Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Criptografia e Curvas Elípticas

Vania Batista Schunck Flose

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática Universitária do Departamento de Matemática como requisito parcial para a obtenção do grau de Mestre

Orientador
Prof. Dr. Henrique Lazari

2011

111	Flose, Vania B. S.
X111x	Criptografia e Curvas Elípticas/ Vania Batista Schunck Flose- Rio Claro: [s.n.], 2011.
	55 f. : fig.
	Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.
	Orientador: Henrique Lazari
	1. Criptografia. 2. Corpo finito. 3. Problema do Logaritmo Discreto. 4. Teorema de Hasse. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Vania Batista Schunck Flose

Criptografia e Curvas Elípticas

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Prof. Dr. Henrique Lazari
Orientador

Prof. Dr. Jaime Edmundo Apaza Rodriguez
FE - UNESP - Ilha Solteira

Profa. Dra.Carina Alves
IGCE - UNESP - Rio Claro

Rio Claro, 18 de novembro de 2011

Dedico este trabalho à minha mãe e ao meu noivo: Sara e Maurício.

Agradecimentos

Primeiramente a Deus que é onipresente, onisciente e onipotente.

À minha família pelo carinho, compreensão e estímulo em especial a minha mãe, que mesmo sem saber muito sobre matemática, se esforçou para ensinar-me as primeiras “continhas”.

Ao professor Henrique Lazari pela compreensão e paciência.

Aos professores da UNESP de Ilha Solteira que foram mais do que professores.

Aos meus amigos que de diversas formas me ajudaram na minha caminhada "matemática": Adriana, Ana Paula, Andréia, Bruno, Divane, Douglas, Elen, Marinéia, Rafael, Rejane, Thalita e Thiago.

Aos meus amigos que me ajudaram em oração nos momentos decisivos: Denise, Elisa, Érica, Fernando, Heidi, João e Selma.

Aos meus amigos da Igreja Batista Central, em especial as famílias Amaral e Batista sempre receptivos partilhando do aconchego de seus lares, e aos amigos da Primeira Batista de São Caetano do Sul pelo apoio.

Aos meus alunos e aos amigos de trabalho no Instituto Federal de São Paulo, pelo estímulo.

E por último, e não menos importante, Maurício, meu grande companheiro, presente em todas as horas.

"A matemática é a rainha das ciências e a aritmética é a rainha da matemática"

Gauss

Resumo

Com o crescimento da comunicação nos dias atuais, a segurança na troca de informações tem se tornado cada vez mais importante o que tem dado destaque a Criptografia. A criptografia consiste de técnicas baseadas em conceitos matemáticos que tem por objetivo transmitir informações sigilosas forma segura através de canais monitorados por terceiros. Um ramo da Criptografia que vem crescendo está ligado ao estudo de curvas elípticas, que é uma das áreas mais ricas da matemática. O nome "curvas elípticas" é de certa forma enganoso, pois diferente do sentido literal da palavra, que leva a pensar em elipses, se trata de equações relacionadas a um determinado tipo de curva algébrica. Neste trabalho, as curvas elípticas serão estudadas do ponto de vista da álgebra e da teoria dos números com o objetivo de conhecer a Criptografia de Curvas Elípticas que é uma variação do Problema do Logaritmo Discreto.

Palavras-chave: Criptografia, Corpo finito, Problema do Logaritmo Discreto, Teorema de Hasse.

Abstract

With the growth of communication these days, security in exchange for information has become increasingly important what has given prominence to Cryptography. Encryption techniques is based on concepts mathematical aims to transmit sensitive information securely through channels monitored by third parties. A branch of cryptography that has growing up is connected to the study of elliptic curves, which is one of the most rich mathematics. The name " elliptic curves"is somewhat misleading, as different from the literal sense of the word, which makes one think of ellipses if equations is related to a certain type of algebraic curve. in this work, elliptic curves are studied from the viewpoint of algebra and of number theory in order to know the Curve Cryptography Elliptic is a variation of the discrete logarithm problem.

Keywords: Cryptography, Finite field, Discrete Logarithm Problem, Hasse's theorem.

Sumário

1 Pré-requisitos

1.1 Álgebra

Vamos ver neste capítulo alguns conceitos e resultados sa Álgebra Abstrata e da Teoria dos Números de grande importância para nosso estudo

1.1.1 Grupos

Uma das estruturas mais simples da álgebra é o grupo, que consiste em um conjunto não-vazio e uma operação inversível.

Definição 1.1. *Seja $*$ uma operação definida em um conjunto G. Dizemos que o par $(G, *)$ é um grupo se e somente se:*

- *O conjunto G é fechado sob a operação $*$, isto é, $\forall g, h \in G$, $g * h \in G$.*
- *A operação $*$ é associativa, isto é, $\forall g, h, k \in G$, $(g * h) * k = g * (h * k)$*
- *Existe um elemento identidade $e \in G$ para $*$, isto é, $\exists e \in G$, $\forall g \in G$, $g * e = e * g = g$*
- *Para todo elemento $g \in G$ existe um elemento inverso $h \in G$, $\forall g \in G$, $\exists h \in G$, $g * h = h * g = e$*

Definição 1.2. *Seja $(G, *)$ um grupo. Dizemos que esse grupo é abeliano se $*$ for um operação comutativa em G (isto é, $\forall g, h \in G, g * h = h * g$).*

Proposição 1.1. *Se $(G, *)$ um grupo, então*

1. *o elemento neutro é único;*
2. *o elemento inverso é único;*
3. *se a^{-1} e b^{-1} são os inversos de a e b respectivamnte, então $(a * b)^{-1} = a^{-1} * b^{-1}$.*

Exemplo 1.1. $(\mathbb{Z}, +)$: O conjunto dos números inteiros com a operação de adição usual é um grupo abeliano, pois vale o axioma da comutatividade, com o elemento neutro 0, e o inverso de um elemento $a \in \mathbb{Z}$ é o oposto em $\mathbb{Z}$. Como a operação nesse grupo é a adição, o chamamos de grupo aditivo.

Definição 1.3. *Seja n um inteiro positivo. Definimos*

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : mdc(a, n) = 1\}$$

Exemplo 1.2. Consideremos $\mathbb{Z}_{14}^*$. Os elementos invertíveis para a multiplicação módulo 14, que denotamos por $(\otimes)$ em $\mathbb{Z}_{14}^*$,são os elementos relativamente primos com 14, a saber: 1, 3, 5, 9, 11 e 13. Assim,

$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$$

A tabela de $\otimes$ para $\mathbb{Z}_{14}^*$ é a seguinte:

$\otimes$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

Os inversos dos elementos neste $\mathbb{Z}_{14}^*$ podem ser encontrados na tabela acima, assim:

$$\begin{array}{llllll} 1^{-1} = 1 & 3^{-1} = 5 & 5^{-1} = 3 \\ 9^{-1} = 11 & 11^{-1} = 9 & 13^{-1} = 13 \end{array}$$

Proposição 1.2. *Seja n um inteiro positivo. Então, $(\mathbb{Z}_n^*, \otimes)$ é um grupo.*

Definição 1.4. *A ordem de um grupo é o número de elementos do conjunto G. Denotamos por $|G|$.*

Exemplo 1.3. Seja o grupo aditivo $(\mathbb{Z}_n, \oplus)$, onde $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ e $\oplus$ é a soma seguida do cálculo do resto da divisão por n. Dessa forma $\mathbb{Z}_n$ tem n elementos, sendo eles $0, 1, ...,$ e $n-1$. Portanto o grupo $(\mathbb{Z}_n, \oplus)$ tem ordem n.

G pode ser um grupo de ordem infinita, por exemplo $(\mathbb{Z}, +)$. Neste caso dizemos que a ordem de G é infinita.

Definição 1.5. *Seja $(G, *)$ um grupo, e seja $H \subseteq G$. Se $(H, *)$ for também um grupo com a restrição à H da operação de G, o chamamos de subgrupo de $(G, *)$.*

Exemplo 1.4. $H = \{0, 2, 4, 6, 8\}$ é um subgrupo de $(\mathbb{Z}_{10}, \oplus)$.
Note que H contém os elementos pares de $\mathbb{Z}_{10}$. Se somarmos dois números pares arbitrários, o resultados é par, e quando reduzimos o resultado $\mod 10$, a resposta ainda é par. Vemos que $0 \in H$ e que os inversos de $0, 2, 4, 6, 8$ são $0, 8, 6, 4, 2$, respectivamente. Portanto, H é um subgrupo de $(\mathbb{Z}_{10}, \oplus)$

Um elemento de G da forma $a_1^{m_1} * a_2^{m_2} * ... * a_k^{m_k}$, onde $a_i \in X$, $m_i \in \mathbb{Z}$ é chamado *palavra* em X. O conjunto de todas estas palavras em X é um subgrupo de G, chamado *subgrupo gerado por X*. Se G é este subgrupo, dizemos que G é gerado por X e denotamos por $G = \langle X \rangle$ e X é chamado um conjunto de geradores.

Definição 1.6. *Seja $a \in G$, onde $(G, *)$ é um grupo. A ordem de a é a ordem de $\langle a \rangle$, ou equivalente no caso finito, a ordem de a é menor inteiro positivo n tal que $a^n = e$.*

Definição 1.7. *Seja $(G, *)$ um grupo. Um elemento $a \in G$ é chamado um gerador de G se, e somente se, todo elemento de G pode ser expresso em termos de a e a^{-1} utilizando apenas a operação $*$. Neste caso, dizemos que $(G, *)$ é um grupo cíclico.*

Os grupos de ordem finita são chamados de *gruposfinitos*, e são os mais interessantes no estudo da criptografia.

Proposição 1.3. *Sejam $(G, *)$ um grupo finito de ordem $n + 1$ e $g \in G$. Então, para algum inteiro positivo n, temos*

$$g^{-1} = \underbrace{g * g * g * ... * g}_{nvezes}.$$

Teorema 1.1. *Todo grupo cíclico é abeliano.*

Teorema 1.2. *Todo subgrupo de um grupo cíclico é cíclico.*

Definição 1.8. *Seja $(G, *)$ um grupo. Dizemos que G é um grupo de torção se todo elemento de G é de ordem finita. Se apenas a identidade $e \in G$ tem ordem finita, então G é livre de torção.*

Vejamos agora algumas relações em um grupo finito, utilizando o número de elementos do grupo e do subgrupo. Isto torna mais fácil a tarefa de determinar os subgrupos de um dado grupo finito.

Teorema 1.3. ***(Lagrange)*** *Seja $(H, *)$ um subgrupo de um grupo finito $(G, *)$, e sejam $a = |H|$ e $b = |G|$. Então $a|b$.*

Teorema 1.4. *Todo grupo finito de ordem prima é cíclico.*

Teorema 1.5. *Se G é um grupo cíclico de ordem n, então a ordem de qualquer elemento $a \in G$ divide n.*

Corolário 1.1. *Se G é um grupo finito e $a \in G$, então $a^{|G|} = e$*

Definição 1.9. *Sejam os grupos $(G, *)$ e $(H, \bullet)$. Uma função $f : G \to H$ é um isomorfismo (de grupos) se, e somente se, f é bijetiva e se verifica*

$$\forall g, h \in G, f(g * h) = f(g) \bullet f(h).$$

Se existe um isomorfismo de G para H, dizemos que G é isomorfo a H e escrevemos $G \cong H$.

Teorema 1.6. *Seja $(G, *)$ um grupo cíclico finito e $n = |G|$. Então, $(G, *)$ é isomorfo a $(\mathbb{Z}_n, \oplus)$.*

1.1.2 Anéis

A noção de anel surgiu a partir da sistematização das propriedades dos números inteiros no século XIX, mas apenas no século XX as propriedades foram organizadas na forma das definições que são utilizadas hoje.

Definição 1.10. *Diz-se que um conjunto A com as operações binárias de adição $(+)$ e multiplicação $(.)$ é um anel se:*

1. *$(A, +)$ é um grupo abeliano.*

   - *Associatividade: Quaisquer que sejam $a, b, c \in A$ temos que*

     $$a + (b + c) = (a + b) + c;$$

   - *Elemento neutro: Existe um elemento neutro $0 \in A$ tal que para todo $a \in A$,*

     $$a + 0 = 0 + a = a;$$

   - *Elemento inverso: Dado $a \in A$, existe um elemento $-a \in A$, chamado inverso de a, tal que*

     $$a + (-a) = (-a) + a = 0;$$

   - *Comutatividade: Para todo $a, b \in A$, temos que $a + b = b + a$.*

2. *$(A, .)$ é um semigrupo, ou seja, em A é válida as seguintes propriedades:*

   - *Fechamento: Para todo $a, b \in A$, $a.b \in A$;*
   - *Associatividade: Quaisquer que sejam $a, b, c \in A$ temos que*

     $$a.(b.c) = (a.b).c;$$

3. *Em A, a operação "." é distributiva em relação a "+", ou seja:*

   - *Quaisquer que sejam $a, b, c \in A$ temos que*

$$\text{à esquerda } (a+b).c = a.c + b.c$$
$$\text{à direita } a.(b+c) = a.b + a.c$$

Definição 1.11. *Se além dessas propriedades A satisfaz também essas outras duas:*

- *Elemento neutro na multiplicação ou Elemento identidade: Existe um elemento $1 \in A$ tal que para todo $a \in A$, $a.1 = 1.a = a$;*
- *Comutatividade na multiplicação: Para todo $a, b \in A$, temos que $a.b = b.a$*

então dizemos que A é um anel comutativo com identidade.

Definição 1.12. *Seja A um anel. Dizemos que um elemento $a \in A$, $a \neq 0$, é* divisor de zero *se existe $b \in A$, $b \neq 0$,tal que $a.b = 0 \in A$.*

Definição 1.13. *Se um anel comutativo com identidade A não possui divisores de zero, então A é dito anel de integridade.*

Proposição 1.4. *(Lei do cancelamento): Seja A um anel de integridade, temos que dados $a, b, c \in A$ com $c \neq 0$, então:*

$$a.c = b.c \Rightarrow a = b$$
$$c.a = c.b \Rightarrow a = b$$

1.1.3 Corpos

Definição 1.14. *Seja A um anel comutativo com identidade. Dizemos que $a \in A^*$ é inversível se existe $a^{-1} \in A$, tal que*

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

Se para todo $a \in A^*$ existir a^{-1}, dizemos que A é um *corpo*.

Teorema 1.7. *Todo corpo é um anel de integridade, ou seja, dado um corpo K e $a \in K$, $a \neq 0$, então a não é divisor de zero.*

Teorema 1.8. *Todo anel de integridade com um número finito de elementos é um corpo.*

Teorema 1.9. *Temos que $a \in \mathbb{Z}_n$ é inversível para a multiplicação se, e somente se, $mdc(a, n) = 1$*

Teorema 1.10. *O anel $\mathbb{Z}_n$ é um corpo se, e somente se, n é primo.*

1.1.4 Anel de polinômios

Seja $(A, +, .)$ um anel. Um polinômio numa variável sobre A é uma sequência $(a_0, a_1, ..., a_n, ...)$, onde $a_i \in A$ para todo índice e onde $a_i \neq 0$ somente para um número finito de índices. Denotamos por $A[X]$ o conjunto formado por tais polinômios.

Teorema 1.11. *Seja A um anel. Temos que:*

1. *Se A é um anel comutativo então $A[X]$ também é um anel comutativo.*
2. *Se A é um anel com identidade então $A[X]$ também é um anel com identidade.*
3. *Se A é um anel de integridade então $A[X]$ também é um anel de integridade.*

Definição 1.15. *Seja A um anel e seja $f(X) := a_0 + a_1X + ... + a_nX^n \in A[X]$ com $a_n \neq 0$. O número n se chama o grau de $f(X)$ e denotamos por $gr(f(X))$. O coeficiente a_n é chamado coeficiente líder de $f(X)$. Quando o coeficiente líder for igual a 1, o polinômio é dito mônico.*

Teorema 1.12. ***Algoritmo da divisão*** *Seja A um corpo. Dados dois polinômios $p(X)$ e $q(X)$ em $A[X]$, então existem dois únicos polinômios $t(X)$ e $r(X)$ em $A[X]$ tais que $p(X) = t(X).q(X) + r(X)$, onde $r(X) = 0$ ou $gr(r(X)) < gr(q(X))$.*

Definição 1.16. *Um polinômio $p(X) \in A[X]$ é dito irredutível sobre A se sempre que $p(X) = a(X).b(X)$, com $a(X), b(X) \in A[X]$, então $gr(a(X)) = 0$ ou $gr(b(X)) = 0$, ou seja, $a(X)$ ou $b(X)$ é uma constante.*

Definição 1.17. *Seja A um anel e seja $p(X) \in A[X]$. Diremos que $\alpha \in A$ é uma raiz de $p(X)$ se $p(\alpha) = 0$.*

Teorema 1.13. *Seja A um corpo. Temos que se $p(X) \in A[X]$ é um polinômio de grau n, então $p(X)$ possui, no máximo, n raízes distintas em A.*

Proposição 1.5. *Sejam A um anel, $p(X) \in A[X]$ e $\alpha \in A$. Então $f(\alpha) = 0$ se e somente se existe um polinômio $t(X) \in A[X]$ tal que $f(X) = (X - \alpha).t(X)$.*

Definição 1.18. *Sejam A um anel, $p(X) \in A[X]$, $\alpha \in A$, e um inteiro $s \geq 1$. Dizemos que α é uma raiz de $f(X)$ de multiplicidade s se $(X-\alpha)^s$ divide $p(X)$ mas $(X-\alpha)^{s+1}$ não divide $p(X)$.*

1.2 Elementos de Teoria dos números

1.2.1 Alguns conceitos básicos

Nas seções anteriores já utilizamos o conceito de congruência, mas a seguir definiremos formalmente tal conceito.

Definição 1.19. *Sejam a, b e $n > 1$ números inteiros. Diremos que a é congruente com b módulo n quando $a - b$ for divísivel por n. Denotamos por*

$$a \equiv b \mod n.$$

Assim, a congruência $a \equiv b \mod n$ é verdadeira se, e somente se,

$$a \mod n = b \mod n.$$

ou seja, o resto da divisão inteira de a por n é igual ao resto da divisão inteira de b por n.

Teorema 1.14. *Sejam a, b, c e n números inteiros com $n \neq 0$. Se $a \equiv b \mod n$, então*

1. $a + c \equiv b + c \mod n$
2. $a \times c \equiv b \times c \mod n$
3. $a - c \equiv b - c \mod n$
4. $a \equiv b + cn \mod n$

Corolário 1.2. *Quando a e n forem primos entre si e $ac \equiv b \mod n$, então $c \equiv ba^{-1} \mod n$.*

Definição 1.20. *Para cada número natural n definimos $\varphi(n)$, a função de Euler, como sendo o número de inteiros positivos que não excedem n e são primos com n.*

Exemplo 1.5. O conjunto de restos módulo 28 é formado por todos os inteiros positivos a menores que 28 tais que m.d.c$(28, a) = 1$.

Logo temos o conjunto $\{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$, e $\varphi(28)$ é dado pela ordem deste conjunto, ou seja, 12.

Proposição 1.6. *Seja n um inteiro com $n \geq 2$. Então*

$$|\mathbb{Z}_n^*| = \varphi(n)$$

Teorema 1.15. *Seja m e n inteiros positivos tais que m.d.c(m, n)=1, então:*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Teorema 1.16. *Seja p um inteiro primo, então*

$$\varphi(p) = p - 1.$$

1.2.2 Os teoremas de Euler, Fermat e Wilson

Teorema 1.17. ***(Teorema de Wilson)*** *Se p é um primo, então* $(p-1)! \equiv -1 \mod p$.

Vejamos um exemplo extraído da referência [1].

Exemplo 1.6. Dentro os números $1, 2, ..., 12$ somente os números 1 e 12 são os seus próprios inversos módulo 13 pois $1 \equiv 1 \mod 13$ e $12 \equiv -1 \equiv 12 \mod 13$. Mas demais números (2,3,4,5,6,7,8,9,10) tem inversos listados abaixo dois a dois:

$$2 \times 7 \equiv 13\ ,\ 3 \times 9 \equiv 13\ ,\ 4 \times 10 \equiv 13\ ,\ 5 \times 8 \equiv 13\ ,\ 6 \times 11 \equiv 13.$$

Ao multiplicar estas congruências membro a membro, temos:

$$2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \equiv 1 \mod 13$$

e multiplicando os dois lados por 12, teremos:

$$2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 \equiv 1 \times 12 \mod 13$$

e portanto, como $12 \equiv -1 \mod 13$, temos finalmente

$$(13-1)! \equiv -1 \mod 13$$

Teorema 1.18. ***(Pequeno teorema de Fermat)*** *Seja p um número primo e seja a um inteiro. Então,*

$$a^p \equiv a \mod p$$

Teorema 1.19. ***(Euler)*** *Sejam n um inteiro positivo e a um inteiro relativamente primo com n. Então*

$$a^{\varphi(n)} \equiv 1 \mod n$$

1.2.3 Equações de congruência e o Teorema chinês do resto

Dados os números inteiros a, b e $n > 1$, consideremos a equação de congrência na incógnita x:

$$ax \equiv b \mod n$$

Quando $mdc(a, n) = 1$, uma solução que pertence ao intervalo $0 \leq x_0 < n$ é

$$x_0 = a^{-1}b \mod n,$$

onde a^{-1} é o inverso de a módulo n. A solução não é unica pois $x_0 + qn$ também será solução, para qualquer número inteiro q.

Quando $mdc(a, n) = d > 1$, nem sempre existe x tal que

$$ax \equiv b \mod n$$

Esta congruência terá uma solução se e só se d dividir b. Neste caso,

$$\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \mod \frac{n}{d}$$

Como a/d e n/d são primos entre si, $x_0 = (a/d)^{-1} \mod n/d$ é uma solução desta equação e

$$x_0, x_0 + \left(\frac{n}{d}\right), x_0 + 2\left(\frac{n}{d}\right), ..., x_0 + (d-1)\left(\frac{n}{d}\right)$$

são todas as soluções em $\mathbb{Z}_n$ da equação original $ax \equiv b \mod n$.

Teorema 1.20. ***(Teorema chinês do resto)*** *Sejam m_1, m_2,...,m_k, números inteiros dois a dois primos entre si e $m = m_1 m_2 ... m_k$. Dados os números inteiros a_1, a_2,...,a_k, o sistema de congruências na incógnita x*

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \quad \vdots \\ x \equiv a_k \mod m_k \end{cases}$$

possui solução e é dada por:

$$x_0 = a_1 M_1 N_1 + a_2 M_2 N_2 + ... + a_k M_k N_k$$

onde $M_i = m/m_i$ e $N_i = M_i^{-1} \mod m_i$, para $i = 1, 2, ..., k$.

Esta solução não é única pois para qualquer inteiro q, o número $y \equiv x_0 + qm$ também é solução do sistema de congruência e duas soluções quaisquer difere por um múltiplo de m.

Exemplo 1.7. Vamos determinar as soluções de

$$\begin{cases} x \equiv 1 \mod 15 \\ x \equiv -1 \mod 8 \\ x \equiv 2 \mod 13 \end{cases}$$

Neste sistema de congruências, $a_1 = 1$, $m_1 = 15$, $a_2 = -1$, $m_2 = 8$, $a_3 = 2$ e $m_1 = 13$ e calculamos o produto $m = m_1 m_2 m_3 = 15.8.13 = 1560$ para encontrar os números:

$$\begin{cases} M_1 = m/m_1 = 1560/15 = 104 \\ M_2 = m/m_2 = 1560/8 = 195 \\ M_3 = m/m_3 = 1560/13 = 120 \end{cases}$$

e seus inverso modulares

$$\begin{cases} N_1 = M_1^{-1} \mod 15 = 104^{-1} \mod 15 = 14 \\ N_2 = M_2^{-1} \mod 8 = 195^{-1} \mod 8 = 3 \\ N_3 = M_3^{-1} \mod 13 = 120^{-1} \mod 13 = 9 \end{cases}$$

Calculamos todos os números necessários para a solução do problema:

$$\begin{aligned} x &= a_1M_1N_1 + a_2M_2N_2 + a_3M_3N_3 \\ &= 1.104.14 - 1.195.3 + 2.120.9 \\ &= 3031 \end{aligned}$$

Reduzindo módulo m, segue que $3031 \equiv 1471 \mod 1560$ é uma solução para o sistema dado.

1.2.4 Resíduos quadráticos

Um dos primeiros resultados da Teoria dos números moderna foi a Lei de Reciprocidade Quadrática conjecturada independentemente por Euler e Legendre na primeira metade do século XVIII, porém eles só obtiveram a demonstração para casos particulares. Em 1796 Gauss deu a primeira demonstração da Lei de Reciprocidade Quadrática e durante sua vida encontrou outras demonstrações desse trabalho. Tratando-se de resíduos quadráticos, as ideias desenvolvidas para solucioná-las são de grande riquezas em informações aritméticas e de oferecimento de problemas a serem solucionados.

A palavra "resíduo quadrático" é atribuído a um inteiro a que satisfaz a equação $x^2 \equiv a \mod n$. Formalmente:

Definição 1.21. *Dizemos que a é resíduo quadrático módulo n se, se somente se, a equação $x^2 \equiv a \mod n$ possui solução. Caso não possua solução dizemos que a não é resíduo quadrático módulo n.*

Exemplo 1.8. Se fixarmos $n = 7$ então a classe de resíduos módulo 7 possui exatamente 7 elementos dos quais 3 elementos são quadrados, a saber: $1 = 1^2, 4 = 2^2, 9 = 3^2$, $(3^2 = 9 \equiv 2 \mod 7)$. Portanto, o inteiro 2 é resíduo quadrático módulo 7, enquanto 5 não é resíduo quadrático módulo 7, pois nenhum dos elementos so conjunto $\{1, 2, 3, 4, 5, 6\}$ satisfaz a equação $x^2 \equiv 5 \mod 7$.

Os inteiros cujas raízes quadradas são elas próprias, números inteiros recebem o nome de *quadrados perfeitos*

Proposição 1.7. *Sejam p um número primo e $a \in \mathbb{Z}_p$. Então, a tem no máximo duas raízes quadradas em $\mathbb{Z}_p$.*

Proposição 1.8. *Seja p um número primo, com $p \equiv 3 \mod 4$. Seja $a \in \mathbb{Z}_p$ um resíduo quadrático. Então, as raízes quadradas de a em $\mathbb{Z}_p$ são*

$$\pm a^{(p+1)/4} \mod p.$$

Exemplo 1.9. 17 é um resíduo quadrático $\mod 59$, pois 59 é primo e $59 \equiv 3 \mod 4$, logo

$$17^{59+1/4} = 17^{15} = 28$$

e podemos obeservar que $28^2 = 28 \times 28 = 17$ e $-28 \equiv 31$ e $31^2 = 31 \times 31 = 17$.

1.2.5 Símbolo de Legendre

Definição 1.22. *Seja p um inteiro primo ímpar. Para um inteiro a, definimos o símbolo de Legendre por*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & se\ \ p|a, \\ 1 & se\ \ a\ \ é\ \ resíduo\ \ quadrático\ \ módulo\ \ p, \\ -1 & se\ \ a\ \ é\ \ não\ \ resíduo\ \ quadrático\ \ módulo\ \ p. \end{cases}$$

O próximo resultado, descoberto por Euler, permite calcular o símbolo de Legendre.

Teorema 1.21. ***Critério de Euler*** *Sejam a um inteiro e p um primo, tais que $mdc(a,p) = 1$. Então*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p.$$

Exemplo 1.10. $4^{(11-1)/2} \equiv 1 \mod 11$ e $4 \in \left(\frac{a^2}{p}\right) = 1$;
$7^{(11-1)/2} \equiv 10 \equiv -1 \mod 11$ e $7 \in \mathbb{Q}_{11}$.
Em particular $\left(\frac{1}{p}\right) = 1$ $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Portanto

$$-1 \in \mathbb{Q}_p \text{ se } p = 1 \mod 4 \text{ e } -1 \in \mathbb{Q}_p \text{ se } p = 3 \mod 4.$$

Teorema 1.22. *Seja p um primo. Pelo critério de Euler e pela definição do símbolo de Legendre, seguem as seguintes propriedades:*

1. *Se $a \equiv b \mod p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & se\ \ p \equiv 1 \mod 4, \\ -1 & se\ \ p \equiv 3 \mod 4. \end{cases}$
5. *Se p é primo, então $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$*
6. *Lei da reciprocidade quadrática (Legendre-Gauss): Se p e q são primos ímpares, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1 & se\ \ p \equiv 1 \mod 4\ \ ou\ \ q \equiv 1 \mod 4 \\ -1 & se\ \ p \equiv q \equiv 3 \mod 4. \end{cases}$$

2 Criptografia

2.1 Um pouco de História

Atualmente é comum realizar compras pela internet, porém não imaginamos o quanto uma simples compra pode trazer de criptografia em seus bastidores. Suponha que Alice deseja fazer uma compra pela internet. Para isto, ela visita um site de compras, faz seu pedido e para pagá-lo, introduz o número do seu cartão de crédito. Sabemos que é de grande perigo que outras pessoas saibam o número do seu cartão de crédito a não ser o fornecedor, que chamaremos de Bob. Quando Alice aciona o botão SEND, a informação confidencial, que é o número do cartão, percorre um trajeto até o fornecedor passando por vários computadores, como o computador do seu provedor de internet, que tem como operador Eva. Mas como garantir que Eva não irá descobrir o número do cartão de crédito de Alice? Alice pode ceder esta informação ao Bob com segurança? Será este um problema somente da atualidade?

A segurança na transmissão de informação tem relatos antigos, e um dos primeiros datam de *Heródoto*, o "pai da história", segundo o filósofo e estadista romano Cícero. Heródoto escreveu *As histórias* que descreviam os conflitos entre a Grécia e a Pérsia, ocorridos no século V a.C., e nele era relatado que a escrita secreta salvou a Grécia de ser conquistada pelo líder persa Xerxes. Nesta ocasião havia um grego chamado Demarato, que exilado da Grécia, vivia numa cidade da Pérsia, e testemunhou os planos de Xerxes para para destruir a Grécia. Para evitar isso ele raspou a cera de um par de tabuletas de madeira escrevendo sobre elas os planos de Xerxes, cobriu-as com cera novamente e enviou à Grécia. Com tal informação os gregos se preparam para a chegada da frota de Xerxes, e surpreendendo-o, conseguiram escapar de uma possível dominação persa.

Outro relato nos conta que os antigos chineses escreviam mensagens em seda fina, que era amassada até formar uma pequena bola e a cobriam com cera. Esta era engolida por um mensageiro que levava a mensagem até seu destino. Um outro exemplo foi do cientista Giovani Porta, no século XVI que descreveu como esconder uma mensagem dentro de um ovo cozido fazendo uma tinta com uma onça de alume e um quartilho de vinagre, onde a solução penetrava na casca do ovo e deixa a mensagem sobre a clara endurecida. O destinatário para ler apenas retirava a casca.

O primeiro documento que usou uma cifra de substituição para fins militares aparece em Roma nas guerras de Gália de Júlio César, chamadas de cifras de César, que consistia em substituir as letras do alfabeto romano por letras gregas e assim a mensagem ficou incompreensível para o inimigo.

Ainda na antiguidade, os estudisos árabes inventaram a Criptoánalise, ciência que permite decifrar uma mensagem sem conhecer a chave. Eles utilizavam um alfabeto cifrado, que era um simples rearranjo de alfabeto cifrado, conhecido também como cifra de substituição monoalfabética, que consite em substituir cada letra por um símbolo. Este método acabou sendo vulnerável, pois conhecendo o idioma o qual a mensagem foi escrita, eram utilizados métodos estatísticos utilizando das letras mais frequentes no idioma e comparando com o símbolo que mais aparece na mensagem codificada de forma sucessiva até a mensagem ser descoberta.

As técnicas utilizadas de ocultação utilizadas nestes fatos são tipos de esteganografia, que é um nome derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever. Com o desenvolvimento da esteganografia, houve a evolução da Criptografia, cujo objetivo não é ocultar a existência de uma a mensagem, e sim, esconder o seu significado utilizando de um processo conhecido como encriptação, onde o texto é misturado de acordo com um parâmetro específico.

Na segunda guerra mundial, a forma de esteganografia que se tornou popular foi o microponto. Agentes alemães operando na América Latina, reduziam fotograficamente uma página de texto até transformá-la num ponto com menos de um milímetro de diâmetro. O microponto era ocultado sobre o ponto final de uma carta aparentemente inofensiva e para saber o conteúdo era necessária uma lupa.

Nesta mesma época os britânicos construíram o primeiro computador programável que decifrava a cifra alemã *Lorenz* usada para estabelecer a comunicação entre Hitler e seus generais. Era o início da criptografia moderna.

2.2 Conceitos básicos de criptografia

A palavra criptografia vem do grego *cryptos* que significa oculto, secreto e estuda métodos para codificar uma mensagem onde apenas o destinatário legítimo tem ferramentas suficientes para interpretá-la.

Sejam como antes, Alice o remetente da mensagem, Bob o destinátario e Eva uma invasora. A partir de um algoritmo criptográfico de Alice utilizando uma chave criptografa k e uma mensagem x, obtem-se uma outra mensagem $y = f_K(x)$, que chamamos de *mensagem criptografada*. A mensagem criptografada y é enviada para Bob onde y é *decriptografada* pelo algoritmo inverso $f_K^{-1}(y)$ obtendo-se x se, e somente se, Bob conhece a chave k.

Vamos supor agora que Eva, deseja decifrar a mensagem, e lhe é conhecido o algoritmo, mas não a chave. Esta realização é de pequena ou grande dificuldade, depen-

dendo da complexidade do algoritmo utilizado.

2.3 Criptografia de chave pública ou assimétrica

Imagine que Alice deseja enviar uma mensagem pessoal e altamente secreta para Bob. Ela coloca sua carta secreta em uma caixa de ferro com um cadeado e envia para Bob. Este coloca um outro cadeado e envia para Alice novamente. Ao receber, Alice retira seu cadeado colocado inicialmente e reenvia para Bob, que agora pode abrí-la e ler a carta pois a caixa está trancada apenas pelo seu cadeado. Observamos aqui que é possível realizar a troca de chaves através de um canal inseguro já que todos podem saber do transporte da caixa de ferro, porém ninguém além de Alice e Bob podem descobrir o que estava escrito na carta no interior da caixa. Este é o princípio utilizado na troca de chaves de Diffie-Hellman que abriu portas para o estudo da criptografia de chave pública.

2.3.1 Problema do logaritmo discreto (PLD)

Antes de conhecermos melhor a criptografia de chave pública, vamos conhecer o que é o problema do logaritmo discreto (PLD), já que a mesma está baseada neste problema.

Definição 2.1. *Seja um grupo G e $y, \alpha \in G$ tal que y é potência de α. Dizemos que o logaritmo discreto de y na base α é o menor inteiro não negativo x tal que $\alpha^x = y$, denotado por $log_\alpha y = x$.*

Assim o problema do logaritmo discreto consiste em garantir que não é possível determinar tal x em tempo computacionalmente razoável.

2.3.2 A troca de chaves Diffie-Hellman

O problema sobre troca de informações entre Alice e Bob em um canal inseguro, exemplificado no início deste capítulo, foi um dos questionamentos que estimulou a criação da troca de chaves públicas por Whitfield Diffie e Martin Hellman com contribuições de Ralph Merkle em 1976.

Vejamos como Alice e Bob combinam uma chave secreta k utilizando o método de Diffie-Hellman.

1. Alice e Bob escolhem publicamente um primo p e $\alpha \in \mathbb{Z}_p^*$ tal que $m.d.c(\alpha, p) = 1$;
2. Alice escolhe aleatoriamente um número a tal que $1 \leq a \leq p-2$ e envia para Bob o número $m = \alpha^a \mod p$;
3. Bob escolhe b da mesma forma feita por Alice e a retorna $n = \alpha^b \mod p$;

4. Alice calcula $k = n^a = (\alpha^b)^a \mod p$;

5. Bob calcula $k = m^b = (\alpha^a)^b \mod p$.

No fim deste processo, Alice e Bob compartilham da chave k e as mensagens cifradas com esta chave poderão ser decifradas apenas com a chave privada correspondente.

Exemplo 2.1. Seja o grupo $\mathbb{Z}_{17}$ e $\alpha = 3$. Alice escolhe $a = 7$ e calcula $m = 3^7 \equiv 11 \mod 17$ e envia o resultado para Bob. Bob escolhe $b = 4$ e calcula $n = 3^4 \equiv 18 \mod 17$ e envia o resultado n para Alice. Por sua vez, Alice calcula $n^7 \equiv 4 \mod 17$ e Bob calcula $m^4 \equiv 4 \mod 17$. Desta forma a chave secreta k encontrada pelo método de Diffie-Hellman é 4.

Vamos pensar agora em uma terceira pessoa, Eva, que conhece p e α, pois estes são escolhidos publicamente e ainda consegue descobrir n e m, pois estes valores são transmitidos em um canal inseguro, o que facilita esse acesso. Poderia Eva descobrir qual a chave secreta de Alice e Bob?

Esta questão encontra sua resposta na garantia de segurança do método, baseada na dificuldade de solução do Problema do Logaritmo Discreto. Para encontrar a chave secreta, Eva precisa encontrar b atráves do logaritmo discreto de n na base α e calcular $k = m^b$. Logo, quanto maior a dificuldade em resolver este algoritmo, não terá como um espião como Eva descobrir a chave secreta atráves das informações de conhecimento público.

Até os dias atuais não foi provado que se Eva descobrir o problema do logaritmo discreto, ela conseguirá calcular de forma eficiente logaritmos discretos $\mod p$, e por isso podemos dizer que o método de troca de chaves de Diffie-Hellman é ainda seguro na atualidade.

2.3.3 O método de ElGamal

O método desenvolvido por Taher ElGamal em 1985 é baseado também na dificuldade de solução do problema do logaritmo discreto. Utilizamos geralmente este método sobre o grupo multiplicativo $\mathbb{Z}_p^*$, mas podemos generalizá-lo para qualquer grupo cíclico finito G, desde que as operações sobre este sejam de fácil aplicação e que seja intratável o problema do logaritmo discreto no grupo G.

Para a geração de chaves, Alice escolhe um grupo cíclico finito G com ordem n e gerador g e seleciona um inteiro a tal que $1 \leq a \leq n-2$ e calcula $A = g^a$. Assim é produzida a chave pública (A, g), onde deve-se lembrar que o grupo G é conhecido. Temos a partir daí um Problema de Logaritmo Discreto, já que a é conhecido apenas por Alice.

Para Bob codificar uma mensagem usando a chave pública de Alice, ele escolhe um número b, tal que $1 \leq b \leq n-2$, calcula $B = g^b$, e para cada mensagem m, com

$m \in \mathbb{Z}_p^*$, determina $c = A^b m \mod p$. Após este processo, ele envia o texto ilegível para Alice, que é o par (B, c).

Para decriptografar o texto recebido, Alice é conhecedora de $A = g^a$, assim ela efetua $mB^{-a} = m(A^b)(g^b)^{-a} = m(g^{ab})(g^{-ab}) \mod p$ encontrando m, que é o elemento de $\mathbb{Z}_p^*$ associado a mensagem original de forma combinada pelo rementente e o destinatário.

Exemplo 2.2. Tomamos o grupo multiplicativo $\mathbb{Z}_{2579}^*$ gerado por 2 e escolhemos $a = 765$, assim temos $A = 2^{765} \equiv 949 \mod 2579$. Para criptografar $m = 1299$, Bob escolhe $b = 853$ e calcula $B = 2^{853} \equiv 435 \mod 2579$, e $c = 1299.949^{853} \equiv 2396 \mod 2579$. Ao receber $(B, c) = (435, 2396)$, calculamos $2396.(435^{765})^{-1} \equiv 1299 \mod 2579$.

Dois aspectos relacionados ao problema do logaritmo discreto formam a base para a segurança do método de ElGamal: Se um intruso não conseguir calcular a, não terá ferramentas suficientes para calcular g^a e muito menos $mB^{-a} = m$, ou seja, para decifar a mensagem ele deve ser capaz de calcular $B = g^b \mod p$ De mesma forma, $A = g^a \mod p$ deve ser calculado.

2.3.4 RSA

O primeiro método de criptografia de chave pública foi o RSA, criado em 1977. As letras RSA correspondem as iniciais dos sobrenomes dos seus inventores Ron Rivest, Adi Shamir e Len Adleman que na época trabalhavam no Massachissets Institute of Technology (MIT). Baseado na dificuldade computacional de fatorar um número inteiro em primos, este é um método muito utilizado na atualidade em *softwares* de navegação da internet e aplicações comerciais.

Para um computador qualquer é relativamente fácil multiplicar dois números primos grandes ou elevar um número a uma potência conhecida. Por exemplo, supomos dois números p e q com cerca de 500 algarismos cada um e encontramos $n = pq$, um número composto por 1000 algarismos em menos de um segundo. Porém as operações inversas não ocorrem em tempo hábil se os números forem suficientemente grandes. Se for conhecido apenas n e se quer encontrar p e q, é necessário realizar cerca de 10^{500} divisões, o que exige um período inimaginavelmente longo no mais rápido dos computadores atuais.

Existem algoritmos mais sofisticados para a fatoração, mais rápidos que a divisão por tentativas, mas mesmo estes tem uma estimativa de quase um século para fatorar n com 1000 algarismos. Podemos ainda trabalhar com p e q com 1000 algarismos, e assim temos $n = pq$ com 2000 algarismos. O tempo para multiplicar p e q aumenta cerca de 4 vezes, porém, o tempo para fatorar n tem um aumento de 10^{1000} vezes maior.

Observamos que é extremamente difícil fatorar inteiros grandes, porém não é impossível. Até o momento, não se tem conhecimento de algoritmos eficientes para fazer isto em tempo hábil, o que também não é garantido que este não possa ser criado. Em 1999 o recorde em fatoração de uma chave RSA com 140 algarismos foi estabelecido por

Adi Shamir com a execução do algoritmo NFS (*Number Field Sieve*). Tais pesquisas exigem o aumento de unidades das chaves para que não ocorra a invasão.

Vejamos como transmitir uma mensagem utilizando o RSA.

- Escolha da chave

  1. Bob escolhe dois números primos p e q ;
  2. Calcula $n = pq$ e $\varphi(n) = (p-1)(q-1)$;
  3. Escolhe e tal que $1 < e < \varphi(n)$ e $mdc(e, \varphi(n)) = 1$;
  4. Bob calcula a chave secreta $d = e^{-1} \mod \varphi(n)$;
  5. O par de números (n, e) é a chave pública de Bob.

- Codificação da mensagem

  1. Alice associa cada bloco da mensagem a um número $0 < m < n$ de forma biunívoca onde todo m tem a mesma quantidade de dígitos;
  2. Calcula para cada bloco associado a mensagem $c = m^e \mod n$;
  3. Envia c para Bob.

- Decodificação da mensagem

  1. Bob calcula $c^d = m \mod n$;
  2. Lê a mensagem.

Observe que para Bob encontrar a mensagem original, ele usa $ed \equiv 1 \mod \varphi(n)$ e $n = pq$ logo

$$c^d \mod n = (m^e)^d \mod n = m \mod n.$$

Exemplo 2.3. Suponha que Alice queira codificar a palavra UNESP para enviar a Bob. Previamente eles escolhem $p = 43$, $q = 53$, e $e = 5$ como descrito acima, obtendo $n = 2279$, $\phi(n) = (43-1).(53-1) = 2182$ e $d = 437$.
Para realizar a pré-codificação, Alice deve associar cada letra a um número, e para isso enumera o alfabeto de 1 a 26 e associar A-01, B-02, C-03 e assim em diante obtendo previamente a sequência 21 14 05 19 16. Posteriormente, quebra-se em blocos de tal forma que o valor númerico de cada bloco seja menor que 2279, assim e pré-codificação resulta em 2114 - 519 - 16.

Para a codificação são realizadas os seguintes cálculos:

$$2114^5 \equiv 1499 \mod 2279$$
$$519^5 \equiv 1447 \mod 2279$$
$$16^5 \equiv 236 \mod 2279$$

Logo a mensagem enviada é 14991447236 e a chave pública é $(2279, 5)$.
Bob ao receber a mensagem codificada e possuindo o valor de d calcula:

$$1499^{437} \equiv 2114 \mod 2279$$
$$1447^{437} \equiv 519 \mod 2279$$
$$236^{437} \equiv 16 \mod 2279$$

Dessa forma ele retorna a mensagem inicial.

Se Eva, uma invasora, quer decifrar a mensagem conhecendo apenas (n, e) e c, é necessário que ele encontre d, que por sua vez depende de p e q já que $d = e^{-1} \mod \varphi(n)$ e $\varphi(n) = (p-1)(q-1) = n - 1 - p - q$. Eva poderia ainda encontrar $\varphi(n)$ sem conhecer p e q, mas isto também não é viável.

2.4 Noções de teoria de complexidade computacional

O estudo de complexidade de algoritmos tomou forma a partir dos anos 1960, e permitiu a conceituação de vários testes da chamada complexidade de algoritmos. A teoria de complexidade procura classificar os problemas computacionais com critérios de acordo com o tipo de problema ou do modelo computacional. Os algoritmos analisados são procedimentos computacionais bem definidos para resolver um problema que assume variáveis de entrada (dados) e encontra variáveis de saída (solução).

Utilizando um computador, é necessário utilizar algarismos binários ou *bits* e naturalmente, a quantidade de operações aritméticas elementares que são executadas dependentes do tamanho da entrada que é fornecida ao algoritmo.

Uma forma de determinar a quantidade de algarismos no sistema binário de um número n decimal, é utilizar $\log_2 n + 1$, pois existe $k \in \mathbb{N}$ tal que

$$2^{k-1} \leq n < 2^k$$
$$k - 1 \leq \log_2 n < k$$

e assim

$$k = [\log_2 n] + 1$$

O tempo computacional gasto na excução de um determinado algoritmo é chamado *custo* e este é medido através da quantidade de operações aritméticas elementares. Para entendê-lo , usaremos a seguinte definição:

Definição 2.2. *Sejam $f, g : \mathbb{N} \to \mathbb{R}$ com $g(n) \geq 0$ para todo $n \in \mathbb{N}$, então:*

1. *$f(n) = O(g(n))$ se existem constantes $c > 0$ e $n_0 \in \mathbb{N}$ tais que $0 \leq f(n) \leq cg(n)$ para todo $n \geq n_0$;*

2. $f(n) = \Omega(g(n))$ *se existem constantes* $c > 0$ *e* $n_0 \in \mathbb{N}$ *tais que* $0 \leq cg(n) \leq f(n)$ *para todo* $n \geq n_0$*;*

3. $f(n) = \theta(g(n))$ *se existem cosntantes* $c_1, c_2 > 0$ *e* $n_0 \in \mathbb{N}$ *tais que* $c_1 g(n) \leq f(n) \leq c_2 g(n)$ *para todo* $n \geq n_0$*.*

Exemplo 2.4. Um polinômio de grau n, $f(x)$, com coeficientes reais, $f(x)$ é igual a $O(x^n)$. De fato, consideremos $f(x) = a_n x^n + ... + a_0$, onde $a_n, ..., a_0$ são números reais e $a_n \neq 0$. Escolhemos um número real $b > a_n$ e como

$$\lim_{x \to \infty} \frac{f(x)}{bx^n} = \frac{a_n}{b} < 1,$$

concluímos que, sempre que x for grande o suficiente, teremos $f(x) \leq bx^n$, ou seja $f(x) = O(x^n)$.

Observação 2.1. Intuitivamente, se $f(n) = O(g(n))$, f não cresce assintoticamente mais rápido que um múltiplo de $g(n)$. Se $f(n) = \Omega(g(n))$ significa que f cresce pelo menos tão rápido assintoticamente que um múltiplo de $g(n)$.

Dessa forma um algoritmo A é de *tempo polinomial* se a função $f(n)$ do tempo de execução de A é tal que $f(n) = O(n^k)$ para um constante k fixa. Já um algoritmo A é de *tempo exponencial* se não existe constante k tal que $f(n) = O(n^k)$.

Algoritmos de tempo polinomial são chamados *computacionalmente eficientes* e correspondem a problemas *fáceis ou tratavéis*, e algoritmos de tempo exponencial são *computacionalmente ineficientes*. Diz-se que um problema é *computacionalmente inviável ou difícil* se não se conhece qualquer algoritmo de tempo polinomial para resolvê-lo.

2.4.1 Algoritmos de primalidade

Crivo de Erastótenes

Dado $n \in \mathbb{N}$, se n for divisível por algum natural entre 2 e $\sqrt{n}$ então n é composto, caso contrário é primo.

O método mais antigo utilizado para encontrar primos é o *Crivo de Erastótenes*, que apesar de ser de fácil programação, não é adequado para encontrar primos grandes devido ao custo computacional. Pode-se mostrar que o custo operacional de tal crivo é inferior a $O(n^2)$ [2].

Exemplo 2.5. Seja n um número com 100 dígitos decimais, e um computador capaz de realizar 10^{12} divisões por segundo utilizando o algoritmo acima. Assim o número total de divisões que teríamos que realizar retirando os pares seria da ordem de

$$\frac{\sqrt{10^{100}}}{2} \text{ ou } \frac{10^{50}}{2} \text{ operações.}$$

Analizando estes cálculos temos o tempo gasto:

$$t = \frac{10^{50}}{2.10^{12}} \text{ segundos}$$

$$t = \frac{10^{38}}{2.3600.24.365} = \frac{10^{38}}{3153600}$$

e como $10^7 < 3153600 < 10^8$, temos que

$$\frac{10^{38}}{10^8} < t < \frac{10^{38}}{10^7}$$

$$10^{30} < t < 10^{31}$$

ou seja, seria necessário mais de 10^{30} anos para testar se o número n é primo.

3 Curvas Elípticas

A teoria das curvas elípticas é um tópico interessante e amplo da geometria algébrica as quais, quando definidas sobre corpos finitos, tem encontrado diversas aplicações em Criptografia. O principal motivo disto é porque os corpos finitos fornecerem uma quantidade inesgotável de grupos abelianos que, mesmo quando se tem um número grande de elementos, ainda são adequados aos processos computacionais por causa da sua rica estrutura algébrica.
O estudo da criptografia de curvas elípticas é similar em vários aspectos ao estudo da criptografia no grupo multiplicativo de um corpo finito, mas existe uma maior flexibilidade para a escolha de um grupo associado a uma curva elíptica do que a um grupo multiplicativo de um corpo finito.

3.1 Conceitos Básicos

Seja K um corpo que pode ser $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ ou $\mathbb{F}_q$, um corpo finito de $q = p^r$ elementos, onde p é um número primo e $r \in \mathbb{Z}^+$.

Definição 3.1. *Seja K um corpo, com característica diferente de 2,3 e seja X^3+aX+b (onde $a, b \in K$), um polinômio cúbico sem raízes múltiplas. Uma curva elíptica sobre K é o conjunto de pontos $(x, y) \in K^2$ que satisfazem equação:*

$$y^2 = x^3 + ax + b \qquad (1)$$

juntamente com um elemento denotado O chamado ponto no infinito.

Se K é um corpo de característica 2, então uma *curva elíptica sobre K* é um conjunto de pontos que satisfazem uma equação do tipo

$$y^2 + cy = x^3 + ax + b \qquad (2a)$$

ou então

$$y^2 + xy = x^3 + ax^2 + b \qquad (2b)$$

juntamente com um ponto no infinito O.
No caso acima é necessário impor que o polinômio cúbico a direita não possua raízes múltiplas.

Se K é um corpo de característica 3, então a curva elíptica sobre K é um conjunto de pontos que satisfaz a equação

$$y^2 = x^3 + ax^2 + bx + c \qquad (3)$$

juntamente com um ponto no infinito O.

Neste caso, novamente supomos que o polinômio cúbico a direita não possui raízes múltiplas.

Observação 3.1. Existe uma forma geral da equação de uma curva elíptica, conhecida como *Equação de Weierstrass*, válida para qualquer corpo:

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

Quando a característica é diferente de 2, podemos simplificar a equação completando quadrados e substituindo y por $\frac{1}{2}(y - a_1x - a_3)$. E então a forma geral pode ser transformada em

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \qquad (4)$$

onde
$b_2 = a_1^2 + 4a_2$
$b_4 = 2a_4 + a_1a_3$
$b_6 = a_3^2 + 4a_6$
e substituindo y por $2y$, pode-se usar:

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

Já se a característica é diferente de 2 e 3, trocamos, x por $\frac{(x - 3b_2)}{36}$ e y por $\frac{y}{108}$, eliminamos o termo x^2 e obtemos:

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

onde
$c_4 = b_2^2 - 24b_4$
$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$,

e assim podemos escrever:

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

Observação 3.2. Seja $F(x, y) = 0$ uma equação implícita que define uma curva elíptica e que tem y e x como variáveis dessa função em (1) (ou (2a ou 2b), ou ainda,(3)), isto é,

$$F(x, y) = y^2 - x^3 - ax - b,$$
$$F(x, y) = y^2 + cy + x^3 + ax + b,$$
$$F(x, y) = y^2 + xy + x^3 + ax + b,$$
$$F(x, y) = y^2 - x^3 - ax^2 - bx - c,$$

então um ponto (x, y) na curva é chamado *"não-singular"* ou ponto suave se pelo menos uma das derivadas parciais $\frac{\partial F}{\partial x}$ ou $\frac{\partial F}{\partial y}$ é não-nula neste ponto.

Pode-se mostrar que a condição para que os polinômios cúbicos à direita de (1) e (3) não tenha raízes múltiplas é equivalente a dizer que todos pontos na curva são não singulares [3].

3.1.1 Curvas Elípticas sobre os Reais

Um importante fato sobre o conjunto de pontos de uma curva elíptica juntamente com ponto no infinito O e que eles formam um grupo abeliano. Para se ver tal fato, definiremos ponto no infinito e a soma de dois pontos sobre um corpo K.

Um ponto no infinito, por definição, é a identidade de um grupo e o modo mais natural de introduzir o ponto no infinito O na estrutura é utilizando um argumento de geometria projetiva, a saber:

Por plano projetivo entendemos como sendo o conjunto de classes de equipolência das triplas (X, Y, Z), com elementos não todos nulos.

Duas triplas (X, Y, Z) e $\left(X', Y', Z'\right)$ são ditas equivalentes se existe λ tal que $(\lambda X, \lambda Y, \lambda Z)$=$\left(X', Y', Z'\right)$. Tal classe de equivalência é chamada de *ponto projetivo*. Se um ponto projetivo tem coordenada Z diferente de 0, então existe uma e somente uma tripla em sua classe de equivalência de forma $(x, y, 1)$, ou simplesmente $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$.

Assim o plano projetivo pode ser identificado como todos os pontos (x, y) do plano cartesiano ("afim") mais os pontos para os quais $Z = 0$. Esses últimos pontos formam o que é chamada de *reta no infinito* que intuitivamente pode ser visualizado como "o horizonte do plano".

Qualquer equação $F(x, y) = 0$, de uma curva no plano afim corresponde a uma equação $\tilde{F}(X, Y, Z) = 0$ satisfeita pelos pontos projetivos correspondentes, ou seja, $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$ multiplicados por uma potência adequada de Z para eliminar os denominadores. Por exemplo, aplicando este procedimento na equação afim $y^3 = x^3+ax+b$ de uma curva elíptica, obtemos a *equação projetiva* $Y^2Z = X^3+aXZ^2+bZ^3$. Esta última equação é satisfeita por todos pontos projetivos (X, Y, Z) com $Z \neq 0$

para os quais o ponto correspondente afim (x, y), onde $x = \frac{X}{Z}$ e $y = \frac{Y}{Z}$ satisfaz $y^3 = x^3 + ax + b$.

Além disso, que ponto projetivo (X, Y, Z) sobre a reta do infinito satisfaz a equação $\tilde{F} = 0$? Fazendo $Z = 0$ na equação, obtemos $X^6 = 0$, isto é, $X = 0$. Mas a única classe de equivalência de triplas (X, Y, Z) com X e Z iguais a zero é classe de $(0, 1, 0)$. Este é o ponto no infinito O, que é o ponto na intersecção do eixo y com a linha do infinito.

Para definir a soma de dois pontos de uma curva elíptica, assumiremos o corpo $K = \mathbb{R}$.

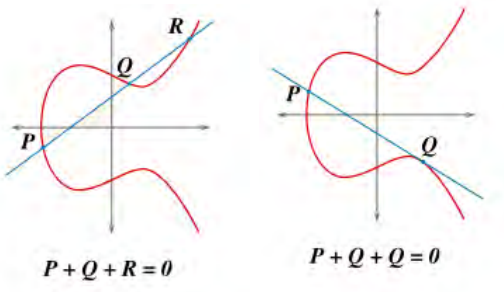
Definição 3.2. *Seja E uma curva elíptica sobre os reais $F(x, y) = y^2 - x^3 - ax - b$ com $K = \mathbb{R}$, e sejam P e Q dois pontos em E. Define-se o oposto de P e a soma $P + Q$ de acordo com as seguintes regras:*

1. *Se P é um ponto no infinito, então define-se $-P$ como O e $P + Q$ como Q, ou seja, O serve como identidade aditiva ou "elemento neutro"do grupo de pontos.*

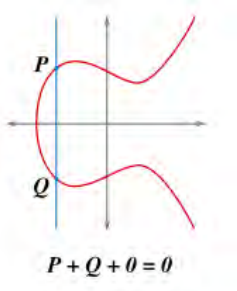
   No que se segue, P e nem Q são pontos no infinito.

2. *O oposto $-P$ é um ponto formado pela mesma coordenada x de P e pelo oposto da coordenada y, isto é, $-(x, y) = (x, -y)$. Nota-se pela equação (1) que P e $-P$ pertencem simultaneamente a curva.*

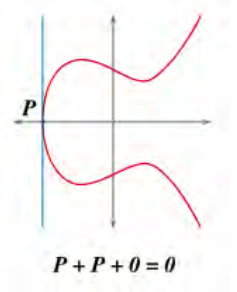
3. *Se P e Q tem diferentes coordenadas x, então mostra-se que a reta $l = \overline{PQ}$ intercepta a curva em exatamente mais um ponto R (a menos que a reta seja tangente a curva em P, neste caso toma-se $R = P$, ou em Q, onde tomamos $R = Q$). Então define-se $P + Q$ como $-R$, isto é, a imagem simétrica do terceiro ponto de intercecção com relação ao eixo x.*



4. *Se $Q = -P$, ou seja, Q tem coordenada x positiva e coordenada y negativa, então $P + Q$ (por (2)) é definido como ponto no infinito O.*



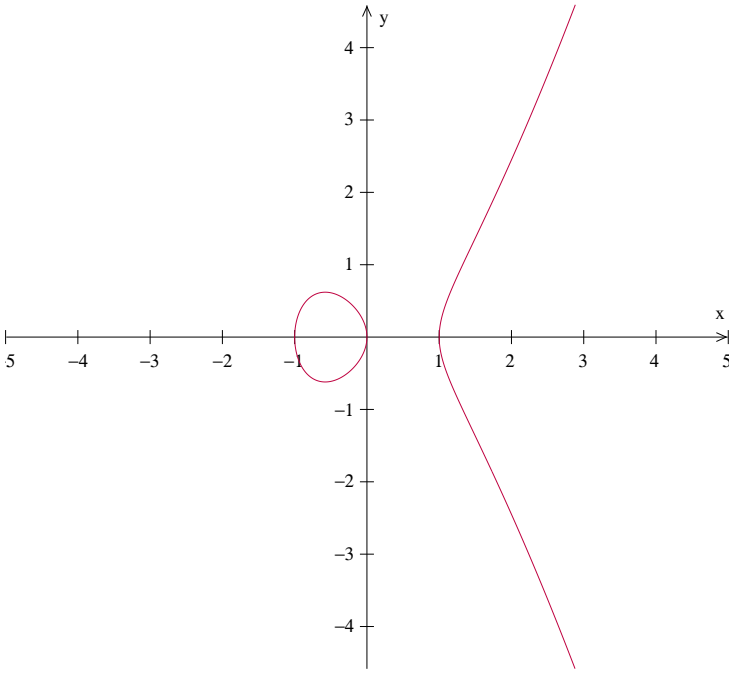
5. *A última possibilidade é $P = Q$. Então seja l a linha tangente a curva em P e seja R o único ponto de interceção de l com a curva. Definimos $P + Q = -R$ onde R é igual P se a linha tangente tem uma dupla tangência em P, ou seja se P é um ponto de inflexão. Neste caso l encontra E em um único ponto.*



Com a soma de dois pontos de uma curva elíptica definida de tal forma, podemos encontrar as propriedades de associação, um elemento neutro que é o ponto no infinito, o elemento oposto e a comutatividade da soma, mostrando assim que o conjunto de pontos de uma curva elíptica sobre os reais formam um grupo abeliano. Podemos ainda generalizar tal resultado para qualquer corpo K o qual a curva elíptica possa estar definida sobre ele.

Exemplo 3.1. Considere a curva elíptica $y^2 = x^3 - x$ sobre os reais no plano xy.

Para encontrar a soma entre P e Q desenhamos uma reta passando por P a Q e tomamos $P + Q$ como o ponto de simetria em relação ao eixo x do terceiro ponto da reta que passa por P e Q intercepta a curva.



Se P e Q são o mesmo ponto, então desejamos encontrar $2P$, e usamos a reta tangente a curva em P para isto. Então $2P$ é o ponto de simetria ao segundo ponto em que a reta tangente intercepta a curva.

Vamos ver agora porque existe exatamente um único ponto na reta l passando por P e Q e interceptando a curva. Vamos obter também a fórmula das coordenadas do terceiro ponto, ou seja, as coordenadas de $P+Q$.

Sejam (x_1, y_1), (x_2, y_2), (x_3, y_3) as coordenadas P, Q e $P+Q$, respectivamente. Deseja-se expressar x_3 e y_3 em termos de x_1, y_1, x_2 e y_2.

Supomos o caso (3) da definição de $P+Q$, e seja $y = \alpha x + \beta$ a equação da reta l que passa por P e Q, a qual não é uma reta vertical. Então $\alpha = \dfrac{(y_2 - y_1)}{(x_2 - x_1)}$ e $\beta = y_1 - \alpha x_1$. Um ponto em l, ou seja , um ponto da forma $(x, \alpha x + \beta)$, está situado na curva elíptica se, e somente se, $(\alpha x + \beta)^2 = x^3 + ax + b$. Assim, existe um ponto de interseção para cada uma das raizes da equação cúbica $x^3 - (\alpha x + \beta)^2 + ax + b = 0$.

Sabe-se que existem duas raízes x_1 e x_2 pois $(x_1, \alpha x_1 + \beta)$ e $(x_2, \alpha x_2 + \beta)$ são os pontos P e Q da curva. Uma vez que a soma das raízes de um polinômio mônico é igual ao oposto do coeficiente de segundo maior grau que compõe o polinômio, concluímos que a terceira raiz é $x_3 = \alpha^2 - x_1 - x_2$, que é uma expressão para x_3. Como $y_3 = -\alpha x_3 + \beta$ temos

$$
\begin{aligned}
y_3 &= -\alpha x_3 - (y_1 - \alpha x_1) \\
y_3 &= -\alpha x_3 + \alpha x_1 - y_1 \\
y_3 &= -y_1 + \alpha(x_1 - x_3) \\
y_3 &= -y_1 + \frac{(y_2 - y_1)}{(x_2 - x_1)}(x_1 - x_3)
\end{aligned}
$$

e assim podemos expressar $P + Q$ em termos de x_1, y_1, x_2 e y_2:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \qquad (5)$$
$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3).$$

O caso (5) no qual $P = Q$ é similar. Exceto que α é a derivada de $\dfrac{\partial y}{\partial x}$ em P. A diferenciação implicita da equação (1) leva á fórmula:

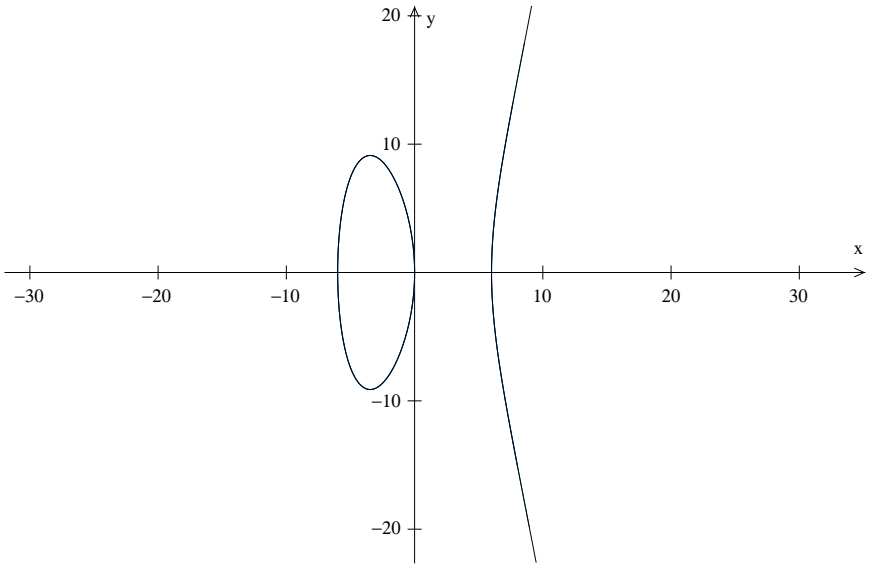
$$\alpha = \left(\frac{3x_1^2 + a}{2y_1}\right)$$

e então obtemos as fórmulas para as coordenadadas de $(2P)$.

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \qquad (6)$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right).(x_1 - x_3).$$

Exemplo 3.2. Em uma curva elíptica $y^2 = x^3 - 36x$ sobre os reais, considere $P(-3, 9)$ e $Q(-2, 8)$. Encontre $P + Q$ e $2P$.



Solução: Substituimos as coordenadas de P e Q na primeira equação de (4) obtemos $x_3 = 6$ e na segunda equação de (4), $y_3 = 0$. Já para o segundo caso, substituimos P e $a = -36$ em (5), e chegamos a $x_3 = \dfrac{25}{4}$ e $y_3 = \dfrac{35}{8}$.

Em grupos abelianos, usamos a notação nP para denotar P adicionado a ele mesmo n vezes se n é positivo, caso contrário, o oposto $-P$ adicionado a ele mesmo $|n|$ vezes.

3.1.2 Curvas Elípticas sobre os números racionais

Na equação (1), se a e b são números racionais, é natural buscar por soluções racionais (x, y), isto é, considerar a curva elíptica sobre o corpo $\mathbb{Q}$ de números racionais.

É possível mostrar que o grupo abeliano da curva elíptica é finitamente gerado, (este resultado é conhecido como *teorema de Mordell* demonstrado em [4]). Isto significa que este consiste de um subgrupo finito de torção (os pontos de ordem finita) junto com o subgrupo gerado por um número finito de pontos de ordem infinita. O número de geradores necessários para esta parte infinita é dito *posto* r e é zero se, e somente se, o grupo inteiro é finito.

3.1.3 Pontos de ordem finita

A ordem n de um ponto P em uma curva elíptica é o menor inteiro positivo tal que $nP = O$, sendo que tal n não precisa necessariamente existir. É interessante achar pontos P de ordem finita em uma curva elíptica, especialmente para curvas definidas sobre $\mathbb{Q}$.

Exemplo 3.3. Ache a ordem de $P = (2, 3)$ em $y^2 = x^3 + 1$ sobre os reais.
Solução: Usando (5), encontramos que $2P = (0, 1)$, e pela definição de elemento oposto, temos $-2P = (0, -1)$. Como $4P = 2(2P) = (0, -1) = -2P$, a ordem de P é 2,3 ou 6. Se P tem ordem 2, então $2P = 0$, o que neste caso não acontece pois $2P = (0, 1)$. Se P tem ordem 3, então $4P = P$, o que também não é verdade. Logo concluimos que P tem ordem 6.

3.1.4 Curvas Elípticas sobre um corpo finito

Seja K um corpo finito $\mathbb{F}_q$ com $q = p^r$ elementos onde p é um número primo. Seja E uma curva elíptica definida sobre $\mathbb{F}_q$. Se $p = 2$ ou 3, então E é dada por uma equação da forma (2) e (3), respectivamente.

Podemos observar que uma curva elíptica pode ter no máximo $2q + 1$ pontos em $\mathbb{F}_q$, isto é, o ponto no infinito juntamente com $2q$ pares (x, y) com $x, y \in \mathbb{F}_q$ os quais satisfazem (1), (2a), (2b) ou (3), onde para cada x temos duas possibilidades para y pois

$$(x, y) \in E \Rightarrow (x, -y) \in E.$$

A metade dos elementos de $\mathbb{F}_q^*$ tem raízes quadradas, pois $\mathbb{F}_q^* = < g >$ é cíclico. Assim temos que $\mathbb{F}_q^{*2} = < g^2 >$ tem $\dfrac{q-1}{2}$ elementos. Logo se $x^3 + ax + b$ são elementos quaisquer do corpo, dever ter apenas cerca de metade dos números de pontos de $\mathbb{F}_q$. Seja a função χ que leva $x \in \mathbb{F}_q^*$ para ± 1, dependendo ou não se x tem a raiz quadrada

em $\mathbb{F}_q$ tomando $X(0) = 0$. Por exemplo, se $q = p$, um primo, então $\chi(x) = \left(\frac{x}{p}\right)$ é o símbolo de *Legendre*. Assim, em todos os casos o número de soluções de $y \in \mathbb{F}_q$ da equação $y^2 = u$ é igual a $1 + \chi(u)$, e então o número de solução para (1), juntamente com ponto no infinito é,

$$1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(x^3 + ax + b)) = q + 1 + \sum_{x \in \mathbb{F}_q} \chi(x^3 + ax + b). \qquad (6)$$

O resultado a seguir apresenta uma estimativa do números de pontos de uma curva elíptica E sobre $\mathbb{F}_q$. O mesmo não será demonstrado aqui, mas a demonstração pode ser vista em [5] com um argumento baseado em " randow walk", que pode ser encontrada em [6].

Teorema 3.1. *(Teorema de Hasse): Seja N o número de pontos em uma curva elíptica E definida sobre $\mathbb{F}_q$, então:*

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

Além do número N, podemos encontrar a estrutura do grupo abeliano. Este grupo abeliano não é necessariamente cíclico, mas é possível mostrar que é sempre um produto de dois grupos cíclicos. Isto significa que existe um isomorfismo entre um produto de grupos $p-$primos da forma $\mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/p^\beta\mathbb{Z}$, onde o produto é tomado sobre números primos p dividindo N, com $\alpha \geq 1$, $\beta \geq 0$. No caso de grupo abeliano de $\mathbb{F}_q$-pontos e E, escrevemos $(..., p^\alpha, p^\beta, ...)_{p|N}$ das ordens dos fatores p-primos cíclicos, e omitimos p^β quando $\beta = 0$.

Exemplo 3.4. Encontre a classe de $y^2 = x^3 - x$ sobre $\mathbb{F}_{71}$.
Solução: Primeiro encotramos o número N de pontos. Em (6) nota-se que na soma dos termos para x e os termos para $-x$ cancelam-se pois

$$\chi\left((-x)^3 - (-x)\right) = \chi(-1)\chi(x^3 - x)$$
$$\text{e } \chi(-1) = \frac{-1}{71} = -1,$$

então $N = q + 1 = 72$

Note que existem exatamente 4 pontos de ordem 2, incluindo a identidade O, porque estes correspondem as raízes de $y^2 = x^3 - x = x(x-1)(x+1)$. Isto mostra que a parte 2-primário do grupo tem o tipo $(4, 2)$ e então a classe do grupo é $(4, 2, 3, 3)$ ou então $(4, 2, 9)$ dependendo da existência de 9 ou 3 pontos da ordem 3, respectivamente. Assim falta determinar se existem ou não 9 pontos de ordem 3. Observemos que para algum $P \neq 0$, a equação $3P = 0$ é equivalente para $2P = \pm P$, isto é, a condição para a coordenada x de P e $2P$ seja a soma. Por (5), temos

$$y = \left(\frac{(3x^2-1)}{2y}\right)^2 - 2x = x, \text{ isto é ,}$$
$$(3x^2-1)^2 = 12xy^2$$
$$12x^4 - 12x^2 = 0$$
$$3x^4 - 6x^2 - 1 = 0$$

Logo existem no máximo 4 raízes para a equação dada sobre o corpo $\mathbb{F}_{71}$. Se existem 4 raízes distintas, então cada raiz pode fornecer mais 2 pontos pois se $x^3 - x$ tem uma raiz quadrada módulo 71 toma-se $y = \pm\sqrt{x^3 - x}$, e então podemos obter pontos de ordem 3, incluindo a identidade O no infinito. Por outro lado, pode-se ter menos de 9 pontos de ordem 3, e consequentemente 3 pontos de ordem 3. Se a raiz x do polinômio quadrado tem o valor $x^3 - x$ como um quadrado módulo 71, então a raiz $-x$ tem $(-x)^3 - (-x) = -(x^3 - x)$ que não é quadrado módulo 71, e então a classe do grupo é $(4, 2, 9)$.

Para concluir esta seção, observamos que existem muitas analogias entre o grupo de $\mathbb{F}_q$-pontos em uma curva elíptica e o grupo multiplicativo $\mathbb{F}_q$. Por exemplo, eles são semelhantes na soma de elementos, pelo teorema de Hasse. Mas a construção anterior de um grupo abeliano a vantagem de explicar a sua utilidade em criptografia: por um único grupo de ordem q, existem várias curvas elípticas diferentes e vários N diferentes que podemos escolher. Curvas elípticas sobre uma rica "fonte natural" de grupos abelianos finitos.

3.2 Criptossistemas de curvas elípticas

Sabemos que um grupo abeliano multiplicativo $\mathbb{F}_q^*$ de um corpo finito pode ser usado para criar chaves criptográficas. Contudo, a dificuldade em resolver o problema de logaritmo discreto em corpos finitos leva aos criptossistemas RSA, El-Gammal, etc. O propósito desta seção é fazer uma analogia entre sistemas chave pública baseadas em grupos abelianos finitos e sistemas de curvas elípticas definidas sobre $\mathbb{F}_q$.

3.2.1 Multiplicação de pontos

O análogo da multiplicação de dois elementos de uma curva elíptica sobre $\mathbb{F}_q^*$ é a adição de dois pontos em E, onde E é um curva elíptica sobre $\mathbb{F}_q^*$. Então, a analogia de elevação para a k-ésima potência de $\mathbb{F}_q$ é a multiplicação do ponto $P \in E$ por um inteiro k. A elevação k-ésimo no corpo finito pode ser realizada pela repetição do método de elevação ao quadrado em $O(\log k \log^3 q)$ unidades de operações. Similarmente, temos que a multiplicação $kP \in E$ pode ser encontrada com $O(\log k \log^3 q)$ unidades de operações pelo método de duplicação repetida.

Exemplo 3.5. Para encontrar $100P$, escrevemos

$$100P = 2(50P)$$
$$100P = 2(2P + 48P)$$
$$100P = 2(2P + 2(24P))$$
$$100P = 2(2P + 2(2(12P)))$$
$$100P = 2(2P + 2(2(2(6P))))$$
$$100P = 2(2P + 2(2(2(2(3P)))))$$
$$100P = 2(2P + 2(2(2(2(2P + P)))))$$
$$100P = 2(2(P + 2(2(2(P + 2P)))))$$

e assim realizamos 6 duplicações e 2 adições de pontos na curva para obtermos o resultado.

A proposição a seguir fala sobre o número de unidades de operações em uma multiplicação por escalar. A demonstração encontramos em [3].

Proposição 3.1. *Seja uma curva elíptica E definida pela equação de Weierstrass sobre um corpo finito $\mathbb{F}_q$. Dado $P \in E$, as coordenadas de kP podem ser calculadas em $O(logk(log^3 q))$ unidades de operações.*

Observação 3.3. O tempo estimado na proposição anterior não é o melhor possível, especialmente no caso em que o corpo finito tem característica $p = 2$, mas pode ser melhorada com as estimativas que resultam da aplicação dos algoritmos mais convenientes da aritmética em corpos finitos.

Observação 3.4. Se conhecemos o número N de pontos em uma curva elíptica E e se $k > N$, como $NP = O$ podemos substituir k pelo menor resíduo não negativo módulo N antes de calcular kP; neste caso pode-se substituir o tempo estimado por $O(log^4 q)$ (uma vez que $N \leq q + 1 + 2\sqrt{q} = Oq$). Existe um algoritmo desenvolvido por René Schoof em [7] que calcula N em $O(\log^8 q)$ unidades de operações.

3.2.2 Codificando textos

Queremos codificar um texto puro na forma de pontos em uma curva elíptica dada E sobre um corpo finito $\mathbb{F}_q$. Fazemos isto de maneira simples e sistemática de modo que o texto puro m (que pode ser considerado como um inteiro em algum intervalo) seja facilmente determinado a partir do conhecimento das coordenadas do ponto correspondente P_m. Observe que essa codificação não é a mesma coisa que encriptação. Posteriormente, discutiremos maneiras de se encriptar os textos sobre pontos P_m. Mas, um usuário autorizado do sistema deve ser capaz de recuperar m após decifrar o ponto criptografado.

Observação 3.5. Não existe um algoritmo *determinístico* de tempo polinomial (em $\log q$) conhecido que permite escrever um grande número de pontos em uma curva elíptica E sobre $\mathbb{F}_q$, entretanto existem algoritmos *probabilísticos* para os quais a probabilidade de falha é muito pequena.

Observação 3.6. Não é suficiente gerar pontos aleatórios de E a fim de codificar um grande número de possíveis textos puros m. Precisamos de uma forma sistemática para gerar pontos e que de alguma forma que esses pontos estejam relacionados com m, por exemplo, a coordenada x tem uma relação simples com o número inteiro m.

Apresentamos um possível método probabilístico para codificar textos usando pontos de uma curva elíptica E definida sobre $\mathbb{F}_q$, onde $q = p^r$ é um número ímpar considerado grande.

Seja k um inteiro grande o suficiente, de modo que tenha uma probabilidade de falha 1 em 2^k quando tentamos encaixar uma unidade de texto puro m. Na prática seria suficiente considerar $k = 30$, ou no pior caso $k = 50$ deve ser suficiente. Supomos que as unidades da mensagem m sejam associadas a inteiros tais que $0 \leq m \leq M$. Supomos também que o corpo finito é escolhido de tal forma que $q > M.k$. Escrevemos os inteiros de 1 a M_k na forma $m.k + j$, onde $1 \leq j \leq k$, e estabelecemos uma correspondência bijetiva entre tais inteiros e um conjunto de elementos do conjunto $\mathbb{F}_q$. Por exemplo, escrevemos tal inteiro como um inteiro de r-digitos na base p e tomamos r digitos, considerados como elementos de $\mathbb{Z}/p\mathbb{Z}$, os coeficientes de um polinômio de grau $r-1$ correspondente a um elemento de $\mathbb{F}_q$. Isto é, o inteiro $(a_{r-1}a_{r-2}...a_1a_0)_p$ corresponde ao polinômio $\sum_{i=0}^{r-1} a_j X^j$, e é considerado como um polinômio de grau r fixo sobre $\mathbb{F}_q$, dado um elemento de $\mathbb{F}_q$.

Assim, dado m, para cada $j = 1, 2, ...k$ obtemos um elemento x de $\mathbb{F}_q$ correspondente a $mk + j$. Para cada x, calcula-se o lado direito da equação

$$y^2 = f(x) = x^3 + ax + b,$$

para encontrar uma raiz quadrada de $f(x)$.

3.2.3 Problema do logaritmo discreto no uso de curvas elípticas

A criptografia de chave pública baseada no problema de logaritmo discreto no grupo multiplicativo em um corpo finito é bastante conhecida. A seguir, falaremos da mesma no grupo formado pelos pontos de uma curva elíptica E definida sobre um corpo finito F_q.

Definição 3.3. *Se E é uma curva elíptica sobre $\mathbb{F}_q$ e B um ponto de E. Então o problema de logaritmo discreto em E na base B é: Dado uma ponto $P \in E$, deve-se encontrar um inteiro $x \in \mathbb{Z}$ tal que $xB = P$, se tal inteiro existir.*

O problema de logaritmo discretono grupo de pontos de uma curva elíptica, mostra-se ser mais intratável do que o problema do logaritmo discreto em corpos finitos. A técnica mais forte desenvolvida para o uso em corpos finitos, parece não funcionar em

curvas elípticas. Isso é especialmente verdade para o caso de curvas elípticas com característica 2. Na referência [8] são explicados métodos para a solução do problema de logaritmo discreto em $\mathbb{F}_{2^r}^*$ relativamente fáceis de calcular e, portanto, de quebrar criptossistemas sobre $\mathbb{F}_{2^r}^*$, a não ser que o r escolhido seja muito grande. O sistema análogo utilizando curvas elípticas sobre $\mathbb{F}_{2^r}$ é mais seguro para valores significativamente menores de r. Uma vez que existem razões práticas relacionadas a hardware e software para a preferência por realizar cálculos aritméticos sobre o corpo $\mathbb{F}_{2^r}$, a aplicação desses criptossistemas de chave pública torna-se mais conveniente do que em sistemas baseados em problemas de logaritmo discreto em $\mathbb{F}_{q^k}^*$.

Até 1990, os únicos algoritmos de logaritmo discreto conhecidos para uma curva elíptica era os que funcionavam em qualquer grupo, independente da estrutura particular. Estes são algoritmos de tempo exponencial, desde que a ordem do grupo seja divisível por um grande fator primo. Mas então *Menezes, Okamoto e Vanstone* em [9] desenvolveram uma nova abordagem para o problema de logaritmo discreto sobre uma curva elíptica E definida sobre $\mathbb{F}_q$. A saber, eles usaram o emparelhamento de Weil para imergir o grupo E no grupo multiplicativo de alguma extensão de corpo $\mathbb{F}_q^k$. Esta imersão reduziu um problema do logaritmo discreto sobre E em um problema de logaritmo em $\mathbb{F}_{q^k}^*$. Este algoritmo está descrito na referência [5].

Entretanto, para que a redução emparelhamento de Weil funcione, é importante que o grau de extensão k seja pequeno. Essencialmente, as únicas curvas elípticas para as quais k é pequeno são chamadas *"super-singulares"*. Os exemplos mais conhecidos são as curvas da forma $y^2 = x^3 + ax$ quando a característica p de $\mathbb{F}_q$ é tal que $p \equiv -1 \mod 4$, e curvas de forma $y^2 = x^3 + b$, quando $p \equiv -1 \mod 3$. A grande maioria das curvas elípticas, entretanto, não são super-singulares. Para estas a redução quase nunca leva a um algoritmo sub-exponencial.

Assim, a principal vantagem dos sistemas criptográficos de curvas elípticas é que não é conhecido nenhum algoritmo sub-exponencial que possa quebrar o sistema, desde que se evite curvas super-singulares e também curvas cuja ordem não tenha nenhum fator primo grande. Descreveremos agora sistemas de chave pública baseada no problema do logaritmo discreto sobre o grupo de pontos dem uma curva elíptica E definida sobre um corpo finito $\mathbb{F}_q$.

3.2.4 A troca de chaves de Diffie-Hellman com curvas elípticas

Suponha que Alice e Bob querem chegar a um acordo sobre uma chave que mais tarde será usada em conjunto com um sistema criptográfico clássico. Primeiro eles escolhem publicamente um corpo finito $\mathbb{F}_q$ e uma curva elíptica E definida sobre ele. A chave deles será construída a partir de um ponto aleatório P da curva elíptica. Por exemplo, se eles tem um ponto aleatório $P \in E$, tomando a coordenada x de P obtemos um elemento aleatório de $\mathbb{F}_q$, que pode ser convertido em um inteiro aleatório com r dígitos na base p, onde $q = p^r$, que serve como chave para o criptossistema clássico

mencionado. (Aqui, estamos usando a palavra aleatório em um sentido impreciso; isto quer dizer que a escolha de P é arbitrária e imprevisível em um grande conjunto de chaves possíveis). Deve-se escolher o ponto de P de tal forma que todas as comunicações um com o outro sejam públicas, e mais ninguém, além deles dois, sabe o que é P.

Supomos que B seja um ponto fixo em E conhecido publicamente, cuja ordem é muito grande (N ou um divisor grande de N). Seguimos os seguintes passos para gerar a chave P:

1. Alice e Bob primeiro escolhem publicamente um ponto $B \in E$ para servir como base.

2. Alice escolhe aleatoriamente um inteiro a de uma ordem de grandeza q, que é aproximadamente a mesma ordem de N, a qual ela mantém secreta. Ela calcula $aB \in E$, a qual ela torna público.

3. Bob escolhe um número aleatoriamente b e torna público $bB \in E$.

4. Alice conhece bB (o qual é de conhecimento público) e seu próprio segredo a, assim ela pode calcular $P = abB \in E$. Bob conhece aB, e pode calcular $P = abB \in E$.

De qualquer modo, uma terceira pessoa conhece somente aB e bB. Sem resolver o problema de logaritmo discreto - encontra a conhecendo B e aB (ou encontra b conhecendo B e bB)- não há como calcular abB conhecendo apenas aB e bB.

Observação 3.7. B desempenha o papel de gerador de G no corpo finito do sistema de Diffie-Hellman. No entanto, não é necessário que B seja um gerador do grupo de pontos em E. Na verdade esse grupo pode não ser cíclico e mesmo que seja cíclico, desejamos evitar o esforço de verificar se B é um gerador (ou mesmo a determinar o número de N pontos). Desejamos que o subgrupo gerado por B seja grande, e de preferência, com a mesma ordem de grandeza de E. Basta supor que B seja um ponto fixo em E conhecido publicamente, cuja ordem é muito grande (N ou um divisor grande de N).

Exemplo 3.6. Suponha que Alice e Bob queiram utilizar a curva elíptica $E : y^2 = x^3 + 373x + 402$ sobre o corpo primo finito $\mathbb{Z}_{3697}$. Eles escolhem publicamente $B = (32, 1368)$ em E. Alice escolhe $a = 512$ que será sua chave secreta e envia para Bob $S = aB = 512(32, 1368) = (1612, 1867)$. Ele, por sua vez, escolhe $b = 867$ e retorna $T = bB = 867(2100, 2001)$ e verifica a chave calculando $P = baB = bS = 867((1612, 1867) = (3382, 2775)$. Alice ao receber T calcula $P = aT = abB = 512(2100, 2001) = (3382, 2775)$. Dessa forma apenas Alice e Bob compartilham da chave $P = aT = abB = baB = aS = (3382, 2775)$.

3.2.5 A analogia de Massey-Omura

Como no caso do corpo finito, este é um criptossistema de chave pública para transmissão de unidades de mensagens m, a qual supomos estar imersas como pontos P_m em alguma (e publicamente conhecida) curva elíptica E sobre $\mathbb{F}_q$ fixa (onde q é grande).

Supomos que o número N de pontos em E tenha sido calculado (e é também conhecido publicamente). Cada usuário do sistema escolhe secretamente um inteiro aleatório e entre 1 e N tal que m.d.c.$(e, N) = 1$ e usando o algoritmo de Euclides podemos calcular $d \equiv e^{-1} \mod N$, isto é, um inteiro d tal que $de \equiv 1 \mod N$. Se Alice quer enviar a mensagem P_m para Bob, primeiro ela envia o ponto $e_A P_m$ para ele (onde o subscrito A denota a usuária Alice).

Isso não significa nada para Bob, que não conhece d_A nem e_A, e não pode recuperar P_m. Mas, sem tentar dar sentido, por enquanto, ele multiplica $e_A P_m$ por e_B, e envia $e_B e_A P_m$ de volta para Alice. Na terceira etapa, Alice multiplica o ponto $e_B e_A P_m$ por d_A. Como $NP_m = O$ e $d_A e_A \equiv 1 \mod N$, $d_A e_B e_A P_m = e_B P_m$, Alice retorna para Bob, que pode ler a mensagem multiplicando o ponto $e_B P_m$ por d_B.

Note que um invasor conheceria $e_A P_m$, $e_B e_A P_m$ e $e_B P_m$. Se ele pudesse resolver o problema do logaritmo discreto sobre E, determinaria e_B sobre os dois primeiros pontos e então calcularia $d_B = e_B^{-1} \mod N$ e $P_m = d_B(e_B P_m)$.

3.2.6 Analogia de ElGamal

Este é um outro criptossistema de chave pública para transmissão de mensagens P_m. Como no sistema de troca de chaves acima, começamos fixando um corpo finito $\mathbb{F}_q$, uma curva elíptica E definida sobre ele, e um ponto inicial $B \in E$. (Não é preciso conhecer o número de pontos N). Cada usuário escolhe um inteiro aleatório a, que é mantido em segredo, calcula e publica o ponto aB.

Para enviar uma mensagem P_m para Bob, Alice escolhe um inteiro aleatório a e envia um par de pontos $(aB, P_m + a(bB))$, onde bB é a chave pública de Bob. Para escrever a mensagem, Bob multiplica a coordenada do primeiro ponto por sua chave secreta b e subtrai o resultado do segundo ponto,

$$P_m + a(bB) - b(aB) = P_m.$$

Exemplo 3.7. Consideremos que Alice e Bob realizaram a troca de chaves como no exemplo anterior utilizando o ponto $B = (32, 1368)$ na curva elíptica $y^2 = x^3 + 373x + 402$.

Alice quer enviar para Bob a palavra UNESP. Para isso ela associada a cada letra do alfabeto a um número a começar de $A = 1$, $B = 2$, e assim por diante. Dessa forma ela obtem a seguinte sequência para representar a palavra UNESP: 21 14 05 19 16. Para facilitar o envio da mensagem sobre a curva elíptica escolhida, ela quebra a sequência

em três blocos, 2114 0519 16, e utiliza cada um deles como valores de a, calculando P_{m_1}:

$$P_{m_1} = a_1 B = 2114(32, 1368) = (662, 3395)$$
$$P_{m_2} = a_2 B = 519(32, 1368) = (359, 1770)$$
$$P_{m_3} = a_3 B = 16(32, 1368) = (1403, 543)$$

Assim, Alice envia P_m disfarçado juntamente com uma pista aB que é suficiente para remover a máscara abB se for conhecido o inteiro secreto b, ou seja , para cada a_i Alice calcula $c_i = P_i + aT$ e o envia juntamente com aB para Bob. Ao receber o conjunto de pontos $\{aB, c_1, c_2, c_3\}$, Bob faz a leitura da mensagem atráves dos seguintes cálculos:

$$P_{m_i} = c_i - bS$$
$$P_{m_1} = (1827, 1152) - 867(1612, 1867) = (662, 3395)$$
$$P_{m_2} = (545, 947) - 867(1612, 1867) = (359, 1770)$$
$$P_{m_3} = (3063, 826) - 867(1612, 1867) = (1403, 543)$$

3.2.7 A escolha do ponto na curva e seleção "aleatória"de (E, B)

Existem vários caminhos para escolher uma curva elíptica e utilizar a troca de chaves de Diffie-Hellman e o sistema de ElGamal com um ponto B na mesma. Uma vez que escolhemos o corpo finito $\mathbb{F}_q$ grande, podemos escolher tanto E quanto o ponto $B = (x, y) \in E$ ao mesmo tempo como segue.

Vamos supor que a característica é maior que 3, de modo que as curvas elípticas são dadas pela equação $y^2 = x^3 + ax + b$. Primeiro, seja x, y, a três elementos aleatórios de $\mathbb{F}_q$. Colocamos $b = y^2 - (x^3 + ax)$ e verificamos que a cúbica $x^3 + ax + b$ não tem raízes múltiplas, o que é equivalente a dizer que $4a^3 + 27b^2 \neq 0$. Se esta condição não é satisfeita, então devemos fazer uma outra escolha aleatória de x, y e a. Seja $B = (x, y)$, então B é um ponto na curva elíptica $y^2 = x^3 + ax + b$.

Se é preciso conhecer o número N de pontos, existem várias técnicas disponíveis para calcular N atualmente. O primeiro algoritmo polinomial que calcula o número de elementos de E, descoberto por *René Schoof* é determinístico. Ele basea-se na ideia de determinar o número de elementos de E módulo l, para todo primo l menor que um certo valor. Este é feito pelo exame da ação do *automorfismo de Frobenius* (p-ésima potência) nos pontos de ordem l.

No artigo original [7] o limite de tempo de funcionamento era essencialmente $O(\log q^8)$, que é polinomial, mas pouco conveniente. De início, parecia que o algoritmo não era prático, mas desde então, muitas pessoas tem trabalhado sobre a aceleração desse algoritmo. Além disso, no mesmo artigo é citado que *Atkins* desenvolveu um método um pouco diferente, que embora não garante o trabalho em tempo polinomial, mas

na prática funciona muito bem (não foi possível obter tal manuscrito). Como resultado de todos estes esforços, tornou-se possível calcular a ordem de uma curva elíptica arbitrária sobre $\mathbb{F}_q$ se q é uma potência de primo, de 50 ou de 100 dígitos inicialmente.

Também deve ser ressaltado que, embora tenha-se que conhecer N, a fim de implementar o sistema de Diffie-Hellman ou o sistema de ElGamal, na prática se quer garantir sua segurança, devemos tomar N com um fator primo grande. Se N é um produto de números primos pequenos, então o método de *Pohlig-Prata-Hellman* citado em [3] pode ser usado para resolver o problema do logaritmo discreto. Assim, é preciso saber que N não é um produto dos números primos pequenos, é pouco provável que se saiba disto a menos que se tenha o valor real de N.

3.2.8 A redução Global de $(E, B) \mod p$

Vamos agora mencionar uma segunda maneira de determinar um par constituído por uma curva elíptica e um ponto sobre ela. Inicialmente escolha uma curva elíptica sobre um corpo infinito e um ponto de ordem infinita sobre ele. Assim, seja E uma curva elíptica definida sobre o corpo dos números racionais (ou, de modo mais geral, poderíamos usar uma curva elíptica definida sobre um corpo de números algébricos), e seja B um ponto de ordem infinita em E.

Em seguida, escolhemos um primo grande p (ou, se a curva elíptica está definida sobre uma extensão K de $\mathbb{Q}$, optamos por um ideal primo do anel de inteiros de K) e consideramos a redução de E e B módulo p.

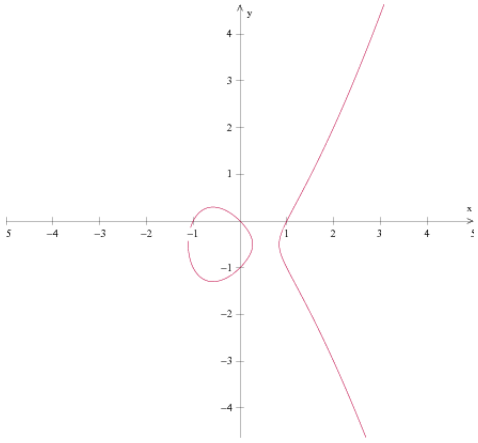
Mais precisamente, para todos os primos p, com exceção de alguns pequenos, os coeficientes da equação para E não tem p em seus denominadores, então podemos considerar os coeficientes desta equação módulo p. Se fizermos uma mudança de variável, obtendo a equação resultante sobre $\mathbb{F}_p$ na forma $y^2 = x^3 + ax + b$, a cúbica à direita não tem raízes múltiplas (exceto no caso de alguns primos pequenos p), e assim obtemos uma curva elíptica (denotado por $E \mod p$) sobre $\mathbb{F}_p$. As coordenadas de B também irá reduzir-se a módulo p para dar um ponto (o que denota que $B \mod p$) sobre a curva elíptica $E \mod p$.

Exemplo 3.8. Considere a curva elíptica $E : y^2 + y = x^3 - x$ sobre os racionais. Graficamente temos:

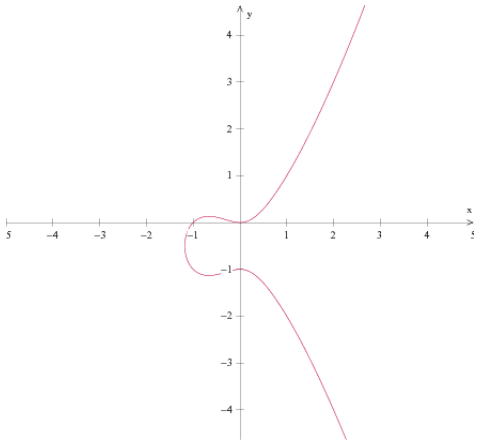
Subtituindo y por $y - \dfrac{1}{2}$, obtemos:

$$y^2 = x^3 - x + \frac{1}{2}.$$

Assim o ponto $B = (0, 0)$ é um ponto de ordem infinita sobre a curva elíptica $E : y^2 + y = x^3 - x$, pois não existe n tal que $n.B = O$ e assim gera todo o grupo de pontos racionais de E.



Exemplo 3.9. Na curva elíptica $E : y^2 + y = x^3 + x^2$, temos o seguinte gráfico:



Substituindo y por $y - \frac{1}{2}$ obtemos

$$y^2 + y = x^3 + x^2 + \frac{1}{4}.$$

E nessa última, substituimos x por $x - \frac{1}{3}$, e obtemos a equação:

$$y^2 = x^3 - \frac{1}{3}x + \frac{35}{108}.$$

Da mesma forma o ponto $B = (0, 0)$ é um ponto de ordem infinita sobre a curva elíptica $E : y^2 + y = x^3 + x^2$, e gera todo o grupo de pontos racionais de E.

Quando usamos este método, fixamos E e B e, em seguida, testamos as possibilidades diversas, variando o primo p.

3.2.9 Ordem do ponto B

Quais são as chances de que um ponto B em uma curva elíptica seja um gerador da mesma? Ou, no caso do nosso segundo método de seleção de (E, B), quais são as

chances, de que variando p, B se reduza módulo p a um gerador de $E \mod p$? Esta questão é análoga à seguinte questão sobre grupos multiplicativos de corpos finitos: Dado um inteiro b, que é escolhido, conforme p varia, b é um gerador de $\mathbb{F}_p^*$? A questão tem sido estudada tanto em corpos finitos quanto em curvas elípticas.

Como mencionado anteriormente, para a segurança da encriptação não é necessário que B seja um gerador. O necessário é que o subgrupo cíclico gerado por B seja um grupo em que o problema do logaritmo discreto seja intratavél. Este será o caso em que todos os métodos conhecidos para resolver o problema de logaritmo discreto de um grupo abeliano arbitrário serão muito lentos, por exemplo, se a ordem de E for divisível por um primo de grandeza quase tão grande quanto N.

Uma maneira de garantir que a escolha de b seja adequada, e que de fato que B gera a curva elíptica, é escolher o corpo finito e a curva elíptica de modo que o número N de pontos da curva elíptica seja primo com a ordem do corpo finito, então todo ponto $B \neq O$ será um gerador. Assim, se usarmos o primeiro método descrito acima, para um corpo fixado $\mathbb{F}_q$ podemos escolher pares (E, B) até encontrarmos aquele para o qual o número de pontos em E é um número primo. Se usarmos o segundo método, depois de uma curva elíptica fixa E sobre $\mathbb{F}_q$, escolhemos primos p até encontrar um primo para o qual o número de pontos de $E \mod p$ seja um número primo. Qual é o tempo gasto? Esta questão é análoga à seguinte pergunta sobre os grupos $\mathbb{F}_p^*$: Se $(p-1)/2$ é primo, isto é, todo elemento diferente de ± 1 ou é um gerador ou o quadrado de um gerador? Nem para a curva elíptica, nem para o corpo finito foi obtida uma resposta definitiva, mas conjectura-se em ambos os casos, que a probabilidade que a escolha de um determinado p tenha a propriedade desejada seja $O(1/\log p)$.

Observação 3.8. Para que $E \mod p$ tenha alguma chance de ter ordem prima N para uma valor grande de p, E deve ser escolhida de forma a ter torção trivial, isto é, não ter pontos, exceto O da ordem finita. Caso contrário, N será divisível pela ordem do subgrupo de torção [3].

4 Considerações finais

A principal vantagem no uso de curvas elípticas na Criptografia em relação a outros métodos, como o RSA, é o tamanho da chave utilizada. O grupo formado pelos pontos de uma curva elíptica sobre um corpo apresenta estrutura diferenciada de grupos normalmente utilizados, assim a maioria dos ataques ao logaritmo discreto não funciona tão bem quando executados em curvas elípticas, o que leva a uma diminição significativa do tamanho da chave usada sem alterar a segurança do sistema, tornado assim um algoritmo mais rápido. Vale ressaltar que foi visto neste trabalho foi apenas uma parte da vasta e rica teoria de curvas elípticas. Além das aplicações em criptografia, é possível encontrar aplicações na teoria dos números, mais precisamente em testes de primalidade e fatoração de um número, e até mesmo na demonstração do *Último Teorema de Fermat* feita em 1995 por Andrew Willes.

Referências

[1] SANTOS, J. P. O. *Introdução à Teoria dos Números*. 3. ed. Rio de Janeiro: IMPA, 2003.

[2] COUTINHO, S. C. *Primalidade em Tempo Polinomial: Uma introdução ao Algoritmo AKS*. 1. ed. Rio de Janeiro: SBM, 2004.

[3] KOBLITZ, N. *A Course in Number Theory and Cryptography*. 2. ed. New York: Springer-Verlag, 1994.

[4] MORDELL, L. J. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc*, v. 21, p. 179–192, 1922.

[5] J.H.SILVERMAN. *The Arithmetic of Elliptic Curves*. 2. ed. New York: Springer, 1992.

[6] STEWART, I. *Game, Set e Math - Enigmas and Conundrums*. 1. ed. Oxford: Basil Blackwell, 1989.

[7] SCHOOF, R. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, v. 44, p. 483–494, 1985.

[8] ODLYZKO, A. M. Discrete logarithms in finite fields and their cryptographic significance. *Proc. Eurocrypt*, v. 94, p. 224–314, 1985.

[9] A.MENEZES T.OKAMOTO, S. Reducing elliptic curve logaritms to logaritms in a finite field. *IEEE Trans on Information Theory*, v. 39, p. 1639–1646, 1993.

A Alguns Algoritmos

Para a realização dos exemplos deste trabalho, foram criados alguns algoritmos no programa *SCILAB* para facilitar os cálculos. Em nenhum deles houve a preocupação em a otimizar o número de iterações.

A.1 Gerador de pontos e múltiplos de pontos de uma curva elíptica sobre um corpo finito

Neste primeiro algoritmo é possível encontrar alguns pontos de uma curva elíptica da forma $y^2 = x^3 + ax + b$ sobre um corpo finito. Não podemos afirmar que são todos os pontos possivéis.

GERADOR DE PONTOS

```
function[P]=pontoselipticos(a,b,F)
    k=1;
    lsup=((F+1)/2)**2
    for i=0:F-1
        z=i**3+a*i+b;
        z=z-F*int(z/F)
        if z<0
            z=z+F
        end
        stop=0
        while stop =1
            y=sqrt(z)
            if int(y)==y
                P(k,1)=i
                P(k,2)=y
                k=k+1
                if y =0
                    y2=-y+F
```

```
                P(k,1)=i
                P(k,2)=y2
                k=k+1
            end
            stop=1
        end
        if z =0
            z=z+F
        end
        if z<0
            z=z+F
        end
        if z>lsup
            break
        end
    end
end
endfunction
```

O algoritmo abaixo permite realizar a operação nP dado um ponto da curva elíptica sobre um corpo finito utilizando as fórmula de duplicação de uma ponto encontradas na seção 3.1.

MULTIPLICADOR DE PONTOS

```
function[A]=gpeliptico(a,xp,yp,F)
//teorema de Hasse
    aux=sqrt(F)
    if int(aux) =aux
        aux=int(aux)+1
    end
    N=F+1+2*aux;
    A(1,1)=1;
    A(1,2)=xp;
    A(1,3)=yp;
    stop=0;
    xq=xp;
    yq=yp;
    //passo P=Q
    tn=(3*xp**2+a);
    td=2*yp;
```

```
while tn/td =int(tn/td)
    tn=tn+F
end
t=tn/td
xr=t**2-xp-xq;
yr=t*(xp-xr)-yp;
xr=xr-F*int(xr/F);
yr=yr-F*int(yr/F);
if xr<0
    xr=xr+F
end
if yr<0
    yr=yr+F
end
A(2,1)=2;
A(2,2)=xr;
A(2,3)=yr;
j=3;
xq=xr;
yq=yr;
//passo P =Q
while stop==0
    tn=(yq-yp);
    td=(xq-xp);
    while tn/td =int(tn/td)
        tn=tn+F
    end
    t=tn/td;
    xr=t**2-xp-xq;
    yr=t*(xp-xr)-yp;
    xr=xr-F*int(xr/F);
    yr=yr-F*int(yr/F);
    if xr<0
        xr=xr+F
    end
    if yr<0
        yr=yr+F
    end
    A(j,1)=j;
    A(j,2)=xr;
```

```
        A(j,3)=yr;
        xq=xr;
        yq=yr;
        j=j+1;
        if xr==xp
            stop=1
        elseif j==N
            stop=1
        end
    end
endfunction
```

A.2 Codificador e decodificador de mensagens

Para codificar e decodificar a palavra UNESP no exemplo 3.7, utilizamos os algoritmos abaixo baseados que juntos colocam em prática o método de El-Gammal.

SOMA DE PONTOS

```
function[xp3,yp3]=somador(a,xp1,yp1,xp2,yp2,F)
    if xp1==xp2
    //passo P=Q
        tn=(3*xp1**2+a);
        td=2*yp1;
        while tn/td =int(tn/td)
            tn=tn+F
        end
        t=tn/td
        xr=t**2-xp1-xp2;
        yr=t*(xp1-xr)-yp1;
        xr=xr-F*int(xr/F);
        yr=yr-F*int(yr/F);
        if xr<0
            xr=xr+F
        end
        if yr<0
            yr=yr+F
        end
        xp3=xr;
        yp3=yr;
```

```
    else
    //passo P =Q
        tn=(yp2-yp1);
        td=(xp2-xp1);
        while tn/td =int(tn/td)
            tn=tn+F
        end
        t=tn/td;
        xr=t**2-xp1-xp2;
        yr=t*(xp1-xr)-yp1;
        xr=xr-F*int(xr/F);
        yr=yr-F*int(yr/F);
        if xr<0
            xr=xr+F
        end          if yr<0
            yr=yr+F
        end
        xp3=xr;
        yp3=yr;
    end
endfunction

// dados da curva usados no exemplo 3.7:
a=373
b=402
F=3697
xp=32
yp=1368
```

CODIFICAÇÃO DA MENSAGEM

```
function[c2,aP,m1,bP]=crip(num)
//cripitografandu a palavra UNESP
    A=gpeliptico(a,xp,yp,F);
    aP=[A(512,2),A(512,3)]; //alice escolheu o numero 512
    bP=[A(867,2),A(867,3)]; //bob escolheu o numero 867
    A1=gpeliptico(a,bP(1),bP(2),F);
    abP=[A1(512,2),A1(512,3)];
    m1=[A(num,2),A(num,3)];
    [xp3,yp3]=somador(a,m1(1),m1(2),abP(1),abP(2),F);
```

```
    c2=[xp3,yp3];
endfunction
```

DECODIFICAÇÃO DA MENSAGEM

```
function[m1n,baP]=decrip(c2,aP)
    A2=gpeliptico(a,aP(1),aP(2),F);
    baP=[A2(867,2),A2(867,3)];
    baP(2)=-baP(2)+F;
    [xp4,yp4]=somador(a,c2(1),c2(2),baP(1),baP(2),F);
    m1n=[xp4,yp4];
endfunction
```