INTERMATHS, VOL. 3, NO. 2 (**2022**), **92–100**
https://doi.org/10.22481/intermaths.v3i2.11364

Uma Curva Elíptica sobre F_{23}

An Elliptic Curve over F_{23}

Jaime Edmundo Apaza Rodriguez [a,*]

[a] Universidade Estadual Paulista (UNESP), Câmpus de Ilha Solteira-SP, Brasil

* Correspondence: jaime.rodriguez@unesp.br

Resumo: Neste trabalho apresentamos um modelo de uma Curva Elíptica definida sobre um Corpo Primo. Nas primeiras seções fazemos um estudo preliminar das Curvas Elípticas e dos Corpos Finitos, em especial dos Corpos de Galois, com a operação de adição na curva elíptica (dependendo da característica do corpo em questão). Na última seção apresentamos o modelo de uma Curva Elíptica definida sobre o corpo F_{23}.

Palavras-chave: Curva Elíptica; Corpo Finito; Corpo Primo; Equação de Weierstrass; Característica de um Corpo.

Abstract: In this work we present a model of an Elliptic Curve defined over a prime field. In the first sections, we do a preliminary study of the curves Elliptic and Finite Fields, especially Galois Fields, with the addition operation on the elliptical curve (depending on the characteristic of the field in question). In the last section we present the model of an Elliptic Curve defined over the field F_{23}.

Keywords: Elliptic Curve; Finite Field; Prime Field; Weierstrass Equation; Characteristic of a Field.

Classification MSC: 11G07

1 Introdução

A Teoria das Curvas Elípticas é um dos mais belos assuntos da Matemática e tem aplicações em diversas áreas, como por exemplo em, Geometria Diferencial (Superfícies Mínimas), Teoria dos Números (último Teorema de Fermat, Teorema de Wiles-Taylor), Geometria Algébrica sobre Corpos Finitos (Teorema de Hasse-Weil, Hipótese de Riemann) e Criptografía (senhas, autenticações, assinaturas digitais, etc.)

As Curvas Elípticas se definem mediante equações cúbicas (polinômios de grau 3). Elas têm sido usadas para provar o Último Teorema de Fermat e se empregam também em Criptografia e em Fatoração de inteiros. É bom mencionar que estas curvas não são elipses.

As Curvas Elípticas são "regulares" ou "não-singulares", o que significa que não têm cúspides nem auto-interseções, e pode-se definir uma operação binária no conjunto de seus pontos de uma maneira geométrica natural, o que fornece a este conjunto uma estrutura de grupo abeliano.

As Curvas Elípticas podem definir-se sobre qualquer corpo $\mathbb{K}$. Se a característica de

Recebido em 19 de setembro de 2022; Aceito em 26 de dezembro de 2022; Publicado em 31 de dezembro 2022
ISSN 2675-8318

$\mathbb{K}$ não é nem 2 nem 3, então toda Curva Elíptica sobre $\mathbb{K}$ pode-se escrever na forma

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

onde a *e* b são elementos de $\mathbb{K}$, com $\Delta = 4a^3 + 27b^2 \neq 0$ (discriminante não-nulo), de modo que o polinômio $x^3 + ax + b$ não tenha nenhuma raiz dupla. Se a característica for 2 ou 3 será necessário considerar mais termos na equação acima.

Normalmente se define uma curva algébrica como o conjunto de todos os pontos (x, y) que satisfazem a equação acima dada, tais que x *e* y sejam elementos do fecho algébrico do corpo $\mathbb{K}$. Os pontos da curva cujas coordenadas pertençam ambas a $\mathbb{K}$ se chamam pontos $\mathbb{K}$-racionais. Se adicionarmos um ponto no "infinito", iremos obter a versão projetiva de tal curva. A condição sobre os coeficientes do polinômio que define a curva ($\Delta \neq 0$) é equivalente à não existência de pontos singulares da curva. O ponto no infinito é o único na Curva Elíptica, que é um ponto de inflexão e não é ponto singular. Portanto o gênero (um invariante) da curva é um.

Se tivermos dois pontos da curva, P *e* Q então podemos descrever, de forma unívoca, um terceiro ponto R, que seja a interseção da curva com a reta que passa pelos dois pontos P *e* Q. Se a reta é tangente à curva em um ponto, então esse ponto contaría duas vezes; e se a reta for paralela ao eixo y, definimos o terceiro ponto como o ponto no "infinito". Então justamente uma dessas condições será a que cumpra qualquer par de pontos de uma Curva Elíptica.

2 Curvas Elípticas

Definição 2.1. Uma Curva Elíptica E, definida sobre um corpo arbitrário $\mathbb{K}$ é uma curva projetiva plana, não singular, de grau 3 sobre $\mathbb{K}$, com um ponto $\mathbb{K}$-racional $\mathcal{O}$ (com coordenadas em $\mathbb{K}$) sobre a curva E.

Tal curva pode ser descrita pela chamada forma de Weierstrass, em coordenadas homogêneas x, y, z:

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

onde $a_1, \cdots, a_6 \in \mathbb{K}$, com discriminante $\Delta \neq 0$.

Este discriminante é uma expressão polinômica nos coeficientes $a_1, \cdots, a_6$. A restrição $\Delta \neq 0$ é necessária e suficiente para que E seja não-singular. A curva E tem exatamente um $\mathbb{K}$-racional ponto no "infinito" $\mathcal{O} = (0 : 1 : 0)$, obtido fazendo $z = 0$ na equação acima. Este ponto faz o papel da origem. Algumas vezes é preciso destacar o corpo $\mathbb{K}$ na definição da Curva Elíptica, denotando isto por $E/\mathbb{K}$.

Em geral estaremos interessados na parte afim da curva E, ou seja, quando $z \neq 0$. Em particular, para $z = 1$ temos

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

Para corpos $\mathbb{K}$ com característica maior do que 2, pode-se transformar a forma de Weierstrass, por meio da mudança de coordenadas:

$$x = x + \frac{a_1^2 + 4a_2}{12} \qquad e \qquad y = y + \frac{a_1}{2}x + \frac{a_3}{2},$$

para a forma afim $E : y^2 = x^3 + ax + b$, onde $a, b \in \mathbb{K}$, tal que o discriminante $\Delta = 4a^3 + 27b^2 \neq 0$. Esta forma é também conhecida como a forma curta de Weierstrass e é usada algumas vezes.

Observação 2.2. Para aplicações práticas, corpos finitos do tipo $\mathbb{K} = GF(2^m) = F_{2^m}$ são muito importantes. Para Curvas Elípticas sobre este tipo de corpos, a teoria acima mencionada deve ser modificada ligeramente.

Em 1955, Yutaka Taniyama respondeu algumas questões sobre acerca de Curvas Elípticas da forma $y^2 = x^3 + ax + b$, onde a e b são constantes. Em 1971, Yves Hellegouarch estudou a aplicação das Curvas Elípticas para resolver o Último Teorema de Fermat. As Curvas Elípticas também podem ser vistas nas construções matemáticas da Teoria dos Números e Geometria Algébrica, as quais tem encontrado numerosas aplicações criptográficas nos últimos anos.

O criptossistema com Curvas Elípticas (ECC) é relativamente novo. O ECC foi introduzido pela primeira vez por Miller e independentemente por Klobitz ao redor de 1980 e hoje tem evoluido para se tornar um sistema criptográfico maturo. O ECC, desde o seu inicio, foi proposto como uma alternativa para sistemas de chave pública tais como o DH (desenvolvido por Whitfield Diffie e Martin Hellman, um dos primeiros exemplos práticos de métodos de troca de chaves implementado dentro do campo da criptografia, publicado em 1976), DSA (Digital Signature Algorithm, codificação de chave pública usado apenas para gerar assinaturas digitais usando criptografia de Curva Elíptica. A assinatura baseia-se na assinatura do ElGamal, mas é computacionalmente mais econômica porque trabalha com um grupo menor de potências do corpo finito), RSA (sistema assimétrico desenvolvido por Rivest-Shamir-Adleman) e ElGamal (sistema com o uso de chaves assimétricas criado pelo egípcio Taher Elgamal em 1984).

Neste cenário, as Curvas Elípticas não introduzem novos algoritmos criptográficos, mas elas permitem implementar algoritmos ja existentes. Desta forma, as variantes de esquemas ja existentes podem ser planejados de modo que a sua segurança dependa de um problema subjacente de dificil solução.

3 Adição em Curvas Elípticas

Existe uma regra chamada Regra da Corda-Tangente para somar dois pontos sobre o conjunto de pontos de uma Curva Elíptica E definida no corpo $\mathbb{F}_p$ (denota-se por $E(\mathbb{F}_p)$), de modo a obter um terceiro ponto. Com essa operação de adição, o conjunto de pontos $E(\mathbb{F}_p)$ forma um grupo, tendo o elemento $\mathcal{O}$ como identidade. Este é o grupo usado para a implementação de criptossistemas com Curvas Elípticas.

(1) Se a característica de $\mathbb{F}_p$ é maior do que 3, a curva elíptica tem a forma

$$E : y^2 = x^3 + ax + b,$$

onde $a, b \in \mathbb{F}_p$, com $4a^3 + 27b^2 \neq 0$, junto com o ponto especial $\mathcal{O}$. Sabemos que $E(\mathbb{F}_p)$ um grupo abeliano, sendo o ponto $\mathcal{O}$ o elemento identidade.

Fórmulas de Adição: Seja $P = (x_1, y_1) \in E$. Então $-P = (x_1, -y_1)$. Se $Q = (x_2, y_2) \in E,\ Q \neq -P$, então $P + Q = (x_3, y_3)$, onde

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

sendo

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{se } P \neq Q \\ \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{se } P = Q, \end{cases}$$

(2) Se a característica de $\mathbb{F}_q$ é 2, temos dois tipos de curvas elípticas:

2a) Uma curva elíptica E sobre $\mathbb{F}_q$, cuja equação é $E : y^2 + cy = x^3 + ax + b$, onde $a, b, c \in \mathbb{F}_q,\ c \neq 0$, junto com o ponto especial $\mathcal{O}$. Neste caso tem-se:

Fórmulas de adição: Seja $P = (x_1, y_1) \in E$. Então $-P = (x_1, y_1 + c)$. Se $Q = (x_2, y_2) \in E,\ Q \neq -P$, então $P + Q = (x_3, y_3)$, onde

$$x_3 = \begin{cases} (\dfrac{y_1 + y_2}{x_1 + x_2})^2 + x_1 + x_2, & se \ \ P \neq Q \\ \\ \dfrac{x_1^4 + a^2}{c^2}, & se \ \ P = Q \end{cases}$$

e

$$y_3 = \begin{cases} (\dfrac{y_1 + y_2}{x_1 + x_2})(x_1 + x_3) + y_1 + c, & se \ \ P \neq Q \\ \\ (\dfrac{x_1^2 + a}{c})(x_1 + x_3) + y_1 + c, & se \ \ P = Q \end{cases}$$

2b) Uma curva elíptica E sobre $\mathbb{F}_q$, cuja equação é $E : y^2 + xy = x^3 + ax^2 + b$, onde $a, b \in \mathbb{F}_q,\ b \neq 0$, junto com o ponto especial $\mathcal{O}$. Neste caso tem-se:

Fórmulas de adição: Seja $P = (x_1, y_1) \in E$. Então $-P = (x_1, y_1 + x_1)$. Se $Q = (x_2, y_2) \in E,\ Q \neq -P$, então $P + Q = (x_3, y_3)$, onde

$$x_3 = \begin{cases} (\dfrac{y_1 + y_2}{x_1 + x_2})^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a, & se \ P \neq Q \\ \\ x_1^2 + \dfrac{b}{x_1^2}, & se \ \ P = Q \end{cases}$$

e

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

4 Corpos Finitos

Uma Curva Elíptica pode ser definida sobre qualquer corpo (por exemplo, reais, racionais, complexos, etc). No entanto, as Curvas Elípticas usadas em Criptografia são principalmente definidas sobre corpos finitos.

Um corpo é uma estrutura algébrica em que as operações de adição e multiplicação são bem-definidas. Os corpos são importantes objetos de estudo na Álgebra visto que constituem uma generalização útil de sistemas numericos, como os números racionais, os números reais e os números complexos. Em particular, são válidas as regras usuais de associatividade, comutatividade e distributividade.

Sistemas Criptográficos ou Criptossistemas com Curvas Elípticas, definidas sobre corpos finitos, baseiam sua segurança na versão elíptica do problema do logaritmo discreto (DLP), chamado de Problema do Logaritmo Discreto de Curva Elíptica (ECDLP). Aqui, o corpo subjacente dos inteiros, módulo um primo p, é substituído pelo grupo de pontos de uma Curva Elíptica definida sobre um corpo finito. Dado que o problema ECDLP é significativamente mais difícil do que o problema DLP, mesmo um sofisticado hacker requeriria um alto poder computacional e alguns anos para poder quebrar o Criptossistema. A implementação da Criptografia com Curvas Elípticas requer de várias escolhas tais como, o tipo de corpo finito, o algoritmo para implementar a operação no grupo de pontos da Curva Elíptica e os protocolos para Curvas Elípticas que influenciam a performance da ECC. As Curvas Elípticas têm se mostrado extremamente úteis em uma variedade de aplicações, incluindo testes de primalidade e fatoração inteira.

Criptossistemas com Curvas Elípticas também incluem distribuição de chaves, algoritmos de Criptografia e assinatura digital. O algoritmo de distribuição de chaves é usado para compartilhar uma chave secreta; já o algoritmo de Criptografia permite uma comunicação confidencial e os algoritmos de assinatura digital são usados para autenticar o signatário e validar a integridade da mensagem.

Definição 4.1. Um corpo finito consiste de um conjunto finito $\mathbb{F}$ de elementos junto com a descrição de duas operações, adição e multiplicação, de modo que todo elemento não nulo possua inverso multiplicativo.

Corpos finitos também são chamados corpos de Galois em honra ao matemático francês Évariste Galois.

Sabe-se que existe um corpo finito contendo q elementos se, e somente se, q é potência de um número primo. Além disso, tem-se que para cada tal q existe precisamente um corpo finito. O corpo finito contendo q elementos é denotado por $\mathbb{F}_q$.

Neste trabalho usaremos unicamente dois tipos de corpos finitos $\mathbb{F}_q$: Corpos finitos com $q = p$, sendo p um número primo ímpar (Corpos Primos) e corpos finitos com $q = 2^m$, para algum $m \in \mathbb{N}$, sob a operação binária (Corpos Binários). A ordem de um corpo finito é o seu número de elementos. Existe um corpo finito de ordem q se, e somente se, q é potência de um primo p, ou seja, $q = p^m$, para algum $m \in \mathbb{N}$.

Se somamos a identidade multiplicativa 1 a si mesma em $\mathbb{F}$ e nunca dá zero, dizemos que $\mathbb{F}$ tem característica zero; neste caso $\mathbb{F}$ contém uma cópia do corpo dos números racionais. Caso contrário, existe um número primo p tal que $1 + 1 + \cdots + 1 = 0$ (p vezes) e p é a característica do corpo. Neste caso $\mathbb{F}$ contém uma cópia do corpo $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$,

que é chamado de seu corpo primo.

Se $q = p^m$, onde p é um número primo e m inteiro positivo, então p é a característica de $\mathbb{F}_p$ e m é dito de grau da extensão $\mathbb{F}_p$ de $\mathbb{F}$.

A maioria das normas que especificam as técnicas da Criptografia com Curvas Elípticas restringem a ordem do corpo finito subjacente a ser um número primo ímpar ($q = p$) ou uma potência de 2 ($q = 2^m$).

Seja p um número primo. O corpo finito $\mathbb{F}_p$, chamado de corpo primo, está formado pelo conjunto de inteiros $\{0, 1, 2, \cdots, p-1\}$ junto às seguintes operações aritméticas:

(1) Adição módulo p: Se a *e* $b \in \mathbb{F}_p$, então $a + b = r$, onde r é o resto da divisão de $a + b$ por p, com $0 \leq r \leq p - 1$.

(2) Multiplicação módulo p: Se a *e* $b \in \mathbb{F}_p$, então $a \cdot b = s$, onde s é o resto da divisão de $a \cdot b$ por p, com $0 \leq s \leq p - 1$.

(3) Inversão módulo p: Se a é um elemento não-nulo de $\mathbb{F}_p$, o inverso de a, módulo p, denotado por a^{-1}, é o único inteiro $c \in \mathbb{F}_p$ para o qual vale $a \cdot c = 1$.

5 Corpos de Galois

A principal razão para o atrativo dos sistemas ECC é o fato de que não existe qualquer algoritmo sub-exponencial conhecido que resolva adequadamente o problema do logaritmo discreto na curva escolhida. Isto significa que parâmetros significativamente pequenos podem ser usados no ECC comparados com outros sistemas competitivos tais como RSA, DH e DSA. Isto ajuda a ter tamanhos de chaves menores e, portanto, cálculos mais rápidos.

Definição 5.1. Um grupo de curva elíptica sobre o Corpo de Galois $E_p(a, b)$, onde $p > 3$ é primo, é o conjunto de soluções ou pontos $P = (x, y) \in E_p(a, b)$ que satisfazem a equação

$$y^2 = x^3 + ax + b \ (mod\ p),$$

para $0 \leq x < p$, junto com o ponto extra $\mathcal{O}$, chamado de ponto no infinito.

Para um ponto dado $P = (x_p, y_p)$, temos que x_p, y_p são as coordenadas de P. O número de pontos em $E_p(a, b)$ é denotado por $|E_p(a, b)|$.

O resultado a seguir (Teorema de Hasse) estabelece uma importante cota para o número de pontos de uma Curva Elíptica.

Teorema 5.2.

$$p + 1 - 2\sqrt{p} \leq |E_p(a, b)| \leq p + 1 + 2\sqrt{p}.$$

As constantes a *e* b são inteiros não-negativos menores que o número primo p e satisfazem a equação

$$\triangle = 4a^3 + 27b^2 \neq 0 (mod\ p).$$

Para cada valor de x, é preciso determinar se é ou não um resíduo quadrático. Se for o caso, então há dois valores no grupo elíptico. Se não for, então o ponto não está no grupo elíptico $E_p(a, b)$.

Porque os coeficientes do polinômio cúbico na equação $y^2 = x^3 + ax + b$ devem satisfazer a condição $\triangle = 4a^3 + 27b^2 \neq 0 \ (mod\ p)$? Observemos que

$$\triangle = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 = \frac{4a^3 + 27b^2}{4 \times 27}$$

é o discriminante do polinômio cúbico $f(x) = x^3 + ax + b$. Se $\triangle = 0$ então a equação $f(x) = 0$ tem, pelo menos, uma raiz dupla e então o ponto $P_0 = (x, 0)$ está sobre a curva E. Para $F(x, y) = y^2 - x^3 - ax - b$, este ponto satisfaz

$$\frac{\partial F}{\partial y}|_{P_0} = 0, \quad \frac{\partial F}{\partial x}|_{P_0} = 0.$$

Isto significa que P_0 é um ponto singular para o qual não há uma definição de reta tangente real e, assim, $E_p(a, b)$ não pode ser um grupo.

Curvas elípticas definidas sobre corpos finitos $GF(2^m)$, de característica 2, os quais têm 2^m elementos, também têm sido construidas e estão sendo padronizadas para seu uso no ECC como alternativa para as curvas elípticas sobre corpos finitos primos.

6 A Curva Elíptica sobre $\mathbb{F}_{23}$

Consideremos o primo $p = 23$ e a curva elíptica $E : y^2 = x^3 + x + 4$ definida sobre $\mathbb{F}_{23}$. Observar que nesta equação temos $a = 1$ *e* $b = 4$.

Verifica-se que

$$4a^3 + 27b^2 = 436(mod\ 23) = 22 \neq 0,$$

e portanto E é uma curva elíptica.

Agora iremos determinar o conjunto de resíduos quadráticos, Q_{23}, do conjunto reduzido de resíduos $\mathbb{Z}_{23} = \{1, 2, 3, \cdots, 21, 22\}$.

O conjunto Q_{23}, contendo $(p-1)/2 = 11$ resíduos quadráticos, é

$$Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

Agora, para $0 \leq x < p$, calculamos $y^2 = x^3 + x + 4(mod\ 23)$ e verificamos se y^2 esta ou não no conjunto Q_{23} (tabelas 1 e 2 a seguir).

Tabela 1: Resíduos Quadráticos de Q_{23}

$x^2(mod\ p)$	$(p-x)^2(mod\ p)$	=
$1^2(mod\ 23)$	$22^2(mod\ 23)$	1
$2^2(mod\ 23)$	$21^2(mod\ 23)$	4
$3^2(mod\ 23)$	$20^2(mod\ 23)$	9
$4^2(mod\ 23)$	$19^2(mod\ 23)$	16
$5^2(mod\ 23)$	$18^2(mod\ 23)$	2
$6^2(mod\ 23)$	$17^2(mod\ 23)$	13
$7^2(mod\ 23)$	$16^2(mod\ 23)$	3
$8^2(mod\ 23)$	$15^2(mod\ 23)$	18
$9^2(mod\ 23)$	$14^2(mod\ 23)$	12
$10^2(mod\ 23)$	$13^2(mod\ 23)$	8
$11^2(mod\ 23)$	$12^2(mod\ 23)$	6

Tabela 2: Resíduos Quadráticos de Q_{23} e suas raízes

x	y^2	$y^2 \in Q_{23}$	y_1	y_2
0	4	sim	2	21
1	6	sim	11	12
2	14	nâo		
3	11	não		
4	3	sim	7	16
5	19	não		
6	19	não		
7	9	sim	3	20
8	18	sim	8	15
9	6	sim	11	12
10	2	sim	5	18
11	12	sim	9	14
12	19	não		
13	6	sim	11	12
14	2	sim	5	18
15	13	sim	6	17
16	22	não		
17	12	sim	9	14
18	12	sim	9	14
19	5	não		
20	20	não		
21	17	não		
22	2	sim	5	18

Portanto os pontos em $E_p(a,b) = E_{23}(1,4)$ são, o ponto no infinito $\mathcal{O}$ e os pontos:

$$(0,2),\ (0,21),\ (1,11),\ (1,12),\ (4,7),\ (4,16),\ (7,3),\ (7,20),\ (8,8),\ (8,15),$$

$$(9,11),\ (9,12),\ (10,5),\ (10,18),\ (11,9),\ (11,14),\ (13,11),\ (13,12),\ (14,5),$$

$$(14,18),\ (15,6),\ (15,17),\ (17,9),(17,14),\ (18,9),\ (18,14),\ (22,5),\ (22,18).$$

Observação 6.1. Na prática, o número primo p é escolhido de modo a ser muito grande. Tomemos, por exemplo, um grupo grande de pontos com o número primo

$$p = 6\ 227\ 101\ 735\ 386\ 680\ 763\ 835\ 789\ 423\ 207$$

$$666\ 416\ 083\ 908\ 700\ 390\ 324\ 961\ 279.$$

Existe uma curva definida sobre este espaço da forma $E : y^2 = x^3 + ax + b\ (mod\ p)$, onde a e b são dois números grandes cuidadosamente escolhidos de modo que a curva não seja fraca e que $4a^3 + 27b^2 \neq 0(mod\ p)$. Esta curva contém exatamente N pontos, onde

$$N = 6\ 227\ 101\ 735\ 386\ 680\ 763\ 835\ 789\ 423$$

$$337\ 720\ 473\ 986\ 773\ 608\ 255\ 189\ 015\ 329.$$

Estes pontos formam um grupo, de acordo com a regra anterior, que é ideal para usar o algoritmo Diffie-Hellman de Curva Elíptica. Computadores modernos não têm problemas em lidar com números deste tamanho, que na verdade são muito menores que aqueles usados nos tradicionais criptossistemas DH e RSA. Se consideramos o número p como

binário, observa-se que ele tem a forma especial, $p = 2^{192} - 2^{64} - 1$, o que torna o cálculo mais fácil. É interessante observar que p e N são muito "próximos" um do outro, relativamente falando, pois eles diferem apenas na metade de seus bits. A teoria das Curvas Elípticas já previa isto.

ORCID.
Jaime Edmundo Apaza Rodriguez https://orcid.org/0000-0002-1359-9898

Referências

1. J. A. Buchmann, "Introdução à Criptografia", Berkeley, São Paulo, 2002.
2. N. Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag, New York, 1994.
3. N. Koblitz, A. Menezes and S. Vanstone, "The State of Elliptic Curve Cryptography, Designs, Codes and Cryptography", 19, 173-193 (2000).
4. K. Rabah, "Theory and Implementation of Elliptic Curve Cryptography", Journal of Applied Sciences 5(4); 604-633, 2005.
5. N. Torii and K. Yokoyama, "Elliptic Curve Cryptosystem", Fujitsu Sci. Tech. J., 36, 2, pp. 140 - 146 (2000).