tiene

$$\#\, E(F_q) = 1 + \sum_{x \in F_q} \left(1 + \left(\frac{x^3 + Ax + B}{F_q}\right)\right)$$

Sumando el término 1 de cada uno de los q sumandos se tiene el resultado.

4.5.5. Corolario

Sea $x^3 + Ax + B$ un polinomio con $A, B \in F_q$, donde q es impar. Entonces

$$\left|\sum_{x \in F_q} \left(\frac{x^3 + Ax + B}{F_q}\right)\right| \leq 2\sqrt{q}$$

Prueba

Cuando $x^3 + Ax + B$ no tiene raíces repetidas, $y^2 = x^3 + Ax + B$ da una curva elíptica, luego usando el teorema 4.5.4 se tiene

$$q + 1 - \#\, E(F_q) = -\sum_{x \in F_q} \left(\frac{x^3 + Ax + B}{F_q}\right)$$

El resultado ahora se sigue del teorema de Hasse.

Así por ejemplo, sea E la curva dada por $y^2 = x^3 + x + 1$ sobre F_5, los cuadrados mod 5 diferentes de cero son 1 y 4. Por lo tanto

$$\#\, E(F_5) = 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{5}\right)$$

$$= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right)$$

$$= 6 + 1 - 1 + 1 + 1 + 1 = 9$$

Nota: El teorema 4.5.4 que es conocido como el método de Lang - Trotter trabaja eficientemente para valores pequeños de q, por ejemplo $q < 100$. Sin embargo para valores grandes es imposible de usar, por ejemplo $q = 10^{100}$.

4.6. Orden de un punto

Sea $P \in E(F_q)$. El orden de P es el menor entero positivo k tal que $kP = \infty$. Un resultado fundamental de teoría de grupos (un corolario del teorema de Lagrange) es que el orden de un punto siempre divide el orden del grupo $E(F_q)$. También para un entero n, se tiene $nP = \infty$ si y solo si el orden de P divide a n. Por el teorema de Hasse, $\# E(F_q)$ está en un intervalo d longitud $4\sqrt{q}$. Por lo tanto si podemos hallar un punto de orden mayor que $4\sqrt{q}$ solo puede haber un múltiplo de este orden en el intervalo correcto y este debería ser $\# E(F_q)$. Incluso si el orden del punto es menor que $4\sqrt{q}$, podemos tener una lista pequeña de posibilidades para $\# E(F_q)$.

¡Como hallamos el orden de un punto P? Si conocemos el orden de todo el grupo de puntos, entonces podemos mirar sus factores. Nuestro objetivo es discutir un método para hallar el orden de un punto.

4.6.1. Método Baby step, Giant step

Sea $P \in E(F_q)$, queremos hallar el orden de P. Primeramente deseamos hallar un entero k tal que $kP = \infty$. Sea $\# E(F_q) = N$. Por el teorema de Lagrange $NP = \infty$. Podriamos no conocer N aun, pero conocemos que $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$. Podríamos intentar valores en este rango y ver cuales satisfacen $NP = \infty$. Esto toma alrededor de $4\sqrt{q}$ pasos. Sin embargo es posible mejorar esto con el siguiente algoritmo.

1) Compute $Q = (q + 1)P$
2) Escoja un entero $m > q^{1/4}$. Compute y almacene los puntos jP para $j = 1, \ldots, m$.
3) Compute los puntos

$$Q + k(2mP), \text{ para } k = -m, -(m-1), \ldots, m$$

Hasta que se tenga una coincidencia $Q + k(2mP) = \pm jP$ con un punto (o su negativo) de la lista almacenada.

4) Concluya que $(q + 1 + 2mk \mp j)P = \infty$. Sea $q + 1 + 2mk \mp j = M$
5) Factorice $M = P_1 \dots P_r$ en sus factores primos
6) Compute $(M/p_i)P$, para $i = 1, \dots, r$. Si $(M/p_i)P = \infty$ para algún i, reemplace Mcon (M/p_i) y regrese al paso 5). Si $(M/p_i)P \neq \infty$ para todo i entonce M es el orden del punto P.
7) Si estamos buscando el $\#\ E(F_q)$, repetimos los pasos del 1) al 6) con puntos escogidos aleatoriamente en $E(F_q)$ hasta que el mínimo común múltiplo de los órdenes divida solamente un entero N con $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$. Entonces $N = \#\ E(F_q)$.

Hay dos asuntos que deberían ser dirigidos.

Primero: Asumiendo que existe una coincidencia, este método claramente produce un entero que aniquila P. Pero, ¿por qué existe una coincidencia?. El lema 5 da la respuesta.

Lema 5.

Sea a un entero con $|a| \leq 2m^2$. Existen enteros a_0, a_1 con $-m < a_0 < m$ y $-m < a_1 < m$ tal que

$$a = a_0 + 2ma_1$$

Asumiendo el lema 5, sea $a_0 \equiv a\ (mod\ 2m)$ con $-m < a_0 < m$ y sea $k = -a_1$. Entonces

$$Q + k(2mP) = (q + 1 - 2ma_1)P = (q + 1 - a - a_0)P = NP + a_0P = a_0P$$
$$= \pm jP$$

Donde $j = |a_0|$. Por lo tanto existe una coincidencia.

En segundo lugar, ¿Por qué el paso 6) nos produce el orden de P? el lema 6 nos da la respuesta. ([2] LAWRENCE C. WASHINGTON, Elliptic Curves, Number Theory and Cryptography, pag. 112-113)

Lema 6.

Sea G un grupo aditivo (con elemento identidad 0) y sea $g \in G$. Supongamos que $Mg = 0$ para algún entero positivo M. Sean $p_1, p_2, \ldots, p_r$ los distintos primos que dividen M. Si $(M/p_i)g \neq 0$ para todo i, entonces M es el orden de g.

Prueba

Sea k el orden de g. Entonces $k \setminus M$. Supongamos que $k \neq M$. Sea p_i un primo dividiendo M / k. Entonces $p_i k \setminus M$, así $k \setminus (M/p_i)$. Por lo tanto, $(M/p_i)g = 0$, contrario a lo que hemos asumido, por lo tanto $k = M$.

Por lo tanto el paso 6) halla el orden de P.

Observaciones:

(1) Para ahorrar capacidad de almacenamiento, sería mas eficiente almacenar solamente la x coordenada de los puntos jP (juntamente con el correspondiente j), puesto que buscando una coincidencia con $\pm jP$ solamente requiere la x coordenada (asumiendo que estamos trabajando con la ecuación de Weierstrass). Cuando se encuentra una coincidencia, las dos posibles y coordenadas pueden ser computados.

(2) Computar $Q + k(2mP)$ puede ser hecho computando Q y $2mP$ de una vez por todas. Llegar de $Q + k(2mP)$ a $Q + (k + 1)(2mP)$ simplemente sumar $2mP$ en vez de computar cada cosa. Similarmente, una vez que jP ha sido computado, sumar P para tener $(j + 1)P$.

(3) Estamos asumiendo que podemos factorizar M. Si no, podemos al menos hallar un factor primo pequeño p_i y chequear que $\left(\frac{M}{p_i}\right)P \neq \infty$. Entonces M será un buen candidato para el orden de P.

(4) ¿Por qué este método es llamado "Baby Step, Giant Step? Los Baby steps son de un punto jP a $(j + 1)P$. Los giant step son de un punto $k(2mP)$ a $(k + 1)(2mP)$, puesto que estamos tomando el "mas grande" step $2mP$.

4.6.2. Ejemplo y representación gráfica.

Para ilustrar el algoritmo sea E la curva elíptica $y^2 = x^3 - 10x + 21$ sobre F_{557}. Sea $P = (2,3)$. La curva tiene 567 puntos (incluyendo el punto en el infinito). El sub grupo generado por P tiene 189 puntos. El teorema de Hasse implica que $511 \leq N_{557} \leq 605$. El único múltiplo de 189 en este rango es $3 \times 189 = 567$.

Siguiendo el procedimiento dado en el algoritmo.

(1) $Q = 558(2,3) = (78,412)$

(2) Sea $m = 5$ que es mayor que $557^{1/4}$. La lista de los jP es

$$\infty,$$

$$(2,3),$$

$$2(2,3) = (58,164),$$

$$3(2,3) = (44,294),$$

$$4(2,3) = (56,339),$$

$$5(2,3) = (132,364)$$

(3) Cuando $k = 1$, tenemos que $Q + k(2mP) = (2,3)$, que coincide con el punto de nuestra lista para $j = 1$.

(4) Tenemos $(q + 1 + 2mk - j)P = 567 = \infty$

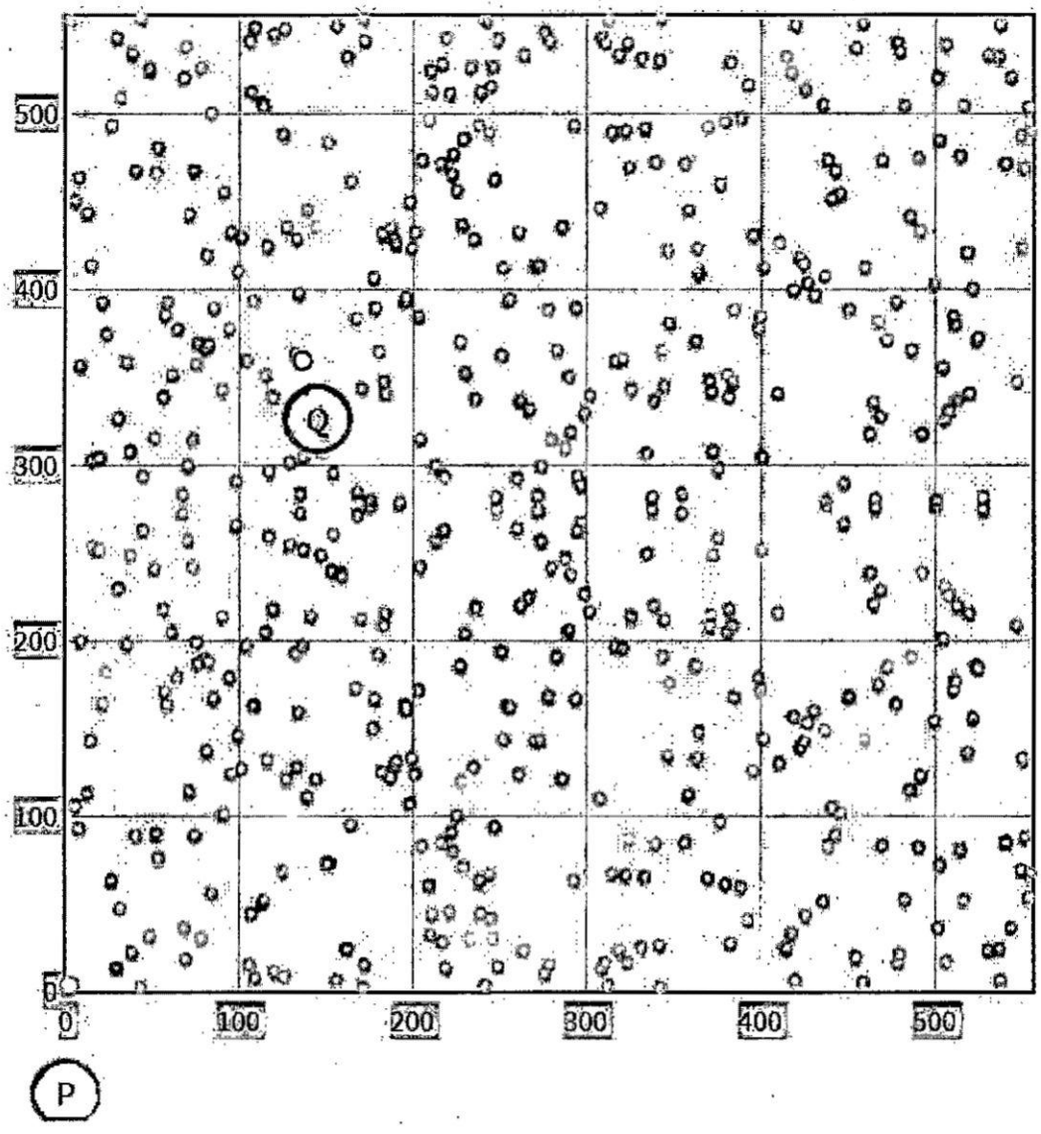
(5) Factorizando $567 = 3^4 \times 7$. Compute $\frac{567}{3}P = 189P = \infty$. Tenemos a 187 como candidato para el orden de P.

(6) Factorice $189 = 3^3 \times 7$. Compute $\frac{189}{3}P = 63P = (38,535) \neq \infty$ y $\frac{189}{7}P = 27P = (136.360) \neq \infty$. Por lo tanto 189 es el orden de P.

En EL gráfico 4.8 se tiene los puntos de la curva.

GRÁFICO 4.8

GRÁFICA DE $y^2 = x^3 - 10x + 21$ EN F_{557}



Fuente: Elaboración propia con la herramienta visual **HTML5/JavaScript visual tool**, disponible en:

http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

4.7. Tópicos de Criptografía

Curvas elípticas han sido usadas para resolver diferentes tipos de problemas, uno de ellos es el problema de números congruentes: números enteros que representan las longitudes de un triángulo rectángulo; otro ejemplo es la prueba del último teorema de Fermat, el cual establece que la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras para x, y, z cuando $n > 2$.

En 1985, Neal Koblitz y Victor Miller independientemente propusieron curvas elípticas para diseñar sistemas criptográficos de clave pública. Desde entonces una gran cantidad de investigaciones han sido publicados sobre la seguridad e implementación eficiente de criptografía con curvas elípticas.

En 1990 sistemas de curvas elípticas comenzaron a recibir aceptación comercial cuando organizaciones especificaron protocolos estándar para curvas elípticas y compañías privadas incluyeron estos protocolos en seguridad de sus productos. En esta parte nos interesa explicar la ventaja de criptografía con curvas elípticas.

4.7.1. Criptografía Básica

Alicia desea enviar un mensaje, a menudo llamado el plaintext, a Bob. A fin de mantener la seguridad del mensaje, ella encripta el mensaje obteniendo el ciphertex. Cuando Bob recibe el ciphertex, él decifra este y lee el mensaje. A fin de encriptar el mensaje, Alicia usa una clave encriptadora. Bob usa una clave decifradora para decifrar el ciphertex. Claramente, la clave decifradora debería mantenerse en secreto siempre.

Así también A y B podrían ser dos personas comunicándose por un teléfono celular, y E alguien que está intentando escuchar su conversación.

4.7.2. Sistema de clave simétrica

Los sistemas criptográficos pueden ser generalmente divididos en dos: En sistemas de clave simétrica y en sistemas de clave pública. En ecriptamiento simétrico, la clave encriptadora y decifradora son la misma, o una puede fácilmente ser deducida de la otra.

4.7.3. Criptografía de clave pública

En un sistema criptográfico de clave pública relacionamos un par de claves de modo que el problema de descubrir la clave privada de la correspondiente clave pública es equivalente a resolver un problema computacionalmente intratable tales como:

- ❖ El problema de factorización entera, cuya dureza es esencial para los sistemas de seguridad RSA.
- ❖ El problema de logaritmo discreto, cuya dificultad es esencial para la seguridad del sistema El Gamal de clave pública y el Sistema Digital (DSA)
- ❖ El problema de logaritmo discreto para curvas elípticas, cuya dureza es esencial para la seguridad de todos los sistemas criptográficos con curvas elípticas.

[2] LAWRENCE C. WASHINGTON, Elliptic Curves, Number Theory and Cryptography, pag. 169, resume el Sistema RSA.

4.7.4. Sistema RSA

Este es un sistema criptográfico inventado por Ransey Shamir y Adleman (RSA) que usa el problema de factorización entera de un número suficientemente grande.

Generación de claves: Un par de claves son generados usando el algoritmo 1. La clave pública consiste de un par de enteros (n, e) donde el módulo RSA n es un producto de dos enteros p y q aleatorios (secretos) de la misma longitud. El exponente encriptador e es un entero entre 1 y φ con

$$\text{MCD}(e, \varphi) = 1, \qquad \varphi = (p-1)(q-1)$$

La clave privada d, también llamado el exponente de decifrado satisface

$$1 < d < \varphi, \;\; ed = 1 \bmod \varphi.$$

Se prueba que determinar la clave privada d de la clave pública (n, e) es computacionalmente equivalente al problema de determinar los factores p y q de n.

Algoritmo 1. Clave de generación RSA

Entrada: Parámetro de seguridad l

Salida: Clave pública (n, e) y clave privada d.

i) Selección al azar de dos primos p y q de longitud bit $\frac{l}{2}$

ii) Compute $n = pq,\ \varphi = (p-1(q-1)$

iii)Seleccione un entero arbitrario $e, 1 < e < \varphi,\ \text{MCD}(e, \varphi) = 1$

iv)Compute el entero d satisfaciendo $1 < d < \varphi,\ \ ed = 1\, mod\ \varphi$

v) Retorne (n, e, d)

El sistema de encriptado RSA y sistema de firmas RSA usan el hecho que para todos los enteros m

$$m^{ed} \equiv m(mod\ n)$$

$$c^d \equiv (m^e)^d \equiv m(mod\ n)$$

La seguridad está en la dificultad de computar el plaintext m del ciphertext

$$c \equiv m^e(mod\ n)$$

y los parámetros públicos n, e.

Algoritmo 2. Encriptado básico RSA

Entrada: Clave de encriptado básico RSA, plaintext $m \in [0, n-1]$

Salida: Ciphertext c

i) Compute $c \equiv m^e(mod\ n)$

ii) Retorne c

Algoritmo 3. Clave de decifrado básico RSA

Entrada: Clave pública RSA (n, e), clave privada RSA d, ciphertext c

Salida: Plaintext m

i) Compute $m \equiv c^d(mod\ n)$

ii) Retorne m

4.8. El Problema del logaritmo discreto

Sea p un número primo, y a, b enteros diferentes de cero modulo p. Supongamos que conocemos que existe un entero k tal que

$$a^k \equiv b \ (mod\ p)$$

El problema de logaritmo discreto clásico consiste en hallar k. Como $k + p - 1$ es también una solución, k debería ser reescrita como siendo definida módulo $p - 1$.

Mas generalmente, sea G un grupo multiplicativo, sea $a, b \in G$. Supongamos que se tiene $a^k \equiv b$ para algún entero k. En este contexto el problema del logaritmo discreto consiste nuevamente en hallar k. Por ejemplo G podría ser el grupo multiplicativo F_q^x de un campo finito. G También puede ser $E(F_q)$ para alguna curva elíptica en el que a, b son puntos sobre E y estamos interesados en hallar el entero k tal que $ka = b$.

Existen aplicaciones criptográficas del problema del logaritmo discreto. La seguridad de los criptosistemas dependerá de la dificultad de resolver el problema del logaritmo discreto.

Enseguida presentamos algunas formas de resolver el problema del logaritmo discreto.

4.8.1. Algoritmos existentes para el cálculo del logaritmo discreto

(i) Fuerza bruta

Una forma de resolver el problema del logaritmo discreto se conoce con el nombre de "fuerza bruta". Se dan valores a k hasta encontrar uno que verifique la igualdad, o podemos calcular todas las potencias de a hasta que obtengamos b.

Esto es impracticable cuando k es un entero de varios cientos de dígitos, que es como típicamente se usa en criptografía. Por lo tanto se busca otras formas técnicas de resolver el problema.

(ii) Index-Cálculus

Este algoritmo no es general, funciona en ciertos grupos como los grupos multiplicativos de los campos finitos, sin embargo este no se aplica a grupos mas generales.

La idea es calcular el logaritmo para varios primos pequeños y usar esta información para calcular lo que se pide. Veamos primero que el logaritmo discreto transforma el producto en suma, igual que ocurre con el logaritmo clásico.

Sea p primo y g generador del grupo cíclico F_p^*, entonces todo $h \equiv 0(\text{mod } p)$ puede ser escrito en la forma $h \equiv g^k$ para cierto entero k univocamente determinado $\text{mod } p-1$.

Denotemos por $L_g(h)$ el logaritmo discreto de h respecto de g y p, es decir, $L_g(h)$ es un entero (no único) que cumple

$$g^{L_g(h)} = h \ (\text{mod } p)$$

Proposición.

$$L_g(h_1h_2) = L_g(h_1) + L_g(h_2) \ (\text{mod } p-1)$$

Demostración

Supongamos que $h = h_1h_2$

Entonces

$$g^{L_g(h_1h_2)} = h_1h_2 = g^{L_g(h_1)+L_g(h_2)} (\text{mod } p)$$

Lo cual implica que:

$$L_g(h_1h_2) \equiv L_g(h_1) + L_g(h_2) \ \ (\text{mod } p-1)$$

Así por ejemplo. Sea $p = 1217$ y $g = 3$. Queremos resolver

$$3^k = 37 \ (\text{mod } 1217)$$

Escojamos un conjunto de primos pequeños $B = \{2,3,5,7,11,13\}$, buscamos relaciones de la forma:

$$3^k = \pm\text{producto de algunos primos en } B \pmod{1217}$$

Así por ejemplo

$3^1 = 3 \pmod{1217}$

$3^{24} = -2^2.7.13 \pmod{1217}$

$3^{25} = 5^3 \pmod{1217}$

$3^{30} = -2.5^2 \pmod{1217}$

$3^{54} = -5.11 \pmod{1217}$

$3^{87} = 13 \pmod{1217}$

Ahora utilizamos la definición de logaritmo y la propiedad que tienen de transformar productos en sumas para transformar esta congruencia (mod p) en (mod $p-1$). Y sabiendo además que

$$3^{\frac{(p-1)}{2}} = -1 \pmod{1217}$$

Lo cual significa que

$$L_3(-1) \equiv 608$$

De la relación

$$3^{24} \equiv -2^2.7.13 \pmod{1217}$$

Se tiene que

$$24 = L_3(-2^2.7.13) \pmod{1217}$$

$$24 = L_3(-1) + 2L_3(2) + L_3(7) + L_3(13) \pmod{1216}$$

Procediendo similarmente para las otras relaciones se obtiene

(i) $1 = L_3(3) \ (mod\ 1216)$

(ii) $24 = 608 + 2L_3(2) + L_3(7) + L_3(13) \pmod{1216}$

(iii) $25 = 3L_3(5) \pmod{1216}$

(iv) $30 = 608 + L_3(2) + 2L_3(5) \pmod{1216}$

(v) $54 \equiv 608 + L_3(5) + L_3(11) \pmod{1216}$

(vi) $87 \equiv L_3(13) \ (mod\ 1216)$

La primera ecuación nos dice que $L_3(3) = 1 \pmod{1216}$, y aplicando el algoritmo de Euclides obtenemos de la tercera que

$$L_3(5) = 819 \pmod{1216}$$

Y de la sexta que

$$L_3(13) = 87 \pmod{1216}$$

De la cuarta obtenemos $L_3(2) = 30 - 608 - 2(819) = 216 \pmod{1216}$.

De la quinta que $L_3(11) \equiv 54 - 608 - L_3(5) \equiv 1059 \pmod{1216}$ y por último de la segunda

$$L_3(7) = 24 - 608 - 2L_3(2) - L_3(13) = 113 \pmod{1216}$$

De esta manera conocemos todos los logaritmos discretos de todos los elementos del conjunto base de factores primos.

Queremos resolver

$$3^k \equiv 37 \pmod{1216}$$

Calculemos $3^j . 37 \pmod{p}$ para valores aleatorios de j hasta que obtengamos un entero que pueda ser expresado como productos de primos en B. En nuestro caso:

$$3^{16} . 37 = 2^3 . 7.11 \pmod{1217}$$

Por lo tanto

$$L_3(37) = 3L_3(2) + L_3(7) + L_3(11) - 16 \equiv 588 \pmod{1216}$$

Y obtenemos

$$3^{588} = 37 \pmod{1217}$$

Nota: El tamaño de B es importante, Si B es demasiado pequeño, entonces será muy difícil hallar las potencias de g tal que factoricen con primos en B. Si B es demasiado grande, será fácil hallar relaciones, pero el álgebra necesaria para resolver los

logaritmos de los elementos de B será pesado, mientras mayores elementos tiene B el problema se torna más complicado.

(iii) Baby step- Giant step

Puesto que nuestro principal objetivo es resolver el problema de logaritmo discreto para curvas elípticas, vamos a considerar un grupo G dado aditivamente. Así, dados $P, Q \in G$; queremos resolver $kP = Q$. Vamos a denotar por N al orden de G y por simplicidad supondremos que P genera G. Este algoritmo, desarrollado por D. Shauk requiere aproximadamente $\sqrt{N}$ pasos, por lo tanto solo funciona bien para tamaños moderados de N.

Algoritmo Baby step-Giant step

1) Fijamos un entero $m \geq \sqrt{N}$ y calculamos mP.
2) Calculamos y guardamos los valores iP con $0 \leq i < m$.
3) Calculamos los puntos $Q - jmP$ con $j = 0,1,\cdots,m-1$ hasta que alguno coincida con la lista anterior.
4) Si $iP = Q - jmP$, tenemos que $Q = kP$ con $k = i + jm \pmod N$

¿Por qué este método funciona? Como $m^2 > N$, podríamos asumir que la solución de $kP = Q$, satisface $0 \leq k < m^2$. Tomamos $k = k_0 + mk_1$ con $k_0 \equiv k \pmod m$ y $0 \leq k_0 < m$, y $k_1 = \frac{k-k_0}{m}$.

Entonces $0 \leq k_1 < m$, cuando $i = k_0, j = k_1$ tenemos que

$$Q - k_1 mP = kP - k_1 mP = k_0 P$$

Luego, existe una coincidencia en la lista.

El punto iP se calcula sumando P (un baby step) a $(i-1)P$. El punto $Q - jmP$ se calcula sumando $-mP$ (un giant step) a $(Q - (j-1)mP)$, de allí el nombre. No necesitamos conocer el valor exacto de N, solo una cota superior. Para curvas elípticas sobre F_q podemos usar el teorema de Hasse: Obteniéndose que $m^2 \geq q + 1 + 2\sqrt{q}$.

Así por ejemplo, Sea $G = E(F_{41})$ donde E está dado por $y^2 = x^3 + 2x + 1$. Sea $P = (0,1)$, $Q = (30,40)$. Por el teorema de Hasse el orden de G es a lo mas 54,

tomamos $m = 8$. Usando una herramienta para calcular los puntos iP para $1 \leq i \leq 7$ se tiene:

$$(0,1), (1,39), (8,23), (38,38), (23,23), (20,28), (26,9)$$

Calculamos: $Q - jmP$ para $j = 0,1,2$ y obtenemos

$$\underbrace{(30,40)}_{j=0}; \underbrace{(9,25), \ldots, (30,1)}_{j=1}; \underbrace{(28,22), \ldots, (26,9)}_{j=2}$$

Punto en el que paramos puesto que coincide con $7P$, como estamos en $j = 2$ tenemos que

$$(30,40) = (7 + 2.8)P = 23P$$

Y por lo tanto $k = 23$.

V. MATERIALES Y MÉTODOS

5.1. Universo

Se trata de una investigación básica aplicada que considera la teoría de curvas elípticas sobre cualquier campo K, y de manera particular sobre campos finitos F_q.

5.2. Metodología

En nuestro caso no hay técnicas de recopilación de datos pues se trata de una investigación básica aplicada, por lo que hacemos uso del método inductivo deductivo. Usamos la teoría de las curvas elípticas sobre el campo de los números racionales y de manera particular la teoría sobre campos finitos en la solución del problema de logaritmo discreto de gran aplicabilidad en criptografía.

Se ha usado la herramienta **the HTML5/JavaScript visual tool** para la verificación de los resultados en la suma de puntos sobre una curva elíptica definida en un campo finito, así como con la multiplicación. Otra herramienta que se podría usar es el Pari/GP que es un sistema de algebra computacional libre, que está disponible en http/:pari.math.u-bordeaux.fr/.

VI. RESULTADOS

6.1. El problema del logaritmo discreto para curvas elípticas

Sea una curva elíptica E definida sobre un campo finito F_q, un punto $P \in E(F_q)$ de orden n, y un punto $Q \in \langle P \rangle$, hallar el entero $l \in [0, n-1]$ tal que $Q = lP$. El entero l es llamado el logaritmo discreto de Q en la base P, denotado por $l = \log_P Q$.

Los parámetros de la curva elíptica para sistemas criptográficos deben escogerse cuidadosamente a fin de resistir todos los conocidos ataques para el PLDCE:

6.1.1. El ataque búsqueda exhaustiva.

En este ataque se calcula $P, 2P, 3P, 4P, \ldots$ hasta que se tenga Q. El tiempo de corrida es aproximadamente n pasos en el peor caso y $n/2$ pasos en promedio. Por lo tanto, búsqueda exhaustiva puede ser evitado seleccionando curvas elípticas con parámetros y con n suficientemente grandes.

6.1.2. El ataque de Pohlig- Hellman

El algoritmo de Pohlig- Hellman reduce eficientemente el computo de $l = \log_P Q$ al computo de logaritmos discretos en los subgrupos primos de orden primo de $\langle P \rangle$.

Supongamos que la factorización prima de n es $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ la estrategia de Pohlig- Hellman es computar $l_i = l \ (mod p_i^{e_i})$ para cada $1 \leq i \leq r$ y luego resolver el sistema de congruencias

$$l = l_1 \ (mod \ p_1^{e_1})$$

$$l = l_2 \ (mod \ p_2^{e_2})$$

$$\vdots$$

$$l = l_r \ (mod \ p_r^{e_r})$$

Para $l \in [0, n-1]$. (El teorema chino del resto garantiza una única solución). Mostremos como el computo de cada l_i puede ser reducido al computo de e_i logaritmos discretos en el subgrupo de orden p_i de $\langle P \rangle$. Para simplificar la notación, escribimos p por p_i y e por e_i. Sea la representación de l_i en la base p.

$$l_i = z_0 + z_1 p + z_2 p^2 + \cdots + z_{e-1} p^{e-1}$$

Donde cada $z_i \in [0, p-1]$. Los dígitos $z_0, z_1, \ldots, z_{e-1}$ son computados uno a la vez como sigue. Primeramente computamos $P_0 = \frac{n}{p} P$ y $Q_0 = \frac{n}{p} Q$. Como el orden de P_0 es p, tenemos

$$Q_0 = \frac{n}{p} Q = l\left(\frac{n}{p} P\right) = lP_0 = z_0 P_0$$

Entonces $z_0 = \log_{P_0} Q_0$ puede ser obtenido resolviendo una instancia del PLDCE en $\langle P_0 \rangle$. Seguidamente calculamos $Q_1 = \left(\frac{n}{p^2}\right)(Q - z_0 P)$. Se tiene

$$Q_1 = \left(\frac{n}{p^2}\right)(Q - z_0 P) = \frac{n}{p^2}(l - z_0)P = (l - z_0)\left(\frac{n}{p^2} P\right) = (z_0 + z_1 p - z_0)\left(\frac{n}{p^2} P\right)$$
$$= z_1\left(\frac{n}{p} P\right) = z_1 P_0$$

Entonces $z_1 = \log_{P_0} Q_1$ puede ser obtenido resolviendo una instancia del PLDCE en $\langle P_0 \rangle$. En general, si los dígitos $z_0, z_1, \ldots, z_{t-1}$ han sido computados, entonces $z_t = \log_{P_0} Q_t$, donde

$$Q_t = \frac{n}{p^{t+1}}(Q - z_0 P - z_1 pP - z_2 p^2 P - \cdots - z_{t-1} p^{t-1} P)$$

6.1.3. Ataque rho de Pollard

La idea principal detrás del algoritmo de Pollard es hallar distintos pares (c', d') y (c'', d'') de enteros modulo n tal que

$$c'P + d'Q = c''P + d''Q$$

Luego

$$(c' - c'')P = (d'' - d')Q = (d'' - d')lP$$

Y así

$$(c' - c'') \equiv (d'' - d')l \ (mod\ n)$$

Entonces $l = \log_P Q$ puede ser obtenido calculando

$$l = (c' - c'')(d'' - d')^{-1} \ (mod\ n)$$

Un método natural para hallar tales pares (c', d') y (c'', d'') es seleccionar aleatoriamente enteros $c, d \in [0, n-1]$ y guardar las ternas $c, d, cP + dQ)$ en una tabla ordenada por la tercera componente hasta que un punto $cP + dQ$ sea obtenida por segunda vez, tal ocurrencia es llamada una colisión. Por The birthday paradox, el número esperado de iteraciones antes de una colisión se obtiene en aproximadamente $\sqrt{\pi n/2}$. El inconveniente de este algoritmo es la cantidad de espacio requerido para las $\sqrt{\pi n/2}$ ternas.

El algoritmo rho de Pollard halla (c', d') y (c'', d'') es estrictamente hablando el mismo tiempo esperado que el método natural, pero tiene un despreciable requerimiento de espacio. La idea es definir una función iteradora $f: \langle P \rangle \to \langle P \rangle$ tal que dado $X \in \langle P \rangle$ y $c, d \in [0, n-1]$ con $X = cP + dQ$, es fácil computar $\overline{X} = f(X)$ y $\overline{c}, \overline{d} \in [0, n-1]$ con $\overline{X} = \overline{c}P + \overline{d}Q$. Además f debería tener la característica de una función aleatoria.

La siguiente es un ejemplo de una función de iteración adecuada. Sea $\{S_1, S_2, \ldots, S_L\}$ una partición aleatoria de $\langle P \rangle$ en L de aproximadamente el mismo tamaño. Típicos valores del número de elementos de la partición L son 16 y 32. Por ejemplo, si $L = 32$ entonces un punto $X \in \langle P \rangle$ puede ser asignado a S_j si los 5 bits menos significantes de la x coordenada de X representa al entero $j - 1$. Escribimos $H(X) = j$ si $X \in S_j$ y llamamos a H la función partición. Finalmente, sea $a_j, b_j \in_R [0, n-1]$ para $1 \leq j \leq L$, entonces $f: \langle P \rangle \to \langle P \rangle$ está definida por

$$f(X) = X + a_j P + b_j Q, \text{ donde } j = H(X)$$

Observe que si $X = cP + dQ$ entonces $f(X) = \bar{X} = \bar{c}P + \bar{d}Q$ donde $\bar{c} = c + a_j \ mod\ n$ y $\bar{d} = d + b_j \ mod\ n$.

Ahora, cualquier punto $X_0 \in \langle P \rangle$ determina una sucesión $\{X_i\}_{i \geq 0}$ de puntos donde $X_i = f(X_{i-1})$ para $i \geq 1$. Como el conjunto $\langle P \rangle$ es finito, la sucesión eventualmente colisiona y entonces cicla siempre, esto es, existe un menor índice t para el que $X_t = X_{t+s}$ para algún $s \geq 1$ y entonces $X_i = X_{i-s}$ par todo $i \geq t + s$. Aquí t es llamado la

longitud de la cola y s es la longitud del ciclo de la sucesión. Si f se asume siendo una función aleatoria, entonces la sucesión tendrá su primera colisión después de aproximadamente $\sqrt{\pi n/2}$ términos. Además, la longitud de la cola esperada es $t \approx \sqrt{\pi n/8}$ y la longitud del ciclo esperado es $s \approx \sqrt{\pi n/8}$.

Una colisión, es decir, puntos X_i, X_j con $X_i, = X_j, i \neq j$ puede ser hallado usando el algoritmo de Floy donde uno computa pares (X_i, X_{2i}) de puntos para $i = 1,2,3, \ldots$ hasta que $X_i = X_{2i}$, después de computar un nuevo par, el anterior puede ser descartado; así el espacio de almacenamiento requerido es despreciable. El número esperado k de tales pares que fueron computados antes de $X_i = X_{2i}$ se ve fácilmente que satisfacen $t \leq k \leq t + s$.

En efecto, asumiendo que f es una función aleatoria, el valor esperado de k es alrededor de $1.0308\sqrt{n}$, y entonces el número esperado de operaciones sobre el grupo de curvas elípticas es cerca de $3\sqrt{n}$.

Algoritmo rho de Pollard

Entrada: $P \in E(F_q)$ de orden primo n. $Q \in \langle P \rangle$

Salida: El logaritmo discreto $l = \log_P Q$

1) Seleccione el número L de branches (por ejemplo $L = 16$ o $L = 32$)
2) Seleccione un función partición $H: \langle P \rangle \rightarrow \{1,2, \ldots, L\}$
3) Para $j = 1$ hasta $j = L$ hacer
   3.1. Seleccionar $a_j, b_j \in_R [0, n-1]$
   3.2. compute $R_j = a_j P + b_j Q$

4) Seleccione $c', d' \in_R [0, n-1]$ y compute $X' = c'P + d'Q$
5) Hacer $X'' \leftarrow X',\ c'' \leftarrow c',\ d'' \leftarrow d'$.
6) Repetir lo siguiente
   6.1. Compute $j = H(X')$
   Hacer $X' \leftarrow X' + R_j, c' \leftarrow c' + a_j \bmod n,\ d' \leftarrow d' + b_j \bmod n$
   6.2. Para i desde 1 a 2 hacer
   Compute $j = H(X'')$

Hacer Hacer $X'' \leftarrow X'' + R_j, c'' \leftarrow c'' + a_j \bmod n,\ d'' \leftarrow d'' + b_j \bmod n$

Hasta que $X' = X''$

7) Si $d' = d''$ entonces retorne "Error"
8) Caso contrario compute $l = (c' - c'')(d'' - d')^{-1} \bmod n$ y retorne l.

Presentamos un par de ejemplos de solución del problema del logaritmo discreto para curvas elípticas sobre campos finitos. Los resultados han sido verificados con la herramienta provista en la página **HTML5/JavaScript visual tool**, de uso gratuito.

6.2. Ejemplo. (El ataque de Pohlig- Hellman)

Considere la curva elíptica E definida sobre F_{7919} por la ecuación:

$$E: y^2 = x^3 + 1001x + 75$$

Sea $P = (4023,6036) \in F_{7919}$. El orden de P es $n = 7889 = 7^3.23$.

Sea $Q = (4135,3169) \in \langle P \rangle$. Deseamos determinar $l = \log_P Q$.

i) Primeramente determinamos $l_1 = \log_P 7^3$. Escribimos $l_1 = z_0 + z_1 7 + z_2 7^2$ y computamos

$$P_0 = 7^2 23P = (7801,2071)$$

$$Q_0 = 7^2 23Q = (7801,2071)$$

Como hemos hallado que $P_0 = Q_0$, entonces $z_0 = 1$. Seguidamente computamos

$$Q_1 = 72.23(Q - P) = (7285,14)$$

Hallamos que $Q_1 = 3P_0$, entonces $z_1 = 3$. Finalmente computamos

$$Q_2 = 23(Q - P - 3.7P) = (7285,7905)$$

Hallamos que $Q_2 = 4P_0$, entonces $z_2 = 4$. Así $l_1 = 1 + 3.7 + 4.7^2 = 218$

ii) Luego determinamos $l_2 = l \log_P 23$. Computamos

$$P_0 = 7^3P = (7190, 7003)$$

$$Q_0 = 7^3Q = (2599, 759)$$

Hallamos que $P_0 = 10P_0$, entonces $l_2 = 10$.

iii) Finalmente, resolvemos el par de congruencias

$$l \equiv 218 \ (mod \ 7^3)$$

$$l = 10 \ \ (mod \ 23)$$

Y obtenemos $l = 4334$.

6.3. Ejemplo (Algoritmo rho de Pollard)

Considere la curva elíptica definida sobre F_{229} por la ecuación

$$E: y^2 = x^3 + x + 44$$

El punto $P = (5, 116) \in F_{229}$ tiene orden primo $n = 239$. Sea $Q = (155, 166) \in \langle P \rangle$ queremos determinar $l = \log_P Q$

Seleccionamos la función partición $H: \langle P \rangle \rightarrow \{1,2,3,4\}$ con $L = 4$ ramas;

$$H(x, y) = (x \ mod \ 4) + 1$$

Y las cuatro ternas

$$[a_1, b_1, R_1] = [79, 163, (135,117)]$$

$$[a_2, b_2, R_2] = [206, 19, (96, 97)]$$

$$[a_3, b_3, R_3] = [87, 109, (84, 62)]$$

$$[a_4, b_4, R_4] = [219, 68, (72, 134)]$$

La siguiente tabla lista las ternas (c', d', X') y (c'', d'', X'') computados en el algoritmo para el caso $(c', d') = (54, 175)$ en el paso 4.

Iteración	c'	d'	X'	c''	d''	X''
-	54	175	(39,159)	54	175	(39, 159)
1	34	4	(160,9)	113	167	(130, 182)
2	113	167	(130, 182)	180	105	(36, 97)
3	200	37	(27, 17)	0	97	(108, 89)
4	180	105	(36, 97)	46	40	(223, 153)
...						
12	192	24	(57, 105)	213	104	(57, 105)

Luego se tiene

$$192P + 24Q = 213P + 104Q$$

Y entonces

$$l = (192 - 213).(104 - 24)^{-1}\ mod\ 239 = 176$$

VII. DISCUSIÓN DE RESULTADOS

7.1. Si bien es cierto podemos resolver el Problema del logaritmo discreto para curvas elípticas sobre campos finitos, teniendo los parámetros A y B relativamente pequeños, como se muestra en los ejemplos 6.2 y 6.3; para las aplicaciones en criptografía se dan los parámetros de la curva elíptica $E: y^2 = x^3 + Ax + B, A.B$ suficientemente grandes, de modo que la solución del problema del logaritmo discreto sobre curvas elípticas sea muy difícil o imposible de resolver para un enemigo que podría descubrir la clave dada por el algoritmo criptográfico basado en el problema de logaritmo discreto.

7.2. La dificultad del problema del logaritmo discreto depende del Grupo G. Podemos afirmar que el problema es fácil, y por lo tanto se tienen algoritmos de tiempo polinomial, por ejemplo cuando $G = (\mathbb{Z}_n, +)$. Bastaría hacer una búsqueda exhaustiva, como se afirma en 6.1.1.

7.3. El problema del logaritmo discreto es difícil, y por lo tanto se tienen algoritmos de tiempo subexponencial, por ejemplo cuando $G = (F_p, .)$, para p suficientemente grande, como se muestra en el algoritmo del Index-Calculus en 4.8.1 (ii) pag. 52-55, ejemplo dado por [2] LAWRENCE C. WASHINGTON, Elliptic Curves, Number Theory and Cryptography, pag.144, 145.

VIII. REFERENCIALES

[1] DARREL HANKERSON, ALFRED MENESES, **Guide to Elliptic Curve Cryptography**, New York Springer-Verlag. Inc 2004.

[2] LAWRENCE C. WASHINGTON, **Elliptic Curves, Number Theory and Cryptography**, Chapman & Hall/CRC, Second Edition,2008.

[3] DALE HUSEMOLLER. **Elliptic Curves**, Springer-Verlag New York, Inc. Second Edition 2004.

[4] J. W CASSELS, **Lectures on Elliptic curves, London Mathematical Society Student Test 24,** Cambridge University Press, 1991.

[5] ALVARO LOZANO ROBLEDO, **Buscando Puntos Racionales en curvas Elípticas: Métodos Explícitos,** 2006.

[6] WALTER MORA F. **Introducción a la Teoría de Números: Ejemplos y Algoritmos**, Instituto Tecnológico de Costa Rica, 2014.

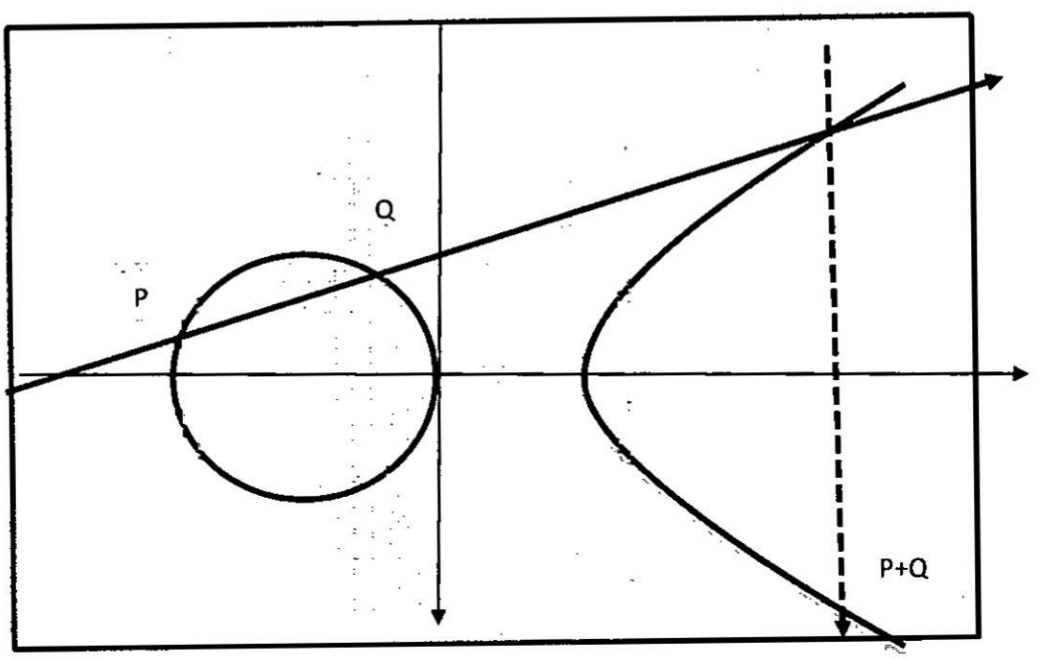
[7] JOSHEP H. SILVERMAN, JOHN TATE, **Rational Point on Elliptic Curves**, Springer Verlag, 1991.

IX. APÉNDICE

Representación gráfica de la ley de composición sobre el grupo de puntos sobre una curva elíptica.

GRÁFICO 4.3.

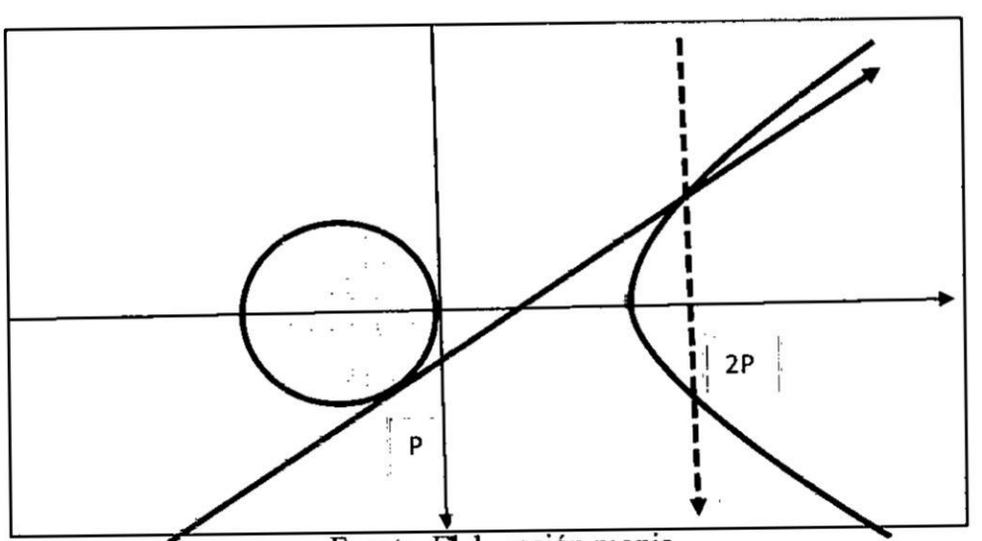
ADICIÓN DE PUNTOS SOBRE CURVAS ELÍPTICAS



Fuente. Elaboración propia.

GRÁFICO 4.4

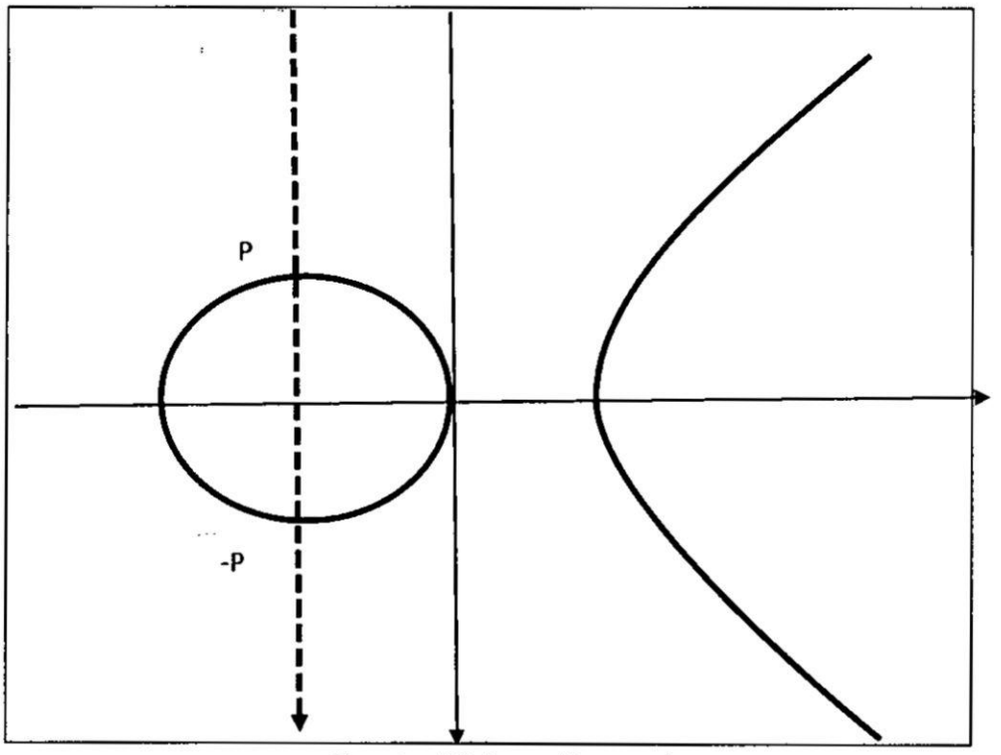
DUPLICACION DE UN PUNTO



Fuente. Elaboración propia.

GRÁFICO 4.5

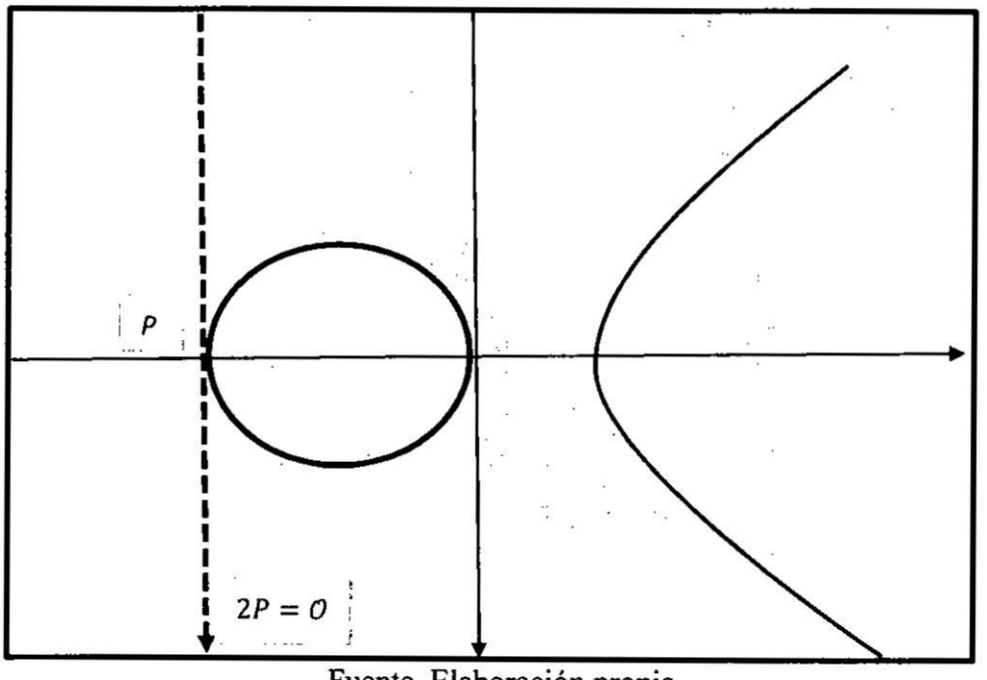
ELEMENTO OPUESTO



Fuente. Elaboración propia.

GRÁFICO 4.6

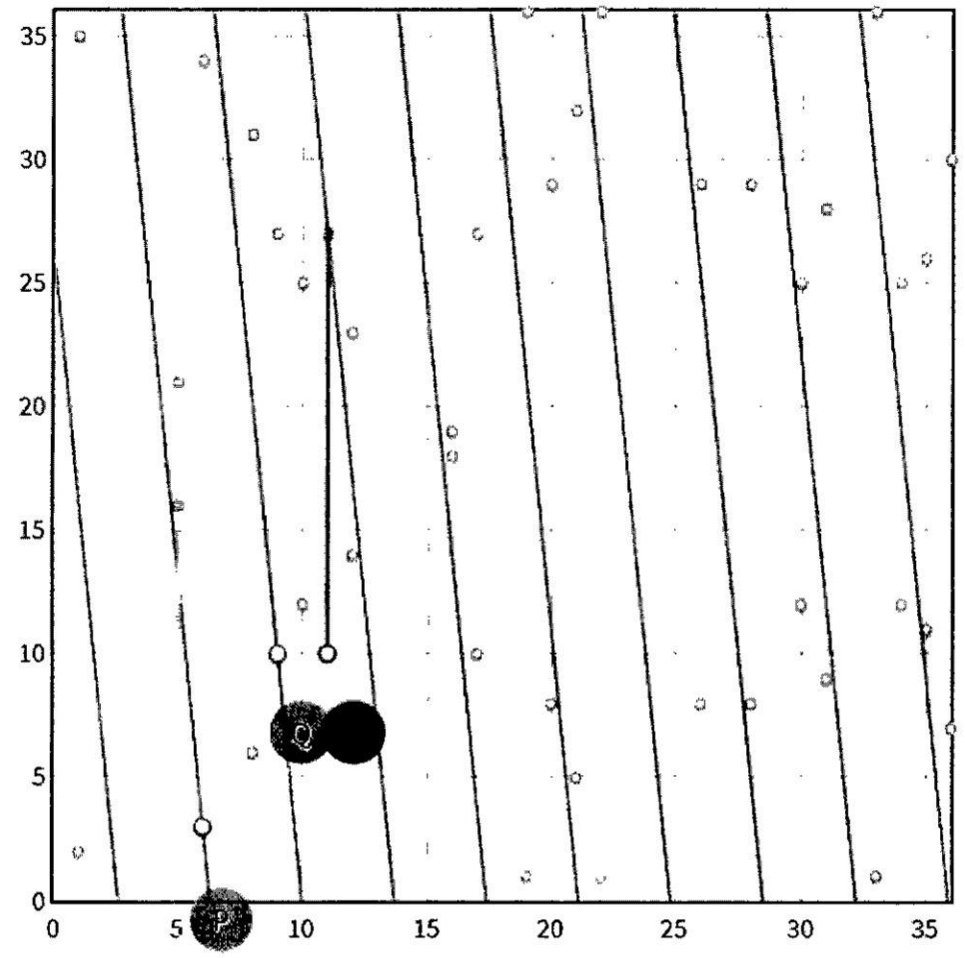
PUNTO DE ORDEN 2



Fuente. Elaboración propia.

Gráfico 4.7.

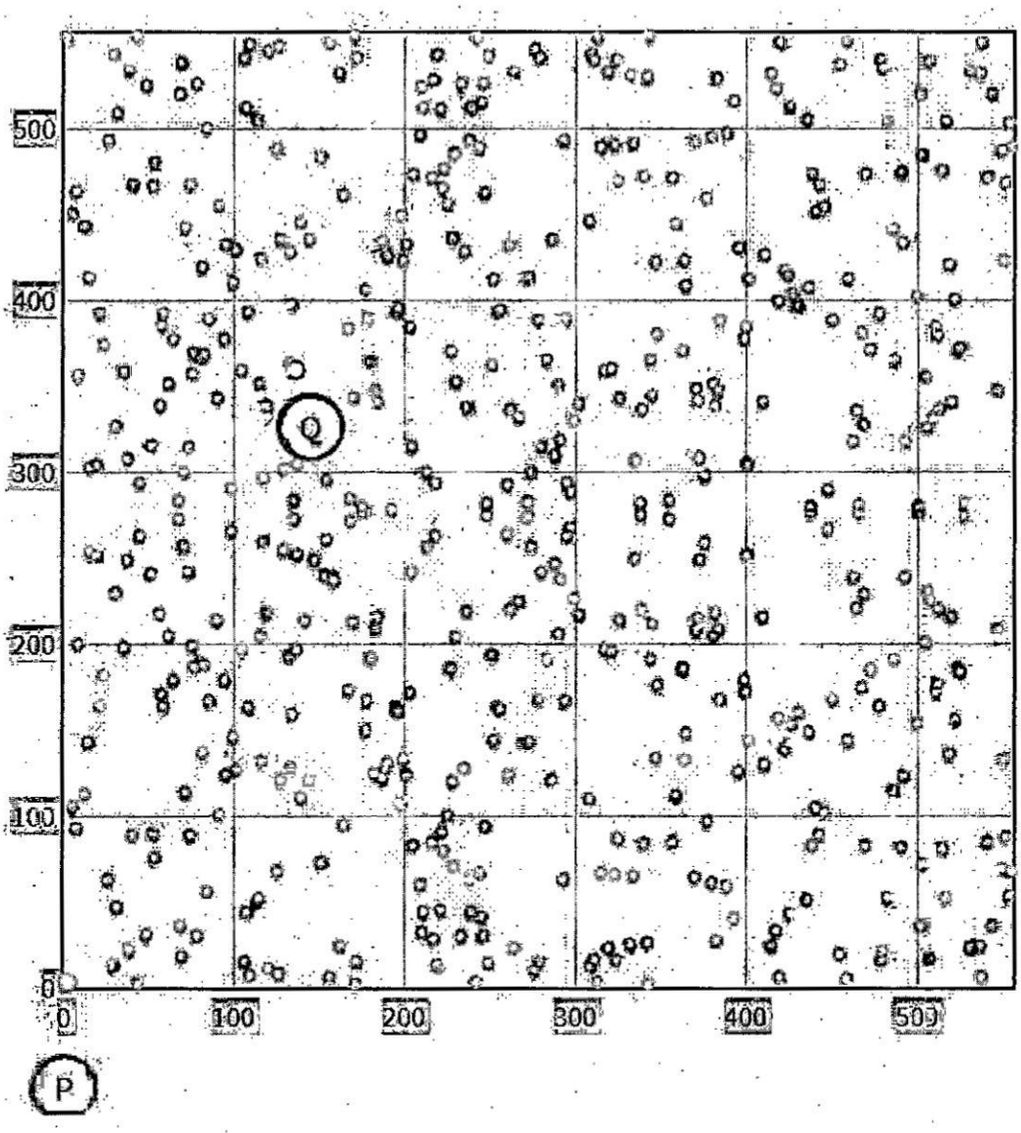
GRÁFICA DE PUNTOS EN UN CAMPO FINITO



Fuente: Elaboracićn propia con la herramienta visual **HTML5/JavaScript visual tool**.

GRÁFICO 4.8

GRÁFICA DE $y^2 = x^3 - 10x + 21$ EN F_{557}



Fuente: Elaboración propia con la herramienta visual **HTML5/JavaScript visual tool**, disponible en:

http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

X. ANEXOS

MATRIZ DE CONSISTENCIA

Formulación del problema	Objetivo general	Hipótesis	Metodología
¿Se puede usar la teoría de curvas elípticas sobre campos finitos para resolver el problema de logaritmo discreto?	Desarrollar la teoría de curvas elípticas sobre campos finitos para resolver el problema de logaritmo discreto.	La teoría de curvas elípticas sobre campos finitos se puede usar para resolver el problema de logaritmo discreto.	Se trata de una investigación básica aplicada, por lo que usaremos el método inductivo deductivo.
Sub problemas	Objetivos específicos	Hipótesis específicas	
1. Se pueden definir las curvas elípticas sobre campos finitos? 2. ¿Se puede resolver el problema del logaritmo discreto usando aritmética modular?	1. Desarrollar la teoría de curvas elípticas sobre curvas campos finitos. 2. Resolver el problema de logaritmo discreto usando aritmética modular.	1. Las curvas elípticas se pueden definir sobre campos finitos. 2. El problema del logaritmo discreto se puede resolver usando aritmética modular	Haremos un estudio dela teoría de curvas elípticas sobre el campo de los números racionales y lo aplicaremos a campos finitos. Resolveremos el problema del logaritmo discreto usando aritmética modular.