UNIVERSIDADE FEDERAL DO MATO GROSSO DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO
MATEMÁTICA EM REDE NACIONAL
MESTRADO PROFISSIONAL

FATORAÇÃO DE INTEIROS

Nivaldo Alves de Souza Marques

CAMPO GRANDE - MS
29 de outubro de 2015

UNIVERSIDADE FEDERAL DO MATO GROSSO DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO
MATEMÁTICA EM REDE NACIONAL
MESTRADO PROFISSIONAL

FATORAÇÃO DE INTEIROS

Nivaldo Alves de Souza Marques
Orientadora: Profa. Dra. Elisabete Sousa Freitas

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Instituto de Matemática da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

CAMPO GRANDE - MS
29 de outubro de 2015

FATORAÇÃO DE INTEIROS

Nivaldo Alves de Souza Marques

Dissertação submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional do Instituto de Matemática da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

Banca examinadora:

Profa. Dra. Elisabete Sousa Freitas - UFMS (orientadora)
Prof. Dr. Fabrício Sérgio de Paula - UEMS
Profa. Dra. Lilian Milena Ramos Carvalho - UFMS

CAMPO GRANDE - MS
29 de outubro de 2015

Dedico aos meus pais Noel Marques e Magnória Alves de Souza Marques, que sempre me apoiaram para que eu alcançasse meus objetivos, que deixaram muitas vezes os seus sonhos para realizarem os meus e que fizeram de tudo para me proporcionar um futuro melhor.

Agradecimentos

Agradeço primeiramente a Deus, que nos momentos de maiores dificuldades segurou em minhas mãos, e quando pensei em desistir, levantou a minha cabeça e me deu forças para continuar. Além de ter me dado sabedoria e conhecimento, porque tudo isso vem Dele.

A meus pais Noel e Magnória que são os meus heróis, que sempre estiveram ao meu lado, sempre me apoiaram e que mesmo em meio às dificuldades, às vezes tendo que acordar as três horas da madrugada para me levar para estudar, nunca reclamaram e sempre fizeram de tudo para me dar o direito de aprender, ter uma boa educação e um futuro melhor. E se hoje cheguei aqui, devo muito a eles.

A mulher mais linda desse mundo, minha esposa Kauany, minha companheira que me apoiou muito e entendeu toda minha falta de atenção, minhas preocupações, meus nervosismos, minhas angústias e passou junto comigo essa caminhada, e que mesmo em pouco tempo de casados, já é o meu alicerce, o meu braço forte.

A meus irmãos Valber e Vanessa, meu cunhado Lucas, meu sobrinho Douglas e a toda minha família, que sempre entenderam minha ausência no meio familiar por estar ocupado com minhas atividades de estudo e sempre me deram força.

Aos meus colegas de mestrado, em especial, Everton, Elton e Mônica, pela grande contribuição no nosso grupo de estudos, com os lanchinhos na casa da Mônica, e pelas broncas que me deram quando quis desanimar, me ajudando a conseguir chegar até o fim.

Aos meus irmãos da igreja, principalmente ao meu pastor Luiz Carlos Lopes Martinez que me ajudou muito em oração e com palavras de fé e apoio que me fizeram acreditar em mim, e aos meus amigos Max e Dayana que nesses últimos dias, foram usados por Deus com palavras que me deram muita força e confiança.

Aos diretores Silmara e Kássio e às coordenadoras Rita e Adriana, que foram anjos que Deus colocou em minha vida, que me encontraram, acreditaram em mim e me fizeram crescer como professor e que em toda essa correria sempre me deram apoio para terminar o meu mestrado, entendendo minhas faltas em reuniões importantes e nas aulas nas quais tive que enviar substitutos.

E um muito obrigado super especial a minha professora orientadora Dra. Elisabete Sousa Freitas que não desistiu de mim, mesmo quando eu pensei em desistir, que ficou até de madrugada trocando mensagens e me ajudando a corrigir meu trabalho e que conseguiu fazer um rapaz às vezes desanimado com os estudos crescer muito em dedicação e conhecimento, que me fez gostar ainda mais do que faço.

Um muito obrigado a todos.

Resumo

Neste trabalho estudaremos Fatoração de Números Inteiros. Nos dois primeiros capítulos apresentaremos conceitos e resultados básicos da teoria dos Números necessários para o entendimento dos capítulos seguintes. Nos capítulos 3 e 4 serão estudados testes de primalidade e métodos de fatoração, começando pelo crivo de Eratóstenes e o Algoritmo Usual de Fatoração (uma prova da existência da fatoração enunciada no Teorema Fundamental da Aritmética). No último capítulo falaremos sobre o sistema de criptografia RSA, um importante exemplo de aplicação dos conceitos estudados no trabalho.

Palavras-chave: Números Inteiros. Congruência. Primalidade. Fatoração. Criptografia.

Abstract

In this work we study integer Factorization. In the first two chapters present basic concepts and results of number theory required for the understanding of the following chapters. In chapters 3 and 4 will be studied primality testing and factorization methods, starting with the sieve of Eratosthenes and the Usual factorization Algorithm (a proof of the existence of the factoring set out in the Fundamental Theorem of arithmetic). In the last chapter we will talk about the RSA encryption system, an important example of application of the concepts studied in the work.

Keywords: Integers. Congruence. Primality. Factoring. Encryption.

Sumário

Introdução p. 9

1 Conceitos e resultados básicos p. 10

1 Divisibilidade . . . . . p. 10

2 Divisão Euclidiana . . . . . p. 11

3 Máximo Divisor Comum . . . . . p. 11

4 Mínimo Múltiplo Comum . . . . . p. 12

5 Números primos . . . . . p. 13

6 Teorema Fundamental da Aritmética . . . . . p. 14

7 Algoritmo Euclidiano . . . . . p. 14

2 Inteiros módulo n p. 19

1 Congruência e classes de equivalência . . . . . p. 19

2 Teorema de Euler e Teorema de Fermat . . . . . p. 23

3 Fatoração p. 27

1 Crivo de Eratóstenes . . . . . p. 27

2 Teorema Fundamental da Aritmética . . . . . p. 31

2.1 Algoritmo Usual de Fatoração . . . . . p. 31

3 Algoritmo de Fermat . . . . . p. 33

4 Testes de primalidade e métodos de fatoração p. 38

1 Pseudoprimos . . . . . p. 38
1.1 Pseudoprimos . . . . . p. 38
1.2 Números de Carmichael . . . . . p. 39
2 Teste de Miller . . . . . p. 41
3 Mersenne e Fermat . . . . . p. 44
3.1 Números de Mersenne . . . . . p. 44
3.2 Números de Fermat . . . . . p. 46
4 Teste de Lucas . . . . . p. 48
4.1 Teste de Lucas . . . . . p. 48
4.2 Teste de Pepin . . . . . p. 50
4.3 Outro teste determinístico de primalidade . . . . . p. 51
5 Métodos de Pollard . . . . . p. 53
5.1 Método Rho de Pollard . . . . . p. 53
5.2 Método p-1 . . . . . p. 54

5 Criptografia RSA p. 60
1 Pré-codificação . . . . . p. 60
2 Codificação e decodificação . . . . . p. 61
3 Funcionamento . . . . . p. 63
4 Segurança do RSA . . . . . p. 64

Conclusão p. 68

Referências p. 69

Introdução

A fatoração de números inteiros em primos é um problema simples de compreender e é abordado no 6º ano do ensino fundamental. Mas quando trabalhamos com números muito grandes, determinar se um certo número é primo ou composto e, no caso composto, obter a fatoração completa são problemas complexos. É claro que existem números grandes que podem ser rapidamente fatorados dependendo de suas características, mas em geral, essa tarefa não é fácil. Por exemplo os números 100! e 10^{100} são fáceis de serem fatorados, mas se somarmos 1 a cada um deles, a fatoração se torna difícil.

O objetivo deste trabalho é estudar Fatoração de Números Inteiros. Através da apresentação de alguns testes de primalidade e métodos de fatoração, e também do sistema de criptografia RSA, daremos uma idéia de conceitos e aplicações ligados a esse assunto.

Começando com o Algoritmo Usual da Fatoração e o Crivo de Eratóstenes, que é o mais antigo método para se encontrar primos, estudaremos outros métodos de primalidade e de fatoração de números inteiros.

Existem testes de primalidade chamados testes probabilísticos, os quais não nos permite afirmar, com certeza, que determinado número é primo mas que nos darão como resposta que o número é composto ou provavelmente primo. Os testes de primalidade chamados testes determinísticos, nos darão a resposta exata. Os testes determinísticos de primalidade são, em geral, muito mais lentos e difíceis de aplicar do que os testes probabilísticos.

A eficiência dos algoritmos de fatoração depende do tipo de fator que tem o número que queremos fatorar e não existe um algoritmo de fatoração que funcione bem para todos os números inteiros. Finalizaremos nosso trabalho com a descrição do sistema de criptografia RSA, cuja segurança depende da dificuldade da fatoração de números grandes.

1 Conceitos e resultados básicos

Neste capítulo apresentaremos conceitos e resultados básicos da aritmética dos inteiros necessários para a compreensão dos testes de primalidade e métodos de fatoração que estudaremos neste trabalho. Demonstraremos apenas o Teorema Fundamental da Aritmética, que estabelece a fatoração de números inteiros. No final deste capítulo apresentaremos o Algorimo Euclidiano para o cálculo do máximo divisor comum (mdc) entre dois inteiros e o Algoritmo Euclidiano Estendido.

1 Divisibilidade

Definição 1. ***(Divisibilidade)*** *Sejam a e b inteiros. Dizemos que a divide b, se existir um inteiro c tal que $b = a.c$. Neste caso, dizemos também que a é um divisor de b, ou que b é um múltiplo de a, ou ainda, que b é divisível por a. Quando a divide b, denotamos por $a|b$ e caso contrário por $a \nmid b$.*

Proposição 1. *Sejam $a, b, c, d, b_1, ..., b_n, c_1, ..., c_n$ números inteiros quaisquer. São válidas as seguintes propriedades:*

i) $a|0$ *e* $a|a$

ii) Se $a|b$ *e* $b|c$*, então* $a|c$

iii) Se $a|b$ *e* $c|d$*, então* $a.c|b.d$

iv) Se $a|(b + c)$ *e* $a|b$*, então* $a|c$

v) Se $a|b_1, ..., a|b_n$*, então* $a|(c_1 \cdot b_1 + ... + c_n \cdot b_n)$.

vi) Se $a|b$ *e* $b|a$*, então* $a = \pm b$.

Proposição 2. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b|a^n - b^n$.*

Proposição 3. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b|a^{2n+1} + b^{2n+1}$.*

Proposição 4. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b|a^{2n} - b^{2n}$.*

2 Divisão Euclidiana

Teorema 5. ***(Divisão Euclidiana)*** *Sejam a e b inteiros com $b \neq 0$. Existem dois números inteiros q e r, tais que*

$$a = b \cdot q + r \text{ e } 0 \leq r < |b|$$

onde q e r que satisfazem a relação são únicos, e serão chamados, respectivamente de quociente e resto da divisão de a por b. Observamos que $b|a$ se, e somente se, $r = 0$.

Corolário 6. *Dados dois números inteiros a e b com $b \neq 0$, existe um único inteiro n (o quociente da divisão de a por b) tal que*

$$n \cdot b \leq a < (n+1) \cdot b.$$

Observação. O inteiro q, quociente da divisão euclidiana de a por b, pode ser interpretado como o maior inteiro menor ou igual do que o número racional $\frac{a}{b}$, é denotado por $\left[\frac{a}{b}\right]$ e chamado de parte inteira do número racional $\frac{a}{b}$.

3 Máximo Divisor Comum

Definição 2. *Dizemos que um inteiro c é um divisor comum de dois inteiros a e b, se $c|a$ e $c|b$.*

Definição 3. *Um máximo divisor de dois inteiros a e b, é um inteiro d tal que*

1. *d é um divisor comum de a e b;*
2. *d é divisível por todo divisor comum de a e b.*

Teorema 7. *Sejam a e b inteiros, não ambos nulos. Existe um único natural d, denotado por (a, b), tal que d é um máximo divisor comum (mdc) de a e b.*

Definição 4. *Dizemos que dois inteiros a e b são primos entre si, ou primos relativos, se $(a, b) = 1$.*

Proposição 8. *Sejam a e b números inteiros e $a = b \cdot q + r$, onde q e r são inteiros, então $(a, b) = (b, r)$.*

Proposição 9. *Sejam a e b números inteiros. Temos que,*

1. se $(a, b) = d$, então existem inteiros x e y tais que $d = a \cdot x + b \cdot y$.

2. $(a, b) = 1$ se, e somente se, existem existem inteiros x e y tais que $1 = a \cdot x + b \cdot y$.

Corolário 10. *Sejam a e b inteiros. Se $d = (a, b)$, então $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proposição 11. ***(Lema de Gauss)*** *Sejam a, b e c números inteiros. Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Proposição 12. *Sejam $a, m, n \in \mathbb{Z}$. Teremos que $(a, m.n) = 1$ se, e somente se, $(a, m) = (a, n) = 1$.*

A noção de mdc pode ser generalizada como a seguir.

Definição 5. *Um número natural d será dito mdc de dados inteiros $a_1, ..., a_n$, não todos nulos, se possuir as seguintes propriedades:*

i) d é um divisor comum de $a_1, ..., a_n$;

ii) Se c é um divisor comum de $a_1, ..., a_n$ então $c|d$.

Proposição 13. *Dados inteiros $a_1, \ldots, a_n$, não todos nulos, existe o seu mdc, denotado por $(a_1, \ldots, a_n)$, e*

$$(a_1, \ldots a_n) = (a_1, \ldots, (a_{n-1}, a_n)).$$

Definição 6. *Os inteiros $a_1, ..., a_n$ serão ditos primos entre si, ou coprimos, quando $(a_1, ..., a_n) = 1$.*

4 Mínimo Múltiplo Comum

Definição 7. *Dizemos que um número inteiro c é um múltiplo comum de dois números inteiros a e b, se $a|c$ e $b|c$.*

Definição 8. *Dizemos que um inteiro $m \geq 0$ é um mínimo múltiplo comum (mmc) dos inteiros a e b, se possuir as seguintes propriedades*

i) m é um múltiplo comum de a e b;

ii) Se c é um múltiplo comum de a e b, então $m|c$.

Proposição 14. *Dados dois inteiros a e b, existe seu mínimo múltiplo comum, denotado por* $[a, b]$ *e*

$$[a, b] \cdot (a, b) = |ab|.$$

Corolário 15. *Se a e b são números inteiros primos entre si, então* $mmc(a, b) = |ab|$.

Definição 9. *Diremos que um número natural m é um mmc dos inteiros não nulos* $a_1, ..., a_n$, *se m é um múltiplo comum de* $a_1, ..., a_n$, *e, se para todo múltiplo comum* m' *desses números, tem-se que* $m|m'$.

Proposição 16. *Dados* $a_1, \ldots, a_n$ *números inteiros não nulos, temos que existe o seu mínimo múltiplo comum, denotado por* $[a_1, \ldots a_n]$, *e*

$$[a_1, \ldots a_n] = [a, \ldots [a_{n-1}, a_n]].$$

5 Números primos

Definição 10. *Diz-se que um número positivo* $p > 1$ *é um número primo ou apenas um primo se, e somente se,* 1 *e p são seus únicos divisores positivos. Um inteiro maior que* 1 *e que não é primo diz-se composto.*

Proposição 17. *Sejam p e q dois números primos e a um inteiro qualquer. Temos que:*

i) Se $p|q$, *então* $p = q$.

ii) Se $p \nmid a$, *então* $(p, a) = 1$.

Proposição 18. *Sejam a, b e c números inteiros, tais que a e b são primos entre si. Temos que:*

i) Se $b|a \cdot c$, *então* $b|c$.

ii) Se $a|c$ *e* $b|c$, *então* $a \cdot b|c$.

Proposição 19. ***(Propriedade Fundamental dos Primos)****Se p é um primo tal que* $p|a \cdot b$, *então* $p|a$ *ou* $p|b$ *(podendo ser fator de ambos, a e b).*

Corolário 20. *Se* $p, p_1, ..., p_n$ *são números primos e, se* $p|p_1 \cdots p_n$, *então* $p = p_i$ *para algum* $i = 1, ..., n$.

Teorema 21. ***(Teorema de Euclides)*** *Existem infinitos números primos.*

6 Teorema Fundamental da Aritmética

Do ponto de vista da estrutura multiplicativa dos inteiros, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números inteiros não nulos, como veremos no Teorema da Fatoração Única, também conhecido como Teorema Fundamental da Aritmética, enunciado pela primeira vez por Gauss em seu famoso livro *Disquisitiones arithmeticae*.

Teorema 22. ***(Teorema Fundamental da Aritmética)*** *Todo número inteiro positivo maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Vamos usar a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente verificado. Agora vamos supor que o resultado é válido para todo inteiro positivo menor que n e vamos provar que será válido para n. É claro que se n é primo, nada temos a demonstrar. Então, suponhamos que n seja composto. assim, existem números naturais n_1 e n_2 tais que $n = n_1 \cdot n_2$, onde $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto $n = p_1 \cdots p_r \cdot q_1 \cdots q_s$.

Agora, vamos provar a unicidade dessa escrita. Vamos supor que $n = p_1 \cdots p_r = p'_1 \cdots p'_s$, onde cada um dos termos p_i e p'_j são números primos. Como $p_1 | p'_1 \cdots p'_s$ pelo Corolário 20, temos que $p_1 = p'_j$ para algum j, que reordenando os primos $p'_1, ..., p'_s$, podemos supor que seja p'_1. Portanto,

$$p_2 \cdots p_r = p'_2 \cdots p'_s.$$

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e p'_j são iguais aos pares. Assim, está provada a unicidade da escrita. □

7 Algoritmo Euclidiano

A seguir, vamos descrever dois algoritmos: um (Algoritmo Euclidiano) para calcular o mdc de dois inteiros a e b, não ambos nulos; e o outro (Algoritmo Euclidiano Estendido) para determinar inteiros x e y tais que $(a, b) = a \cdot x + b \cdot y$.

Algoritmo de Euclides: Sejam a e b inteiros tais que $a \geq b$. Se $b = 1$ ou $b = a$, ou ainda $b|a$, temos que (a,b)=a. Então, vamos supor $1 < b < a$ e que $b \nmid a$. Daí, pela

divisão euclidiana, podemos escrever

$$a = b \cdot q_1 + r_1, \quad \text{com} \;\; 0 < r_1 < b.$$

Aqui teremos duas possibilidades:

a) $r_1 | b$. Nesse caso, $r_1 = (b, r_1)$ e, pela Proposição 8, temos que

$$r_1 = (b, r_1) = (b, a) = (a, b),$$

e o algoritmo termina.

b) $r_1 \nmid b$. Nesse caso, podemos efetuar a divisão euclidiana de b por r_1, obtendo

$$b = r_1 \cdot q_2 + r_2, \quad \text{com} \;\; 0 < r_2 < r_1.$$

Novamente, teremos duas possibilidades:

a') $r_2 | r_1$. Em tal situação, $r_2 = (r_1, r_2)$ e outra vez, pela Proposição 8, teremos

$$r_2 = (r_1, r_2) = (r_1, b) = (a, b).$$

b') $r_2 \nmid r_1$. Em tal situação, podemos efetuar a divisão euclidiana de r_1 por r_2, obtendo

$$r_1 = r_2 \cdot q_3 + r_3, \quad \text{com} \;\; 0 < r_3 < r_2.$$

Prosseguimos dessa maneira até que o algoritmo pare. Isso sempre ocorre, pois caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > ...$ sem menor elemento, o que não é possível. Logo, para algum n, temos que $r_n | r_{n-1}$, donde $(a, b) = r_n$.

Portanto, o algoritmo da divisão é sucessivamente aplicado obtendo $r_j = r_{j+1} \cdot q_{j+2} + r_{j+2}$, com $0 \leq r_{j+2} < r_{j+1}$ e quando chegarmos à $r_{n+1} = 0$ teremos $(a, b) = r_n = r_{n-2} - r_{n-1} \cdot q_n$, onde r_n é o último resto não nulo.

Exemplo 1. *Utilizando o Algoritmo de Euclides, vamos mostrar que* $mdc(1001, 780) = 13$. *Fazendo as divisões sucessivas, obtemos*

$$1001 = 1 \cdot 780 + 221$$

$$780 = 3 \cdot 221 + 117$$

$$221 = 1 \cdot 117 + 104$$

$$117 = 1 \cdot 104 + 13$$

$$104 = 8 \cdot 13 + 0$$

Podemos representar essas divisões utilizando o seguinte diagrama

	$q_1 = 1$	$q_2 = 3$	$q_3 = 1$	$q_4 = 1$	$q_5 = 8$
$a = 1001$	$b = 780$	$r_1 = 221$	$r_2 = 117$	$r_3 = 104$	$r_4 = 13$
$r_1 = 221$	$r_2 = 117$	$r_3 = 104$	$r_4 = 13$	$r_5 = 0$	

Portanto, como $r_5 = 0$, $r_4 = 13$ *é o mdc de* 1001 *e* 780.

Algoritmo de Euclides Estendido: Sejam a e b inteiros positivos, com $a > b$. Temos, com as notações do Algoritmo Euclidiano, que $a = b \cdot q_1 + r_1, b = r_1 \cdot q_2 + r_2$ e $r_i = r_{i+1} \cdot q_{i+2} + r_{i+2}$, para $i \geq 1$.

Tomando $r_{-1} = a$ e $r_0 = b$, temos que $r_i = r_{i+1} \cdot q_{i+2} + r_{i+2}$, para $i \geq -1$.

Observando que $r_{-1} = a = 1 \cdot a + 0 \cdot b,\ r_0 = b = 0 \cdot a + 1 \cdot b,\ r_1 = 1 \cdot a + (-q_1) \cdot b$ temos que

$$r_2 = b - r_1 \cdot q_2 = b - (a - b \cdot q_1) \cdot q_2 = (-q_2) \cdot a + (1 + q_1 \cdot q_2) \cdot b.$$

Supondo agora que já calculamos $r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$ e $r_i = s_i \cdot a + t_i \cdot b$, como $r_{i-1} = r_i \cdot q_{i+1} + r_{i+1}$ obtemos

$$r_{i+1} = r_{i-1} - r_i \cdot q_{i+1} = s_{i-1} \cdot a + t_{i-1} \cdot b - q_{i+1}(s_i \cdot a + t_i \cdot b) =$$

$$\underbrace{(s_{i-1} - q_{i+1} \cdot s_i)}_{s_{i+1}} \cdot a + \underbrace{(t_{i-1} - q_{i+1} \cdot t_i)}_{t_{i+1}} \cdot b.$$

Portanto, temos uma recorrência para calcularmos x, y tais que

$$(a, b) = r_n = x \cdot a + y \cdot b.$$

Começamos com $s_{-1} = 1, t_{-1} = 0, s_0 = 0, t_0 = 1$ e a partir daí usamos a recorrência

$$s_{i+1} = s_{i-1} - q_{i+1} \cdot s_i \ \text{ e } \ t_{i+1} = t_{i-1} - q_{i+1} \cdot t_i \ \text{ para } \ i \geq 0$$

para obter $x = s_n$ e $y = t_n$.

Exemplo 2. *Vimos, utilizando o algoritmo de Euclides que* $(1001, 780) = 13$. *Agora, vamos utilizar o Algoritmo de Euclides estendido, e os valores de* q_j *encontrados no Exemplo* 1 *para encontrar* s_4 *e* t_4 *tais que* $1001 \cdot s_4 + 780 \cdot t_4 = 13$.

Procedemos da seguinte maneira

$$s_{-1} = 1, t_{-1} = 0,$$

$$s_0 = 0, t_0 = 1,$$

$$s_1 = s_{-1} - q_1 s_0 = 1 - 1 \cdot 0 = 1,\ t_1 = t_{-1} - q_1 t_0 = 0 - 1 \cdot 1 = -1$$

$$s_2 = s_0 - q_2 s_1 = 0 - 3 \cdot 1 = -3,\ t_2 = t_0 - q_2 t_1 = 1 - 3 \cdot (-1) = 4$$

$$s_3 = s_1 - q_3 s_2 = 1 - 1 \cdot (-3) = 4,\ t_3 = t_1 - q_3 t_2 = -1 - 1 \cdot 4 = -5$$

$$s_4 = s_2 - q_4 s_3 = -3 - 1 \cdot 4 = -7,\ t_4 = t_2 - q_4 t_3 = 4 - 1 \cdot (-5) = 9$$

Portanto $s_4 = -7$ *e* $t_4 = 9$. *De fato, teremos que* $1001 \cdot (-7) + 780 \cdot 9 = -7007 + 7020 = 13$

Podemos organizar as informações contidas acima em uma tabela, da seguinte maneira.

restos	*quocientes*	s	t
r_{-1}=*1001*	*	1	0
$r_0 = 780$	*	0	1
$r_1 = 221$	$q_1 = 1$	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$
$r_2 = 117$	$q_2 = 3$	$0 - 3 \cdot 1 = -3$	$1 - 3 \cdot (-1) = 4$
$r_3 = 104$	$q_3 = 1$	$1 - 1 \cdot (-3) = 4$	$-1 - 1 \cdot 4 = -5$
$r_4 = 13$	$q_4 = 1$	$-3 - 1 \cdot 4 = -7$	$4 - 1 \cdot (-5) = 9$

2 Inteiros módulo n

Neste capítulo, além de estudarmos alguns conceitos e propriedades de congruência, apresentaremos a função phi de Euler e os Teoremas de Euler e Fermat, assuntos que serão de grande importância para o desenvolvimento dos capítulos 4 e 5.

1 Congruência e classes de equivalência

Definição 11. *Seja um número inteiro $n > 1$. Dizemos que dois inteiros a e b são congruentes módulo n se os restos da divisão de a por n e de b por n forem os mesmos, e escrevemos*

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

Decorre, imediatamente, da definição a seguinte proposição.

Proposição 23. *Sejam $a,\ b,\ c,$ de n inteiros com $n > 1$. Temos que:*

i) $a \equiv a\ (mod\ n)$;

ii) Se $a \equiv b\ (mod\ n)$, *então* $b \equiv a\ (mod\ n)$;

iii) Se $a \equiv b\ (mod\ n)$ *e* $b \equiv c\ (mod\ n)$, *então* $a \equiv c\ (mod\ n)$.

Portanto, temos que a relação de congruência módulo n, com $n > 1$, é uma relação de equivalência.

Proposição 24. *Sejam $a, b, n \in \mathbb{Z}$, com $n > 1$. Tem-se que $a \equiv b\ (mod\ n)$ se, e somente se, $n|(a - b)$.*

Demonstração. Sejam $a = nq + r$, com $0 \leq r < n$ e $b = nq' + r'$, com $0 \leq r' < n$, as divisões euclidianas de a e b por n. Teremos que

$$b - a = n(q' - q) + (r' - r), \quad \text{com} \quad |r - r'| < n.$$

Portanto, $n|(a-b)$ se, e somente se, $r'-r=0$, ou seja, $r'=r$, o que, em vista da igualdade acima, é equivalente a dizer que $a \equiv b \ (mod\ n)$. □

Proposição 25. *Sejam $a,\ b,\ c,\ d,\ m$ e n inteiros com $n>1$ e $m \geq 1$. Temos que:*

i) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, então $a+c \equiv b+d \ (mod\ n)$.

ii) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, então $a \cdot c \equiv b \cdot d \ (mod\ n)$.

iii) Se $a \equiv b \ (mod\ n)$, então $a^m \equiv b^m \ (mod\ n)$.

Demonstração.

i) Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, temos, pela proposição 24, que $n|(b-a)$ e $n|(d-c)$. Daí $n|((b-a)+(d-c))$ e, portanto, $n|((b+d)-(a+c))$, o que prova o resultado.

ii) Note que $bd-ac = d(b-a)+a(d-c)$. Pela Proposição 24, temos que $n|(b-a)$ e $n|(d-c)$. Logo $n|(bd-ac)$, e o resultado está provado.

iii) Este item será demonstrado utilizando indução sobre m. Se $m=1$, a congruência é obviamente verificada. Então, vamos supor que o resultado seja válido para m e iremos prová-lo para $m+1$. Assim, devemos mostrar que $a^{m+1} \equiv b^{m+1} \ (mod\ n)$. Note que $a^{m+1} = a^m \cdot a$. Como por hipótese, $a \equiv b \ (mod\ n)$ e $a^m \equiv b^m \ (mod\ n)$, podemos concluir, pelo item anterior, que $a \cdot a^m = a^{m+1} \equiv b \cdot b^m = b^{m+1} \ (mod\ n)$.

□

Proposição 26. *Sejam $a, b, c, n \in \mathbb{Z}$, com $n>1$. Temos que*

$$a+c \equiv b+c \ mod\ n \iff a \equiv b \ mod\ n.$$

Demonstração. A volta segue-se imediatamente pelo item i) da Proposição 25, pois $c \equiv c \ (mod\ n)$.

Reciprocamente, se $a+c \equiv b+c \ (mod\ n)$, então $n|((b+c)-(a+c))$, donde $n|(b-a)$, ou seja, $a \equiv b \ (mod\ n)$. □

Proposição 27. *Sejam $a, b, c, n \in \mathbb{Z}$, com $n>1$. Tem-se que*

$$ac \equiv bc \ mod\ n \iff a \equiv b \ mod\ \frac{n}{(c,n)}.$$

Demonstração. Como $\frac{n}{(c,n)}$ e $\frac{c}{(c,n)}$ são coprimos, temos que

$$ac \equiv bc \iff n|(b-a)c \iff \frac{n}{(c,n)}|(b-a)\frac{c}{(c,n)} \iff \frac{n}{(c,n)}|b-a \iff a \equiv b\,(mod\,\frac{n}{(c,n)}).$$

□

O corolário a seguir é um caso particular da proposição anterior.

Corolário 28. *Sejam $a, b, c, n \in \mathbb{Z}$, com $n > 1$ e $(c, m) = 1$. Segue que*

$$ac \equiv bc\ mod\ n \iff a \equiv b\ mod\ n.$$

Observação. Segue da definição de congruência módulo n que todo número inteiro a é congruente módulo n ao seu resto pela divisão Euclidiana por n e, portanto, é congruente módulo n a um dos números $0, 1, \ldots, n-1$. Além disso, dois desses números distintos não são congruentes módulo n.

Portanto, para encontrar o resto da divisão de um número a por n, basta achar o número natural r dentre os números $0, 1, \ldots, n-1$ que seja congruente a a módulo n.

Definição 12. *Seja dado um número inteiro $n > 1$. Definimos como a classe residual módulo n do elemento a de $\mathbb{Z}$ como sendo a classe de equivalência de a segundo a relação de equivalência dada pela congruência módulo n:*

$$\overline{a} = \{x \in \mathbb{Z}; x \equiv a\ (mod\ n)\}.$$

O conjunto de todas as classes residuais módulo n é representado por $\mathbb{Z}_n$. Esse conjunto possui n elementos que podem ser representados por $\overline{0}, \overline{1}, ..., \overline{n-1}$. As classes residuais transformam a congruência $a \equiv b\ (mod\ n)$ na igualdade $\overline{a} = \overline{b}$.

Algumas vezes, em vez de escrevermos $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$, escrevemos apenas $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$.

Em $\mathbb{Z}_n$ definimos as seguintes operações:

Adição: $\overline{a} + \overline{b} = \overline{a+b}$.

Multiplicação: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Pela proposição 25, estas operações estão bem definidas, isto é, não dependem dos representantes das classes.

As operações que definimos acima gozam das seguintes propridades:

Propriedades da Adição

Para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, temos:

A1) Associatividade $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

A2) Comutatividade $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;

A3) Existência de zero $\overline{a} + \overline{0} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_n$;

A4) Existência de oposto $\overline{a} + \overline{-a} = \overline{0}$.

Propriedades da Multiplicação

Para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, temos:

A1) Associatividade $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$;

A2) Comutatividade $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$;

A3) Existência de unidade $\overline{a} \cdot \overline{1} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_n$;

AM) Distributividade $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

As propriedades acima seguem diretamente das propriedades dos números inteiros.

Definição 13. *Dizemos que um elemento $\overline{a} \in \mathbb{Z}_n$ é invertível, quando existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.*

Observação. Se $\overline{a}$ é invertível em $\mathbb{Z}_n$ existe um único $\overline{b}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$ e é denotado por $\overline{a}^{-1}$. De fato, supondo $\overline{a} \cdot \overline{b} = \overline{1} = \overline{a} \cdot \overline{b_1}.$, segue que $(a, n) = 1$ e $a \cdot b \equiv a \cdot b_1 \ (mod\ n)$, donde $b \equiv b_1 \ (mod\ n)$. Portanto $\overline{b} = \overline{b_1}$

Proposição 29. *Sejam $\overline{a} \in \mathbb{Z}_n$ e $n > 1$. Então existe $\overline{b} \in \mathbb{Z}_n$ com $\overline{a} \cdot \overline{b} = \overline{1}$ se e somente se $(a, n) = 1$.*

Demonstração. Se $\overline{a} \cdot \overline{b} = \overline{1}$ temos $a \cdot b \equiv 1 \ (mod\ n)$, daí $n \cdot k = 1 - a \cdot b$ para algum inteiro k, donde $a \cdot b + n \cdot k = 1$, e portanto $(a, n) = 1$. Se $(a, n) = 1$ temos $a \cdot x + n \cdot y = 1$ para certos inteiros x e y, donde $a \cdot x \equiv 1 \pmod{n}$. Portanto $\overline{a} \cdot \overline{x} = \overline{1}$. □

Definição 14. *Denotaremos por U(n) o conjunto dos elementos inversíveis de $\mathbb{Z}_n$, isto é,*

$$U(n) = \{\overline{a} \in \mathbb{Z}_n : \overline{a} \ \ é\ inversível\ \}$$

Pela Proposição 29, temos que $U(n) = \{\overline{a} \in \mathbb{Z}_n | mdc(a, n) = 1\}$.

2 Teorema de Euler e Teorema de Fermat

Definição 15. ***(Função de Euler)*** *Para $n > 1$, seja $\phi(n)$ o número de inteiros do intervalo $[1, n]$ que são primos relativos com n. A função ϕ que a cada natural n associa $\phi(n)$ é chamada de função ϕ de Euler, onde definimos $\phi(1) = 1$.*

Observação. Podemos concluir que o número de elementos de $U(n)$ é dado por $\phi(n)$, onde $n > 1$.

Definição 16. *Um conjunto com n números inteiros $a_1, a_2, ..., a_n$ é dito um sistema completo de resíduos (s.c.r.) módulo n se $\{\overline{a_1}, \overline{a_2}, ..., \overline{a_n}\} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, isto é, se os $a_i's$ representam todas as classes de congruência módulo n.*

Definição 17. *Um conjunto com $\phi(n)$ números inteiros $\{b_1, b_2, ..., b_{\phi(n)}\}$ é dito um sistema completo de invertíveis (s.c.i.) módulo n se $\{\overline{b_1}, \overline{b_2}, ..., \overline{b_{\phi(n)}}\} = U(n)$, isto é, se os $b_i's$ representam todas as classes invertíveis módulo n.*

Proposição 30. *Sejam $k, b, n \in \mathbb{Z}$, $n > 0$ tal que $(k, n) = 1$. Se $\{a_1, a_2, ..., a_n\}$ é um s.c.r. (módulo n), então $\{ka_1 + b, ka_2 + b, ..., ka_n + b\}$ formam um s.c.r. (módulo n).*

Demonstração. Basta provar que se $ka_i + b \equiv ka_j + b \ (mod\ n)$, então $i = j$, pois nesse caso teremos n classes de congruências distintas módulo n, que devem ser todas as classes de $\mathbb{Z}_n$. Note que, como $ka_i + b \equiv ka_j + b \ (mod\ n)$, teremos que $ka_i \equiv ka_j \ (mod\ n)$. Daí, como $(k, n) = 1$ teremos que $a_i \equiv a_j \ (mod\ n)$ donde $i = j$. □

Proposição 31. *Sejam $n > 1, k \in \mathbb{Z}$ e $\{b_1, b_2, ..., b_{\phi(n)}\}$ um sistema completo de invertíveis (s.c.i.) módulo n. Se $(k, n) = 1$, então $\{kb_1, kb_2, ..., kb_{\phi(n)}\}$ também será um sistema completo de invertíveis (s.c.i).*

Demonstração. Para cada $i = 1, 2, ..., \phi(n)$, como $(b_i, n) = 1$ e $(k, n) = 1$, temos que $(b_ik, n) = 1$, logo b_ik é invertível. Além disso, supondo $b_ik \equiv b_jk \ (mod\ n)$, segue que $b_i \equiv b_j (mod\ n)$ o que implica que $i = j$, e portanto $\{qb_1, qb_2, ..., qb_{\phi(n)}\}$ é um s.c.i. (módulo n). □

Proposição 32. ***(Propriedades da função ϕ de Euler)***

(i) p é primo $\iff \phi(p) = p - 1$.

(ii) A função ϕ de Euler é multiplicativa, isto é, se mdc(m, n) = 1, então $\phi(mn) = \phi(m).\phi(n)$.

Demonstração. (i) Se p é primo qualquer um dos números $1, 2, 3, ..., p-1$ é primo relativo com n, portanto $\phi(n) = p-1$. Reciprocamente, se $\phi(n) = p-1$, o número de elementos do intervalo $[1, p]$ que são primos relativos com p é $p-1$, então $1, 2, 3, ..., p-1$ são primos com p, e portanto p é primo.

(ii) O resultado é trivial se $m = 1$ ou $n = 1$. Portanto, vamos supor que $m > 1$ e $n > 1$. Considere a seguinte tabela formada pelos números naturais de 1 a $m.n$

1	2	...	k	...	n
$n+1$	$n+2$	...	$n+k$	...	2n
...	...		...		...
$(m-1)n+1$	$(m-1)n+2$	...	$(m-1)n+k$	...	m.n

Como temos que $(t, m.n) = 1$ se, e somente se, $(t, m) = (t, n) = 1$, temos que para calcular $\phi(m.n)$, devemos encontrar dentre os inteiros da tabela acima, aqueles que são primos simultaneamente com m e n.

Se o primeiro elemento de uma coluna qualquer não for primo com n, então todos os outros elementos dessa mesma coluna não serão primos com n. Portanto, os elementos primos com n estão necessariamente nas colunas que restaram, que são em quantidade $\phi(n)$, e cujos elementos são primos com n. Agora, vamos ver quais são os elementos primos com m em cada uma dessas colunas. Como $(m, n) = 1$, a sequência

$$k, n+k, ..., (m-1)n+k$$

forma um sistema completo de resíduos módulo m (veja Proposição 30), e portanto, $\phi(m)$ desses elementos são primos com m. Logo, o número de elementos simultaneamente primos com m e n é $\phi(m).\phi(n)$.

□

Proposição 33. *Se p é primo, então* $\phi(p^r) = p^r - p^{r-1}$.

Demonstração. De 1 até p^r, temos um total de p^r números naturais. Para obter $\phi(p^r)$ temos que excluir, desses, os números que não são primos relativos com p^r, ou seja, todos os múltiplos de p, que são exatamente os números $p, 2p, \ldots, p^{r-1}p$, que são num total de p^{r-1} números. Portanto, $\phi(p^r) = p^r - p^{r-1}$. □

Proposição 34. *Seja $n > 1$ e $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ a decomposição de n em fatores primos. Então $\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$.*

Demonstração. Como $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$ são primos entre si, temos que

$$\phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots (p_r^{\alpha_r}).$$

Daí, o resultado segue da proposição anterior. □

Teorema 35. ***(Teorema de Euler)*** *Seja $n \geq 2$ um inteiro. Se $a \in \mathbb{Z}$ e $(a, n) = 1$ então, $a^{\phi(n)} \equiv 1 \ (mod\ n)$.*

Demonstração. Seja $r_1, r_2, ..., r_{\phi(n)}$ um sistema completo de invertíveis(s.c.i.) módulo n , pela Proposição 31, $ar_1, ar_2, ..., ar_{\phi(n)}$ também é, já que $(a, n) = 1$. Daí chegamos em

$$ar_1 ar_2 \cdots ar_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \ (mod\ n)$$

ou seja

$$a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \ (mod\ n).$$

Logo, temos, pelo Corolário 28, que

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

□

Os dois corolários a seguir serão, assim como o Teorema anterior, de grande importância para o estudo de alguns testes de primalidade e métodos de fatoração que serão estudados nos capítulos posteriores.

Corolário 36. ***(Pequeno Teorema de Fermat)*** *Se p é um número primo e a é um inteiro não é divisível por p, então $a^{p-1} \equiv 1 \ (mod\ p)$.*

Demonstração. Basta notar que, sendo p primo, teremos que $(a, p) = 1$ e $\phi(p) = p - 1$, e daí a congruência é valida pelo Teorema de Euler. □

Corolário 37. ***(Teorema de Fermat)*** *Seja p um número primo e a um número inteiro, então $a^p \equiv a \ (mod\ p)$.*

Demonstração. Se $(a, p) = 1$, o resultado segue do corolário acima multiplicando ambos os membros da congruência $a^{p-1} \equiv 1 \ (mod\ p)$ por a.

No caso em que $(a, p) \neq 1$, segue-se, como p é primo, que $p|a$, e daí, $p|(a^p - a)$, donde $a^p \equiv a \ (mod\ p)$.

□

Proposição 38. *Sejam $a, n \in \mathbb{Z}$, com $n \geq 2$. Existe um inteiro positivo k tal que $a^k \equiv 1 \ (mod\ n)$ se, e somente se $(a, n) = 1$.*

Demonstração. Se $mdc(a, n) = 1$, temos, pelo Teorema de Euler, que $a^{\phi(n)} \equiv 1 \ (mod\ n)$, mostrando a existência do expoente desejado. Reciprocamente, suponhamos $a^k \equiv 1 \ (mod\ n)$ para algum inteiro positivo k. Se $k = 1$, temos $a \equiv 1 \ (mod\ n)$, logo existe x tal que $a - xn = 1$, o que implica que $mdc(a, n) = 1$. Se $k > 1$, temos que $a^k = aa^{k-1} \equiv 1 \ (mod\ n) \iff aa^{k-1} - 1 = qn$ (com q inteiro) $\iff aa^{k-1} - qn = 1$, o que nos dá, pelo item 2 da Proposição 9, que $mdc(a, n) = 1$. □

A partir da proposição acima, podemos definir a ordem do elemento a com respeito a n.

Definição 18. *Sejam $a, n \in \mathbb{Z}$,com $n > 1$ e $mdc(a, n) = 1$. A ordem de a, denotada por $o_n(a)$, é o menor inteiro positivo t tal que $a^t \equiv 1 \ (mod\ n)$.*

Proposição 39. *Sejam $a, n, s \in \mathbb{Z}$,com $n > 1$, $s \geq 1$ e $mdc(a, n) = 1$. Temos que $a^s \equiv 1 \ (mod\ n)$ se, e somente se, $o_n(a)|s$. Em particular $o_n(a)|\phi(n)$.*

Demonstração. Seja $t = o_n(a)$

Suponhamos que $t|s$. Logo $s = q \cdot t$, donde,

$$a^s = a^{q \cdot t} = (a^t)^q \equiv 1^q = 1 \ (mod\ n).$$

Reciprocamente, suponhamos $a^s \equiv 1 \ (mod\ n)$. Queremos provar que t|s. Pela divisão euclidiana podemos escrever que $s = tq + r$, onde $0 \leq r < t$. Suponhamos por absurdo que $r \neq 0$. Então,

$$1 \equiv a^s \equiv a^{tq+r} \equiv (a^t)^q a^r \equiv a^r,$$

o que é um absurdo, pois $0 < r < t$ e $o_n(a) = t$. Portanto devemos ter $r = 0$, o que significa que $t|s$. □

3 Fatoração

Neste capítulo, começaremos com o Crivo de Eratóstenes, que é o mais antigo método para se encontrar números primos e logo depois vamos para o Teorema Fundamental da Aritmética, fazendo uma prova algorítmica da existência da fatoração e assim já teremos um método para encontrar os fatores primos de um número natural n. Esse método é conhecido como Algoritmo Usual de Fatoração. A partir daí, estudaremos o algoritmo de Fermat.

1 Crivo de Eratóstenes

Proposição 40. *O menor divisor, maior do que* 1*, de qualquer número inteiro* $n \neq 0$ *é necessariamente primo.*

Demonstração. Seja p o menor inteiro, maior do que 1, tal que $p|n$. Suponhamos $d > 1$ tal que $d|p$. Daí, temos que $d \leq p$ e $d|n$, logo $d = p$. Portanto p é primo. □

Proposição 41. *Seja n um número natural. Se n é composto, então seu menor fator, maior do que* 1*, é necessariamente menor ou igual a* $\sqrt{n}$.

Demonstração. Seja $f > 1$ o menor fator de n. Segue que existe um natural a tal que $n = f \cdot a$. Como f é o menor fator de n, temos que $f \leq a$. Multiplicando esta desigualdade por f, temos $f^2 \leq f \cdot a$, $f^2 \leq n$. Portanto $f \leq \sqrt{n}$. □

O *crivo de Eratóstenes* é o mais antigo dos métodos para achar primos. Esse método não envolve nenhuma fórmula explícita, mas funciona como uma peneira de números primos. Nicômaco em sua *Aritmética*, publicada por volta de 100 d.C., introduz o crivo de Eratóstenes da seguinte forma:

> "O método para obtê-los[os números primos] é chamado por Eratóstenes uma peneira, porque tomamos os números ímpares misturados de maneira in-

> discriminada e, por esse método, como se fosse pelo uso de um instrumento ou peneira, separamos os primos ou indecomponíveis dos secundários ou compostos".

O que significa que o crivo funciona como uma peneira que só deixa os números primos. Vejamos como proceder para encontrar primos utilizando esse método.

Primeiramente escolhemos um inteiro positivo n. Listamos todos os números ímpares de 3 a n, já que o único primo par é o número 2. Agora vamos aplicar o crivo na lista de números obtida. O primeiro número da nossa lista é 3, que é primo; riscamos, contando de 3 em 3, todos múltiplos de 3 que fazem parte da lista, pois esses não serão primos. Em seguida procuramos o primeiro elemento da lista, maior que 3, que não foi riscado; que nesse caso é 5. Procedemos da mesma maneira que fizemos para o número 3, riscando, contando de 5 em 5, todos os múltiplos de 5, pois os mesmos são compostos. E prosseguimos assim, até chegar a n.

Por exemplo, se $n = 39$, a lista de números será

$$3 \;\; 5 \;\; 7 \;\; 9 \;\; 11 \;\; 13 \;\; 15 \;\; 17 \;\; 19 \;\; 21 \;\; 23 \;\; 25 \;\; 27 \;\; 29 \;\; 31 \;\; 33 \;\; 35 \;\; 37 \;\; 39.$$

Após a primeira passagem do crivo (de 3 em 3), ficamos com

$$3 \;\; 5 \;\; 7 \;\; \not{9} \;\; 11 \;\; 13 \;\; \not{15} \;\; 17 \;\; 19 \;\; \not{21} \;\; 23 \;\; 25 \;\; \not{27} \;\; 29 \;\; 31 \;\; \not{33} \;\; 35 \;\; 37 \;\; \not{39}.$$

Após a segunda passagem (de 5 em 5), teremos

$$3 \;\; 5 \;\; 7 \;\; \not{9} \;\; 11 \;\; 13 \;\; \not{15} \;\; 17 \;\; 19 \;\; \not{21} \;\; 23 \;\; \not{25} \;\; \not{27} \;\; 29 \;\; 31 \;\; \not{33} \;\; \not{35} \;\; 37 \;\; \not{39}.$$

Após a terceira passagem do crivo (de 7 em 7), a lista continuará a mesma. E novamente, na quarta passagem, que seria de 11 em 11, nada mudaria na lista. Isso, na verdade, vai ocorrer para todas as seguintes passagens do crivo, o que significa que, além do 2 que não incluímos na lista, os números primos menores que 39 são

$$3 \;\; 5 \;\; 7 \;\; 11 \;\; 13 \;\; 17 \;\; 19 \;\; 23 \;\; 29 \;\; 31 \;\; 37.$$

Através do exemplo anterior podemos observar algumas características importantes do crivo de Erastótenes. Primeiramente a questão de que alguns números são riscados da lista em mais de uma passagem, como foi o caso do 15. Além disso, podemos observar que para o exemplo acima, na segunda passagem, já haviamos riscado todos os números compostos da lista e as passagens posteriores seriam redundantes, isto é, o crivo poderia parar ainda na segunda passagem.

A segunda observação nos indica que possivelmente podemos parar de riscar os números muito antes de se chegar a n. De fato, se m é um inteiro da lista, temos que $m \leq n$. Se m for composto, ele terá um fator menor ou igual a $\sqrt{m}$. No entanto, $\sqrt{m} \leq \sqrt{n}$. Portanto, qualquer número composto da lista terá um fator menor ou igual a $\sqrt{n}$. Assim podemos parar de riscar números de r em r quando $r > \sqrt{n}$. No exemplo anterior $[\sqrt{39}] = 6$; por esse motivo foi suficiente riscar de 3 em 3 e de 5 em 5 para obter todos os primos da lista.

Sobre a primeira observação, não conseguimos evitar completamente que alguns números sejam riscados várias vezes, mas podemos melhorar um pouco o crivo. Vamos dizer que queremos encontrar primos até n, e que vamos riscar os números de p em p para um certo primo p. Claramente, todos os múltiplos de p que também são múltiplos de primos menores que p já foram riscados da lista. Portanto, nessa etapa, podemos começar a riscar de p em p a partir do menor múltiplo de p que não seja múltiplo de um primo menor que p, ou seja, a partir de p^2. De fato, se $s < p$, tomando o número $s.p$, múltiplo de p, temos que $s.p$ também é múltiplo de s. Como supomos que $s < p$, esse número já terá sido riscado com os múltiplos de s. Então, o menor múltiplo de p que não será múltiplo de outro primo menor que p é p^2. Logo, para evitar algumas duplicações e assim tornar o crivo um pouco mais econômico, podemos riscar de p em p a começar de p^2.

Digamos que escolhemos um inteiro positivo n e que queremos determinar todos os primos menores ou iguais a n. Para isso vamos criar uma lista com todos os números ímpares de 3 a n, o que nos dará uma lista com $(n-1)/2$ números. A posição j, é a posição do j-ésimo número ímpar positivo, que é $2j+1$. Por exemplo, o primeiro número é $3 = 2.1+1$, na posição 2 está o número $2.2+1 = 5$ e assim por diante. Obtemos assim, o seguinte algoritmo:

Crivo de Erastótenes

Entrada: inteiro positivo ímpar n.

Saída: lista de primos ímpares $\leq n$.

Etapa 1: Comece criando uma lista com $(n-1)/2$ posições, cada uma das quais deve ter um número de 3 a n; e tome $p = 3$.

Etapa 2: Se $p^2 > n$ escreva todos os números menores que n que não foram riscados e pare; senão vá para a Etapa 3.

Etapa 3: Se o número que está na posição $(p-1)/2$ foi riscado, incremente p de 2 unidades e volte à Etapa 2; senão vá para a Etapa 4.

Etapa 4: Atribua o valor de p^2 a uma nova variável T: Risque o número da posição $(T-1)/2$ da lista e incremente T de $2p$, até que $T > n$; quando isto acontecer incremente p de 2 unidades e volte à Etapa 2.

Observe que na última Etapa incrementamos T de $2p$, e não de p, como esperávamos. Mas, lembremos que só estamos listando os números ímpares. Se T e p são ímpares, então $T + p$ é par. Portanto, quando estamos riscando de p em p,o próximo ímpar a ser riscado depois de T, é $T + 2p$.

Para entender melhor o funcionamento do crivo, vamos fazer outro exemplo.

Se $n = 55$, a lista de números será

3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 53 55.

Na primeira passagem do crivo, tomamos o número $p = 3$. Vamos direto para a Etapa 4. Então riscamos o número 9 e vamos aumentando de 6 em 6 até que obtenhamos um número maior que 55, que nesse caso será $51 + 6 = 57$ e obtemos a seguinte lista

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 25 ~~27~~ 29 31 ~~33~~ 35 37 ~~39~~ 41 43 ~~45~~ 47 49 ~~51~~ 53 55.

Agora voltamos para a Etapa 2, com $p = 5$. Novamente vamos direto para a Etapa 4. Então vamos para o número 25 e aumentaremos de 10 em 10 até chegar num número maior que 55. Então riscaremos 35, 45 e 55 e chegaremos na seguinte lista

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 ~~25~~ ~~27~~ 29 31 ~~33~~ ~~35~~ 37 ~~39~~ 41 43 ~~45~~ 47 49 ~~51~~ 53 ~~55~~.

Agora, voltamos para a Etapa 2, com $p = 7$. Mais uma vez vamos direto para a Etapa 4. Vamos para o número 49, que será o único a ser riscado nessa passagem. Daí chegaremos à lista

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 ~~25~~ ~~27~~ 29 31 ~~33~~ ~~35~~ 37 ~~39~~ 41 43 ~~45~~ 47 ~~49~~ ~~51~~ 53 ~~55~~.

Nessa passagem, voltaremos para a Etapa 2, com $p = 11$, pois 9 já está riscado, mas $11^2 > 55$, então não temos mais números a riscar e agora é só copiar os números que não foram riscados que serão os primos ímpares menores que n. Nesse caso esses números são

3 5 7 11 13 17 19 23 29 31 37 41 43 47 53.

2 Teorema Fundamental da Aritmética

Teorema 42. ***(Teorema Fundamental da Aritmética)*** *Dado um inteiro $n \geq 2$ podemos sempre escrevê-lo de modo único, na forma*

$$n = {p_1}^{e_1} \cdots {p_k}^{e_k},$$

onde $1 < p_1 < p_2 < p_3 < \ldots < p_k$ são números primos e $e_1, \ldots, e_k$ são inteiros positivos.

2.1 Algoritmo Usual de Fatoração

Dado um número inteiro $n \geq 2$, vamos procurar os divisores de n, maiores do que 1. Se $d > 1$ e $d|n$ então $d \leq n$. Se n for composto, o menor fator de n é primo e além disso é menor do que ou igual a $[\sqrt{n}]$.

Assim, começamos dividindo n por cada número de 2 a $[\sqrt{n}]$. Se nenhum deles for fator de n, então n é primo.

Caso contrário, tomamos o menor fator de n, encontrado de 2 a $[\sqrt{n}]$. Indicando este menor fator por q_1, temos que q_1 é primo e $n = q_1 \cdot n_1$.

Agora repetimos o procedimento para o número n_1, determinando assim um segundo fator primo de n que chamaremos de q_2, assim $n = q_1 \cdot n_1 = q_1 \cdot q_2 \cdot n_2$, onde $q_1 \leq q_2$, podendo ocorrer o caso $q_1 = q_2$, e $n_1 > n_2$.

Continuando o processo, teremos uma sequência de números primos

$$q_1 \leq q_2 \leq \ldots \leq q_i \leq \ldots$$

cada um fator de n. A esta sequência corresponde uma outra, formada pelos cofatores

$$n > n_1 > n_2 > \ldots > 0$$

Esta última sequência é estritamente decrescente de números inteiros positivos. Como há apenas $n - 1$ inteiros positivos entre n e 0, o processo vai parar depois de no máximo n passos e daí obtemos

$$n = q_1 \cdot q_2 \cdots q_s$$

O algoritmo na primeira etapa do procedimento acima pode ser descrito do seguinte modo:

Algoritmo de fatoração

Entrada: inteiro positivo n

Saída: Inteiro positivo f que é o menor fator primo de n ou uma mensagem indicando que n é primo.

Etapa 1: Comece fazendo $f = 2$.

Etapa 2: Se n/f é inteiro escreva f é fator de n e pare; senão vá para a Etapa 3.

Etapa 3: Agora vá para o próximo primo depois de f e vá para a etapa 4.

Etapa 4: Se F $> \sqrt{n}$ escreva n é primo e pare; senão volte à Etapa 2.

Dessa maneira, dado um inteiro n conseguimos determinar através do algoritmo se n é primo ou composto, e no segundo caso, achar um fator de n. Se n for primo, já temos sua fatoração. Agora, caso n seja composto, devemos encontrar todos os seus fatores primos com suas multiplicidades. Para tal objetivo, aplicamos o algoritmo acima sucessivamente até obter um número que não pode mais ser decomposto, ou seja, primo.

Exemplo 3. *Vamos fatorar o número* 429*, utilizando o algoritmo usual da fatoração. Primeiramente, vamos tomar* $f = 2$*. Mas* $429 = 214 \cdot 2 + 1$*, isto é,* $2 \nmid 429$*. Então, vamos tomar* f *como sendo o próximo primo depois de* 2*, que é o número* 3*. Teremos que* $429 = 3 \cdot 143$*, então* 3 *é o menor fator de* 429*. Mas, ainda não sabemos se fatoramos completamente o número* 429*, pois apenas encontramos seu menor fator. Agora, vamos aplicar novamente o algoritmo no número* 143*. Prosseguindo, vemos que* 143 *não é divisível* 5 *e nem por* 7*, mas* $11|143 = 11 \cdot 13$*. Assim, os fatores de* 143 *são* 11 *e* 13 *e portanto* $429 = 3 \cdot 11 \cdot 13$

Exemplo 4. *Vamos considerar o número* 173 *e tentar fatorá-lo usando o Algoritmo Usual da fatoração. Fazendo as divisões, veremos que* 173 *não é divisível por* $2, 3, 5, 7, 11$ *e nem por* 13*, e como* 17 *que é o próximo primo é maior que* $\sqrt{173}$*, concluímos que* 173 *é primo.*

Esse algoritmo é simples, mas não é eficiente se estivermos trabalhando com números muito grandes. Por exemplo, seja n um número primo com 100 ou mais algarismos. Logo, $n \geq 10^{100}$ e portanto $\sqrt{n} \geq 10^{50}$. Logo serão necessários 10^{50} laços para determinar que n é primo. Se o computador executa 10^{10} divisões por segundo, levaremos $\dfrac{10^{50}}{10^{10}} = 10^{40}$ segundos, ou seja 10^{31} anos, sendo que o tempo estimado de existência do universo é de $2 \cdot 10^{11}$ anos. Portanto, se um número ímpar é muito grande pode ser impossível determinar se ele é primo ou não utilizando esse algoritmo.

Por outro lado, se vamos fatorar um inteiro, há sempre a possibilidade que tenha um fator primo pequeno e o algoritmo acima encontrará tal fator rapidamente.

Existem outros métodos de fatoração, alguns dos quais estudaremos neste trabalho. A eficiência destes algoritmos depende do tipo de fator que tem o número a ser fatorado. Não existe um algoritmo de fatoração que funcione bem para todo número inteiro.

Apresentaremos agora o método de Fermat, que acha rapidamente fatores próximos à raiz quadrada do número a se fatorado.

3 Algoritmo de Fermat

Proposição 43. *Se $n > 1$ é um inteiro número ímpar e não é um quadrado, então existem naturais x e y com $[\sqrt{n}] \leq x < \dfrac{n+1}{2}$ tais que $n = x^2 - y^2$.*

Demonstração. Suponha n um primo composto ímpar e não quadrado, isto é, $n = a \cdot b$ com $1 < a < b < n$, com a e b ímpares. Para se ter $n = x^2 - y^2 = (x-y)\cdot(x+y)$ tomamos $a = x - y$ e $b = x + y$.

Daí, obtemos números naturais $x = \dfrac{a+b}{2}$ e $y = \dfrac{b-a}{2}$.

De fato, expandindo os produtos notáveis

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

Como

$$x < \frac{n+1}{2} \iff a+b < n+1 \iff a+b < a\cdot b+1 \iff a-1 < a\cdot b-b \iff a-1 < b\cdot(a-1)$$

$$x < \frac{n+1}{2} \iff a-1 < b\cdot(a-1) \iff 1 < b$$

temos que $x < \dfrac{n+1}{2}$.

Além disso, temos que

$$[\sqrt{n}] \leq \sqrt{n} = \sqrt{x^2 - y^2} \leq \sqrt{x^2} = x.$$

□

Proposição 44. *Se $n > 1$ é um primo ímpar e $n = x^2 - y^2$, com $x, y \in \mathbb{N}$, então $x = \dfrac{n+1}{2}$ e $y = \dfrac{n-1}{2}$.*

Demonstração. Suponha n um primo ímpar e $n = x^2 - y^2 = (x-y)\cdot(x+y)$, com $x, y \in \mathbb{N}$. Como n é primo, segue que $x - y = 1$ e $x + y = n$, donde obtemos $x = \dfrac{1+n}{2}$ e $y = \dfrac{n-1}{2}$.

□

As proposições acima nos fornecem um algoritmo, que é muito eficiente quando n tem um fator primo que não é muito menor que $\sqrt{n}$.

Para começar vamos supor que n é ímpar, já que se n for par, 2 será um de seus fatores. A idéia do algoritmo de Fermat é tentar achar números inteiros positivos x e y tais que $n = x^2 - y^2$. Se encontrarmos esses números, teremos que

$$n = x^2 - y^2 = (x + y).(x - y).$$

Precisamos considerar separadamente o que acontece na situação em que n é composto e na situação em que n é primo.

Se n é primo, a única possibilidade é $x = \dfrac{(n+1)}{2}$ e $y = \dfrac{(n-1)}{2}$.

Se n é um quadrado perfeito teremos $n = x^2 - 0^2$ e assim $x = \sqrt{n}$ e $y = 0$.

Portanto, vamos supor que n seja um número ímpar composto que não seja um quadrado perfeito. Nesse caso, existem naturais x e y com $[\sqrt{n}] \leq x < \dfrac{n+1}{2}$ tais que $n = x^2 - y^2$ e só precisamos encontrá-los.

Como $y = \sqrt{x^2 - n}$, começamos fazendo $x = [\sqrt{n}]$, vamos incrementando 1 à variável x e calculando o respectivo valor y.

Este procedimento para, antes de $x = \dfrac{n+1}{2}$, quando obteremos y natural.

Observe, no exemplo a seguir, como utilizar essa estratégia para encontrar fatores de um número inteiro n.

Exemplo 5. *Seja* $n = 5959$. *Iniciamos nossa tentativa com a raiz quadrada de* 5959, *mas como a raiz quadrada não é exata, começaremos com* $x = [\sqrt{n}] = 77$. *Mas* $x^2 = 77^2 = 5929 < 5959$. *Então agora vamos passar a incrementar* x *de uma unidade até que* $\sqrt{x^2 - n}$ *seja inteiro, ou* x *seja igual a* $\dfrac{(n+1)}{2}$ *que nesse caso é igual a* 2980. *Vamos resumir o processo em uma tabela:*

x	$\sqrt{x^2 - n}$
78	$11,18$
79	$16,79$
80	21

Observe que quando $x = 80$, *obtemos um valor inteiro para* $\sqrt{x^2 - n}$ *que nesse caso é* 21. *Portanto* $x = 80$ *e* $y = 21$ *são os valores que queremos e os fatores correspondentes de* n *são* $x + y = 101$ *e* $x - y = 59$.

Exemplo 6. *Seja* $n = 1197397$ *o número que queremos fatorar. Iniciamos com* $x = [\sqrt{n}] = 1094$. *Mas* $x^2 = 1094^2 = 1196836 < 1197397$. *Então agora vamos passar a incrementar* x *de uma unidade até que* $\sqrt{x^2 - n}$ *seja inteiro, ou* x *seja igual a* $\dfrac{(n+1)}{2}$ *que nesse caso é igual a* 598699. *Vamos resumir o processo em uma tabela:*

x	$\sqrt{x^2 - n}$
1095	$40,34$
1096	$61,79$
1097	$77,53$
1098	$90,59$
1099	102

Observe que obtemos um inteiro no quinto laço. Portanto $x = 1099$ *e* $y = 102$ *são os valores que queremos e os fatores correspondentes de* n *são* $x + y = 1201$ *e* $x - y = 997$.

Exemplo 7. *Como vimos, quando o número for primo, o algoritmo só pára quando* $x = \frac{n+1}{2}$. *Vamos verificar o que acontece para* $n = 41$. *Iniciamos com* $x = [\sqrt{n}] = 6$. *Mas* $x^2 = 6^2 = 36 < 41$. *Então agora vamos passar a incrementar* x *de uma unidade até que* $\sqrt{x^2 - n}$ *seja inteiro, ou* x *seja igual a* $\frac{(n+1)}{2}$ *que nesse caso é igual a* 21. *Construindo uma tabela como a do exemplo anterior, observe o que ocorre:*

x	$\sqrt{x^2 - n}$
7	$2,82$
8	$4,79$
9	$6,32$
10	$7,68$
11	$8,94$
12	$10,14$
13	$11,31$
14	$12,44$
15	$13,56$
16	$14,66$
17	$15,74$
18	$16,82$
19	$17,88$
20	$18,94$
21	20

Conseguimos, facilmente, descobrir que 41 *é primo usando o algoritmo usual de fatoração, mas aqui mostramos que quando* n *é primo o algoritmo não para até que* x *seja igual a* $\frac{(n+1)}{2}$ *que nesse caso é* 21. *O que nos dá que* 41 *é primo e que seus fatores são* $x + y = 41$ *e* $x - y = 1$.

O algoritmo de Fermat pode ser descrito do seguinte modo:

Algoritmo de Fermat

Entrada: inteiro positivo n.

Saída: um fator de n ou uma mensagem indicando que n é primo.

Etapa 1: Comece com $x = [\sqrt{n}]$; se $n = x^2$ então x é fator de n e podemos parar.

Etapa 2: Caso contrário incremente x de uma unidade e calcule $y = \sqrt{x^2 - n}$.

Etapa 3: Repita a Etapa 2 até encontrar um valor inteiro para y, ou até que x seja igual a (n+1)/2; no primeiro caso n tem fatores $x + y$ e $x - y$, no segundo n é primo.

4 Testes de primalidade e métodos de fatoração

1 Pseudoprimos

1.1 Pseudoprimos

O Pequeno Teorema de Fermat nos fornece um teste de não primalidade, isto é, que nos permite determinar se um número é composto, sem precisar descobrir seus fatores. O teste pode ser escrito da seguinte forma:

Teste: *Se $n > 0$ e $1 < b < n - 1$ são números inteiros e $b^{n-1} \not\equiv 1 \ (mod\ n)$, então n é um número composto. O número b é conhecido como uma testemunha de que n é composto.*

Exemplo 8. *Consideremos $n = 2049$. Queremos saber se é um número primo. Vamos calcular 2^{2048} módulo 2049. Com cálculos simples, utilizando as propriedades de congruência obtemos que $2^{11} = 2048 \equiv -1 \ (mod\ 2049)$. Como $2048 = 11 \cdot 186 + 2$, segue que $2^{2048} = (2^{11})^{186} \cdot 2^2 \equiv 4 \ (mod\ 2049)$. Assim*

$$2^{2048} \equiv 4 \neq 1 \ (mod\ 2049).$$

Portanto 2049 é composto.

A recíproca do pequeno teorema de Fermat não é verdadeira. De fato, temos, por exemplo, que $2^{340} \equiv 1 \ (mod\ 341)$ e $341(31 \cdot 11)$ é composto. Muitos matemáticos usaram a recíproca como verdadeira, tanto que Leibniz, famoso pela invenção do cálculo, usou isto como um critério de primalidade. Estes 'falsos primos' são conhecidos como *pseudoprimos*.

Definição 19. *Um número positivo n, ímpar e composto, é um pseudoprimo para a base b, com $1 < b < n - 1$, quando $b^{n-1} \equiv 1 \ (mod\ n)$.*

Exemplo 9. *O número* 341 *é um pseudoprimo para a base* 2.

Observação. Como vimos, o teste utilizado por Leibniz às vezes pode dar errado, mas esse teste não deixa de ser eficiente. Para números pequenos, ele mais acerta do que erra. Por exemplo, entre 1 e 10^9 temos 50847534 primos e apenas 5597 pseudoprimos para a base 2. Logo se tomarmos um número inteiro ímpar menor que um milhão e este passar no teste de Leibniz, tem-se uma grande probabilidade desse número ser primo.

Podemos melhorar o teste usado por Leibniz utilizando outras bases diferentes de 2. Por exemplo, $3^{340} \equiv 56\ (mod\ 341)$. Logo 3 é testemunha de que 341 é composto. Para as bases 2 e 3, existem apenas 1272 pseudoprimos entre 1 e 10^9.

Podemos observar que se o número inteiro ímpar n é muito grande, testar todas as bases no intervalo de 1 a $n-1$ se torna inviável no ponto de vista prático. No entanto esse problema nos levará a algumas questões de interesse prático.

1.2 Números de Carmichael

Proposição 45. *Seja n um número inteiro composto e $b > 1$ um número inteiro. Se $b|n$, então n não será pseudoprimo para a base b.*

Demonstração. Como $mdc(b, n) = b \neq 1$, teremos (pela Proposição 29) que b não é inversível módulo n, donde $b^{n-1} \not\equiv 1\ (mod\ n)$. □

Pela proposição acima, vemos que não há números que sejam pseudoprimos para todas as bases. Mas, um número composto n pode ser pseudoprimo para todas as bases que são primas a n.

Definição 20. ***(Números de Carmichael)*** *Um número composto $n > 0$ é um número de Carmichael quando $b^n \equiv b\ (mod\ n)$ para todo $1 < b < n-1$. Neste caso, se $(b, n) = 1$, teremos $b^{n-1} \equiv 1\ (mod\ n)$.*

O menor número de Carmichael é 561, mas para chegar à essa conclusão, utilizando a definição, teríamos que verificar que $b^{561} \equiv b\ (mod\ 561)$ para $b = 2, 3, 4, ..., 559$, isto é, um total de 558 bases. Existem infinitos números de Carmichael, e isso significa que esses números podem ser tão grandes que até mesmo um computador terá dificuldade de verificar, utilizando a definição, se o mesmo é um número de Carmichael. Por exemplo, o número 3494075153422874350506032047195872 01 é um número de Carmichael.

Existe uma maneira mais fácil de se verificar se um certo número composto é um número de Carmichael. Esse método é baseado no seguinte teorema:

Teorema 46. ***(Teorema de Korselt)*** *Um inteiro positivo ímpar n é um número de Carmichael se cada fator primo p de n satisfaz as duas condições seguintes:*

(1) p^2 não divide n;

(2) $p-1$ divide $n-1$.

Demonstração. Nosso objetivo é mostrar que se n satisfaz as condições (1) e (2), então $b^n \equiv b \ (mod\ n)$ para todo $1 < b < n-1$, isto é, que n divide $b^n - b$.

Como a condição (1) equivale a dizer que n não tem fatores primos repetidos, pelo item ii) da Proposição 18, basta mostrar que cada fator primo de n divide $b^n - b$. Então, seja p um fator primo de n, vamos mostrar que

$$b^n \equiv b \ (mod\ p).$$

Se b é divisível por p, então b^n e b são congruentes a zero módulo p e a congruência é imediatamente verificada. Então, vamos considerar que p não divide b. Daí, o pequeno Teorema de Fermat nos garante que $b^{p-1} \equiv 1 \ (mod\ p)$. Pela condição (2), $p-1$ divide $n-1$, isto significa que $n-1 = (p-1)q$, para algum inteiro q. Donde segue que

$$n = (n-1)q + 1.$$

Assim

$$b^n \equiv (b^{p-1})^q \cdot b \equiv 1 \cdot b \equiv b \ (mod\ p).$$

Logo $b^n \equiv b \ (mod\ p)$ para qualquer fator primo p de n. Portanto, se $n = p_1 ... p_k$ onde $p_1 < ... < p_k$ são primos distintos, teremos que $b^n \equiv b \ (mod\ p_1 \cdots p_k)$, ou seja,$b^n \equiv b \ (mod\ n)$. □

Pelo teorema acima, vemos que um número inteiro n é um número de Carmichael se ele não tem fatores primos repetidos e se cada um de seus fatores diminuído de uma unidade divide n diminuído de uma unidade.

Exemplo 10. *Consideremos o número* 561*. Esse número pode ser facilmente fatorado*

$$561 = 3 \cdot 11 \cdot 17.$$

Note que os fatores de 561 *são todos distintos e* $3-1=2$, $11-1=10$ *e* $17-1=16$ *dividem* $561-1=560$. *Portanto* 561 *é um número de Carmichael.*

2 Teste de Miller

A existência dos números de Carmichael pode nos fazer tomar várias bases que satisfazem a equação $b^n \equiv b\ (mod\ n)$ e mesmo assim, n não ser primo. Isso pode dificultar muito o nosso trabalho em concluir se o número estudado é primo ou composto utilizando o teste fornecido no início da seção anterior. O teste pode ser melhorado com uma modificação simples. Este novo teste foi introduzido em 1976 por G.L.Miller.

Proposição 47. ***(Teste de Miller)*** *Sejam* $n \neq 2$ *um número primo e* $1 < b < n-1$. *Escrevendo* $n-1 = 2^k \cdot q$ *com* $k \geq 1$ *e* q *ímpar. Então pelo menos uma das potências*

$$b^q,\ b^2q, ...,\ b^{2^{k-1}\cdot q}$$

deve ser congruente a -1 *módulo* n *ou* $b^q \equiv 1\ (mod\ n)$.

Demonstração. Considere a sequência

$$b^q,\ b^2q, ...,\ b^{2^{k-1}\cdot q},\ b^{2^k\cdot q}.$$

Como n é primo temos que

$$b^{n-1} \equiv b^{2^k\cdot q} \equiv 1\ (mod\ n).$$

Considere $j \geq 0$ o menor expoente de 2 tal que $b^{2^j\cdot q} \equiv 1\ (mod\ n)$. Temos dois casos a considerar, $j = 0$ ou $1 \leq j \leq k$.

No caso em que $j = 0$ obtemos $b^q \equiv 1\ (mod\ n)$.

Suponhamos então $1 \leq j \leq k$. Assim $b^{2^j\cdot q} \equiv 1\ (mod\ n)$, ou equivalentemente, $n | b^{2^j\cdot q} - 1 = (b^{2^{j-1}q})^2 - 1 = (b^{2^{j-1}\cdot q}+1).(b^{2^{j-1}\cdot q}-1)$.

Como n é primo e $n \not| b^{2^{j-1}\cdot q} - 1$($j$ é o menor expoente tal que $n | b^{2^j\cdot q} - 1$), concluímos que $n | b^{2^{j-1}\cdot q} + 1$, isto é, $b^{2^{j-1}\cdot q} \equiv -1\ (mod\ n)$ com $0 \leq j-1 \leq k-1$.

Portanto, um dos termos da sequência $b^q,\ b^2q, ...,\ b^{2^{k-1}\cdot q}$ é congruente a -1 módulo n. □

Devemos tomar cuidado, pois a recíproca não é verdadeira, como será mostrado num exemplo dessa seção.

Esta proposição só nos permite concluir que, se nada disso ocorre, então n é composto.

Observe, no exemplo a seguir, como utilizar essa estratégia para verificar se um número inteiro n é composto.

Exemplo 11. *Vimos que, através do teste da seção anterior não conseguimos detectar que* 341 *é composto usando apenas* 2 *como base. Agora vamos aplicar o teste de Miller para* 341*. Primeiramente, verifiquemos que* $341-1=340=2^2\cdot 85$*. Então vamos calcular as potências de* 2 *módulo* 341 *para os expoentes* $2^0\cdot 85=85$ *e* $2^1\cdot 85=170$*. Teremos que*

$$2^{85}\equiv 32\not\equiv 1\ (mod\ 341)$$

e

$$2^{85}\equiv 32\not\equiv -1\ (mod\ 341)$$

$$2^{170}=\left(2^{85}\right)^2\equiv 32^2\equiv 1\not\equiv -1\ (mod\ 341).$$

Portanto 341 *é composto.*

A seguir, apresentaremos o algoritmo do teste de Miller, que tem como grande vantagem sobre o teste do início da seção anterior, o fato de que podemos encontrar números compostos mesmo entre os pseudoprimos.

Teste de Miller

Entrada: um inteiro ímpar n, que se quer testar, e a base b, onde $1<b<n-1$.

Saída: uma das mensagens:'n é composto ou teste inconclusivo'.

Etapa 1: Divida $n-1$ sucessivamente por 2 até encontrar q(um número ímpar) e k tais que $n-1=2^k.q$.

Etapa 2: Comece fazendo $i=0$ e $r=$ resto de b^qpor n.

Etapa 3: Se $i=0$ e $r=1$ ou se $i\geq 0$ e $r=n-1$ a saída é 'teste inconclusivo'.

Etapa 4: Incremente i de 1 unidade e substitua r pelo resto da divisão de r^2 por n.

Etapa 5: Se $i<k$ volte à Etapa 3, senão a saída é 'n é composto'.

Quando a saída do teste for *inconclusivo*, n pode ser primo, ou n pode ser composto. Mas, infelizmente, a segunda hipótese acontece na prática. Vejamos alguns exemplos:

Exemplo 12. *Vamos mostrar outro exemplo interessante, o número de Carmichael* 561*. Através do teste de Miller, chegamos a conclusão que* 561 *é composto, testando apenas para a menor base possível, isto é, para base* 2*. De fato, com cálculos simples podemos verificar que* $561 - 1 = 560 = 2^4 \cdot 35$*. Calculando os restos módulo* 561 *das potências de* 2 *obtemos*

$$2^{35} \equiv 263 \ (mod\ 561)$$

$$2^{2\cdot 35} = (2^{35})^2 \equiv 263^2 \equiv 166 \ (mod\ 561)$$

$$2^{2^2\cdot 35} = 2^{2\cdot(2\cdot 35)} = (2^{2\cdot 35})^2 \equiv 166^2 \equiv 67 \ (mod\ 561)$$

$$2^{2^3\cdot 35} = 2^{2\cdot(2^2\cdot 35)} = (2^{2^2\cdot 35})^2 \equiv 67^2 \equiv 1 \ (mod\ 561)$$

Portanto 561 *tem que ser composto.*

Exemplo 13. *Vamos agora a um exemplo ruim. O mais simples é o número* 25*. Sabemos que* $24 = 2^3 \cdot 3$*. Tomando como base o número* 7*, obtemos os seguintes resultados*

$$7^3 \equiv 18 \ (mod\ 25)$$

$$7^{2\cdot 3} = (7^3)^2 \equiv 18^2 \equiv 24 \equiv -1 \ (mod\ 25)$$

Assim, o teste é inconclusivo para a base 7 *e o expoente* 2.3*, embora* 25 *seja composto. Entretanto se escolhessemos a base* 2*, chegaríamos facilmente que* 25 *é composto.*

Definição 21. *Quando um número composto* n *tem resultado inconclusivo para o teste de Miller com respeito a uma base* b*, dizemos que* n *é um pseudoprimo forte para a base* b*. Isto significa que se pelo menos uma das potências* $b^q,\ b^{2q}, ...,\ b^{2^{k-1}\cdot q}$ *for congruente a* -1 *módulo* n *ou* $b^q \equiv 1 \ (mod\ n)$ *e* n *for composto,* n *é dito pseudoprimo forte para* b*.*

No exemplo anterior, 25 é um pseudoprimo forte para a base 7.

Proposição 48. *Todo pseudoprimo forte para uma certa base é pseudoprimo para aquela base.*

Demonstração. Se n é pseudoprimo forte para uma certa base, utilizando os elementos definidos no início da seção, teremos que $b^q \equiv 1 \ (mod\ n)$ ou alguma das potências $b^{2^i\cdot q}$ com $i = 0, 1, ..., k-1$ ($n - 1 = 2^k \cdot q$, q ímpar), é congruente a -1 $(mod\ n)$. Se ocorrer o primeiro caso teremos que $b^q \equiv 1 \ (mod\ n)$. Elevando ambos os membros por 2^k obtemos $b^{2^k\cdot q} = b^{n-1} \equiv 1 \ (mod\ n)$, donde $b^n \equiv b \ (mod\ n)$ e n é pseudoprimo para a base b. Se o segundo caso ocorre, teremos que $b^{2^i\cdot q} \equiv -1 \ (mod\ n)$ para algum $0 \leq i \leq k-1$. Elevando

ambos os membros por 2^{k-i}, obtemos $b^{2^k \cdot q} = b^{n-1} \equiv 1 \ (mod\ n)$, donde $b^n \equiv b \ (mod\ n)$ e novamente n é pseudoprimo para a base b. □

Observação. Como já foi dito, 25 não é um pseudoprimo forte para a base 2. O menor pseudoprimo forte forte para a base 2 é o número 2047. E mais, existem apenas 1282 pseudoprimos fortes entre 1 e 10^9, o que nos dá uma idéia da eficiência do Teste de Miller, que pode ser testado para várias bases.

3 Mersenne e Fermat

A melhor maneira de se encontrar números primos grandes é através de fórmulas exponenciais. Para isso, vamos utilizar aqui, os números de Fermat e Mersenne para procurar primos entre números da forma $2^n \pm 1$.

3.1 Números de Mersenne

Proposição 49. *Seja n um número natural maior do que 1. Se n é composto, então $2^n - 1$ é composto.*

Demonstração. Se $n = r \cdot s$,com $1 < r, s < n$, temos que

$$2^n - 1 = (2^r)^s - 1 \text{ e, pela proposição 2, } 2^r - 1 | 2^{r \cdot s} - 1 = 2^n - 1.$$

Como $2^r - 1 \neq 1$ e $2^r - 1 \neq 2^n - 1$, concluímos que $2^n - 1$ é composto. □

Definição 22. ***(números de Mersenne)***. *Os números de Mersenne são os números da forma*

$$M(p) = 2^p - 1, \textit{ onde } p \textit{ é um número primo.}$$

Observação. O fato de p ser primo não nos garante que M(p) também seja. Observe que M(11) é composto

$$M(11) = 2047 = 23 \cdot 89.$$

Definição 23. *Os números de Mersenne que são primos são conhecidos como primos de Mersenne.*

No intervalo $2 \geq p \geq 5000$, os primos de Mersenne são os correspondentes aos seguintes valores de p: $2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253$ e 4423. Até hoje, o maior número primo conhecido é o número de Mersenne $M(57885161)$, descoberto em janeiro de 2013, e que possui, no sistema decimal, 17425170 dígitos.

Vamos descrever agora, um método relativamente eficiente para encontrar fatores primos para números de Mersenne não muito grandes. Esse método é devido à Fermat e utiliza uma fórmula geral para os números primos que podem ser fatores de um número de Mersenne.

Proposição 50. ***(Método de Fermat).*** *Seja $p \neq 2$ um primo e q um fator primo de $M(p)$. Então $q = 1 + 2rp$ para algum inteiro positivo r.*

Demonstração. Suponhamos que $p \neq 2$ é um número primo e que q é um fator primo de $M(p) = 2^p - 1$. Então

$$2^p \equiv 1 \ (mod \ q).$$

O que significa que em $U(q) = \mathbb{Z}_q \backslash \{\overline{0}\}$ temos a seguinte identidade

$$\overline{2}^p = \overline{1}.$$

Pela Proposição 39, temos que $o_q(\overline{2})$ deve dividir p. Como p é primo e $o_q(\overline{2}) \neq 1$, concluímos que $o_q(\overline{2}) = p$. Por outro lado, como q é ímpar, temos também, pelo teorema de Fermat

$$\overline{2}^{q-1} = \overline{1} \ em \ U(q).$$

Outra vez pela Proposição 39, a ordem de 2, que nesse caso é p, divide $q - 1$. Isto significa que existe um inteiro k tal que $q - 1 = kp$.

Podemos observar ainda, que $M(p) = 2^p - 1$ é um número ímpar e consequentemente todo fator de $M(p)$ é ímpar, inclusive q. Donde $q - 1$ é par. Como $q - 1$ é par e p é ímpar, o número k, da fórmula acima, deve ser obrigatoriamente par. Assim, concluímos que $q - 1 = 2rp$ para algum inteiro r. O que equivale a dizer que $q = 1 + 2rp$, para algum inteiro positivo r. □

A proposição nos diz que, dado um inteiro n, para aplicar o método, substituimos o valor de n na fórmula geral dos fatores de n e vamos substituindo valores inteiros, começando por 1, para r, até encontrar um q primo e que divida n. Se não encontrarmos tal valor de q, então n é primo.

Exemplo 14. *Vamos usar o método de Fermat para achar um fator de* $M(29)$

Como 29 *é primo, segue pelo método de Fermat, que os fatores primos de* $2^{29}-1$ *são da forma* $1+2\cdot r\cdot 29 = 1+58r$. *Vamos tabelar estes fatores para valores de* $r \geq 1$ *e calcular o resto da divisão de* $M(29) = 2^{29}-1$ *por* $q = 1+58r$, *quando* q *é primo. Obtemos*

r	$q = 1+58r$	*primo ou composto?*	*resto de* 2^p-1 *por* q
1	59	*primo*	58
2	117	*múltiplo de* 3	*
3	175	*múltiplo de* 5	*
4	233	*primo*	0

Logo 233 *é o menor fator primo de* $M(29)$

3.2 Números de Fermat

Proposição 51. *Se* 2^n+1 *é primo, então* $n = 2^m$, *com* $m > 0$.

Demonstração. Suponhamos que exista $p \neq 2$ tal que $p|n$. Segue que $n = p\cdot n'$ com $n' \neq n$. Como p é ímpar, temos, pela Proposição 3 do Capítulo 1, que

$$2^{n'}+1 | 2^{p\cdot n'}+1 = 2^n+1.$$

com $2^{n'}+1 \neq 1$ e $2^{n'}+1 \neq 2^n+1$. O que é uma contradição, pois por hipótese 2^n+1 é primo. Portanto n não possui fatores primos diferentes de 2, isto é, $n = 2^m (m > 0)$. □

Definição 24. *Um número inteiro positivo é dito um número de Fermat quando esse número é da forma*

$$F_n = 2^{2^n}+1, n = 0, 1, 2, ...$$

Em 1640, Fermat sugeriu que estes números fossem sempre primos. É verdade que os números F_k é sempre primo quando k varia de 0 *a* 4. De fato, $F_0 = 1, F_1 = 5, F_2 = 17, F_3 = 257$ *e* $F_4 = 65537$. Porém, F_5 é composto. Isso foi provado, em 1732, pelo matemático suiço Leonhard Euler, utilizando um método baseado no método da seção anterior, inventado pelo próprio Fermat.

Definição 25. *Os números de Fermat que são primos são conhecidos como primos de Fermat.*

Vamos enunciar agora o método utilizado por Euler para encontrar um fator primo de um número de Fermat, encontrando a fórmula geral desse fator.

Proposição 52. ***(Método de Euler)*** *Se q é um fator primo de F_k então existe um número inteiro positivo r tal que $q = 1 + 2^{k+1}r$.*

Demonstração. Digamos que q é um fator primo de F_k. Então

$$\overline{2}^{2^k} = \overline{-1} \text{ em } U(q).$$

Donde, $\overline{2}^{2^k \cdot 2} = \overline{2}^{2^{k+1}} = \overline{1}$ *em* $U(q)$. Daí, pela Proposição 39, teremos que a ordem de $\overline{2}$ divide 2^{k+1}; mas como $\overline{2}^{2^k} = -1$ *em* $U(q)$, temos também que a ordem não pode ser uma potência menor que 2^{k+1}. Logo a ordem de $\overline{2}$ *em* $U(q)$ é exatamente 2^{k+1}. Mas, o teorema de Fermat nos garante que a ordem de $\overline{2}$ divide $q-1$, donde $q - 1 = 2^{k+1}r$, isto é, $q = 1 + 2^{k+1}r$ para um número inteiro positivo r. □

Para aplicar esse método para descobrir se um determinado número n é primo ou composto, e no segundo caso encontrar um fator de n, basta substituirmos o valor de n na fórmula geral dos seus fatores e depois substituir valores inteiros, começando por 1, para r, até encontar um q primo e que divida n. Se não encontrarmos tal valor de q, então n é primo.

Exemplo 15. *Vejamos como utilizar o método de Euler para encontrar um fator de F_5 e assim, mostrar que esse número é composto. Vamos tomar $F_5 = 2^{2^5} + 1 = 2^{32} + 1$. Pelo método de Euler, um fator primo q de F_5 tem que ser da forma $q = 1 + 2^{5+1}r = 1 + 64r$. Precisamos verificar se q é um fator de F_5 para os valores de r onde*

$$q < \sqrt{2^{32} + 1} \leq 66000.$$

Isto nos dá $r < 1031$, um número bem grande. O menor valor de r para o qual q é primo é $r = 3$, que dá $q = 193$.

$$2^{32} \equiv (2^8)^4 \equiv 63^4 \equiv 108 \ (mod\ 193).$$

Portanto 193 não é fator de F_5. Para $r = 4$ temos $q = 257$ que é primo, mas

$$2^{32} \equiv 1 \ (mod\ 257).$$

Logo 257 *também não é fator de* F_5. *O próximo valor de* r *em que* q *é primo é* $r = 7$, *onde obtemos* $q = 449$, *mas*

$$2^{32} \equiv (2^{16})^2 \equiv 431^2 \equiv 324 \ (mod\ 449).$$

Logo 449 *não é fator de* F_5. *Prosseguindo, o próximo valor de* r *que gera* q *primo é* $r = 9$, *para o qual* $q = 577$.

Neste caso,

$$2^{32} \equiv 287 \ (mod\ 577).$$

Donde 577 *também não é fator de* F_5. *Quando tomamos* $r = 10$, *temos* $q = 641$ *que é finalmente um fator de* F_5.

Por sorte, o fator é pequeno, assim, podemos encontrá-lo utilizando o método de Euler e uma máquina de calcular, mas essa tarefa pode se tornar muito mais complexa se o fator for muito grande.

4 Teste de Lucas

4.1 Teste de Lucas

Aqui vamos apresentar um teste que nos permite verificar se um número é primo sem tentar achar seus fatores.

Proposição 53. ***(Teste de Lucas)*** *Seja* n *um inteiro positivo ímpar e* b *um inteiro tal que* $2 \leq b \leq n-1$. *Se*

$$b^{n-1} \equiv 1 \ (mod\ n) \quad e \quad b^{\frac{(n-1)}{p}} \not\equiv 1 \ (mod\ n),$$

para cada fator primo p *de* $n-1$, *então* n *é primo.*

Demonstração. Como $b^{n-1} \equiv 1 \ (mod\ n)$ $(n \geq 2)$, temos que $(b, n) = 1$.

Seja k a ordem de b com respeito a n. Queremos mostrar que $k = n - 1$.

Como $b^{n-1} \equiv 1 \ (mod\ n)$, pela Proposição 39, $k | n-1$. Digamos que $n - 1 = k.t$, onde t é um inteiro positivo. Nosso objetivo é mostrar que $t = 1$.

Então, vamos supor por absurdo, que $t > 1$. Assim, t deve ser divisível por algum q

primo. Mas se $q|t$, então $q|n-1$. Portanto $\frac{(n-1)}{q}$ e $\frac{t}{q}$ são inteiros e

$$\frac{n-1}{q} = k.\frac{t}{q}.$$

Daí, $k|\frac{(n-1)}{q}$.

Novamente pela Proposição 39, deduzimos que

$$b^{\frac{(n-1)}{q}} \equiv 1 \ (mod\ n);$$

o que contradiz a hipótese.

Com isso, concluímos que $t = 1$ e, consequentemente, $k = n - 1$.

Assim, $o_n(b) = n - 1$ e $n - 1$ divide $n - 1|\phi(n)$. Daí

$$n - 1 \leq \phi(n) \leq n - 1$$

Logo $\phi(n) = n - 1$ e daí n é primo. □

Este teste determina com certeza se um dado número é primo.

Observe que para aplicá-lo com sucesso precisamos ser capazes de fatorar $n - 1$.

Vamos mostrar agora, através de um exemplo, como o teste funciona para descobrir se um número é primo.

Exemplo 16. *Pegue* $n = 71$. *Então* $n - 1 = 70$ *e os fatores primos de* 70 *são* $2, 5$ *e* 7. *Vamos escolher aleatoriamente um* $b = 17 < n$. *Notemos que:* $17^{70} \equiv 1 \mod 71$.

Temos que

$b^{n-1} \equiv 1 \ (mod\ n)$ *se, e somente se,* $o(b)|(n-1)$.

Mas, a ordem de $17(mod\ 71)$ *não é, necessariamente,* 70 *porque algum fator de* 70 *pode também satisfazer a congruência. Então vamos conferir para* 70 *dividido por seus fatores primos:*

$17^{35} \equiv 70 \not\equiv 1 \ (mod\ 71)$

$17^{14} \equiv 25 \not\equiv 1 \ (mod\ 71)$

$17^{10} \equiv 1 \equiv 1 \ (mod\ 71)$.

Infelizmente, temos que $17^{10} \equiv 1 \ (mod\ 71)$. *Portanto, ainda não sei se* 71 *é primo*

ou não.

Tentamos outra forma aleatória, desta vez escolhendo $b = 11$*. Chegamos que:*

$11^{70} \equiv 1 \ (mod\ 71)$.

Novamente, isto não indica que a ordem de $11(mod\ 71)$ *é* 70*, porque algum fator de* 70 *também pode funcionar. Então confira* 70 *dividido por seus fatores primos:*

$11^{35} \equiv 70 \not\equiv 1 \ (mod\ 71)$

$11^{14} \equiv 54 \not\equiv 1 \ (mod\ 71)$

$11^{10} \equiv 32 \not\equiv 1 \ (mod\ 71)$.

Portanto, a ordem de $11(mod\ 71)$ *é* 70*, portanto* 71 *, é primo.*

Na prática há vários primos interessantes para os quais está condição é facilmente verificada. Por exemplo, este teste é excelente para os números de Fermat $F_n = 2^{2^n} + 1$, pois $F_n - 1$ tem apenas um fator primo, que é o número 2.

4.2 Teste de Pepin

Proposição 54. ***(Teste de Pepin)*** *O número de Fermat* $F_k = 2^{2^K} + 1$ *é primo para* $k > 1$ *se* $5^{\frac{F_k - 1}{2}} \equiv -1 \ (mod\ F_k)$.

Demonstração. Suponhamos que $5^{\frac{F_k - 1}{2}} \equiv -1 \ (mod\ 2^{2^K} + 1)$.

Daí

$$5^{F_k - 1} \equiv 1 \ (mod\ 2^{2^K} + 1).$$

Como por hipótese $5^{\frac{F_k - 1}{2}} \equiv -1 \not\equiv 1 \ (mod\ 2^{2^K} + 1)$ e 2 é o único fator primo de $F_k - 1$, teremos pelo Teste de Lucas que F_k é primo. □

Observação. Vale a recíproca e sua prova depende da *lei de reciprocidade quadrática*, mas não iremos prová-la aqui.

Exemplo 17. *Vamos aplicar o teste de Pepin ao número de Fermat* F_4*, para verificar se o mesmo é primo.*

Temos que $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$*, daí*

$$\frac{F_4 - 1}{2} = 2^{15}.$$

Fazendo os cálculos teremos que

$$5^{2^{15}} \equiv 5^{32768} \equiv 65536 \equiv -1 \ (mod\ F_4).$$

Logo, pelo teste de Pepin, F_4 é primo.

Exemplo 18. *Vamos utilizar o Teste de Pepin para verificar que F_5 é composto.*

Temos que $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967$, daí

$$\frac{F_5 - 1}{2} = 2^{31}$$

Fazendo os cálculos obtemos

$$5^{2^{31}} \equiv 2405788 \ (mod\ F_5)$$

Portanto F_5 não passa no teste de Pepin, donde F_5 é composto.

Observação. Poderemos ter muita dificuldade em aplicar o teste de Lucas para alguns inteiros, pois, dado um inteiro n, o teste requer que uma única base satisfaça todas as equações para os fatores de $n - 1$.

Existe um teste que enunciaremos a seguir, baseado no teste de Lucas, só que mais eficiente, pois utiliza bases distintas para fatores distintos de $n - 1$.

4.3 Outro teste determinístico de primalidade

Proposição 55. ***(Teste de primalidade)****Seja $n > 0$ um inteiro tal que*

$$n - 1 = p_1^{e_1} \cdots p_r^{e_r}$$

onde $p_1 < ... < p_r$ são primos. Se para cada $i = 1, ..., r$ existirem inteiros positivos $b_i (2 \leq b \leq n - 1)$ que satisfaçam

$$b_i{}^{n-1} \equiv 1 \ (mod\ n) \quad e \quad b_i{}^{\frac{(n-1)}{p_i}} \not\equiv 1 \ (mod\ n)$$

então n é primo.

Demonstração. Vamos considerar o caso em que $i = 1$.

Suponhamos que s_1 seja a ordem de b_1 com respeito a n. Assim, pela Proposição 39, teremos que $s_1 | n - 1$. Logo s_1 não pode ter fatores primos diferentes dos de n, isto é, seus

fatores estão entre os primos $p_1 < ... < p_r$. Assim

$$s_1 = {p_1}^{k_1} \cdots {p_r}^{k_r}, \quad \text{onde} \quad 0 \leq k_1 \leq e_1, ..., 0 \leq k_r \leq e_r$$

Mas, sabemos que $b_i^{\frac{(n-1)}{p_1}} \not\equiv 1 \ (mod\ n)$, donde $\frac{(n-1)}{p_1}$ não é divisível por s_1. Por outro lado,

$$\frac{(n-1)}{p_1} = {p_1}^{e_1-1} \cdot {p_2}^{e_2} \cdots p_r^{e_r}.$$

Assim, para que s_1 não divida $\frac{(n-1)}{p_1}$ devemos ter $k_1 = e_1$. Isto significa que ${p_1}^{e_1}$ divide s_1. Como s_1 é a ordem de b_1 com respeito a n, temos, pela Proposição 39, que $s_1|\phi(n)$. Daí, ${p_1}^{e_1}|\phi(n)$. De modo análogo, ${p_2}^{e_2}, \ldots, p_r^{e_r}$ dividem $\phi(n)$. Além disso, como estas potências são formadas por primos distintos, elas são primas entre si. Então, pelo item *ii*) da Proposição 18, podemos concluir que o produto $p_1^{e_1} \cdots p_r^{e_r} = n - 1$ divide $\phi(n)$. A partir disso, chegamos à conclusão que

$$n - 1 \leq \phi(n) \leq n - 1.$$

Donde, $\phi(n) = n - 1$ e portanto, n é primo. □

Observação. Na proposição acima não é necessário que os $b_i's$ sejam todos distintos.

O teste acima nos diz que, se aplicando o teste de Lucas, uma base falhar em alguma das equações para os fatores do inteiro n, podemos mudar essa base e continuar o teste para as equações dos fatores que ainda restaram.

Vamos entender isso melhor através de um exemplo.

Exemplo 19. *Quando utilizamos o teste de Lucas para provar que o número* 41 *é primo, fatoramos* $n - 1 = 40$*, obtendo* $n - 1 = 2^3.5$*. Daí, precisamos encontrar uma base inteira* b *tal que* $2 \leq b \leq 40$ *e que satisfaça as equações:*

$$b^{40} \equiv 1 \ (mod\ 41)$$

$$b^{20} \not\equiv 1 \ (mod\ 41)$$

$$b^{8} \not\equiv 1 \ (mod\ 41).$$

Começando com $b = 2$*, logo verificamos que* $2^{20} \equiv 1 \ (mod\ 41)$*. Passamos a* $b = 3$*, onde obtemos* $3^{20} \equiv 40 \ (mod\ 41)$*, mas* $3^8 \equiv 1 \ (mod\ 41)$*. Além disso, podemos observar que* $2^8 \equiv 10 \ (mod\ 41)$*. No entanto, nenhuma dessas bases serve para o teste de Lucas. A primeira base que satisfaz todas as equações para o teste de Lucas seria o número*

7. *Em contrapartida, se aplicarmos o teste anterior, bastaria observar que* $2^{\frac{40}{5}} = 2^8 \equiv 10\ (mod\ 41)$ *e* $3^{\frac{40}{2}} = 3^{20} \equiv 40\ (mod\ 41)$ *e já provamos que* 41 *é primo.*

5 Métodos de Pollard

Em 1974 e 1975, John Pollard anunciou dois novos algoritmos para se obter fatores de números inteiros grandes. Esses dois algoritmos são probabilísticos e na prática, com esses métodos, encontraremos um fator do número dado, bem mais rápido do que se utilizássemos um algoritmo determinístico.

5.1 Método Rho de Pollard

Seja n um número inteiro grande, composto, e p o menor fator primo de n. Vamos considerar uma sequência de inteiros $x_0, x_1, ..., x_s$ não congruentes 2 a 2, módulo n. Se $x_i \equiv x_j\ (mod\ p)$, com $i \neq j$, então $(x_i - x_j, n)$ é um divisor não trivial de n. De fato, $p|x_i - x_j$ e $n \nmid x_i - x_j$. Além disso, se $(x_i - x_j, n) = d$, então $d|n$ e $d|x_i - x_j$. Como $p|x_i - x_j$ e $n \nmid x_i - x_j$, teremos que $d \neq n$ e $d \geq p$. Donde d é um divisor não trivial de n.

Proposição 56. *Dados n inteiro e p o menor fator primo de n. Considere* x_0 *um valor aleatório e defina* $(x_k)_{k\geq 0}$ *recursivamente como*

$$x_{k+1} \equiv f(x_k)\ (mod\ n), \quad com \quad 0 \leq x_{k+1} \leq n-1.$$

onde $f(x)$ *é uma função polinomial arbitrária com coeficientes inteiros e grau maior que 1. Se* $x_i \equiv x_j\ (mod\ p)(i, j > 1)$ *então a sequência* x_k *se torna periódica mod p com um período* $j - i$.

Demonstração. Utilizando a definição recursiva de x_k temos que se

$$x_i \equiv x_j\ (mod\ p),$$

onde p é um inteiro positivo, então

$$x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv x_{j+1}\ (mod\ p).$$

e assim por diante. O que significa que dois termos sempre serão congruentes quando a diferença de seus índices for $j - i$, o que prova nossa tese. □

Corolário 57. *Se a sequência definida acima é periódica mod p com período $j-i$, então $x_s \equiv x_{2s}$ $(mod\ p)$, onde s é o menor múltiplo de $j-i$.*

Demonstração. Da hipótese segue que dois termos de x_k sempre são congruentes mod p, quando a diferença entre seus índices for $j-i$. Assim, teremos que $x_q \equiv x_r$ $(mod\ p)$ sempre que $q \equiv r$ $(mod\ j-i)$ e $q \geq i$ e $r \geq j$. O que significa que dois termos da sequência x_k sempre serão congruentes módulo p quando a diferença de seus índices for um múltiplo de $j-i$. Disto, podemos ver que sendo s o menor múltiplo de $j-i$, então $x_s \equiv x_{2s}$ $(mod\ p)$. □

Para encontrar um fator de um inteiro n, utilizando o método Rho de Pollard, escolhemos um valor para x_0 e uma função como a definida na Proposição 56, depois achamos os termos da sequência definida, segundo a fórmula recursiva dada na mesma proposição e por último calculamos o mdc de $x_{2k} - x_k$ e n para $k = 1, 2, 3, ...$ O fator de n será encontrado quando ocorrer um valor de k para o qual $1 < (x_{2k} - x_k, n) < n$.

Exemplo 20. *Vamos encontrar um fator não trivial do número $n = 8051$ utilizando método Rho, tomando valor inicial $x_0 = 2$ e polinômio gerador $f(x) = x^2+1$. Nesse caso, encontraremos a sequência*

$$x_1 = 5, x_2 = 26, x_3 = 677, x_4 = 7474, x_5 = 2839, x_6 = 871, ...$$

Utilizando o algoritmo de Euclides para calcular o $(x_{2k} - x_k, n)$ obtemos $(x_2 - x_1, 8051) = (26 - 5, 8051) = (21, 8051) = 1$; $(x_4 - x_2, 8051) = (7474 - 26, 8051) = (7448, 8051) = 1$; $(x_6 - x_3, 8051) = (871 - 677, 8051) = (194, 8051) = 97$. Então, encontramos nesse passo um fator não trivial de 8051, que é o número 97.

A sequência gerada no exemplo anterior será periódica módulo p e terá período $6-3 = 3$. Note que $x_0 \equiv x_3$ $(mod\ 97)$; $x_1 \equiv x_4$ $(mod\ 97)$; $x_2 \equiv x_5$ $(mod\ 97)$ e assim por diante.

Observação. Na prática, o polinômio $f(x) = x^2 + 1$ e o valor inicial $x_0 = 2$ são frequentemente escolhidos para gerar a sequência de inteiros $x_o, x_1, x_2, ..., x_k, ...$

O método Rho é prático quando o inteiro a ser fatorado tem fatores primos não muito grandes.

5.2 Método p-1

Este método de fatoração, que têm como base o Pequeno Teorema de Fermat, nos permite encontar um fator não trivial de um inteiro n que tem um fator primo p tal que

os fatores de $p-1$ são relativamente pequenos. O método de Pollard não funciona bem para qualquer inteiro n, como a maioria dos métodos, mas quando ele funciona, é muito eficiente. A ideia na qual esse método se baseia é dada pela seguinte proposição.

Proposição 58. *Sejam n um número inteiro positivo ímpar composto e p um fator primo de n. Sejam a e k números inteiros tais que $mdc(a,p) = 1$ e $p-1|k$. Então, $p|mdc(a^k-1, n)$.*

Demonstração. Por hipótese, $p-1|k$, donde $k = k'(p-1)$, para algum inteiro k'. Como p é primo e $p \nmid a$, segue do Pequeno Teorema de Fermat que $a^{p-1} \equiv 1 \ (mod\ p)$. Elevando ambos os termos da congruência ao expoente k' e usando a relação entre k e k' obtemos $a^k \equiv 1 \ (mod\ p)$, que é equivalente a $p|a^k - 1$. Assim, p é fator comum de $a^k - 1$ e n. Portanto $p|mdc(a^k-1, n)$. □

Para utilizar o método de Pollard, baseado na proposição acima, e tentar encontrar um fator primo p de um inteiro composto n, escolhemos inteiros positivos a e k de modo que $mdc(a,n) = 1$ (o que significa que $mdc(a,p) = 1$ para todo fator primo p de n) e k seja divisível por potências de primos pequenos (por exemplo $k = mmc(1,2,3,...,B)$ ou $k = B!$, para um certo inteiro B). Em seguida, calculamos $d = mdc(a^k-1, n)$ e esperamos encontrar um fator não trivial de n, conforme a proposição anterior. Como $mdc(a,b) = mdc(b, a \ mod\ b)$, então não é necessário calcular $a^k - 1$; basta calcular $(a^k - 1) \ mod\ n$. Uma vez calculado d, temos 3 possibilidades.

1. $1 < d < n$. Neste caso, d é um fator não trivial de n.
2. $d = 1$. Este caso ocorre quando $p-1$ não divide k. Devemos então aumentar o valor de k e aplicar novamente o método.
3. $d = n$. Quando isso ocorre, devemos escolher outro valor para a e começar novamente.

Portanto, podemos enunciar o método de Pollard na forma de algoritmo da seguinte maneira.

Algoritmo 59. ***(Algoritmo p-1 de Pollard)*** *Seja $n \geq 2$ um inteiro composto para o qual desejamos achar um fator primo.*

1. *Escolha um número k sendo um produto primos pequenos elevados a potências pequenas. Por exemplo, considere*

$$k = mmc(2,3,...,B)$$

para um certo inteiro B.

2. *Escolha um inteiro qualquer a tal que $0 < a < n$.*

3. *Calcule $mdc(a, n)$. Se ele é estritamente maior que 1, então ele é um fator não trivial de n. Daí pare. Caso contrário vá para a etapa 4.*

4. *Calcule $d = mdc(a^k - 1, n)$. Se $1 < d < n$, então d é um fator não trivial de n. Então pare. Se $d = 1$, volte para a etapa 1 e tome um k maior. Se $d = n$, volte para a etapa 2 e escolha outro valor para a.*

Observação. Note que o algoritmo de Pollard certamente irá parar, pois em certo momento, teremos no passo 1, um valor de B tal que $B = \frac{1}{2}(p-1)$ para algum primo p que divide n, e portanto $p-1$ certamente dividirá k, donde $a^k - 1 = a^{(p-1)q} - 1$ que, pelo Pequeno Teorema de Fermat, é divisível por p e daí $d = mdc(a^k - 1, n)$ será igual a p que nesse caso é fator de n . Por exemplo, dado $n = 143$, pelo método $p-1$, começando com $k = 2$ e tomando $a = 2$, obteremos até a quarta tentativa $mdc(2^k - 1, 143) = 1$, só que quando chegamos em $k = mmc(2, 3, ..., 5) = 60$ teremos $mdc(2^{60} - 1, 143) = 11$, pois 11 é um fator de 143, e como $11 - 1 = 10$ divide 60, temos também que $2^{60} - 1$ é divisível por 11. No entanto, este processo pode gastar muito tempo e o algoritmo não será prático para valores grandes de k. O algoritmo só roda numa quantidade de tempo razoável quando n tem um divisor primo p tal que $p-1$ é produto de primos pequenos elevados a potências pequenas.

Exemplo 21. *Vamos calcular, utilizando o método $p-1$ de Pollard, um fator de $n = 35318303$.*

Primeiramente, vamos supor o número 35318303 composto. Agora vamos encontrar um fator desse número.

Inicialmente, vamos tomar $a = 2$ e $k = mmc(2, 3, ..., 5) = 60$. Para facilitar os cálculos, escrevemos 60 na base 2, obtendo

$$60 = 2^5 + 2^4 + 2^3 + 2^2$$

Calculamos, então, os valores $2^{2^i} \pmod n$, $0 \leq i \leq 5$, e apresentamo-los na tabela a seguir:

i	2^{2^i} mod 35318303
0	2
1	4
2	16
3	256
4	65536
5	21452633

A partir da tabela calculamos

$$2^{60} = 2^{2^5+2^4+2^3+2^2} = 2^{2^5} \cdot 2^{2^4} \cdot 2^{2^3} \cdot 2^{2^2} \equiv 30748919 \ (mod\ 35318303)$$

Utilizando o algoritmo euclidiano obteremos

$$mdc(2^{60} - 1, 35318303) = mdc(30748918, 35318303) = 1$$

Portanto, para esses valores o teste falha. Isso se deve ao fato de que para nenhum fator primo p de 35318303*, teremos que $p - 1$ divide* 60*. O que fazemos então é aumentar o valor de k e esperar que exista um fator primo p de* 35318303 *tal que $p - 1$ divida o novo valor de k. Então, tomemos $k = mmc(2, 3, ..., 7) = 420$. Escrevendo* 420 *na base* 2 *obtemos*

$$420 = 2^8 + 2^7 + 2^5 + 2^2$$

Calculando, os valores de 2^{2^i} $(mod\ n)$ para $i = 6, 7, 8$ obtemos

i	2^{2^i} mod 35318303
6	32844765
7	24017239
8	26510038

Daí

$$2^{420} = 2^{2^8+2^7+2^5+2^2} = 2^{2^8} \cdot 2^{2^7} \cdot 2^{2^5} \cdot 2^{2^2} \equiv 2502093 \ (mod\ 35318303)$$

Utilizando o algoritmo euclidiano obteremos

$$mdc(2^{60} - 1, 35318303) = mdc(2502092, 35318303) = 1$$

e novamente o teste falha.

Vamos tomar agora $k = mmc(2, 3, ..., 11) = 27720$. *Então escrevemos esse novo valor de* k *na base* 2 *obtendo*

$$27720 = 2^{14} + 2^{13} + 2^{11} + 2^{10} + 2^6 + 2^3$$

Agora, estendemos a tabela, calculando os valores de 2^{2^i} $(mod\ n)$ *de que precisamos obtendo*

i	2^{2^i} mod 35318303
9	14876672
10	5160260
11	13402447
12	16450291
13	22433108
14	15795689

Utilizando esses valores obtidos podemos calcular $2^{27720} = 2^{2^{14}+2^{13}+2^{11}+2^{10}+2^6+2^3} = 2^{2^{14}} \cdot 2^{2^{13}} \cdot 2^{2^{11}} \cdot 2^{2^{10}} \cdot 2^{2^6} \cdot 2^{2^3} \equiv 14301996\ (mod\ 35318303)$

Agora, usando o algoritmo euclidiano obtemos

$$mdc(2^{27720} - 1, 35318303) = mdc(14301995, 35318303) = 4621$$

E assim, encontramos, como queríamos um fator não trivial de 35318303. *Além disso, fatoramos* 35318303 *como* $4621 \cdot 7643$ *e cada um destes fatores é primo, e assim fatoramos* n *completamente.*

Tivemos sucesso em encontrar um fator não trivial de n *nessa passagem, pelo fato de que o fator* $p = 4621$ *encontrado é tal que* $p - 1 = 4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ *divide* $k = 27720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$. *Observe também que como* 4621, *que é um fator de* 35318303, *diminuido de uma unidade é produto de primos pequenos elevados a expoentes*

pequenos, isso nos permitiu fatorar esse número em um tempo razoável utilizando esse método.

Observação. Existe um outro método de fatoração de inteiros baseado no Método $p-1$. Esse método é devido a H. W. Lenstra, e utiliza curvas elíticas. O método de Lenstra é mais vantajoso e eficiente em relação a qualquer um dos métodos estudados nesse trabalho, mas não será estudado aqui pois exige outros conhecimentos, além dos tratados neste trabalho.

5 *Criptografia RSA*

Nesse capítulo, iremos descrever o método de criptografia RSA que é muito importante e muito utilizado na criação de senhas codificadas. A segurança do RSA é baseada na ineficiência dos métodos de fatoração atualmente conhecidos.

1 Pré-codificação

Primeiramente, vamos entender as características iniciais para se criar uma mensagem codificada através do método RSA, o que chamamos de pré-codificação. A mensagem inicial será um texto com palavras e o espaço entre elas. Na pré codificação convertemos as letras em números usando, por exemplo, 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

O espaço entre duas palavras será substituido pelo número 99, quando for feita a conversão. Por exemplo, a frase “Estudar é bom”é convertida no número

$$14282829131027991499112422.$$

Cada letra corresponde a um número a partir de 10, isto é, de dois algarismos, pois isso evita que hajam ambiguidades. Se começassemos do 1, poderia ocorrer que 13 poderia ser AC ou M, que é a décima terceira letra do alfabeto.

Na pré-codificação do RSA, vamos utilizar dois números inteiros primos p e q, os quais chamaremos de parâmetros e que serão multiplicados resultando num número $n = p \cdot q$. A parte final da pré-codificação consiste em quebrar o longo número, obtido quando fizemos a conversão da frase utilizando a tabela, em blocos que devem ser números menores que n. Por exemplo, se os números primos escolhidos forem $p = 11$ e $q = 13$, então teremos $n = 143$. Neste caso, a frase convertida pode ser quebrada em blocos da seguinte maneira:

$$14 - 28 - 28 - 29 - 13 - 102 - 79 - 91 - 49 - 91 - 124 - 22$$

A maneira de se escolher esses blocos não é única, mas devemos tomar certos cuidados. Por exemplo, se tomarmos um bloco começando pelo número 0, isto pode nos trazer problemas na hora de decodificar a mensagem, então isso deve ser evitado. Além disso, devemos evitar tomar blocos que depois de decodificados formem alguma palavra ou letra, pois isso melhora a segurança da mensagem, sendo que torna praticamente impossível a decodificação por contagem de frequência ou por adivinhação da frase antes que a mesma seja toda decodificada.

2 Codificação e decodificação

Agora, vamos entender como codificar e decodificar uma mensagem utilizando o sistema RSA. Para codificar a mensagem por este sistema precisamos de um número inteiro n, que seja produto de dois números primos, como vimos na pré-codificação, e também de um inteiro positivo e, que seja inversível módulo $\phi(n)$. O que significa que devemos ter $(e, \phi(n)) = 1$. É claro que se conhecermos os fatores p e q de n, é fácil encontrar $\phi(n)$ já que

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

O par $(n; e)$ será chamado de chave de codificação do sistema RSA que estamos utilizando. Codificaremos a mensagem, codificando separadamente cada um dos blocos de números menores que n obtidos na pré-codificação, utilizando a chave de codificação. É muito importante frisar que após codificarmos a mensagem não podemos reunir os blocos formando um único e longo número, porque isso torna a impossível decodificar a mensagem, como veremos adiante.

Vamos ver agora, como proceder para codificar a mensagem utilizando a chave de codificação (n, e).

Vamos tomar um certo bloco b da mensagem, onde b é um inteiro positivo menor que n. Denotando por $C(b)$ o bloco codificado, encontraremos $C(b)$ da seguinte maneira:

$$C(b) = \text{ resto da divisão de } b^e \text{ por } n.$$

O que significa que $C(b)$ é a forma reduzida de b^e módulo n. Vamos ver como ficaria a codificação no exemplo que estamos considerando. Temos que $p = 11$ e $q = 13$, donde $n = 143$, então $\phi(n) = (11-1)\cdot(13-1) = 120$. Agora, nos falta escolher e de modo que $(e, 120) = 1$. Neste caso, o menor valor possível para e é 7, que é o menor primo que não divide 120. Assim, por exemplo, para codificar o bloco 124 da mensagem, encontraremos o resto da divisão de 124^7 por 143. Fazendo as contas, teremos

$$124^7 \equiv (-19)^7 \equiv -19^7 \equiv 25\cdot(-19) \equiv -46 \equiv 97 \ (mod\ 143).$$

Portanto $C(124) = 97$.

Codificando toda a mensagem, otemos:

$$53 - 63 - 63 - 94 - 117 - 119 - 40 - 130 - 36 - 130 - 97 - 22$$

Vamos ver agora, como decodificar uma mensagem codificada pelo método RSA.

Para decodificar uma mensagem precisamos de duas informações: o número n e um número que denotaremos por d, que é o inverso de e módulo $\phi(n)$. O par (n, d) será a nossa chave de decodificação. Utilizando a chave de decodificação, decodificaremos um bloco a da mensagem codificada, calculando o resto da divisão de a^d por n. Então, sendo $D(a)$ o resultado da decodificação de um bloco a, teremos que

$$D(a) = \text{ resto da divisão de } a^d \text{ por } n.$$

Nesse caso, $D(a)$ é a forma reduzida de a^d módulo n.

No exemplo temos que $n = 143$ e $e = 7$. Para encontrar d vamos aplicar o Algoritmo Euclidiano Estendido. Nesse exemplo, o cálculo é simples, pois dividindo $\phi(143) = 120$ por 7, obtemos

$$120 = 7\cdot 17 + 1, \quad \text{donde} \quad 1 = 120 + (-17)\cdot 7.$$

Assim, o inverso de 7 módulo 120 é -17. Mas, como d será usado como expoente de potências, vamos tomar d positivo. Logo $d = 120 - 17 = 103$. Assim, para decodificar

o bloco 97 da mensagem codificada, calculamos a forma reduzida de 97^{103} módulo 143. Utilizando uma calculadora, obtemos

$$97^{103} \equiv 97^{100}.47 \equiv 114^{50}.47 \equiv 56^{10}.47 \equiv 100.47 \equiv 124 \ (mod\ 143).$$

Portanto $D(97) = 124$.

Podemos perceber que o método funciona para este bloco, mas será que isso sempre acontece? Isso é o que vamos ver na próxima seção.

3 Funcionamento

Para que o método funcione, esperamos que, decodificando um bloco da mensagem codificada, encontremos o bloco correspondente da mensagem original. Em outras palavras, dadas as fórmulas de codificação e decodificação do RSA:

$$C(b) \equiv b^e \ (mod\ n);$$

$$D(a) \equiv a^d \ (mod\ n);$$

sendo a um bloco codificado e b um bloco da mensagem original e d é o inverso de e módulo $\phi(n)$. Esperamos que sempre ocorra que $D(C(b)) = b$. Vamos provar que isso sempre é válido e assim provar o funcionamento do RSA. Para isso vamos enunciar essa propriedade em forma de proposição e demonstrá-la.

Proposição 60. *$D(C(b)) = b$.*

Demonstração. Temos que $D(C(b)) \equiv C(b)^d \equiv b^{ed} \ (mod\ n)$. Mas, como d é inverso de e módulo $\phi(n)$, $ed = 1 + k\phi(n)$. Daí, segue que $D(C(b)) \equiv b^{1+k\phi(n)} \equiv (b^{\phi(n)})^k b \ (mod\ n)$. Como $n = pq$, temos que $\phi(n) = (p-1)(q-1)$ o que implica que $D(C(b)) \equiv (b^{p-1})^{(q-1)k} b$ $(mod\ p)$. Se p não divide b, então

$$D(C(b)) \equiv b \ (mod\ p)$$

pelo Pequeno Teorema de Fermat. Se p divide b, então $b \equiv 0 \ (mod\ n)$ ou seja $D(C(b)) \equiv (b^{p-1})^{(q-1)k} b \equiv 0 \ (mod\ p)$. Analogamente, é possível mostrar que $D(C(b)) \equiv b \ (mod\ q)$ e como p e q são primos,

$$D(C(b)) \equiv b \ (mod\ n)$$

Como b e $D(C(b))$ são menores do que n, temos a igualdade

$$D(C(b)) = b.$$

□

4 Segurança do RSA

O RSA é um sistema de chave pública, isto significa que a chave de codificação (n, e) é pública, isto é, ela é acessível para qualquer usuário do sistema. Portanto, a segurança do RSA depende da dificuldade de se calcular d conhecendo n e e.

Na prática, só conseguimos calcular d, conhecendo e e $\phi(n)$. Mas, devemos lembrar que os parâmetros p e q não são públicos, e para calcular $\phi(n)$, temos que saber fatorar n para obter esses parâmetros. Assim, a segurança do RSA é baseada na dificuldade de se fatorar um número utilizando os algoritmos de fatoração atualmente conhecidos.

De fato, podemos verificar que, se fatoramos n, então podemos encontrar $\phi(n)$ e utilizar as operações da seção anterior para decifrar a mensagem. Por outro lado, se for inventado um algoritmo eficiente para se calcular $\phi(n)$ sem conhecer os parâmetros p e q, teremos $n = p.q$ e $\phi(n) = (p-1) \cdot (q-1)$ conhecidos. Daí,

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

portanto, $p + q = n - \phi(n) + 1$. Em contrapartida, temos que

$$(p+q)^2 - 4n = (p^2 + q^2 + 2pq) - 4n = (p^2 + q^2 - 2pq) = (p-q)^2$$

logo

$$p - q = \sqrt{(n - \phi(n) + 1)^2 - 4n}$$

e destas duas equações segue que

$$p = \frac{\sqrt{(n - \phi(n) + 1)^2 - 4n} + n - \phi(n) + 1}{2}$$

e

$$q = -\frac{\sqrt{(n - \phi(n) + 1)^2 - 4n} + n - \phi(n) + 1}{2}$$

E portanto, temos uma fatoração do número n.

Isso significa que não adianta pensarmos que alguém possa ter inventado um algoritmo para encontrar $\phi(n)$, sem encontrar fatores de n, pois conhecendo n e $\phi(n)$ encontramos os fatores de n.

Por tudo que vimos nesta seção, concluímos que quanto mais difícil de se fatorar o inteiro escolhido, mais difícil quebrar o sistema RSA. Então, é claro que não podemos escolher n de qualquer maneira, pois se esse número for fácil de ser fatorado, o RSA será quebrado facilmente. Primeiramente, podemos verificar que em vários momentos, frisou-se que se "n é grande", é praticamente impossível fatorá-lo. Então não podemos escolher primos pequenos. Um exemplo disso é a escolha do valor de n do exemplo que trabalhamos, pois 143 é um primo pequeno e podemos facilmente encontrar sua fatoração e consequentemente descobrir a mensagem codificada. Estudiosos desse método supõem que o indicado sejam números com aproximadamente 231 algarismos. Mas é claro que, não basta também escolhermos inteiros grandes, mas que podem ser facilmente fatorados utilizando alguns métodos de fatoração. Por exemplo, se escolhermos um inteiro que tem fatores p e q relativamente próximos, o mesmo pode ser facilmente fatorado pelo algoritmo de Fermat, ou quando os fatores p e q diminuídos de uma unidade tem fatores pequenos podemos utilizar o método $p-1$ de Pollard e fatorá-lo sem muita dificuldade. Isto significa que, a segurança do RSA depende muito da escolha do inteiro n, pois está intimamente ligada à dificuldade de fatorar esse número.

Exemplo 22. *A chave pública utilizada por um banco para codificar suas mensagens é a seguinte:* $n = 10403$ *e* $e = 8743$. *Recentemente os computaderes do banco receberam, de local indeterminado, a seguinte mensagem:*

$$4746 - 8214 - 9372 - 9009 - 4453 - 8198$$

Vamos descobrir o que diz a mensagem mandada ao banco.

A primeira coisa a se fazer é fatorar n para encontrar $\phi(n)$. *Pelo teorema de Fermat, obtemos:*

x	$\sqrt{x^2 - n}$	*Inteiro?*
102	1	*sim*

Então, os fatores de 10403 *são* $p = 103$ *e* $q = 101$ *e* $\phi(n) = (103 - 1) \cdot (101 - 1) = 10200$.

Agora, já podemos encontrar o valor do inverso de e módulo $\phi(n)$, *que será usado*

para decodificar a mansagem juntamente com n. Basta encontrar d, de modo que

$$d.8743 \equiv 1 \ (mod \ \phi(n))$$

Da congruência acima, temos que existe um k inteiro tal que

$$8743d - 1 = k\phi(n) \iff 8743d - k10200 = 1$$

Aplicando o algoritmo Euclidiano estendido teremos

restos	*quocientes*	k	d
10200	*	1	0
8743	*	0	1
1457	1	$1 - 1.0 = 1$	$0 - 1.1 = -1$
1	6	$0 - 6.1 = -6$	$1 - 6.(-1) = 7$

Assim, encontramos $d = 7$. *Agora, para decodificar cada bloco a da mensagem, calculamos o resto da divisão de* a^7 *por* $n = 10403$, *isto é, encontraremos os valores de b, que são os blocos da mensagem origiginal, em que cada b é a forma reduzida de* a^7 *módulo* 143. *Então, vamos à decodificação de cada bloco. Fazendo os cáculos obtemos que*

$$4746^7 \equiv 1514 \ (mod \ 10403)$$

$$8214^7 \equiv 2722 \ (mod \ 10403)$$

$$9372^7 \equiv 1029 \ (mod \ 10403)$$

$$9009^7 \equiv 9931 \ (mod \ 10403)$$

$$4453^7 \equiv 1831 \ (mod \ 10403)$$

$$8198^7 \equiv 14 \ (mod \ 10403)$$

Portanto, decodificando os blocos chegamos na seguinte situação

$$1514 - 2722 - 1029 - 9931 - 1831 - 14$$

Juntando os blocos teremos o número

$$151427221029993118 3114$$

E, portanto, a mensagem é "FERMAT VIVE"

Podemos notar que a segurança do sistema do exemplo é fraca, pois o número 10403 é fatorado com uma facilidade incrível utilizando o Algoritmo de Fermat. Então, a escolha do primo para codificar a mensagem, neste caso, foi infeliz.

Exemplo 23. *Seja* $(35318303, 299)$ *uma chave pública do RSA. Vamos utilizar essa chave para decodificar a seguinte mensagem, que foi codificada com esses parâmetros.*

$$34619207 - 27434838$$

Primeiramente, devemos encontrar os fatores de n, para calcular $\phi(n)$.

Os fatores de 35318303 *não são calculados tão facilmente, pelo Algoritmo de Fermat, como no número do exemplo anterior. Mas, já calculamos os fatores desse número utilizando o método* $p-1$ *de Pollard, na seção anterior. Então, a partir disso vamos calcular* $\phi(n)$.

Temos que $n = 35318303 = 4621 \cdot 7643$. *Daí,* $\phi(n) = 4620 \cdot 7642 = 35306040$. *Agora, vamos calcular o valor de d, encontrando o inverso de* 299 *módulo* $\phi(n)$. *Para isso, vamos aplicar o algoritmo Euclidiano estendido.*

Realizando os cálculos, chegamos que $d = 17357819$. *Então para decodificar a mensagem, encontraremos a forma reduzida de* $34619207^{17357819}$ *e* $27434838^{17357819}$ *módulo* 35318303.

Executando os cáculos chegamos que

$$34619207^{17357819} \equiv 272 \ (mod\ 35318303) \quad e \quad 27434838^{17357819} \equiv 810 \ (mod\ 35318303)$$

Portanto, decodificando os blocos e juntando teremos

$$272810$$

Logo, utilizando a tabela de conversão, concluímos que a mensagem é RSA

Como vimos neste trabalho, fatorar um número inteiro é um grande problema da matemática. Então até que se crie um método que fatore qualquer número com facilidade, o RSA continua sendo um sistema seguro.

Conclusão

Neste trabalho desenvolvemos a base matemática necessária para se entender alguns métodos de fatoração e testes de primalidade probabilísticos e determinísticos (tanto os mais usuais, quanto outros menos conhecidos). Na educação básica, a fatoração de inteiros se limita a números bem pequenos, o que pode passar uma idéia falsa do problema. É claro que muitos resultados estudados aqui não são aplicáveis no Ensino Básico, mas seria importante que professores estudassem mais sobre esse assunto, para entender os problemas e aplicações, como por exemplo, o sistema RSA apresentado no último capítulo.

Os testes determinísticos que estudamos em nosso trabalho tem um custo exponencial, isto é, conforme o valor de n aumenta, o tempo de execução, para determinar se dado número é primo ou composto, aumenta exponencialmente.

Em agosto de 2002, com a publicação de seu artigo original, os indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena impactaram a comunidade matemática com a publicação do *algoritmo AKS*, o primeiro teste de primalidade determinístico e de tempo polinomial, isto é, alem de determinar com certeza se o número é primo, o tempo que esse algoritmo gasta para chegar a tal conclusão pode ser bem menor do que se utilizássemos outros testes. Eles resolveram, de maneira brilhante, um problema que durava milênios e para entender a solução precisaremos apenas de conhecimentos estudados numa graduação de matemática ou da ciência em computação.

Esse algoritmo é de grande importância para a história da matemática e poderá ser um bom tema para um novo trabalho.

Referências

[1] S.C. Coutinho, *Números inteiros e Criptografia RSA*, Coleção Matemática e Aplicações, IMPA, Segunda edição, 2014.

[2] A. Hefes, *Aritmética*, Coleção PROFMAT, IMPA, 2013.

[3] C. Cardoso, *Fatoração de números inteiros usando curvas elíticas*, Dissertação de Mestrado, Departamento de Computação e Estatística - CCET - UFMS, 2003.

[4] A. Hefes, *Curso de Álgebra*, Coleção Matemática Universitária, IMPA, 2010.

[5] M. C. Oliveira, *Aritmética: Criptografia e outras aplicações de congruência*, Dissertação de Mestrado, PROFMAT - UFMS, 2013.
Http://bit.profmat-sbm.org.br/xmlui/handle/123456789/372

[6] C. M. Antunes, *Métodos de Fatoração de Números Inteiros*, Dissertação de Mestrado, PPGMAp da UFRGS, 2002.
http://www.lume.ufrgs.br/handle/10183/1626

[7] A. C. Campelo e I. Leal, *Teoria Aritmética dos Números e Criptografia RSA*, Monografia, IME - UNICAMP, 2007.
Http://www.ime.unicamp.br/∼ftorres/ENSINO/MONOGRAFIAS/antonio_ RSA.pdf

[8] S.C. Coutinho, *Primalidade em Tempo Polinomial: Uma introdução ao Algoritmo AKS*, Coleção Iniciação Científica, SBM, 2004.

[9] A. B. Chagas, *Testes de Primalidade: Uma Visão Computacional*, Trabalho de Graduação do curso de Ciência da Computação, UFPE, 2009.
Http://www.cin.ufpe.br/∼tg/2009-2/abc.pdf

[10] N.C. Saldanha, *Ordens e raízes primitivas*, PUC - RIO, 1999.
Http://www.mat.puc-rio.br/∼nicolau/papers/mersenne/node13.html.

[11] M. A. Faria e S. Serconek, *Números Primos: Testes de primalidade e aplicações*, Mini curso XXIII semana do IMPE, UFG, 2008.
Https://semanadoime.mat.ufg.br/up/34/o/min_ Cida.pdf

[12] F. F. Nunes, *Uma análise comparativa entre os testes de primalidade AKS e Miller-Rabin*, Trabalho de conclusão do curso de Matemática, UCB, 2007.
Https://www.ucb.br/sites/100/103/TCC/22007/FernandodeFarias.pdf