Números primos e criptografia RSA

Mirella Kiyo Okumura

Números primos e criptografia RSA

Mirella Kiyo Okumura

Orientador: **Prof. Dr. Miguel Vinícius Santini Frasson**

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre – Programa de Mestrado Profissional em Matemática. *VERSÃO REVISADA*.

USP – São Carlos
Março de 2014

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

O41n

Okumura, Mirella Kiyo
Números primos e criptografia RSA / Mirella Kiyo Okumura; orientador Miguel Vinícius S. Frasson. -- São Carlos, 2014.
41 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2014.

1. Números primos. 2. Criptografia RSA. 3. Aritmética modular. 4. Atividades em sala de aula. I. Frasson, Miguel Vinícius S., orient. II. Título.

Para minha família …

Agradecimentos

Agradeço a Deus por sempre cuidar do meu caminho e por proporcionar condições para que eu pudesse chegar até aqui.

Aos meus pais, responsáveis por minha formação pessoal e profissional, que me deram as melhores oportunidades de estudo e base para crescer e alcançar meus objetivos. Agradeço também a eles e a toda a minha família pela compreensão, apoio e incentivo para que eu pudesse concluir este curso. Ao Ricardo, pelo companheirismo, pela paciência e por ter me dado força nos momentos mais difíceis.

Ao professor Miguel Frasson, meu orientador, pela dedicação, pelos ensinamentos, pela paciência e pela força que me deu para que este trabalho fosse concluído.

Aos colegas do PROFMAT que dividiram comigo todas as inseguranças, angústias e alegrias que tivemos durante toda essa jornada. A todos os meus amigos, por acreditarem em mim e pelos os momentos de lazer e divertimento que passamos juntos.

À coordenadora, professora Ires Dias, que esteve sempre ao nosso lado nos apoiando diante das dificuldades e compartilhando os momentos bons e ruins durante todo o curso.

Aos professores do PROFMAT, pelo conhecimento transmitido, compreensão, incentivo, pelas manhãs e tardes de sábado que passaram com a gente. Em especial, ao professor Hermano que sempre nos incentivou e não mediu esforços para nos ajudar e nos aliviar nos momentos difíceis.

À SBM e à CAPES, pela iniciativa, visando a tão necessária melhoria do ensino de matemática na Educação Básica de nosso país. Ao ICMC, por nos proporcionar um ambiente favorável aos estudos.

Enfim, a todos que participaram direta ou indiretamente deste trabalho.

Resumo

Estudamos a criptografia RSA como uma importante aplicação dos números primos e da aritmética modular. Apresentamos algumas sugestões de atividades relacionadas ao tema a serem desenvolvidas em sala de aula nas séries finais do ensino fundamental.

Abstract

We studied RSA cryptography as an important application to prime numbers and modular arithmetic. We present some suggestions of activities related to the subject to be developed in classrooms of the final years of elementary school.

Sumário

1 Números primos **3**

1.1 Teorema Fundamental da Aritmética 3
1.2 A infinidade dos primos 4
1.3 O reconhecimento dos primos 4
1.4 A distribuição dos primos 5
1.4.1 O Teorema dos Números Primos 5

2 Testes de primalidade **7**

2.1 Fatoração 7
2.1.1 Algoritmo usual 7
2.1.2 Fatoração de Fermat 8
2.2 O Crivo de Eratóstenes 8
2.3 Fermat e os pseudoprimos 10
2.4 Teorema de Wilson 11
2.5 O custo dos algoritmos 11
2.5.1 Complexidade computacional 11

3 Criptografia RSA **13**

3.1 A inspiração 13
3.2 A origem do método 13
3.3 Descrição matemática do método 14
3.3.1 Como escolher as chaves de encriptação e decriptação? 14
3.4 $D(E(M)) = M = E(D(M))$ 15
3.5 Por que o RSA é seguro? 16
3.5.1 Dificuldade de se fatorar n 16
3.5.2 Conhecer $\phi(n)$ é o mesmo que fatorar n 16
3.5.3 Conhecer d é o mesmo que fatorar n 16
3.5.4 Calcular D de uma outra forma 16
3.6 Exemplo de mensagem criptografada 17
3.7 Assinatura digital 20

4 Aplicações em sala de aula **21**
4.1 Calculando potências de um jeito diferente 21
4.2 Código de César e a contagem de frequências 22
4.3 Criptografando 26
4.4 Jogo – Dias da semana 27
4.5 Jogo – Torre, parede ou contêiner? 29
4.6 Jogo – Amarelinha de números primos 30

A Teoria dos números **33**
A.1 A aritmética modular 33
A.2 As classes residuais e sua aritmética 33
A.2.1 O anel das classes residuais 34
A.3 Sistema completo de Resíduos 36

B Demonstrações **37**
B.1 Pequeno Teorema de Fermat 37
B.2 Teorema de Wilson 37
B.3 Propriedade da Seção 3.4 38

Notação **39**

Referências Bibliográficas **41**

Introdução

A existência de uma forma de comunicação secreta se mostra necessária há muito tempo, seja para a troca de mensagens num "romance proibido" ou para auxiliar os governantes no comando de exércitos durante as guerras.

A primeira ideia foi ocultar essas mensagens, técnica conhecida como esteganografia (do grego — "escrita coberta"), muito utilizada antigamente através de tabuletas de madeira, escritas no couro cabeludo, em ovos cozidos e até utilizando leites de plantas que quando secos ficavam invisíveis, mas quando expostos ao calor, tomavam a cor marrom — as famosas tintas invisíveis. Apesar de essas mensagens estarem escondidas, caso fossem descobertas, apareceriam de forma explícita, entregando segredos preciosos ou revelando informações para tropas inimigas.

Tal risco motivou a criação de códigos e cifras, com o objetivo de esconder não só a mensagem, mas também o seu significado, de modo que apenas o destinatário pudesse decifrá-la. O primeiro uso documentado da criptografia foi em torno de 1900 a.c., no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição.

A forma mais simples de codificação de mensagens consiste em substituir uma letra pela seguinte; isto é, deslocar o alfabeto uma casa para diante. Um código semelhante foi utilizado por Júlio César para comunicar-se com as legiões em combate pela Europa. No Código de César, cada letra da mensagem original era substituída pela letra que fica três posições à sua frente no alfabeto.

Outra forma de codificar mensagens consiste em substituir letras por outras letras ou por símbolos. Esse método foi bastante usado por algum tempo mas perdeu sua utilidade quando foi descoberta a contagem de frequências. Em cada língua, se analisarmos textos suficientemente grandes, a frequência com que cada letra do alfabeto se repete é quase constante, ficando fácil descobrir qual letra ou símbolo está substituindo cada letra original e, consequentemente, decifrar o texto codificado.

Com a evolução dos meios de comunicação, tornou-se necessário desenvolver métodos confiáveis de codificação de mensagens. Isso ocorreu com o surgimento da criptografia de chave pública, notável por sua simplicidade e grande dificuldade de violação. Também conhecida por criptografia assimétrica, este é um método em que duas chaves distintas são utilizadas. Uma dessas chaves — a *chave pública* — é divulgada livremente e usada para codificar mensagens, que só poderão ser decodificadas por quem tiver posse da *chave privada* correspondente. O mais famoso método desse tipo de criptografia é o RSA, assunto do Capítulo 3 e tema central deste trabalho.

Os Capítulos 1 e 2 apresentam propriedades dos números primos e descreve alguns testes de primalidade, mostrando a grande dificuldade de se fatorar números. A importância desse fato cresce quando, no Capítulo 3, mostramos que a dificuldade de se quebrar o RSA é, provavelmente, a mesma de se fatorar um número grande. Finalmente, o Capítulo 4 propõe diversas sugestões de atividades para séries do Ensino Fundamental, que abordam alguns dos temas desenvolvidos neste texto.

Capítulo 1

Números primos

Um número é dito *primo* quando é maior que 1 possui exatamente dois divisores naturais: 1 e ele mesmo. Esses números são os átomos da aritmética. São números indivisíveis, que não podem ser representados pela multiplicação de dois números menores.

A importância matemática dos primos é que, a partir deles, conseguimos construir todos os outros números através da multiplicação. Por exemplo, sabemos que ao se tratar da operação de soma, partindo do zero e somando 1 consecutivamente, podemos obter os demais naturais. Se utilizássemos a mesma técnica para a multiplicação, não teríamos sucesso, pois ao multiplicar qualquer número por 1, não sairíamos do lugar.

Um número que não é primo é dito *composto*. Todo número composto é múltiplo de algum número primo. Consequentemente, todo número composto é um produto de primos.

Apesar de sua aparente simplicidade e de seu caráter essencial, os números primos perduram como os objetos mais misteriosos já estudados pelos matemáticos. Se observarmos uma lista de números primos, veremos que é impossível prever quando surgirá o próximo deles; ela não nos fornece qualquer pista sobre como determinar o próximo número.

1.1 Teorema Fundamental da Aritmética

O **Teorema Fundamental da Aritmética** ou **Teorema da Fatoração Única** garante que todo número inteiro, com módulo maior que 1, possui uma única fatoração em primos, a menos pela ordem dos fatores. Assim, dizemos que os números primos são aqueles que geram os demais a partir da operação de multiplicação.

Este Teorema encontra-se demonstrado através de duas proposições dadas por *Euclides* no Livro VII de seus *Elementos* [4, Prop. 30 e 32]:

Proposição 1.1. *Se o produto de dois números é divisível por um certo fator primo, então esse mesmo fator divide um dos dois números.*

Proposição 1.2. *Todo número ou é primo ou é múltiplo de algum primo.*

1.2 A infinidade dos primos

Teorema 1.3. *Existem infinitos números primos.*

Para este teorema existem várias demonstrações conhecidas. Segue a demonstração também dada por Euclides [4, Lv. IX, prop. 20]:

Demonstração. Suponha que exista apenas um número finito de números primos $p_1, \ldots, p_r$. Considere o número natural $n = p_1 p_2 \ldots p_r + 1$. O número n possui um fator primo p que, portanto, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, p divide o produto $p_1 p_2 \ldots p_r$. Mas isto implica que p divide 1, o que é absurdo. □

1.3 O reconhecimento dos primos

Não se conhece nenhuma fórmula simples para gerar números primos arbitrariamente grandes. Essa questão tem atormentado as mentes matemáticas de todas as épocas. Depois de mais de dois mil anos de esforços, os primos parecem resistir a qualquer tentativa de encaixá-los em um padrão reconhecível.

Algumas fórmulas produzem números primos:

- $x^2 - x + 41$ fornece primos quando $x = 0, 1, 2, \ldots, 40$.
  (Se $x = 41$, a fórmula resulta em 41^2 que não é primo).
- $2^{2^n} + 1$, chamados de números de Fermat e denotados por F_n. (Fermat acreditava que sua fórmula resultaria em diversos primos, porém, apenas os cinco primeiros números gerados por sua fórmula são conhecidamente primos: $F_0 = 3; F_1 = 5; F_2 = 17; F_3 = 257$ e $F_4 = 65.537$).

Outras fórmulas são tão complicadas que não ajudam muito nem a gerar números primos explicitamente nem a responder perguntas teóricas sobre a distribuição dos primos. Um exemplo disso é a fórmula para determinar p_n, o n-ésimo primo:

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor$$

onde

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0,0203000500000007...$$

e $\lfloor x \rfloor$ denota o menor inteiro maior ou igual a x. A inutilidade desta fórmula vem do fato que para calcular c devemos encontrar todos os primos; a fórmula

se tornaria mais interessante se existisse outra interpretação para o número real c, o que parece muito improvável.

Uma questão relacionada com a de gerar números primos é a de *testar* se um determinado número é primo. Com a chegada dos computadores surgiram inúmeras tentativas de se obter um algoritmo eficiente para o teste de primalidade de um número. A importância desse problema tem crescido imensamente devido à utilização intensa de números primos em algoritmos de criptografia. Dessa forma, o problema do teste de primalidade se tornou um importante problema para a ciência da computação teórica.

1.4 A distribuição dos primos

1.4.1 O Teorema dos Números Primos

O Teorema dos Números Primos descreve a distribuição assintótica dos números primos, isto é, de como os primos estão distribuídos entre os números inteiros. Através desse teorema, formaliza-se a ideia de que quanto maiores, os primos se tornam menos frequentes.

Dizemos que $a(x)$ é assintótica a $b(x)$ (ou $a(x) \sim b(x)$) se o limite da razão $\frac{a(x)}{b(x)}$ é 1, quando x tende ao infinito. Isso não significa que a diferença entre essas funções seja pequena, por exemplo, x^2 é assintótica a $x^2 - x$, mas a diferença entre elas, x, cresce à medida que x tende ao infinito.

Seja $\pi(x)$ a função que retorna a quantidade de primos menores ou iguais a x. O Teorema dos Números Primos declara que $x/\ln(x)$ é uma boa aproximação para $\pi(x)$ uma vez que

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

ou seja, $\pi(x) \sim x/\ln(x)$.

Com isso, podemos usar $x/\ln(x-a)$, para qualquer constante a, para aproximar $\pi(x)$. No Teorema dos Números Primos temos $a = 0$, mas estudos mostraram que $a = 1$ é a melhor escolha para essa aproximação. Dessa forma, podemos ter uma boa aproximação de $\pi(x)$ através de $x/\ln(x-1)$. Se $p(n)$ é o enésimo primo, através desse teorema também podemos concluir que $p(n) \sim n \cdot \ln(n)$. Por fim, ainda pode-se afirmar que se um número inteiro for escolhido aleatoriamente no intervalo de 0 até N, a probabilidade de que o número escolhido seja primo é cerca de $1/\ln(N)$.

Há ainda muito o que se dizer sobre os números primos e sua distribuição. Alguns resultados, porém, fogem do objetivo desse texto por sua grande complexidade matemática. Aos interessados, recomendamos a leitura do artigo [12], que trata do teorema e menciona um dos problemas não resolvidos mais importantes da matemática — a hipótese de Riemann — e sua relação

com os números primos, como por exemplo, a precisão das estimativas de sua distribuição entre os números inteiros.

Capítulo 2

Testes de primalidade

2.1 Fatoração

Já sabemos que todo número ou é primo ou é um produto de números primos. O processo de encontrar os fatores primos de um número composto denomina-se fatoração. Existem diversos algoritmos de fatoração. A eficiência destes algoritmos depende do tipo de fator que tem o número que queremos fatorar. Quando tomamos um número suficientemente grande, fatorá-lo pode se transformar em uma tarefa muito trabalhosa e, consequentemente, demorada. Não existe um algoritmo de fatoração que funcione bem (no sentido de que um computador o possa executar em tempo viável) para todos os números inteiros. E é nessa dificuldade em que se baseiam os métodos de criptografia atuais, como a criptografia RSA que veremos mais adiante.

2.1.1 Algoritmo usual

A ideia mais intuitiva para se tentar fatorar um número é tentar dividir esse número por cada um dos inteiros positivos menores do que seu valor absoluto. Caso alguma das divisões resulte em um número inteiro, pelo menos dois fatores do número original foram desvendados. Caso contrário, o número é primo. O algoritmo caracteriza um teste de primalidade, pois ao final do procedimento podemos determinar se um número é primo ou composto. Mas caso o número seja muito grande, esta técnica mostra-se inviável. Logo percebeu-se que, caso um número N fosse composto: $N = a \cdot b$, um dos fatores a ou b seria, necessariamente, menor ou igual a $\sqrt{N}$.

Demonstração. De fato,

$$1 < a < N$$
$$1 < b < N$$

Seja $a \leqslant b$:

$$a \leqslant b \Rightarrow a^2 \leqslant a \cdot b$$

Mas $a \cdot b = N$ e isso implica $a^2 \leqslant N$. Assim, $a \leqslant \sqrt{N}$, como queríamos demonstrar. □

Dessa forma, para determinar se um número N é primo ou composto, calcula-se o resto da divisão de N por cada primo menor ou igual que $\sqrt{N}$. Se algum do restos for igual a zero, N é composto e pelo menos dois fatores de N foram desvendados. Caso isso não ocorra, N é primo.

2.1.2 Fatoração de Fermat

Outra forma de fatoração foi proposta por Fermat e é muito eficiente no caso de n ter um de seus fatores próximos de $\sqrt{N}$. Suponha que N seja um número inteiro. Suponhamos, sem perda de generalidade, N ímpar (uma vez que se N for par, alguma potência de 2 será um de seus fatores e poderíamos descartá-la). O algoritmo consiste em tentar encontrar números inteiros x e y tais que $N = x^2 - y^2$. Encontrados tais números, teremos:

$$N = x^2 - y^2 = (x + y)(x - y)$$

Dessa forma, $(x - y)$ e $(x + y)$ são os fatores de N. Por outro lado, se $N = a \cdot b$, com $a \geqslant b \geqslant 1$, sempre podemos escrever:

$$N = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

O objetivo é encontrar x tal que $x^2 - N = y^2$, para algum valor de y. Tome k o menor inteiro maior que $\sqrt{N}$. Se $x = k$ for uma solução da equação acima, encontramos um fator de N. Caso contrário, tome $x = k+1$, e assim por diante. O processo se repete até que se encontre um fator não trivial de N ou se chegue em $x = (N+1)/2$, que nos dá a fatoração trivial, concluindo que N é primo.

2.2 O Crivo de Eratóstenes

Uma outra maneira para determinar a primalidade dos números foi proposta por Eratóstenes, no século III A.C.. Eratóstenes propôs um crivo, que posteriormente herdou o seu nome, onde os números até N são colocados em forma de lista na sua ordem natural e vão sendo eliminados caso sejam múltiplos de um primo menor que ele (até $\sqrt{N}$). Ao final deste processo, os números que sobraram, ou seja, aqueles que não foram eliminados, são os números primos dessa lista.

O método descrito constitui a base da teoria do crivo, que foi desenvolvida com o objetivo de fornecer estimativas da quantidade de números primos. Logo percebe-se que o crivo não nos dá esta estimativa, já que não há uma frequência na distribuição dos primos.

~~1~~	**2**	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~
101	~~102~~	**103**	~~104~~	~~105~~	~~106~~	**107**	~~108~~	**109**	~~110~~
~~111~~	~~112~~	**113**	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	**127**	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	**137**	~~138~~	**139**	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	**149**	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	**157**	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	**163**	~~164~~	~~165~~	~~166~~	**167**	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	**173**	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	**179**	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	**193**	~~194~~	~~195~~	~~196~~	**197**	~~198~~	**199**	~~200~~
~~201~~	~~202~~	~~203~~	~~204~~	~~205~~	~~206~~	~~207~~	~~208~~	~~209~~	~~210~~
211	~~212~~	~~213~~	~~214~~	~~215~~	~~216~~	~~217~~	~~218~~	~~219~~	~~220~~
~~221~~	~~222~~	**223**	~~224~~	~~225~~	~~226~~	**227**	~~228~~	**229**	~~230~~
~~231~~	~~232~~	**233**	~~234~~	~~235~~	~~236~~	~~237~~	~~238~~	**239**	~~240~~
241	~~242~~	~~243~~	~~244~~	~~245~~	~~246~~	~~247~~	~~248~~	~~249~~	~~250~~
251	~~252~~	~~253~~	~~254~~	~~255~~	~~256~~	**257**	~~258~~	~~259~~	~~260~~
~~261~~	~~262~~	**263**	~~264~~	~~265~~	~~266~~	~~267~~	~~268~~	**269**	~~270~~
271	~~272~~	~~273~~	~~274~~	~~275~~	~~276~~	**277**	~~278~~	~~279~~	~~280~~
281	~~282~~	**283**	~~284~~	~~285~~	~~286~~	~~287~~	~~288~~	~~289~~	~~290~~
~~291~~	~~292~~	**293**	~~294~~	~~295~~	~~296~~	~~297~~	~~298~~	~~299~~	~~300~~

Tabela 2.1: Crivo de Eratóstenes até 300.

Na tabela 2.1, foi implementado um crivo até o número 300. Como $\sqrt{300} \approx 17,3$, foram cortados os múltiplos dos primos até 17. Com isto, obtemos a lista dos primos até 300: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293.

2.3 Fermat e os pseudoprimos

Para desenvolver este assunto, usaremos elementos de aritmética modular, que recordamos brevemente no Apêndice A. Veja também [1, 5].

Teorema 2.1 (Pequeno Teorema de Fermat)**.** *Se p é um número primo e se a é um número natural tal que $p \nmid a$, então*

$$a^{p-1} \equiv 1 \mod p.$$

A demonstração encontra-se na Seção B.1 do Apêndice.

Corolário 2.2. *Se p é um número primo e se a é um número natural, então*

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

Através do Pequeno Teorema de Fermat, é possível concluir que um número é composto mesmo sem conseguir encontrar seus fatores:

Teste. Dado um número N ímpar (pois se for par e $N \geqslant 2$, N é composto), se existir um inteiro b tal que $b^N \not\equiv b \mod N$, então N é composto.

Observação. O número b, caso exista, é conhecido como uma *testemunha* do fato de N ser composto.

Um *pseudoprimo* é um número inteiro que compartilha alguma propriedade comum aos números primos mas, na verdade não é primo. Pseudoprimos podem ser classificados de acordo com a propriedade satisfeita por eles. Por exemplo, um inteiro positivo n, impar e composto, é chamado um *pseudoprimo de Fermat* para a base b (onde $1 < b < n-1$) se $b^{n-1} \equiv 1 \mod n$.

Dado um número ímpar n que satisfaz $b^{n-1} \equiv 1 \mod n$, para *alguma* base $1 < b < n-1$, podemos afirmar que ele é primo? Infelizmente não. Existem números que satisfazem a congruência acima em determinadas bases, mas que não são primos. O primeiro exemplo disso é o 341 na base 2:

$$\begin{gathered} 2^{10} = 1024 = 3 \cdot 341 + 1 \implies 2^{10} \equiv 1 \mod 341 \\ 2^{340} = (2^{10})^{34} \equiv 1^{34} \mod 341 \\ 2^{340} \equiv 1 \mod 341 \end{gathered}$$

Como 341 satisfaz o teorema de Fermat para a base 2, se a recíproca do teorema fosse verdadeira, 341 seria um número primo. Mas 341 é um número composto ($341 = 11 \cdot 31$). Dessa forma, conclui-se que 341 é um pseudoprimo de Fermat para a base 2.

2.4 Teorema de Wilson

Teorema 2.3. *p é um número primo se, e somente se,*

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

A demonstração encontra-se na Seção B.2 do Apêndice.

2.5 O custo dos algoritmos

Os testes de primalidade apresentados consistem em algoritmos cuja complexidade depende do tempo que se leva para chegar a uma conclusão. O tempo necessário, por sua vez, é proporcional ao número de operações que serão efetuadas a partir do número N a ser testado. É fácil observar que ao usar o primeiro teste citado, serão necessárias até $N-1$ operações para determinar a primalidade do número N. Já no segundo teste, esse número cai para, no máximo, $\sqrt{N}$.

Um ponto crucial é que, para números suficientemente grandes, esses algoritmos tornam-se inviáveis, dentro da tecnologia disponível atualmente. E é nisso que se baseia a segurança da Criptografia RSA, que será discutida no capítulo seguinte.

Os recordes de fatoração em vigência atualmente nos dão uma ideia da dificuldade de fatorar números, especialmente se estes são produtos de dois primos grandes, escolhidos aleatoriamente. Por exemplo, um recorde estabelecido em 2010 (ver [6]), seus autores fatoraram uma chave RSA de 232 dígitos e fizeram alguns comentários sobre a complexidade da tarefa:

> *Nós gastamos meio ano em 80 processadores em seleção polinomial. Isto foi cerca de 3% da tarefa principal, a fatoração propriamente dita, que foi feita em muitas centenas de máquinas e levou quase dois anos. Em um processador de um único núcleo AMD Opteron de 2,2 GHz com 2 GB de memória RAM, a fatoração levaria por volta de quinze mil anos. [6, p. 1].*

2.5.1 Complexidade computacional

A teoria da complexidade computacional é um ramo da teoria da computação que se concentra em classificar problemas computacionais de acordo com sua dificuldade e relacionar essas classes entre si. Um problema é considerado difícil se a sua solução requer recursos significativos, qualquer que seja o algoritmo usado. A teoria estuda modelos matemáticos de computação para quantificar os recursos necessários para resolvê-los, tais como tempo e armazenamento.

Nosso mundo está repleto de problemas em que uma solução proposta pode ser rapidamente verificada – os problemas de busca. Alguns desses problemas podem ser resovidos eficientemente, outros parecem ser muito difíceis. A classe NP (nondeterministic polynomial time) é a classe de todos os problemas de busca e a classe P (polynomial time) é a classe de todos os problemas de busca que são resovidos em tempo polinomial. Essa definição faz com que P seja uma sub-classe de NP, ou seja, $P \subseteq NP$. Um dos grandes problemas não resolvidos da matemática consiste em determinar se $P = NP$ ou $P \neq NP$. A maioria das pessoas acredita que $P \neq NP$ e há algumas razões para isso, no entanto, até hoje ninguém conseguiu provar esse fato (nem o contrário).

Uma das razões para se acreditar que $P \neq NP$, é uma outra classe de problemas – NP-completo – que são os problemas de busca considerados mais complexos. Na prática, os problemas NP estão na classe P ou em NP-completo, porém, para alguns problemas isso ainda não está definido: é o caso da fatoração.

Capítulo 3

Criptografia RSA

Neste capítulo, nossa principal referência foi o livro [1].

3.1 A inspiração

Um artigo publicado em 1976 por Whitfield Diffie e Martin Hellman [2] sugeria que, com o desenvolvimento das redes de computadores, algumas informações deveriam ser encriptadas antes de serem enviadas, possivelmente para estranhos. Mas se a chave fosse enviada por correio ou por e-mail, não faria muito sentido pois poderia ser interceptada. Os dois cientistas da computação propuseram um novo método para que a chave fosse enviada de forma segura, em que todas as informações necessárias para a troca eram disponibilizadas publicamente. A ideia consiste em usar uma função que seja fácil de se calcular mas computacionalmente difícil de inverter, a menos que se conheça o segredo. É a chamada *"função arapuca" (trap-door one-way function)*.

Um criptossistema de chave pública deve conter um esquema público de encriptação E e um esquema privado de decodificação D, em que D e E são fáceis de calcular e, para uma mensagem M, $D(E(M)) = M = E(D(M))$.

3.2 A origem do método

Pouco depois da publicação deste artigo, três amigos, estudantes do Massachusetts Institute of Technology (MIT) passaram a buscar um novo tipo de criptografia, satisfazendo às condições propostas por Diffie e Hellman. Para isso, eles estabeleceram a seguinte dinâmica: dois deles — Ron e Adi — davam ideias de como "esconder" uma mensagem e Len tentava adivinhar a técnica utilizada. Len estava indo bem até que num certo dia, Ron trouxe um algoritmo que Len não conseguiu quebrar. Esse algoritmo — chamado

RSA [9] (em homenagem aos seus criadores: Ronald Rivest, Adi Shamir e Leonard Adleman) — permanece inviolado até os dias de hoje.

Durante esses quase 40 anos, pesquisadores encontraram algumas fraquezas na implementação do algoritmo, que foram sendo corrigidas. Porém, ele resistiu a todos os ataques que as melhores mentes da criptografia puderam imaginar. Como um primeiro exemplo dos chamados criptossistemas de chave pública e o único que resistiu a mais de 30 anos de ataques, o RSA se tornou a melhor alternativa para encriptar as transações com cartões de crédito via internet, segurança de e-mails e autenticação de chamadas telefônicas.

3.3 Descrição matemática do método

Para criptografar uma mensagem M, usando uma chave pública (e, n), onde e e n são inteiros positivos, façamos o seguinte:

- Represente a mensagem como um inteiro entre 0 e $n-1$. (Se a mensagem for longa, quebre-a em blocos de modo que isso possa ser feito).
- Criptografe a mensagem elevando cada bloco M à "e-ésima" potência módulo n. Então, o resultado criptografado C é o resto da divisão de M^e por n:
$$C \equiv M^e \mod n.$$
- Para decifrar a mensagem criptografada, eleve-a a uma outra potência d e calcule o resto da divisão de C^d por n. Assim,
$$M \equiv C^d \mod n.$$

Observe que a criptografia não aumenta o tamanho da mensagem, tanto a mensagem original quanto a criptografada são inteiros entre 0 e $n-1$.

3.3.1 Como escolher as chaves de encriptação e decriptação?

Primeiramente, tome n como sendo o produto de dois primos p e q:

$$n = p \cdot q.$$

Tomando p e q grandes, podemos tornar n público, pois a grande dificuldade de fatorá-lo fará com que os fatores p e q fiquem implícitos. Escolha um inteiro d que seja primo com $\phi(n) = (p-1)(q-1)$, isto é,

$$\text{mdc}(d, \phi(n)) = 1.$$

Por último, escolhemos e a partir de p, q e d, onde e e d devem ser inversos multiplicativos módulo $\phi(n)$:

$$e \cdot d \equiv 1 \mod \phi(n).$$

3.4 $D(E(M)) = M = E(D(M))$

No início deste capítulo, citamos a ideia de Diffie-Hellman, que sugeria uma função em que, para uma mensagem M, $D(E(M)) = M = E(D(M))$. O método de criptografia apresentado na seção anterior satisfaz essa condição e o objetivo desta seção é comprovar isso matematicamente.

Seja a um dos blocos da mensagem M. Queremos mostrar que $(a^e)^d \equiv (a^d)^e \equiv a \mod n$, onde e e d são as chaves de encriptação e decriptação, respectivamente. Uma das propriedades de potências transforma os expoentes em um produto de números inteiros, que é comutativo. Assim, basta mostrar que $(a^e)^d \equiv a \mod n$. Para iniciar a comprovação, usaremos a seguinte propriedade cuja demonstração encontra-se na seção B.3 do apêndice:

$$a \equiv b \mod pq \quad \Leftrightarrow \quad \begin{cases} a \equiv b \mod p \\ a \equiv b \mod q. \end{cases}$$

Pela seção anterior, sabemos que $e \cdot d \equiv 1 \mod \phi(n)$, $\phi(n) = (p-1)(q-1)$. Através dessas informações, podemos concluir que

$$e \cdot d = k(p-1)(q-1) + 1$$

para algum $k \in \mathbb{N}$. Dessa forma, queremos mostrar que

$$a^{k(p-1)(q-1)+1} \equiv a \mod pq. \tag{3.1}$$

Observe que, segundo a propriedade enunciada acima, para provar o que queremos, basta mostrar:

1. $a^{k(p-1)(q-1)+1} \equiv a \mod p$
2. $a^{k(p-1)(q-1)+1} \equiv a \mod q$.

Demonstração. (1): Se $p \mid a$, então $0 \equiv a \equiv a^{k(p-1)(q-1)+1} \mod p$, o que mostra (3.1). Se $p \nmid a$, pelo teorema 2.1, temos:

$$a^{p-1} \equiv 1 \mod p$$

o que implica

$$[a^{p-1}]^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 \mod p.$$

Podemos multiplicar a equivalência por a, obtendo

$$a^{k(p-1)(q-1)+1} \equiv a \mod p.$$

A prova de (2) é análoga. □

Com isso, conseguimos mostrar que em todo bloco a de uma mensagem M, criptografada segundo o método RSA, se usarmos as duas chaves, e e d, independente da ordem, voltamos ao bloco original.

3.5 Por que o RSA é seguro?

Vimos anteriormente que a Criptografia RSA é um método de chave pública. A chave de codificação (e, n) é acessível a todos. Podemos tentar quebrar o código através de propriedades desses números e algumas relações matemáticas. Lembrando que, quanto maior a dificuldade de se descobrir d, p, q ou $\phi(n)$, maior será a segurança do método.

3.5.1 Dificuldade de se fatorar n

Na criptografia RSA, a chave n é pública e, se conseguirmos fatorá-la, fica fácil determinar d. Dessa forma, fatorar n significa quebrar o código. No Capítulo 2, vimos quão complexa pode ser a tarefa de se fatorar um número. Quando esse número é o resultado da multiplicação de dois primos grandes, isso pode se tornar ainda mais complicado, não existindo algoritmos eficientes o bastante para realizar a fatoração em tempo hábil. É nessa fraqueza que se baseia a segurança da Criptografia RSA.

3.5.2 Conhecer $\phi(n)$ é o mesmo que fatorar n

Sabemos que n é o produto de dois primos p e q. Então,

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

Com isso, podemos escrever

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

Logo, p e q são as raízes da equação do 2º grau

$$x^2 - \big(n + 1 - \phi(n)\big)x + n = 0.$$

Isto mostra conhecer $\phi(n)$ implica em fatorar n.

3.5.3 Conhecer d é o mesmo que fatorar n

Vimos, na Seção 3.3.1, que $e \cdot d \equiv 1 \mod \phi(n)$. Se conhecermos d, sabemos que $e \cdot d - 1$ é um múltiplo de $\phi(n)$. Miller [8] (apud [9]) mostrou que n pode ser fatorado a partir de qualquer múltiplo de $\phi(n)$. Porém, se n for muito grande, esta tarefa é equivalente em dificuldade a fatorar n.

3.5.4 Calcular D de uma outra forma

Outra maneira de quebrar o RSA seria extraindo a raiz "e-ésima" de cada bloco da mensagem criptografada, obtendo assim, o bloco original da mensagem. Embora não se conheça a real complexidade dessa tarefa (principalmente quando e e n são muito grandes), não existe algoritmo eficiente

para realizar esses cálculos computacionalmente. Com isso, acredita-se que executar tal tarefa seja um método eficiente de fatorar n. Ver [1, 9].

3.6 Exemplo de mensagem criptografada

Para ilustrar o método de criptografia RSA, iremos criptografar a palavra **PROFMAT**. Antes de iniciar o processo de codificação propriamente dito fazemos uma pré-codificação, que consiste em converter a mensagem em uma sequência de números. Para essa conversão, usaremos a seguinte tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 3.1: Tabela de conversão.

Convertendo nossa mensagem letra a letra, obtemos: $P = 25, R = 27, O = 24, F = 15, M = 22, A = 10, T = 29$. Assim, a mensagem a ser encriptada é dada pelo número: 25272415221029. Para este exemplo, especificamente, iremos trabalhar com números primos pequenos, afim de que os cálculos possam ser verificados facilmente. É importante observar que para uma maior segurança no método sejam escolhidos fatores grandes, pela dificuldade da fatoração vista no capítulo anterior. Sejam $p = 17$ e $q = 19$, temos que $n = p \cdot q = 17 \cdot 19 = 323$. E ainda, $\phi(n) = (p-1) \cdot (q-1) = 16 \cdot 18 = 288$.

Para iniciar o processo, devemos "quebrar" a mensagem em blocos, de modo que cada um deles seja menor do que $n = 323$, assim:

252	72	41	52	210	29
M_1	M_2	M_3	M_4	M_5	M_6

Cada um desses blocos será criptografado pela fórmula $C_i \equiv (M_i)^e \mod n$ (para este exemplo foi escolhida a chave pública $e = 5$):

$$\begin{aligned}
C_1 \equiv 252^5 \mod 323 &\implies C_1 \equiv 199 \mod 323 \\
C_2 \equiv 72^5 \mod 323 &\implies C_2 \equiv 21 \mod 323 \\
C_3 \equiv 41^5 \mod 323 &\implies C_3 \equiv 300 \mod 323 \\
C_4 \equiv 52^5 \mod 323 &\implies C_4 \equiv 86 \mod 323 \\
C_5 \equiv 210^5 \mod 323 &\implies C_5 \equiv 58 \mod 323 \\
C_6 \equiv 29^5 \mod 323 &\implies C_6 \equiv 3 \mod 323
\end{aligned}$$

Dessa forma, a mensagem encriptada será 199.21.300.86.58.3.

Mensagem Original	252.72.41.52.210.29
Mensagem Criptografada	199.21.300.86.58.3

A partir da mensagem criptografada 199.21.300.86.58.3 e da chave privada d (correspondente à chave pública $e = 5$) podemos desfazer a criptografia e verificar os cálculos realizados. Observe que ainda não temos o valor d. Esse é o motivo de termos escolhido números pequenos para este exemplo. Através de poucos cálculos é possível encontrar $d = 173$, pois $5 \cdot 173 = 865 = 3 \cdot 288 + 1$. Portanto, 5 e 173 são inversos multiplicativos mod 288 ($e \cdot d \equiv 1 \mod \phi(n)$). Para cada bloco da mensagem criptografada, faremos $M_i \equiv (C_i)^d \mod n$.

$$\begin{aligned}
M_1 \equiv 199^{173} \mod 323 &\implies M_1 \equiv 252 \mod 323 \\
M_2 \equiv 21^{173} \mod 323 &\implies M_2 \equiv 72 \mod 323 \\
M_3 \equiv 300^{173} \mod 323 &\implies M_3 \equiv 41 \mod 323 \\
M_4 \equiv 86^{173} \mod 323 &\implies M_4 \equiv 52 \mod 323 \\
M_5 \equiv 58^{173} \mod 323 &\implies M_5 \equiv 210 \mod 323 \\
M_6 \equiv 3^{173} \mod 323 &\implies M_6 \equiv 29 \mod 323
\end{aligned}$$

Obtemos, então, a mensagem original 252.72.41.52.210.29. Como as letras do nosso alfabeto foram convertidas em números, de acordo com a Tabela 3.1, sabemos que cada uma delas é representada por um número de 2 algarismos. Reorganizando a mensagem: 25.27.24.15.22.10.29, que corresponde à palavra **PROFMAT**.

Observação. Uma planilha eletrônica com um aplicativo em VBA (*Visual Basic for Applications*) — Figura 3.3 — foi desenvolvida para auxiliar na realização dos cálculos desta seção. O algoritmo empregado é o apresentado na atividade da Seção 4.1, p. 21. As figuras 3.1 e 3.2 ilustram a utilização da planilha:

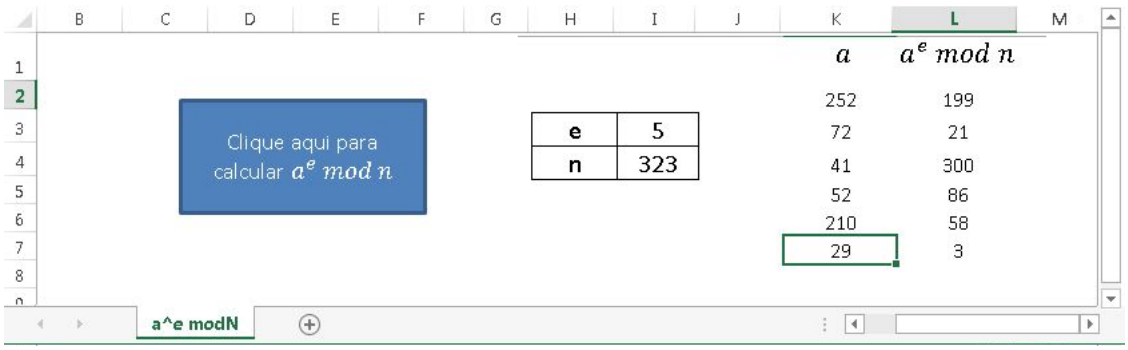

Figura 3.1: Planilha eletrônica encriptando a mensagem.

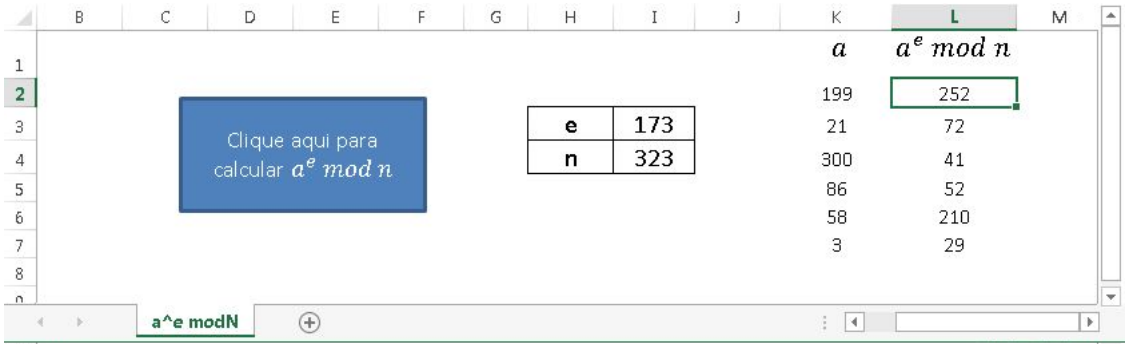

Figura 3.2: Planilha eletrônica decriptando a mensagem.

```
Private Sub CalculaModN()
    Dim xA, xE, xN, xP As Integer
    xA = txtA.Text
    xE = txtE.Text
    xN = txtN.Text
    xP = 1
    Do while xE <> 0
        If xE Mod 2 = 1 Then
            xP = (xA * xP) Mod xN
            xE = (xE - 1) / 2
        Else
            xE = xE / 2
        End If
        xA = (xA * xA) Mod xN
    Loop
    txtModN.Text = xP
End Sub
```

Figura 3.3: Código em VBA utilizado em planilha eletrônica.

3.7 Assinatura digital

Uma forma bastante segura e eficaz de se esconder uma mensagem é codificá-la usando duas chaves — uma pública e outra privada. Para uma mensagem M, faz-se $E_b(D_a(M))$, onde E_b é a chave pública do destinatário e D_a é a chave privada do emissor. Ao receber essa mensagem, o destinatário deverá utilizar a chave pública do emissor, juntamente com a sua chave privada, para decifrar a mensagem.

A grande vantagem desse método é a segurança oferecida. É mais confiável, pois ao cifrar uma mensagem usando uma chave pública, somente o dono da chave privada correspondente poderá decodificá-la; além disso, é possível também cifrar a mensagem usando uma chave privada fazendo com que quem possua a chave pública correspondente possa se certificar da autoria da mensagem — a assinatura digital.

Capítulo 4

Aplicações em sala de aula

O objetivo desse capítulo é propor atividades em que alguns dos conteúdos abordados neste texto sejam trabalhados em sala de aula com alunos do Ensino Fundamental.

4.1 Calculando potências de um jeito diferente

O algoritmo apresentado nesta seção é o mesmo descrito no paper [9] e o usado na planilha para cálculo de potências módulo n, na Seção 3.6.

Tema Potências

Objetivos Calcular potências com expoentes suficientemente grandes utilizando o sistema binário.

Conteúdos Relacionados Sistema binário de numeração, multiplicação de números naturais, propriedades de potências.

Série a que se destina 8º ano do Ensino Fundamental

Duração 4 aulas.

Recursos Pedagógicos Lousa e giz, caderno, lápis, borracha, calculadora.

Metodologia Antes de iniciar a atividade faremos uma revisão do método de conversão de um número decimal para o binário (visto no caderno do aluno — volume 1 — 7º ano). O objetivo dessa revisão é lembrar que todo número natural pode ser escrito como uma soma de potências de 2. Para isso, alguns exemplos podem ser feitos na lousa:

$$50 = 32 + 16 + 2$$
$$393 = 256 + 128 + 8 + 1$$

Para relembrar a "técnica" e fixar essa propriedade, alguns números podem ser sugeridos como exercício para que os alunos tentem fazer sozinhos e depois verifiquem com a correção feita na lousa.

A próxima etapa do processo é a retomada de um conteúdo trabalhado no 1º bimestre deste ano (8º ano).

Ao trabalhar a propriedade das potências, uma delas diz que *para calcular o produto de potências de mesma base basta conservar a base e somar os expoentes.*

Unindo essas duas propriedades vistas, para calcular a potência de um número, sendo o expoente muito grande, podemos transformar o expoente numa soma de potências de 2 fazendo com que o cálculo vire um produto de potências cujo os expoentes são potências de 2. Para ilustrar, veja os exemplos a seguir:

$$5^{50} = 5^{32+16+2} = 5^{32} \cdot 5^{16} \cdot 5^{2}$$

ou

$$4^{393} = 4^{256+128+8+1} = 4^{256} \cdot 4^{128} \cdot 4^{8} \cdot 4^{1}$$

Avaliação A avaliação ocorrerá durante todo o processo, desde o início da revisão até uma atividade avaliativa escrita. Serão observados o envolvimento e a participação do aluno em cada etapa do processo, assim como suas contribuições para o desenvolvimento das aulas e das atividades propostas.

4.2 Código de César e a contagem de frequências

Os instrumentos utilizados nesta atividade foram extraídos de [7, p.151/152]

Tema Sistemas de criptografia e a contagem de frequências

Objetivos Compreender o funcionamento da criptografia por substituição; observar a frequência com que as letras do alfabeto ocorrem em textos variados (suficientemente grandes); cálculo de frequências a partir de quantas vezes cada letra aparece com relação ao todo; interdisciplinaridade: os textos podem ser escolhidos livremente ou a partir da escolha de um tema específico.

Conteúdos Relacionados Frações – Representação; Transformação de fração em decimal; Porcentagem.

Série a que se destina 8º ano do Ensino Fundamental

Duração 3 aulas duplas

Recursos Pedagógicos Lápis e papel, calculadora, tesoura, lápis de cor.

Metodologia

- **1ª aula – Construção de instrumentos de criptografar:**

  Após uma breve introdução sobre o nascimento e a utilização de métodos para se esconder o significado de uma mensagem — criptografia, faremos a construção de um instrumento utilizado para criptografar uma mensagem segundo o Código de César, que mostramos na Figura 4.1.

Figura 4.1: Régua de codificação por substituição. Fonte: [7, p. 151].

  A construção é bem rápida e em seguida, é dado um tempo para que os alunos brinquem de esconder palavras, mas logo perceberam que é fácil de descobrir, pois são poucas as possibilidades de substituição.

  Passamos, então, para a segunda parte da aula, que é a construção do disco (ver Figura 4.2):

  Ao brincar novamente de esconder palavras, os alunos perceberão o significativo aumento na dificuldade para se decifrar. Logo, percebe-se que isso se deve ao aumento nas possibilidades, pois agora temos 26 alfabetos para fazer as substituições.

  E esse número pode ser muito maior de pudermos combinar formas de embaralhar o alfabeto, ou utilizarmos números e símbolos misturados às letras.

- **2ª aula – A contagem de frequências**

  No final da aula anterior, vimos que podemos ter muitas formas de criptografar uma mensagem usando a substituição de letras por outras letras e até por símbolos.

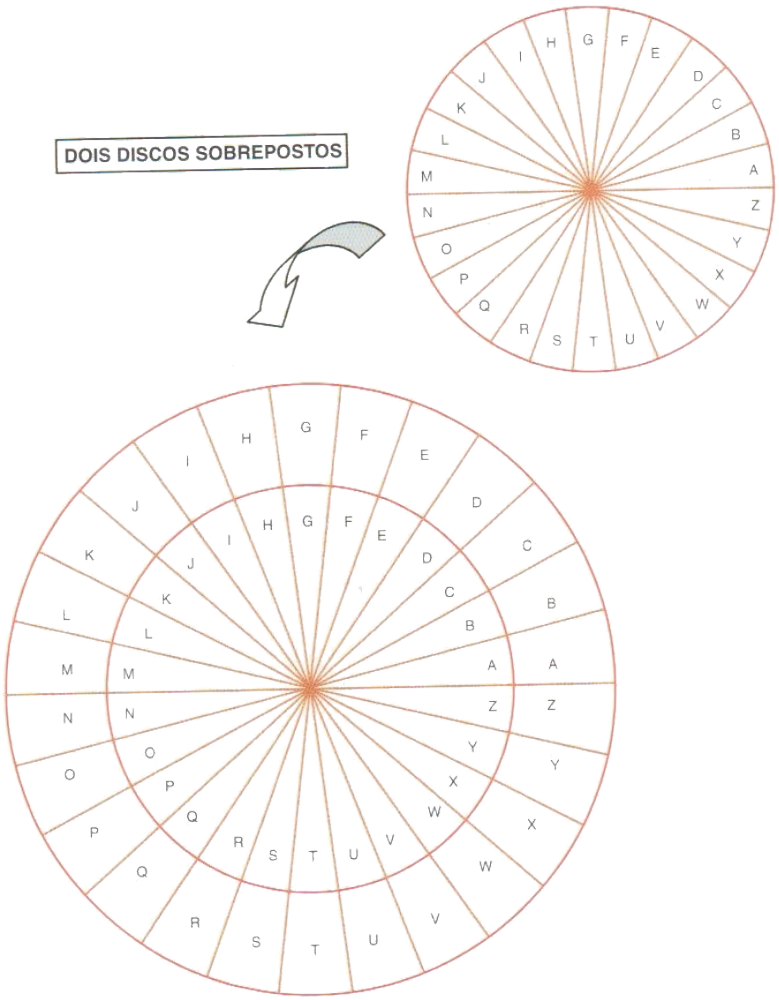

Figura 4.2: Discos de codificação por substituição. Fonte: [7, p. 152].

Para ter uma ideia de como se faz para quebrar uma mensagem desse tipo. faremos uma atividade de contagem de frequência.

Antes de começar a atividade propriamente dita, faremos uma pesquisa com os alunos, perguntando quais letras eles acham que mais aparecem quando lemos um texto. Certamente, entre as letras mais votadas estarão as vogais A, E, O e entre as consoantes, R e S.

Com a sala dividida em grupos de 4 ou 5 alunos, cada grupo trabalhará um texto fornecido ou que pode ter sido pedido anteriormente para que trouxessem. Cada grupo escolherá 3 ou 4 letras entre as que foram citadas para fazer a contagem. Cada integrante do grupo fica responsável por contar a ocorrência de cada uma dessas letras e um deles por contar todas as letras contidas no texto. Vale ressaltar, nesse momento, a importância da concentração para que não errem na contagem que estão fazendo.

Após a conclusão das contagens, pede-se que os alunos representem em forma de fração a ocorrência de cada letra com relação ao total de letras do texto.

Utilizando uma calculadora, os alunos devem transformar cada uma dessas frações em números decimais e, finalmente, em porcentagem.

Ao final dessa atividade, espera-se que os resultados obtidos sejam próximos e com isso, os alunos percebam que se fizermos o mesmo com as mensagens codificadas, é possível decifrar o segredo.

- **3ª aula – Jogo "A forca criptográfica"**

  Para finalizar esta Situação de Aprendizagem, faremos um jogo utilizando o disco construído anteriormente.

  Como no jogo da forca, cada grupo deverá codificar uma palavra, utilizando qualquer alfabeto do disco (chave) e informar sua categoria (animal, fruta, cidade, ...).

  É natural que nas rodadas iniciais, as primeiras tentativas sejam nas letras mais frequentes da nossa língua. Mas logo os alunos lembram que o alfabeto está alterado e as tentativas passam a ser aleatórias, até que a palavra seja desvendada.

  O processo se repete com cada grupo e variações podem ser feitas. Por exemplo, as palavras podem ser substituídas por ditados populares, e assim por diante.

Avaliação A avaliação ocorrerá durante todo o processo. Serão observados o envolvimento e a participação do aluno em cada etapa do processo, assim como suas contribuições para o desenvolvimento das aulas e das atividades propostas.

4.3 Criptografando

Tema Criptografia RSA

Objetivos Utilizar o método de criptografia RSA de forma simplificada para que os alunos consigam aplicar o método.

Conteúdos Relacionados Números primos, potenciação, divisão de números naturais.

Série a que se destina 8º ano do Ensino Fundamental

Duração 4 aulas

Recursos Pedagógicos Lousa e giz, caderno, lápis, borracha, calculadora.

Metodologia Utilizando o método descrito na Seção 3.3, os alunos deverão criptografar uma mensagem. Para simplificar o processo, ao invés de usarmos a chave gerada pelo produto de dois números primos, utilizaremos apenas um número primo. Dessa forma, seja a chave $n = p$ (p primo), sabemos que $\phi(n) = p - 1$ e, através desses valores, a criptografia será realizada. Como exemplo, será apresentado aos alunos o método utilizado para criptografar a palavra "MATEMATICA", utlizando as chaves $n = 23$ e $e = 3$. O primeiro passo é transformar a mensagem em números, de acordo com a tabela 3.1. Assim, a mensagem a ser criptografada é $M = 22102914221029181210$. Quebrando a mensagem em blocos menores que $n = 23$, obtemos:

22	10	2	9	14	22	10	2	9	18	12	10
M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_10	M_11	M_12

Cada um desses blocos será criptografado pela fórmula $C_i \equiv (M_i)^e \mod n$ (para este exemplo foi escolhida a chave pública $e = 3$): Durante essa explicação, será explicado aos alunos como foi obtido o resto de cada uma das divisões, utilizando somente uma calculadora comum.

$$
\begin{aligned}
C_1 \equiv 22^3 \mod 23 &\implies C_1 \equiv 22 \mod 23 \\
C_2 \equiv 10^3 \mod 23 &\implies C_2 \equiv 11 \mod 23 \\
C_3 \equiv 2^3 \mod 23 &\implies C_3 \equiv 8 \mod 23 \\
C_4 \equiv 9^3 \mod 23 &\implies C_4 \equiv 16 \mod 23 \\
C_5 \equiv 14^3 \mod 23 &\implies C_5 \equiv 7 \mod 23 \\
C_6 \equiv 22^3 \mod 23 &\implies C_6 \equiv 22 \mod 23 \\
C_7 \equiv 10^3 \mod 23 &\implies C_7 \equiv 11 \mod 23 \\
C_8 \equiv 2^3 \mod 23 &\implies C_8 \equiv 8 \mod 23 \\
C_9 \equiv 9^3 \mod 23 &\implies C_9 \equiv 16 \mod 23 \\
C_{10} \equiv 18^3 \mod 23 &\implies C_{10} \equiv 13 \mod 23 \\
C_{11} \equiv 12^3 \mod 23 &\implies C_{11} \equiv 3 \mod 23 \\
C_{12} \equiv 10^3 \mod 23 &\implies C_{12} \equiv 11 \mod 23
\end{aligned}
$$

Dessa forma, a mensagem encriptada será 22.11.8.16.7.22.11.8.16.13.3.11. Após a apresentação do método e explicações de possíveis dúvidas, será pedido aos alunos que escolham uma palavra e as chaves para que cada um faça sua criptografia. O professor deverá ficar sempre à disposição para auxiliar nas escolhas das chaves e na execução dos cálculos necessários. A atividade pode ser realizada individualmete ou em duplas.

Avaliação A avaliação ocorrerá durante todo o processo. Serão observados o envolvimento e a participação do aluno em cada etapa do processo, assim como suas contribuições para o desenvolvimento das aulas e das atividades propostas.

4.4 Jogo – Dias da semana

Tema A aritmética modular no calendário

Objetivos Desvendar a regularidade existente em nosso calendário quando queremos descobrir em qual dia da semana cai determinado dia do ano.

Conteúdos Relacionados Divisibilidade, meses do ano

Série a que se destina 8º ano do Ensino Fundamental

Duração 2 aulas

Recursos Pedagógicos

- Kit de cartas que compõem o jogo:
  - 12 cartas amarelas com os meses do ano.
  - 31 cartas azuis numeradas de 1 até 31.
- Folhas de rascunho
- Lápis e borracha
- Giz e lousa

Metodologia Cada grupo receberá um kit de cartas e um dos integrantes será escolhido (por sorteio ou pelo grupo) para conferir as respostas encontradas (esse integrante não participa do jogo). Os demais, um por vez, sortearão 2 cartas — uma de cada cor — obtendo assim uma data do calendário. (Caso a data sorteada não exista, por exemplo 30 de fevereiro, o jogador sorteia novamente).

A tarefa consiste em descobrir qual o dia da semana correspondente à data sorteada. A única informação que eles possuem é que dia 01 de Janeiro de 2013 caiu numa terça-feira.

O primeiro integrante a chegar a uma conclusão, para o jogo e confere sua resposta. Se acertar ganha 2 pontos e o jogo continua com o próximo sorteio por um outro integrante. Se errar perde 1 e, nesse caso, o jogador é eliminado e os demais continuam tentando até que algum acerte ou todos sejam eliminados. O jogo continua até que alguém atinja 10 pontos.

A ideia é que os alunos percebam que se numerarmos os dias do ano de 1 até 365 e trocarmos a data sorteada pelo número correspondente, os números que deixam mesmo resto quando divididos por 7, caem no mesmo dia da semana:

Seja x o número correspondente à data sorteada:

$$\begin{aligned}
x &\equiv 1 \mod 7 \rightarrow \text{Terça-feira} \\
x &\equiv 2 \mod 7 \rightarrow \text{Quarta-feira} \\
x &\equiv 3 \mod 7 \rightarrow \text{Quinta-feira} \\
x &\equiv 4 \mod 7 \rightarrow \text{Sexta-feira} \\
x &\equiv 5 \mod 7 \rightarrow \text{Sábado} \\
x &\equiv 6 \mod 7 \rightarrow \text{Domingo} \\
x &\equiv 0 \mod 7 \rightarrow \text{Segunda-feira}
\end{aligned}$$

Avaliação Serão observados a participação e o envolvimento dos alunos durante a atividade, assim como as estratégias utilizadas para resolver o problema e a relação com os demais integrantes do grupo.

4.5 Jogo – Torre, parede ou contêiner?

Essa atividade foi retirada de [11].

Tema Números primos e compostos

Objetivos Mostrar como os números primos nos ajudam a decidir qual a melhor maneira de arrumar caixas em um espaço determinado.

Conteúdos Relacionados Soma e fatoração de números naturais

Série a que se destina 7º ano do Ensino Fundamental

Duração 2 aulas

Recursos Pedagógicos

- 36 ou mais caixinhas de fósforos
- dado comum
- Folhas de rascunho
- Lápis e borracha
- Giz e lousa

Metodologia O jogo poderá ser realizado com a sala toda ou com a sala dividida em grupos. Antes de iniciar, é sorteada uma ordem entre os jogadores (pode ser pela ordem da lista de chamada ou sorteio no dado).

Quem começar o jogo terá como tarefa lançar o dado e "empilhar certo" esse número de caixas, seguindo essas regras:

- Se o número for *primo*, ele deve dizer *"Torre!"*, e empilhar as caixas todas uma sobre a outra, numa única pilha;
- Se o número for um *produto de dois primos*, ele deve dizer *"Parede!"*, e construir uma "parede" com as caixas, sendo o maior dos primos a altura e o menor a largura;
- Se o número for um *produto de três ou mais primos*, o jogador dirá *"Contêiner!"* e construirá um "contêiner" entre as possibilidades existentes (que dever ter profundidade de duas ou mais caixas).

Na primeira rodada, apenas os números 2, 3 e 5 serão primos (correspondem à torre). Os números 4 e 6 são produtos de dois primos e, por isso, correspondem à parede. Portanto, na primeira rodada, não existirá a opção contêiner. Na segunda rodada, cada jogador acumulará o resultado do seu primeiro lançamento com o segundo e deverá

construir “torre, parede ou contêiner” com esse número de caixinhas. O jogador que desistir de tentar a construção é eliminado da partida. As caixas são as mesmas para uso de todos. Quando um jogador ultrapassar as 36 caixas disponíveis na soma de seus lançamentos, ele será o vencedor.

Avaliação Serão observados a participação e o envolvimento dos alunos durante a atividade, assim como as estratégias utilizadas para resolver os desafios do jogo e a relação com os demais integrantes do grupo.

4.6 Jogo – Amarelinha de números primos

Essa atividade foi retirada de [3].

Tema Números primos

Objetivos Observar a irregularidade na distribuição dos primos.

Conteúdos Relacionados Números primos, raciocínio lógico.

Série a que se destina 7º ano do Ensino Fundamental

Duração 2 aulas

Recursos Pedagógicos

- Tabuleiro (Figura 4.3)
- Fichas ou tampinhas de garrafa

Metodologia O jogo é realizado em duplas — um jogador contra o outro. O primeiro jogador pega uma ficha e a coloca sobre um número primo que esteja, no máximo, a cinco passos da casa 1. O segundo jogador pega a ficha e a move para um primo maior que esteja no máximo cinco casas adiante de onde o primeiro jogador a colocou. O primeiro jogador, em seguida, move a ficha para um primo ainda maior que esteja, no máximo, cinco casas adiante. O perdedor é o primeiro jogador incapaz de mover a ficha segundo as regras. As regras são:

- A ficha não pode ser movida mais de cinco casas adiante;
- Ela deve ser movida sempre até um número primo;
- E não pode ser movida para trás nem ficar onde está.

A Figura 4.3 mostra um cenário típico. O jogador 1 perdeu porque a ficha está na casa 23, e não há primos nos cinco números seguintes a 23, que é primo.

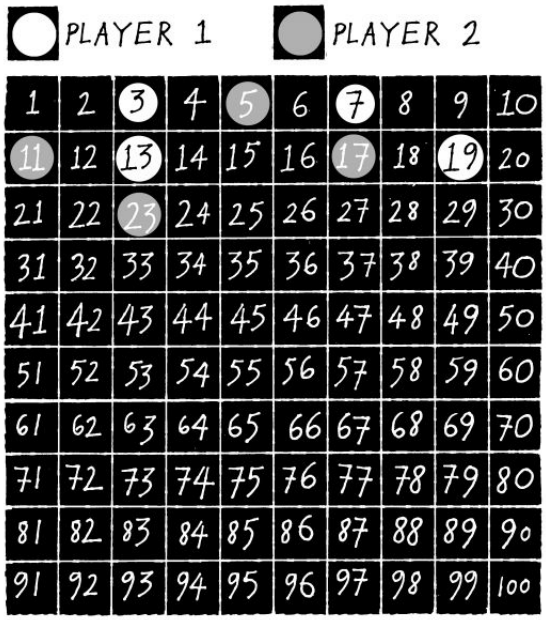

Figura 4.3: Exemplo de um jogo de amarelinha de números primos em que o movimento máximo é de cinco passos. Fonte: [3].

Avaliação Serão observados a participação e o envolvimento dos alunos durante a atividade, assim como as estratégias utilizadas para resolver os desafios do jogo e a relação com os demais integrantes do grupo.

Apêndice A

Teoria dos números

Nesse capítulo serão desenvolvidos alguns tópicos de Teoria dos Números fundamentais para o entendimento de algumas passagens e demonstrações que aparecerão mais adiante no texto.

A.1 A aritmética modular

Seja m um número inteiro diferente de zero. Diremos que dois inteiros a e b são *congruentes módulo* m se os restos de sua divisão por m são iguais e, nesse caso, escreve-se $a \equiv b \mod m$.

Quando a relação $a \equiv b \mod m$ for falsa, diremos que a e b não são congruentes módulo m. Escreveremos, nesse caso, $a \not\equiv b \mod m$.

A.2 As classes residuais e sua aritmética

A partir da divisão euclidiana, Gauss teve a ideia de desenvolver uma aritmética dos restos da divisão dos números inteiros por um número fixado e aplicá-la no desenvolvimento da teoria dos números já existente.

Atualmente, essa aritmética é a base de todos os procedimentos de cálculos computacionais e possui muitas aplicações tecnológicas. O método consiste em repartir o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números que possuem o mesmo resto quando divididos por m. Isto nos dá a seguinte partição de $\mathbb{Z}$:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z}; x \equiv 0 \mod m\} \\
[1] &= \{x \in \mathbb{Z}; x \equiv 1 \mod m\} \\
&\vdots \\
[m-1] &= \{x \in \mathbb{Z}; x \equiv m-1 \mod m\}
\end{aligned}$$

A partir daí, os restos começam a se repetir: $[m] = [0]$, $[m+1] = [1]$, e assim por diante ...

O conjunto

$$[a] = \{x \in \mathbb{Z}; x \equiv a \mod m\}$$

é chamado de *classe residual módulo* m do elemento a de $\mathbb{Z}$. O conjunto de todas as classes residuais módulo m será representado por $\mathbb{Z}_m$. Existem exatamente m classes residuais módulo m distintas, a saber: $[0], [1], \ldots, [m-1]$. Portanto,

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

A.2.1 O anel das classes residuais

Considere as seguintes operações em $\mathbb{Z}_m$:

- **Adição:** $[a] + [b] = [a + b]$
- **Multiplicação:** $[a] \cdot [b] = [a \cdot b]$

As operações que acabamos de definir, gozam das seguintes propriedades:
Propriedades da Adição:

- A_1) Associatividade
- A_2) Comutatividade
- A_3) Elemento Neutro
- A_4) Simétrico

Propriedades da Multiplicação:

- M_1) Associatividade
- M_2) Comutatividade
- M_3) Elemento Neutro
- AM) Distributividade

Um conjunto munido de uma operação de adição e de uma operação de multiplicação, com as propriedades acima, é denominado *anel*. Portanto, $\mathbb{Z}_m$, com as operações definidas acima, é um anel, chamado *anel das classes residuais módulo* m. Além disso, um anel onde todo elemento não nulo possui um inverso multiplicativo é chamado de *corpo*.

Proposição A.1. ***(Identidade de Bézout)*** *Dados números inteiros a e b, $a \cdot b \neq 0$ existem inteiros x e y tais que $a \cdot x + b \cdot y = \text{mdc}(a, b)$.*

Demonstração. Considere o conjunto das combinações lineares de a e b:

$$S = \{au + bv \mid au + bv > 0\}$$

Note primeiro que S é um conjunto não-vazio: se $a \neq 0$, então $|a| = a \cdot u + b \cdot 0$ pertence a S, basta escolher $u = 1$ ou $u = -1$, dependendo se a é positivo ou negativo. Pelo Princípio da Boa Ordenação, S deve conter um menor elemento d. Pela definição de S, existem x e y de modo que $d = a \cdot x + b \cdot y$. Vamos mostrar que $d = \text{mdc}(a, b)$. Usando o algoritmo da divisão, podemos obter inteiros q e r tais que $a = q \cdot d + r$, onde $0 \leqslant r < d$. Então, r pode ser escrito como

$$r = a - q \cdot d = a - q(a \cdot x + b \cdot y) = a(1 - q \cdot x) + b(-q \cdot y)$$

Se r fosse positivo então essa representação implicaria que $r \in S$, contradizendo o fato de d ser o menor inteiro em S. Logo, $r = 0$, e ainda, $a = q \cdot d$, ou seja, $d \mid a$. Analogamente, mostra-se que $d \mid b$, isto é, d é um divisor comum de a e b. Se c é um divisor comum de a e b, temos que $c \mid (a \cdot x + b \cdot y)$, isto é, $c \mid d$, o que implica que d é o maior divisor comum de a e b. □

Uma consequência disso é o seguinte corolário:

Corolário A.2. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros x e y tais que $x \cdot a + y \cdot b = 1$.*

Exemplo. Seja $a = 47$ e $b = 17$. Como 47 e 17 são números primos, segue que $\text{mdc}(47, 17) = 1$. Queremos encontrar inteiros x e y tais que $47 \cdot x + 17 \cdot y = 1$. Usando o algoritmo da divisão de Euclides, Podemos escrever as igualdades a seguir:

$$47 - 2 \cdot 17 = 13$$
$$17 - 13 = 4$$
$$13 - 3 \cdot 4 = 1 = \text{mdc}(47, 29)$$

Podemos reescrever as igualdades acima, voltando à notação a e b, uma vez que $a = 47$ e $b = 17$:

$$a - 2b = 13$$
$$b - (a - 2b) = 4 \Rightarrow 3b - a = 4$$
$$a - 2b - 3(3b - a) = 1 \Rightarrow 4a - 11b = 1$$

Assim, conseguimos escrever $\text{mdc}(47, 17)$ como uma combinação dos números 47 e 17:

$$4 \cdot 47 - 11 \cdot 17 = 1$$

A seguir, caracterizaremos os elementos invertíveis de $\mathbb{Z}_m$:

Proposição A.3. *$[a] \in \mathbb{Z}_m$ é invertível se, e somente se,* $\text{mdc}(a, m) = 1$.

Demonstração. ($\Rightarrow$) Hipótese: $[a]$ é invertível em $\mathbb{Z}_m$. Existe $[b] \in \mathbb{Z}_m$ tal que $[a]\cdot[b] \equiv 1 \mod m$. $a\cdot b \equiv 1 \mod m \Rightarrow a\cdot b - t\cdot m = 1 \Rightarrow \text{mdc}(a, m) = 1$
($\Leftarrow$) Hipótese: $\text{mdc}(a, m) = 1$. Existem b e t naturais tais que $a\cdot b - t\cdot m = 1$.
$[a] \cdot [b] = [a \cdot b] = [1 + m \cdot t] = [1] + [m \cdot t] = [1]$, pois $m \cdot t \equiv 0 \mod m$.
$[a] \cdot [b] = [1] \Rightarrow [a]$ é invertível em $\mathbb{Z}_m$ □

Corolário A.4. *$\mathbb{Z}_m$ é um corpo se, e somente se m é primo.*

Demonstração. ($\Rightarrow$) Suponha que $\mathbb{Z}_m$ é um corpo e m não é primo. Seja $m = m_1 \cdot m_2$ com $1 < m_1 < m$ e $1 < m_2 < m$. Logo, $[0] = [m] = [m_1] \cdot [m_2]$ com $[m_1] \neq 0$ e $[m_2] \neq 0$, o que é absurdo. Portanto, m é primo.
($\Leftarrow$) m primo $\Rightarrow \text{mdc}(i, m) = 1$ para $i = 1, 2, \ldots, m-1 \Rightarrow [1], [2], \ldots, [m-1]$ invertíveis. Logo, $\mathbb{Z}_m$ é um corpo. □

A.3 Sistema completo de Resíduos

Chamaremos de *sistema completo de resíduos* módulo m a todo conjunto de números inteiros cujos restos pela divisão por m são os números 0, 1, $\ldots$, $m - 1$, sem repetições e numa ordem qualquer. Portanto, um sistema completo de resíduos módulo m possui m elementos.

Observação. Note que, se p for primo, pela Proposição A.3, todos os elementos do sistema completo de resíduos módulo p possuem um único inverso em $\mathbb{Z}_p$. Além disso, os únicos elementos que são seu próprio inverso são 1 e $p-1$:

$$\begin{aligned} z^2 \equiv 1 \mod p &\iff (z-1)(z+1) \equiv 0 \mod p \\ &\iff z \equiv 1 \mod p \quad \text{ou} \quad z \equiv -1 \equiv p-1 \mod p. \end{aligned}$$

Apêndice B

Demonstrações

B.1 Pequeno Teorema de Fermat

Teorema B.1. *Se p é um número primo e se a é um número natural tal que $p \nmid a$, então*

$$a^{p-1} \equiv 1 \mod p$$

Demonstração. Considere os primeiros $p-1$ múltiplos de a:

$$a, 2a, 3a, \ldots, (p-1)a.$$

Sabemos que nenhum desses números é congruente módulo p com algum outro deles e nem é congruente a zero módulo p. De fato, sem perda de generalidade, se $ra \equiv sa \mod p$ com $1 \leqslant r < s \leqslant p-1$, pela regra do cancelamento (pois $p \nmid a$), teríamos $r \equiv s \mod p$, o que é uma contradição. Dessa forma, tais números formam um sistema completo de resíduos. Logo, eles são congruentes, em alguma ordem, a $1, 2, \ldots, (p-1)$. Assim,

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \mod p$$

então

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p$$

Como $p \nmid (p-1)!$, podemos dividir os dois lados da equivalência por $(p-1)!$, obtendo:

$$a^{p-1} \equiv 1 \mod p$$

como queríamos demonstrar. □

B.2 Teorema de Wilson

Teorema B.2. *p é um número primo se, e somente se,*

$$(p-1)! \equiv -1 \mod p.$$

Demonstração. ($\Rightarrow$): Se p é primo, então todo elemento de $\mathbb{Z}_p$, exceto $[-1]$ e $[1]$ (ver Seção A.3) possui um único inverso distinto de si. Logo

$$(p-2)\cdot(p-3)\ldots 3\cdot 2 \equiv 1 \mod p$$

Mas

$$(p-1)! = (p-1)\cdot(p-2)\ldots 2\cdot 1 \equiv p-1 \equiv -1 \mod p,$$

como queríamos demonstrar. □

($\Leftarrow$) Suponha por absurdo que m seja composto. Então existe um inteiro d, com $1 < d < m$, que divide m. Portanto, $(m-1)! \equiv -1 \mod d$. Por outro lado, como $d < m$, d é um divisor $(m-1)!$:

$$(m-1)! \equiv 0 \mod d,$$

o que é uma contradição. Portanto, m é primo. □

B.3 Propriedade da Seção 3.4

$$a \equiv b \mod pq \quad \Leftrightarrow \quad \begin{cases} a \equiv b \mod p \\ a \equiv b \mod q. \end{cases}$$

Demonstração. ($\Rightarrow$)

$$a \equiv b \mod pq \Rightarrow a - b = k \cdot pq$$

$$\begin{cases} a - b \equiv 0 \mod p, \\ a - b \equiv 0 \mod q. \end{cases}$$

□

($\Leftarrow$)

$$a - b \equiv 0 \mod p \Rightarrow a = k_1 \cdot p + b$$

$$a - b \equiv 0 \mod q \Rightarrow a = k_2 \cdot q + b$$

Dessa forma,

$$a - b = k_1 \cdot p$$

$$a - b = k_2 \cdot q$$

Como p e q são primos, existe um inteiro k, tal que

$$a - b = k \cdot pq \Rightarrow a - b \equiv 0 \mod pq \Rightarrow a \equiv b \mod pq$$

□

Notação

$a \mid b$	a divide b
$a \nmid b$	a não divide b
$\lfloor x \rfloor$	menor inteiro $\geqslant x$
$a \equiv b \mod n$	$n \mid a - b$
$\phi(n)$	número de inteiros entre 1 e $n-1$ primos com n

Referências Bibliográficas

[1] Coutinho, S. C. *Números inteiros e criptografia RSA*, 2ª ed., vol. 2 de *Série de Computação e Matemática*. Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2000.

[2] Diffie, W. e Hellman, M. E. New directions in cryptography. *IEEE Transactions on Information Theory 22*, 6 (November 1976), 644–654.

[3] Du Sautoy, M. *Os mistérios dos números: Uma viagem pelos grandes enigmas da matemática (que até hoje ninguém foi capaz de resolver)*, 1ª ed., Zahar, 2013.

[4] Euclides. *Os elementos*. UNESP, 2009. Tradução brasileira por Irineu Bicudo.

[5] Hefez, A. *Elementos de Aritmética*. SBM, 2010.

[6] Kleinjung, T. *et al* Factorization of a 768-bit rsa modulus. Em *Proceedings of the 30th annual conference on Advances in cryptology* (Berlin, Heidelberg, 2010), CRYPTO'10, Springer-Verlag, pp. 333–350.

[7] Malagutti, P. L. A. *Inteligência artificial no ensino*. Coleção Matemática. EdUFSCar, 2010.

[8] Miller, G. L. Riemann's hypothesis and tests for primality. Em *Seventh Annual ACM Symposium on Theory of Computing (Albuquerque, N.M., 1975)*. Assoc. Comput. Mach., New York, 1975, pp. 234–239.

[9] Rivest, R. L., Shamir, A. e Adleman, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM 21*, 2 (1978), 120–126.

[10] Singh, S. *O livro dos Códigos*, 1ª ed., Record, 2001.

[11] Wilmer, C., Ed. *MAT3MÁTICA no DIA a DIA*. Senac Editoras, 2013.

[12] Tengan, E. *O Teorema dos Números Primos – Nível U*. OBM. Acessível em 21/03/2014: ⟨`www.obm.org.br/export/sites/default/semana_olimpica/docs/2011/E_tengan_primos.pdf`⟩