UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

RIGO JULIAN OSORIO ANGULO

Criptografia de Curvas Elípticas

Goiânia-GO
2017

sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[x] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação

Nome completo do autor: Rigo Julian Osorio Angulo

Título do trabalho: Criptografia de Curvas Elípticas

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.

Rigo Julian Osorio Angulo

Assinatura do (a) autor (a)

Data: 15 /03 /2017

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

RIGO JULIAN OSORIO ANGULO

Criptografia de Curvas Elípticas

Dissertação apresentada ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Mestrado em Matemáticas.

Área de concentração: Álgebra.

Orientadora: Profa. Dra. Ana Paula de Araújo Chaves

Goiânia-GO
2017

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Osorio Angulo, Rigo Julian
Criptografia de Curvas Elípticas [manuscrito] / Rigo Julian Osorio Angulo. - 2017.
100 f.: il.

Orientador: Profa. Dra. Ana Paula de Araújo Chaves.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), Programa de Pós-Graduação em Matemática, Goiânia, 2017.
Bibliografia.
Inclui tabelas, lista de figuras, lista de tabelas.

1. Criptografia. 2. Corpos finitos. 3. Curvas Elípticas. I. de Araújo Chaves, Ana Paula , orient. II. Título.

CDU 512.5

UFG

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Campus Samambaia – Caixa Postal 131 – CEP: 74.001-970 – Goiânia-GO.
Fones: (62) 3521-1208 e 3521-1137 www.ime.ufg.br

ATA DA REUNIÃO DA BANCA EXAMINADORA DA DEFESA DE DISSERTAÇÃO DE RIGO JULIAN OSORIO ANGULO – Aos quinze dias do mês de março do ano de dois mil e dezessete (15/03/2017), às 14:00 horas, reuniram-se os componentes da Banca Examinadora: Profa. Ana Paula de Araújo Chaves - Orientadora, Prof. Paulo Henrique de Azevedo Rodrigues e Prof. Hemar Teixeira Godinho, para, sob a presidência da primeira, e em sessão pública realizada na sala de aula do Instituto de Matemática e Estatística, procederem a avaliação da defesa de dissertação intitulada: **"Criptografia de Curvas Elípticas"**, em nível de Mestrado, área de concentração em Álgebra, de autoria de Rigo Julian Osorio Angulo, discente do Programa de Pós-Graduação em Matemática da Universidade Federal de Goiás. A sessão foi aberta pela Presidente da Banca, Profa. Ana Paula de Araújo Chaves, que fez a apresentação formal dos membros da Banca. A seguir, a palavra foi concedida ao autor da dissertação que, em 45 minutos procedeu a apresentação de seu trabalho. Terminada a apresentação, cada membro da Banca arguiu o examinando, tendo-se adotado o sistema de diálogo sequencial. Terminada a fase de arguição, procedeu-se a avaliação da defesa. Tendo-se em vista o que consta na Resolução nº. 1068 do Conselho de Ensino, Pesquisa, Extensão e Cultura (CEPEC), que regulamenta o Programa de Pós-Graduação em Matemática e procedidas as correções recomendadas, a dissertação foi **APROVADA** por unanimidade, considerando-se integralmente cumprido este requisito para fins de obtenção do título de **MESTRE EM MATEMÁTICA**, na área de concentração em Álgebra pela Universidade Federal de Goiás. A conclusão do curso dar-se-á quando da entrega na secretaria do PPGM da versão definitiva da dissertação, com as devidas correções supervisionadas e aprovadas pela orientadora. Cumpridas as formalidades de pauta, às 16:00 horas a presidência da mesa encerrou esta sessão de defesa de dissertação e para constar eu, Ulisses José Gabry, secretário do PPGM, lavrei a presente Ata que, depois de lida e aprovada, será assinada pelos membros da Banca Examinadora em quatro vias de igual teor.

Ana Paula de A. Chaves
Profa. Dra. Ana Paula de Araújo Chaves
Presidente - IME/UFG

Prof. Dr. Paulo Henrique de Azevedo Rodrigues
Membro – IME/UFG

Hemar T. Godinho
Prof. Dr. Hemar Teixeira Godinho
Membro – DM/UnB

RIGO JULIAN OSORIO ANGULO

CRIPTOGRAFIA DE CURVAS ELÍPTICAS

Dissertação defendida no Programa de Pós-Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Matemática, aprovada no dia 15 de março de 2017, pela Banca Examinadora constituída pelos professores:

Ana Paula de G. Chaves

Profa. Dra. Ana Paula de Araújo Chaves
Instituto de Matemática e Estatística - UFG
Presidente da Banca

Prof. Dr. Paulo Henrique de Azevedo Rodrigues
Instituto de Matemática e Estatística - UFG

Hemar T. Godinho

Prof. Dr. Hemar Teixeira Godinho
Departamento de Matemática – UnB

Rigo Julian Osorio Angulo

É bacharel em Matemática pela Universidade del Cauca-Colômbia.

Aos meus pais, Otilia Angulo, Rigoberto Osorio, meu irmão Martin Osorio, e meu sobrinho John Anderson, por seu infinito apoio.

Agradecimentos

Agradeço a tudo o pessoal que de alguma forma ou outra me ajudou nesta etapa de minha vida que concluiu: a meus familiares, que desde Colômbia estiveram torcendo por mim, para que tudo fora sucesso. A meus professores do mestrado da UFG, por me ajudar na minha formação como mestre, foi de grande valor seus conhecimentos. À professora Ana Paula Chaves, por ter me orientado. À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), pelo apoio econômico. Aos meus colegas colombianos e brasileiros, por compartilhar estes dois anos comigo. Graças a todos!

Todo mundo é um gênio. Mas se você julgar um peixe por sua capacidade de subir em uma árvore, ele vai passar toda a sua vida acreditando que ele é um tolo.

Anônimo.

Resumo

Osorio, Rigo. **Criptografia de Curvas Elípticas**. Goiânia-GO, 2017. 100p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Segundo a história, o objetivo principal da criptografia sempre foi oferecer segurança nas comunicações, para mantê-las fora do alcance de entidades não autorizadas. No entanto, com o advento da era da computação e as telecomunicações, as aplicações da criptografia se expandiram para oferecer além de segurança, a capacidade de: verificar que uma mensagem não tenha sido alterada por um terceiro, poder verificar que um usuário é quem diz ser, entre outras. Neste sentido, a criptografia de curvas elípticas, oferece certas ventagens sobre seu sistemas análogos, referentes ao tamanho das chaves usadas, redundando isso na capacidade de armazenamento dos dispositivos com certas limitações de memória.

Assim, o objetivo deste trabalho é fornecer ao leitor as ferramentas matemáticas necessárias para a compreensão de como as curvas elípticas são usadas na criptografia de chave pública.

Palavras–chave

Criptografia, Corpos finitos, Curvas Elípticas.

Abstract

Osorio, Rigo. **Cryptography of Elliptic Curves**. Goiânia-GO, 2017. 100p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

According to history, the main objective of cryptography was always to provide security in communications, to keep them out of the reach of unauthorized entities. However, with the advent of the era of computing and telecommunications, applications of encryption expanded to offer security, to the ability to: verify if a message was not altered by a third party, to be able to verify if a user is who claims to be, among others. In this sense, the cryptography of elliptic curves, offers certain advantages over their analog systems, referring to the size of the keys used, which results in the storage capacity of the devices with certain memory limitations.

Thus, the objective of this work is to offer the necessary mathematical tools for the understanding of how elliptic curves are used in public key cryptography.

Keywords

Cryptography, Finite Fields, Elliptic Curves.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

Criptografia é o ramo da criptologia que trata do desenho de algoritmos para encriptação e desencriptação, destinada a assegurar o carácter secreto e/ou a autenticidade da mensagem. Mais precisamente, na atualidade, graças aos estudos de Shanon [32] em 1949, se considera a criptografia como uma ciência aplicada, a qual se encarga do estudo das técnicas matemáticas relacionadas com os aspectos da segurança da informação, tais como: a confidencialidade, a integridade dos dados, a autenticidade e o não-repúdio. Podemos descrever brevemente estos aspectos como segue:

- **A confidencialidade** é usada para assegurar o conteúdo da informação, onde só as pessoas autorizadas puderem sabê-lo.
- **A integridade** dos dados refere-se à alteração não autorizada dos dados.
- **A autenticação** é relacionada com a identificação.
- **O não-repúdio** impede a uma entidade negar as ações acima.

A criptografia, dada a sua natureza, foi principalmente usada na antiguidade com fins bélicos, por governantes e militares, pela necessidade de transmitir, durante as guerras, de maneira secreta e segura estratégias de ataque, e outros comunicados classificados como confidenciais, mas também teve, em menor escala, usos comercias, especialmente por banqueiros.

A história da criptografia, se acredita que começou mais ou menos há 4000 anos, em 1900 a.C. durante a civilização egípcia, onde se encontraram inscrições cifradas sobre a tumba do nobre chamado Khnumhotep II, na cidade de Menet Khufu, perto do rio Nilo. Se supõe que a técnica usada foi "substituição simples", o que significa que cada símbolo da mensagem original é substituído por outro símbolo, e somente a pessoa que soubesse as substituições corretas, podia ler a mensagem. Já do ano 590 a.C., se tem conhecimento do primeiro algoritmo de cifra, usado pelos hebreus e chamado de *Atbash*, o qual consiste simplesmente em fazer uma substituição, tomado o alfabeto original de trás para frente, motivo pelo qual também é conhecido como o método do espelho, tal e como mostra a Tabela 1. Assim, com esta técnica, a mensagem "BOM DIA" é cifrada como "YLN WRZ".

A	B	C	⋯	Z
↓	↓	↓		↓
Z	Y	X	⋯	A

Tabela 1: *Método Atbash.*

No ano 487 a.C. os Espartanos da antiga Grécia criaram o primeiro aparelho cifrador chamado de *Cítala*, que significa bastão, o qual consiste no uso de duas varas da mesma espessura, que estavam cada uma na posse de um dos participantes da comunicação. Para enviar uma mensagem, era enrolada uma tira de couro ou papiro, de forma espiral, a um dos bastões e era escrita a mensagem longitudinalmente como na Figura 1, de forma que em cada volta da tira aparecesse uma letra de cada vez. Uma vez escrita a mensagem, a tira era desenrolada e era enviada ao receptor, que só tinha que a enrolar no bastão gémeo para ler a mensagem original. Note que a "chave" deste método é o diâmetro da vara.

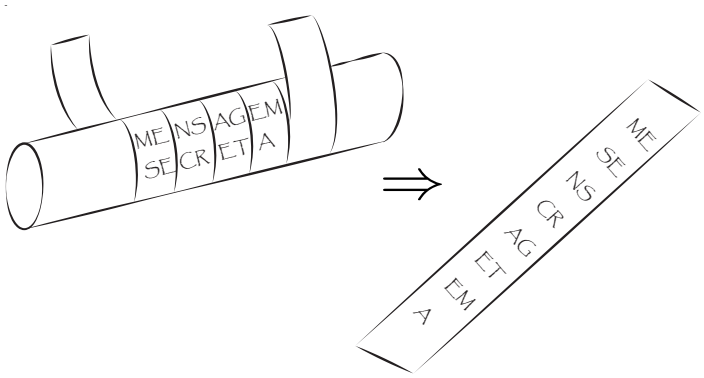

Figura 1: *Cítala espartana.*

Uma outra técnica usada pelos gregos foi a Tabela 2 chama de "Polybius", inventada pelo historiador Polívio no ano 150 a.C. a qual consistia em associar cada letra do alfabeto com um par de números correspondentes as coordenadas da sua posição na tabela. Assim, com este método, a mensagem "OLÁ" é cifrado como "343111".

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Tabela 2: *Tabela Polybius.*

Os romanos também fizeram contribuições à criptografia, com o método mais conhecido dessa época, denominado *Cifrado de César*, o qual estudaremos em detalhe

na Subseção 3.1.1. Assim como estes, existem outros métodos usados na antiguidade, os quais também eram baseados no uso de substituições e transposições monoalfabéticas. Já na Europa da Idade Média e o Renascimento, no ano 1466, graças a León Battista Alberti, que fora músico, pintor, escritor e arquiteto; surgiram métodos mais avançados que usavam a substituição polialfabética, os quais requeriam vários alfabetos em círculos concêntricos como mostra a Figura 2, pulando de um para outro cada três ou quatro palavras. Um século depois, era introduzido por Blaise Vigenère, um dos primeiros

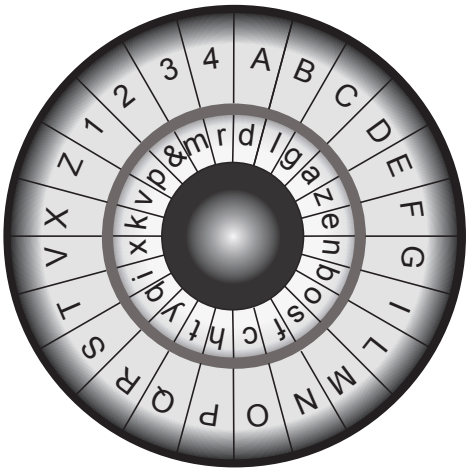

Figura 2: *Disco de Alberti.*

métodos compostos para cifrar, o chamado *Cifrado Vigenère*, o qual, de algum modo, generaliza o Cifrado de César. Na Observação 3.9, o veremos com mais detalhe.

Entre os anos 1790 e 1800, o presidente dos Estados Unidos da América, Thomas Jefferson, inventou a primeira máquina manual para cifrar, a qual consistia de um conjunto de discos que giravam em torno de um eixo, onde nos mesmos se colocava o alfabeto de maneira aleatória como mostra a Figura 3. Para cifrar uma mensagem, se colocavam os discos em uma ordem estabelecida (a chave), alinha-se a mensagem, e toma-se como mensagem cifrada as outras letras alinhadas. Este aparelho é um dos mais antigos, que

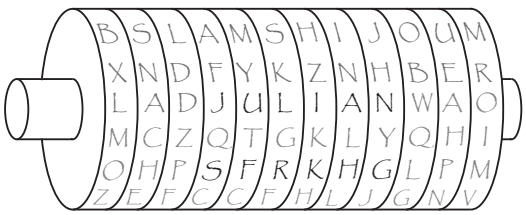

Figura 3: *Primeiro Dispositivo Manul-mecânico.*

se conservou, e que inspirou as bases dos sistemas electro-mecânicos posteriores de cifrador, que surgiram no século XX, século no qual se revolucionou a criptografia graças

à proliferação desses aparelhos os quais foram usados em maior parte na segunda guerra mundial. Esses consistiam de uma sequência de rotores móveis, que giravam de acordo com cada tecla que era puxada sobre um teclado, e retornavam num painel a respetiva letra cifrada. O exemplo mais importante deste tipo de máquinas, é a **Enigma**, Figura 4, uma máquina inventada pelo alemão Arthur Scherbius e usada pelos nazistas na segunda guerra mundial. As máquinas de cifrar foram desaparecendo entre os anos 60 e 70, coincidindo

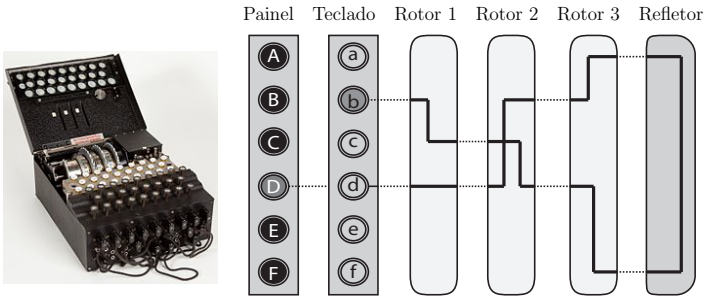

Figura 4: *Máquina Enigma.*

com o começo da época de ouro da criptografia com a invenção da criptografia de "chave pública". Para mais detalhes sobre história da criptografia ver [13], [34].

Existem dois tipos de criptografia, *criptografia simétrica*, ou de *chave privada* e *criptografia assimétrica*, ou de *chave pública*. Todos os sistemas vistos acima são de chave privada, significando que empregam a mesma "chave privada" tanto para cifrar como para decifrar. Este tipo de sistemas somente oferecem **confidencialidade**. Já no ano 1976 começa a revolução na criptografia com os estudos feito por Whitfield Diffie e Martin Hellman [2], que introduziram o conceito de *Criptografia de Chave Pública*, cuja diferença para simétrica é que se usam duas chaves, uma pública e outra privada. Uma vez introduzido este tipo de criptografia, começam a ser desenvolvidos sistemas criptográficos que oferecem confidencialidade, integridade, autenticação e não-repúdio. A criptografia de chave pública baseia seu funcionamento no uso de dois problemas matemáticos antigos, os quais são denominados como **funções trapdoor**.

Uma função trapdoor, é uma função para a qual sua imagem direta é fácil de calcular, mas sua imagem inversa, é computacionalmente difícil de calcular sem a ajuda de uma certa informação extra: a "chave de desencriptação". Neste sentido, foram usados o problema do logaritmo discreto, e o problema da fatoração inteira.

Dado um grupo finito G e dois elementos $a, b \in G$, tais que $a = b^x$ para um certo $x \in \mathbb{Z}$, se define o logaritmo discreto de a na base b como sendo x, e denotado por $\log_b a$.

Note que, dados $b \in G$ e $x \in \mathbb{Z}$, é fácil calcular b^x usando o método dos quadrados repetidos, mas dado $a \in G$ (o qual sabemos é da forma b^x) é computacionalmente inviável encontrar x. Este último, é chamado o *problema do Logaritmo Discreto*. Essa simples

idéia, mas tomada no corpo finito F_q, foi explorada por Diffie e Hellman, para definir seu sistema de troca de chaves.

Um ano mais tarde, os matemáticos Ron Rivest, Adi Shamir e Len Adleman [27], inventam o sistema criptográfico RSA, o qual baseia seu funcionamento no problema da fatoração inteira, no qual um usuário escolhe dois números primos p e q como sua chave privada, e publica seu produto $n = pq$, como sua chave pública. Vemos aqui, que encontrar n dados p e q é fácil, mas dado n, é computacionalmente inviável descobrir p e q. Entretanto, devido ao progresso recente em fatorar números cada vez maiores com mais facilidade, chaves públicas de RSA devem agora ter milhares de longos bits para fornecer a segurança adequada.

Já no ano 1985, a ideia de usar o problema do logaritmo discreto foi retomada por Neal Koblitz e Victor Miller, de maneira independente, mas desta vez eles usaram o grupo finito de uma *curva elíptica*.

Dado um corpo K, uma curva elíptica E definida sobre o fecho algébrico $\overline{K}$ é o conjuntos de pontos $(x,y) \in \overline{K} \times \overline{K}$ que satisfazem a equação

$$y_1^2 + a_1x_1y_1 + a_3y_1 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6, \quad \text{onde} \quad a_1,a_2,a_3,a_4,a_6 \in \overline{K}.$$

O conjunto de pontos em uma curva E pode ser pode ser dotado de uma certa operação de adição, a qual junto com um ponto especial que atua como o elemento neutro, e é chamado de ponto no infinito, formam um grupo abeliano.

Se as coordenadas x e y de uma curva elíptica E forem escolhidas de um grande corpo finito F_q, as soluções darão forma a um Grupo Abeliano finito. O problema com Logaritmo Discreto é que em tais grupos de curvas elípticas ele é visto como mais difícil do que o problema correspondente no corpo finito subjacente. Assim, o grande atrativo de trabalhar com o grupo formado por uma curva elíptica é que as chaves do sistema criptográfico podem ser escolhidas para serem muito mais curtas mas com um nível comparável da segurança.

Neste trabalho serão estudados os aspectos essenciais da Criptografia em Curvas Elípticas, os quais serão divididos da seguente maneira: no Capítulo 1, serão estudados brevemente conceitos básicos da teoria de corpos, para depois fazer ênfase nos tópicos referentes a corpos finitos e reciprocidade quadrática; no Capítulo 3 estudaremos em detalhe os conceitos relativos à criptografia; no Capítulo 4 sarão estudados alguns tópicos importantes de curvas elípticas, para depois estudar sua aplicação na criptografia, e finalmente, no Capítulo 5 são apesentadas duas aplicações das curvas elípticas para teste de primalidade e fatoração de números inteiros.

CAPÍTULO 1

Corpos Finitos e Resíduos Quadráticos

Neste capítulo são apresentados os conceitos básicos necessários, referentes à teoria dos números, para o desenvolvimento do nosso trabalho. Na primeira parte será apresentado um breve resumo dos conceitos de: corpo, espaço vetorial, anel de polinômios, extensões de corpos, entre outros tópicos, e suas propriedades fundamentais, para as quais suas provas serão omitidas, mas podem ser consultadas em [10]. Fazemos particular ênfase nas Seções 1.1 e 1.2, de Corpos finitos e Resíduos Quadráticos respectivamente, as quais, para maior profundidade, podem também ser consultadas em [15] e [11].

Um corpo é um conjunto F não vazio com as operações de multiplicação e adição, que satisfazem as propriedades já familiares — associativa e comutativa de ambas, lei distributiva, existência de uma identidade aditiva 0, e uma identidade multiplicativa 1, inversos aditivos, e inversos multiplicativos para todo elemento distinto de 0.

Um espaço vetorial pode ser definido sobre qualquer corpo F por as mesma propriedades que são usadas para definir um espaço vetorial sobre os números reais.

Qualquer espaço vetorial tem uma base, e o número de elementos na base é chamado de dimensão. Uma extensão de corpo, ou seja, um corpo contendo F, é automaticamente um espaço vetorial sobre F. Dizemos que a extensão é finita se este é um espaço vetorial de dimensão finita. O grau de uma extensão finita é a dimensão desta, vista como espaço vetorial. Uma forma de obter uma extensão de corpos é adjuntar um elemento à F: dizemos que $K = F(\alpha)$ se K é o corpo consistindo de todas as expressões racionais formadas usando α e os elementos de F.

Da mesma forma, um anel de polinômios pode ser definido sobre qualquer corpo F. É denotado por $F[X]$; e consiste de todas as somas finitas de potências de X com coeficientes em F.

A soma e a multiplicação em $F[X]$ são feitas da mesma maneira como nos polinômios sobre os reais. O *grau d* de um polinômio é a maior potência de X que ocorre com o coeficiente não nulo; num *polinômio mônico* o coeficiente de X^d é 1. Dizemos que g divide f, onde $f, g \in F[X]$, se existir um polinômio $h \in F[X]$ tal que $f = gh$. Os polinômios irredutíveis $f \in F[X]$ são aqueles que não são divisíveis por nenhum polinômio de menor grau exceto por constantes; eles têm o mesmo papel entre os polinômios, que os primos

entre os inteiros. O anel de polinômios tem fatoração única, isso significa que cada polinômio mônico pode ser escrito de maneira única (exceto pela ordem dos fatores) como o produto de polinômios mônicos irredutíveis. (Um polinômio não mônico pode ser unicamente escrito como uma constante vezes um produto desse tipo).

A *derivada* de um polinômio é definida usando a regra nX^{n-1} (não como um limite, já que limites não tem sentido em F a menos que exista um conceito de distância ou topologia em F). Um polinômio f de grau d pode ou não ter uma *raiz* $r \in F$, ou seja, $F(r) = 0$. Se isso acontecer, então $g(X) = X - r$ divide f; se m é a maior potência de g que divide f, então dizemos que r é uma *raiz de multiplicidade m*. Por conta da fatoração única, o número total de raízes de f em F, contando multiplicidade, não pode exceder d. Se um polinômio $f \in F[X]$ tem uma raiz múltipla r, então r será uma raiz do máximo divisor comum de f e sua derivada f'.

Um elemento α em algum corpo de extensão K, contendo F, é dito *algébrico* sobre F, se é raiz de um polinômio com coeficientes em F. Em tal caso existe um único polinômio mônico irredutível em $F[X]$ do qual α é raiz (e qualquer outro polinômio do qual α é raiz, deve ser divisível por este polinômio mônico irredutível).

Se este polinômio mônico irredutível tem grau d, então qualquer elemento de $F(\alpha)$ pode ser expresso como uma combinação linear das potências $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$. Assim, essas potências de α formam uma base de $F(\alpha)$ sobre F, e portanto o grau da extensão obtida pela adjunção de α é o mesmo grau do polinômio mônico irredutível de α. Qualquer outra raiz α' do mesmo polinômio irredutível é chamada de *conjugado* de α sobre F. Os corpos $F(\alpha)$ e $F(\alpha')$ são isomorfos, por meio da transformação que toma qualquer expressão em termos de α e a envia à mesma expressão com α substituído por α'. Se todos os conjugados de α estão no corpo $F(\alpha)$, então $F(\alpha)$ é chamada uma extensão de Galois de F.

Dado um polinômio $f(X) \in F[X]$, existe um corpo de extensão K de F tal que $f(X)$ se divide em um produto de fatores lineares (equivalentemente, tem d raízes em K, contando multiplicidade, onde d é o grau) e tal que K é o menor corpo de extensão contendo essas raízes. K é chamado corpo de decomposição de f. O corpo de decomposição é único salvo isomorfismos, isso significa que se temos qualquer outro corpo K' com as mesma propriedades, então existe uma correspondência 1-1 $K \to K'$ a qual preserva adição e multiplicação.

Se somamos a identidade multiplicativa 1 com ela mesma repetidas vezes em F, e nunca obtemos 0, então dizemos que F tem característica zero; caso contrário, existe p primo tal que, se somamos 1 p vezes obtemos zero, ou seja, $1 \cdot p = \underbrace{1 + \cdots + 1}_{p-vezes} = 0$, dizemos que F tem característica p.

Se F tem característica zero, então F contém uma cópia do corpo dos números racionais. Por outra parte, se F tem característica p, então F contém uma cópia do corpo

$\mathbb{Z}/p\mathbb{Z}$, o qual é chamado de corpo primo.

1.1 Corpos Finitos

Definição 1.1 *Seja q um inteiro positivo, denotamos por F_q o corpo finito que tem q elementos.*

Note que, um corpo finito não pode ter característica zero, pois do contrário, ele tem uma cópia de $\mathbb{Q}$, que é impossível pois F_q é finito. Assim, seja p a característica de F_q. Então F_q contém o corpo primo $F_p = \mathbb{Z}/p\mathbb{Z}$, e portanto é um espaço vetorial — necessariamente de dimensão finita — sobre F_p.

Proposição 1.2 *Seja f a dimensão do F_p-espaço vetorial F_q. Existem então exatamente p^f elementos em F_q.*

A prova decorre do fato de poder escolher uma base adequada para F_q sobre F_p de f elementos, e estabelecer uma correspondência 1-1 entre as combinações lineares desses elementos e o conjunto das f-uplas de elementos de F_p.

Logo veremos que para toda potência prima $q = p^f$ existe um único corpo finito de q elementos (salvo isomorfismos). Seja F_q^* o conjunto de elementos não nulos de F_q. Entendemos pela *ordem* de $x \in F_q$, como a menor potência inteira positiva n, para qual $x^n = 1$.

1.1.1 Existência de Geradores Multiplicativos de Corpos Finitos

Existem $q-1$ elementos não nulos, e, pela definição de corpo, eles formam um grupo abeliano com respeito à multiplicação. O que segue, é um aspecto geral acerca de grupos finitos: que a ordem de qualquer elemento divide o número de elementos no grupo.

Proposição 1.3 *A ordem de qualquer elemento $a \in F_q^*$ divide $q-1$.*

Definição 1.4 *Um gerador g de um corpo finito F_q é um elemento de ordem $q-1$; equivalentemente, as potências de g percorrem todos os elementos de F_q^*.*

A seguinte proposição é um dos dos fatos mais básicos acerca de corpos finitos. Esta diz que os elementos não nulos de um corpo finito formam um grupo cíclico, ou seja, são todos potências de um único elemento.

Proposição 1.5 *Todo corpo finito tem um gerador. Se g é um gerador de F_q^*, então g^j também é gerador se, e somente se, $m.d.c.(j, q-1) = 1$. Em particular, existe um total de $\varphi(q-1)$ geradores distintos em F_q^*, onde $\varphi(n) = |\{1 \leq i \leq n \ : \ m.d.c.(i,n) = 1\}|$.*

Corolário 1.6 *Para cada primo p, existe um inteiro g tal que as potências de g geram todas as classes residuais não nulas módulo p.*

1.1.2 Existência e Unicidade de Corpos Finitos com uma Potência Prima de Elementos

Provaremos a existência e unicidade mostrando que um corpo finito de $q = p^f$ elementos é o corpo de decomposição do polinômio $X^q - X$. A seguinte proposição mostra que, para toda potência prima q, existe um, e apenas um (salvo isomorfismos), corpo finito com q elementos.

Proposição 1.7 *Se F_q é um corpo de $q = p^f$ elementos, então cada elemento satisfaz a equação $X^q - X = 0$, e F_q é precisamente o conjunto das raízes dessa equação. Reciprocamente, para cada potência prima $q = p^f$ o corpo de decomposição sobre F_p do polinômio $X^q - X$ é um corpo de q elementos.*

Prova. Primeiro suponha que F_q é um corpo finito. Já que a ordem de qualquer elemento diferente de zero divide $q-1$, segue-se que qualquer elemento diferente de zero satisfaz a equação $X^{q-1} = 1$, e, portanto, multiplicando ambos os lados por X, obtemos a equação $X^q = X$. É claro que, o elemento 0 também satisfaz esta última equação. Assim, todos os q elementos de F_q são as raízes do polinômio de grau q, $X^q - X$. Já que este polinômio não pode ter mais de q raízes, suas raízes são precisamente os elementos de F_q. Note-se que isto significa que F_q é o corpo de decomposição do polinômio $X^q - X$, isto é, a menor extensão do corpo de F_p que contém todas as suas raízes.

Reciprocamente, seja $q = p^f$ uma potência primária, e seja F o corpo de decomposição sobre F_p do polinômio $X^q - X$. Note que $X^q - X$ tem derivada $qX^{q-1} - 1 = -1$ (isso segue de q ser um múltiplo de p, sendo nulo em F_p); Por isso, o polinômio $X^q - X$ não tem raízes em comum com a sua derivada (que não tem nenhuma raiz), e, portanto, não tem raízes múltiplas. Assim, F deve conter, pelo menos, as q raízes distintas de $X^q - X$. Mas reivindicamos que o conjunto das q raízes já é um corpo. O ponto-chave é que uma soma ou produto de duas raízes é novamente uma raiz. Ou seja, se a e b satisfazem o polinômio, temos $a^q = a$, $b^q = b$, e, portanto, $(ab)^q = ab$, isto é, o produto é também uma raiz. Para ver que a soma $a+b$ também satisfaz o polinômio $X^q - X$, podemos constatar um fato fundamental sobre qualquer corpo de característica p:

Lema 1.8 $(a-b)^p = a^p + b^p$ *em qualquer corpo de característica p.*

Aplicando repetidamente este lema temos: $a^p + b^p = (a+b)^p, a^{p^2} + b^{p^2} = (a^p + b^p)^p = (a+b)^{p^2}, \ldots, a^q + b^q = (a+b)^q$. Assim, se $a^q = a$ e $b^q = b$ temos então que $(a+b)^q = a+b$, e portanto $a+b$ também é raiz de $X^q - X$. Concluímos que o conjunto das q raízes é o menor corpo contendo as raízes de $X^q - X$, ou seja, o corpo de decomposição deste polinômio é um corpo de q elementos. □

Na prova acima vimos que elevar a potências p-ésimas preserva adição e multiplicação. Derivamos outra importante consequência deste fato na seguinte proposição:

Proposição 1.9 *Seja F_q o corpo finito de $q = p^f$ elementos, e seja σ a aplicação que leva todos os elementos a sua p-ésima potência: $\sigma(a) = a^p$. Então, σ é um automorfismo do corpo F_q. Os elementos de F_q, que são mantidos fixos por σ são precisamente os elementos do corpo primo F_p. A potência f-ésima (e nenhuma potência inferior) da aplicação σ é a aplicação identidade.*

Prova. Uma aplicação que eleva a uma potência sempre preserva multiplicação. O fato de que σ preserva adição vem do Lema 1.8. Nota-se que para qualquer j, a potência j-ésima de σ (o resultado de repetir σ, j vezes) é a aplicação $a \mapsto a^{p^j}$. Assim, os elementos à esquerda fixados por σ^i são as raízes de $X^{p^j} - X$. Se $j = 1$, estes são precisamente os p elementos do corpo primo (este é o caso especial $q = p$ da Proposição 1.7, ou seja, o Pequeno Teorema de Fermat). Os elementos à esquerda fixados por σ^f são as raízes de $X^q - X$, isto é, todo o F_q. Já que a potência f-ésima de σ é a aplicação identidade, σ deve ser 1-1 (sua aplicação inversa é $\sigma^{f-1} : a \mapsto a^{p^{f-1}}$). Nenhuma potência inferior de σ dá a aplicação identidade, já que para $j < f$ nem todos os elementos de F_q podem ser raízes do polinômio $X^{p^j} - X$. □

Proposição 1.10 *Na notação da Proposição 1.9, se α é qualquer elemento de F_q, então, os conjugados de α sobre F_p são os elementos $\sigma^j(\alpha) = \alpha^{p^j}$.*

Prova. Seja d o grau de $F_p(\alpha)$ como extensão de F_p. Ou seja, $F_p(\alpha)$ é uma cópia de F_{p^d}. Então α satisfaz $X^{p^d} - X$ mas não satisfaz $X^{p^j} - X$ para $j < d$. Assim, obtemos d elementos diferentes aplicando varias vezes σ a α. Agora basta provar que cada um desses elementos satisfaz o mesmo polinômio mônico irredutível $f(X)$ que α, caso no qual devem ser as d raízes. Para isto, basta provar que, se α satisfaz um polinômio $f(X) \in F_p[X]$, então α^p também. Seja $f(X) = \sum a_j X^j$, onde $a_j \in F_p$. Então $0 = f(\alpha) = \sum a_j \alpha^j$. Elevando ambos lados à p-ésima potência obtemos pelo Lema 1.8 que, $0 = \sum (a_j \alpha^j)^p$. Mas $a_j^p = a_j$ pelo Pequeno Teorema de Fermat, e portanto temos $0 = \sum a_j (\alpha^p)^j = f(\alpha^p)$, como queríamos. □

Até agora, nossa discussão sobre corpos finitos tem sido bastante teórica. A nossa única experiência tem sido com os corpos finitos da forma $F_p = \mathbb{Z}/p\mathbb{Z}$. Vamos agora discutir como trabalhar com extensões finitas de F_p. Neste ponto, devemos lembrar como, no caso dos números racionais $\mathbb{Q}$, trabalhamos com uma extensão $\mathbb{Q}(\sqrt{2})$. Ou seja, obtemos este corpo, tomando uma raiz α da equação $X^2 - 2$ e olhando para expressões da forma $a + b\alpha$, que são adicionadas e multiplicadas da maneira usual, exceto que α^2

deve sempre ser substituído por 2. (no caso de $\mathbb{Q}(\sqrt[3]{2})$ trabalhamos com expressões da forma $a+b\alpha+c\alpha^2$, e, quando multiplicamos sempre substituímos α^3 por 2). Podemos ter a mesma abordagem geral, com corpos finitos.

Exemplo 1.11 *Para construir F_9, tomamos qualquer polinômio quadrático mônico em $F_3[X]$, que não tem raízes em F_3. Ao tentar todas as opções possíveis de coeficientes e testar se os elementos $0,\pm 1 \in F_3$ são raízes, descobrimos que há três quadráticos mônicos irredutíveis : $X^2+1, X^2\pm X-1$. Se, por exemplo, vamos tomar α uma raiz de X^2-1 (vamos chamá-la i em vez de α — ao afinal, estamos simplesmente adjuntando uma raiz quadrada de -1), então, os elementos de F_9 são todas as combinações $a+bi$, onde a e b são 0, 1, ou -1. Fazer aritmética em F_9 é, portanto, muito parecido como fazer aritmética nos inteiros de Gauss, exceto que a nossa aritmética com os coeficientes a e b ocorre no pequeno corpo F_3.*

Nota-se que o elemento i, que adjuntamos, não é um gerador de F_9^*, já que tem ordem 4 em vez de $q-1=8$. Se, no entanto, adjuntamos uma raiz α de X^2-X-1, podemos obter todos os elementos diferentes de zero de F_9, tomando as potências sucessivas de α (lembrando que α^2 deve ser sempre substituído por $\alpha+1$, já que α satisfaz $X^2=X+1$): $\alpha^1=\alpha$, $\alpha^2=\alpha+1$, $\alpha^3=-\alpha$, $\alpha^4=-1$, $\alpha^5=-\alpha$, $\alpha^6=-\alpha-1$, $\alpha^7=\alpha-1$, $\alpha^8=1$. Às vezes, dizemos que o polinômio X^2-X-1 é primitivo, o que significa que qualquer raiz do polinômio irredutível é um gerador do grupo de elementos não nulos do corpo. Existem $4=\varphi(8)$ geradores de F_9^*, pela Proposição 1.5: duas são as raízes de X^2-X-1 e duas são as raízes de X^2+X-1. (A segunda raiz de X^2-X-1 é o conjugado de α, ou seja, $\sigma(\alpha)=\alpha^3=-\alpha+1$). Dos quatro elementos restantes diferentes de zero, dois são as raízes de X^2+1 (ou seja, $\pm i=\pm(\alpha+1)$) e os outros dois são os dois elementos diferentes de zero ± 1 de F_3 (que são raízes dos polinômios mônicos irredutíveis de grau 1, $X-1$ e $X+1$).

No exemplo acima, podemos ver que o grau dos polinômios considerados divide o grau da extensão F_9 sobre o corpo primo F_3. Em geral, temos a seguinte proposição.

Proposição 1.12 *Os subcorpos de F_{p^f} são os F_{p^d} para os quais d divide f. Se algum elemento de F_{p^f} é adjuntado a F_p, obtemos um desses corpos.*

Prova. Seja F_q um corpo finito qualquer, com $q=p^f$, cada elemento α de F_q satisfaz um polinômio mônico irredutível único sobre F_p de algum grau d. Então, o corpo $F_p(\alpha)$ obtido adjuntando este elemento ao corpo primo é uma extensão de grau d que está contida em F_q. Ou seja, é uma cópia do corpo F_{p^d}. Já que o grande corpo F_q contém F_{p^d}, é por isso um F_{p^d}-espaço vetorial de alguma dimensão f', segue-se que o número de elementos em F_{p^f} deve ser $(p^d)^{f'}$, isto é, $f=df'$. Assim, $d|f$.

Reciprocamente, para qualquer $d|f$ (ou seja $f = dd'$) o corpo finito F_{p^d} está contido em F_q, porque qualquer solução de $X^{p^d} = X$ também é uma solução de $X^{p^f} = X$. Para ver isto, note que para d', se substituir repetidamente X por X^{p^d} à esquerda na equação $X^{p^d} = X$, obtemos $X^{p^{dd'}} = X$. □

Vamos agora mostrar uma fórmula muito útil na hora de determinar o número de polinômios mônicos irredutíveis de um certo grau.

Proposição 1.13 *Para qualquer $q = p^f$ o polinômio $X^q - X$ se fatora em $F_p[X]$ como o produto de todos os polinômios mônicos irredutíveis de grau $d|f$.*

Prova. Se adjuntamos a F_p a raiz α de qualquer polinômio mônico irredutível de grau $d|f$, obtemos uma cópia de F_{p^d}, que está contida em F_{p^f}. Já que α satisfaz $X^q - X = 0$, o mônico irredutível deve dividir esse polinômio.

Reciprocamente, seja $f(X)$ um polinômio mônico irredutível que divide $X^q - X$. Então $f(X)$ deve ter suas raízes em F_q (já que é onde todas as raízes de $X^q - X$ estão). Assim, $f(X)$ deve ter grau de dividindo f, pela Proposição 1.12, já que adjuntando uma raiz dá um subcorpo de F_q. Assim, os polinômios mônicos irredutíveis que dividem $X^q - X$ são precisamente todos os de grau dividindo f. Já vimos que $X^q - X$ não tem múltiplos fatores, isso significa que $X^q - X$ é igual ao produto de todos esses polinômios irredutíveis. □

Corolário 1.14 *Se f é um número primo, então existem $(p^f - p)/f$ polinômios mônicos irredutíveis diferentes, de grau f em $F_p[X]$.*

Prova. Note primeiro que $(p^f - p)/f$ é um número inteiro pois pelo Pequeno teorema de Fermat, para o primo f temos que $p^f \equiv p \pmod{f}$. Seja n o número de polinômios mônicos irredutíveis de grau f. Pela proposição acima, o polinômio de grau p^f, $X^{p^f} - X$ é o produto de n polinômios de grau f e os p polinômios irredutíveis de grau 1, $X - a$ para $a \in F_p$. Assim, igualando graus temos: $p^f = nf + f$. □

De modo mais geral, suponha que f não é necessariamente primo. Então, seja n_d o número de polinômios mônicos irredutíveis de grau d sobre F_p. Temos que $n_f = (p^f - \sum dn_d)/f$, onde o somatório é sobre todos $d < f$ que dividem f.

1.2 Resíduos Quadráticos e Reciprocidade

Definição 1.15 *Seja F_q um corpo finto de q elementos. As soluções da equação $x^n = 1$, com n inteiro positivo são chamada de raízes n-ésimas da unidade. Dizemos que uma*

solução da equação acima é uma raiz n-ésima primitiva da unidade, se as suas potências percorrem todas as raízes n-ésimas da unidade.

Em várias situações, é muito útil fazermos a seguinte pergunta: quantas raízes n-ésimas da unidade existem em F_q? A seguinte proposição nos dá uma resposta.

Proposição 1.16 *Seja g um gerador de F_q^*. Então g^j é uma raiz n-ésima da unidade se, e somente se, $nj \equiv 0 \pmod{q-1}$. O número de raízes n-ésimas da unidade é $m.d.c.(n,q-1)$. Em particular, F_q tem uma raiz n-ésima primitiva da unidade se, e somete se, $n|q-1$. Se ξ é uma raiz n-ésima primitiva da unidade, então ξ^j é também uma raiz n-ésima primitiva se, e somente se, $m.d.c.(j,n) = 1$.*

Prova. Qualquer elemento de F_q pode-se escrever como uma potência g^j do gerador g. Note que uma potência de g dá 1 se e somente se seu exponente é divisível por $q-1$. Assim, um elemento g^j é raiz n-ésima da unidade se e somente se $nj \equiv 0 \pmod{q-1}$.

Seja agora $d = m.d.c.(n,q-1)$, e seja j desconhecido. Note que a equação $nj \equiv 0 \pmod{q-1}$ é equivalente á $\frac{n}{d}j \equiv 0 \pmod{\frac{q-1}{d}}$. Já que n/d é coprimo a $(q-1)/d$, a última congruência é equivalente a requerer que j seja um múltiplo de $(q-1)/d$. Ou seja, com $j = (q-1)/d$ podemos obter d potências distintas de $g^{(q-1)/d}$, as quais são precisamente as raízes n-ésimas da unidade.

Observe que, existem exatamente n dessas tais raízes se e somente se $d = n$, ou seja, se e somente se $n|q-1$. Logo $\xi = g^{(q-1)/n}$ é raiz primitiva.

Finalmente, se $n|q-1$, seja $\xi = g^{(q-1)/n}$. Então $\xi^j = 1$ se e somente se $n|j$. A k-ésima potência de ξ^j é igual a 1 se e somente se $kj \equiv 0 \pmod{n}$. Note que ξ^j tem ordem n se e somente se $m.d.c.(j,n) = 1$. De fato, suponha que a ordem de ξ^j é n e que $m.d.c.(j,n) \neq 1$. Seja $m.d.c.(j,n) = d$, logo existem $k_1, k_2 \in \mathbb{Z}$ tais que $j = dk_1$ e $n = dk_2$, temos assim $\xi^j = \xi^{dk_1}$ o que implica $\xi^{jk_2} = \xi^{dk_1k_2} = (\xi^{dk_2})^{k_1} = (\xi^n)^{k_1} = 1$, ou seja, $(\xi^j)^{k_2} = 1$ o qual não é possível pois $k_2 < n$. Reciprocamente, suponha que $m.d.c.(j,n) = 1$ e seja $k < n$ a ordem de ξ^j. Logo $(\xi^j)^k = 1$ implica que $jk \equiv 0 \pmod{n}$, então $n|kj$, e por hipótese temos $n|k$ o qual é impossível. Note assim que, existem $\varphi(n)$ raízes n-ésimas primitivas da unidade se $n|q-1$. □

Corolário 1.17 *Se $m.d.c.(n,q-1) = 1$, então 1 é a única raiz n-ésima da unidade.*

Corolário 1.18 *O elemento $-1 \in F_q$ tem uma raiz quadrada em F_q se e somente se $q \equiv 1 \pmod{4}$.*

O Corolário 1.18 diz que se $q \equiv 3 \pmod{4}$, sempre podemos obter uma extensão quadrática F_{q^2} adjuntando uma raiz de X^2+1, ou seja, considerando expressões do tipo $a+bi$.

1.2.1 Resíduos Quadráticos

Definição 1.19 *Sejam p um número primo maior do que 1 e $a \in \mathbb{Z}$. Se $x^2 \equiv a \pmod{p}$ possui solução, dizemos que a é um resíduo quadrático módulo p. Caso contrário, dizemos que a é um resíduo não quadrático módulo p.*

Exemplo 1.20 *Os quadrados em F_{11} são obtidos da seguinte forma: $1^2 = 1,\ 2^2 = 4,$ $3^2 = 9,\ 4^2 = 5,\ 5^2 = 3$. Assim, os quadrados de F_{11} são $1,4,9,5,3$. Note que, se continuamos essas contas, obtemos $6^2 = 3,\ 7^2 = 5,\ 8^2 = 9,\ 9^2 = 4,\ 10^2 = 1$, donde só precisamos fazer as contas de 1 até $(11-1)/2$. Além disso, temos que os elementos que não estão na primeira conta, são precisamente os resíduos não quadráticos, ou seja, $2,6,7,8,10$. Temos assim o seguinte teorema.*

Teorema 1.21 *Seja $p > 2$. Existem $(p-1)/2$ resíduos quadráticos, e $(p-1)/2$ resíduos não quadráticos em F_p. Mais ainda, $1^2,\ 2^2,\ \ldots, ((p-1)/2)^2$ formam um conjunto completo de resíduos quadráticos.*

Lema 1.22 *Seja g um gerador de F_p. Então, $a \in F_p$ é um quadrado se, e somente se, $a = g^j$, com j par. Note que $a = g^j$, com j par, é o quadrado de $\pm g^{j/2}$.*

Definição 1.23 *Sejam a um inteiro e $p > 2$ um primo. Definimos o símbolo de Legendre $\left(\frac{a}{p}\right)$ como sege:*

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

O símbolo de Legendre é uma maneira simples de identificar quando um inteiro é, ou não, um resíduo quadrático módulo p.

Proposição 1.24 ***(Critério de Euler).***

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

Prova. Se $p|a$, então ambos lados são $\equiv 0 \pmod{p}$. Suponha que $p \nmid a$. Se $\left(\frac{a}{p}\right) = 1$ então $x^2 \equiv a \pmod{p}$ tem solução, logo temos que

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Seja $\left(\frac{a}{p}\right) = -1$. Note que a equação $y^{(p-1)/2} \equiv 1 \pmod{p}$ tem no máximo $(p-1)/2$ soluções. Mas pelo Teorema 1.21 os $(p-1)/2$ resíduos quadráticos satisfazem essa

equação. Logo como a é um resíduo não quadrático então $p \nmid a^{(p-1)/2} - 1$. Por outra parte, pelo Pequeno Teorema de Fermat temos que

$$p|a^{p-1} - 1 = \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right),$$

isso implica $p|a^{(p-1)/2} + 1$, ou seja, $a^{(p-1)/2} \equiv -1 \pmod{p}$. □

Proposição 1.25 *O símbolo de Legendre satisfaz as seguintes propriedades*

1. $\left(\frac{a}{p}\right)$ *depende somente do resíduo de a módulo p;*
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
3. *Para b coprimo a p, temos que* $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;
4. $\left(\frac{1}{p}\right) = 1$ *e* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Prova. A prova decorre imediatamente da definição e a Proposição 1.24. □

Note que o item *4.* indica que -1 é um resíduo quadrático ou não, segundo $p \equiv 1$ ou $3 \pmod 4$. Por outro lado, se podermos decompor a em seus fatores primos da seguinte forma $a = \pm 2^m \cdot q_1^{\alpha_1} \cdots q_n^{\alpha_n}$, onde $2 < q_1 < \cdots < q_n$, então o item *2.* implica

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m \left(\frac{q_1}{p}\right)^{\alpha_1} \cdots \left(\frac{q_n}{p}\right)^{\alpha_n},$$

logo, a avaliação do símbolo de Legendre se reduz à avaliação de

$$\left(\frac{-1}{p}\right), \ \left(\frac{2}{p}\right), \ \left(\frac{q}{p}\right),$$

onde q é um primo ímpar. O primeiro símbolo já foi calculado na parte *4.* da Proposição 1.25, os outros dois casos serão estudados no *Lema de Gauss* e na *Lei de Reciprocidade Quadrática*.

Teorema 1.26 ***(Lema de Gauss).*** *Seja $p > 2$, $p \nmid a$. Denote por m o número de elementos dos $(p-1)/2$ números $a, 2a, \ldots, \frac{p-1}{2}a$ que deixam resto maior que $p/2$ na divisão por p. Então*

$$\left(\frac{a}{p}\right) = (-1)^m.$$

Exemplo 1.27 *sejam $p = 11$ e $a = 2$. Temos os resíduos $2, 4, 6, 8, 10 \pmod{11}$, e só três excedem $11/2$, ou seja $m = 3$ e assim $\left(\frac{2}{11}\right) = (-1)^3 = -1$.*

Proposição 1.28 *Se $p > 2$ então*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 8; \\ -1, & \text{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

Prova. Considere $a = 2$ no Teorema 1.26, então a lista de números $2,\ 2\cdot 2,\ 3\cdot 2, \cdots, \frac{p-1}{2}\cdot 2$, estão todos no intervalo de 0 a p. Podemos agora determinar o número de inteiros que satisfazem $\frac{p}{2} < 2k < p$, ou equivalentemente $\frac{p}{4} < k < \frac{p}{2}$. Seja m a quantidade desses tais números, logo note que

$$m = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right].$$

Seja $p = 8n + r$, como p é primo ímpar podemos considerar os casos seguintes, $r = 1,3,5,7$. Analisemos a paridade de m:

$$m = 2n + \left[\frac{r}{2}\right] - \left[\frac{r}{4}\right] \equiv 0,1,1,0 \pmod 2.$$

Logo m é par se $p \equiv 1$ ou $7 \pmod 8$ ou m é ímpar se $p \equiv 3$ ou $5 \pmod 8$, e portanto

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 8 \\ -1, & \text{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

Para finalizar, analisemos a paridade de $(p^2-1)/8$. Considerando os respectivos casos para p acima temos: se $p \equiv 1 \pmod 8$, então $p+1 \equiv 2 \pmod 8$ e $p-1 \equiv 0 \pmod 8$, logo

$$\frac{p^2-1}{8} = \frac{(p+1)(p-1)}{8} = \frac{(8a+2)(8b)}{8} = 2(4a+1)b,$$

que é par. Assim por diante, obtemos

$$\frac{p^2-1}{8} = \begin{cases} \text{Par}, & \text{se } p \equiv \pm 1 \pmod 8 \\ \text{ímpar}, & \text{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

Isso conclui a prova. □

O último símbolo de Legendre, do tipo $\left(\frac{q}{p}\right)$, é facilmente calculado pela *Lei de Reciprocidade Quadrática*, com o auxílio do item *1.* da Proposição 1.25, assumindo que os fatores primos de a são menores do que p. Em outras palavras, a seguinte proposição nos diz como relacionar $\left(\frac{q}{p}\right)$ com $\left(\frac{p}{q}\right)$, de modo que este último símbolo seja mais fácil de avaliar, já que podemos imediatamente substituir p por seu resíduo módulo q.

Proposição 1.29 ***(Lei de Reciprocidade Quadrática).*** *Sejam p e q dois primos ímpares.*

Então

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right).$$

A Lei de Reciprocidade Quadrática estabelece que $\left(\frac{q}{p}\right)$ e $\left(\frac{p}{q}\right)$ são os mesmos, a menos que p e q sejam ambos $\equiv 3 \pmod 4$, caso no qual eles terão sinais opostos.

Exemplo 1.30 *Vamos determinar os primos $p \neq 5$ para os quais 5 é um resíduo quadrático. Note que, da Lei de reciprocidade quadrática obtemos imediatamente $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, e considerando os respectivos casos para $p \pmod 5$ temos:*

$$\left(\frac{1}{5}\right) = 1,\ \left(\frac{2}{5}\right) = (-1)^{(5^2-1)/8} = -1,\ \left(\frac{3}{5}\right) = \left(\frac{-2}{5}\right) = -1,\ \left(\frac{4}{5}\right) = 1,$$

portanto

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 5; \\ -1, & \text{se } p \equiv \pm 2 \pmod 5. \end{cases}$$

1.2.2 Símbolo de Jacobi

Uma dificuldade do método visto, para avaliar os símbolos de Legendre, é que em cada fase, deve-se fatorar o número de cima, a fim de aplicar a Proposição 1.29. Se os nossos números são muito grandes, isso pode ser muito demorado. Felizmente, é possível evitar a necessidade de fatorar (exceto tirando potências de 2, o que é muito fácil), fazendo uma generalização da lei da reciprocidade quadrática e da Proposição 1.28, que se aplicam a todos os inteiros ímpares positivos, não necessariamente primos. Mas primeiro precisamos de uma definição que generaliza a definição do símbolo de Legendre.

Definição 1.31 *Sejam a um inteiro, e n qualquer número ímpar positivo. Seja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ a fatoração prima de n. Então definimos o símbolo de Jacobi $\left(\frac{a}{n}\right)$ como o produto dos símbolos de Legendre para os factores primos de n:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Note que devemos ter cuidado na hora de avaliar o simbolo de Jacobi, pois se $\left(\frac{a}{n}\right) = 1$ para n composto, não necessariamente é verdade que a seja um quadrado módulo n. Por exemplo, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, mas não existe nenhum inteiro tal que $x^2 \equiv 2 \pmod{15}$.

Proposição 1.32 *Para qualquer inteiro positivo ímpar n, temos*

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

Proposição 1.33 *Para quaisquer dois inteiros ímpares m e n temos que*

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right).$$

Os conceitos discutidos nesta seção, tais como: Resíduos Quadráticos, Símbolo de Legendre, Reciprocidade Quadrática e suas generalizações, são aplicados em um tipo de sistema de criptografia probabilístico desenvolvido por Shafi Goldwasser e Silvio Micali no início dos anos 80; este foi o primeiro sistema de chave pública probabilística que é comprovadamente seguro sob os pressupostos de criptografia padrão (Ver [7],[8]). No próximo capítulo vamos formalizar os conceitos necessários para desenvolver o nosso estudo de sistemas criptográficos.

CAPÍTULO 2

Criptografia

CAPÍTULO 3

Criptografia

A palavra **criptografia** vem da união dos termos gregos κρυπτω, kripto (oculto) e γραφως, graphos (escrever), e seu significado é: "escrita oculta". As origens da criptografia datam milhares de anos para trás na história, sabe-se que os primeiros a usar um método de comunicação secreta eram os antigos habitantes de Esparta, no entanto, geralmente uma figura histórica está associada com as origens da criptografia: Júlio César. Criptografia é o estudo de métodos de envio de mensagens em forma "disfarçada" de modo que somente os destinatários poderão remover o disfarce e ler a mensagem.

Neste capítulo serão estudados os conceitos de: sistemas criptográficos, indo desde alguns sistemas muito simples até outros mais complexos, fazendo particular enfase nos sistemas de chave publica, em particular o sistema RSA. Finalmente fazemos uma pequena descrição dos sistemas de troca de chaves Diffie-Hellman, Massey-Omura, ElGamal, e Assinatura Digital Padrão; os quais serão utilizados mais adiante quando discutirmos os sistemas criptográficos de curvas elípticas.

3.1 Sistemas de Criptografia

Definição 3.1 *Um sistema de criptografia é uma quíntupla* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, onde:*

- $\mathcal{P}$ *representa o conjunto de mensagens sem cifrar denominado* ***texto original****, que podem ser enviados.*
- $\mathcal{C}$ *representa o conjunto de todas as possíveis mensagens cifrados, denominados* ***texto cifrado****.*
- $\mathcal{K}$ *representa o conjunto de* ***chaves de encriptação*** *que podem ser usadas no sistema.*
- $\mathcal{E}$ *é o conjunto de* ***transformações de cifragem*** *ou família de funções que se aplicam a cada elemento de* $\mathcal{P}$ *para obter um elemento de* $\mathcal{C}$*.*
- $\mathcal{D}$ *é o conjunto de* ***transformações de decifração****, análogo a* $\mathcal{E}$*.*

Tais que, para cada $k \in \mathcal{K}$ existe uma função de cifrar $f_k \in \mathcal{E}$ e sua função correspondente de decifração que notamos por $f_k^{-1} \in \mathcal{D}$:

$$\mathcal{P} \xrightarrow{f_k} \mathcal{C} \xrightarrow{f_k^{-1}} \mathcal{P},$$

que verificam a propriedade: $f_k^{-1}(f_k(x)) = x$, para todo $x \in \mathcal{P}$, ou seja, f_k é uma aplicação injetora.

O texto original e o texto cifrado são escritos em algum alfabeto (geralmente, mas nem sempre são escritos no mesmo alfabeto), constituído por um certo número N de letras. O termo "letra" (ou "caractere") pode referir-se não só para o alfabeto familiar A,B,...,Z, mas também para os números, espaços, sinais de pontuação, ou quaisquer outros símbolos que permitimos usar ao escrever as mensagens. O processo de conversão de um texto original a um texto cifrado é chamado de *cifragem* ou *encriptação*, e o processo inverso é chamado de *decifração* ou *decodificação*. O texto original e o texto cifrado são divididos em *unidades de mensagens*. A unidade de mensagem pode ser uma única letra, um par de letras (dígrafo), um triplo de letras (trígrafo), ou um bloco de 50 letras.

O primeiro passo para inventar um sistema de criptografia é "etiquetar" todas as possíveis unidades de mensagens de texto original e todas as possíveis unidades de mensagem de texto cifrado, por meio de objetos matemáticos a partir do qual as funções podem ser facilmente construídas. Esses objetos são muitas vezes simplesmente os números inteiros em algum intervalo. Por exemplo, se nossas unidades de texto original e mensagens de texto cifrado são 26 letras do alfabeto A,B,...,Z, então podemos etiquetar as letras usando os números inteiros 0, 1, 2, ..., 25, que chamamos de seus "equivalentes numéricos":

A	B	C	$\cdots$	Z
$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$
0	1	2	$\cdots$	25

Tabela 3.1: *"Etiquetado" do alfabeto.*

3.1.1 Exemplos

Vamos começar com o primeiro caso quando se toma uma unidade de mensagem (de texto original ou de texto cifrado) a ser uma única letra em um alfabeto de N letras marcado pelos números inteiros $0, 1, 2, \ldots, N-1$. Então, por definição, uma transformação cifragem é uma permutação destes N inteiros.

No segundo caso iremos estudar quando tomarmos unidades de texto como sendo blocos de duas letras ou dígrafos.

Unidades de Mensagem de uma Única Letra

Para facilitar a rápida cifragem e decifração, é conveniente ter uma regra relativamente simples para a realização de tal permutação. Uma maneira é pensar no conjunto de inteiros $\{0,1,\ldots,N-1\}$ como $\mathbb{Z}/N\mathbb{Z}$, e fazer uso das operações de adição e multiplicação módulo N.

Exemplo 3.2 ***(Cifrado de César)***. *Suponha que estamos usando as 26 letras do alfabeto de A,B,...,Z com os equivalentes numéricos 0,...,25 como na Tabela 3.1. Seja a letra* $P \in \{0,1,..,25\}$ *uma unidade de mensagem de texto original. Defina uma função* f *do conjunto* $\{0,1,...,25\}$ *em si mesmo pela regra*

$$f(P) = \begin{cases} P+3, & \text{se } P < 23, \\ P-23, & \text{se } P \geq 23. \end{cases}$$

Portanto, f *simplesmente adiciona 3 módulo 26:* $f(P) \equiv P+3 \pmod{26}$. *Note que a definição usando a aritmética modular é mais fácil de escrever e trabalhar com ela.*

Assim, com este sistema, para cifrar a palavra "SIM", primeiro convertemos em números:24 4 18, em seguida, adicione 3 módulo 26: 1 7 21, logo levamos de volta para letras: "BHV". Para decifrar uma mensagem, subtraímos 3 módulo 26. Por exemplo, o texto cifrado "UXD" produz um texto original "RUA". Em outras palavras, o que faz o cifrado de César é um simples deslocamento de três unidades no alfabeto:

A	B	C	D	$\cdots$	X	Y	Z
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$
D	E	F	G	$\cdots$	A	B	C

Tabela 3.2: *Cifrado de César.*

Este sistema de criptografia foi aparentemente usado na Roma antiga por Júlio César, quem supostamente o inventou, e pode ser generalizado como se segue. Suponha que estamos usando um alfabeto de N letras com os equivalentes numéricos $0,1,2,\ldots,N-1$. Seja b um inteiro fixo. Por uma **transformação deslocamento** entendemos a função de cifragem f definida pela regra $C = f(P) \equiv P+b \pmod{N}$. O sistema de criptografia de Júlio César foi o caso $N = 26$, $b = 3$. Para decifrar uma unidade de mensagem cifrado $C \in \{0,1,...,N-1\}$, simplesmente calculamos $P = f^{-1}(C) \equiv C-b \pmod{N}$.

No exemplo acima podemos identificar os conjuntos referentes à Definição 3.1 como sendo:

- $\mathcal{P} = \mathcal{C} = \{0,1,2,\ldots,25\}$,
- $\mathcal{K} = \{0,1,\ldots,25\}$,

- $\mathcal{E} = \{f_k : \mathcal{P} \to \mathcal{P} \ : f_k(P) \equiv P + k \pmod{N}, k \in \mathcal{K}\}$,
- $\mathcal{D} = \{f_k^{-1} : \mathcal{P} \to \mathcal{P} \ : f_k^{-1}(C) \equiv C - k \pmod{N}, k \in \mathcal{K}\}$.

Note que um sistema como este é muito fácil de quebrar, pois só temos que procurar a chave adequada k, que é muito simples pois só temos 26 opções para escolher. Assim, depois de umas quantas tentativas para decifrar uma mensagem, obteremos uma que faz sentido. Sistemas de criptografia mais complicadas, têm geralmente várias chaves, como no seguinte exemplo.

Exemplo 3.3 ***(Transformação afim).*** *Considere a e b números inteiros fixos e defina a transformação $C = f(P) \equiv aP + b \pmod{N}$, aqui o par (a,b) forma a chave de encriptação. Por exemplo, trabalhando novamente no alfabeto de 26 letras, se quisermos cifrar o mensagem "COLÔMBIA" usando a transformação afim com $a = 7$, $b = 12$, obtemos:* $2\ 14\ 11\ 14\ 12\ 1\ 8\ 0 \longmapsto 0\ 6\ 11\ 6\ 18\ 19\ 16\ 12 =$ *"AGLGSTQM". Para decifrar uma mensagem que foi cifrada por meio desta transformação afim, $C \equiv 7P + 12 \pmod{26}$, usamos a transformação $P \equiv 15C + 16 \pmod{26}$. Note que aqui $15 = 7^{-1} \pmod{26}$, e $16 = -7^{-1} \cdot 12 \pmod{26}$.*

Em resumo, um sistema de criptografia afim em um alfabeto de N letras com os parâmetros $a \in (\mathbb{Z}/N\mathbb{Z})^*$ e $b \in \mathbb{Z}/N\mathbb{Z}$ consiste das regras:

$$C \equiv aP + b \pmod{N}, \quad P \equiv a'C + b' \pmod{N},$$

onde

$$a' = a^{-1} \in (\mathbb{Z}/N\mathbb{Z})^*, \quad b' = -a^{-1}b.$$

No exemplo acima, temos que $a \in (\mathbb{Z}/26\mathbb{Z})^*$ e $b \in \mathbb{Z}/26\mathbb{Z}$, ou seja, $\mathcal{K} = (\mathbb{Z}/26\mathbb{Z})^* \times \mathbb{Z}/26\mathbb{Z}$. Além disso, como $|(\mathbb{Z}/26\mathbb{Z})^*| = \varphi(26) = 12$, então temos um total de $12 \cdot 26 = 312$ transformações afins.

Note que se $mdc(a,N) > 1$, então é fácil ver que mais de uma letra de texto original dará o mesmo texto cifrado, portanto, não se pode recuperar de forma única o texto original do cifrado. Por definição, esta não é uma transformação de cifragem: sempre exigimos que a transformação seja 1-1. isto é, que o texto original seja determinado univocamente a partir do texto cifrado.

Como um caso especial dos sistemas criptográficos afins podemos definir $a = 1$, obtendo-se assim as transformações deslocamento. Outro caso especial é quando $b = 0$: $C \equiv aP \pmod{N}$, $P \equiv a^{-1}C \pmod{N}$. O caso $b = 0$ é chamado uma *transformação linear*, o que significa que a transformação leva uma soma em uma soma, ou seja, se C_1 e C_2 são a encriptação de P_1 e P_2 respectivamente, então $C_1 + C_2$ é a encriptação de $P_1 + P_2$ (onde, é claro, estamos adicionando módulo N).

Transformações de Dígrafos

Vamos agora supor que nossas unidades de mensagens de texto original e encriptado são blocos de duas letras, chamados dígrafos. Isso significa que o texto original é dividido em segmentos duas letras. Se todo o texto original tem um número ímpar de letras, então a fim de se obter um número inteiro de dígrafos adicionamos uma letra extra no final; escolhemos uma letra que não é susceptível de causar confusão, como um branco se nosso alfabeto contém um espaço em branco, ou então "X" ou "Q" se estamos usando apenas as 26 letras do alfabeto.

A cada dígrafo é então atribuído um equivalente numérico. A maneira mais simples de fazer isso é tomar $xN + y$, onde x é o equivalente numérico da primeira letra no dígrafo, y é o equivalente numérico da segunda letra no dígrafo, e N é o número de letras no alfabeto. Equivalentemente, pensamos em um dígrafo como um inteiro de dois dígitos na base N . Isto dá uma correspondência 1-1 entre o conjunto de todos os dígrafos do alfabeto de N letras e o conjunto de todos os inteiros não-negativos menores que N^2.

Em seguida, decidimos sobre uma transformação de cifragem, isto é, uma permutação dos inteiros $\{0,1,2,...,N^2-1\}$. Entre as transformações de cifragem mais simples estão as afins, onde vemos este conjunto de inteiros como $\mathbb{Z}/N^2\mathbb{Z}$, e definimos a codificação de P como sendo um número inteiro não negativo C menor que N^2 satisfazendo a congruência $C \equiv aP + b \pmod{N^2}$. Aqui, como antes, a não deve ter nenhum fator comum com N (o que significa que não tem fator comum com N^2), a fim de termos uma transformação inversa dizendo-nos como decifrar: $P \equiv a'C + b' \pmod{N^2}$, onde $a' \equiv a^{-1} \pmod{N^2}$, $b' \equiv -a^{-1}b \pmod{N^2}$. Note que C é transformado num bloco de duas letras do texto cifrado, escrevendo-o na forma $C = x'N + y'$, e, em seguida, olhando para as letras como equivalentes numéricos x' e y'.

Exemplo 3.4 *Suponha que trabalhamos no alfabeto de 26 letras, usando a transformação de cifragem dígrafo* $C \equiv 159P + 580 \pmod{676}$. *Então, o dígrafo "NO" tem equivalente numérico* $13 \cdot 26 + 14 = 352$ *e é levado para o dígrafo cifrado* $159 \cdot 352 + 580 \equiv 440 \pmod{676}$, *que é "QY", pois* $440 = 16 \cdot 26 + 24$. *O dígrafo "ON" tem equivalente numérico 377, e é levado a 359 = "NV".*

Note que os dígrafos mudam como uma unidade, e não há nenhuma relação entre a encriptação de um dígrafo e a de outro que tem uma letra em comum com ele, ou mesmo que consiste das mesmas letras na ordem inversa.

Em geral, podemos etiquetar blocos de k letras em um N-alfabeto por números inteiros entre 0 e $N^k - 1$ por um inteiro de k dígitos na base N. Em algumas situações, pode-se querer rotular unidades de mensagens usando outros objetos matemáticos além inteiros, como por exemplo, vetores ou pontos em alguma curva.

3.1.2 Matrizes de Encriptação

Suponha que temos um alfabeto de N letras e queremos enviar dígrafos como nossas unidades de mensagens. Uma possível alternativa é deixar que cada dígrafo corresponda a um vetor, ou seja, a um par de inteiros $\begin{pmatrix} x \\ y \end{pmatrix}$ com x e y considerados módulo N. Por exemplo, se estamos usando as 26 letras do alfabeto de A,B,...,Z com equivalentes numéricas 0,1,...,25, respectivamente, então o dígrafo NO corresponde ao vector $\begin{pmatrix} 13 \\ 14 \end{pmatrix}$

Imaginemos cada dígrafo P como um ponto em uma matriz quadrada $N \times N$. Ou seja, temos um "plano-xy," exceto que cada eixo, em vez de ser uma cópia da reta dos números reais, é agora uma cópia de $\mathbb{Z}/N\mathbb{Z}$. Denotamos essa matriz $N \times N$ por $(\mathbb{Z}/N\mathbb{Z})^2$.

Uma vez que visualizamos os dígrafos como vetores (pontos no plano), então interpretamos uma "transformação de cifragem" como uma permutação de pontos da matriz $N \times N$. Mais precisamente, uma aplicação de cifragem é uma função 1-1 de $(\mathbb{Z}/N\mathbb{Z})^2$ em si mesmo.

Álgebra Linear Módulo N

Daremos uma breve descrição de como a Álgebra linear em $\mathbb{Z}/N\mathbb{Z}$ pode ser usada como uma ferramenta na hora de codificar mensagens. Estudos mais detalhados podem ser consultados em [15]. Na Subsecção 3.1.1, quando estávamos lidando com caracteres individuais e aplicações de cifragem de $\mathbb{Z}/N\mathbb{Z}$, descobrimos dois tipos de aplicações fáceis para trabalhar:

1. Aplicações "lineares" $C = aP$;
2. Aplicações "afins" $C = aP + b$,

onde a é inversível em $\mathbb{Z}/N\mathbb{Z}$. Temos uma situação similar quando nossa unidade de mensagem são dígrafos de vetores. Primeiro consideramos transformações lineares. A diferença, quando trabalhamos com $(\mathbb{Z}/N\mathbb{Z})^2$ em vez de $\mathbb{Z}/N\mathbb{Z}$, é que agora, em vez de um inteiro a precisamos de uma matriz 2×2, que vamos denotar por A, e de um vetor coluna 2×1 que denotamos por B. Vamos começar dando uma explicação sistemática do tipo de matrizes que precisamos.

Seja R qualquer anel comutativo. Denotamos por R^* o subconjunto de elementos invertíveis de R. Por exemplo, se $R = \mathbb{Z}/N\mathbb{Z}$ então $(\mathbb{Z}/N\mathbb{Z})^* = \{0 < j < N \ : \ mdc(j,N) = 1\}$.

Se R é um anel comutativo, denotamos por $M_2(R)$ o conjunto de todas as matrizes 2×2 com entradas em R, com a soma e multiplicação definidas de maneira usual para matrizes. Chamamos a $M_2(R)$ de o "anel de matrizes 2×2 sobre R"; $M_2(R)$ é de fato um anel, mas não é comutativo.

Suponha que $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$ e $D = det(A) = ad - bc \in R^*$. Seja D^{-1} o inverso multiplicativo de D em R. Então

$$\begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} D^{-1}(da-bc) & 0 \\ 0 & D^{-1}(-cb+ad) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

e obtemos o mesmo resultado se multiplicamos na ordem oposta. Assim, A tem uma matriz inversa dada pela fórmula análoga ao caso dos números reais :

$$A^{-1} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix}.$$

Exemplo 3.5 *Encontremos a inversa de* $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(\mathbb{Z}/26\mathbb{Z})$. *Aqui* $D = 2 \cdot 8 - 3 \cdot 7 = -5 = 21$ *em* $\mathbb{Z}/26\mathbb{Z}$, *Já que* $mdc(21,26) = 1$, *o determinante D tem inverso, a saber,* $21^{-1} = 5$. *Assim,*

$$A^{-1} = \begin{pmatrix} 5 \cdot 8 & -5 \cdot 3 \\ -5 \cdot 7 & 5 \cdot 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}.$$

Aqui, já que trabalhamos em $\mathbb{Z}/26\mathbb{Z}$, *usamos "=" o que significa que as entradas são congruentes módulo 26.*

Tal como no caso dos números reais, uma matriz 2×2

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

com entradas no anel R pode ser multiplicada por um vetor coluna $\begin{pmatrix} x \\ y \end{pmatrix}$ com $x, y \in R$ para obter um outro vetor $\begin{pmatrix} x' \\ y' \end{pmatrix}$:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

Isto dá uma "aplicação linear" de vetores em vetores, ou seja a combinação linear $\begin{pmatrix} k_1x_1 + k_2x_2 \\ k_1y_1 + k_2y_2 \end{pmatrix}$, onde k_1 e k_2 estão no anel R, é levada em $\begin{pmatrix} k_1x'_1 + k_2x'_2 \\ k_1y'_1 + k_2y'_2 \end{pmatrix}$. A única diferença com o caso real, é que tudo agora é no anel R.

Queremos aplicar tudo isto ao caso em que o nosso anel é $R = \mathbb{Z}/N\mathbb{Z}$. A seguinte proposição trata deste caso, embora a proposição análoga é válida para qualquer R.

Proposição 3.6 *Sejam* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z})$ *e* $D = ad - bc$. *As seguintes afirmações são equivalentes:*

a) $mdc(D,N) = 1$;

b) A tem matriz inversa;

c) Se x e y não são ambos zero em $\mathbb{Z}/N\mathbb{Z}$, *então* $A\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$;

d) A dá uma correspondência 1-1 de $(\mathbb{Z}/N\mathbb{Z})^2$ *com ele mesmo.*

Prova. Note que se $mdc(D,N) = 1$ então existe D^{-1} módulo N, e A^{-1} se define como acima, assim $a) \Rightarrow b)$.

Suponha que se tem $b)$, então a parte $d)$ tem-se também, pois A^{-1} dá a transformação inversa de $\begin{pmatrix} x' \\ y' \end{pmatrix}$ em $\begin{pmatrix} x \\ y \end{pmatrix}$. Assim A dá uma correspondência 1-1, logo $b) \Rightarrow d)$.

Se temos d) então $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ implica que $A\begin{pmatrix} x \\ y \end{pmatrix} \neq A\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, tem-se assim $c)$ e por tanto $d) \Rightarrow c)$.

Finalmente para mostrarmos $c) \Rightarrow a)$ vamos provar que se $a)$ é falso então $c)$ é falso. Então, suponha que $a)$ é falso, e sejam $m = mdc(D,N) > 1$ e $m' = N/m$. Considere os seguintes três casos.

i) Se as quatro entradas de A são divisíveis por m, seja $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} m' \\ m' \end{pmatrix}$, e note que $A\begin{pmatrix} m' \\ m' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, que é uma contradição com $c)$.

ii) Se a e b não são ambos divisíveis por m, considere $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -bm' \\ am' \end{pmatrix}$. Então

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -bm' \\ am' \end{pmatrix} = \begin{pmatrix} -abm' + bam' \\ -cbm' + dam' \end{pmatrix} = \begin{pmatrix} 0 \\ Dm' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

pois $m|D$ e assim $N = mm'|Dm'$.

iii) Se c e d não são ambos divisíveis por m, considere $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} dm' \\ -cm' \end{pmatrix}$, e proceda como no caso anterior.

Estes três casos são todas as possibilidades. Concluímos assim que, se $a)$ é falso então $c)$ é falso. □

Para retornar à criptografia, comecemos com as **transformações lineares** e notemos, a partir da Proposição 3.6, que podemos obter transformações de cifragem dos nossos vetores de dígrafos usando matrizes $A \in M_2(\mathbb{Z}/N\mathbb{Z})$, cujo determinante não tem nenhum fator comum com N:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad D = ad - bc, \qquad mdc(D,N) = 1.$$

Ou seja, cada unidade de texto original $P = \begin{pmatrix} x \\ y \end{pmatrix}$ é levada ao texto cifrado $C = \begin{pmatrix} x' \\ y' \end{pmatrix}$ pela regra:

$$C = AP, \qquad \text{isto é,} \qquad \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Para decifrar a mensagem, usamos simplesmente a matriz inversa:

$$P = A^{-1}AP = A^{-1}C, \qquad \text{isto é,} \qquad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Observação 3.7 *Para codificar uma sequência de texto original de k dígrafos $P = P_1P_2P_3\cdots P_k$, podemos escrever os k vetores como colunas de uma matriz $2 \times k$, que também denotamos por P, e depois multiplicar a matriz 2×2, A, pela matriz $2 \times k$, P, para obter uma matriz $2 \times k$, $C = AP$ de dígrafos de vetores codificados.*

Exemplo 3.8 *Trabalhando no alfabeto de 26 letras, usar a matriz A do Exemplo 3.5 para encriptar o texto original "BOANOITE".*

O equivalente numérico de "BOANOITE" é a sequência de vetores $\begin{pmatrix} 1 \\ 14 \end{pmatrix} \begin{pmatrix} 0 \\ 13 \end{pmatrix} \begin{pmatrix} 14 \\ 8 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix}$. *Temos assim,*

$$C = AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 1 & 0 & 14 & 19 \\ 14 & 13 & 8 & 4 \end{pmatrix} = \begin{pmatrix} 44 & 39 & 52 & 50 \\ 119 & 104 & 162 & 165 \end{pmatrix}$$
$$= \begin{pmatrix} 18 & 13 & 0 & 24 \\ 15 & 0 & 6 & 9 \end{pmatrix},$$

ou seja, a mensagem codificada é "SPNAAGYJ".

Uma maneira mais geral de encriptar um vetor dígrafo $P = \begin{pmatrix} x \\ y \end{pmatrix}$ é aplicar a matriz 2×2, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z})$, e logo somar um vetor constante $B = \begin{pmatrix} e \\ f \end{pmatrix}$, ou seja, usar uma **transformação afim:**

$$C = AP + B,$$

isto é,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} ax+by+e \\ cx+dy+f \end{pmatrix}.$$

Note de novo que, como antes, usamos "=" que significa que as entradas correspondentes são congruentes módulo N. A transformação inversa que expressa P em termos de C pode ser encontrada subtraindo B de ambos os lados e, em seguida, aplicar A^{-1} á esquerda em ambos os lados:

$$P = A^{-1}C - A^{-1}B.$$

Note que esta também é uma transformação afim $P = A'C + B'$, onde $A' = A^{-1}$ e $B' = -A^{-1}B$. Note que devemos supor que A é uma matriz invertível de modo a ser capaz de decifrar de forma única.

Observação 3.9 *Durante vários séculos um dos mais populares métodos de criptografia era o chamado "cifrado Vigenère," nomeado assim pelo francês B. de Vigenère, que em 1586 escreveu seu Traicté des Chiffres [37], descrevendo uma versão mais difícil deste sistema. Este sistema pode ser descrito como se segue. Para algum k fixo, considere blocos de k letras como vetores em $(\mathbb{Z}/N\mathbb{Z})^k$. Escolha algum vetor fixo b in $(\mathbb{Z}/N\mathbb{Z})^k$ (geralmente b é o vetor correspondente à "chave"), e cifre por meio do vector translação $C = P + b$ (onde a unidade de mensagem de texto cifrado C e a unidade de mensagem de texto original P são k-tuplas de inteiros módulo N). Este sistema de criptografia, infelizmente, é quase tão fácil de quebrar como o de uma única letra de translação. Em [36] também podemos encontrar uma descrição mais detalhada deste sistema.*

3.1.3 Sistemas Criptográficos Simétricos

Daremos uma breve descrição do que são os sistemas criptográficos simétricos, também conhecidos como *sistemas clássicos* ou *de chave privada*.

Definição 3.10 *Um sistema criptográfico simétrico é aquele que usa a mesma chave $k \in \mathcal{K}$ tanto para cifrar como para decifrar.*

Outra maneira de olhar para a definição destes tipos de sistemas, é como aqueles que, uma vez se conhece a informação de cifragem ou o texto cifrado, a transformação de decifração pode ser implementada aproximadamente na mesma ordem de grandeza do tempo que a transformação de cifragem. Uma definição mais precisa e estudos detalhados podem-se encontrar em [5], mas para os propósitos desta seção, isto nos é suficiente.

Todos os sistemas de encriptação nas Subseções 3.1.1, 3.1.2 são exemplos de sistemas simétricos. Note que, ocasionalmente, é preciso um pouco mais de tempo para a decifração, pois, como nos exemplos acima, é preciso aplicar o algoritmo de Euclides

para encontrar um inverso módulo N ou se deve inverter uma matriz, no entanto, o tempo adicional necessário não é elevado. Alem disso, geralmente o tempo adicional é necessário apenas uma vez, para encontrar a chave de decifração, depois disso ele não é mais necessário.

Exemplo 3.11 *Usando uma transformação afim em* $\mathbb{Z}/N\mathbb{Z}$*:* $C \equiv aP + b \pmod{N}$*, sabemos que a chave de encriptação é o par* $(a,b) \in (\mathbb{Z}/N\mathbb{Z})^* \times \mathbb{Z}/N\mathbb{Z}$*, uma vez que a conheçamos, podemos calcular a chave de decifração dada pelo par* $(a^{-1}, -a^{-1}b)$*, por meio do algoritmo de Euclides em um tempo estimado de* $O(\log^3(N))$ *operações binárias, e dado que novamente temos uma transformação afim, então decifrar requere o mesmo tempo que para cifrar.*

Se, por outro lado, o tempo de cifragem for polinomial em $\log B$ e o tempo para decifrar (com base no conhecimento da chave de encriptação mas não da chave de decifração) for, por exemplo, polinomial em B mas não em $\log B$, então deixamos de ter um sistema de criptografia clássica, donde teríamos o que é conhecido como um sistema de chave pública, o qual é nosso objeto de estudo na seção a seguir.

3.2 Sistemas Criptográficos de Chave Pública

Nesta seção, vamos continuar a descrição de alguns sistemas criptográficos, descrevendo a origem dos chamados *sistemas de chave pública*, também conhecidos como *sistemas assimétricos* (em contrapartida aos sistemas simétricos). Posteriormente ilustraremos sistemas criptográficos específicos deste tipo, como o *sistema RSA*, o qual baseia a sua segurança na dificuldade de fatorar grandes números. Nos sistemas descritos até agora, o procedimento de decifração não é difícil, uma vez que o método de cifragem, e assim a chave, são conhecidos. De fato, nesses casos a função de decifrar é, de certa forma, simétrica em relação à função de cifragem: ou seja, tanto computacional como logicamente, são funções do mesmo tipo. Em particular, todos os sistemas criptográficos clássicos dizem respeito à troca de mensagens entre dois usuários e dependem da troca de uma chave que, basicamente, permite tanto cifrar como decifrar.

Em uma época como a atual, quando a maioria das informações é transmitida por telefone ou correio eletrônico ou rádio, cada mensagem enviada, bem como cada chave enviada, são susceptíveis de ser facilmente interceptadas. Além disso, é necessário tornar possível a comunicação para os usuários que nunca se encontraram e, portanto, não tiveram, em princípio, a oportunidade de trocar chaves de cifragem privadas. Portanto, é indispensável encontrar maneiras novas e mais seguras de decifrar as mensagens.

Estes sistemas foram introduzidos em 1976 na sequência dos trabalhos de W. Diffie e M. Hellman [2], e independentemente por Ralph Merkle [21], procurando

eliminar o difícil problema de transmissão de chave. Os sistemas assimétricos usam uma chave dupla (k_E, k_D), onde k_E é conhecida como a *chave pública* e k_D é conhecida como a *chave privada*. A primeira delas serve para transformação de cifragem f_{k_E} e a segunda para a transformação de decifração $f_{k_D}^{-1}$. A essência do sistema de chave pública reside na propriedade de que alguém que só sabe cifrar não pode usar a chave de encriptação para encontrar a chave de decodificação sem uma computação excessivamente longa. Em outras palavras a, função de cifragem $f : \mathcal{P} \longrightarrow \mathcal{C}$ é fácil de calcular uma vez que a chave de encriptação k_E é conhecida, mas é muito difícil, na prática, para calcular a função inversa $f^{-1} : \mathcal{C} \longrightarrow \mathcal{P}$. Isso é, do ponto de vista de computabilidade realista, a função f não é invertível (sem alguma informação adicional — a chave de decifração k_D). Formalmente W. Diffie e M. Hellman definem um sistema de chave pública como segue:

Definição 3.12 *Um sistema criptográfico de chave pública é um par de famílias* $\{E_k\}_{k\in\mathcal{K}}$ *e* $\{D_k\}_{k\in\mathcal{K}}$ *de algoritmos representando transformações invertíveis,*

$$E_k : \mathcal{P} \to \mathcal{P},$$

$$D_k : \mathcal{P} \to \mathcal{P},$$

sobre o espaço finito de mensagens $\mathcal{P}$*, tais que*

1. *Para cada* $k \in \mathcal{K}$*,* E_k *é a inversa de* D_k*,*
2. *Para cada* $k \in \mathcal{K}$ *e cada* $P \in \mathcal{P}$*, os algoritmos* E_k *e* D_k *são fáceis de computar,*
3. *Para quase todo* $k \in \mathcal{K}$*, é computacionalmente inviável derivar a partir de* E_k *cada algoritmo facilmente calculado equivalente a* D_k*.*
4. *Para cada* $k \in \mathcal{K}$*, é viável calcular, a partir de k, os pares inversos* E_k *e* D_k*.*

Devido à terceira propriedade, a chave de cifragem E_k de um usuário pode ser tornada pública sem comprometer a segurança de sua chave de decifração secreta D_k. O sistema criptográfico é, portanto, dividido em duas partes, uma família de transformações de cifragem e uma família de transformações decifradoras de tal forma que, dado um membro de uma família, é impossível encontrar o membro correspondente da outra.

A quarta propriedade garante que há uma maneira viável de computar pares correspondentes de transformações inversas quando nenhuma restrição é colocada sobre o que deve ser a transformação de cifragem ou decifração.

Segundo as nossas notações do inicio deste seção, $E_k = f_k$ e $D_k = f_k^{-1}$, e $\mathcal{C} = \mathcal{P}$. Note que, dadas as propriedades que exibe f_k, ela é o que se conhece como uma função trapdoor, mais precisamente temos:

Definição 3.13 *Uma função unidirecional é uma função $f : A \to B$ com as seguinte propriedades:*

1. *$f(a)$ é fácil de calcular para qualquer $a \in A$,*
2. *É computacionalmente inviável calcular $f^{-1}(b)$ para quase todo $b \in B$.*

Uma função trapdoor, é uma função unidirecional f, satisfazendo além disso a seguinte propriedade:

3. *Dado $b \in B$, é fácil de calcular $f^{-1}(b)$, dada uma certa informação adicional.*

A noção de uma função trapdoor, aparentemente, apareceu pela primeira vez em 1978, juntamente com a invenção do sistema de criptografia de chave pública RSA, mas a noção de função unidirecional é um pouco mais antiga. O que parece ter sido o primeiro uso de funções unidirecionais para a criptografia, era descrito no livro de Wilkes sobre sistemas de compartilhamento de tempo que foi publicado em 1968. O autor descreve um novo sistema de cifrado unidirecional usado por R.M. Needham, para permitir que um computador verifique senhas sem armazenar informações que possam ser usadas por um intruso, se ele passar por um usuário legítimo.

> No sistema de Needham, quando o primeiro usuário estabelece a sua palavra chave, ou sempre que ele mudá-la, ela é imediatamente submetida ao processo de encriptação, e é a forma cifrada que é armazenada no computador. Sempre que a senha é digitada em resposta a uma demanda do supervisor para a identidade do usuário ser estabelecida, ela é novamente cifrada e o resultado comparado com a versão armazenada. Seria inútil a um suposto malfeitor, obter uma cópia da lista de senhas cifradas, uma vez que ele teria que decifrá-las antes que ele pudesse usá-las. Para este propósito, ele precisa ter acesso a um computador e até mesmo se todos os detalhes do algoritmo de encriptação estiverem disponíveis, o processo de decifração levaria um longo tempo, ver [24].

Em 1974, G. Purdy publica a primeira descrição detalhada de uma função unidirecional. As senhas originais e as suas formas cifradas são consideradas como inteiros módulo um primo "grande" p, e a função unidirecional $F_p \to F_p$ é dada por um polinômio $f(x)$, que não é difícil de avaliar por meio de computador, mas que tem um tempo excessivamente longo para inverter. Purdy usou $p = 2^{64} - 59$, $f(x) = x^{2^{24}+17} + a_1 x^{2^{24}+3} + a_2 x^3 + a_3 x^2 + a_4 x + a_5$, onde os coeficientes a_i são inteiros arbitrários de 19 dígitos. Em [5] podemos encontrar uma breve lista e estudos mais detalhados de funções que podem ser candidatas a serem função unidirecional, como por exemplo:

Exemplo 3.14 *A função $f(x,y) = xy$ é conjecturada ser uma função unidirecional, pois o problema da fatoração é computacionalmente inviável.*

Exemplo 3.15 *Seja $N = pq$ o produto de dois primos. Acredita-se que tal N é difícil de factorar. A função $f(x) = x^e \pmod N$, onde e é coprimo com $(p-1)(q-1)$. A função f parece ser "trapdoor", pois o conhecimento dos primos p e q permite inverter f facilmente. Até o momento o melhor "ataque" é tentar factorar N, o que parece computacionalmente inviável, pois a função do exemplo acima é uma função unidirecional.*

As definições acima de um sistema de criptografia de chave pública e de uma função unidirecional ou função trapdoor não são precisos do ponto de vista matemático rigoroso. Aqui a noção de "computabilidade realista" desempenha um papel fundamental. Mas isso é um conceito empírico que é afetado pelos avanços na tecnologia de computadores (por exemplo, técnicas de processadores paralelos) e a descoberta de novos algoritmos que aceleram o desempenho de tarefas aritméticas (às vezes por um grande fator). Assim, é possível que uma transformação de cifragem que pode seguramente ser considerado como uma função unidirecional ou trapdoor em 1994, poderá perder o seu estado de função unidirecional ou trapdoor em 2004 ou no ano 2994.

A razão para o nome "chave pública" é que a informação necessária para enviar mensagens secretas —a chave de encriptação k_E— pode ser feita uma informação pública, sem permitir que qualquer pessoa posa ler as mensagens secretas. Ou seja, suponha que temos alguma população de usuários do sistema de criptografia, cada um dos quais quer ser capaz de receber comunicações confidenciais de qualquer um dos outros utilizadores sem um terceiro (ou outro usuário, ou um estranho) ser capaz de decifrar a mensagem. Algum escritório central pode recolher a chave de cifragem $K_{E,A}$, de cada usuário A e publicar todas as chaves em uma "lista telefônica" com a forma

AAA Companhia Bancaria	(9974398087453939, 2975290017591012)
Sousa, Joaquim	(8870004228331, 7234752637937)
⋮	⋮

Alguém que quer enviar uma mensagem apenas, tem que procurar a chave de encriptação nesta "lista telefônica" e, em seguida, usar o algoritmo geral de encriptação com os parâmetros chave correspondentes ao destinatário pretendido. Apenas o destinatário pretendido tem a chave de decifração correspondente necessária para ler a mensagem. Observe que com um sistema de chave pública, é possível que duas partes iniciem comunicações secretas sem nunca ter tido qualquer contacto prévio, sem ter estabelecido qualquer confiança prévia para o outro, sem trocar qualquer informação preliminar. Todas as informações necessárias para enviar uma mensagem cifrada está disponível publicamente.

Em épocas pazadas, este tipo de sistema parecia não ter quaisquer vantagens particularmente notáveis. Tradicionalmente, a criptografia foi usada principalmente para fins militares e diplomáticos. Geralmente havia um grupo pequeno, bem definido, de usuários que pudessem compartilhar todo um sistema de chaves, e novas chaves poderiam ser distribuídas periodicamente (usando correios), de modo a manter o inimigo "adivinhando".

No entanto, nos últimos anos, as aplicações reais e potenciais de criptografia têm-se expandido para incluir muitas outras áreas, onde os sistemas de comunicação desempenham um papel vital — a coleta e manutenção de registos de dados confidenciais, transações financeiras eletrônicas, e assim por diante. Muitas vezes, tem-se uma grande rede de usuários, quaisquer dois dos quais deve ser capaz de manter suas comunicações em segredo de todos os outros usuários, bem como intrusos de fora da rede. Duas partes podem compartilhar uma comunicação secreta em uma ocasião, e, em seguida, um pouco mais tarde um deles pode querer enviar uma mensagem confidencial a um terceiro. Isto é, as "alianças" — quem está a compartilhar um segredo com quem — podem estar continuamente mudando. Pode ser impraticável sempre trocar chaves com todos os possíveis correspondentes confidenciais.

3.2.1 Autenticação

Muitas vezes, uma das partes mais importantes de uma mensagem é a assinatura. A assinatura de uma pessoa — esperançosamente, escrita com um toque idiossincrático da caneta, que é difícil de duplicar — permite que o destinatário saiba que a mensagem é realmente da pessoa cujo nome está escrito no final da mensagem. Se a mensagem é particularmente importante, pode ser necessário utilizar métodos adicionais para autenticar a comunicação. Nas comunicações eletrônicas, em que a pessoa não tem uma assinatura física, tem-se que confiar inteiramente em outros métodos. Por exemplo, quando um oficial de uma corporação quer retirar dinheiro da conta corporativa por telefone, ele/ela é frequentemente solicitado para dar algumas informações pessoais (por exemplo, nome de solteira da mãe) que o gestor corporativo sabe e o banco sabe (a partir dos dados apresentados quando a conta foi aberta), mas que um impostor não seria provável que saiba. Esta é uma ideia muito breve de assinatura, em [28] pode se encontrar uma definição formal do que é um sistema de assinatura e como alguns sistemas criptográficos podem ser transformados em sistemas de assinatura.

Na criptografia de chave pública, há uma maneira especialmente fácil de identificar-se de tal forma que ninguém poderia simplesmente fingir ser você. Sejam A (Ayrton) e B (Bryon) dois usuários do sistema. Seja f_A a transformação de cifragem com que qualquer usuário do sistema envia uma mensagem para Ayrton, e seja f_B o mesmo para Bryon. Para simplificar, vamos assumir que o conjunto $\mathcal{P}$ de todas as possíveis uni-

dades de mensagens de texto original e o conjunto $\mathcal{C}$ de todas as unidades de mensagens de texto cifrado possíveis são iguais, e são as mesmas para todos os usuários. Seja P a "assinatura" de Ayrton (talvez incluindo um número de identificação, uma declaração do momento em que a mensagem foi enviada, entre outras). Isso não seria suficiente para Ayrton enviar a mensagem codificada $f_B(P)$ para Bryon, já que todos os usuários sabem como fazer isso, então não haveria nenhuma maneira de saber que a assinatura não foi esquecida. Em vez disso, no início (ou fim) da mensagem Ayrton transmite $f_B f_A^{-1}(P)$. Então, quando Bryon decifrar a mensagem inteira, incluindo esta parte, através da aplicação de f_B^{-1}, ele descobre que tudo se tornou texto original, exceto por uma pequena secção de algaravia, que é $f_A^{-1}(P)$. Já que Bryon sabe que a mensagem é reivindicada a ser de Ayrton, ele aplica f_A (que ele conhece, já que a chave de encriptação de Ayrton é pública), e obtém P. Já que ninguém além de Ayrton poderia ter aplicado a função f_A^{-1} que é invertida pela f_A, ele sabe que a mensagem era de Ayrton.

3.2.2 Funções Hash

Uma função hash geralmente significa "uma função que comprime", significando que a saída é menor do que a entrada. Estas funções são usadas em muitas partes da criptografia, e existem muitos tipos diferentes de funções hash, com propriedades de segurança diferentes, formalmente temos:

Definição 3.16 *Uma função hash também conhecida como* `SHA-1` *é uma aplicação facilmente calculável $f : x \longmapsto h$ de uma entrada muito longa x de cadeias de cerca de 10^6 bits a uma saída muito mais curta h, de cadeias de 150 ou 200 bits, que tem a seguinte propriedade: não é computacionalmente viável encontrar duas entradas diferentes x e x' tal que $f(x) = f(x')$, esta propriedade é chamada de resistência à colisão.*

Uma maneira comum de assinar um documento é com a ajuda de uma função hash. Se parte da "assinatura" de Ayrton consiste do valor hash $h = f(x)$, onde x é todo o texto da sua mensagem, então Bryon pode verificar não apenas que a mensagem foi realmente enviada por Ayrton, mas também que não foi adulterado durante a transmissão, assim Bryon pode verificar a **integridade** da mensagem. Ou seja, Bryon aplica a função hash f a seu texto original decifrado de Ayrton, e verifica que o resultado está de acordo com o valor h na assinatura de Ayrton. Se assume, que nenhum transgressor teria sido capaz de alterar x sem alterar o valor de $h = f(x)$.

3.2.3 RSA

Na procura de uma função trapdoor f para ser usada num sistema de criptografia de chave pública, deseja se usar uma ideia que é bastante simples conceitualmente e se

presta a fácil implementação. Por outro lado, deseja se ter evidência empírica muito forte — baseada em uma longa história de tentativas de encontrar algoritmos para f^{-1} — que a decodificação não pode ser realizada sem o conhecimento da chave secreta de decodificação. Por esta razão, é natural olhar para um problema antigo da teoria dos números: o problema de encontrar a fatoração completa de um grande inteiro composto cujas fatores primos não são conhecidos antecipadamente. O sucesso do chamado sistema de criptografia "RSA", que é um dos mais antigos (38 anos) e mais populares sistemas de criptografia de chave pública, é baseado na tremenda dificuldade para factorar números inteiros grandes. Este código foi inventado em 1978 por Ron L. Rivest, Adi Shamir e Leonard Adelman [27], que na época trabalhavam no Massachussets Institute of Technology (M.I.T). As letras RSA correspondem às iniciais dos inventores do código (ver [1]). O algoritmo foi patenteado pelo M.I.T. em 1983 nos Estados Unidos com o número 4.405.829. Esta patente expirou em 21 de Setembro do 2000. Se tem conhecimento de que o matemático britânico Clifford Cocks, que trabalhava para a agencia de inteligencia britânica GCHQ, tinha descrito um sistema equivalente num documento interno em 1973. Devido ao alto custo dos computadores necessários para implementar na época, a sua ideia não transcendeu. Sua descoberta, no entanto, não foi revelada até 1997, já que era confidencial, por isso Rivest, Shamir e Adleman desenvolveram o RSA de forma independente.

Há vários outros códigos de chave pública, entre eles, o RSA é um dos mais usado na atualidade em aplicações comerciais. Este é um dos métodos utilizado, por exemplo, no BoxCryptor, um dos mais populares aplicativos para salvar arquivos na nuvem.

Como citamos acima, a segurança deste sistema se baseia no problema da fatoração de números inteiros, e seu funcionamento, no produto, conhecido, de dois grandes números primos escolhidos ao acaso e mantidos em segredo. Na atualidade, estes primos são da ordem de 10^{200}, e se prevê que a sua ordem de grandeza cresça com o aumento da capacidade de calculo dos ordenadores. Por outra parte, se acredita que o RSA será seguro enquanto não se conheçam formas eficientes para decompor números grandes como produto de seus fatores primos. A computação quântica poderia fornecer uma solução a este problema de fatoração.

Como o RSA Funciona?

Suponha que um usuário A deseja usar o sistema de criptografia RSA para enviar e receber mensagens, então ele prossegue da seguinte maneira:

1. **Calcular o módulo n.** A escolhe dois grandes primos diferentes p e q, digamos, de cerca de 100 dígitos decimais cada, e define

$$n = pq.$$

Sabendo a fatoração de n, é fácil calcular

$$\varphi(n) = (p-1)(q-1) = n+1-p-q.$$

2. **Calcular os expoentes e e d.** Em seguida A escolhe um número aleatório e tal que $1 \leq e \leq \varphi(n)$, e $mdc(e,\varphi(n)) = 1$. Logo, A calcula o inverso multiplicativo de e módulo $\varphi(n)$:
$$d \stackrel{def}{=} e^{-1} \pmod{\varphi(n)}, \qquad 1 \leq d \leq \varphi(n).$$

3. **Definir as Chaves.** Ele faz pública a chave de codificação
$$k_E = (n,e),$$
e oculta a chave de decodificação
$$k_D = (n,d).$$

4. **Codificação e Decodificação.** A define a transformação de codificação como sendo
$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ P &\longmapsto P^e \pmod{n}, \end{aligned}$$
e a transformação de decifração é definida como
$$\begin{aligned} f^{-1} : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ C &\longmapsto C^d \pmod{n}. \end{aligned}$$
Note que a f é a mesma função trapdoor definida no Exemplo 3.15.

Por que o RSA Funciona?

Como já sabemos, um sistema de criptografia só será útil se, decodificando um bloco codificado, obtemos de volta o bloco correspondente da mensagem original, ou seja, temos que mostrar que a aplicação f acima é 1-1. Dada uma unidade de mensagem $P \in \mathbb{Z}/n\mathbb{Z}$ temos que verificar $f^{-1}(f(P)) = P$. Note que, é muito difícil controlar quem são os números que são blocos da mensagem. Essencialmente qualquer número no intervalo 1 a n pode ocorrer, por isso precisamos dividir a prova em dois casos:

1. Suponha que a unidade de mensagem P é tal que $mdc(P,n) = 1$, logo
$$f^{-1}(f(P)) \equiv (P^e)^d \equiv P^{ed} \pmod{n},$$

como $d = e^{-1} \pmod{\varphi(n)}$, temos $ed = 1 + k\varphi(n)$, para algum inteiro k. Logo pelo teorema de Euler temos

$$P^{ed} \equiv P^{1+k\varphi(n)} \equiv P\left(P^{\varphi(n)}\right)^k \equiv P \pmod{n}.$$

2. Consideremos agora o caso em que $mdc(P,n) \neq 1$. Daqui temos os seguintes três casos:

   (a) $P = 0$, temos assim

   $$P^{ed} \equiv (P^e)^d \equiv 0^d \equiv 0 \pmod{n}.$$

   (b) $p|P$, mas $P \neq 0$. Logo $P \equiv 0 \pmod{p}$, e portanto

   $$P^{ed} \equiv P \pmod{p}.$$

   Por outra lado, pelo Pequeno Teorema de Fermat, temos

   $$P^{ed} \equiv P^{1+k\varphi(n)} \equiv P\left(P^{(p-1)(q-1)}\right)^k \equiv P\left(P^{q-1}\right)^{k(p-1)} \equiv P \pmod{q}.$$

   Note que, como p e q são dois primos diferentes, essas duas ultimas congruências implicam

   $$P^{ed} \equiv P \pmod{pq}.$$

   (c) $q|P$, mas $P \neq 0$. Análogo ao caso anterior.

A partir das descrições feitas acima, parece que estamos trabalhando com conjuntos $\mathcal{P} = \mathcal{C}$ de unidades de mensagens de texto original e texto cifrado que variam de um usuário para outro. Na prática, provavelmente queremos escolher $\mathcal{P}$ e $\mathcal{C}$ uniformemente em todo o sistema. Por exemplo, suponha que estamos trabalhando em um alfabeto de N letras. Então sejam $k < l$ inteiros positivos convenientemente escolhidos, de tal forma que, por exemplo, N^k e N^l tem 200 dígitos decimais aproximadamente. Tomamos como nossas unidades de mensagens de texto original todos os blocos de k letras que consideramos como números inteiros de k dígitos base N, ou seja, atribuímos os equivalentes numéricos entre 0 e N^k. Semelhantemente tomamos unidades de mensagem de texto cifrado para ser blocos de l letras em nosso alfabeto de N letras. Em seguida, cada usuário A deve escolher seus primos grandes p e q de modo que $n = pq$ satisfaz $N^k < n < N^l$. Então qualquer unidade de mensagem de texto original, ou seja, inteiro menor do que N^k, corresponde a um elemento em $\mathbb{Z}/n\mathbb{Z}$ (para qualquer n de um usuário); e, já que $n < N^l$ a imagem $f(P) \in \mathbb{Z}/n\mathbb{Z}$ pode ser escrito exclusivamente como um bloco de l letras. (Nem

todos os blocos de l letras podem surgir — apenas aqueles correspondentes a números inteiros menores do que n para o n específico de um usuário)

Exemplo 3.17 *Escolha $N = 26$, $k = 3$, $l = 4$. Ou seja, o texto original consiste em blocos de três letras e o texto cifrado é composto por blocos de quatro, ambos no habitual alfabeto de 26 letras A,B,...,Z. Para enviar a mensagem "YES" para um usuário A com chave de encriptação $(n,e) = (46927, 39423)$, primeiro encontramos o equivalente numérico de "YES", ou seja: $24 \cdot 26^2 + 4 \cdot 26 + 18 = 16346$, e depois calcular $16346^{39423} \pmod{46927}$, que dá $21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 =$ "BFIC."*

O destinatário A conhece a chave de decodificação $(n,d) = (46927, 26767)$, e assim calcula $21166^{26767} \pmod{46927} = 16346 =$ "YES". Como o usuário A gera as chaves? Em primeiro lugar, ele multiplicou os números primos $p_A = 281$ e $q_A = 167$ para obter n_A; em seguida, escolheu e aleatoriamente (mas sujeita à condição de que $mdc(e, 281) = mdc(e, 167) = 1$). Então, calculou $d = e^{-1} \pmod{280 \cdot 166}$. Os números p, q e d permanecem em segredo, enquanto que os números n e e são de domino público.

Observação 3.18 *Na escolha de p e q, o usuário A deve tomar cuidado e ver que certas condições sejam satisfeitas. As mais importantes são: os dois números primos não devem ser muito próximos um do outro (por exemplo, um deve ser de alguns dígitos decimais mais longo do que o outro); e que $p-1$ e $q-1$ tenham um mdc relativamente pequeno e ambos tenham pelo menos um grande fator primo. Claro, se alguém descobrir um método de fatoração que funciona rapidamente sob certas condições em p e q, então futuros usuários do RSA teriam que tomar cuidado para evitar essas condições também.*

Observação 3.19 *Como vamos enviar uma assinatura em RSA? Ao discutir a autenticação na Subseção 3.2.1, assumimos para simplificar, que $\mathcal{P} = \mathcal{C}$. A configuração na RSA é um pouco mais complicada. Aqui temos uma maneira de evitar o problema de diferentes n_A's e diferentes tamanhos de bloco (k, o número de letras em uma unidade de mensagem de texto original, sendo menor do que l, o número de letras em uma unidade de mensagem de texto cifrado). Suponha que, tal como na Subseção 3.2.1, Ayrton está enviando a sua assinatura (algum texto original P) para Bryon. Ele conhece a chave de codificação de Bryon, $k_{E,B} = (n_B, e_B)$ e sua própria chave de decodificação $k_{D,A} = (n_A, d_A)$. O que ele faz é enviar $f_B f_A^{-1}(P)$ se $n_A < n_B$, ou senão $f_A^{-1} f_B(P)$ se $n_A > n_B$. Isto é, no primeiro caso, ele toma o menor resíduo positivo de P^{d_A} módulo n_A; então, sobre esse número módulo n_B, ele calcula $\left(P^{d_A} \pmod{n_A}\right)^{e_B} \pmod{n_B}$, que ele envia como uma unidade de texto cifrado. No caso $n_A > n_B$, ela primeiro calcula $P^{e_B} \pmod{n_B}$ e então, trabalhando módulo n_A, ele eleva isto à d_A-ésima potência. Assim, Bryon pode verificar a autenticidade da mensagem no primeiro caso elevando à d_B-ésima potência módulo n_B e logo à e_A-ésima potência módulo n_A; no segundo caso ele faz essas operações na ordem contrária.*

3.2.4 Logaritmo Discreto

O sistema RSA, discutido na última seção, é baseado no fato de que a função $f(x,y) = xy$, do Exemplo 3.14, é conjecturada ser unidirecional, ou seja, encontrar dois grandes números primos e multiplicá-los para obter um número n é computacionalmente viável entanto a operação inversa, ou seja, dado n, encontrar os dois primos, é um problema computacionalmente intratável. Além deste, existem outros processos fundamentais na teoria dos números, que, aparentemente, também têm essa propriedade de "trapdoor" ou "unidirecional" . Um dos mais importantes é elevar a uma potência em um "grande" corpo finito.

Ao trabalhar com os números reais, a exponenciação: encontrar b^x a uma precisão requerida, não é significativamente mais fácil do que a operação inversa: encontrar $\log_b x$, a uma precisão requerida. Mas agora suponha que temos um grupo multiplicativo finito, como $(\mathbb{Z}/n\mathbb{Z})^*$ ou F_q^*. Devido ao método dos quadrados repetidos, pode-se calcular b^x para x grande bastante rápido, na verdade em um tempo que é polinomial em $\log x$. Mas, se estamos dando um elemento y que sabemos que é da forma b^x (supomos que a "base" b é fixa), como podemos encontrar a potência de b que dá y, ou seja, como podemos calcular $x = \log_b y$? Esta questão é chamada de o **"problema do logaritmo discreto"**. Embora usemos a mesma notação: "log", a palavra "discreto" distingue a situação dos grupos finitos da situação contínua.

Definição 3.20 *Seja G um grupo finito. Se b é um elemento de G, e y é um elemento de G o qual é uma potência de b, então o logaritmo discreto de y na base b é qualquer número inteiro x tal que* $b^x = y$. *Denotamos x como* $\log_b y$.

Exemplo 3.21 *Se tomamos* $G = F_{19}^* = (\mathbb{Z}/19\mathbb{Z})^*$ *e seja b o gerador 2, então o logaritmo discreto de 7 na base 2 é 6, pois* $7 = 2^6$.

Em [2] Whitfield Diffie e Martin E. Hellman, propõem um sistema de distribuição de chave pública o qual é baseado na aparente dificuldade de calcular logaritmos discretos no corpo finito F_q, ou seja que, o problema do logaritmo discreto é computacionalmente intratável. No que segue descrevemos vários sistemas criptográficos de chave pública, para fins especiais que são baseados na dificuldade computacional de resolver o problema do logaritmo discreto em corpos finitos.

O sistema de Troca de Chaves Diffie-Hellman

Como na prática, sistemas criptográficos de chave pública são relativamente lentos em comparação com sistemas criptográficos clássicos (pelo menos no nosso atual estágio da tecnologia e conhecimento teórico), muitas vezes é mais realista usá-los em um papel limitado, em conjunto com um sistema de criptografia clássica em que as mensagens

reais são transmitidas. Em particular, o processo de acordo sobre uma chave para um sistema de criptografia clássica pode ser realizada bastante eficiente usando um sistema de chave pública. A primeira proposta detalhada para fazer isso, devido ao W. Diffie e M. E. Hellman, baseou-se no problema do logaritmo discreto.

Vamos agora descrever o método Diffie-Hellman para gerar um elemento aleatório de um corpo "grande" finito F_q. Supomos que q é de conhecimento público: todos sabem que a nossa chave estará no corpo finito. Supomos também que g é algum elemento fixo de F_q, que também não é mantida em segredo. Idealmente, g deve ser um gerador de F_q^*, no entanto, isto não é absolutamente necessário. O método descrito a seguir, para gerar uma chave, vai levar apenas elementos de F_q que são potências de g, assim, se realmente queremos nosso elemento aleatório de F_q^* para ter uma chance de ser qualquer elemento, g deve ser um gerador.

Suponha que dois usuários A (Aida) e B (Bernardo) querem acordar uma chave — um elemento aleatório de F_q^* — que eles vão usar para encriptar suas mensagens. Então eles procedem do seguinte modo:

1. Aida escolhe um inteiro aleatório a entre 1 e $q-1$, que ela mantém em segredo. Logo calcula $g^a \in F_q$, que ela torna público.

2. Bernardo faz o mesmo: ele escolhe um aleatório b entre 1 e $q-1$ que mantem em secreto, e faz pública g^b.

3. Finalmente a chave secreta que eles usam é, g^{ab}.

Ambos usuários podem calcular essa chave. Por exemplo, Aida conhece g^b (que é do conhecimento público) e seu próprio a secreto, portanto pode calcular facilmente $(g^b)^a = g^{ab}$. No entanto, um terceiro usuário só conhece g^a e g^b. Se a seguinte suposição vale para o grupo multiplicativo F_q^*, então, esse terceiro não autorizado não será capaz de determinar a chave.

Suposição de Diffe-Hellman. É computacionalmente inviável calcular g^{ab} conhecendo só g^a e g^b.

A suposição de Diffie-Hellman é, a priori, pelo menos, tão forte quanto a suposição de que logaritmos discretos não podem ser calculados facilmente no grupo. Isto é, se logaritmos discretos podem ser calculados, então, obviamente, a suposição de Diffie-Hellman falha. Algumas pessoas conjecturam que a implicação inversa também se mantém, mas que ainda é uma questão em aberto. Em outras palavras, ninguém pode imaginar uma maneira de passar de g^a e g^b a g^{ab} sem primeiro ser capaz de determinar a ou b; mas é concebível que uma tal forma pode existir.

Exemplo 3.22 *Suponha que Aida e Bernardo vão usar uma transformação deslocamento para comunicar-se. Eles usam o alfabeto de 26 letras: A, B,...Z, considerando as unidades*

de texto como sendo blocos de uma única letra. Logo a transformação é: $C \equiv P + B \pmod{26}$. *Considere os parâmetros públicos* $q = 53$ *e* $g = 2$*, neste caso notamos que* g *é um gerador de* F_{53}^**. Para escolher a chave secreta B que eles vão usar, procedem como segue: tome o menor resíduo não negativo módulo 26 de um elemento aleatório em* F_{53}*. Suponha que Aida pegou ao acaso* $a = 29$*, e olhou para a chave pública* 2^b *de Bernardo, que é, digamos,* $12 \in F_{53}$*. Ela então sabe que a chave de encriptação é* $12^{29} = 21 \in F_{53}$*, ou seja,* $B = 21$*. Enquanto isso, ela faz pública sua chave* $2^{29} = 45$*, e assim Bernardo pode também encontrar a chave* $B = 21$ *elevando 45 à b-ésima potência, pois sua chave secreta é o exponente* $b = 19$*.*

É claro, não há segurança no trabalho com um pequeno corpo; um intruso pode facilmente encontrar o logaritmo discreto na base 2, de 12 ou 45 módulo 53. E em qualquer caso, não há segurança no uso de uma transformação deslocação de unidades de mensagens de uma única letra. Mas este exemplo ilustra a mecânica do sistema de troca de chaves Diffie-Hellman.

Sistema Criptográfico de Massey-Omura para a Transmissão de Mensagem

Este sistema criptográfico de chave pública foi proposto em 1982 por James Massey e Jim K. Omura [20]. Este protocolo usa a comutatividade de certas funções (neste caso, a exponenciação) para conseguir, em só três passos, que dois usuários troquem uma mensagem de forma segura sem compartilhar nenhuma chave.

Supomos que todos os usuários tenham acordado um corpo finito F_q, que é fixo e publicamente conhecido. Cada usuário do sistema escolhe secretamente um inteiro aleatório e entre 0 e $q-1$ tal que $mdc(e, q-1) = 1$ e, usando o algoritmo de Euclides, calcula seu inverso $d = e^{-1} \pmod{q-1}$, ou seja, $de \equiv 1 \pmod{q-1}$. Se o usuário A (Ayrton) quer enviar uma mensagem P para Bryon, ele prossegue da seguinte maneira:

1. Ele envia para Bryon o elemento P^{e_A}.

Isso não significa nada para ele, quem, não conhecendo d_A (ou e_A, para o caso), não pode recuperar P. Mas, sem tentar dar sentido a isso,

2. ele eleva P^{e_A} a seu e_B, e envia $P^{e_A e_B}$ de volta para Ayrton,

3. O passo final para Ayrton é desfazer a parte da mensagem elevando à d_A-ésima potência, ou seja $\left(P^{e_A e_B}\right)^{d_A} = P^{e_A e_B d_A} = P^{e_B}$, e retorna P^{e_B} para Bryon, que pode ler a mensagem, elevando à d_B-ésima potência.

A ideia por trás desse sistema é bastante simples, e pode ser generalizada para contextos onde se estejam usando outros processos além de exponenciação em corpos finitos. No entanto, algumas recomendações são necessárias.

Observação 3.23 *É absolutamente necessário usar um bom esquema de assinatura, juntamente com o sistema de Massey-Omura. Caso contrário, qualquer pessoa C que não pode saber a mensagem P poderia fingir ser Bryon, voltando para Ayrton* $P^{e_A e_C}$*; não sabendo que um intruso estava usando seu próprio* e_C*, ele iria continuar a elevar à* d_A *e fazendo possível para C ler a mensagem. Assim, a mensagem* $P^{e_A e_B}$ *de Bryon para Ayrton deve ser acompanhado por alguma autenticação, ou seja, alguma mensagem em algum esquema de assinatura que só Bryon poderia ter enviado.*

Observação 3.24 *É importante que, depois de um usuário, como B ou C decifrou várias mensagens P de A, e assim conhece vários pares* (P, P^{e_A})*, ele não posa usar essas informações para determinar* e_A*. Ou seja, suponha que Bryon poderia resolver o problema* log *discreto em* F_p^**, determinando assim a partir de P e* P^{e_A} *quem deve ser* e_A*. Nesse caso, ele pode rapidamente calcular* $d_A = e_A^{-1} \pmod{q-1}$ *e, em seguida, interceptar e ler todas as mensagens futuras de Ayrton, sejam para ele ou não.*

O Sistema de Criptografia ElGamal

Este sistema criptográfico de chave pública foi proposto por Tather ElGamal [3] em 1984. O sistema é descrito da seguinte maneira: começamos pela fixação de um corpo finito F_q muito grande e um elemento $g \in F_q^*$ (de preferência, mas não necessariamente, um gerador). Supomos que estamos usando unidades de mensagem de texto original com os equivalentes numéricos P, em F_q. Cada usuário escolhe aleatoriamente um número inteiro a, digamos no intervalo de $0 < a < q-1$. Este inteiro a é a chave de decodificação secreta. A chave de encriptação pública é o elemento $g^a \in F_q$.

Suponha que o usuário B quer enviar uma mensagem P para o usuário A, então ele procede assim:

1. B escolhe um inteiro k aleatoriamente,
2. B calcula o elemento $Pg^{a_A k}$,
3. por ultimo B envia para A o par de elementos de F_q: $\left(g^k, Pg^{a_A k}\right)$.

Observe que qualquer usuário pode calcular $g^{a_A k}$ sem conhecer a_A, simplesmente elevando g^{a_A} à k-ésima potência. Agora A, que conhece seu próprio a_A, pode recuperar a mensagem P deste par, da seguente forma:

1. A eleva g^k à a_A-ésima potência,
2. A divide esse resultado pelo segundo elemento e recupera P (ou, de forma equivalente, elevando g^k à $(q-1-a_A)$-ésima potência e multiplicando pelo segundo elemento).

Em outras palavras, o que B enviou a A consiste de uma forma disfarçada da mensagem — P esta "usando uma máscara" $g^{a_A k}$ — juntamente com uma "pista", ou seja g^k, que pode ser usado para tirar a máscara, mas a pista só pode ser utilizada por alguém que conhece a_A.

Alguém que pode resolver o problema de log discreto em F_q quebra o sistema de criptografia descobrindo a chave de decifração secreta a da chave de encriptação pública g^a. Em teoria, poderia haver uma maneira de usar o conhecimento de g^k e g^a para encontrar g^{ak} — e, portanto, quebrar a codificação — sem resolver o problema do log discreto. No entanto, como dissemos em nossa discussão sobre o sistema de troca de chaves Difee-Hellman, conjectura-se que não há nenhuma maneira de ir de g^k e g^a para g^{ak}, sem essencialmente resolver o problema do logaritmo discreto.

Assinatura Digital Padrão

Este sistema de assinatura foi desenvolvido pela Agencia Nacional de Segurança (National Security Agency-NSA) e em 1991 proposto pelo Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology-NIST) do governo dos EUA como um sistema de assinatura digital padrão (Digital Signature Standard-DSS)[4]. O papel de DSS está prevista para ser análogo ao, muito mais antigo Data Encryption Standard (DES), isto é, que é suposto para fornecer um método de assinatura digital padrão para uso de organizações comerciais e governamentais. Mas enquanto DES é um sistema de criptografia clássica ("chave privada"), a fim de construir assinaturas digitais, é necessário o uso de criptografia de chave pública. NIST optou por basear o seu esquema de assinatura no problema do log discreto em um corpo primo finito. O DSS é semelhante ao esquema de assinatura ElGamal. Vamos agora descrever a forma como o DSS funciona.

Para definir o esquema (a fim depois de ser capaz de assinar mensagens), cada usuário A prossegue da seguinte forma:

1. A escolhe um primo q de cerca de 160 bits[1],
2. A em seguida, escolhe um segundo primo p, que é $\equiv 1 \pmod{q}$, e tem cerca de 512 bits,
3. A escolhe um gerador g do único subgrupo cíclico de F_p^* de ordem q.

Calculando $g_0^{(p-1)/q} \pmod{p}$ para um número inteiro aleatório g_0; se esse número é $\neq 1$, será um gerador.

[1]Bit é o acrônimo inglês de "Binary digit" (ou seja de "dígito binário" em português) Um bit é um dígito do sistema de numeração binário. Por exemplo, o número decimal 3, tem uma representação no sistema binário como o número de 4 bits, 0011.

4. A toma um inteiro aleatório x no intervalo $0 < x < q$ como sua chave secreta, e define sua chave pública como sendo $y = g^x \pmod{p}$.

Agora, suponha que A quer assinar uma mensagem. Ele prossegue assim:

1. A aplica uma função hash a seu texto simples, obtendo assim um inteiro h no intervalo $0 < h < q$,

2. A em seguida escolhe um inteiro aleatório k no mesmo intervalo e calcula $g^k \pmod{p}$, e define $r = (g^k \pmod{p}) \pmod{q}$ (ou seja, g^k é primeiro calculado módulo p, e o resultado é, em seguida, reduzido módulo o menor primo q). Logo, A encontra um inteiro s tal que $sk \equiv h + xr \pmod{q}$,

3. finalmente A define sua assinatura como sendo o par de inteiros (r,s) módulo q.

Para verificar a assinatura, o destinatário Bryon prossegue da seguente maneira:

1. ele calcula $u_1 = s^{-1}h \pmod{q}$ e $u_2 = s^{-1}r \pmod{q}$,

2. em seguida calcula $g^{u_1}y^{u_2} \pmod{p}$. Note que $g^{u_1}y^{u_2} = g^{s^{-1}(h+xr)} = g^k \pmod{p}$,

3. finalmente, se o resultado concorda módulo q com r, ele está satisfeito.

Este esquema de assinatura tem as seguentes vantagens:

1. As assinaturas são bastante curtas, consistindo em dois números de 160 bits (A magnitude de q).

2. Por outro lado, a segurança do sistema parece depender da intratabilidade do problema log discreto no grupo multiplicativo do, "bem grande" corpo F_p.

Embora para quebrar o sistema seria suficiente encontrar logaritmos discretos no subgrupo menor gerado por g, na prática, isso parece não ser mais fácil do que encontrar logaritmos discretos arbitrários em F_p^*. Assim, o DSS parece ter atingido um nível bastante elevado de segurança sem sacrificar armazenagem de assinaturas pequenas e tempo de implementação.

CAPÍTULO 4

Curvas Elípticas

Nas últimas décadas, a *criptografia com curvas elípticas* tem adquirido uma crescente importância, chegando a formar parte dos padrões industriais. O principal êxito, se tem conseguido nos sistemas baseados no problema do logaritmo discreto, como os do tipo ElGamal. Estes sistemas criptográficos baseados no grupo de pontos de uma curva elíptica, garantem a mesma segurança que os construídos sobre o grupo multiplicativo de um corpo finito, mas com chaves menores.

A criptografia com curvas elípticas foi proposta em 1985 independentemente por Neal Koblizt [14] e por Victor Miller [22] como alternativa aos sistemas de chave publica clássicos, como o RSA e ElGamal, tanto pela diminuição no tamanho das chaves que se requerem, como pela fonte inesgotável de grupos abelianos finitos que fornecem um mesmo corpo base. No capítulo anterior, trabalhou se com os grupos multiplicativos dos corpos. Em muitas formas, as curvas elípticas são análogos naturais destes grupos, mas com a vantagem de termos mais flexibilidade na escolha de uma curva elíptica, do que na escolha de um corpo finito.

Neste capítulo vamos começar apresentando as definições e os fatos básicos sobre curvas elípticas, para os quais as provas serão omitidas devido a sua complexidade e que estão fora dos objetivos deste trabalho, mas podem ser consultadas em [16] e [33]. Posteriormente, iremos descrever os análogos para curvas elípticas dos sistemas criptográficos de chave pública estudados no capítulo anterior, e finalizaremos com o estudo de como escolher adequadamente uma curva elíptica, e um ponto sobre ela, para serem usados nos sistemas criptográficos.

4.1 Fatos Básicos

Nesta seção, denotamos um corpo por K, e por $\overline{K}$ seu fecho algébrico. Para nós, K poderia ser o corpo $\mathbb{R}$ dos números reais, o corpo $\mathbb{Q}$ dos números racionais, o corpo $\mathbb{C}$ dos números complexos ou o corpo finito F_q de $q = p^r$ elementos.

Definição 4.1 *Uma equação de Weierstrass é uma equação homogênea de grau 3 do tipo*

$$y_1^2 + a_1x_1y_1 + a_3y_1 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6, \tag{1}$$

onde $a_1, a_2, a_3, a_4, a_6 \in \overline{K}$.

Definição 4.2 *Se tomamos*

$$F(x_1, y_1) = y_1^2 + a_1x_1y_1 + a_3y_1 - x_1^3 - a_2x_1^2 - a_4x_1 - a_6$$

como a equação implícita para y_1 *como função de* x_1 *em (1), então um ponto* $P = (x_1, y_1)$ *tal que* $F(P) = 0$ *é chamado de não-singular, ou ponto suave, se pelo menos uma das derivadas parciais*

$$\frac{\partial F}{\partial x_1}, \ \frac{\partial F}{\partial y_1}$$

é não-zero no ponto P. Porém, se essas duas derivadas parciais se anulam em P, então P é chamado de ponto singular. Além disso, dizemos que a equação de Weierstrass é não-singular, se todo ponto $P = (x, y)$*, tal que* $F(P) = 0$*, é não-singular.*

Agora, de posse dos dois conceitos anteriores, podemos dar uma definição do que é uma *curva elíptica* sobre $\overline{K}$.

Definição 4.3 *Uma curva elíptica E definida sobre* $\overline{K}$ *é o conjunto de todos os pontos* $(x, y) \in \overline{K} \times \overline{K}$ *que satisfazem uma equação de Weierstrass não-singular, junto com um único elemento denotado* $\mathcal{O}$ *e chamado de "ponto no infinito".*

Observação 4.4 *1. Note que se* $Char(K) \neq 2$*, então podemos fazer a mudança de variáveis* $(x_0, y_0) = (x_1, 2y_1 + a_1x_1 + a_3)$ *e reduzir (1) à equação* $y_0^2 = 4x_0^3 + b_2x_0^2 + 2b_4x_0 + b_6$*. Além disso, se* $Char(K) \neq 3$*, ou seja,* $Char(K) \neq 2, 3$*, fazendo a substituição* $(x, y) = (36x_0 + 3b_2, 108y_0)$ *na última equação, podemos ver que esta se reduz a* $y^2 = x^3 - 27c_4x - 54c_6$*. Note que esta ultima equação, é do tipo*

$$y^2 = x^3 + ax + b, \tag{2}$$

a qual chamaremos de equação canônica de Weierstrass. A partir de agora, salvo casos especiais, trabalharemos com esta equação como a equação geral de uma curva elíptica definida sobre um corpo K.

2. Se $Char(K) = 2$*, então (1) se pode reduzir a uma equação do tipo*

$$y^2 + cy = x^3 + ax + b \quad ou \quad y^2 + xy = x^3 + ax^2 + b. \tag{3}$$

3. *Se $Char(K) = 3$, então (1) se pode reduzir a uma equação do tipo*

$$y^2 = x^3 + ax^2 + bx + c. \tag{4}$$

4. *Pode se mostrar que a condição de que a equação de Weierstrass seja não-singular é equivalente a que a equação cúbica da direita em (2) e (4) não tenha raízes múltiplas.*

5. *Se os coeficientes $a_1, a_2, a_3, a_4, a_6 \in K$, dizemos que E está definida sobre K, e a denotamos por E_K. Se E está definida sobre K e $(x,y) \in E$ é tal que $x, y \in K$, então dizemos que o ponto (x,y) é um ponto K-racional. Denotamos por $E(K)$ o conjunto dos pontos K-racionais de E*

4.1.1 Curvas Elípticas sobre os Reais

Antes de discutir alguns exemplos específicos de curvas elípticas sobre vários corpos, vamos introduzir um fato centralmente importante sobre o conjunto de pontos em uma curva elíptica: eles formam um grupo abeliano. Para explicar como isso funciona visualmente, para o momento, vamos supor que $K = \mathbb{R}$, isto é, a curva elíptica é uma curva normal no plano, mais um outro ponto $\mathcal{O}$ "no infinito".

Definição 4.5 *Seja E uma curva elíptica sobre os números reais, e sejam P e Q dois pontos em E. Definimos o negativo de P e a soma $P+Q$ de acordo as seguintes regras:*

1. *Se P é o ponto no infinito $\mathcal{O}$, então definimos $-P$ como $\mathcal{O}$ e $P+Q$ como Q; isto é, $\mathcal{O}$ atua como a identidade aditiva ("elemento zero") do grupo de pontos. No que segue, vamos supor que nem P ou Q é o ponto no infinito.*

2. *O negativo $-P$ é o ponto com a mesma coordenada x mas a coordenada y negativa, de P, isto é, $-(x,y) = (x,-y)$. É imediato de (2) que $(x,-y)$ está sobre a curva sempre que (x,y) esteja.*

3. *Se P e Q tem coordenadas x diferentes, então não é difícil ver que a linha $\ell = \overline{PQ}$ intersepta a curva em exatamente mais um ponto, R, (a menos que a linha seja tangente à curva no ponto P (ou Q), em tal caso tomamos $R = P$ (ou $R = Q$)). Então defina $P+Q$ como $-R$, ou seja, a imagem refletida, com respeito ao eixo x do terceiro ponto na interseção.*

4. *Se $Q = -P$ (ou seja, Q tem a mesma coordenada x mas menos a coordenada y), então definimos $P+Q = \mathcal{O}$ (o ponto no infinito). (Isto é forçado por 2.).*

5. *A possibilidade final é $P = Q$. Então ℓ é a linha tangente à curva em P, seja R o único outro ponto da interseção de ℓ com a curva, e defina $P+Q = -R$ (R é tomado para ser P se a linha tangente tem uma "dupla tangencia" no ponto P, ou seja, se P é um ponto de inflexão).*

Exemplo 4.6 *A curva elíptica $y^2 = x^3 - x$, no plano xy, é esboçada abaixo, na Figura 4.1. O diagrama também mostra o típico caso da soma dos pontos P e Q. Para encontrar $P+Q$ desenhamos uma linha através de P e Q, e tomamos $P+Q$ como o ponto simétrico (com respeito ao eixo x) ao terceiro ponto onde a linha que passa por P e Q intersecta a curva. Se P e Q são o mesmo ponto, ou seja, se queremos encontrar $2P$, usaríamos a linha tangente à curva em P; donde $2P$ é o ponto simétrico ao terceiro ponto onde a linha tangente intersecta a curva.*

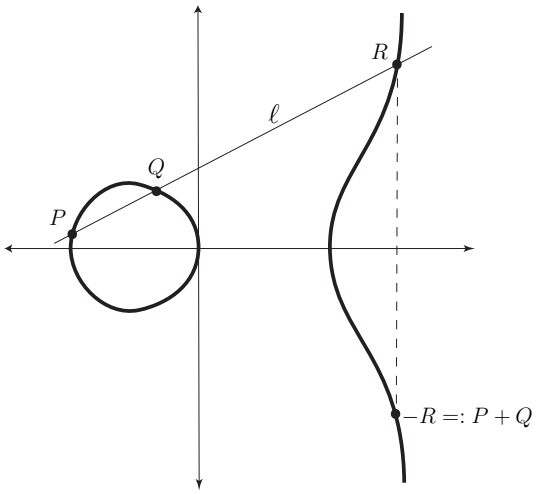

Figura 4.1: *Curva elíptica $y^2 = x^3 - x$.*

Vamos agora mostrar que existe exatamente mais um ponto onde a linha ℓ, que passa por P e Q, intersecta a curva, e ao mesmo tempo vamos a derivar uma fórmula para as coordenadas do terceiro ponto, e portanto para as coordenadas de $P+Q$.

Sejam (x_1, y_1), (x_2, y_2) e (x_3, y_3) as coordenada dos pontos P, Q, e $P+Q$, respectivamente. Queremos expressar x_3 e y_3 em termos de x_1, y_1, x_2, y_2. Suponha que estamos no caso 3. da definição de $P+Q$, e seja $y = \alpha x + \beta$ a equação da linha que passa por P e Q (a qual não é uma linha vertical no caso 3.). Então $\alpha = (y_2 - y_1)/(x_2 - x_1)$, e $\beta = y_1 - \alpha x_1$ .Um ponto sobre ℓ, ou seja, $(x, \alpha x + \beta)$, encontra-se na curva elíptica se e somente se $(\alpha x + \beta)^2 = x^3 + ax + b$. Assim, existe um ponto de interseção para cada raiz da equação cubica $x^3 - (\alpha x + \beta)^2 + ax + b$. Já sabemos que existem duas raízes x_1 e x_2, porque $(x_1, \alpha x_1 + \beta)$, $(x_2, \alpha x_2 + \beta)$ são os pontos P, Q sobre a curva. Já que a soma das raízes de um polinômio mônico é igual a menos o coeficiente da segunda maior potência, concluímos que a terceira raiz neste caso é $x_3 = \alpha^2 - x_1 - x_2$. Isto conduz a uma expressão

para x_3, e portanto $P+Q=(x_3,-(\alpha x_3+\beta))$, em termos de x_1, x_2, y_1, y_2:

$$\begin{aligned} x_3 &= \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2; \\ y_3 &= -y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3). \end{aligned} \tag{5}$$

O caso 5. quando $P=Q$ é similar, exceto que α é agora a derivada dx/dy no ponto P. Derivação implícita da equação (2) conduz à fórmula $\alpha=(3x_1^2+a)/2y_1$, e então obtemos as seguintes fórmulas para as coordenadas de $2P$:

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1; \\ y_3 &= -y_1 + \left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3). \end{aligned} \tag{6}$$

Exemplo 4.7 *Sobre a curva elíptica $y^2=x^3-36x$, sejam $P=(-3,9)$ e $Q=(-2,8)$. Vamos encontrar $P+Q$ e $2P$. Note que substituindo $x_1=-3$, $y_1=9$, $x_2=-2$, $y_2=8$ na primeira equação em (5) obtemos $x_3=6$; então a segunda equação em (5) da $y_3=0$, ou seja que $P+Q=(6,0)$. Em seguida, substituímos $x_1=-3$, $y_1=9$, $a=-36$ na primeira equação em (6) e da $x_3=25/4$; e na segunda equação de (6) da $y_3=-35/8$, e assim $2P=(25/4,-35/8)$.*

Teorema 4.8 *A curva elíptica E definida sobre K, junto com a operação de soma dada na Definição 4.5, formam um grupo abeliano.*

Para provar este importante fato pode-se usar um argumento de geometria projetiva, um argumento analítico complexo com funções duplamente periódicas, ou um argumento algébrico envolvendo divisores nas curvas.

Lema 4.9 *O conjunto $E(K)$ dos pontos K-racionais de E é um subgrupo de E.*

Como em qualquer grupo abeliano, usamos a notação nP para denotar P adicionado a si mesmo n vezes, se n for positivo, e caso contrário, $-P$ adicionado a si mesmo $|n|$ vezes.

Definição 4.10 *A ordem N de um ponto P sobre uma curva elíptica, é o menor inteiro positivo tal que $NP=\mathcal{O}$; tal N, não é necessariamente finito.*

Muitas vezes, é de interesse encontrar pontos P de ordem finita em uma curva elíptica, especialmente para curvas elípticas definidas sobre $\mathbb{Q}$.

Exemplo 4.11 *Para encontrar a ordem de $P = (2,3)$ sobre $y^2 = x^3 + 1$ procedemos como segue. Usando (6), encontramos que $2P = (0,1)$, e usando (6) novamente, temos $4P = 2(2P) = (0,-1)$. Assim, $4P = -2P$, e portanto $6P = \mathcal{O}$. Logo, a ordem de P é 2, 3, ou 6. Mas $2P = (0,1) \neq \mathcal{O}$, e se P tem ordem 3, então $4P = P$, o qual não é verdade. Assim, P tem ordem 6.*

Ainda não temos dito muito sobre o "ponto do infinito" $\mathcal{O}$, o qual por definição, é a identidade da lei do grupo. No diagrama exibido anteriormente, este é o "terceiro ponto de intersecção" de qualquer linha vertical com a curva; isto é, uma tal linha tem pontos de intersecção da forma (x_1, y_1), $(x_1, -y_1)$ e $\mathcal{O}$. Uma maneira mais natural para introduzir o ponto $\mathcal{O}$ é usando o plano projetivo, como segue.

4.1.2 Plano Projetivo

Definição 4.12 *O plano projetivo de dimensão 2 sobre K, $\mathbb{P}^2(K)$, é definido como o conjunto das classes de equivalência de trios $(X,Y,Z) \neq (0,0,0)$, junto com a relação "$\sim$", onde $(X,Y,Z) \sim (X',Y',Z')$ se, e somete se, existe um único elemento $\lambda \in K^*$ tal que $(X',Y',Z') = \lambda(X,Y,Z)$. A classe de equivalência do ponto (X,Y,Z) é denotada por $[X:Y:Z]$, e é chamada de ponto projetivo.*

Definição 4.13 *Uma linha ou reta no plano projetivo se define como o conjunto de pontos projetivos $[X:Y:Z]$, tais que $aX + bY + cZ = 0$, onde a,b,c não são todos nulos.*

Observação 4.14 *1. Note que, se um ponto projetivo tem $Z \neq 0$, então $[X:Y:Z] = [X/Z : Y/Z : 1]$, logo defina $x = X/Z$, $y = Y/Z$, assim existe uma única tripla da forma $(x,y,1)$ na classe de equivalência $[X:Y:Z]$. Portanto, o plano afim $K \times K$ tem uma imersão natural em $\mathbb{P}^2(K)$, que é a função que envia (x,y) em $[x:y:1]$. A imagem desta função, junto com os pontos para os quais $Z = 0$, ou seja, os pontos projetivos $[X:Y:0]$, cobrem $\mathbb{P}^2(K)$.*

Definição 4.15 *O conjunto de pontos projetivos da forma $[X:Y:0]$, compõem o que é chamado de linha no infinto. Além disso, cada ponto projetivo na linha no infinito é chamado de ponto no infinito.*

2. Qualquer equação $F(x,y) = 0$, de uma curva no plano afim, corresponde a uma equação $\widetilde{F}(X,Y,Z) = 0$, satisfeita pelos pontos projetivos correspondentes; basta substituir x por X/Z e y por Y/Z, e multiplicar por uma potência de Z para eliminar os denominadores.

Exemplo 4.16 *Se aplicarmos o procedimento de 3. para a equação afim (2) de uma curva elíptica, obtemos a sua "equação projetiva" :* $Y^2Z = X^3 + aXZ^2 + bZ^3$. *Esta última equação é satisfeita por todos os pontos projetivos* $[X : Y : Z]$ *com* $Z \neq 0$, *para o qual os pontos afins correspondentes* (x,y), *onde* $x = X/Z$, $y = Y/Z$, *satisfazem (2).*

Além disso, que pontos projetivos $[X : Y : Z]$ *na linha no infinito satisfazem a equação* $\widetilde{F} = 0$? *Com* $Z = 0$, *na equação projetiva temos que* $0 = X^3$, *isto é,* $X = 0$. *Mas a única classe de equivalência* $[X : Y : Z]$ *com X e Z ambos nulos, é a classe de* $[0 : Y : 0]$. *Note que, esta classe é igual à* $[0 : 1 : 0]$, *pois* $Y \neq 0$. *Logo o ponto projetivo* $[0 : 1 : 0]$ *é o único ponto da linha no infinito que satisfaz* $\widetilde{F} = 0$, *e este é o ponto que chamamos de* $\mathcal{O}$, *o qual é o ponto de intersecção do eixo y com a linha no infinito.*

4.1.3 Curvas Elípticas sobre os Complexos

As fórmulas algébricas (4)-(5) para a adição de pontos em uma curva elíptica sobre os reais na verdade faz sentido em qualquer corpo. Se o corpo tem característica 2 ou 3, podem se derivar equações similares, a partir da equação (3) ou (4). É possível mostrar que estas fórmulas nos dão uma lei de grupo abeliano em uma curva elíptica, sobre qualquer corpo.

Em particular, seja E uma curva elíptica definida sobre $\mathbb{C}$, o corpo de números complexos. Assim, E é o conjunto de pares (x,y) de números complexos que satisfazem a equação (2), juntamente com o ponto no infinito $\mathcal{O}$. Embora E seja uma "curva", se pensarmos em termos de desenhos geométricos familiares, esta é 2-dimensional, ou seja, é uma superfície no espaço real 4-dimensional, cujas coordenadas são as partes real e imaginária de x e y. Descrevemos agora, como E pode ser visualizado como uma superfície.

Definição 4.17 *Um reticulado complexo é um grupo discreto* $L = \langle \omega_1, \omega_2 \rangle_{\mathbb{Z}} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, *onde* ω_1 *e* ω_2 *são dois números complexos linearmente independentes sobre* $\mathbb{R}$.

Note que, a independência de ω_1 e ω_2 é equivalente a que sejam não nulos e $\tau = \omega_1/\omega_2$ tenha parte real não nula. Escolhendo a ordem de ω_1 e ω_2 podemos exigir que $Im\,\tau > 0$. Dizemos assim que o par (ω_1, ω_2) é uma base orientada do reticulado L. No que segue supomos que as bases com as que trabalhamos estão orientadas.

Definição 4.18 *Chamamos de paralelogramo fundamental associado a uma base* (ω_1, ω_2) *de um reticulado complexo L, o conjunto* $P = \{a\omega_1 + b\omega_2 \ : \ 0 \leq a, b < 1\}$

Por exemplo, se $\omega_1 = 1$ e $\omega_2 = i$, então L é os inteiros Gaussianos, e o paralelogramo fundamental P é o quadrado unitário.

Definição 4.19 *Uma função elíptica com respeito a um reticulado complexo L, é uma função meromorfa $f : \mathbb{C} \to \mathbb{C}^{\infty}$ tal que $f(z+\omega) = f(z)$ para todo $z \in \mathbb{C}$ e todo $\omega \in L$.*

Um número complexo ω que satisfaz $f(z+\omega) = f(z)$ para todo $z \in \mathbb{C}$ é chamado de *período* de f. Assim, os elementos de L são os períodos de f. Note que, para que f seja elíptica com respeito a L, basta que tenha por períodos uma base de L. Em outras palavras, uma função elíptica, com respeito a um reticulado dado, não é mais do que uma função meromorfa duplamente periódica, ou seja, uma função com dois períodos linearmente independentes.

Definição 4.20 *Dado um reticulado L, definimos a função $\wp$ de Weierstrass, denotada por $\wp_L(z)$, como*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Assim, dada uma curva elíptica (2) sobre os números complexos, verifica-se que existe um reticulado L e uma função $\wp$ de Weierstrass, que tem as seguintes propriedades:

1. $\wp(z)$ é uma função elíptica, ou seja, satisfaz que $\wp(z+\omega) = \wp(z)$. E é duplamente periódica, já que tem dois períodos linearmente independentes ω_1 e ω_2, onde $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$,

2. sua derivada $\wp'(z) = -2\sum_{\omega \in L} \frac{1}{(z-\omega)^3}$ também é uma função elíptica sobre L,

3. $\wp(z)$ satisfaz a equação diferencial $\left(\wp^{'}\right)^2 = \wp^3 + a\wp + b$, e portanto para qualquer $z \notin L$ o ponto $(\wp(z), \wp^{'}(z))$ encontra-se na curva elíptica E,

4. dois números complexos z_1 e z_2, produzem o mesmo ponto $(\wp(z), \wp^{'}(z))$ sobre E se, e somente se, $z_1 - z_2 \in L$; isso é imediato do fato que $\wp$ e $\wp'$ são funções elípticas.

Teorema 4.21 *Considere o quociente entre $\mathbb{C}$ e o reticulado L, $\mathbb{C}/L$. Então a aplicação $\phi : \mathbb{C}/L \to E$ tal que*

$$\phi(z) = \begin{cases} (\wp(z), \wp'(z)) \in E, & \text{se } z \notin L, \\ \mathcal{O}, & \text{se } z \in L, \end{cases}$$

é um isomorfismo de grupos.

Assim, podemos pensar no grupo abeliano E como equivalente ao plano complexo módulo um reticulado adequado. Para visualizar esse último grupo, note que cada classe de equivalência $z+L$ tem um, e apenas um, representante no paralelogramo fundamental. Já que os pontos opostos sobre os lados paralelos da fronteira do paralelogramo

diferem por um ponto reticulado, então eles são iguais em $\mathbb{C}/L$. Isto é, considerá-los como "colados um ao outro". Visualizando isto — dobrar ao longo de um lado de um paralelogramo para encontrar o lado oposto, obtendo assim um segmento de um cilindro e, em seguida, dobrar novamente e colando os círculos opostos — vemos que obtemos um toro, mais precisamente temos:

Definição 4.22 *Dado um reticulado complexo L, um toro complexo é definido como o quociente* $T = \mathbb{C}/L$.

Observação 4.23 *Como um grupo, o toro é o produto de duas copias de um circulo, ou seja,* $T \cong S^1 \times S^1$*; seus pontos podem ser parametrizados por pares ordenados de ângulos* (α, β). *Mais precisamente, dado o toro T obtido de um reticulado* $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, *então escrevemos um elemento de* $\mathbb{C}/L$ *na forma* $a\omega_1 + b\omega_2$ *e tomamos* $\alpha = 2\pi a$, $\beta = 2\pi b$. *Temos assim, de acordo com o Teorema 4.21 que a curva elíptica E sobre os números complexos é tal que* $E \cong S^1 \times S^1$, *ou seja, podemos pensar E como uma generalização, em duas dimensões reais, do circulo no plano.*

4.1.4 Curvas Elípticas sobre os Racionais

Na equação (2), se a e b são números racionais, é natural procurar soluções racionais (x, y), ou seja, considerar curvas elípticas sobre o corpo $\mathbb{Q}$ dos números racionais, tais que $x, y \in \mathbb{Q}$. Existe uma vasta teoria de curvas elípticas sobre os racionais. A teoria moderna das equações de Diofantinas, a solução de equações polinomiais usando inteiros ou números racionais, foi iniciada em 1922 quando L.J. Mordell provou um resultado descrevendo $E(\mathbb{Q})$.

Definição 4.24 *Dado um grupo abeliano G e um elemento* $x \in G$, *dizemos que x é um elemento de torção se a ordem de x é finita.*

Proposição 4.25 *O conjunto de elementos de torção de um grupo abeliano G é um subgrupo, chamado de o grupo de torção de G e denotado por* G_T.

Observação 4.26 *Note que o elemento identidade do grupo, é trivialmente um elemento de torção. Além disso, se* $G = G_T$, *dizemos que G é um grupo de torção. Por outro lado, um grupo abeliano sem elementos de ordem finita (exceto o neutro), é dito livre de torção.*

Teorema 4.27 ***(Mordell)*** *Seja E uma curva elíptica definida sobre* $\mathbb{Q}$. *Então, o grupo de pontos* $\mathbb{Q}$*-racionais* $E(\mathbb{Q})$ *é um grupo abeliano finitamente gerado.*

Em outras palavras, existe um conjunto finito de pontos $P_1, \ldots, P_t \in E(\mathbb{Q})$ tal que todo ponto $P \in E(\mathbb{Q})$ pode ser escrito na forma $P = n_1P_1 + \cdots + n_tP_t$, para certos inteiros $n_1, \ldots, n_t$.

Em geral, o teorema fundamental dos grupos abelianos finitamente gerados diz que, existe um inteiro $r \geq 0$, tal que podemos escrever $E(\mathbb{Q})$ como

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_T \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r-\text{vezes}},$$

onde o inteiro r é chamado de posto de $E(\mathbb{Q})$. Note que r é zero, se e somente se, o grupo é finito, em tal caso $E(\mathbb{Q}) = E(\mathbb{Q})_T$.

O estudo do posto r, e outras características do grupo de uma curva elíptica sobre $\mathbb{Q}$, está relacionado à várias perguntas interessantes da Teoria dos Números e Geometria Algébrica. Por exemplo, uma pergunta feita desde tempos antigos — "Dado um inteiro positivo n, quando existe um triângulo retângulo, com lados racionais, cuja área é n?" — resulta ser equivalente à pergunta "O posto da curva elíptica $y^2 = x^3 - n^2x$ é maior que zero?" O caso $n = 6$ e o triângulo retângulo de lados 3-4-5 levam para o ponto P no Exemplo 4.7, que é um ponto de ordem infinita na curva $y^2 = x^3 - 36x$.

4.1.5 Curvas Elípticas sobre um Corpo Finito

Para o restante desta seção vamos tomar K como o corpo finito F_q de $q = p^r$ elementos. Seja E uma curva elíptica definida sobre F_q. Se $p = 2$ ou 3, então E é dada por uma equação da forma (3) ou (4), respectivamente. Note que, se E está definida sobre o corpo finito F_q, então o grupo de pontos F_q-racionais, $E(F_q)$, é um grupo finito. O cálculo da cardinalidade deste grupo é uma questão importante no estudo de curvas elípticas sobre F_q, porém, é uma tarefa muito difícil. A primeira estimativa que temos para a cardinalidade deste grupo, nos diz que

$$|E(F_q)| \leq 2q + 1,$$

ou seja, uma curva elíptica pode ter no máximo $2q+1$ pontos em $E(F_q)$. De fato, para cada $x \in F_q$, seja $f(x) = x^3 + ax + b$, logo se $f(x)$ é um quadrado então existe $y \in F_q$ tal que $f(x) = y^2$. Assim, para cada uma das q escolhas de x, existem no máximo 2 elementos y em F_q, tal que $f(x) = y^2$, digamos $\pm y$. Portanto, existem no máximo $2q$ pares (x, y) com $x, y \in \mathbb{F}_q$ que satisfazem $f(x) = y^2$, mais o ponto no infinito $\mathcal{O}$.

Definição 4.28 *O carácter quadrático χ de F_q é uma aplicação $\chi : F_q \to \{-1,0,1\}$ tal que*

$$\chi(x) = \begin{cases} 1, & \text{se } x \text{ é um quadrado em } F_q, \\ -1, & \text{se } x \text{ é um não quadrado em } F_q, \\ 0, & \text{se } x = 0. \end{cases}$$

Por exemplo, se $q = p$ é um primo, então $\chi(x) = \left(\frac{x}{p}\right)$ é o símbolo Legendre estudado no Capítulo 1.

Por outro lado, já que só metade dos elementos de F_q^* têm raízes quadradas, seria de esperar, se $x^3 + ax + b$ são elementos aleatórios do corpo, que haveria apenas cerca da metade desse número de pontos F_q-racionais, ou seja, $|E(F_q)| \approx \frac{1}{2} \cdot (2q) + 1 = q + 1$. Assim, em todos os casos, o número de soluções $y \in F_q$ para a equação $y^2 = u$ é igual a $1 + \chi(u)$, de modo que o número de soluções para $f(x) = y^2$, ou seja, o número de pontos em $E(F_q)$, contando o ponto no infinito, é

$$1 + \sum_{x \in F_q} (1 + \chi(x^3 + ax + b)) = q + 1 + \sum_{x \in F_q} \chi(x^3 + ax + b). \tag{7}$$

Espera-se que $\chi(x^3 + ax + b)$ seja igualmente provável de resultar em 1 ou -1. Logo, tomando a soma de $\chi(x^3 + ax + b)$ acima, esta é muito parecida com um "passeio aleatório": atirar uma moeda q vezes, movendo-se um passo para frente para as caras, um passo para trás para coroa. Na Teoria de Probabilidade, se calcula que a distância real percorrida após q lançamentos é da ordem de $\sqrt{q}$. A soma $\sum \chi(x^3 + ax + b)$ se comporta um pouco como um passeio aleatório. Mais precisamente, verifica-se que esta soma é limitada por $2\sqrt{q}$. Este resultado é o *Teorema de Hasse*, o qual foi conjeturado por E. Artin e provado por Helmut Hasse em 1930.

Teorema 4.29 ***(Teorema de Hasse)*** *Seja N o número de pontos F_q-racionais sobre uma curva elíptica definida sobre F_q. Então*

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

Em outras palavras, o Teorema de Hasse diz que $E(F_q)$ tem aproximadamente $q+1$ pontos, com um erro de no máximo $2\sqrt{q}$.

Observação 4.30 *Existe ainda um outro resultado, chamado Algoritmo de Schoof, que determina essa cardinalidade com exatidão para uma curva elíptica qualquer. Este algoritmo para calcular $|E|$, foi descoberto por Rene Schoof [29], e é de tempo polinomial. O algoritmo de Schoof é ainda determinista. Baseia-se na ideia de encontrar o valor de $|E|$ módulo l para todos os primos l inferiores a um determinado limite. Isto é feito através*

da análise da ação do "Frobenius" (a aplicação da p-ésima potência) sobre os pontos de ordem l.

No artigo original de Schoof, o tempo limite de execução foi essencialmente $O(\log^8 q)$, que é polinomial mas bastante "desagradável". Em um primeiro momento, parecia que o algoritmo não era prático. No entanto, desde então, muitas pessoas têm trabalhado em acelerar o algoritmo do Schoof (V. Miller, N. Elkies, J. Buchmann, V. Müller, A. Menezes, L. Charlap, R. Coley, e D. Robbins). Além disso, A.O.L. Atkins desenvolveu um método um pouco diferente que, apesar de não garantir o trabalho em tempo polinomial, funciona extremamente bem na prática. Como resultado de todos esses esforços, tornou-se viável calcular a ordem de uma curva elíptica arbitrária sobre F_q se q é, digamos, uma potência prima de 50 dígitos, ou até mesmo de 100 dígitos.

Estrutura de $E(F_q)$

Além do número N de elementos em uma curva elíptica definida sobre F_q, podemos querer conhecer a estrutura real do grupo abeliano. Este grupo abeliano não é necessariamente cíclico, mas se pode demonstrar que é sempre um produto de dois grupos cíclicos. Isso significa que ele é isomorfo a um produto de p-grupos da forma $\mathbb{Z}/p^{\alpha}\mathbb{Z} \times \mathbb{Z}/p^{\beta}\mathbb{Z}$, onde o produto é tomado sobre os primos que dividem N. Aqui, $\alpha \geq 1$ e $\beta \geq 0$.

Definição 4.31 *Pelo **tipo do grupo abeliano de pontos F_q-racionais sobre** E, queremos dizer uma lista $(\ldots, p^{\alpha}, p^{\beta}, \ldots)_{p|N}$ das ordens dos fatores cíclicos, ou seja, dos p-grupos.*

Omitimos p^{β} quando $\beta = 0$. Nem sempre é fácil encontrar o tipo.

Exemplo 4.32 *Encontrar o tipo de $y^2 = x^3 - x$ sobre F_{71}.*

Primeiro encontramos o número de pontos N. Em (7) notamos que, na soma ,o termo para x e o termo para $-x$, se cancelam, porque $\chi((-x)^3 - (-x)) = \chi(-1)\chi(x^3 - x)$, e pela Proposição 1.24, $\chi(-1) = -1$. Assim,

$$N = 1 + q + \sum_{x \in F_{71}} \chi(x^3 - x) = 1 + q + \sum_{x} \chi(x^3 - x) + \sum_{-x} \chi(x^3 - x) = 1 + q = 72.$$

Note que, existem exatamente quatro pontos de ordem 2, incluindo a identidade $\mathcal{O}$. De fato, suponha que $P = (x,y) \in E$ tem ordem 2, ou seja, $2P = \mathcal{O}$, isto implica que $P = -P$, ou seja $(x,y) = (x,-y)$. Mas isso acontece se, e somete se, $y = 0$. Portanto, o ponto P está no eixo x. Agora, como $P = (x,0) \in E$ então $x^3 - x = 0$ de onde $x = 0, 1, -1$. Assim, os pontos $(0,0), (1,0), (-1,0) \in E$ tem ordem 2, junto com $\mathcal{O}$.

Por outro lado, note que $N = 2^3 \cdot 3^2$, portanto, pelo Primeiro Teorema de Sylow temos que E é isomorfo ao produto de um 2-grupo e um 3-grupo. Notamos que o 2-grupo

é da forma $\mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *pois este tem exatamente 4 elementos de ordem 2. Assim, o 2-grupo de E tem tipo* $(2^2, 2)$.

O 3-grupo é da forma $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *ou* $\mathbb{Z}/3^2\mathbb{Z}$*, e assim o tipo do grupo é* $(4,2,3,3)$ *ou senão* $(4,2,9)$*, dependendo se há 9 ou 3 pontos de ordem 3, respectivamente. Resta determinar se podem existir ou não 9 pontos de ordem 3. Note que para qualquer* $P \neq \mathcal{O}$ *a equação* $3P = \mathcal{O}$ *é equivalente a* $2P = \pm P$*, ou seja, a condição que a coordenada x de P e* $2P$ *são iguais, logo Por (6), isto significa que*

$$\left(\frac{3x^2-1}{2y}\right)^2 - 2x = x \implies (3x^2-1)^2 = 12xy^2 = 12x(x^3-x) = 12x^4 - 12x^2,$$

simplificando, obtemos $3x^4 - 6x^2 - 1 = 0$*. Existem no máximo 4 raízes desta equação em* F_{71}*. Se existem quatro raízes, então cada raiz pode dar no máximo 2 pontos, tomado* $y = \pm\sqrt{x^3-x}$ *se* $x^3 - x$ *tem uma raiz quadrada módulo 71, e assim podemos desta maneira obter 9 pontos de ordem 3, incluindo a identidade* $\mathcal{O}$*. Por outra parte note que se a raiz x do polinômio* $3x^4 - 6x^2 - 1 = 0$*, é tal que* $x^3 - x$ *é um quadrado módulo 71, então a raiz* $-x$ *de* $3x^4 - 6x^2 - 1 = 0$ *é tal que* $(-x)^3 - (-x) = -(x^3 - x)$ *é um não quadrado módulo 71. Assim, não podemos obter 9 pontos de ordem 3. Isso implica que deve haver menos de 9 pontos de ordem 3, e portanto exatamente 3 pontos de ordem 3. Em conclusão, o tipo do grupo é* $(4,2,9)$.

Extensões de Corpos Finitos, e a Conjectura de Weil

Se uma curva elíptica E é definida sobre F_q, então também é definida sobre F_{q^r} para $r = 1, 2, \ldots$, e por isso é significativo considerar os pontos F_{q^r}-racionais, ou seja, olhar para soluções de (2) sobre os corpos de extensão. Se começarmos com F_q como o corpo sobre o qual E é definida, denotamos por N_r o número de pontos F_{q^r}-racionais sobre E. Assim, $N_1 = N$ é o número de pontos com coordenadas em nosso "corpo base" F_q.

Definição 4.33 *A função zeta da curva elíptica E sobre* F_q *denotada por* $Z(T; E/F_q)$*, se define partir dos números* N_r *por meio da série de potências formais em* $\mathbb{Q}[[T]]$ *dada pela fórmula*

$$Z(T; E/F_q) = e^{\sum N_r T^r / r}, \tag{8}$$

onde T é uma variável.

A função zeta é um objeto muito importante associado à E. A notação E/F_q designa a curva elíptica e o corpo que estamos tomando como nosso corpo base, e a soma da direita está sobre todas as $r = 1, 2, \ldots$.

Em 1949, André Weil fez uma série de conjeturas acerca da função zeta num contexto mais geral (variedades algébricas de qualquer dimensão). Em particular, ele

afirmou que a função zeta tem uma forma "muito especial". No caso de uma curva elíptica E/F_q Weil demostrou o seguinte:

Teorema 4.34 ***(Conjetura de Weil)*** *$Z(T;E/F_q)$ é uma função racional em T, com coeficientes em $\mathbb{Z}$, que tem a forma*

$$Z(T;E/F_q) = \frac{1-aT+qT^2}{(1-T)(1-qT)}. \tag{9}$$

Entre outras coisas, a conjetura de Weil para curvas elípticas é útil para determinar o número de pontos sobre extensões de corpos de um grande grau. Sobre o quadrático $1-aT+qT^2$ podemos fazer as seguintes observações:

1. O inteiro a depende da curva elíptica E particular e se relaciona com $N = N_1$ como segue: $N = q+1-a$.

2. O discriminante do polinômio é negativo, ou seja, $a^2 < 4q$; que é o teorema de Hasse.

3. O quadrático tem duas raízes complexas conjugadas α, β ambas de valor absoluto $\sqrt{q}$.

4. Se $1/\alpha$ e $1/\beta$ são as raízes do polinômio, e α, β são as "raízes reciprocas" então podemos ver que $1-aT+qT^2 = (1-\alpha T)(1-\beta T)$, de onde temos $\alpha\beta = q$ e $\alpha+\beta = a$.

Observação 4.35 *Se escrevemos $1-aT+qT^2 = (1-\alpha T)(1-\beta T)$ podemos ver que a fórmula (9) é equivalente a escrever a sequência de relações*

$$N_r = q^r + 1 - \alpha^r - \beta^r, \qquad r = 1,2,\ldots. \tag{10}$$

De fato, pela definição de $Z(T;E/F_q)$ temos

$$e^{\sum N_r T^r/r} = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

tomando logaritmo natural a ambos lados da igualdade:

$$\sum \frac{N_r T^r}{r} = \ln(1-\alpha T) + \ln(1-\beta T) - \ln(1-T) - \ln(1-qT),$$

agora, derivamos respeito a T e obtemos

$$\sum N_r T^{r-1} = -\frac{\alpha}{1-\alpha T} - \frac{\beta}{1-\beta T} + \frac{1}{1-T} + \frac{q}{1-qT},$$

e usando a serie geométrica em cada uma das parcelas da direita

$$\sum N_r T^{r-1} = -\sum \alpha(\alpha T)^{r-1} - \sum \beta(\beta T)^{r-1} + \sum T^{r-1} + \sum q(qT)^{r-1},$$

daí,

$$\sum N_r T^{r-1} = \sum (q^r + 1 - \alpha^r - \beta^r) T^{r-1}.$$

Note então agora que de 1. e 4. temos $\alpha\beta = q$ e $\alpha + \beta = q + 1 - N$, assim, uma vez que conheçamos $N = N_1$ podemos encontrar facilmente α e β, e com esse valores, da igualdade (10), ficam determinados todos os valores de N_r para todo $r = 1, 2, 3, \ldots$. Isto significa que o número de pontos F_q-racionais determina o número de pontos sobre qualquer corpo de extensão.

Exemplo 4.36 *A função zeta da curva elíptica $y^2 + y = x^3$ sobre F_2 é facilmente calculada do fato que existem três pontos F_2-racionais. Assim de $N = q + 1 - a$ temos que $a = 0$. Isto é, $(1 + 2T^2)/(1 - T)(1 - 2T)$, por outra parte, as raízes reciprocas do numerador são $\pm i\sqrt{2}$. Portanto $N_r = 2^r + 1 - (-i\sqrt{2})^r - (i\sqrt{2})^r$ para $r = 1, 2, \ldots$. Isto conduz à fórmula*

$$N_r = \begin{cases} 2^r + 1, & \text{se } r \text{ é impar;} \\ 2^r + 1 - 2(-2)^{r/2}, & \text{se } r \text{ é par.} \end{cases}$$

Observamos que há muitas analogias entre o grupo de pontos F_q-racionais de uma curva elíptica e o grupo multiplicativo F_q^*. Por exemplo, eles têm aproximadamente o mesmo número de elementos, pelo teorema de Hasse. Mas a primeira construção tem uma grande vantagem que explica a sua utilidade em criptografia: para um único (grande) q existem muitas curvas elípticas diferentes e muitos N diferente que se pode escolher. As curvas elípticas oferecem uma rica fonte de grupos abelianos finitos de "ocorrência natural" o qual é aproveitado de maneira significativa na criptografia.

4.2 Criptografia de Curvas Elípticas

No Capítulo 3 vimos como o grupo abeliano finito F_q^* pode ser usado para criar sistemas de criptografia da chave pública. Mais precisamente, foi a dificuldade de resolver o problema do logaritmo discreto em corpos finitos que nos levaram aos sistemas criptográficos discutidos aí. O objetivo desta seção é descrever sistemas de chave pública análogas, com base no grupo abeliano finito de uma curva elíptica E definido sobre F_q. (Esta seção é baseada no artigo principal deste trabalho, [14].)

Como já vimos no Capítulo 3, antes de usar nossos sistemas criptográficos, precisamos "etiquetar" todas as possíveis unidades de mensagens de texto original e todas

as possíveis unidades de mensagem de texto cifrado por meio de objetos matemáticos, neste caso, tais objetos são pontos em uma determinada curva elíptica. Antes de descrever esses análogos, vamos estudar como "etiquetar" mensagens.

4.2.1 Incorporação de Textos Originais

Queremos codificar nossos textos originais como pontos em alguma curva elíptica E dada, definida sobre um corpo finito F_q. O objetivo é fazer isso de uma maneira sistemática simples, para que o texto original m (o que podemos considerar como um inteiro em algum intervalo) possa ser facilmente determinado a partir do conhecimento das coordenadas do ponto correspondente P_m. Observe que essa "codificação", não é a mesma coisa que encriptação. Mais adiante, vamos discutir formas de encriptar pontos P_m de texto original, mas de modo que um usuário autorizado do sistema seja capaz de recuperar m, após de decifrar o ponto de texto cifrado. Há duas observações que devem ser feitas aqui:

1. Não existe um algoritmo determinístico (ou seja, um algoritmo em que, dada uma certa entrada, produzirá sempre a mesma saída, com a máquina responsável sempre passando pela mesma sequência de estados), conhecido para escrever um grande número de pontos em uma curva elíptica arbitrária E sobre F_q em tempo polinomial em $\log q$. No entanto, existem algoritmos probabilísticos para os quais a chance de fracasso é muito pequena, como veremos na continuação.

2. Não é suficiente gerar pontos aleatórios de E: a fim de codificar um grande número de mensagens possíveis m, precisamos de uma maneira sistemática para gerar pontos que estão relacionados com m de alguma forma, por exemplo a coordenada x tendo uma relação simples com o inteiro m.

Vamos agora descrever vários métodos para incorporar texto originais numa curva elíptica E definida sobre F_q, onde $q = p^n$ é suficientemente grande.

Método 1

Este é um método probabilístico para incorporar textos originais, onde vamos supor que $q = p^r$. Seja κ um inteiro suficientemente grande, de modo que estejamos "satisfeitos" com a probabilidade de fracasso de 1 para cada 2^κ, quando tentamos incorporar uma unidade de mensagem de texto original m; na prática $\kappa = 30$ ou, na pior das hipóteses, $\kappa = 50$ deve ser suficiente. Supomos que nossas unidades de mensagem m são inteiros $0 \leq m < M$. Supomos também que o nosso corpo finito escolhido é de modo que $q > M\kappa$.

Escrevemos os inteiros de 1 até $M\kappa$ na forma $m\kappa + j$, onde $1 \leq j \leq \kappa$, e montamos a seguente correspondência de 1-1

$$\{1 \leq y \leq M\kappa \ : y = m\kappa + j, 1 \leq j \leq \kappa \} \longrightarrow F_q. \tag{11}$$

Por exemplo, escrevemos um inteiro como um número de r dígitos na base p, e tomar os r dígitos, considerados como elementos de $\mathbb{Z}/p\mathbb{Z}$, como os coeficientes de um polinômio de grau $r-1$ correspondente a um elemento de F_q. Temos assim a correspondência

$$(a_{r-1}a_{r-2}\cdots a_1a_0)_p \longmapsto \sum_{i=0}^{r-1} a_i X^i,$$

o polinômio à direita considerado módulo algum polinômio irredutível de grau r fixado sobre F_q, dá um elemento de F_q.

Assim, dado m, para cada $j = 1,2,\ldots,\kappa$ obtemos um elemento x de F_q que corresponde a $m\kappa + j$. Para esse tal x, calculamos o lado direito da equação

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

e tentamos encontrar uma raiz quadrada de $f(x)$. Se encontramos um y tal que $y^2 = f(x)$, tomamos $P_m = (x,y)$. Se acontece que $f(x)$ é um não-quadrado, então incrementamos j por 1 e tentamos de novo com o correspondente x. Desde que encontrar um x para o qual $f(x)$ é um quadrado antes de j se torna maior do que κ, podemos recuperar m do ponto (x,y) pela fórmula $m = [(\tilde{x}-1)/\kappa]$, onde $\tilde{x}$ é o número inteiro que corresponde a x sob a correspondência (11). Já que $f(x)$ é um quadrado para aproximadamente 50% de todos os x, há apenas uma probabilidade aproximada de $2^{-\kappa}$ de que este método vai deixar de produzir um ponto P_m, cuja coordenada x corresponde a um número inteiro $\tilde{x}$, entre $m\kappa+1$ e $m\kappa+\kappa$. Mais precisamente, a probabilidade de $f(x)$ ser um quadrado é essencialmente igual a $N/2q$, mas $N/2q$ é muito próximo de 1/2.

Método 2

Suponhamos que p é arbitrário (por exemplo, 2) e $n = 2n'$ é par. Suponha que os nossos textos originais são inteiros m, $0 \leq m < p^{n'}$ escritos na forma

$$m = m_0 + m_1 p + \cdots + m_{n'-1}p^{n'-1}; \ \ 0 \leq m_j < p,$$

e seja $b_0,\ldots,b_{n'-1}$ uma base conveniente do espaço vectorial $F_{p^{n'}}$ sobre F_p. Seja

$$x(m) = m_0b_0 + m_1b_1 + \cdots + m_{n'-1}b_{n'-1} \in F_{p^{n'}},$$

e seja $y(m) \in F_{p^n}$ uma solução da equação quadrática (2) ou (3) que define pontos em E. Definimos então

$$P_m = (x(m), y(m)) \in E,$$

uma tal solução $y(m)$ é garantida existir, pelo fato de que F_{q^n} é uma extensão de grau 2 sobre $F_{q^{n'}}$, portanto uma equação de grau 2 tem solução em F_{q^n}.

Método 3

Suponha que $n = 1$ e seja $q = p \equiv 3 \pmod 4$, E é dada pela equação (2). Suponha que nossos textos originais são inteiros m, tais que $0 \leq m < p/1000 - 1$. Tentamos adicionar três dígitos a m até obtermos um x, tal que $1000m \leq x < 1000(m+1) < p$ e $f(x) = x^3 + ax + b$ é um quadrado em F_p. Então defina

$$P_m = \left(x, f(x)^{(p+1)/4}\right) \in E.$$

Note que $P_m \in E$, de fato, como $f(x)$ é um quadrado em F_p então existe $w \in F_p$ tal que $w^2 = f(x)$, logo

$$\left(f(x)^{(p+1)/4}\right)^2 = f(x)^{(p+1)/2} = (w^2)^{(p+1)/2} = w^{p+1} = w^p w = w^2 = f(x).$$

Por outra parte, note que é fácil recuperar m a partir P_m, simplesmente deixando cair os últimos três dígitos da coordenada x. Este é uma incorporação probabilística de $\{m\}$ em E, já que existe uma probabilidade minúscula de que $f(x)$ será um não quadrado para todo $1000m \leq x < 1000(m+1)$.

Método 4

Seja $p = 2$ e $n \equiv 4 \pmod 6$, considere $b_0, \ldots, b_{n-1}$ uma base conveniente do espaço vetorial F_{2^n} sobre F_2, e seja E dada pela equação

$$E : y^2 + y = x^3, \tag{12}$$

suponha que nossos textos originais estão no intervalo $m < 2^{n-10}$, e escreva m como um inteiro de $n-10$ dígitos na base 2

$$m = m_0 + m_1 2 + \cdots + m_{n-11} 2^{n-11};\ m_j \in \{0,1\},$$

e defina

$$y = m_0 b_0 + \cdots + m_{n-11} b_{n-11} + m_{n-10} b_{n-10} + \cdots + m_{n-1} b_{n-1} \in F_{2^n},$$

onde $m_{n-10},\ldots,m_{n-1} \in \{0,1\}$; se y^2+y é um cubo em F_{2^n}, então o ponto (x,y) esta em E para $x=(y^2+y)^{(2^n+2)/9}$, já que existe $z \in F_{2^n}$ tal que $z^3 = y^2+y$, logo

$$x^3 = (y^2+y)^{(2^n+2)/3} = (z^3)^{(2^n+2)/3} = z^{2^n+2} = z^{2^n}z^2 = z^3 = y^2+y.$$

Defina então

$$P_m = (x,y).$$

4.2.2 Logaritmo Discreto sobre E

No Capítulo 3 discutimos sistemas criptográficos de chave pública baseada no problema do logaritmo discreto, no grupo multiplicativo de um corpo finito. Agora vamos fazer o mesmo no grupo aditivo de uma curva elíptica E definida sobre um corpo finito F_q.

Definição 4.37 *Se E é uma curva elíptica sobre F_q e B é um ponto de E, então, o problema de* log *discreto em E, na base B, é o seguinte: dado um ponto $P \in E$, encontrar um inteiro x tal que $xB = P$, se tal x existir.*

É provável que o problema do log discreto sobre curvas elípticas seja mais intratável do que o problema do log discreto em corpos finitos. As técnicas mais fortes desenvolvidos para uso em corpos finitos não parecem funcionar em curvas elípticas. Isto é especialmente verdadeiro no caso de corpos com característica 2. Métodos especiais para resolver o problema de log discreto em $F_{2^r}^*$ tornam relativamente fácil calcular logaritmos discretos e, portanto, quebrar os sistemas criptográficos discutidos no Capítulo 3, a menos que r seja escolhido bastante grande. Parece que os sistemas análogos utilizando curvas elípticas definidas sobre F_{2^r} serão seguros com valores significativamente menores de r. Já que existem razões práticas (relacionados com hardware e software de computador) para preferir fazer contas sobre os corpos $F_{2^r}^*$, os sistemas criptográficos de chave pública discutidos abaixo podem vir a ser mais convenientes em aplicações do que os sistemas baseados no problema de log discreto em F_q^*.

Uma das principais vantagens de sistemas de criptografia de curvas elípticas é que nenhum algoritmo sub-exponencial é conhecido para quebra o sistema, desde que evitamos curvas supersingulares[1] e também curvas cuja ordem não tem grande fator primo.

Descrevemos agora análogos dos sistemas de chave pública do Capítulo 3 baseado em o problema de log discreto em uma curva elíptica E definida sobre um corpo finito F_q.

[1] Uma curva elíptica E definida sobre F_{p^r} é dita supersingular se $|E| \equiv 1 \pmod{p}$.

Análogo do Sistema de Troca de Chaves Diffie-Hellman

Suponha que Aida e Bernardo querem acordar uma chave que será posteriormente utilizada em conjunto com um sistema de criptografia clássica. Eles primeiro escolhem publicamente um corpo finito F_q e uma curva elíptica E definida sobre ele. A sua chave será construída a partir de um ponto aleatório P na curva elíptica. Por exemplo, se eles têm um ponto aleatório $P \in E$, então, tendo a coordenada x do P dá um elemento aleatório de F_q, que pode, então, ser convertido a um inteiro aleatório de r dígitos na base p, onde $q = p^r$; que serve como a chave para o seu sistema de criptografia clássica. Sua tarefa é escolher o ponto P de tal maneira que toda a sua comunicação, com os outros é pública e ainda ninguém além de os dois conhece P.

Aida e Bernardo primeiro escolhem publicamente um ponto $B \in E$ para servir como sua "base". B desempenha o papel do gerador g no sistema de Diffie-Hellman para um corpo finito. No entanto, não queremos insistir em que B seja um gerador do grupo de pontos em E. Na verdade, o último grupo pode deixar de ser cíclico. Mesmo que seja cíclico, queremos evitar o esforço de verificar se B é um gerador, ou até mesmo determinar o número N de pontos, que não precisamos de saber no que se segue. Gostaríamos que o subgrupo gerado por B seja grande, de preferência, da mesma ordem de grandeza como a própria E, ou um grande divisor de N. Para gerar uma chave se procede com segue:

1. Aida primeiro escolhe um número aleatório a da ordem de grandeza q (que é aproximadamente o mesmo que N), o qual ela mantém secreto. Ela calcula $aB \in E$, que ela torna público.

2. Bernardo faz o mesmo: ele escolhe um aleatório b e torna público $bB \in E$.

3. A chave secreta que eles usam é então $P = abB \in E$.

Ambos usuários podem calcular esta chave. Por exemplo, Aida conhece bB (que é de conhecimento público) e seu próprio a segredo. No entanto, um terceiro conhece apenas aB e bB. Sem resolver o problema do logaritmo discreto — encontrar a conhecendo B e aB (ou encontrar b conhecendo B e bB) — parece haver nenhuma maneira de calcular abB conhecendo apenas aB e bB.

Análogo de Massey-Omura

Tal como na situação de corpo finito, isto é um sistema de encriptação de chave pública para a transmissão de unidades de mensagem m, que agora suponha que foram incorporados como pontos P_m em alguma curva elíptica fixa E sobre F_q (onde q é grande), a qual é conhecida publicamente . Também supomos que o número de pontos N sobre E foi calculado, e também é conhecido publicamente. Cada usuário do sistema secretamente

escolhe um número inteiro e aleatório entre 1 e N tal que $mdc(e,N) = 1$ e, utilizando o algoritmo de Euclides, calcula a seu inverso $d = e^{-1} \pmod{N}$, isto é, um número inteiro d tal que $de \equiv 1 \pmod{N}$. Se Ayrton (A) quer enviar o mensagem P_m para Bryon (B), ele prossegue da seguente forma:

1. Ele envia para Bryon o ponto $e_A P_m$.

Isso não significa nada para Bryon, que, sabendo nem d_A nem e_A, não pode recuperar P_m. Mas, sem tentar dar sentido a este ponto,

2. ele multiplica por seu e_B, e envia $e_B e_A P_m$ de volta para Ayrton.

3. O passo final é para Ayrton desfazer a parte da mensagem através da multiplicação do ponto $e_B e_A P_m$ por d_A. Dado que $NP_m = \mathcal{O}$ e $d_A e_A \equiv 1 \pmod{N}$, isso dá o ponto $e_B P_m$, que Ayrton retorna ao Bryon, o qual pode ler a mensagem através da multiplicação do ponto $e_B P_m$ por d_B.

Observe que um intruso conheceria $e_A P_m$, $e_B e_A P_m$ e $e_B P_m$. Se esse intruso poderia resolver o problema de log discreto sobre E, então poderia determinar e_B dos dois primeiros pontos e depois calcular $d_B = e_B^{-1} \pmod{N}$ e $P_m = d_B(e_B P_m)$.

Exemplo 4.38 *Seja E dada pela equação $y^2 + y = x^3$ sobre F_{2^n}, onde $n \equiv 4 \pmod{6}$. Suponha que temos um simples método (probabilística) de incorporação $m \mapsto P_m$ de textos originais em E. Esta E também é conveniente para outras razões. As fórmulas para duplicar um ponto são particularmente simples:*

$$2P = (x^4, y^4 + 1), \quad \textit{para } P = (x,y),$$

o qual decorre do fato que $Char(F_{2^n}) = 2$. Além disso, existe uma fórmula fácil para $N = |E|$, neste caso:

$$N = 2^n + 1 - 2(-2)^{n/2} = \left((-2)^{n/2} - 1\right)^2.$$

Por outra parte, a fim de assegurar que N é divisível por um grande primo, podemos, por exemplo, escolher n de forma que $n/4 \equiv 1 \pmod{3}$ dá um número de Mersenne com um fator grande, por exemplo, um primo de Mersenne (por exemplo, $n = 508$).

Análogo de ElGamal

Este é um outro sistema de criptografia de chave pública para transmitir mensagens P_m. Como no sistema de troca de chave acima, começamos com um corpo finito fixo

F_q de conhecimento público, e uma curva elíptica E definido sobre ele, e o ponto base $B \in E$, note que não precisamos de saber o número de pontos N. Cada usuário escolhe um inteiro aleatório a, que é mantido em segredo, e calcula e publica o ponto aB.

Para enviar uma mensagem P_m para Bryon (B), Aida (A) prossegue da seguente maneira:

1. Aida escolhe um inteiro aleatório k,
2. Aida calcula o elemento $P_m + k(a_B B)$, e
3. envia para Bryon o par de pontos $(kB, P_m + k(a_B B))$, onde $a_B B$ é a chave pública de Bryon.

Para ler a mensagem, Bryon faz o seguente:

1. Multiplica o primeiro ponto no par por seu segredo a_B
2. logo subtrai o resultado do segundo ponto:

$$P_m + k(a_B B) - a_B(kB) = P_m.$$

Assim, Aida envia um P_m disfarçada, juntamente com uma "pista" kB que é suficiente para remover a "máscara" $ka_B B$ se alguém conhece o inteiro segredo a_B. Um intruso que pode resolver o problema de log discreto sobre E pode, é claro, determinar a_B das informações publicamente conhecidas B e $a_B B$.

Exemplo 4.39 *Dado $q = p^n$, escolha tanto E e B aleatoriamente. Por exemplo, vamos definir*

$$g(y) = \begin{cases} y^2, & \text{se } p > 2; \\ y^2 + y, & \text{se } p = 2. \end{cases}$$

Em seguida, escolha aleatoriamente elementos $x, y, a \in F_{p^n}$, e defina $b = g(y) - x^3 - ax$. Então,

$$B = (x,y) \in \begin{cases} y^2 = x^3 + ax + b, & \text{se } p > 2; \\ y^2 + y = x^3 + ax + b, & \text{se } p = 2. \end{cases}$$

Note que o discriminante da equação deve ser diferente de zero, mas esto é virtualmente certo se a e b são elementos aleatórios de um grande corpo finito.

Antes de usar a escolha E e B, deve-se verificar que a ordem de B em E não é um inteiro suave; se um produto de primos pequenos torna B a identidade (o ponto no infinito), em seguida, uma outra escolha aleatória deve ser feita.

Análogo da Assinatura Digital Padrão

O algoritmo de Assinatura Digital de curva elíptica ECDSA, é implementado ao longo da curva elíptica P-192, conforme estipulado pela ANSI X9.62 em linguagem C. O projeto contém módulos necessários para o domínio geração de parâmetros, geração de chaves, geração de assinatura e a verificação de assinatura sobre a curva elíptica. Para mais detalhes ver [12].

ECDSA tem três fases, geração de chaves, geração de assinatura e verificação de assinatura, como seu análogo.

Geerando Chaves.

Um par de chaves do usuário A está associado com um conjunto particular de domínio de parâmetros CE, $D = (q, FR, a, b, G, n, h)$. Onde, E é uma curva elíptica definida sobre o corpo finito de q elementos, G é um ponto de ordem prima n em $E(F_q)$, h é o cofator $|E(F_q)|/n$, e FR é o acrônimo inglês de Field Representation, e indica a representação usada para os elementos de F_q. Cada entidade A faz o seguinte:

1. Escolhe um inteiro aleatório d no intervalo $[1, n-1]$.
2. Calcula $Q = dG$.
3. A chave publica de A é Q, a chave privada de A é d.

Gerando a Assinatura.

Para enviar uma mensagem m, uma entidade A como domino de parâmetros $D = (q, FR, , a, b, G, n, h)$ faz o seguinte;

1. Escolha um inteiro aleatório k no intervalo $[1, n-1]$.
2. Calcula $kG = (x_1, y_1)$, e $r = x_1 \pmod{n}$ (onde x_1 é considerado como um inteiro entre 0 e $q-1$). Se $r = 0$ então volte para o passo 1.
3. Calcule $k^{-1} \pmod{n}$.
4. Calcule $s = k^{-1}\{h(m) + dr\} \pmod{n}$, onde h é uma função Hash, `SHA-1` . Se $s = 0$, então volte pro passo 1.
5. A assinatura para a mensagem m é o par de inteiros (r, s).

Verificando a Assinatura.

Para verificar a assinatura de A, (r, s) em m, B obtém uma copia autenticada do domínio parâmetros de A, $D = (q, FR, a, b, G, n, h)$ e a chave publica Q, e faz o seguinte:

1. Verifica que r e s são inteiros no intervalo $[1, n-1]$.

2. Calcula $w = s^{-1} \pmod{n}$ e $h(m)$.

3. Calcula $u_1 = h(m)w \pmod{n}$ e $u_2 = rw \pmod{n}$.

4. Calcula $u_1G + u_2Q = (x_0, y_0)$ e $v = x_0 \pmod{n}$.

5. B aceita a assinatura se, e somente se, $v = r$.

4.2.3 Escolha da Curva e o Ponto

Existem várias maneiras de escolher uma curva elíptica e um ponto B sobre ela, nos esquemas Diffie-Hellman e ElGamal.

Seleção aleatória de (E, B)

Uma vez que escolhemos o nosso grande corpo finito F_q, podemos escolher E e $B = (x, y) \in E$, ao mesmo tempo como se segue. Vamos assumir que a característica do corpo é > 3, de modo que as curvas elípticas são dadas pela equação (2). Primeiro sejam x, y, a três elementos aleatórios de F_q. Em seguida, defina $b = y^2 - (x^3 + ax)$. Verifique se o cúbico $x^3 + ax + b$ não tem raízes múltiplas, o que é equivalente a: $4a^3 + 27b^2 \neq 0$. Se esta condição não for cumprida, fazer uma outra escolha aleatória de x, y, a. Defina $B = (x, y)$. Então B é um ponto da curva elíptica $y^2 = x^3 + ax + b$.

Reduzir um global (E, B) módulo p

Agora mencionamos uma segunda maneira de determinar um par consistindo de uma curva elíptica e um ponto sobre ela. Primeiro escolhemos uma vez por todas uma curva elíptica"global" e um ponto de ordem infinita nela. Assim, seja E uma curva elíptica definida sobre o corpo de números racionais (ou, mais generalmente, poderíamos usar uma curva elíptica definida sobre um corpo numérico), e seja B um ponto de ordem infinita em E.

Em seguida, escolhemos um grande primo p (ou, se a nossa curva elíptica é definida através de um corpo de extensão K de $\mathbb{Q}$, então escolhemos um ideal primo de K) e consideramos a redução de E e B módulo p. Mais precisamente, para todo p exceto para alguns pequenos primos, os coeficientes na equação para E não têm nenhum p em seus denominadores, por isso, podemos considerar os coeficientes nesta equação módulo p. Se fizermos uma mudança de variáveis tomando a equação resultante sobre F_p com a forma $y^2 = x^3 + ax + b$, o cubo da direita não tem raízes múltiplas (exceto no caso de poucos pequenos primos p), e assim dá uma curva elíptica sobre F_p, que vamos denotar $E \pmod{p}$. As coordenadas de B também irá reduzir módulo p para dar um ponto sobre a curva elíptica e $E \pmod{p}$, que denotamos $B \pmod{p}$.

Exemplo 4.40 *Considere as curvas elípticas* $E_1: y^2+y=x^3-x$, *e* $E_2: y^2+y=x^3+x^2$ *sobre* F_p, *para p um grande primo, e escolha* $B=(0,0)$. *Então, se consideramos as curvas elípticas* E_1, E_2 *sobre o corpo dos números racionais, temos que B é um ponto de ordem infinita e de fato gera todo o grupo de pontos racionais sobre cada curva.*

Quando usamos este segundo método, fixamos E e B, uma vez por todas, e então obtemos muitas possibilidades diferentes variando o primo p.

Pontos primitivos

Definição 4.41 *Um número inteiro m é dito suave se é divisível por primos pequenos. Porem, m é não suave, se é divisível por um primo grande .*

Em sistemas criptográficos de curva elíptica do tipo discutido acima, não se trabalha com todo o grupo E, mas sim com subgrupos cíclicos: os grupos $\langle P_m\rangle$ no sistema Massey-Omura e o grupo $\langle B\rangle$ no sistema ElGamal. É desejável que os grupos $\langle P_m\rangle$ e $\langle B\rangle$ sejam grandes, isto é, para o seu índice em E ser pequeno. Mais precisamente, a fim de estes subgrupos cíclicos deveriam ser não suaves, a fim de evitar fácil solução do problema do logaritmo discreto em eles.

Em nossos exemplos 4.38, 4.39, P ou é um ponto "aleatório" escolhido depois de ter especificado q ou senão um ponto global B como no Exemplo 4.40, ou seja, um ponto fixo de ordem infinita em uma curva elíptica $E_{\mathbb{Q}}$ definida sobre os números racionais que é então reduzida módulo p depois que escolher algum grande p e decidir trabalhar com $E_{F_p}=E \pmod p$. Em ambos os casos, é natural fazer as seguentes perguntas:

1. Qual é a probabilidade quando o p varia de acordo com G fixo, ou como p e o "aleatório" G ambos variam, que G gera $E \pmod p$?

   Ou, se não podemos contar com isso acontecer com frequência suficiente , poderíamos perguntar:

2. Qual é a probabilidade, se $|E \pmod p|$ é divisível por um grande primo ℓ, que $|\langle G \pmod p\rangle|$ também será divisível por ℓ?

A primeira questão é o análogo para curva elíptica do problema de raiz primitiva para F_p que foi considerado por E. Artin, ver [31], [23] e [38] para mais detalhes.

A conjetura de Artin nos diz o seguinte: seja $a\neq 0,\pm 1$ um número inteiro fixo, que não é da forma $\pm b^n$ para qualquer $n>1$, então a é uma raiz primitiva módulo p para uma infinidade de primos p. Artin observou que se pode usar o teorema da densidade de Chebotarev (para detalhes sobre este teorema, ver [35]) para mostrar que, para qualquer primo ℓ, a probabilidade que ℓ divide o índice de $\langle a\rangle$ em F_p^*, ou equivalentemente, que

$$\ell | p-1 \quad \text{e} \quad a^{(p-1)/\ell}\equiv 1 \pmod p,$$

é igual a $1/(\ell(\ell-1))$. Então, ele conjecturou que estes eventos são independentes para diferentes ℓ, no caso da probabilidade de que a é um gerador, ou seja, que nenhum primo ℓ divide o índice de a em F_p^* o qual, é igual

$$\prod_{\text{primos } \ell} \left(1 - \frac{1}{\ell(\ell-1)}\right) = 0.3729\ldots. \tag{13}$$

Mais tarde, foi notado que esses eventos não são necessariamente independentes, e com certeza, alguns dos fatores em (13) devem ser modificados . Por exemplo, o número que tem a maior probabilidade de ser um gerador é $a = -3$, onde esta probabilidade é obtida pela eliminação do termo $\ell = 3$ em (13). Em particular, já que -3 é um quadrado e, portanto, não um gerador quando $p \equiv 1 \pmod 3$, segue-se que -3 é um gerador de F_p^* para 89,7% de todo $p \equiv 2 \pmod 3$. A conjectura modificada de Artin foi mostrada por C. Hooley em 1967, assumindo a hipótese de Riemann generalizada (GRH).

No caso de uma curva elíptica, um análogo da conjectura de Artin foi proposto por Lang e Trotter [17]. Seja E uma curva elíptica fixa definida sobre $\mathbb{Z}$ com discriminante Δ, e seja $p_1, p_2, \ldots$ uma sequência crescente de números primos com os primos que dividem Δ omitidos. Seja G um ponto fixo de ordem infinita em E que não é da forma nG' para qualquer $n > 1$. Se diz que G é "primitivo para p" se $G \pmod p$ gera $E \pmod p$. Seja $f(n)$ a proporção dos primeiros n primos para os quais G é primitiva:

$$f(n) = f_{E,G}(n) = \frac{1}{n}|\{j \leq n \ : \ G \text{ é primitiva para } p_j\}|.$$

Então Lang e Trotter conjecturaram que $f(n)$ se aproxima um limite diferente de zero e descreveram como determinar esse limite. No caso de as três curvas elípticas

$$A : y^2 + y = x^3 - x, \ \ B : y^2 + y = x^3 + x^2, \ \ C : y^2 + xy + y = x^3 - x^2 \tag{14}$$

e o ponto $G = (0,0)$, eles conjecturaram o seguinte valor:

$$\lim_{n\to\infty} f(n) = \prod_{\ell} \left(1 - \frac{\ell^3 - \ell - 1}{\ell^2(\ell-1)(\ell^2-1)}\right) \approx 0.440.$$

Esta conjectura supõe que os acontecimentos $\ell | [E \bmod p : \langle G \bmod p \rangle]$ são independentes para diferentes ℓ.

No caso de curvas elípticas com multiplicação complexa, uma versão mais fraca da conjectura de Lang-Trotter (onde se deve ignorar primos p que não dividem no corpo de multiplicação complexa) foi provado por Gupta e Murty [9] assumindo a GRH. Serre [30],ver também [23], assumindo a GRH, provou um resultado semelhante sobre a questão da ciclicidade de $E \pmod p$: A proporção de p para o qual $E \pmod p$ é um

grupo cíclico se aproxima uma constante diferente de zero.

Lang e Trotter testaram sua conjectura nos casos (14), e $G = (0,0)$ para os primeiros 200 números primos. Os resultados não foram muito perto do valor previsto de 88 números primos para as quais G é primitiva (os números foram 91, 96 e 91, respectivamente; os cálculos mostram que estes números devem ser corrigidos para 92, 96, 92), de modo que então descartados os primeiros vinte p_j, e contou a proporção dos restantes 180. No intervalo p_j, $20 < j \leq 200$, de acordo com a proporção prevista era bastante bom. Trotter estendeu estes cálculos para os primeiros 2000 números primos, obtendo dados estatísticos mais convincentes apoiando a conjectura para as curvas (14).

Subgrupos cíclicos não suaves

A segunda pergunta sobre o índice de $\langle G \pmod p \rangle$ em $E \pmod p$ é mais fraca: se ter garantido que $|E \pmod p|$ é não suave e se sabe que este é divisível por um grande primo ℓ, então qual é a probabilidade de que $|\langle G \pmod p \rangle|$ também é divisível por ℓ? A menos que $\ell^2 || E \pmod p|$, o que não é provável para ℓ grande, isto é equivalente a perguntar sobre a probabilidade de que ℓ divide o índice de $\langle G \pmod p \rangle$ em $E \pmod p$. Em outras palavras, para E, G e ℓ fixos, qual é a probabilidade condicional que $\ell | [E \pmod p : \langle G \pmod p \rangle]$ dado que $\ell || E \pmod p|$? Seguindo o argumento em [17] e usando o teorema da Densidade de Chebotarev e resultados de Serre e Bashmakov para curvas não-CM, tem-se a seguinte resposta.

Teorema 4.42 *Seja G um ponto fixo de ordem infinita numa curva elíptica E de discriminante Δ a qual é definida sobre $\mathbb{Z}$ e não tem multiplicação complexa. Então, para todos exceto um número finito de primos ℓ,*

$$\lim_{x\to\infty} \frac{|\{\textit{primos } p \leq x, p \not| \Delta \,;\, \ell \textit{ divide } [E \pmod p : \langle G \pmod p \rangle]\}|}{|\{\textit{primos } p \leq x, p \not| \Delta \,;\, \ell \textit{ divide } |E \pmod p|\}|} = \frac{\ell^3 - \ell - 1}{\ell^2(\ell^2-2)} = \frac{1}{\ell} + O\left(\frac{1}{\ell^3}\right).$$

Corolário 4.43 *Baixo as condições do teorema acima, para todo, exceto um número finito de primos ℓ,*

$$\lim_{x\to\infty} \frac{|\{\textit{primos } p \leq x, p \not| \Delta \,;\, \ell \textit{ divide } |\langle G \pmod p \rangle|\}|}{|\{\textit{primos } p \leq x, p \not| \Delta \,;\, \ell \textit{ divide } |E \pmod p|\}|} = 1 - \frac{1}{\ell} + \frac{1}{\ell^2} + O\left(\frac{1}{\ell^3}\right).$$

No corolário, o adicional termo ℓ^{-2} decorre da possibilidade de que $\ell^2 || E \pmod p|$. Finalmente, observamos que a essência dessas conjecturas e resultados parciais é que, apesar de $|E \pmod p|$ aumenta com p, o índice $[E \pmod p : \langle G \pmod p \rangle]$, em média, não. Assim, para extremamente grandes p, o subgrupo gerado por G pode ser esperado ser quase "bom" (isto é, não suave) como E em si.

CAPÍTULO 5

Aplicação das Curvas Elípticas á Fatoração e Teste de Primalidade

Desde os tempos antigos, há dois problemas fundamentais na teoria dos números que mantém ocupados muitos importantes matemáticos, e ainda são motivo de pesquisa: o primeiro é decidir se um determinado número inteiro é primo ou não, e o segundo, se esse número não é primo, expressá-lo como um produto de seus fatores primos próprios. Atualmente vários métodos de fatoração e testes de primalidade são conhecidos, mas a principal razão de pesquisa em torno destes problemas é a procura de métodos e algoritmos que sejam executados em tempo polinomial.

Neste capítulo, apresentamos um teste de primalidade devido a Glodwasser S., J. Kilian A. O. L. Atkin, [6], que é um análogo do teste de primalidade de Pocklington [25], baseado no grupo $(\mathbb{Z}/n\mathbb{Z})^*$, e um método de fatoração, devido a Hendrik W. Lenstra [19], o qual é, nada mais, do que o análogo ao método $p-1$ de Pollard, [26]. A atracão principal destes métodos análogos é que eles são ambos baseados no estudo de curvas elípticas definidas sobre um corpo finito.

5.1 Teste de Primalidade de Curva Elíptica

O seguinte teste de primalidade foi proposto por Henry Cabourn Pocklington [25], em 1914.

Proposição 5.1 *Seja n um inteiro positivo. Suponha que existe um divisor primo q de $n-1$, que é maior que $\sqrt{n}-1$. Se existe um inteiro a tal que*

(i) $a^{n-1} \equiv 1 \pmod{n}$*; e*

(ii) $mdc(a^{(n-1)/q}-1, n) = 1$,

então n é primo.

Prova. Se n não é primo, então existe um primo $p \leq \sqrt{n}$ que divide n, logo $\sqrt{n}-1 \geq p-1$, e como $q > \sqrt{n}-1$ então $q > p-1$, daí temos que $mdc(q, p-1) = 1$, e, portanto, existe um inteiro u tal que $uq \equiv 1 \pmod{p-1}$. Então,

$$a^{(n-1)/q} \equiv a^{uq(n-1)/q} = a^{u(n-1)} \equiv 1 \pmod{p}$$

pela condição (i), logo $p|a^{(n-1)/q} - 1$, e como $p|n$ esto contradiz a condição (ii). □

Observação 5.2 *1. Este é um excelente teste, desde que $n-1$ seja divisível por um primo $q > \sqrt{n}-1$, e que sejamos capazes de encontrar q, e provar que é primo. Caso contrário, estamos sem sorte. Mas, na verdade, isso não é bem verdade, pois o teste acima pode ser generalizado para ser usado sempre que temos um grande divisor de $n-1$ na forma plenamente fatorada.*

2. *Note que este teste de primalidade é probabilístico apenas no sentido em que um a, escolhido aleatoriamente, pode ou não satisfazer a condição (ii), naturalmente, se ele não satisfaz (i), então n não é primo. Mas, uma vez que tal a é encontrado (e $a = 2$ normalmente funciona), o teste mostra que n é definitivamente um primo. Ao contrário de outros testes de primalidade, a conclusão do teste de Pocklington é uma certeza: n é primo, não um "provavelmente primo".*

O teste de primalidade com uma curva elíptica, é baseado em uma proposição análoga, onde supomos que temos uma equação $y^2 = x^3 + ax + b$ considerada módulo n. Ou seja, a e b são inteiros módulo n, e deixamos E denotar o conjunto de todos os inteiros $x, y \in \mathbb{Z}/n\mathbb{Z}$ que satisfazem a equação, juntamente com um símbolo $\mathcal{O}$, que chamamos de "ponto no infinito". Se n é primo, como é quase certamente o caso — já que, na prática, estamos considerando apenas os números n, que já passaram alguns prováveis testes de primalidade — então E é uma curva elíptica com o elemento identidade $\mathcal{O}$.

Antes de enunciar o análogo da Proposição 5.1 para E, notamos que, mesmo sem saber que n é primo, podemos aplicar as fórmulas do Capítulo 4 para adicionar elementos de E. Uma das três coisas acontece quando somamos dois pontos (ou dublamos um ponto):

1. obtemos um ponto bem definido,
2. se os pontos são da forma (x, y) e $(x, -y)$ módulo n, então temos o ponto no infinito,
3. as fórmulas são indefinidas, porque temos um denominador que não é invertível módulo n.

Mas o caso (3) significa que n é composto, e podemos encontrar um divisor não trivial tomando o mdc de n com o denominador. Assim, sem perda de generalidade no que se segue podemos assumir que o caso 3. nunca ocorre.

Pode ser mostrado que, para um elemento P de E módulo n, mesmo que n seja composto, a resposta que nosso algoritmo dá para mP não depende da maneira particular em que sucessivamente adicionemos e dobremos pontos. (Isto não é óbvio a priori). No entanto, este fato não irá ser necessário abaixo. Basta denotar mP como qualquer ponto que é obtido trabalhando módulo n com as fórmulas do Capítulo 4.

Assim, como podemos adicionar pontos módulo n sem saber que n é primo, da mesma forma, dado um algoritmo para calcular o número de pontos em uma curva elíptica (tais como o método de Schoof), podemos aplicá-lo para o nosso conjunto E módulo n. Vamos obter algum número m — que se n é primo é garantido para ser o número de pontos na curva elíptica E — ou senão encontrar uma expressão indefinida cujo denominador tem um fator comum não trivial com n. Tal como no caso da adição de pontos, sem perda de generalidade, pode-se supor que isso nunca acontece.

Tal m vai desempenhar o papel de $n-1$ em Proposição 5.1 — note que $n-1$ é a ordem de $(\mathbb{Z}/n\mathbb{Z})^*$ se n é primo.

Agora estamos prontos para enunciar o análogo do critério de curva elíptica de Pocklington.

Proposição 5.3 *Seja n um inteiro positivo. Considere E o conjunto dado por uma equação $y^2 = x^3 + ax + b$ módulo n, como acima. Seja m um número inteiro. Suponha que existe um número primo q que divide m o qual é maior do que $(n^{1/4}+1)^2$. Se existe um ponto P de E tal que*

(i) $mP = \mathcal{O}$*; e*

(ii) $(m/q)P$ *é definido e não é igual a* $\mathcal{O}$*,*

então n é primo.

Prova. Se n não é primo, então existe um primo $p \leq \sqrt{n}$ que divide a n. Seja E' a curva elíptica dada pela mesma equação como E, mas considerada módulo p, e seja m' a ordem do grupo E'. Pelo Teorema de Hasse, temos

$$m' \leq p+1+2\sqrt{p} = (\sqrt{p}+1)^2 \leq (n^{1/4}+1)^2 < q,$$

pois $p \leq \sqrt{n}$, portanto $mdc(q,m') = 1$, assim existe um inteiro u tal que $uq \equiv 1 \pmod{m'}$. Seja $P' \in E'$ o ponto P considerado módulo p. Então em E' temos

$$(m/q)P' = uq(m/q)P' = umP' = \mathcal{O},$$

por (i), já que mP' é obtido utilizando o mesmo procedimento como mP, trabalhando apenas módulo $p|n$ em vez de módulo n. Mas isso contraria (ii), já que, se $(m/q)P$ é definido e $\neq \mathcal{O}$ módulo n, então o mesmo procedimento trabalhando módulo p em vez de módulo n vai dar $(m/q)P' \neq \mathcal{O}$. Isso completa a prova. □

Esta proposição leva a um algoritmo para provar que um inteiro n, que podemos supor que já é conhecido por ser " provavelmente um primo", é definitivamente primo. Procedemos da seguinte forma.

1. Escolhemos aleatoriamente três inteiros a,x,y módulo n e definimos $b \equiv y^2 - x^3 - ax \pmod{n}$. Então $P = (x,y)$ é um elemento de $E : y^2 = x^3 + ax + b$.

2. Usamos o algoritmo de Schoof, ou outro método de contagem do número de pontos sobre uma curva elíptica para encontrar um número m que, se n é primo, é igual ao número de pontos na curva elíptica E sobre F_n.

   Se não podemos escrever m na forma $m = kq$, onde $k \geq 2$ é um inteiro pequeno e q é " provavelmente um primo" (ou seja, ele passou um outro teste de primalidade), então escolhemos outra tripla aleatória a,x,y e começamos novamente. Suponhamos que, finalmente, obtemos uma curva elíptica para a qual m tem a forma desejada.

3. Então usamos as fórmulas no Capítulo 4, trabalhando módulo n para calcular mP e kP.

   Se alguma vez obtemos uma expressão indefinida — seja no cálculo de um múltiplo de P ou ao aplicar o algoritmo de Schoof — então imediatamente encontramos um fator não trivial de n. Podemos supor que isso não aconteça.

4. Se $mP \neq \mathcal{O}$, então sabemos que n é composto, porque se n fosse primo, então o grupo E teria ordem m, e qualquer elemento de E seria morto pela multiplicação de m.

5. Se $kP = \mathcal{O}$ (que é altamente improvável), estamos fora de sorte, e devemos começar novamente com outro triplo.

6. Mas se $mP = \mathcal{O}$ e $kP \neq \mathcal{O}$, em seguida, pela Proposição 5.3 sabemos que n é primo, desde que o grande fator q da m é realmente um primo (só sabemos que era um "primo provável").

Isto reduz o problema a provar primalidade de q, que tem uma magnitude no máximo cerca de $n/2$. Em seguida, começamos de novo com n substituído por q. Assim, obtémos um procedimento recursivo com t repetições do teste de primalidade, onde t é não mais do que cerca de $\log_2 n$. Quando terminarmos, obtivemos um número q_t que sabemos é primo,

do qual resulta que o q_{t-1} anterior era realmente um primo (e não apenas " provavelmente um primo"), do qual resulta que o mesmo é verdadeiro para q_{t-2}, e assim por diante, até $q_1 = q$, e finalmente n em si é verdadeiramente um primo. Isto conclui a descrição do teste de primalidade de curva elíptica.

Observação 5.4 *Existem duas dificuldades com este teste, uma prática e outra teórica.*

1. *Embora o algoritmo de Schoof leva tempo polinomial em* $\log n$*, na prática, é bastante complicado. Algum progresso foi feito recentemente no qual se completa e simplifica, mas mesmo assim é bastante desagradável ter que contar o número de pontos em um grande número de curvas E até finalmente encontrar uma para a qual m tem a forma desejada* $m = kq$*. A fim de lidar com este problema, A. O. L. Atkins desenvolveu uma variante do teste de primalidade de curva elíptica usando curvas elípticas cuidadosamente construídas com multiplicação complexa, para a qual é muito mais fácil calcular o número de pontos sobre a sua redução módulo n, ver [18].*

2. *A segunda dificuldade é teórica. A fim de encontrar uma curva elíptica E sobre* F_n *(assumindo que n é primo), cujo número de pontos é "quase primo" (ou seja, da forma* $m = kq$ *para k pequeno e q primo), temos que saber algo sobre a distribuição dos números primos (em vez, de "primos próximos") no intervalo de* $p+1-2\sqrt{p}$ *a* $p+1+2\sqrt{p}$ *que, pelo Teorema de Hasse, é conhecido por conter m. Como o comprimento deste intervalo é relativamente pequeno, não há teorema que garante que temos uma alta probabilidade de encontrar uma tal E depois de apenas muitas tentativas polinomialmente (polinomiais em* $\log n$*). No entanto, existe uma conjectura muito possível que iria garantir isso, e para efeitos práticos, não deve haver nenhum problema. Mas se alguém quiser um algoritmo probabilístico comprovadamente de tempo polinomial, se tem que trabalhar de modo mais difícil: um tal teste de primalidade foi desenvolvido por Adleman e Huang usando bidimensionais variedades abelianas, que são uma generalização das curvas elípticas de 2 dimensões. No entanto, o seu algoritmo é completamente impraticável, bem como muito complicado.*

5.2 Fatoração de Curva Elíptica

Uma das principais razões para o crescente interesse em curvas elípticas por parte dos criptógrafos é o recente uso engenhoso de curvas elípticas por Hendrik W. Lenstra [19], para obter um novo método de fatoração que em muitos aspectos é melhor do que as anteriormente conhecidas. A melhoria da eficiência não é suficientemente significativa

na prática para representar uma ameaça para a segurança dos sistemas criptográficos baseados na intratabilidade assumido de fatoração, a sua estimativa de tempo tem a mesma forma que encontramos no Capítulo V.3 de [15]; no entanto, a descoberta de uma melhoria usando um novo dispositivo inesperado serve como um aviso de que nunca se deve ser muito "acomodados" sobre a suposta impermeabilidade do problema de fatoração a avanços dramáticos.

Antes de proceder ao algoritmo para fatoração de curva elíptica de Lenstra, damos uma técnica de fatoração clássica, que é análogo ao método de Lenstra. O seguinte algoritmo foi proposto por John Pollard en 1974, [26], é um algoritmo de propósito especial, o qual significa que é unicamente adequado para inteiros com fatores de tipos específicos, e depende unicamente das propriedades de seus fatores desconhecidos tais como o tamanho. Em contrapartida, tem-se os algoritmos de propósito geral, os quais só dependem do número inteiro a fatorar.

5.2.1 O método $p-1$ de Pollard

Suponha que queremos fatorar o número composto n, e p é algum (ainda desconhecido) fator primo de n. Se p passa a ter a propriedade que $p-1$ não tem um grande divisor primo, então o método a seguir é virtualmente certo para encontrar p.

O algoritmo procede como se segue:

1. Escolha um inteiro k que é um múltiplo de todos ou a maioria dos inteiros menores do que algum limite B. Por exemplo, k pode ser $B!$, ou pode ser o mínimo múltiplo comum de todos os inteiros $\leq B$.

2. Escolher um número inteiro a entre 2 e $n-2$. Por exemplo, a pode ser igual 2, ou 3, ou um número inteiro escolhido de forma aleatória.

3. Calcule $a^k \pmod{n}$ pelo método dos quadrados repetidos.

4. Calcule $d = mdc(a^k - 1, n)$ usando o algoritmo de Euclides e o resíduo de a^k módulo n da etapa 3.

5. Se d não é um divisor não trivial de n, começar de novo com uma nova escolha de a e/ou uma nova escolha de k.

Para explicar quando este algoritmo irá funcionar, suponhamos que k é divisível por todos os inteiros positivos $\leq B$, e supor além que p é um divisor primo de n tal que $p-1$ é um produto de pequenas potências primas, todas menores que B. Então segue que k é um múltiplo de $p-1$ (porque ele é um múltiplo de todas as potencias primas na fatoração de $p-1$), e assim, pelo pequeno Teorema de Fermat, temos $a^k \equiv 1 \pmod{p}$.

Então $p|mdc(a^k-1,n)$, e por isso a única maneira de podermos não conseguir obter um fator não trivial de n na etapa 4 é se acontece que $a^k \equiv 1 \pmod{n}$.

Exemplo 5.5 *Para fatorar* $n = 540143$ *pelo método* $p-1$ *de Pollard procedemos como segue.*

1. *Escolha* $B = 8$*, e tome* $k = mdc(1,2,\ldots,8) = 840$*.*
2. *Escolha* $a = 2$*.*
3. *Achamos que* $2^{840} \pmod{n} = 53047$*.*
4. *Assim* $mdc(53046,n) = 421$*.*

Isso leva à fatoração $540143 = 421 \cdot 1283$*.*

A principal fraqueza do método de Pollard, está claro, é ao tentar usá-lo quando todos os divisores primos p de n tem $p-1$ divisível por um primo relativamente grande (potência prima).

Exemplo 5.6 *Seja* $n = 491389$*. Seria improvável encontrar um divisor não trivial até escolher* $B \geq 191$*. Isso ocorre porque verifica-se que* $n = 383 \cdot 1283$*. Temos que* $383-1 = 2 \cdot 191$ *e* $1283-1 = 2 \cdot 641$*, ambos 191 e 641 são números primos. Exceto para* $a \equiv 0, \pm 1 \pmod{383}$*, todas as outras a's tem a ordem módulo 383 ou bem 191 ou 382; e exceto para* $a \equiv 0, \pm 1 \pmod{1283}$*, todas as outras a's tem a ordem módulo 1283 ou bem 641 ou 1282. Portanto, a menos k seja divisível por 191 (ou 641), é provável encontrar mais uma vez que* $mdc(a^k-1,n) = 1$ *no passo 4.*

O dilema básico com o método $p-1$ de Pollard é que estamos depositando nossas esperanças sobre o grupo $(\mathbb{Z}/p\mathbb{Z})^*$ (mais precisamente, os vários grupos $(\mathbb{Z}/p\mathbb{Z})^*$ quando p percorre os divisores primos de n). Para a n fixo, estes grupos são fixos. Se para todos eles acontecer que tem ordem divisível por um grande primo, estamos presos.

A principal diferença no método de Lenstra, como veremos, é que, ao trabalhar com curvas elípticas sobre $F_p = \mathbb{Z}/p\mathbb{Z}$, de repente temos um bando inteiro de grupos para usar, e podemos realisticamente esperar sempre encontrar uma cuja ordem é não divisível por uma grande primo ou potência prima.

Começamos nossa descrição do algoritmo de Lenstra com alguns comentários sobre a redução de pontos em curvas elípticas módulo n, onde n é um inteiro composto.

5.2.2 Curvas Elípticas — Redução Módulo n

Para o restante da seção, vamos denotar n por um número inteiro ímpar composto e p um (ainda desconhecido) fator primo de n. Vamos supor que $p > 3$.

Definição 5.7 *Para qualquer inteiro m e quaisquer dois números racionais x_1, x_2 com denominadores primos a m, vamos escrever $x_1 \equiv x_2 \pmod{m}$, se $x_1 - x_2$, escrito em sua forma simplificada, é uma fracção com numerador divisível por m. Para qualquer número racional x_1 com o denominador primo a m existe um único inteiro x_2, chamado de "menor resíduo não negativo" entre 0 e $m-1$ tal que $x_1 \equiv x_2 \pmod{m}$. Às vezes vamos escrever $x_1 \pmod{m}$ para denotar este menor resíduo não negativo.*

Suponha que temos uma equação da forma $y^2 = x^3 + ax + b$ com $a, b \in \mathbb{Z}$ e um ponto $P = (x, y)$ que a satisfaz. Na prática, a curva E, junto com o ponto P serão gerados, de algum modo "aleatório", por exemplo, pela escolha de três números inteiros aleatórios, a, x, y em algum intervalo e, em seguida, definindo $b = y^2 - x^3 - ax$. Vamos supor que o cubo tem raízes distintas, isto é, $4a^3 + 27b^2 \neq 0$; esto é quase certo se os coeficientes foram escolhidos da forma aleatória descrita. Para simplificar, no que segue também deve supor que $4a^3 + 27b^2$ tem nenhum fator comum com n; em outras palavras, $x^3 + ax + b$ não tem raízes múltiplas módulo p para qualquer primo p divisor de n. Na prática, uma vez que tenhamos feito uma escolha de a e b, podemos verificar isso calculando $mdc(4a^3 + 27b^2, n)$. Se este para > 1, então ou $n | 4a^3 + 27b^2$, caso em que temos de fazer uma outra escolha de a e b; ou então obtivemos um divisor não trivial de n, caso em que acabarmos. Então vamos supor que $mdc(4a^3 + 27b^2, n) = 1$.

Múltiplos de Pontos

A analogia, numa curva elíptica, da multiplicação de dois elementos de F_q^* é a adição de dois pontos em E, onde E é uma curva elíptica definida sobre F_q. Assim, o análogo de elevar à potência k-ésima em F_q^* é a multiplicação de um ponto $P \in E$ por um inteiro k. Elevar à potência k-ésima num corpo finito pode ser realizado pelo método de quadrados repetidos. Da mesma forma, pode ser calculado o múltiplo $kP \in E$ através do método de duplicação repetida, como ilustra o exemplo abaixo.

Exemplo 5.8 *Para encontrar $100P$ escrevemos $100P = 2(2(P + 2(2(2(P + 2P)))))$, e acabamos realizando 6 duplicações e adições de 2 pontos na curva.*

Agora, suponha que queremos encontrar o múltiplo kP, utilizando o método de duplicação repetida descrito acima. Isto pode ser feito em $O(\log k)$ passos, envolvendo cada um deles uma duplicação ou uma adição de dois pontos distintos. Há muitas maneiras de fazer isso. Por exemplo, k pode ser escrito em binário como $a_0 + a_1 2 +$

$\cdots + a_{m-1}2^{m-1}$, então P pode ser sucessivamente dobrado, com 2^jP adicionado à soma parcial sempre que o bit correspondente a_j é 1. Como alternativa, k poderia ser fatorada em um produto de números primos ℓ_j, e, em seguida, pode-se sucessivamente calcular $\ell_1 P, \ell_2(\ell_1 P)$, e assim por diante, onde $\ell_1, \ell_2, \ldots$ são os números primos na fatoração de k (listados, por exemplo, de forma não-decrescente). Aqui, cada múltiplo $\ell_j P_j$, onde $P_j = \ell_{j-1}\ell_{j-2}\cdots\ell_1 P$, é calculado escrevendo ℓ_j em binário e usando duplicações repetidas.

Vamos supor que uma tal técnica foi escolhida para calcular múltiplos kP. E vamos considerar o ponto P e todos os seus múltiplos módulo n. Isso significa que tomamos $P \pmod n = (x \pmod n, y \pmod n)$, e, cada vez que calculamos algum múltiplo kP, realmente calculamos só a redução das coordenadas módulo n. A fim de ser capaz de trabalhar módulo n, existe uma condição não trivial que deve-se manter sempre que executamos um passo de duplicação ou adicionar dois pontos diferentes; ou seja, todos os denominadores devem ser coprimos com n.

Proposição 5.9 *Seja E uma curva elíptica com equação $y^2 = x^3 + ax + b$, onde $a, b \in \mathbb{Z}$ e $mdc(4a^3 + 27b^2, n) = 1$. Sejam P_1 e P_2 dois pontos em E cujas coordenadas têm denominadores primos a n, onde $P_1 \neq -P_2$. Então $P_1 + P_2 \in E$ tem coordenadas com denominadores primos a n se, e somente se, não houver nenhum primo $p|n$ com a seguinte propriedade: os pontos $P_1 \pmod p$ e $P_2 \pmod p$ sobre a curva elíptica $E \pmod p$ somam o ponto no infinito $\mathcal{O} \pmod p \in E \pmod p$. Aqui $E \pmod p$ denota a curva elíptica sobre F_p obtida através da redução módulo p dos coeficientes da equação $y^2 = x^3 + ax + b$.*

Prova. Primeiro suponha que $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, e $P_1 + P_2 \in E$ todos têm coordenadas com denominadores primos a n. Seja p qualquer divisor primo de n. Devemos mostrar que $P_1 \pmod p + P_2 \pmod p \neq \mathcal{O} \pmod p$. Para isso considere os seguintes casos

1. Se $x_1 \not\equiv x_2 \pmod p$, então, de acordo com a descrição da lei de adição 4. em $E \pmod p$, concluímos imediatamente que $P_1 \pmod p + P_2 \pmod p \neq \mathcal{O} \pmod p$. Pois se $P_1 \pmod p + P_2 \pmod p = \mathcal{O} \pmod p$ então $P_1 \pmod p = -P_2 \pmod p$, ou seja $x_1 \pmod p = x_2 \pmod p$, o que implica $x_1 \equiv x_2 \pmod p$.

2. Agora, suponha que $x_1 \equiv x_2 \pmod p$. E considere os dois seguintes casos:

   (a) se $P_1 = P_2$, então as coordenadas de $P_1 + P_2 = 2P_1$ são encontrados pela fórmula (6) do Capítulo 4, e $2P_1 \pmod p$ é encontrado pela mesma fórmula com cada termo substituído pelo seu resíduo módulo p. Temos de mostrar que o denominador $2y_1$ não é divisível por p, pois do contrario se $p|2y_1$ então $(2y_1)^{-1} \pmod p$ não existe e assim $2P_1 \pmod p = \mathcal{O} \pmod p$. Suponha

por contradição que $p|2y_1$, então, porque o denominador do coeficiente x de $2P_1$ não é divisível por p, segue-se que o numerador $3x_1^2+a$ seria divisível por p. Mas isso significaria que x_1 é uma raiz módulo p de o cúbico x^3+ax+b e sua derivada, contradizendo a nossa hipótese de que não existem raízes múltiplas módulo p, assim $p \not| 2y_1$.

(b) Suponha que $P_1 \neq P_2$. Já que $x_1 \equiv x_2 \pmod{p}$ e $x_2 \neq x_1$, podemos escrever $x_2 = x_1 + p^r x$ com $r \geq 1$ escolhida de modo que nem o numerador nem denominador de x é divisível por p, de fato; $x_1 - x_2 = \frac{\bar{n}}{d}$ com $mdc(\bar{n}, d) = 1$ e $p|\bar{n}$; $\bar{n} = pt$, logo tiro todas as potências de p de $\bar{n}$, ou seja $\bar{n} = p^r t_1$, onde $p \not| t_1$ e $r \geq 1$, assim $x_2 = x_1 + p^r \frac{t_1}{d}$, além $p \not| d$.

Já que $P_1 + P_2$ tem denominador não é divisível por p, podemos usar a fórmula (5) do Capítulo 4 para concluir que y_2 é da forma $y_1 + p^r y$. Por outro lado,

$$\begin{aligned} y_2^2 =& (x_1 + p^r x)^3 + a(x_1 + p^r x) + b \\ \equiv& x_1^3 + ax_1 + b + p^r x(3x_1^2 + a) = y_1^2 + p^r x(3x_1^2 + a) \pmod{p^{r+1}}. \end{aligned} \tag{13}$$

Mas já que $x_2 \equiv x_1 \pmod{p}$ e $y_2 \equiv y_1 \pmod{p}$, segue-se que $P_1 \pmod{p} = P_2 \pmod{p}$, e assim $P_1 \pmod{p} + P_2 \pmod{p} = 2P_1 \pmod{p}$, que é $\mathcal{O} \pmod{p}$ se e somente se $y_1 \equiv y_2 \equiv 0 \pmod{p}$. Se esta última congruência é mantida, então $y_2^2 - y_1^2 = (y_2 - y_1)(y_2 + y_1)$ seria divisível por p^{r+1}, pois $y_2 - y_1$ é divisível por p^r, então se $y_1, y_2 \equiv 0 \pmod{p}$, y_1 e y_2 são divisíveis por p, assim $y_1 + y_2$ também é divisível por p e portanto $y_2^2 - y_1^2$ é divisível por p^{r+1}. E assim a congruência (13) implicaria que $3x_1^2 + a \equiv 0 \pmod{p}$, pois $p^r x(3x_1^2 + a) \equiv 0 \pmod{p^{r+1}}$ e daí $p^{r+1} | p^r x(3x_1^2 + a)$ ou seja $p^r x(3x_1^2 + a) = p^{r+1}k$ para algum $k \in \mathbb{Z}$ então $x(3x_1^2 + a) = pk$ assim $p|x(3x_1^2 + a)$ mas $p \not| x$ e portanto $p|3x_1^2 + a$. Isso é impossível, porque o polinomial $x^3 + ax + b$ módulo p não tem raízes múltiplas, e assim x_1 não pode ser uma raiz tanto deste polinômio e sua derivada módulo p. Conclui-se que $P_1 \pmod{p} + P_2 \pmod{p} \neq \mathcal{O} \pmod{p}$.

Reciprocamente, suponha que para todos os primos p divisores de n temos $P_1 \pmod{p} + P_2 \pmod{p} \neq \mathcal{O} \pmod{p}$. Devemos mostrar que as coordenadas de $P_1 + P_2$ têm denominadores primos a n, ou seja, que os denominadores não são divisíveis por p para qualquer $p|n$. Fixe algum $p|n$, se $x_2 \not\equiv x_1 \pmod{p}$, então a fórmula (5) do Capítulo 4 mostra que não há denominadores divisíveis por p. Então, suponha que $x_2 \equiv x_1 \pmod{p}$. Logo $y_2 \equiv \pm y_1 \pmod{p}$, pois $y_1^2 = x_1^3 + ax_1 + b$ e $y_2^2 = x_2^3 + ax_2 + b$, isso implica $y_2^2 - y_1^2 \equiv 0 \pmod{p}$ já que $x_2 \equiv x_1 \pmod{p}$. Mas já que $P_1 \pmod{p} + P_2 \pmod{p} \neq \mathcal{O}$

$(\text{mod } p)$, devemos ter $y_1 \equiv y_2 \not\equiv 0 \pmod{p}$ pois lembre que se $(x_1,y_1)+(x_2,y_2)=\mathcal{O}$ então $(x_1,y_1)=(x_2,-y_2)$. Considere os seguentes dois casos

1. se $P_2 = P_1$, então a fórmula (6) do Capítulo 4, junto com o fato de que $y_1 \not\equiv 0 \pmod{p}$ mostra que as coordenadas do $P_1+P_2=2P_1$ têm denominadores primos a p.

2. Finalmente, se $P_1 \neq P_2$ voltamos a escrever $x_2 = x_1 + p^r x$ com x não é divisível por p, e usamos a congruência (13) acima para escrever

$$\frac{y_2^2 - y_1^2}{x_2 - x_1} \equiv 3x_1^2 + a \pmod{p}.$$

Já que p não divide $y_2 + y_1 \equiv 2y_1 \pmod{p}$, segue-se que não existe p no denominador de

$$\frac{y_2^2 - y_1^2}{(y_2+y_1)(x_2-x_1)} = \frac{y_2 - y_1}{x_2 - x_1},$$

e portanto pela fórmula (5) do Capítulo 4, não existe p no denominador das coordenadas de $P_1 + P_2$.

□

5.2.3 O Método de Lenstra

Nos é dado um número inteiro composto n ímpar e queremos encontrar um fator não trivial $d|n$, $1 < d < n$. Começamos por tomar alguma curva elíptica $E: y^2 = x^3 + ax + b$ com coeficientes inteiros junto com um ponto $P = (x,y)$ sobre ela. O par (E,P) é provavelmente gerado de alguma forma aleatória, embora pudéssemos optar por utilizar algum método determinista que é capaz de gerar muitos desses pares (como no Exemplo 4 abaixo). Tentamos usar E e P para factorar n, como será logo explicado; se a nossa tentativa falhar, tomamos um outro par (E,P), e continuamos desta forma até encontrar um fator $d|n$.

Se a probabilidade de falha de este processo é $\rho < 1$, então a probabilidade de que h escolhas sucessivas de (E,P) todas falhar é ρ^h, o qual é muito pequeno para h grande. Assim, com uma probabilidade muito elevada será factorado n, em um número razoável de tentativas. Uma vez que temos um par (E,P), escolhemos um inteiro k que é divisível por potências de pequenos números primos ($\leq B$) que são menores do que algum limite C. Ou seja, vamos definir

$$k = \prod_{\ell \leq B} \ell^{\alpha_\ell}, \tag{14}$$

onde $\alpha_\ell = [\log C/\log \ell]$ é o maior expoente tal que $\ell^{\alpha_\ell} \leq C$. Então, tentamos calcular kP trabalhando o tempo todo módulo n. Este cálculo é sem complicações e inútil, a menos que nos encontremos com a seguinte dificuldade: quando se tenta encontrar o inverso de $x_2 - x_1$ na fórmula (5) do Capítulo 4, ou o inverso de $2y_1$ em (6), encontrarmos um número que é não primo a n. De acordo com a Proposição 5.9, isso vai acontecer quando temos algum múltiplo k_1P (uma soma parcial encontrada ao ongo do caminho em nosso cálculo de kP) tal que para algum $p|n$ tem a propriedade $k_1(P \pmod p) = \mathcal{O} \pmod p$, ou seja, o ponto $P \pmod p$ no grupo $E \pmod p$ tem ordem dividindo k_1. No processo de utilizar o algoritmo de Euclides para tentar encontrar o inverso módulo n de um denominador que é divisível por p, encontramos o mdc de n com o denominador. Esse mdc vai ser um divisor próprio de n, a menos que seja o próprio n, isto é, a menos que o denominador é divisível por n. Isso significaria, pela Proposição 5.9, que $k_1P \pmod p = \mathcal{O} \pmod p$ para todos os primos p divisores de n — algo que é altamente improvável, se n tem dois ou mais divisores primos muito grandes. Assim, é praticamente certo que logo que tentar calcular k_1P módulo n para um k_1 que é um múltiplo da ordem de $P \pmod p$ para algum $p|n$, obteremos um divisor próprio de n.

Observe a semelhança com o método $p-1$ de Pollard. Em vez de o grupo $(\mathbb{Z}/p\mathbb{Z})^*$, estamos usando o grupo $E \pmod p$. No entanto, desta vez, se a nossa E resulta ser uma escolha ruim — ou seja, para cada $p|n$ o grupo $E \pmod p$ tem ordem divisível por um grande primo (e assim $kP \pmod p$ provavelmente não é igual a $\mathcal{O} \pmod p$ para k dado por (14)) — tudo o que temos que fazer é descartá-lo e escolher outra curva elíptica junto com um ponto $P \in E$. Note que não temos essa opção no método de Pollard.

O Algoritmo

Seja n um inteiro positivo composto impar. Descrevemos agora método probabilístico de Lenstra para fatorar n.

1. Gere um par (E,P) que consiste de uma curva elíptica $E : y^2 = x^3 + ax + b$ com $a,b \in \mathbb{Z}$ e um ponto $P = (x,y) \in E$.

   Se o processo que vamos descrever deixa de produzir um fator de n não trivial, então, geramos um novo par (E,P) e repetimos o processo.

2. Verificar que a curva E é de fato uma curva elíptica módulo qualquer $p|n$, ou seja, que o cubo da direita tem raízes distintas módulo p. Isto é, se e somente se o discriminante $4a^3 + 27b^2$ é primo a n.

   (a) Se $mdc(4a^3 + 27b^2, n) = 1$, podemos prosseguir.

   (b) Se este mdc esta estritamente entre 1 e n, temos um divisor não trivial de n, e o processo acabou.

(c) Se este mdc é igual a n, então, deve-se escolher uma curva elíptica diferente.

3. Escolher dois limites $B, C \in \mathbb{Z}$, positivos.

   B: é um limite para os divisores primos do inteiro k pelo qual multiplicamos o ponto P. Se B é grande, então há uma probabilidade maior que o nosso par (E,P) tem a propriedade que $kP \pmod p = \mathcal{O} \pmod p$ para algum $p|n$; por outro lado, quanto maior B levará mais tempo para calcular $kP \pmod p$. Assim B deve ser escolhido de modo que minimizemos o tempo de execução.

   C: a grosso modo, é um limite para os divisores primos $p|n$ para os quais é provável a obtenção de uma relação $kP \pmod p = \mathcal{O} \pmod p$.

4. Escolhemos k dado por (14), ou seja, $k = \prod_{\ell \leq B} \ell^{\alpha_\ell}$, $\alpha_\ell = [\log C / \log \ell]$ e $\ell^{\alpha_\ell} \leq C$.

   Observação 5.10 *Seja $N = |E \pmod p|$, o Teorema de Hasse nos diz que $N \leq p+1+2\sqrt{p}$. Se p é tal que $p+1+2\sqrt{p} < C$ então $N < C$ e para todo $p^\alpha | N$ temos $p^\alpha < C$. Além disso, se para todo primo q tal que $q > B$ temos que $q \not| N$, então k é um múltiplo de N e assim $kP \pmod p = \mathcal{O} \pmod p$.*

5. Trabalhando módulo n, tentamos calcular kP como segue. Usar o método de duplicação repetida para calcular

   $$2P,\ 2(2P),\ 2(4P), \ldots, 2^{\alpha_2}P, \quad \text{logo} \quad 3(2^{\alpha_2})P,\ 3(3\cdot 2^{\alpha_2}P), \ldots, 3^{\alpha_3}2^{\alpha_2}P,$$

   e assim por diante, até que finalmente tiver $\prod_{\ell \leq B} \ell^{\alpha_\ell} P$. (Multiplique sucessivamente pelos fatores primos ℓ do k do menor ao maior).

   Nestes cálculos, sempre que temos que dividir módulo n, usamos o algoritmo de Euclides para encontrar o inverso módulo n.

   (a) Se em qualquer fase do algoritmo de Euclides não fornecer um inverso então

      (i) encontrou um divisor não trivial de n, caso no qual o algoritmo foi completado com sucesso.

      (ii) ou se obtêm n mesmo como o mdc de n e o denominador. Neste caso, deve voltar atrás e escolher um outro par (E,P).

   (b) Se o algoritmo de Euclides sempre fornece um inverso — e assim kP módulo n é realmente calculado — então também deve voltar atrás e escolher um outro par (E,P).

Isto conclui a descrição do algoritmo de Lenstra.

Exemplo 5.11 *Suponha que escolhemos $B = 20$, e queremos fatorar um inteiro n de 10 dígitos decimais, que pode ser um produto de dois números primos de 5 dígitos (isto é, não é divisível por qualquer primo de menos de 5 dígitos). Então, escolha $C = 100700$ e $k = 2^{16} \cdot 3^{10} \cdot 5^7 \cdot 7^5 \cdot 11^4 \cdot 13^4 \cdot 17^4 \cdot 19^3$.*

Exemplo 5.12 *Vamos usar a família de curvas elípticas $y^2 = x^3 + ax - a$, $a = 1, 2, \ldots$, cada uma das quais contém o ponto $P = (1,1)$, para tentar fatorar o número $n = 5429$.*

1. *Antes de usar um a para um dado n, devemos verificar se o discriminante $4a^3 + 27a^2$ é primo a n.*

2. *Escola $B = 3$ e $C = 92$.*

   Aqui a nossa escolha de C é motivada pelo nosso desejo de encontrar um fator primo p o que poderia ser quase tão grande como $\sqrt{n} \approx 73$; assim para $p = 73$ o limite do número de pontos F_q-racionais sobre uma curva elíptica é $74 + 2\sqrt{73} < 92$.

3. *Utilizando (14), temos que $\alpha_2 = [\log C / \log 2] = 2$ e $\alpha_3 = [\log C / \log 3] = 4$, assim $k = 2^6 \cdot 3^4$.*

4. *Para cada valor de a, sucessivamente multiplicamos P por 2 seis vezes e depois por 3 quatro vezes, trabalhando módulo n, na curva elíptica $y^2 = x^3 + ax - a$.*

   (a) *Quando $a = 1$ vemos que a multiplicação prossegue sem problemas, e verifica-se que $3^4 2^6 P \pmod{p}$ é um ponto finito sobre $E \pmod{p}$ para todo $p|n$.*

   (b) *Assim, tentamos com $a = 2$. Então, descobrimos que quando tentamos calcular $3^2 2^6 P$, obtemos um denominador cujo mdc com n é o fator próprio 61. Isto é, o ponto $P = (1,1)$ tem ordem dividindo $3^2 2^6$ na curva $y^2 = x^3 + 2x - 2$ módulo 61. Assim, a segunda tentativa é bem sucedida e obtemos o fator 61.*

   (c) *Se tentarmos com $a = 3$ encontramos que o método da o fator primo 89 quando tentamos calcular $3^4 2^6 P$.*

Normalmente, mas nem sempre, o método resulta no menor fator primo.

Em conclusão, o método da Lenstra apresenta certas vantagens sobre os seus concorrentes, por exemplo: é o único método que é substancialmente mais rápido se n é divisível por um primo que é muito menor que $\sqrt{n}$. Por este motivo, pode ser utilizado em combinação com outros métodos de fatoração quando a fatoração de certos números auxiliares é necessária.

Da mesma forma como o método $p - 1$ de Pollard, o método de Lestra é um algoritmo de propósito especial, além disso, é o mais adequado para encontrar fatores

pequenos de um número dado n. Nesta ordem de ideias, este método é usado para eliminar fatores pequenos de um inteiro n muito grande com muitos fatores; se o inteiro resultante ainda é composto, então somente tem fatores grandes e portanto é fatorado por meio de métodos de propósito geral.

Referências Bibliográficas

[1] COUTINHO, S. C. **Números inteiros e criptografia RSA**. IMPA, 1997.

[2] DIFFIE, W.; HELLMAN, M. **New directions in cryptography**. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[3] ELGAMAL, T. **A public key cryptosystem and a signature scheme based on discrete logarithms**. In: *Workshop on the Theory and Application of Cryptographic Techniques*, p. 10–18. Springer, 1984.

[4] FIPS, P. **186-2, digital signature standard, federal information processing standards publication 186-2, us department of commerce/national institute of standards and technology, national technical information service, springfield, virginia, 2000**.

[5] GOLDWASSER, S.; BELLARE, M. **Lecture notes on cryptography**. *Summer course "Cryptography and computer security" at MIT*, 1999:1999, 1996.

[6] GOLDWASSER, S.; KILIAN, J. **Almost all primes can be quickly certified**. In: *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, p. 316–329. ACM, 1986.

[7] GOLDWASSER, S.; MICALI, S. **Probabilistic encryption & how to play mental poker keeping secret all partial information**. In: *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, STOC '82, p. 365–377, New York, NY, USA, 1982. ACM.

[8] GOLDWASSER, S.; MICALI, S. **Probabilistic encryption**. *Journal of computer and system sciences*, 28(2):270–299, 1984.

[9] GUPTA, R.; RAM MURTY, M. **Primitive points on elliptic curves**. *Compositio mathematica*, 58(1):13–44, 1986.

[10] HERSTEIN, I. N.; HERSTEIN, I. N. **Abstract algebra**. Macmillan New York, 1990.

[11] HUA, L.-K. **Introduction to number theory**. Springer Science & Business Media, 2012.

[12] JOHNSON, D.; MENEZES, A.; VANSTONE, S. **The elliptic curve digital signature algorithm (ecdsa)**. *International Journal of Information Security*, 1(1):36–63, 2001.

[13] KAHN, D. **The codebreakers**. Weidenfeld and Nicolson, 1974.

[14] KOBLITZ, N. **Elliptic curve cryptosystems**. *Mathematics of computation*, 48(177):203–209, 1987.

[15] KOBLITZ, N. **A course in number theory and cryptography**, volume 114. Springer Science & Business Media, 1994.

[16] KOBLITZ, N. I. **Introduction to elliptic curves and modular forms**, volume 97. Springer Science & Business Media, 2012.

[17] LANG, S.; TROTTER, H. **Primitive points on elliptic curves**. *Bulletin of the American Mathematical Society*, 83(2):289–292, 1977.

[18] LENSTRA, A. K.; LENSTRA JR, H. W. **Algorithms in number theory**. Technical report, Elsevier, 1990.

[19] LENSTRA JR, H. W. **Factoring integers with elliptic curves**. *Annals of mathematics*, p. 649–673, 1987.

[20] MASSEY, J. L.; OMURA, J. K. **Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission**, Jan. 28 1986. US Patent 4,567,600.

[21] MERKLE, R. C. **Secure communications over insecure channels**. *Communications of the ACM*, 21(4):294–299, 1978.

[22] MILLER, V. S. **Use of elliptic curves in cryptography**. In: *Conference on the Theory and Application of Cryptographic Techniques*, p. 417–426. Springer, 1985.

[23] MURTY, M. R. **On Artin's conjecture**. *Journal of Number Theory*, 16(2):147–168, 1983.

[24] NEEDHAM, R. M.; SCHROEDER, M. D. **Using encryption for authentication in large networks of computers**. *Communications of the ACM*, 21(12):993–999, 1978.

[25] POCKLINGTON, H. C. **The determination of the prime or composite nature of large numbers by Fermat's theorem**. In: *Proceedings of the Cambridge Philosophical Society*, volume 18, p. 29–30, 1914.

[26] POLLARD, J. M. **Theorems on factorization and primality testing**. In: *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 76, p. 521–528. Cambridge Univ Press, 1974.

[27] RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. *Communications of the ACM*, 21(2):120–126, 1978.

[28] RUOHONEN, K. **Mathematical cryptology**. *Lecture Notes*, 2010.

[29] SCHOOF, R. **Elliptic curves over finite fields and the computation of square roots** $\mod p$. *Mathematics of computation*, 44(170):483–494, 1985.

[30] SERRE, J.-P. **Résumé des cours de 1977-1978**. *Annuaire du College de France*, p. 67–70, 1978.

[31] SHANKS, D. **Solved and unsolved problems in number theory**, volume 297. American Mathematical Soc., 2001.

[32] SHANNON, C. **A mathematical theory of communication, bell system technical journal 27: 379-423 and 623–656**. *Mathematical Reviews (MathSciNet): MR10, 133e*, 1948.

[33] SILVERMANN, J. H. **The arithmetic of elliptic curves**. *Grad. Texts in Math*, 106, 1986.

[34] SINGH, S. **O livro dos códigos**. Editora Record, 2004.

[35] STEVENHAGEN, P.; LENSTRA, H. W. **Chebotarëv and his density theorem**. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

[36] VAN TILBORG, H. C. **Fundamentals of cryptology: a professional reference and interactive tutorial**, volume 528. Springer Science & Business Media, 2006.

[37] VIGENÈRE, B. D. **Traicté des chiffres**. *Secretes manieres d'escrire (Abel L'Angelier: Paris, 1586), fol. 336r*, 1951.

[38] VOLOCH, J. F. **Raizes primitivas e a conjectura de Artin**.