Universidade Federal de São Carlos
Departamento de Matemática

Teoria dos Números e Criptografia

Autor: Henrique Favarom Barbosa

Este texto foi editado em LaTeX 2$_\varepsilon$ pelo autor, que agradece á comunidade TeX pelos meios disponibilizados.

Teoria dos Números e Criptografia

Departamento de Matemática

Autor: *Henrique Favarom Barbosa*

Orientador: *Roberto Ribeiro Paterlini*

Disciplina: *Trabalho de Conclusão de Curso A*

Prof. Responsáveis:

Artur Darezzo Filho

Margarete Tereza Zanon Baptistini

.....

Orientador: Prof. Dr. Roberto Ribeiro Paterlini

.....

Orientando: Henrique Favarom Barbosa

São Carlos, 21 de novembro de 2008

Agradecimentos

Agradeço primeiramente à Deus por ter me dado a oportunidade e força necessária para concluir este curso superior. Gostaria de agradecer também ao meu orientador pela dedicação e paciência comigo e com este trabalho; aos meus pais por me oferecer todo apoio e dedicação possíveis e aos meus amigos pela paciência e apoio durante todo o curso e principalmente nos momentos difíceis durante a construção deste trabalho.

Resumo

Este trabalho tem como objetivo principal estudar e desenvolver técnicas e idéias matemáticas das áreas de Teoria dos Números e Álgebra e alguns métodos de criptografia, principalmente o método RSA. Neste trabalho, está incluso o Trabalho de Conclusão de Curso A, onde foi iniciado este estudo.

No Capítulo 1 apresentamos os teoremas básicos de Teoria dos Números relativos à divisibilidade, mdc e números primos. No Capítulo 2 vemos o método de fatoração de Fermat. No Capítulo 3 estudamos classes de equivalência e algumas aplicações. No Capítulo 4 apresentamos os números pseudoprimos. No Capítulo 5 trabalhamos com sistemas de congruência, e apresentamos o Teorema Chinês do Resto. No Capítulo 6, vemos alguns métodos elementares de criptografia. No Capítulo 7, apresentamos o método de criptografia RSA.

Sumário

Apresentação

Em grego, cryptos significa secreto, oculto. A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. Naturalmente todo código vem acompanhado de duas receitas: uma para codificar uma mensagem; outra para decodificar uma mensagem codificada. Decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Já decifrar significa ler uma mensagem codificada sem ser um usuário legítimo. O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1978 por R.L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T). As letras RSA correspondem às iniciais dos inventores do código. Porém, antes de descrever e estudar o método em si será necessário desenvolver muitas idéias e técnicas matemáticas da área de Teoria dos Números.

A presente monografia constitui um dos requisitos da disciplina Trabalho de Conclusão de Curso B, que faz parte dos cursos de Matemática da UFSCar. Esta é a monografia principal, onde se encontra incluso o Trabalho de Conclusão de Curso A.

Capítulo 1

Teoremas básicos de Teoria dos Números

1.1 Introdução

Começamos apresentando os teoremas básicos de Teoria dos Números necessários para desenvolvermos nossos estudos de criptografia.

1.2 Propriedade da Boa Ordem

Indicaremos por $\mathbb{N} = \{0, 1, 2, \dots\}$ o conjunto dos números naturais e por $\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2, \dots\}$ o conjunto dos números inteiros.

Seja S um subconjunto de $\mathbb{N}$. Dizemos que um número natural a é um menor elemento de S se possui as seguintes propriedades:

i) $a \in S$

ii) $\forall n \in S, a \leqslant n$

Axioma da Boa Ordem em $\mathbb{N}$, ou Princípio do Menor Número Natural. Todo subconjunto não vazio do conjunto $\mathbb{N}$ possui um menor elemento.

O Axioma da Boa Ordem em $\mathbb{N}$ afirma que se A é um subconjunto do conjunto $\mathbb{N}$ e $A \neq \emptyset$ então existe um elemento n_0 em A satisfazendo $n_0 \leqslant a$ para todo $a \in A$.

1.3 Indução Matemática

Teorema 1.1. ***(Primeiro Princípio de Indução Finita)*** *Seja n_0 um número inteiro e suponhamos que a cada inteiro n, $n \geqslant n_0$, está associada*

uma afirmação $A(n)$. Suponhamos que as condições 1 e 2 abaixo sejam verificadas:

(1) A afirmação $A(n)$ é verdadeira quando $n = n_0$;

(2) Para todo $k \geqslant n_0$, quando $A(k)$ é verdadeira, $A(k+1)$ é também verdadeira (ou seja, $A(k)$ verdadeira $\Rightarrow A(k+1)$ verdadeira).

Então a afirmação $A(n)$ é verdadeira para todo $n \geqslant n_0$.

Teorema 1.2. *(Segundo Princípio de Indução Finita) Seja n_0 um número inteiro e suponhamos que a cada inteiro n, $n \geqslant n_0$, está associada uma afirmação $A(n)$. Suponhamos que as condições 1 e 2 abaixo sejam verificadas:*

(1) A afirmação $A(n)$ é verdadeira para $n = n_0$;

(2) Para todo inteiro $k \geqslant n_0$, se $A(n)$ é verdadeira para todo inteiro n tal que $n_0 \leqslant n \leqslant k$, então $A(k+1)$ é também verdadeira (ou seja $A(n)$ verdadeira para $n = n_0, n_0 + 1, ..., k \Rightarrow A(k+1)$ verdadeira)

Então a afirmação $A(n)$ é verdadeira para todo $n \geqslant n_0$.

1.4 Divisibilidade

Definição 1.3. Um número natural a se diz *múltiplo* de um número natural b se existir um número natural q tal que $a = bq$. Nesse caso, e se $b \neq 0$, dizemos também que b *divide* a ou que b é *divisor* ou *fator* de a.

Proposição 1.4. *Dados números naturais a, b e c, se b e c são múltiplos de a, então, quaisquer que sejam os números naturais x e y, temos que $xb \pm yc$ é múltiplo de a.*

Demonstração. Existem números naturais q e t tais que $b = qa$ e $c = ta$. Portanto $xb \pm yc = xqa \pm yta = (xq \pm yt)a$, e vemos que $xb \pm yc$ é múltiplo de a. □

Teorema 1.5. ***(Algoritmo da Divisão em $\mathbb{Z}$)*** *Sejam a e b inteiros com $b \neq 0$. Existem inteiros q e r tais que $a = bq + r$ e $0 \leq r < |b|$. Além disso, os valores de q e r satisfazendo as relações acima são únicos.*

O algoritmo euclidiano apresentado a seguir, tem como objetivo calcular o máximo divisor comum entre dois números inteiros. Lembrando que:

Definição 1.6. Dados dois inteiros a e b, chama-se *máximo divisor comum* de a e b ao inteiro d satisfazendo:

(1) $d = 0$ se $a = b = 0$

(2) Se $a \neq 0$ ou $b \neq 0$, d é caracterizado pelas seguintes propriedades:

(i) d divide a e d divide b

(ii) $\forall x \in \mathbb{Z}$, se x divide a e x divide b, então $x \leqslant d$

Definição 1.7. Os números inteiros a e b são chamados *primos entre si* se $\mathrm{mdc}(a, b) = 1$.

Precisaremos destes resultados auxiliares:

Lema 1.8. *Sejam a e b inteiros, com $b \neq 0$, e seja r o resto da divisão euclidiana de a por b. Então* $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, r)$.

Para enunciar o Teorema do Algoritmo Euclidiano para o cálculo do mdc, vamos estabelecer algumas notações. Sejam a e b inteiros. Para calcular $\mathrm{mdc}(a, b)$ podemos supor sem perda de generalidade que $a \geq b > 0$, tendo em vista que $\mathrm{mdc}(a, b) = \mathrm{mdc}(|a|, |b|)$ e $\mathrm{mdc}(0, 0) = 0$. Dividindo a por b sucessivamente, obtemos as seguintes relações:

$$\begin{array}{rcll} a & = & bq_1 + r_1 & 0 \leq r_1 < b \\ b & = & r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & & & \\ r_{n-2} & = & r_{n-1} q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_n q_{n+1} + r_{n+1} & 0 = r_{n+1} \end{array} \tag{1.1}$$

Observe que ao fazer as divisões sucessivas obtemos uma sequência de restos $b > r_1 > r_2 > \cdots \geq 0$. Portanto existe n tal que $r_{n+1} = 0$.

Teorema 1.9. ***(Algoritmo Euclidiano para o cálculo do mdc)*** *Sejam a e b inteiros tais que $a \geq b > 0$. Sejam $r_1, r_2, \ldots, r_n, r_{n+1}$ a sequência de restos da divisão euclidiana de a por b, obtidas em 1.1. Então $r_n = mdc(a, b)$.*

Demonstração. Em virtude do Lema 1.8 temos

$$\mathrm{mdc}(a, b) = \mathrm{mdc}(b, r_1) = \mathrm{mdc}(r_1, r_2) = \cdots = \mathrm{mdc}(r_n, 0) = r_n$$

□

Teorema 1.10. ***Algoritmo Euclidiano Estendido*** *Sejam a e b inteiros positivos e seja d o máximo divisor comum entre a e b. Existem inteiros α e β tais que*

$$\alpha a + \beta b = d$$

Os valores de α e β não são únicos. Na verdade existe uma infinidade de pares inteiros α e β que satisfazem esta equação.

Corolário 1.11. *Se a e b são números inteiros primos entre si, existem inteiros m e n tais que*

$$am + bn = 1$$

1.5 Primos

Definição 1.12. Denominamos *primo* a todo número natural > 1 que não tem divisor positivo diferente de 1 e dele mesmo. Chamamos de *composto* a todo número natural que tem divisor positivo diferente de 1 e dele mesmo.

Teorema 1.13. *Todo número natural* ≥ 2 *é primo ou se escreve como produto de primos.*

Demonstração. Para essa demonstração, usaremos o Segundo Princípio de Indução sobre $m \geq 2$. Se $m = 2$, então m é primo. Seja $k \geq 2$ e suponhamos que todo inteiro m, com $2 \leqslant m \leqslant k$, é primo ou se decompõe como produto de fatores primos. Se $k + 1$ for primo, terminamos. Suponhamos que não seja. Vamos demonstrar que $k+1$ se escreve como produto de primos. Como $k + 1$ não é primo, é composto. Então existem inteiros positivos a e b com $1 < a < k + 1$ e $1 < b < k + 1$ tais que $k + 1 = ab$. Agora, como $2 \leq a \leq k$ e $2 \leq b \leq k$, pela hipótese de indução, cada um dos inteiros a e b é primo ou se decompõe como produto de primos. Logo $k + 1$ se decompõe como produto de fatores primos. Assim sendo, todo inteiro $m \geq 2$ é primo ou se escreve como produto de primos. □

Teorema 1.14. *Sejam* a*,* b *e* c *números inteiros tais que* $\text{mdc}(a, b) = 1$*. (1) Se* $b \neq 0$ *e se* b *divide* ac *então* b *divide* c*. (2) Se* $a \neq 0$ *e* $b \neq 0$ *dividem* c *então* ab *divide* c*.*

Demonstração. Parte (1)

Como $mdc(a, b) = 1$ o Algoritmo Euclidiano Estendido garante que existem inteiros α e β tais que

$$\alpha a + \beta b = 1$$

Multiplicando esta equação por c temos

$$\alpha ac + \beta cb = c$$

É claro que b divide βcb. Mas também podemos dizer que b divide αac, pois pela hipótese da afirmação (1) temos que b divide ac. Assim, b divide $\alpha ac + \beta cb$, logo b divide c.

Demonstração. Parte (2)

Se a divide c, podemos escrever $c = at$, para algum inteiro t. Mas b também divide c. Como a e b são primos entre si, segue da afirmação (1) que b tem que dividir t. Assim teremos que $t = bk$, para algum inteiro k. Portanto

$$c = at = a(bk) = (ab)k$$

que é divisível por ab. Assim provamos a afirmação (2). □

Corolário 1.15. *Se p é primo e se p é divisor de ab então p é divisor de a ou de b, quaisquer que sejam os números naturais a e b.*

Demonstração. Se p dividir a, não há mais nada a fazer. Digamos então que p não divide a. Como p é primo, então p e a são primos entre si. Isto ocorre porque qualquer divisor comum a p e a divide p, mas os únicos divisores positivos de p são 1 e p. Portanto, se p não divide a, então $\text{mdc}(a, p) = 1$. Aplicando o Teorema 1.14, temos p divide b. □

Corolário 1.16. *Sejam $p, a_1, \ldots, a_n$ números inteiros com $n \geq 2$ e p primo. Se p divide $a_1 a_2 \ldots a_n$ então p divide a_i para algum índice i, $i \in \{1, 2, \ldots, n\}$.*

Teorema 1.17 (O Teorema Fundamental da Aritmética)**.** *Todo número natural ≥ 2 é primo ou pode ser decomposto como um produto de números primos, e essa decomposição é única a menos da ordem dos fatores.*

Demonstração. A existência da decomposição é garantida pelo Teorema 1.13. Vamos demonstrar a unicidade usando o Segundo Princípio de Indução Finita.

Se $m = 2$, o resultado é claro. Seja $k \geq 2$ e suponhamos que a afirmação seja verdadeira para todo inteiro m, com $2 \leq m \leq k$. Mostraremos que o mesmo se dá com relação ao inteiro $k + 1$.

Suponhamos que $k+1 = p_1 \ldots p_n = q_1 \ldots q_s$, com $n, s \geq 1$, $p_1 \leq \cdots \leq p_n$ e $q_1 \leq \cdots \leq q_s$. Se $n = 1$, então $k+1 = p_1$ é primo e, neste caso é claro que a decomposição é única. O mesmo ocorre se $s = 1$. Suponhamos então $n \geq 2$ e $s \geq 2$. Como $p_1 \ldots p_{n-1} p_n = q_{1\ldots} q_{s-1} q_s$, temos que p_n divide $q_1 \ldots q_s$ e q_s divide $p_1 \ldots p_n$. Pelo Corolário 1.16, temos que p_n divide q_i e q_s divide p_j para certos índices i e j, com $1 \leq i \leq s$ e $1 \leq j \leq n$. Logo, $p_n \leq q_i \leq q_s \leq p_j \leq p_n$, o que então acarreta $p_n = q_s$. Logo, $p_1 \ldots p_{n-1} p_n = q_1 \ldots q_{s-1} q_s$ e $p_n = q_s$, e então $p_1 \ldots p_{n-1} = q_1 \ldots q_{s-1}$. Agora, $2 \leq p_1 \ldots p_{n-1} = q_1 \ldots q_{s-1} < k + 1$, ou seja, $2 \leq p_1 \ldots p_{n-1} = q_1 \ldots q_{s-1} \leq k$. Aplicando a hipótese de indução, temos então que $n - 1 = s - 1$ e além disso, $p_1 = q_1$, ..., $p_{n-1} = q_{n-1}$. Logo, $n = s$ e $p_1 = q_1$, ..., $p_{n-1} = q_{n-1}$, $p_n = q_n$. Assim sendo, a unicidade dos fatores primos de m é válida para todo $m \geq 2$. □

1.6 Como obter números primos

O método mais simples para obter números primos é o conhecido Crivo de Eratóstenes. Este entretanto é um método lento e inviável para obter primos grandes, mesmo quando tratado computacionalmente. Outro método óbvio seria encontrar uma fórmula, mas todas as fórmulas já encontradas são intratáveis computacionalmente. Para ilustrar vamos considerar as fórmulas polinomiais e exponenciais.

Um dos tipos mais simples de fórmula para primos que podemos tentar é a fórmula polinomial. Com isto, nos referimos a um polinômio

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

cujos coeficientes $a_{n-1}, a_n, ..., a_1, a_0$ são números inteiros e que deveria satisfazer a condição de que $f(m)$ é primo para todo inteiro positivo m.

Exemplo 1.18. Seja $f(x) = x^2 + 1$. Para cada valor de x, teremos os respectivos valores para $f(x)$:

$x = 1, \quad f(x) = 2$
$x = 2, \quad f(x) = 5$
$x = 3, \quad f(x) = 10$
$x = 4, \quad f(x) = 17$
$x = 5, \quad f(x) = 26$
$x = 6, \quad f(x) = 37$
$x = 7, \quad f(x) = 50$
$x = 8, \quad f(x) = 65$

Observe que se x for ímpar, então $f(x)$ é par. Assim, a não ser quando $x = 1$, o valor de $f(x)$ é sempre composto(e múltiplo de 2) quando x é ímpar. Portanto quando $x > 1$, temos que $f(x)$ só pode vir a ser primo se x for par. Também não adianta considerar apenas valores pares para x, pois $f(8) = 65$ que é composto. Vemos então que este polinômio não nos dá uma fórmula para primos. Esse comportamento não é específico para esse polinômio, mas é geral.

Teorema 1.19. *Dado um polinômio $f(x)$ com coeficientes inteiros, existe uma infinidade de inteiros positivos m tais que $f(m)$ é composto.*

Demonstração. (Parcial) Vamos provar para o caso em que $f(x)$ tem grau 2. Seja $f(x) = ax^2 + bx + c$, com a, b e c inteiros, e $a > 0$. Se $f(x)$ for composto para todo inteiro positivo x, então acabamos. Caso contrário, existe um inteiro positivo m tal que $f(m) = p$, com p primo positivo. Sendo h inteiro positivo, temos

$$f(m + hp) = a(m + hp)^2 + b(m + hp) + c =$$

$$= a(m^2 + 2hpm + h^2p^2) + bm + bhp + c =$$

$$= am^2 + 2hpam + h^2p^2a + bm + bhp + c =$$

$$= p(2ham + h^2pa + bh) + (am^2 + bm + c) =$$

$$= p(2ham + h^2pa + bh) + f(m) =$$

$$= p(2ham + h^2pa + bh) + p =$$
$$= p(1 + 2ham + h^2pa + bh)$$

Para que $f(m + hp)$ seja composto devemos ter

$$1 + 2amh + aph^2 + bh > 1 \Leftrightarrow 2amh + aph^2 + bh > 0 \Leftrightarrow h > \frac{-b - 2am}{ap}$$

Mostramos assim, que se $f(x) = ax^2 + bx + c$ é um polinômio com coeficientes inteiros, $a > 0$ e $f(m) = p$ primo, então $f(m + hp)$ é composto sempre que

$$h > \frac{-b - 2am}{ap}$$

Ou seja, existem infinitos valores inteiros positivos para x de modo que $f(x)$ seja composto. □

Vemos portanto que os polinômios não fornecem fórmulas para primos.

Já nas fórmulas exponenciais, destacam-se duas: números de Mersenne e números de Fermat. As fórmulas são, respectivamente:

$$M(n) = 2^n - 1$$

e

$$F(n) = 2^{2^n} + 1$$

onde n é um inteiro não negativo.

Segundo Mersenne, os números da forma $M(n) = 2^n - 1$ seriam primos quando $n = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257 e composto para os outros 44 valores primos de n menores que 257. Depois se constatou que $M(61)$, $M(89)$ e $M(107)$ são primos, e $M(67)$ e $M(257)$ são compostos.

Observe que se n for composto, então $M(n)$ também é composto, pois se $n = rs$ com $1 < r < n$, então

$$M(n) = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + ... + 2^r + 1)$$

Portanto, se r divide n então $M(r)$ divide $M(n)$. E temos também que se n for primo isto não significa que $M(n)$ tem que ser primo. Por exemplo $M(67) = 147573952589676412927 = (761838257287)(193707721)$

Já Fermat, considerou os números da forma $F(n) = 2^{2^n} + 1$ para os valores inteiros de n entre 0 e 6. Os valores são: 3, 5, 17, 257, 65537, 4294967297 e 18446744073709551617. Em seguida, conjecturou que todos os números desta forma são primos. Depois se constatou que $F(5)$ e $F(6)$ não são primos. Não se conhece uma maneira de determinar quais desses números são primos ou

compostos. Poranto, essas fórmulas não nos fornecem uma boa maneira de obter primos.

Outra forma de procurar números primos é considerar progressões aritméticas. Vamos provar que existem infinitos primos da forma $4n + 3$.

Um primo ímpar ou é da forma $4n + 1$ ou da forma $4n + 3$. Isto é, tem resto 1 ou resto 3 na divisão por 4. Os lemas a seguir nos levarão à conclusão de que existem infinitos números primos da forma $4n + 3$.

Lema 1.20. *O produto de números inteiros da forma* $4n + 1$ *é da forma* $4n + 1$.

Demonstração. Sejam $4n + 1$ e $4n' + 1$ números inteiros. Então

$$(4n + 1)(4n' + 1) = 4n4n' + 4n + 4n' + 1 = 4(4nn' + n + n') + 1$$

Segue que o produto de uma quantidade finita de números inteiros da forma $4n + 1$ é da forma $4n + 1$. □

Lema 1.21. *Todo número primo diferente de 2 é da forma* $4n+1$ *ou* $4n+3$.

Demonstração. Seja $p \in \mathbb{Z}$, com $p > 2$. Então, dividindo p por 4, temos as seguintes possibilidades:

$p = 4q + 0$ (neste caso p não pode ser primo, pois $p = 4q$ é composto)
$p = 4q + 1$ (p pode ser primo, por exemplo para $q = 1 \Rightarrow p = 5$)
$p = 4q + 2$ ($p = 2(2q + 1)$ é composto, ou seja, não pode ser primo, a não ser para $q = 0$, mas assim $p = 2$, o que não pode ocorrer por hipótese)
$p = 4q + 3$ (p pode ser primo, por exemplo para $q = 1 \Rightarrow p = 7$)

Logo, um número primo qualquer diferente de 2 é da forma $4n + 1$ ou $4n + 3$. □

Observação O produto de números da forma $4n+3$ pode não ser da mesma forma. Por exemplo, $3 \cdot 3 = 9 = 4 \cdot 2 + 1$.

Lema 1.22. *Suponha que* $3 < p_1 < \cdots < p_k$ *sejam primos da forma* $4n + 3$. *Então* $4p_1 \ldots p_k + 3$ *é divisível por um primo da forma* $4n+3$ *que não pertence ao conjunto* $\{3, p_1, \ldots, p_k\}$.

Demonstração. Seja $a = 4p_1 \ldots p_k + 3$. Existe um p primo que divide a. Como p é ímpar, ele é da forma $4n + 1$ ou $4n + 3$. Se todo p que divide a fosse da forma $4n + 1$, então a seria da forma $4n + 1$, o que não é. Posso escolher pelo menos um p da forma $4n + 3$.

Suponha que $p \in \{3, p_1, ..., p_k\}$. Temos então dois casos:

(1) $p = 3$
(2) p é um dos outros p_j

Caso (1): 3 divide $4p_1 \dots p_k + 3 \Rightarrow 3 \mid 4p_1 \dots p_k$. Então, 3 divide p_i, para algum i. Mas p_i é primo, e a única forma de 3 dividir um número primo é se esse primo for 3, mas por hipótese, $p_i > 3$, logo p não pode ser 3.
Caso(2): p_j divide $4p_1 \dots p_k + 3$. Então, p_j divide 3. Mas p_j é maior que 3, o que é uma contradição.

Então, p não pertence ao conjunto $\{3, p_1, ..., p_k\}$. □

Teorema 1.23. *Existem infinitos números primos da forma* $4n + 3$.

Demonstração. Suponha que exista uma quantidade finita. Sejam eles $3 < p_1 < \cdots < p_k$. Seja $a = 4p_1 \dots p_k + 3$. Mostramos que existe um divisor primo de a da forma $4n + 3$ que não pertence ao conjunto $\{3, p_1, ..., p_k\}$. Isso é uma contradição. Logo, existem infinitos números primos da forma $4n + 3$. □

Entretanto, essas sequências também não são uma boa maneira de obter números primos, pois não sabemos quais termos de uma dada sequência são primos ou não.

Existem muitas fórmulas para números primos, mas são fórmulas que não resultam em um algoritmo prático para se obter primos grandes. Por exemplo, em [Ribenboim], pág.121, vemos que existe um número real Θ tal que

$$f(n) = [\Theta^{3^n}]$$

é primo para todo inteiro $n \geqslant 1$ (aqui $[x]$ indica a parte inteira do número real x). Mas não se tem um valor exato para $\Theta \approx 1,3064...$, e o valor de $f(n)$ cresce muito rapidamente, o que dificulta seu uso.

Capítulo 2

Fatoração

2.1 Introdução

Apresentamos neste capítulo o método de fatoração de Fermat com alguns exemplos.

2.2 O método de Fermat

Nesta seção vamos descrever um método para achar um fator de determinado número ou saber se ele primo. Para começar supomos que n é ímpar, pois se fosse par, então 2 seria um de seus fatores. A idéia do algoritmo é tentar achar números inteiros positivos x e y tais que $n = x^2 - y^2$. Supondo que encontramos estes números, temos que

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

Logo $x - y$ e $x + y$ são fatores de n.
Vamos utilizar em nossos cálculos, $[r]$ que chamamos de parte inteira de um número real r. Por exemplo, $[\pi]$=3. É claro que se r é inteiro, então $[r]$=r.

Teorema 2.1. *(Algoritmo de Fatoração de Fermat) Seja $n \geq 3$ um inteiro ímpar. Execute os seguintes passos para $i = 0, 1, 2, 3, \ldots$*

(i) Calcule $x = [\sqrt{n}] + i$ e $y = \sqrt{x^2 - n}$ enquanto y não é inteiro e $x < \frac{n+1}{2}$.

Se o algoritmo pára por ter encontrado algum valor y inteiro, então n é composto. Se o algoritmo pára em $x = \frac{n+1}{2}$ (e nenhum y é inteiro) então n é primo.

Demonstração. Temos $0 < (n-1)^2 \Rightarrow 0 < n^2 - 2n + 1$

$$\Rightarrow 4n < n^2 + 2n + 1 \Rightarrow 4n < (n+1)^2$$

$$\Rightarrow n < \frac{(n+1)^2}{4}$$

Como $0 < [\sqrt{n}] \leq \sqrt{n}$ vem

$$[\sqrt{n}]^2 \leq n < \frac{(n+1)^2}{4}$$

$$\Rightarrow [\sqrt{n}] < \frac{n+1}{2}$$

Como o primeiro valor de x é $[\sqrt{n}]$, então o passo (0) do algoritmo é executado, com $x = [\sqrt{n}]$. Se a resposta do passo (0) for y inteiro o algoritmo pára. Como $[\sqrt{n}]^2 \leq n$ vem $[\sqrt{n}]^2 - n \leq 0$ e $y = \sqrt{[\sqrt{n}]^2 - n}$ é inteiro se e somente se $y = 0$. Então $n = x^2$. Como $n \geq 3$ vem $x > 1$, e n é composto. Se a resposta do passo (0) for y não inteiro, o algoritmo passa para (1), e assim sucessivamente, continuando no máximo até $i = \frac{n-1}{2} - [\sqrt{n}]$.

Se em algum passo (i) y for inteiro e $x < \frac{n+1}{2}$ temos $2x < n + 1 \Rightarrow$

$$\Rightarrow -2x > -n - 1 \Rightarrow -2x + 1 > -n \Rightarrow$$

$$\Rightarrow x^2 - 2x + 1 > x^2 - n \Rightarrow (x-1)^2 > x^2 - n$$

Como $x \geq [\sqrt{n}] \geq 1$ vem $x - 1 > \sqrt{x^2 - n} = y \Rightarrow x - y > 1$. Com maior razão vem $x + y > 1$. Ainda de $y = \sqrt{x^2 - n}$ vem $n = x^2 - y^2 = (x-y)(x+y)$, vem $x - y$ e $x + y$ inteiros > 1. Portanto n é composto.

Falta provar que se n é composto então existem inteiros x e y tais que

$$[\sqrt{n}] \leq x < \frac{n+1}{2} \qquad \text{e} \qquad y = \sqrt{x^2 - n}$$

(isto implica que se o algoritmo pára quando $x = \frac{n+1}{2}$ então n é primo).

Suponhamos então que $n = ab$, sendo a e b, sendo a e b inteiros tais que $1 < b \leq a < n$. Se $b = a$ temos $n = a^2$, e basta tomar $x = a$ e $y = 0$. Neste caso $[\sqrt{n}] = a = x$, e como já vimos que $[\sqrt{n}] < \frac{n+1}{2}$, vem $x < \frac{n+1}{2}$.

Suponhamos $b < a$. Como n é ímpar e $n = ab$, os inteiros a e b também são ímpares. Definimos os inteiros

$$x = \frac{a+b}{2} \qquad \text{e} \qquad y = \frac{a-b}{2}$$

Notemos que

$$x^2 - n = \frac{(a+b)^2}{4} - ab = \frac{a^2 + 2ab + b^2 - 4ab}{4} = \frac{(a-b)^2}{4} = y^2$$

Logo $y = \sqrt{x^2 - n}$. Ainda $x^2 - n \geq 0 \Rightarrow n \leq x^2 \Rightarrow$

$$\Rightarrow \sqrt{n} \leq x \Rightarrow [\sqrt{n}] \leq x$$

Por outro lado $1 < a$ e $b - 1 > 0$ implicam

$$b - 1 < a(b - 1) \Rightarrow b - 1 < ab - a \Rightarrow$$

$$\Rightarrow b + a < ab + 1 \Rightarrow a + b < n + 1 \Rightarrow$$

$$\Rightarrow \frac{a+b}{2} < \frac{n+1}{2} \Rightarrow x < \frac{n+1}{2}$$

Terminamos. □

Exemplo 2.2. Usando o Algoritmo de Fermat, diga se n é primo ou é composto, mostrando pelo menos um de seus fatores nos seguintes casos: (a) $n = 43$ (b) $n = 116617$

(a) Vamos calcular primeiramente a parte interia da raiz de n

$$x = [\sqrt{43}] = 6$$

Assim a variável x é inicializada com valor 6. Mas $x^2 = 6^2 = 36 \neq 43$ Passamos então a incrementar x de uma unidade até que $y = \sqrt{x^2 - n}$ seja inteiro ou $x = \frac{n+1}{2}$, que neste caso vale 22.

Temos então a seguinte tabela:

x	$\sqrt{x^2 - n}$
7	2,44
8	4,58
9	6,16
10	7,54
11	8,83
12	10,04
13	11,22
14	12,36
15	13,49
16	14,59
17	15,68
18	16,76
19	17,83
20	18,89
21	19,94

Chegamos ao valor de $x = 22$ antes de encontramos um valor inteiro para y. Portanto 43 é um número primo.

(b) Temos agora $n = 116617$. A variável x inicia com a raiz inteira de n, ou seja,

$$x = [\sqrt{116617}] = 341$$

e $x^2 = 341^2 = 116281 \neq 116617$. Passamos então a incrementar x em uma unidade até obtermos $y = \sqrt{x^2 - n}$ inteiro ou a variável x chegar a $\frac{n+1}{2}$.

x	$\sqrt{x^2 - n}$
342	18,62
343	32,12
344	41,46
345	49,07
346	55,66
347	61,57
348	66,98
349	72

Assim, obtemos y inteiro para $x = 349$. Portanto 116617 é composto. Como $x = 349$ e $y = 72$ temos os fatores $x + y = 421$ e $x - y = 277$.

O método de fatoração de Fermat é um bom método para fatorar um inteiro composto ou verificar se ele é primo. Mas para números grandes o custo computacional do método é excessivo.

Capítulo 3

Aritmética Modular

3.1 Introdução

A aritmética dos fenômenos cíclicos é conhecida como *aritmética modular*. Este será o tema principal deste Capítulo. Veremos como somar, multiplicar e dividir números nessa aritmética. Apresentaremos depois o Pequeno Teorema de Fermat e os Teoremas de Euler e Wilson.

3.2 Inteiros módulo n

Antes de falarmos diretamente sobre os inteiros módulo n, vale relembrar o assunto sobre relações de equivalência, pois será muito útil.

Seja X um conjunto, que pode ser finito ou infinito. Definimos uma relação em X dizendo como comparar dois elementos deste conjunto. Para definir a relação, precisamos dizer quem é o conjunto cujos elementos estão sendo comparados. Por exemplo, no conjunto dos números inteiros temos duas relações naturais, a de igualdade e a de desigualdade.

As relações de equivalências são de um tipo muito especial. Voltando à situação geral, digamos que X é um conjunto onde está definida uma relação, que denotaremos por R. Esta é uma *relação de equivalência* se, quaisquer que sejam os elementos $x, y, z \in X$, as seguintes propriedades são satisfeitas:

(1) R é uma relação reflexiva se $\forall x \in X$ tem se xRx

(2) R é uma relação simétrica se, $\forall x, y \in X$, vale a implicação $xRy \Rightarrow yRx$

(3) R é uma relação transitiva se, para quaisquer elementos x, y e $z \in X$, vale a implicação xRy e $yRz \Rightarrow xRz$.

As relações de equivalência são usadas para classificar os elementos de um conjunto em subconjuntos com propriedades semelhantes. As subdivisões de um conjunto produzidas por uma relação de equivalência são conhecidas como

classes de equivalência. Seja X um conjunto e R uma relação de equivalência definida em X. Se $x \in X$ então a *classe de equivalência* de x é o conjunto dos elementos de X que são equivalentes a x por R. Denotamos por $\overline{x}$ a classe de equivalência de x.

Definição 3.1. Para cada elemento $x \in X$, a classe de equivalência de x, módulo R (ou classe de equivalência de x, relativamente à relação R) é o subconjunto

$$\overline{x} = \{y \in X : yRx\}$$

Há uma propriedade das classes de equivalência muito importante, que é a seguinte: *qualquer elemento de uma classe de equivalência é um representante de toda a classe*, ou seja, se conhecemos um elemento da classe podemos reconstruir a classe toda.

Para o conjunto X, o príncipio acima nos diz que se y é um elemento da classe de x então as classes de x e y são iguais. Em símbolos,

$$\text{se } x \in X \text{ e } y \in \overline{x} \text{ então } \overline{x} = \overline{y}$$

Para demonstrar isso usamos as propriedades das relações de equivalência. Se $y \in \overline{x}$, então, por definição, yRx; e pela propriedade simétrica, xRy. Seja então $z \in \overline{x}$. Temos zRx. Logo, como temos zRx e xRy, pela propriedade transitiva zRy. Portanto $z \in \overline{y}$. Mostramos assim que $\overline{x} \subseteq \overline{y}$. Agora seja $z \in \overline{y}$, então pela definição zRy. Logo, pela propriedade transitiva temos zRx. Portanto $z \in \overline{x}$. Mostramos assim que $\overline{y} \subseteq \overline{x}$, logo, $\overline{x} = \overline{y}$.

Consideremos agora as seguintes propriedades do conjunto X com a relação R:

(1) X é a união de todas as classes de equivalência.
(2) Duas classes de equivalência distintas não podem ter um elemento em comum.

A primeira propriedade é uma consequência do fato de que cada elemento pertence à sua própria classe de equivalência. A segunda propriedade segue do principio enunciado acima.

O conjunto das classes de equivalência de R em X tem um nome especial: conjunto quociente de X por R.

Definição 3.2. Seja X um conjunto não vazio e seja R uma relação de equivalência em X. Chama-se *conjunto quociente* de X pela relação R o conjunto, denotado por X/R, das classes de equivalência da relação R

$$X/R = \{\overline{x} | x \in X\}$$

Note que X/R é um conjunto de subconjuntos de X. Um exemplo bastante interessante e pouco visto, é a verdadeira natureza das frações. Considere o conjunto X dos pares (a,b) onde a e b são inteiros e $b \neq 0$. Definimos neste conjunto uma relação de equivalência da seguinte maneira. Os pares (a,b) e (a',b') são equivalentes se $ab' = a'b$, que é uma relação de equivalência no conjunto X. Uma fração é uma classe de equivalência nesse conjunto. A razão pela qual podemos pensar em uma fração olhando apenas para um representante a/b (que é o par (a,b)) é que qualquer representante de uma classe de equivalência nos permite reconstruir toda a classe, que é o princípio enunciado anteriormente. Assim o conjunto dos números racionais o conjunto quociente de X pela relação definida acima. Por exemplo, os números 1/2, 2/4, 3/6 e assim por diante, pertencem à mesma classe de equivalência, já os números 1/3, 2/6, 3/9 pertencem a uma outra classe de equivalência.

Depois de termos visto o que são as relações de equivalência, vamos entrar definitivamente no tema *inteiros módulo n*.

Definição 3.3. Dois inteiros a e b são *congruentes módulo* n se $a - b$ é um múltiplo de n. Se a e b são congruentes módulo n, escrevemos

$$a \equiv b \pmod{n}$$

Exemplo 3.4. Escolhendo $n = 8$ como módulo, então

$$8 \equiv 0 \pmod{8} \text{ e } 18 \equiv 10 \pmod{8}$$

Sendo $n = 5$ como módulo, então

$$5 \equiv 0 \pmod{5} \text{ e } 17 \equiv 27 \pmod{5}$$

Proposição 3.5. *Sendo n um inteiro, a relação de congruência módulo n definida em* $\mathbb{Z}$ *conforme a definição anterior é uma relação de equivalência em* $\mathbb{Z}$.

Demonstração. Seja a um inteiro. Para mostrar que $a \equiv a \pmod{n}$, temos que verificar, por definição, que a diferença $a - a$ é um múltiplo de n. Mas isto é claro, pois 0 é múltiplo de qualquer inteiro. Portanto vale a reflexiva.

Agora, se $a \equiv b \pmod{n}$, então $a - b$ é um múltiplo de n. Mas $b - a = -(a-b)$; logo $b-a$ também é múltiplo de n. Portanto $b \equiv a \pmod{n}$. Assim, provamos a propriedade simétrica.

Quanto à propriedade transitiva, suponhamos que $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$; onde a, b e c são inteiros. A primeira congruência nos diz que $a - b$ é múltiplo de n; a segunda que $b - c$ é múltiplo de n. Somando múltiplos de

n temos de volta múltiplos de n; logo $(a-b)+(b-c)=a-c$ é um múltiplo de n. Portanto $a \equiv c \pmod{n}$, verificando a transitividade.

Mostramos assim as três propriedades e podemos concluir que a congruência módulo n é uma relação de equivalência. □

O conjunto que mais nos interessa é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo n. Este conjunto tem uma notação própria, $\mathbb{Z}_n$. Sabemos por definição que são subconjuntos de $\mathbb{Z}$: as classes de equivalência da congruência módulo n. Seja $a \in \mathbb{Z}$, a classe de a é a formada pelos $b \in \mathbb{Z}$ que satisfazem $b-a$ é múltiplo de n; isto é, $b-a=kn$, para algum $k \in \mathbb{Z}$. Podemos assim descrever a classe de a na forma

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}$$

Proposição 3.6. *Fixando $n \in \mathbb{Z}$, ≥ 2, o conjunto $\mathbb{Z}_n$ dos inteiros módulo n tem precisamente n elementos, a saber*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$$

Demonstração. Como a congruência módulo n é uma relação de equivalência em $\mathbb{Z}$ temos

$$\forall x, y \in \mathbb{Z},\ x \equiv y \Leftrightarrow \overline{x} = \overline{y}$$

Para cada $a \in \mathbb{Z}$, temos que $a \equiv r \pmod{n}$, sendo r o resto da divisão euclidiana de a por n. Como sabemos, $0 \leq r \leq n-1$.

Assim temos $\overline{a} = \overline{r}$, e portanto, $\overline{a}$ coincide com uma das classes de congruência $\overline{0}, \overline{1}, ..., \overline{n-1}$.

Só nos resta então provar que as classes $\overline{0}, \overline{1}, ..., \overline{n-1}$ são distintas entre si. Mas se r_1 e r_2 são inteiros satisfazendo

$$0 \leq r_1 < r_2 \leq (n-1)$$

então temos

$$0 < r_2 - r_1 < n \Rightarrow n \nmid r_2 - r_1$$

Assim, r_2 não é congruente a r_1 módulo n, e deste modo, $\overline{r_2} \neq \overline{r_1}$.

Logo, $\mathbb{Z}_n$ tem precisamente n elementos, sendo eles as classes $\overline{0}, \overline{1}, \cdots, \overline{n-1}$.

□

3.3 Aritmética modular

Definição 3.7. Dado $n \geqslant 2$, as operação de adição e multiplicação em $\mathbb{Z}_n$ são definidas por:
(i) $\overline{a} + \overline{b} = \overline{a+b}$
(ii) $\overline{a}\overline{b} = \overline{ab}$
quaisquer que sejam $\overline{a}$ e $\overline{b} \in \mathbb{Z}_n$

Note que em (i), à esquerda temos a soma de duas classes; à direita temos a classe da soma de dois números inteiros. Observe que em $\mathbb{Z}_8$ por exemplo, $\overline{5} + \overline{4} = \overline{9}$. Mas $9 - 1 = 8$ temos que 9 e 1 estão na mesma classe de equivalência módulo 8, isto é $\overline{9} = \overline{1}$. Somamos as classes $\overline{5}$ e $\overline{4}$ usando o elemento 5 da primeira e o elemento 4 da segunda. Mas $\overline{13} = \overline{5}$ e $\overline{12} = \overline{4}$. Então, se somássemos $\overline{13}$ a $\overline{12}$, qual seria o resultado? Repare que

$$\overline{13} + \overline{12} = \overline{25}$$

Como $25 - 1 = 24$ édivisível por 8, então $\overline{25} = \overline{1}$ e obtivemos o mesmo resultado da soma de $\overline{5}$ e $\overline{4}$.

Perceba que quaisquer que sejam os representantes escolhidos para efetuar a soma de duas classes, o resultado sempre é a mesma classe. E assim como na soma, na multiplicação o resultado também é independente da escolha de representantes para as classes.

Teorema 3.8. *A adição e a multiplicação em $\mathbb{Z}_n$ são bem definidas, ou seja, se a, b, a', b' são inteiros, com $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$, então*

$$\overline{a+b} = \overline{a'+b'} \quad e \quad \overline{ab} = \overline{a'b'}$$

Demonstração. Soma:

Temos $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Queremos verificar que $\overline{a+b} = \overline{a'+b'}$. Mas $\overline{a} = \overline{a'}$ é equivalente a dizer que $a - a'$ é múltiplo de n, e $\overline{b} = \overline{b'}$ é equivalente a dizer que $b - b'$ é múltiplo de n. Logo

$$(a+b) - (a'+b') = (a-a') + (b-b')$$

é múltiplo de n. Portanto $\overline{a+b} = \overline{a'+b'}$, como queríamos.

Multiplicação:

Temos $\overline{a} = \overline{b}$ e $\overline{a'} = \overline{b'}$. Queremos verificar que $\overline{ab} = \overline{a'b'}$. Como $\overline{a} = \overline{a'}$ temos que $a - a'$ é um múltiplo de n; digamos que $a = a' + rn$, para algum inteiro r. Do mesmo modo, $b = b' + sn$, para algum inteiro s. Assim,

$$ab = (a'+rn)(b'+sn) = a'b' + (a's + rb' + srn)n$$

Logo $ab - a'b'$ é um múltiplo de n. Portanto $\overline{ab} = \overline{a'b'}$, que é o que queríamos provar. □

Vamos ver agora as propriedades das operações.

Para a adição:

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$$
$$\overline{a} + \overline{b} = \overline{b} + \overline{a}$$
$$\overline{a} + \overline{0} = \overline{a}$$
$$\overline{a} + \overline{-a} = \overline{0}$$

Para a multiplicação:

$$(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$$
$$\overline{a}\overline{b} = \overline{b}\overline{a}$$
$$\overline{a}\overline{1} = \overline{a}$$

O elemento $\overline{-a}$ é chamado o *simétrico* de $\overline{a}$ para a operação de soma, assim como no caso dos inteiros.

Há ainda uma propriedade que relaciona a operação de adição com a multiplicação, chamada *distributividade*.

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

Note que nos inteiros, a multiplicação de dois números não nulos dará como resultado um outro número não nulo. Mas em $\mathbb{Z}_n$ não funciona dessa maneira. Tomemos $\mathbb{Z}_6$ como exemplo. As classes $\overline{2}$ e $\overline{3}$ são claramente diferentes da classe $\overline{0}$, mas

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$$

O produto de duas classes não nulas pode ser a classe $\overline{0}$.

3.4 Potências

Outra aplicação importante das congruências é no cálculo de restos da divisão de uma potência por um número qualquer.

Exemplo 3.9. Calcular o resto da divisão de 10^{135} por 7.

Note que $10^6 \equiv 1 \pmod 7$. Dividindo 135 por 6 temos $135 = 6 \cdot 22 + 3$. Temos então as seguintes congruências módulo 7:

$$10^{135} \equiv (10^6)^{22}10^3 \equiv 1^{22}10^3 \equiv 6$$

Logo o resto da divisão de 10^{135} por 7 é 6.

Exemplo 3.10. Calcule o resto da divisão de 6^{35} por 16

Não adianta tentar encontrar qual a menor potência de 6 cujo resto por 16 é 1, pois não existe. De fato

$$6^4 \equiv 2^4 3^4 \equiv 0 \cdot 3^4 \equiv 0 \pmod{16}$$

Assim

$$6^{35} \equiv 6^4 6^{31} \equiv 0 \pmod{16}$$

3.5 Equações diofantinas

Antes de mais nada, uma equação é chamada de *diofantina* quando é uma equação em várias incógnitas com coeficientes inteiros. Por exemplo, $3x - 2y = 1$, $x^3 + y^3 = z^3$ e $x^2 - 7y^2 = 3$ são equações diofantinas. Nosso maior interesse será encontrar as soluções inteiras destas equações.

Como as equações têm várias variáveis, pode haver uma infinidade de soluções inteiras.

Tomemos como exemplo a equação $x^2 - 7y^2 = 3$. Neste caso, não existe solução para ela.

Digamos que exista uma solução inteira. Isto significa que existem inteiros x_0 e y_0 tais que $x_0^2 - 7y_0^2 = 3$. Esta última é uma relação entre números inteiros, logo podemos reduzi-la módulo 7. Sabemos que 7 é divisível por 7, e $x_0^2 \equiv x_0^2 - 7y_0^2$, pois $x_0^2 - x_0^2 + 7y_0^2 = 7q$, com q inteiro, então

$$x_0^2 \equiv x_0^2 - 7y_0^2 \equiv 3 \pmod{7}$$

Logo, se a equação dada tem soluções inteiras x_0 e y_0 então $x_0^2 \equiv 3 \pmod 7$. Mas isso não é possível, pois

$$\begin{array}{c} \text{classes módulo 7: } \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6} \\ \text{quadrados módulo 7: } \overline{0}, \overline{1}, \overline{4}, \overline{2}, \overline{2}, \overline{4}, \overline{1} \end{array}$$

Logo, o quadrado de qualquer inteiro é congruente, módulo 7, a 0, 1, 2 ou 4, e nunca a 3. Portanto, $x_0^2 \equiv 3 \pmod 7$ não tem solução. E assim, $x^2 - 7y^2 = 3$ não tem soluções inteiras.

3.6 Divisão modular

Seja a e b números reais. Dizer dividir a por b é o mesmo que multiplicar a por $1/b$. O número real $1/b$ é conhecido como o *inverso* de b. O que caracteriza $1/b$ é a equação $b(1/b) = 1$. Trabalhar com inversos ao invés de falar diretamente em divisão tem uma vantagem conceitual. Note que precisamos assumir que $b \neq 0$ para as afirmações acima. Isto é, um número real só tem inverso se é diferente de zero. Agora, vamos ver o que acontece em $\mathbb{Z}_n$.

Digamos que $\overline{a} \in \mathbb{Z}_n$. Diremos qua a classe $\overline{\alpha} \in \mathbb{Z}_n$ é o *inverso* de $\overline{a}$ se a equação $\overline{a\alpha} = \overline{1}$ é verificada em $\mathbb{Z}_n$. Se $\overline{a} = \overline{0}$, então $\overline{a}$ não tem inverso. Mas fiquemos atentos, pois poderão existir outros elementos sem inverso além da classe $\overline{0}$ em $\mathbb{Z}_n$.

Suponhamos que $\overline{a} \in \mathbb{Z}_n$ tem inverso $\overline{\alpha}$. Então a equação

$$\overline{a\alpha} = \overline{1}$$

corresponde a dizer que $a\alpha - 1$ é divisível por n, ou seja

$$a\alpha + kn = 1$$

para algum inteiro k. Observe que esta última equação implica que $\text{mdc}(a, n) = 1$. Concluimos que se $\overline{a}$ tem inverso em $\mathbb{Z}_n$ então $\text{mdc}(a, n) = 1$. Veja também que a recíproca é verdadeira.

Suponhamos que a é um inteiro e que $\text{mdc}(a, n) = 1$. Logo, podemos aplicar o algoritmo euclidiano estendido aos números a e n para obter inteiros α e β tais que

$$a\alpha + n\beta = 1$$

O que é equivalente a dizer que

$$\overline{a\alpha} = \overline{1}$$

em $\mathbb{Z}_n$. Logo a classe $\overline{\alpha}$ calculada pelo algoritmo euclidiano estendido é o inverso de a em $\mathbb{Z}_n$. Concluimos assim que se $\text{mdc}(a, n) = 1$ então $\overline{a}$ tem inverso em $\mathbb{Z}_n$. Resumindo:

Teorema 3.11. *A classe $\overline{a}$ tem inverso em $\mathbb{Z}_n$ se, e somente se, a e n são primos entre si.*

Demonstração. Suponhamos que $\overline{a}$ é invertível em $\mathbb{Z}_n$. Então existe $\overline{b} \in \mathbb{Z}_n$, com $b \in \mathbb{Z}_n$, satisfazendo $\overline{ab} = \overline{1}$.

Daí, temos $\overline{ab} = \overline{1} \Rightarrow ab \equiv 1 \pmod{n} \Rightarrow m|(ab-1) \Rightarrow ab - 1 = mq$ para algum inteiro $q \Rightarrow ab - mq = 1$. Logo, $\text{mdc}(a, m) = 1$, ou seja, a e m são primos entre si.

Reciprocamente, se a e m são primos entre si, então $\alpha a + \beta m = 1$ para certos inteiros α e β. Daí, $\overline{\alpha a + \beta m} = \overline{1} \Rightarrow \overline{\alpha a} + \overline{\beta m} = \overline{1} \Rightarrow \overline{\alpha}\,\overline{a} + \overline{\beta}\overline{m} = \overline{1}$. Como $\overline{m} = \overline{0}$, chegamos que a $\overline{\alpha}\,\overline{a} = \overline{1}$, e portanto $\overline{a}$ é invertível, já que a multiplicação em $\mathbb{Z}_n$ é comutativa, sendo $\overline{a}^{-1} = \overline{\alpha}$. □

Exemplo 3.12. Quais os elementos de $\mathbb{Z}_{15}$ que têm inversos?

Antes de mais nada, precisamos saber quais são os elementos de $\mathbb{Z}_{15}$.

$$\mathbb{Z}_{15} = \{\overline{0}, \overline{1}, ..., \overline{14}\}$$

Um elemento $\overline{a}$ de $\mathbb{Z}_{15}$ para ser invertível tem que satisfazer $\text{mdc}(a, 15) = 1$. Portanto, os elementos invertíveis de $\mathbb{Z}_{15}$ são: $\overline{1},\ \overline{2},\ \overline{4},\ \overline{7},\ \overline{8},\ \overline{11},\ \overline{13},\ \overline{14}$.

O conjunto dos elementos de $\mathbb{Z}_n$ que têm inverso é denotado por $U(n)$.

$$U(n) = \{\overline{a} \in \mathbb{Z}_n | \text{ mdc}(a, n) = 1\}$$

Quando p é primo, temos que $\text{mdc}(a, p) = 1$, significa que p não divide a. Mas se p divide a então $\overline{a} = \overline{0}$. Portanto, quando p é primo, todas as classes diferentes de $\overline{0}$ têm inverso. Assim

$$U(p) = \mathbb{Z}_p - \{\overline{0}\}$$

Uma propriedade importante do conjunto $U(n)$ é que o produto de dois elementos de $U(n)$ é um elemento de $U(n)$, ou seja, se $\overline{a}$ e $\overline{b}$ em $\mathbb{Z}_n$ têm inverso, então $\overline{a}\overline{b}$ também tem inverso em $\mathbb{Z}_n$. Vejamos o porque.

Digamos que $\overline{a}$ tem inverso $\overline{\alpha}$ e $\overline{b}$ tem inverso $\overline{\beta}$ em $\mathbb{Z}_n$. Então,

$$(\overline{a}\overline{b})(\overline{\alpha}\overline{\beta}) = (\overline{a}\,\overline{\alpha})(\overline{b}\,\overline{\beta}) = \overline{1} \cdot \overline{1} = \overline{1}$$

E o inverso de $\overline{a}\overline{b}$ será $\overline{\alpha}\overline{\beta}$.

Nosso maior interesse será determinar o número de elementos de $U(n)$ em função de n, e descobrir quando $U(n)$ tem uma *raiz primitiva*. Uma classe de $\overline{a}$ de $U(n)$ é uma *raiz primitiva* se todo elemento de $U(n)$ é igual a uma potência de $\overline{a}$. Por exemplo $\overline{3}$ é uma raiz primitiva de $U(7)$. De fato, em $\mathbb{Z}_7$ temos que

$$\begin{array}{lcccl} \overline{3}^1 & = & \overline{3} & & \\ \overline{3}^2 & = & \overline{2} & & \\ \overline{3}^3 & = & \overline{3}\cdot\overline{2} & = & \overline{6} \\ \overline{3}^4 & = & \overline{3}\cdot\overline{6} & = & \overline{4} \\ \overline{3}^5 & = & \overline{3}\cdot\overline{4} & = & \overline{5} \\ \overline{3}^6 & = & \overline{3}\cdot\overline{5} & = & \overline{1} \end{array}$$

Voltando à divisão, se queremos dividir $\overline{a}$ por $\overline{b}$ precisamos saber se b está ou não em $U(n)$. Se não estiver, a divisão não é possível. Se estiver, calculamos o inverso de $\overline{b}$ em $\mathbb{Z}_n$ (digamos que é $\overline{\beta}$) e dividimos $\overline{a}$ por $\overline{b}$ calculando o produto $\overline{a}\overline{\beta}$.

Exemplo 3.13. Calcular a divisão de $\overline{a}$ por $\overline{3}$ em $\mathbb{Z}_8$. Como $\text{mdc}(3,8) = 1$, então $\overline{3}$ tem inverso em $\mathbb{Z}_8$. O fato dos números serem pequenos, facilita achar o inverso por tentativa. O inverso de $\overline{3}$ em $\mathbb{Z}_8$ ó próprio $\overline{3}$. Assim o resultado da divisão de $\overline{2}$ por $\overline{3}$ em $\mathbb{Z}_8$ é $\overline{6}$.

3.7 Congruência linear

Uma *congruência linear* é uma equação do tipo

$$ax \equiv b \pmod{n}$$

onde a, $b \in \mathbb{Z}$. Para resolvê-la, precisamos dividir b por a para deixar o x livre do lado esquerdo da equação, mas só será possível se $\text{mdc}(n,a) = 1$. Digamos que esta última hipótese é satisfeita. Então existe $\alpha \in \mathbb{Z}$ tal que $\alpha a \equiv 1 \pmod{n}$. Multiplicando a equação anterior por α, obtemos $\alpha a x \equiv \alpha b \pmod{n}$. Como $\overline{\alpha}$ é o inverso de $\overline{a}$ em $\mathbb{Z}_n$ esta equação se reduz a

$$x \equiv \alpha b \pmod{n}$$

Exemplo 3.14. Resolva a seguinte equação: $7x \equiv 3 \pmod{15}$

Primeiramente, precisamos multiplicá-la pelo inverso de $\overline{7}$ em $\mathbb{Z}_{15}$. Como $15 - 2\cdot 7 = 1$, o inverso de $\overline{7}$ é $\overline{-2} = \overline{13}$. Multiplicando a congruência por 13, temos

$$x \equiv 13\cdot 3 \equiv 39 \equiv 9 \pmod{15}$$

Analisando este método de congruências, podemos chegar à seguinte conclusão. Se $\text{mdc}(a,n) = 1$, então a congruência linear $ax \equiv b \pmod{n}$ tem uma e uma só solução em $\mathbb{Z}_n$. Isto pode não ser verdadeiro se eliminamos a condição $\text{mdc}(a,n) = 1$. Por exemplo, a equação $2x \equiv 1 \pmod{8}$ não tem solução.

3.8 Os Teoremas de Euler, Wilson e o Pequeno Teorema de Fermat

O Pequeno Teorema de Fermat afirma que se p é um número primo e a é um inteiro qualquer então p divide $a^p - a$. Antes de demonstrá-lo precisamos de um resultado auxiliar.

Lema 3.15. *Sejam p um número primo e a e b inteiros. Então*

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Demonstração. Usando a expressão usual do binômio de Newton temos

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i$$

Para obter o Lema é suficiente mostrar que o termo $\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i$ é congruente a zero módulo p. Considere o número binomial

$$\binom{p}{i} = p(p-1)\ldots(p-i+1)/i!$$

Sabemos que este é um número inteiro. Para que a fração acima dê lugar a um número inteiro é preciso que o denominador seja completamente cancelado por termos do numerador. Agora suponha que $1 \leq i \leq p-1$ Então o denominador $i!$ não tem p como um de seus fatores primos. Assim o fator p que aparece no numerador não é cancelado por nenhum fator do denominador. Portanto o número inteiro $\binom{p}{i}$ é múltiplo de p quando $1 \leq i \leq p-1$. Conseqüentemente,

$$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i \equiv 0 \pmod{p}$$

e provamos o que queríamos. □

Teorema 3.16. *(Pequeno Teorema de Fermat, versão I) Seja p um número primo. Então*

$$a^p \equiv a \pmod{p} \text{ para todo } a \in \mathbb{Z} \tag{3.1}$$

Demonstração. Suponhamos primeiro $a \geq 0$. Consideremos a afirmação $P(a)$ seguinte: $a^p \equiv a \pmod{p}$. Vemos claramente que $P(0)$ é válido. Suponhamos então que $a^p \equiv a \pmod{p}$. Queremos mostrar que $(a+1)^p \equiv (a+1) \pmod{p}$. Usando o Lema 3.15 temos

$$(a+1)^p \equiv a^p + 1^p \equiv a^p + 1 \pmod{p}$$

Pela hipótese de indução temos $a^p \equiv a \pmod{p}$. Então

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

Provamos que $a^p \equiv a \pmod{p}$ para todo $a \geq 0$. Mas o Teorema foi enunciado para qualquer $a \in \mathbb{Z}$. Assim, falta provar para os inteiros negativos. Seja a um inteiro negativo. Então $-a$ é positivo, e podemos aplicar o que já provamos, ou seja,

$$(-a)^p \equiv -a \pmod{p}$$

Supondo p ímpar, $(-a)^p = -a^p$. Substituindo na equação acima temos $-a^p \equiv -a \pmod{p}$. Multiplicando ambos os membros por -1, concluímos que $a^p \equiv a \pmod{p}$, que é o resultado do Teorema. Falta apenas o caso em que $p = 2$, pois é o único primo par. Mas se isso ocorrer, note que $a^2 - a$ é par, logo $2 \mid a^2 - a$. Portanto $a^2 \equiv a \pmod{2}$. □

Teorema 3.17. *(Pequeno Teorema de Fermat, versão II) Seja p um primo e a um inteiro que não é divisível por p. Então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração. Como pelo Teorema 3.16, p divide $a(a^{p-1}-1)$ e como $\text{mdc}(a, p) = 1$, segue-se, imediatamente, que p divide $a^{p-1} - 1$. □

Definição 3.18. A função $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$ que associa a cada número inteiro positivo m a quantidade de elementos do conjunto $\{k \in \mathbb{Z}_+ | 1 \leqslant k \leqslant m - 1 \text{ e } \text{mdc}(k, n) = 1\}$ é chamada *função φ de Euler.*

Ou seja, $\varphi(m)$ indica quantos dos números da sequência 1, 2, ..., $m - 1$ são relativamente primos com m.

Teorema 3.19. *(Teorema de Euler) Sejam $m, a \in \mathbb{Z}_+$ com $m > 1$ e $\text{mdc}(a, m) = 1$. Então*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Demonstração. Sejam $s_1 = 1 < s_2 < \ldots < s_k$ os inteiros de 1 a $m - 1$ que são relativamente primos com m (logo $k = \varphi(m)$). Dividindo cada produto as_i por m temos

$$as_i = mq_i + r_i \quad (0 \leqslant r_i < m)$$

Notemos que $r_i \geq 1$. De fato se $r_i = 0$ para algum i, temos $as_i = mq_i$. Então se p é um primo tal que $p \mid m$, temos $p \mid a$ ou $p \mid s_i$, contrariando as hipóteses $\text{mdc}(a, m) = 1$ ou $\text{mdc}(m, s_i) = 1$. Portanto $r_i \geq 1$.

Vamos mostrar agora que $\text{mdc}(m, r_i) = 1$ para todo i. Se $r_i = 1$ isso é verdade. Suponhamos $r_i > 1$. Suponhamos que exista um primo p tal que $p \mid m$ e $p \mid r_i$. De $as_i = mq_i + r_i$ decorre que $p \mid as_i$. Assim $p \mid a$ ou $p \mid s_i$, o que é impossível já que $\text{mdc}(a, m) = 1$ e $\text{mdc}(m, s_i) = 1$ devido às escolhas dos s_i. Segue que m e r_i são primos entre si, para todo i tal que $1 \leqslant i \leqslant k$.

Vamos mostrar agora que não há elementos repetidos na sequência r_1, r_2, ..., r_k. De fato, se $r_i = r_j$ para $1 \leqslant i < j \leqslant k$, então $as_i - mq_i = as_j - mq_j$ e assim $a(s_j - s_i) = m(q_j - q_i)$. Como $\text{mdc}(a, m) = 1$, então $m \mid s_j - s_i$. Mas $1 \leqslant s_i < s_j \leqslant m - 1$, então $0 < s_j - s_i < m - 1$, o que não é possível. Provamos que não há elementos repetidos.

Temos então que $\{s_1, s_2, \ldots, s_k\} = \{r_1, r_2, \ldots, r_k\}$. Segue que $s_1 s_2 \ldots s_k = r_1 r_2 \ldots r_k$.

Agora multiplicamos membro a membro as congruências $as_i \equiv r_i \pmod{m}$ decorrentes de $as_i = mq_i + r_i$ $(1 \leqslant i \leqslant k)$ do que obtemos

$$a^k s_1 s_2 \ldots s_k \equiv (as_1)(as_2) \ldots (as_k) \equiv r_1 r_2 \ldots r_k \pmod{m}$$

portanto

$$a^k r_1 r_2 \ldots r_k \equiv r_1 r_2 \ldots r_k \pmod{m}$$

Como m é primo com cada r_i e, portanto, com o produto $r_1 r_2 \ldots r_k$, então esse produto pode ser cancelado na última congruência, obtendo:

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

pois $k = \varphi(m)$. □

Teorema 3.20. *(Teorema de Wilson) Se p é um número primo então*

$$(p-1)! \equiv p - 1 \pmod{p}$$

Demonstração. Suponhamos p primo. Para todo $i \in \{1, ..., p-1\}$ a congrência $iX \equiv 1 \pmod{p}$ possui uma única solução $\pmod{p}$ ou seja, dado $i \in \{1, \cdots, p-1\}$ existe $j \in \{1, \cdots, p-i\}$ tal que $ij \equiv 1 \pmod{p}$. Por outro lado, se $i \in \{1, \cdots, p-1\}$ é tal que $i^2 \equiv 1 \pmod{p}$, então $p \mid i^2 - 1$, o que equivale a $p \mid i-1$ ou $p \mid i+1$ o que só pode ocorrer se $i = 1$ ou $i = p-1$.

Logo,

$$2 \cdots (p-2) \equiv 1 \pmod{p}$$

e portanto

$$1 \cdot 2 \cdots (p-2)(p-1) \equiv p - 1 \pmod{p}$$

□

Capítulo 4

Pseudoprimos

4.1 Introdução

Neste Capítulo veremos como utilizar a recíproca do Teorema de Fermat para obter testes de primaridade. Um teste de primaridade é uma condição para a qual ocorre: dado $n > 1$ inteiro, se n satisfaz à condição, então n é primo.

4.2 Pseudoprimos

Vamos rever o enunciado do Pequeno Teorema de Fermat, versão I, demonstrado na página 25.

Teorema 4.1. *(Pequeno Teorema de Fermat, versão I) Seja p um número primo. Então*

$$a^p \equiv a \pmod{p} \text{ para todo } a \in \mathbb{Z} \tag{4.1}$$

Uma afirmação útil é a contrapositiva desse teorema, cujo enunciado é

Teorema 4.2. *(Contrapositiva da versão I do Pequeno Teorema de Fermat) Seja $n > 1$ um inteiro. Se*

$$a^n \not\equiv a \pmod{n} \text{ para algum } a \in \mathbb{Z} \tag{4.2}$$

então n é composto.

Conforme veremos, para verificar que n é composto basta procurar a tal que $1 < a < n-1$ e $a^n \not\equiv a \pmod{n}$

Vejamos agora a recíproca da versão I do Pequeno Teorema de Fermat. Um primeiro enunciado seria o seguinte:

(?) Seja $n > 1$ um inteiro. Se

$$a^n \equiv a \pmod{n} \text{ para todo } a \in \mathbb{Z} \tag{4.3}$$

então n é primo.

Veremos que esta afirmação é falsa. Antes de dar um contraexemplo faremos algumas observações. Notemos primeiro que se $a = 0$ ou $a = 1$ a condição 4.3 está satisfeita. Portanto convém excluir esses dois valores no enunciado da recíproca. Ainda se a e b são inteiros tais que $a \equiv b \pmod{n}$ então $a^n \equiv b^n \pmod{n}$, devido a uma propriedade das congruências. Portanto $a^n \equiv a \pmod{n} \iff b^n \equiv b \pmod{n}$. Portanto na condição 4.3 podemos nos limitar aos valores $1 < a \leq n-1$. Por outro lado $(n-1)^n \equiv qn + (-1)^n \equiv (-1)^n \pmod{n}$. Se $n > 2$ for par, então $(n-1)^n \equiv 1 \not\equiv n-1 \pmod{n}$, portanto a condição 4.3 nunca estará satisfeita. Se n for ímpar, então $(n-1)^n \equiv -1 \equiv n-1 \pmod{n}$, logo podemos excluir o valor $a = n-1$ da condição 4.3. Excluímos também $n = 2$, pois já sabemos que 2 é primo.

Conjectura 4.3. *(Falsa) Seja $n > 2$ um inteiro ímpar. Se*

$$a^n \equiv a \pmod{n} \text{ para todo } a \in \mathbb{Z} \text{ tal que } 1 < a < n-1 \tag{4.4}$$

então n é primo.

O menor contraexemplo é $n = 561$. Esse contraexemplo pode ser verificado através de um programa computacional. No final deste capítulo disponibilizamos um procedimento que pode ser executado no aplicativo computacional Maple (Programa 4.14 na página 38).

Vemos assim que a recíproca da versão I do Pequeno Teorema de Fermat não nos fornece diretamente um teste de primaridade. Na tentativa de salvar essa idéia, podemos procurar caracterizar todos os contraexemplos dessa conjectura. A princípio fazemos a seguinte definição

Definição 4.4. Chamamos de *número de Carmichael* a qualquer número composto ímpar $n > 0$ tal que $a^n \equiv a \pmod{n}$ para todo $1 < a < n-1$.

Os dez primeiros números de Carmichael são

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341

Esses números levam o nome do matemático Robert Daniel Carmichael (1879 - 1967) que estudou suas propriedades. Infelizmente existem infinitos números de Carmichael. Ocorre também que é alto o custo computacional para verificar se um dado número é de Carmichael ou não. Existem propriedades desses números que podem facilitar seu estudo. Veremos algumas dessas propriedades mais adiante.

Vamos rever o Pequeno Teorema de Fermat em sua segunda versão, demonstrado na página 26.

Teorema 4.5. *(Pequeno Teorema de Fermat, versão II) Se p é primo então*

$$a^{p-1} \equiv 1 \pmod{p} \quad \textit{para todo } a \in \mathbb{Z} - p\mathbb{Z}$$

Perguntamos se esse Teorema pode ser usado como um teste de primaridade.

Consideraremos a recíproca da versão II do Pequeno Teorema de Fermat.

Recíproca do Pequeno Teorema de Fermat, versão II. Dado um inteiro $n > 1$, se

$$a^{n-1} \equiv 1 \pmod{n} \textit{ para todo } a \in \mathbb{Z} - n\mathbb{Z} \tag{4.5}$$

então n é primo.

Façamos algumas considerações iniciais. Nessa recíproca não nos interessa considerar $n = 2$, pois já sabemos que 2 é primo. Tampouco nos interessa considerar $n \geqslant 4$ par, pois já sabemos que n é composto. Inclusive observamos que tais n não satisfazem a condição 4.5. De fato, note que 2^{n-1} é par logo $2^{n-1} - 1$ é ímpar. Portanto, se n for par, temos 2^{n-1} não é congruente a $1 \pmod{n}$ pois, sendo $2^{n-1} - 1$ ímpar e n par, temos $n \nmid 2^{n-1} - 1$.

Portanto, vamos escrever a recíproca da seguinte forma:

Dado um inteiro $n > 1$ ímpar, se $a^{n-1} \equiv 1 \pmod{n}$ para todo $a \in \mathbb{Z} - n\mathbb{Z}$ então n é primo.

Notemos agora o seguinte: seja $n > 1$ um inteiro. Se a e b são inteiros tais que $a \equiv b \pmod{n}$, então

$$a^{n-1} \equiv 1 \pmod{n} \Leftrightarrow b^{n-1} \equiv 1 \pmod{n}$$

De fato, se $a \equiv b \pmod{n}$ temos $a^{n-1} \equiv b^{n-1} \pmod{n}$. O resultado segue da propriedade transitiva das congruências.

Portanto, na recíproca, ao dar a condição 4.5, basta considerar $0 \leqslant a \leqslant n - 1$. Como $0 \in n\mathbb{Z}$, reduzimos para $0 < a \leqslant n - 1$. Como sempre ocorre que $1^{n-1} \equiv 1 \pmod{n}$, não precisamos considerar $a = 1$. Como $(n-1)^{n-1} = qn + (-1)^{n-1}$, se n for ímpar temos $(-1)^{n-1} = 1$, de modo que sempre ocorre $(n-1)^{n-1} \equiv 1 \pmod{n}$. Portanto em 4.5 também não precisamos considerar o valor $a = n - 1$. Dessa forma a recíproca pode ser assim enunciada:

Teorema 4.6. *(Recíproca do Pequeno Teorema de Fermat, versão II) Dado um inteiro $n > 1$ ímpar, se*

$$a^{n-1} \equiv 1 \pmod{n} \textit{ para todo } a \in \mathbb{Z} - n\mathbb{Z} \textit{ tal que } 1 < a < n - 1 \tag{4.6}$$

então n é primo.

Demonstração. Suponhamos que n seja composto, logo $n \geqslant 5$. Existe um primo p tal que $p \mid n$ e $1 < p < n-1$. Pela condição dada temos $p^{n-1} \equiv 1 \pmod{n}$. Portanto $n \mid p^{n-1} - 1$. Mas $p \mid n \Rightarrow p \mid p^{n-1} - 1 \Rightarrow p \mid 1$, o que é uma contradição. Portanto n é primo. □

Vemos assim que a recíproca do Teorema de Fermat nos fornece um teste de primaridade. O problema é que o custo computacional é muito alto, de modo que, em termos práticos, esse teste tem interesse muito limitado. Entretanto, continuando nessa linha de raciocínio, obtemos resultados muito interessantes.

Consideremos a afirmação contrapositiva da recíproca do Teorema de Fermat, versão II.

Teorema 4.7. *Se $n > 0$ e $1 < b < n-1$ são números inteiros e $b^{n-1} \not\equiv 1 \pmod{n}$, então n é composto.*

Definição 4.8. Se $n > 0$ e $1 < b < n-1$ são números inteiros e $b^{n-1} \not\equiv 1 \pmod{n}$, o número b é conhecido como uma *testemunha* do fato de n ser composto.

Se n é ímpar, e satisfaz $b^{n-1} \equiv 1 \pmod{n}$, para algum $1 < b < n-1$, não podemos afirmar que n é primo. Por exemplo, $2^{340} \equiv 1 \pmod{341}$, mas 341=11.31, é composto. O número 341 é um exemplo do que chamamos de *pseudoprimo* para a base 2.

Definição 4.9. Seja n um inteiro positivo ímpar e composto. Se existir um inteiro b tal que $1 < b < n-1$ e $b^{n-1} \equiv 1 \pmod{n}$, dizemos que n é um pseudoprimo para a base b.

Vimos portanto que um inteiro $n > 1$ ímpar pode ser um pseudoprimo para uma determinada base b, e assim não é primo. Uma antiga conjectura chinesa afirmava que se um número inteiro n satisfizesse $2^{n-1} \equiv 1 \pmod{n}$ então n seria primo. Já vimos que isso não é verdade, e o menor contraexemplo é 341. Mas não de todo inútil fazer essa verificação. Por exemplo, entre 1 e 10^6 existem 78498 primos, mas apenas 245 pseudoprimos para a base 2. Se incluirmos a verificação para a base 3, o teste fica mais eficiente. Sabemos que existem apenas 66 pseudoprimos para as bases 2 e 3 entre 1 e 10^6. Esses resultados foram verificados pelo Programa 4.18 na página 42.

Na próxima seção vamos explorar melhor essas idéias apresentando o chamado Teste de Miller. Para o momento veremos alguma propriedades adicionais dos números de Carmichael.

Vejamos primeiro uma forma mais econômica de verificar se um determinado número é de Carmichael.

Exemplo 4.10. Fatore $n = 29341$ e mostre que é um número de Carmichael

Fatorando n, temos que $29341 = 13 \cdot 37 \cdot 61$. Seja b um inteiro entre 2 e 29339, iremos mostrar que

$$b^{29341} \equiv b \pmod{29341}$$

Vamos mostrar que 13, 37 e 61 dividem $b^{29341} - b$. Como 13, 37 e 61 são primos distintos, então o produto destes primos divide $b^{29341} - b$, e este produto é 29341, logo é o mesmo que dizer $b^{29341} \equiv b \pmod{29341}$.

Agora, basta mostrar que $b^{29341} - b$ é divisível por cada um dos fatores encontrados acima.

1) $b^{29341} \equiv b \pmod{13}$

Se 13 divide b, acabou, pois ambos os membros são congruentes a zero módulo 13. Caso contrário, usamos o Teorema de Fermat: $b^{12} \equiv 1 \pmod{13}$

Temos também que $29341 = 2445 \cdot 12 + 1$. Assim

$$b^{29341} \equiv (b^{12})^{2445} \cdot b \equiv b \pmod{13}$$

2) $b^{29341} \equiv b \pmod{37}$ Se 37 divide b, acabou, pois ambos os membros são congruentes a zero módulo 37. Caso contrário, usamos o Teorema de Fermat: $b^{36} \equiv 1 \pmod{37}$

Temos também que $29341 = 815 \cdot 36 + 1$. Assim

$$b^{29341} \equiv (b^{36})^{815} \cdot b \equiv b \pmod{37}$$

3) $b^{29341} \equiv b \pmod{61}$ Se 61 divide b, acabou, pois ambos os membros são congruentes a zero módulo 61. Caso contrário, usamos o Teorema de Fermat: $b^{60} \equiv 1 \pmod{61}$

Temos também que $29341 = 489 \cdot 60 + 1$. Assim

$$b^{29341} \equiv (b^{60})^{489} \cdot b \equiv b \pmod{61}$$

Mostramos assim, que $b^{29341} - b$ é divisível por 13, 37 e 61, e consequentemente pelo produto deles, e assim, é um número de Carmichael.

Repare que só pudemos resolver o exemplo acima, com $n = 29341$, porque o resto da divisão de 29341 por 12, 36 e 60 deu 1, e também porque 29341 é

um produto de primos distintos, ou seja, a multiplicidade de cada um desses fatores é 1.

Existem infinitos números de Carmichael, e em todos eles verificamos as propriedades do exemplo anterior.

Teorema 4.11. *(Teorema de Korselt) Um inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as duas condições seguintes:*
(i) p^2 não divide n
(ii) $p-1$ divide $n-1$

Para ver uma demonstração do Teorema de Korselt, consulte [1], página 109.

4.3 Teste de Miller

Dado n inteiro ímpar $\geqslant 5$ e um inteiro b tal que $1 < b < n-1$, o teste responde "n é composto" ou "teste inconclusivo". Se a resposta for "n é composto", então n é composto. Se a resposta for "teste inconclusivo", n pode ser primo ou composto. Neste caso , se n é composto, é dito ser um *pseudoprimo forte* para a base b.

Algoritmo:

Dado $n \geq 5$ inteiro ímpar e $1 < b < n-1$, escreva $n-1 = 2^k q$, com q ímpar e $k \geq 1$. Faça as seguintes etapas:

Etapa (0): Calcule r_0 =resto da divisão de b^q por n.
Se $r_0 = 0$, pare e responda "n é composto".
Se $r_0 = 1$, pare e responda "teste inconclusivo".
Se $r_0 = n-1$, pare e responda "teste inconclusivo".
Se $2 \leqslant r_0 < n-1$ faça a Etapa (1), (2), (3), etc.

Para $i \geq 1$, e enquanto $i < k$, faça:
Etapa (i): Seja r_i o resto da divisão de r_{i-1}^2 por n.
Se $r_i = 0$, pare e responda "n é composto".
Se $r_i = n-1$ pare e responda "teste é inconclusivo".
Se $1 \leqslant r_i < n-1$ faça a etapa $i = i+1$.

Se $i = k$ responda "n é composto".

Demonstração. O Teste de Miller começa escolhendo um n ímpar $\geqslant 5$. Como n é ímpar, $n-1$ é par. Escrevemos então $n-1 = 2^k q$, com q inteiro ímpar e $k \geqslant 1$. Vejamos porque o teste funciona.

Lembremos que se n for primo, então pelo Teorema de Fermat, temos

$$b^{n-1} \equiv b^{2^k q} \equiv 1 \pmod{n} \tag{4.7}$$

para todo b tal que $1 < b < n-1$.

O algoritmo usa a contrapositiva do Teorema de Fermat. Assim, se essa condição não ocorrer para algum b tal que $1 < b < n-1$, n não pode ser primo; logo é composto. Vejamos mais detalhes.

Dado um tal b, seja j o menor inteiro tal que $0 \leqslant j \leqslant k$ e

$$b^{2^j q} \equiv 1 \pmod{n}$$

Se $j = 0$, não temos contradição, e nada podemos afirmar sobre n. De fato $b^q \equiv 1 \pmod{n} \Rightarrow b^{2^k q} \equiv 1 \pmod{n}$, e a condição 4.7 está satisfeita.

Suponhamos $j \geqslant 1$. Temos

$$b^{2^j q} - 1 = (b^{2^{j-1} q} - 1)(b^{2^{j-1} q} + 1)$$

donde $n \mid b^{2^{j-1} q} + 1$, pois $b^{2^{j-1} q} - 1$ não pode ter n como fator devido à minimalidade de j. Temos então que $b^{2^{j-1} q} \equiv -1 \equiv n-1 \pmod{n}$.

Em resumo, se n é primo e $j \geqslant 1$, então

$$\text{alguma das potências } b^q, b^{2q}, \ldots, b^{2^{k-1} q} \text{é congruente a } n-1 \pmod{n} \tag{4.8}$$

Vejamos agora com detalhes o que ocorre na Etapa (0) e nas posteriores.

Na Etapa (0), se $r_0 = 1$, o teste é inconclusivo, pois teríamos $b^q \equiv 1 \pmod{n}$, e isso corresponde a ter $j = 0$, e já vimos que não temos contradição. Se $r_0 = n-1$, o teste também é inconclusivo, pois neste caso $b^q \equiv n-1 \pmod{n}$, o que corresponde ao resultado esperado 4.8. Portanto neste caso o teste também é inconclusivo.

Se o resto da divisão de b^q por n for $r_0 = 0$, então $b^q \equiv 0 \pmod{n}$, o que implica $n \mid b^q$. Se n for primo isso implica $n \mid b$, o que é impossível pois $1 < b < n-1$. Portanto se $r_0 = 0$ temos que n é composto.

Se $2 \leqslant r_0 < n-1$, precisamos continuar procurando qual é o j mínimo para o qual $n \mid b^{2^{j-1} q} + 1$. Nesse caso devemos prosseguir para a etapa (i), começando com $i = 1$. Se isso ocorrer temos $j \geqslant 1$.

Anotaremos r_i como o resto da divisão de $b^{2^i q}$ por n. Observe que isso é o mesmo que calcular o resto da divisão de r_{i-1}^2 por n, pois

$$b^{2^i q} \equiv \left(b^{2^{i-1} q}\right)^2 \equiv r_{i-1}^2 \pmod{n}$$

Se $r_i = 0$, n é composto, conforme já observamos acima para $r_0 = 0$.

Se $r_i = n - 1$ o teste é inconclusivo, pois $r_{i-1}^2 \equiv (n-1) \pmod{n}$, logo $b^{q^i} \equiv n - 1 \equiv -1 \pmod{n}$, e está satisfeita a condição 4.8.

Se $1 \leqslant r < n - 1$, faça a etapa $i = i + 1$.

Se $i = k$, n é composto, pois verificamos todos os $b^{2^i q}$ e nenhum foi congruente a -1.

□

Exemplo 4.12. Usando o Teste de Miller, o que podemos dizer para os seguintes números?

(a) $n = 645$ e $b = 2$

$$644 = 2^2 \cdot 161$$

Temos neste caso $q = 161$ e $k = 2$. Começamos com $i = 0$.

Etapa (0): O resto da divisão de 2^{161} por 645 é 257, ou seja

$$2^{161} \equiv 257 \pmod{645}$$

Então $r_0 = 257$

Assim temos $2 \leqslant r_0 < 644$, então neste caso façamos a Etapa(1).

Etapa (1): $i = 1$, $k = 2$

O resto da divisão de $r_i^2 = 257^2$ por 645 é 259, pois

$$257^2 \equiv 259 \pmod{645}$$

Assim temos $1 \leqslant 259 < 644$, então neste caso façamos a Etapa(2):

Etapa (2): $i = 2$, $k = 2$

Como chegamos ao caso em que $i = k$, podemos dizer que $n = 645$ é *composto*.

(b) $n = 2047$ e $b = 2$

$$2046 = 2 \cdot 1023$$

Temos neste caso $q = 1023$ e $k = 1$. Começamos com $i = 0$.

Etapa (0): O resto da divisão de 2^{1023} por 2047 é 1, pois

$$2^{1023} \equiv 1 \pmod{2047}$$

Então $r_0 = 1$. Podemos então dizer, neste caso, que o teste é inconclusivo para $n = 2047$ e $b = 2$

Assim como fizemos para encontrar números de Carmichael, vamos utilizar o Maple também para aplicar o Teste de Miller, que deixará o processo muito mais fácil que feito manualmente. Confira o Programa 4.15.

4.4 Procedimentos Computacionais

Programa 4.13. *Dado um inteiro positivo ímpar composto m, verifica se m é de Carmichael.*

Este programa usa a definição, portanto é bem lento. Por exemplo, para verificar que 29341 é de Carmichael, demora 431 segundos. Segue o código fonte do programa.

```
> ecarmichael:=proc(m::posint)
> local b,q; b:=2; q:=0;
> if irem(m,2)=0 then
> ERROR(‘entre com um inteiro positivo impar‘);
> fi;
> if isprime(m) then
> ERROR(m,‘e primo e nao e carmichael entre com um inteiro
composto‘);
> fi;
> while b<m-1 do q:=irem(b^m-b,m); if q=0 then b:=b+1;
else break;fi;od;
> if b=m-1 then print(m,‘e carmichael‘); else
print(m,‘nao e carmichael‘);fi;
> end:
```

Vamos fazer alguns cálculos, verificando que 561, 1105, 1729, 2465 e 29341 são números de Carmichael.

```
> ecarmichael(561);
561, e carmichael

> ecarmichael(1105);
1105, e carmichael

> ecarmichael(1729);
1729, e carmichael

> ecarmichael(2465);
2465, e carmichael

> ecarmichael(29341);
29341, e carmichael
```

Programa 4.14. *Dados $n < m$, verifica quais números $\geqslant n$ e $\leqslant m$ são de Carmichael*

```
> atecarmichael:=proc(n::posint,m::posint)
> local j,b,q;
> b:=2;q:=0;
> if n>m then ERROR(‘o primeiro argumento deve ser menor
do que o segundo‘); else
> for j from n to m do
> if irem(j,2)=1 then
> if not isprime(j) then b:=2;
> while b<j-1 do q:=irem(b^j-b,j); if q=0 then b:=b+1;
else break;fi;if b=j-1 then print(j,‘ecarmichael‘);fi;
> od;
> fi;fi;od;fi;
> end:
```

Vamos fazer alguns cálculos para mostrar quais são os números de Carmichael entre 1 e 2465, e depois entre 5001 e 10000. Este cálculo também verifica que o menor número de Carmichael é 561, conforme afirmamos acima.

```
> atecarmichael(1,2465);
561, e carmichael
1105, e carmichael
1729, e carmichael
2465, e carmichael

> atecarmichael(5001,10000);
6601, e carmichael
8911, e carmichael
```

Programa 4.15. *Procedimento para aplicar o teste de Miller. Dado um inteiro ímpar $n \geq 5$ e um inteiro b tal que $1 < b < n-1$, verifica se n é um pseudoprimo na base b.*

Se o programa responde n é composto, então n é realmente composto. Se o programa responde teste inconclusivo então n pode ser primo ou composto.

```
> Miller:=proc(n::posint,b::posint)
> local k,r,q,i;
> k:=0;i:=0;
> if n<5 then ERROR(‘o primeiro argumento deve ser >=5‘);fi;
```

```
> if irem(n,2)=0 then ERROR
(‘o primeiro argumento deve ser impar‘);fi;
> if b=1 then ERROR(‘o segundo argumento deve ser >1‘);fi;
> if b>=n-1 then ERROR(‘o segundo argumento deve ser <‘, n-1);
fi;
> while irem(n-1,2^(k+1))=0 do k:=k+1;
> od;
> q:=(n-1)/2^k;
> r:=irem(b^q,n);
> if r=1 then
> print(‘teste inconclusivo‘);
> elif r=n-1 then
> print(‘teste inconclusivo‘);
> elif r=0 then
> print(n,‘e composto‘);
> else
> while i<k do r:=irem(r^2,n);
> if r=0 then
> print(n,‘e composto‘);
> elif r=n-1 then
> print(‘teste inconclusivo‘); break;
> else i:=i+1;
> fi;
> od;
> if i=k then print(n,‘e composto‘);
> fi;
> fi:
> end:
```

Veja alguns testes com o procedimento de Miller.

```
> Miller(25,2);
25, e composto

> Miller(25,7);
teste inconclusivo
```

Se $n = 25$, vemos que o teste de Miller é inconclusivo para a base 7, e conclusivo para a base 2. Podemos fazer uma pesquisa usando o loop abaixo e verificar que se $n = 25$, o teste de Miller é inconclusivo para as bases 7 e 18, e conclusivo para as outras bases. Podemos inferir que o teste de Miller é bom do ponto de vista probabilístico.

```
> for b from 2 to 23 do print(b, Miller(25,b)):od:
```

Vejamos alguns outros experimentos.

```
> Miller(341,2);
341, e composto

> Miller(341,3);
341, e composto

> Miller(341,4);
teste inconclusivo

> Miller(341,5);
341, e composto

> Miller(341,6);
341, e composto

> Miller(341,11);
341, e composto
```

Se n é primo, o teste sempre falha. Por exemplo:

```
> Miller(41,2);
teste inconclusivo

> Miller(43,2);
teste inconclusivo
```

Programa 4.16. *O procedimento Leibniz verifica se o inteiro positivo ímpar $n \geqslant 9$ é pseudoprimo na base b com $1 < b < n - 1$.*

```
> Leibniz:=proc(n::posint,b::posint)
> if n<=8 then ERROR(‘o primeiro argumento
deve ser >=9‘);fi;
> if irem(n,2)=0 then ERROR(‘o primeiro argumento
deve ser impar‘);fi;
> if isprime(n) then ERROR(‘o primeiro argumento
deve ser composto‘);fi;
> if b<=1 then ERROR(‘o segundo argumento
deve ser >1‘);fi;
```

```
> if b>=n-1 then ERROR(‘o segundo argumento
deve ser <‘, n-1);fi;
> if irem(b^(n-1)-1,n)=0 then print(n,‘e pseudoprimo
para a base‘,b);fi;
> if not irem(b^(n-1)-1,n)=0 then print(n,‘nao e pseudoprimo
para a base‘,b);fi;
> end:
```

Vejamos alguns exemplos.

```
> Leibniz(341,2);
341, e pseudoprimo para a base, 2

> Leibniz(341,3);
341, nao e pseudoprimo para a base, 3

> Leibniz(561,2);
561, e pseudoprimo para a base, 2

> Leibniz(561,3);
561, nao e pseudoprimo para a base, 3

> Leibniz(1373653,2);
1373653, e pseudoprimo para a base, 2

> Leibniz(1373653,3);
1373653, e pseudoprimo para a base, 3
```

Programa 4.17. *Dado um inteiro positivo $n \geqslant 9$, calcula quantos inteiros entre 1 e n são pseudoprimos na base 2.*

Um pseudoprimo na base 2 é um número composto n tal que $2^{n-1} \equiv 1 \pmod{n}$.

```
> quantospseudoprimos:=proc(n::posint)
> local j,k; k:=0;
> if n<=8 then ERROR(‘o argumento deve ser >=9‘);
fi;
> for j from 9 to n do
> if irem(j,2)=1 then
> if not isprime(j) then
> if irem(2^(j-1)-1,j)=0 then k:=k+1;
```

```
> fi;fi;fi;od;
> print(k);
> print(‘a quantidade de pseudoprimos para
a base 2 de 1 a‘, n, ‘e‘, k);
> end:
```

Vamos fazer alguns cálculos. Sabemos que 341 é o menor pseudoprimo para a base 2. Vamos verificar isso.

```
> quantospseudoprimos(341);
1
a quantidade de pseudoprimos para
a base 2 de 1 a, 341, e, 1
```

Vamos verificar que existem 245 pseudoprimos na base 2 entre 1 e 1000000, conforme afirmado no texto.

```
> quantospseudoprimos(1000000);
245
a quantidade de pseudoprimos para
a base 2 de 1 a, 1000000, e, 245
```

Programa 4.18. *Dado um inteiro positivo $n \geqslant 9$, calcula quantos inteiros entre 1 e n são pseudoprimos nas bases 2 e 3.*

Um pseudoprimo na base 2 é um número composto n tal que $2^{n-1} \equiv 1 \pmod{n}$. Um pseudoprimo na base 3 é um número composto n tal que $3^{n-1} \equiv 1 \pmod{n}$.

```
> quantospseudoprimos2:=proc(n::posint)
> local j,k; k:=0;
> if n<=8 then ERROR(‘o argumento deve ser >=9‘);
fi;
> for j from 9 to n do
> if irem(j,2)=1 then
> if not isprime(j) then
> if irem(2^(j-1)-1,j)=0 and irem(3^(j-1)-1,j)=0
then k:=k+1;
> fi;fi;fi;od;
> print(k);
> print(‘a quantidade de pseudoprimos para
as bases 2 e 3 de 1 a‘, n, ‘e‘, k);
> end:
```

A seguir, faremos um teste para verificar quantos pseudoprimos para base 2 e 3 existem entre 1 e 1000000. Confirmamos assim a afirmação feita no texto.

```
> quantospseudoprimos2(1000000);
66
a quantidade de pseudoprimos
para a base 2 e 3 de 1 a, 1000000, e, 66
```

Capítulo 5

Sistemas de Congruências

5.1 Introdução

Neste capítulo, retomaremos o assunto de Congruências Lineares iniciado no capítulo 3, estudando a solução de sistemas de equações lineares, utilizando o algoritmo chinês do resto, e por fim uma aplicação deste algoritmo.

5.2 Resolvendo Equações Lineares

Como vimos anteriormente, uma congruência linear é uma equação do tipo

$$ax \equiv b \pmod{n} \text{ onde } a,\, b \in \mathbb{Z}. \tag{5.1}$$

Vamos começar considerando apenas o caso de uma equação linear, onde n é um inteiro positivo.

Sabemos que se $\text{mdc}(n, a) = 1$, então existe $\lambda \in \mathbb{Z}$ tal que $\lambda \cdot a \equiv 1 \pmod{n}$, onde $\overline{\lambda}$ é o inverso de $\overline{a}$ em $\mathbb{Z}_n$. Multiplicando ambos os menbros da equação 5.1 por λ temos:

$$\lambda(ax) \equiv \lambda b \pmod{n} \Rightarrow x \equiv \lambda b \pmod{n}$$

que é a solução da equação, e se n for primo e a não for congruente a 0 módulo n, então a equação sempre tem solução, pois neste caso, sempre teremos $\text{mdc}(n, a) = 1$.

Se $\overline{a}$ não tiver inverso em $\mathbb{Z}_n$, então $\text{mdc}(n, a) \neq 1$. Se a equação tem solução, então existem x, $y \in \mathbb{Z}$ tais que $ax - b = ny$, então

$$ax - ny = b$$

E isto só ocorrerá se $\text{mdc}(a, n)$ divide b. Ou seja, $ax \equiv b \pmod{n}$ só terá solução quando b for divisível pelo $\text{mdc}(a, n)$.

Seja $d = \text{mdc}(a, n)$ e ele divide b, podemos escrever $a = da_1$, $b = db_1$ e $n = dn_1$. Temos então

$$da_1x - dn_1y = db_1 \Rightarrow a_1x - n_1y = b_1$$

que é a equação $a_1x \equiv b_1 \pmod{n_1}$, onde $\text{mdc}(a_1, n_1) = 1$.

5.3 Algoritmo Chinês do Resto

Vejamos agora um exemplo de sistema de congruências lineares.

Exemplo 5.1. Determine o menor inteiro positivo que deixa resto 2 na divisão por 5, resto 4 na divisão por 7 e resto 5 na divisão por 11.

Podemos reescrever nosso problema, como um sistema de congruências

$$\begin{array}{ll} x \equiv 2 & \pmod{5} \\ x \equiv 4 & \pmod{7} \\ x \equiv 5 & \pmod{11} \end{array} \tag{5.2}$$

Não podemos somar ou subtrair as equações, pois os módulos são diferentes. Então começaremos analisando a primeira equação. Temos que $x \equiv 2 \pmod{5}$ corresponde a $x = 2 + 5t$, que é um inteiro e pode ser substituído na segunda:

$$2 + 5t \equiv 4 \pmod{7}$$

ou seja

$$5t \equiv 2 \pmod{7}$$

Como $\text{mdc}(5, 7) = 1$, então $\overline{5}$ é invertível, e seu inverso em $\mathbb{Z}_7$ é $\overline{3}$. Assim, $3 \cdot 5t \equiv 3 \cdot 2 \pmod{7} \Rightarrow t \equiv 6 \pmod{7}$. Chegamos que $t = 6 + 7u$. Substituindo em $x = 2 + 5t$ vem

$$x = 2 + 5t = 2 + 5(6 + 7u) = 2 + 30 + 35u = 32 + 35u$$

Substituindo na última equação

$$32 + 35u \equiv 5 \pmod{11} \Rightarrow 35u \equiv -27 \pmod{11} \Rightarrow 2u \equiv 6 \pmod{11}$$

Como $\text{mdc}(2, 11) = 1$, $\overline{2}$ é invertível em $\mathbb{Z}_{11}$, onde $\overline{6}$ é seu inverso. Assim

$$2 \cdot 6u \equiv 6 \cdot 6 \pmod{11} \Rightarrow u \equiv 36 \pmod{11} \Rightarrow u \equiv 3 \pmod{11}$$

Temos então $u = 3 + 11v$. Substituindo novamente

$$x = 32+35u = 32+35(3+11v) = 32+105+385v = 137+385v = 137+5.7.11$$

E desta maneira, encontramos nossa solução para o sistema 5.2, que é 137.

Esse algoritmo generaliza o método que utilizamos no exemplo anterior.

Teorema 5.2. *Teorema Chinês do Resto: Sejam m e n inteiros positivos, primos entre si. O sistema*

$$\begin{array}{l} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{array} \tag{5.3}$$

sempre tem uma única solução em $\mathbb{Z}_{mn}$.

Demonstração. Podemos escrever a primeira equação de 5.3 como $x = a + my$, $y \in \mathbb{Z}$, e substituíndo na segunda, temos $a + my \equiv b \pmod{n}$, ou então, $my \equiv b - a \pmod{n}$. Para existir solução é preciso que $\text{mdc}(m, n)$ divida $(b - a)$. Como $\text{mdc}(m, n) = 1$, podemos afirmar que tem solução. Assim, $\overline{m}$ tem inverso α em $\mathbb{Z}_n$. Temos então

$$\begin{aligned} (my)\alpha &\equiv (b-a)\alpha \pmod{n} \\ \Rightarrow y &\equiv (b-a)\alpha \pmod{n} \\ \Rightarrow y &= (b-a)\alpha + nz \end{aligned}$$

para algum $z \in \mathbb{Z}$.

Substituindo em $x = a + my$

$$x = a + m((b-a)\alpha + nz) = a + m\alpha(b-a) + mnz$$

Como

$$1 \equiv \alpha m \pmod{n} \Rightarrow 1 - \alpha m = \beta n \text{ para algum } \beta \in \mathbb{Z}$$

Então

$$\begin{aligned} x &= a + m\alpha b - m\alpha a + mnz \\ \Rightarrow x &= a(1 - m\alpha) + m\alpha b + mnz = a\beta n + m\alpha b + mnz \end{aligned}$$

Portanto, o sistema tem como solução os números $a\beta n + b\alpha m + kmn$, $k \in \mathbb{Z}$.

Suponhamos x e y inteiros e que sejam solução do sistema 5.3. Podemos escrever $x \equiv a \pmod{m}$ e $y \equiv a \pmod{m}$. Como ambas são mesmo módulo, podemos somar ou subtrair uma da outra

$$x - y \equiv 0 \pmod{m}$$

Concluímos que $m \mid x - y$

Da mesma forma, de $x \equiv b \pmod{n}$, podemos concluir que $n \mid x - y$.

Se $\text{mdc}(m, n) = 1$, então $mn \mid x - y$. Logo x e y são solução de $x \equiv y \pmod{mn}$. Ou seja, o sistema tem infinitas soluções inteiras, mas apenas uma solução em $\mathbb{Z}_{mn}$ quando $\text{mdc}(m, n) = 1$. □

Para facilitar os cálculos, podemos montar uma tabela. Ela terá mn casas, onde escrevemos na parte superior, na horizontal, os elementos de $\mathbb{Z}_m$ e na vertical os de $\mathbb{Z}_n$, e a intersecção dos elementos $\overline{a}$ de $\mathbb{Z}_m$ com $\overline{b}$ de $\mathbb{Z}_n$ será ocupada pelo inteiro x de forma que $0 \leqslant x \leqslant mn-1$, $x \equiv a \pmod{m}$ e $x \equiv b \pmod{n}$. E mais, pelo Teorema Chinês do Resto, se $\text{mdc}(m, n) = 1$, então todas as casas da tabela serão preenchidas de modo que não haja repetição dos valores de x. Diremos que x tem coordenadas $(\overline{a}, \overline{b})$ na tabela.

Vamos ilustrar melhor com um exemplo

Exemplo 5.3. Vamos desenhar a tabela quando $m = 5$ e $n = 6$. Note que $\text{mdc}(m, n) = 1$.

	0	1	2	3	4
0	0	6	12	18	24
1	25	1	7	13	19
2	20	26	2	8	14
3	15	21	27	3	9
4	10	16	22	28	4
5	5	11	17	23	29

Para preencher a tabela, devemos recordar que todas as classes $\mathbb{Z}_n$ estão ao longo de uma circunferência, ou seja, nossa tabela não se limita apenas aos valores da horizontal e da vertical, ela se prolonga, ou melhor, a parte de baixo se junta com a de cima, e a da direita com a esquerda, formando uma superfície chamada *toro*.

Voltando à tabela, os valores da diagonal são facilmente preenchidos, pois são as casas com coordenadas iguais. Deste modo, a diagonal será preenchida com os valores 0, 1, 2, 3 e 4. O próximo número a ser colocado será o 5, mas a diagonal acabou, porém, sabemos que os lados da tabela são colados,

então continuamos preenchendo, só que o que deveria vir na linha de baixo à direita, se desloca para a primeira casa à esquerda nesta mesma linha.

	0	1	2	3	4	0
0	0					
1		1				
2			2			
3				3		
4					4	
5	**5**					**5**

Continuamos preenchendo na diagonal, mas novamente a tabela acabou, porém a parte de baixo e colada com a de cima. Assim, o 6 que viria na linha de baixo na coluna da direita, se desloca pra a primeira linha da mesma coluna, e continuamos preenchendo a tabela sempre na diagonal.

	0	1	2	3	4
0	0	**6**			
1		1	7		
2			2	8	
3				3	9
4					4
5	5				
0		**6**			

Desta forma preenchemos todas as casas obtendo a tabela do início do exemplo.

A versão apresentada a seguir do Teorema Chinês do Resto serve para mais de duas equações.

Teorema 5.4. *Teorema Chinês do Resto Sejam $n_1, \ldots, n_k$ inteiros positivos dois a dois primos entre si. Então o sistema*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

tem uma única solução em $\mathbb{Z}_{n_1 \ldots n_k}$

O Teorema Chinês do Resto pode ser utilizado no cálculo de potências módulo n em alguns casos especiais. Suponhamos que $n = p_1 \dots p_k$ onde $p_1 < \dots < p_k$ são números primos. Usamos o Teorema de Fermat para achar a forma reduzida de a^m módulo cada um dos primos $p_1 \dots p_k$ separadamente. Suponhamos então que já demonstramos

$$\begin{aligned} a^m &\equiv r_1 \pmod{p_1} \quad \text{e} \quad 0 \leqslant r_1 \leqslant p_1 \\ a^m &\equiv r_2 \pmod{p_2} \quad \text{e} \quad 0 \leqslant r_2 \leqslant p_2 \\ &\dots \\ a^m &\equiv r_k \pmod{p_k} \quad \text{e} \quad 0 \leqslant r_k \leqslant p_k \end{aligned}$$

Resolvemos o sistema

$$\begin{aligned} x &\equiv r_1 \pmod{p_1} \\ x &\equiv r_2 \pmod{p_2} \\ &\vdots \\ x &\equiv r_k \pmod{p_k} \end{aligned}$$

Como os módulos são primos distintos, então este sistema sempre tem solução. Além disso, o Teorema Chinês do Resto nos garante que o sistema tem uma única solução r módulo $p_1 \dots p_k = n$. Portanto $a^m \equiv r \pmod{n}$.

Capítulo 6

Elementos de Criptografia

6.1 Introdução

A criptografia é conhecida como a arte da escrita secreta. Derivada da palavra grega *kriptos*, que quer dizer oculto, secreto, essa arte tem sido praticada há milhares de anos, principalmente para fins militares e diplomáticos, e atualmente é um dos métodos mais seguros de transmitir informações. Seu objetivo é esconder o significado de uma mensagem, sendo que apenas o destinatário, um usuário legítimo consiga entendê-la, o que se chama decodificar. Já decifrar uma mensagem significa ler a mensagem sem ser o destinatário, ou usuário legítimo.

A criptografia é dividida em dois ramos: transposição e substituição. A transposição consiste em rearranjar as letras, gerando um anagrama. Já na substituição, as letras são substituídas por símbolos, números ou por outras letras. O primeiro documento em que se verificou o uso de uma cifra de substituicão para fins militares foi em Guerras de Gália, do imperador Julio César. Ele usava frequentemente este método, que ficou conhecido como *Cifra de Deslocamento de César* ou simplismente *Cifra de César*. Esse nome é dado a qualquer cifra que usa o método de substituição criptográfica, e vamos estudá-la neste capítulo, além de conhecer alguns outros métodos básicos de criptografia.

6.2 A Cifra de César

Originalmente, a Cifra de César consistia em substituir cada letra do alfabeto por aquela que está três casas à direita, ou seja, escolhemos um deslocamento de $b = 3$ casas, de modo que a seja substituído por d, b por e, etc., até x que é substituído por a, y por b e z por c. Mas podemos escolher qualquer valor

para b, porém, note que nosso alfabeto contém 26 letras, assim trabalhamos com congruência módulo 26, ou seja, se tomarmos $b = 27$ por exemplo, seria a mesma coisa se escolhermos $b = 1$, que seria trocar a letra do alfabeto pela seguinte à direita, pois temos que $27 \equiv 1 \pmod{26}$. Tomando então $b = 3$, temos a seguinte relação:

letra:	A	B	C	D	E	F	G	H	I	J	K	L	M
cifra:	D	E	F	G	H	I	J	K	L	M	N	O	P

letra:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
cifra:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Por exemplo, a palavra EXEMPLAR seria escrita:

$$\text{HAHPSODU} \tag{6.1}$$

Para decifrar um texto, basta olhar a letra na linha da cifra e depois o correspondente na linha superior.

Note que podemos mudar a ordem das linhas na relação anterior:

cifra:	D	E	F	G	H	I	J	K	L	M	N	O	P
letra:	A	B	C	D	E	F	G	H	I	J	K	L	M

cifra:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
letra:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

E reorganizando as letras, afim de começarmos a primeira linha com o A ao invés do D, temos:

cifra:	A	B	C	D	E	F	G	H	I	J	K	L	M
letra:	X	Y	Z	A	B	C	D	E	F	G	H	I	J

cifra:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
letra:	K	L	M	N	O	P	Q	R	S	T	U	V	W

Repare que nesta última tabela, vemos mais claramente que a parte inferior é deslocada 23 posições em relação à superior. Ela é usada para decifrarmos as mensagens. Ou seja, temos um resultado muito importante: quando nós ciframos a mensagem usando $b = 3$, iremos decifrá-la usando $b = 23$. Vemos facilmente que a soma é 26, que é o número de letras do alfabeto. Podemos dizer então que para cifrar, nós deslocamos o alfabeto em b casas, e para decifrar, deslocamos o alfabeto em $26 - b$ casas. Algumas vantagens deste sistema é que ele é facilmente implementado, bastando ao

usuário lembrar-se do número b de deslocamento, e também o processo de cifrar e decifrar são simétricos.

Agora, vamos analisar matemáticamente como ocorre a Cifra de César. Primeiramente, a cada letra associamos um número:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Veja que cada letra está associada a sua posição no alfabeto. Assim, a letra A está associada ao 1, a letra B ao 2 e assim por diante. A palavra EXEMPLAR ficaria então da seguinte forma:

$$\text{EXEMPLAR} \leftrightarrow 5\ 24\ 5\ 13\ 16\ 12\ 1\ 18 \tag{6.2}$$

Quando associamos estes números com o texto original da palavra EXEMPLAR, chamamos esta sequência de números de *código* numérico associado ao texto original. O processo de mudança de letras para números é chamado *codificação*, assim como a mudança de número para letras é a *decodificação*.

Voltando ao exemplo, para cifrar a palavra EXEMPLAR usando $b = 3$, adicionamos 3 unidades a cada número em 6.2, e logo depois, transformamos as letras em números.

$$8\ 27\ 8\ 16\ 19\ 15\ 4\ 21 \leftrightarrow \text{H?HPSODU} \tag{6.3}$$

Repare que não temos nehuma letra correspondente ao número 27. Nesta cifra alfabética, quando chegamos letra Z, recomeamos depois com A, isso significa que matematicamente, assim que chegarmos a 26, vamos começar de novo do 1. Isto é, $27 \equiv 1$. Temos então

$$8\ 1\ 8\ 16\ 19\ 15\ 4\ 21 \leftrightarrow \text{HAHPSODU} \tag{6.4}$$

Assim, o texto cifrado é HAHPSODU, que é o mesmo encontrado em 6.1.

Para decifrar, usamos o mesmo processo. Por exemplo, suponhamos que queremos decifrar o texto LROAJ que está cifrado usando como chave $b = 9$. Primeiramente convertemos as letras em números:

$$\text{LROAJ} \leftrightarrow 12\ 18\ 15\ 1\ 10 \tag{6.5}$$

Para decifrar, adicionamos $26 - 9 = 17$ a cada número de 6.5:

$$29\ 35\ 32\ 18\ 27 \tag{6.6}$$

Utilizando congruência módulo 26 em 6.6:

$$3\ 9\ 6\ 18\ 1 \leftrightarrow \text{CIFRA}$$

Chegamos então que LROAJ é a palavra CIFRA cifrada.

Note que para decifrar somamos $26 - 9 = 17$ a cada número de 6.5, porém podemos também subtrair 9 de cada elemento que chegaremos na mesma resposta:

$$3\ 9\ 6\ \text{-}8\ 1$$

Como $-8 \equiv 18 \pmod{26}$, chegamos no mesmo que 3 9 6 18 1, que é a palavra CIFRA.

Descrevendo matematicamente a Cifra de César, começamos escolhendo um número b entre 1 e 25, inclusive. Para cifrar, encontramos seu código numérico, adicionamos b a ele, reduzimos módulo 26, e então decodificamos.

Iremos usar a seguinte notação: P representa o código numérico de um texto original e C o código numérico do texto cifrado. Quando ciframos um texto original usando um deslocamento de cifragem b, temos

$$C \equiv P + b \pmod{26}$$

ou equivalentemente

$$P + b \equiv C \pmod{26} \tag{6.7}$$

Para podermos decifrar uma mensagem cifrada, precisamos encontrar a chave, deslocamento de cifragem, encontrando P em 6.7, isto é

$$P \equiv C - b \equiv C + (26 - b) \pmod{26} \tag{6.8}$$

Vemos em 6.8 que o deslocamento para decifrar é $26 - b$. Apesar de já conhecermos esta informação, 6.8 nos diz a razão de isto acontecer. Esta congruência também nos mostra como podemos ver a decifração de duas maneiras diferentes: somando $26 - b$ ou subtraindo b

Usar a Cifra de César é muito simples, basta algum conhecimento elementar de aritmética. Mas infelizmente esse método não é seguro. A criptoanálise, ciência que estuda métodos de decifrar uma mensagem sem ser um usuário legítmo, resolve facilmente uma Cifra de César.

6.3 Cifra com Matrizes

Nesta seção, mostraremos como criar cifras baseadas no uso de matrizes com elementos em $\mathbb{Z}_{26}$. O primeiro passo é transformar as letras das palavras em números, ou seja, vamos colocar as letras do alfabeto em correspondência 1 a 1 com os inteiros de 1 a 26, que representam as classes de equivalência em $\mathbb{Z}_{26}$. Note que usamos os números de 1 a 26 para representar as classes de equivalência módulo 26. Temos então

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Como $\mathbb{Z}_{26}$ é um anel comutativo podemos formar colunas de vetores dos elementos de $\mathbb{Z}_{26}$ e matrizes $n \times n$ com entradas em $\mathbb{Z}_{26}$ e podemos ainda multiplicar vetores por matrizes e matrizes de tamanhos adequados. Muitas vezes, podemos e será necessário, encontrar a inversa de uma matriz $n \times n$. É importante anotar que o fato de uma matriz A $n \times n$ com entradas em um anel comutativo R tem inversa B com entradas em R se e somente se o determinante de A tem inverso em R.

As cifras podem envolver matrizes de vários tamanhos. Iremos ilustrá-las com um exemplo, sendo que não usaremos a acentuação das palavras. Seja a mensagem

TEORIA DOS NUMEROS

onde colocaremos um X nos espaços entre as palavras.

TEORIAXDOSXNUMEROS

Escrevemos então a mensagem como uma sequência de números usando a correspondência da tabela anterior

20 5 15 18 9 1 24 4 15 19 24 14 21 13 5 18 15 19

ou mais facilmente, usando congruência módulo 26 podemos escrever

-6 5 -11 -8 9 1 -2 4 -11 -7 -2 -12 -5 13 5 -8 -11 -7 (6.9)

Usaremos este exemplo para montar cifras de matrizes dos tipos 1×1 e 2×2.

Códigos da forma 1×1

Começamos tomando um elemento inversível de $\mathbb{Z}_{26}$, como por exemplo 5 ($\text{mdc}(5, 26) = 1$). Então multiplicamos cada elemento de 6.9 por 5 e encontramos

-30 25 -55 -40 45 5 -10 20 -55 -35 -10 -60 -25 65 25 -40 -55 -35

ou então, usando novamente congruência módulo 26 chegamos a

$$22\ 25\ 23\ 12\ 19\ 5\ 16\ 20\ 23\ 17\ 16\ 18\ 1\ 13\ 25\ 12\ 23\ 17 \tag{6.10}$$

Transformando os números de volta em letras temos

$$\text{VYWLSEPTWQPRAMYLWQ} \tag{6.11}$$

que é o texto cifrado.

Para decodificar a mensagem recebida, basta transformar 6.11 em números e depois multiplicar cada número por -5, que resultará na sequência da mensagem original, pois $5(-5) \equiv 1 \pmod{26}$, portanto -5 é o inverso de 5.

Este tipo de código é facilmente quebrado, pois cada letra sempre terá o mesmo correspondente. Neste exemplo, o S sempre estará sendo substituído pelo Q, ou seja, sempre corresponderá a uma mesma letra no código, e um criptoanalista pode facilmente decifrar a mensagem e o código.

Porém, o próximo tipo já torna muito mais difícil a quebra do código.

Códigos da forma 2×2

Neste caso, começamos montando matrizes da forma 2x1, com dois números que estão um ao lado do outro em 6.9 como seus elementos:

$$\begin{pmatrix} -6 \\ 5 \end{pmatrix}\begin{pmatrix} -11 \\ -8 \end{pmatrix}\begin{pmatrix} 9 \\ 1 \end{pmatrix}\begin{pmatrix} -2 \\ 4 \end{pmatrix}\begin{pmatrix} -11 \\ -7 \end{pmatrix}\begin{pmatrix} -2 \\ -12 \end{pmatrix}\begin{pmatrix} -5 \\ 13 \end{pmatrix}$$

$$\begin{pmatrix} 5 \\ -8 \end{pmatrix}\begin{pmatrix} -11 \\ -7 \end{pmatrix}$$

Para codificar, multiplicamos cada matriz por outra matriz A 2×2 inversível.

Tomemos

$$A = \begin{pmatrix} 8 & 13 \\ -5 & -8 \end{pmatrix}$$

O determinante desta matriz A é 1, e mdc$(1, 26) = 1$. Então temos

$$A^{-1} = \begin{pmatrix} -8 & -13 \\ 5 & 8 \end{pmatrix}$$

A mensagem codificada é a multiplicação de cada matriz 2×1 dada acima por A:

$$\begin{pmatrix} 17 \\ -10 \end{pmatrix} \begin{pmatrix} -16 \\ 9 \end{pmatrix} \begin{pmatrix} 85 \\ -53 \end{pmatrix} \begin{pmatrix} 36 \\ -22 \end{pmatrix} \begin{pmatrix} -179 \\ 111 \end{pmatrix} \begin{pmatrix} -172 \\ 106 \end{pmatrix} \begin{pmatrix} 129 \\ -79 \end{pmatrix}$$

$$\begin{pmatrix} -64 \\ 39 \end{pmatrix} \begin{pmatrix} -179 \\ 111 \end{pmatrix}$$

Colocando os números obtidos anteriormente em ordem, temos a sequência:

17 -10 -16 9 85 -53 36 -22 -179 111 -172 106 129 -79 -64 39 -179 111

Novamente usando a congruência (mod 26) temos

$$17\ 16\ 10\ 9\ 7\ 25\ 10\ 4\ 3\ 7\ 10\ 2\ 25\ 25\ 14\ 13\ 3\ 7 \tag{6.12}$$

Desse modo, a mensagem codificada ficaria assim

QPJIGYJDCGJBYYNMCG

Repare que a letra O está sendo substituída por J e por C também. Para decodificar, basta fazer o caminho inverso, multiplicando 6.12 por A^{-1} e mudando os números encontrados para letras.

Podemos também criar códigos da forma 3×3 ou 5×5, a diferença é que na primeira separamos a sequência em vetores com 3 elementos, formando matrizes da forma 3×1, e na segunda separamos em vetores com 5 elementos, formando matrizes 5×1. Em todos os casos, se ocorrer de faltar elementos na última matriz, completamos com a letra X.

Capítulo 7

Criptografia RSA

7.1 Introdução

Chegamos agora ao capítulo final, onde descreveremos o método RSA, além de entender porque ele funciona.

Este método de chave pública é o mais conhecido. Para podermos utilizar o RSA, precisamos de dois parâmetros: dois números primos, que chamaremos de p e q. Para codificar uma mensagem, precisamos conhecer o produto de p e q, que chamamos de n. Para decodificar uma mensagem, precisamos conhecer p e q.

7.2 Pré-Codificação

A primeira etapa a ser feita é converter a mensagem em uma sequência numérica. Para facilitar o entendimento, usaremos como mensagem original texto com palavras apenas, sem números e também sem o uso de acentos.

Nesta etapa, vamos converter as letras em números usando 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

No texto, substituiremos o espaço entre duas palavras pelo número 99. Por exemplo, a frase *Criptografia RSA* é convertida em

12271825292416271015181099272810

Note que cada letra é substuída por um número de dois algarismos. Fazemos isso para evitar ambiguidades. Se fizessemos A corresponder ao 1, B ao 2 e assim por diante, e encontrássemos o 13 em uma sequência, ele poderia corresponder à letra M ou então a AC.

Como dissemos anteriormente, precisamos de dois primos distintos, os quais denotaremos p e q, que serão os parâmetros do sistema RSA, e seja $n = p \cdot q$. O próximo passo é "quebrar" a sequência de números encontrada anteriormente em blocos, de modo que eles sejam números menores que n. Por exemplo, se escolhermos $p = 13$ e $q = 17$, então $n = 221$. A mensagem convertida acima, pode ser quebrada nos seguintes blocos:

$$122 - 71 - 82 - 52 - 92 - 41 - 6 - 27 - 101 - 51 - 8 - 109 - 92 - 7 - 28 - 10$$

Os blocos podem ser escolhidos de várias maneiras diferentes, mas algumas precauções devem ser tomadas:

(1) Os blocos não podem começar em 0

(2) Os blocos em que a mensagem foi quebrada não podem corresponder a nenhuma unidade linguística - palavra, letra ou qualquer outra

No primeiro caso, evitamos problemas na hora de decodificar, já a segunda evita a decodificação por contagem de frequência.

7.3 Codificando e Decodificando

Codificação

Para podermos codificar uma mensagem, vamos precisar de inteiros positivos n e e tais que e seja inversível módulo $\varphi(n)$, ou seja, $\text{mdc}(e, \varphi(n)) = 1$. Recordemos que vimos em 3.18 que $\varphi(n)$ corresponde à quantidade de números naturais entre 0 e $n - 1$ que são primos com n.

Vamos precisar de algumas propriedades da função de Euler φ. Sejam r e s inteiros positivos tais que $\text{mdc}(r, s) = 1$. Temos

$$\varphi(rs) = \varphi(r)\varphi(s)$$

Além disso, se p é primo e e é um inteiro positivo, então $\varphi(p^e) = p^{e-1}(p-1)$. Lembremos também que para todo inteiro $r \geq 2$ vale a decomposição canônica

$$r = p_1^{e_1} \cdots p_k^{e_k}$$

onde $p_1 < \cdots < p_k$ são primos. Então

$$\varphi(r) = \varphi(p_1^{e_1}) \cdots \varphi(p_k^{e_k})$$

logo

$$\varphi(r) = p_1^{e_1-1} \cdots p_k^{e_k-1}(p_1 - 1) \cdots (p_k - 1)$$

Portanto, dados os primos p e q e $n = pq$, facilmente achamos $\varphi(n)$, pois

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

O par (n,e) será chamado de *chave de codificação* do sistema RSA.

O próximo passo será codificar cada bloco encontrado na pré codificação separadamente, e a mensagem codificada será a sequência dos blocos codificados. Porém, é importante saber que os blocos já codificados não podem ser agrupados, caso contrário será impossível decodificar a mensagem.

Seja b um bloco que queremos codifcar. Sabemos que b é inteiro positivo menor que n. Chamaremos o bloco codificado de $C(b)$, e será calculado da seguinte forma:

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

ou seja, $C(b)$ é a forma reduzida de b^e módulo n.

No exemplo, utilizamos $p = 13$ e $q = 17$, e $n = 221$, assim $\varphi(n) = (13-1)(17-1) = 192$. Podemos escolher $e = 5$, que é o menor primo para que $\text{mdc}(e, 192) = 1$. Desta maneira, o bloco 122 da mensagem anterior codificado se transforma no resto da divisão de 122^5 por 221. Como $122^5 \equiv 5 \pmod{221}$, temos então que $C(122) = 5$.

Dessa forma podemos codificar toda a mensagem acima. O resultado é:

$$5-158-114-52-79-45-41-40-186-51-60-96-79-11-214-108$$

Decodificação

Para decodificar um bloco da mensagem codificada, necessitamos dos números n e o inverso de e mod $\varphi(n)$, que chamaremos de d. O par (n,d) será denotado *chave de decodificação*.

Seja a um bloco da mensagem codificada, então $D(a)$ será o resultado do processo de decodificação

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

ou seja, $D(a)$ é a forma reduzida de a^d módulo n.

Para calcular d, basta conhecer $\varphi(n)$ e e, e aplicar 1.10, que é o algoritmo euclidiano estendido.

No exemplo, $\varphi(n) = 192$ e $e = 5$. Queremos encontrar α e β tais que $192 \cdot \alpha + 5 \cdot \beta = 1$. Aplicando o algoritmo euclidiano estendido, chegamos a:

$$192 \cdot (-2) + 5 \cdot 77 = 1$$

donde obtemos que $5 \cdot 77 \equiv 1 \pmod{192}$, logo o inverso de 5 módulo 192 é 77. Assim, para decodificar o bloco 5 da mensagem codificada, achamos a forma reduzida de 5^{77} módulo 221. Como $5^{77} \equiv 122 \pmod{221}$, chegamos ao bloco inicial, que é 122.

Note que se b é um bloco original da mensagem, temos que ter $D(C(b)) = b$, ou seja, decodificando um bloco codificado, temos que encontrar o bloco correspondente da mensagem original.

7.4 Explicação do método

Queremos provar aqui, que decodificando um bloco codificado, obtemos novamente o bloco correspondente da mensagem original. Suponhamos que temos p e q como parâmetros de nosso sistema RSA, e $n = pq$. Os dados de codificação serão n e e, e os dados de decodificação, n e d. Queremos mostrar que $DC(b) = b$. Porém, basta apenas mostrar que $DC(b) \equiv b \pmod{n}$, pois tanto $DC(b)$ quanto b estão entre 1 e $n - 1$, logo só podem ser congruentes módulo n se são iguais. Por este motivo temos que escolher $b < n$ e também temos que manter os blocos separados mesmo após a codificação.

Por definição, temos que:

$$DC(b) \equiv (b^e)^d \equiv b^{ed} \pmod{n} \tag{7.1}$$

Sabemos que d é o inverso de e módulo $\varphi(n)$, então $ed \equiv 1 \pmod{\varphi(n)} \Rightarrow ed = 1 + k\varphi(n)$, para algum inteiro k. Observe que e e d são inteiros maiores que 2 e $\varphi(n) > 0$, então $k > 0$. Substituindo em 7.1

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv (b^{\varphi(n)})^k b \pmod{n}$$

Vimos que p e q são primos distintos. Calcularemos a forma reduzida de b^{ed} módulo p e módulo q.

Temos que

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

logo

$$b^{ed} \equiv b(b^{p-1})^{k(q-1)} \pmod{p}$$

Vamos agora usar o teorema de Fermat, mas para isto precisamos supor que p não divide b.

Suponhamos então que $p \nmid b$, então por Fermat $b^{p-1} \equiv 1 \pmod{p}$, e obtemos assim $b^{ed} \equiv b \pmod{p}$.

Agora, se p divide b, temos também por hipótese que p é primo. Assim, neste caso $b \equiv 0 \pmod{p}$ e a congruência é verificada. Deste modo, $b^{ed} \equiv b \pmod{p}$ para qualquer b.

O argumento para calcular a forma reduzida de b^{ed} módulo q é análogo. Ou seja, $b^{ed} \equiv b \pmod{q}$.

Desta maneira, $b^{ed} - b$ é divisível por p e por q. Como p e q são primos distintos, $\text{mdc}(p, q) = 1$, então pq divide $b^{ed} - b$. Logo, como $n = pq$, então $b^{ed} \equiv b \pmod{n}$ para qualquer valor de b.

Referências Bibliográficas

[1] Coutinho, S. C., *Números Inteiros e Criptografia.* Série de Computação e Matemática. Rio de Janeiro, Sociedade Brasileira de Matemática e Instituto de Matemática Pura e Aplicada, 1997.

[2] Hefez, A., *Elementos de Aritmética.* Coleção Textos Universitários. Rio de Janeiro, Sociedade Brasileira de Matemática, 2005.

[3] Santos, J.P.O., *Introdução à Teoria dos Números.* Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 1998.

[4] Childs, L., *A Concrete Introduction to Higher Algebra.* New York, Springer-Verlag, 1979.

[5] Young, A. L., *Mathematical Ciphers: from Cesar to RSA.* Providence: American Mathematical Society, 2006.

[6] Domingues, H. H., *Fundamentos de Aritmética.* São Paulo, Atual, 1991.

[7] Yan, S., *Number Theory for Computing.* New York, Springer, 2000.

[8] Ribenboim, P., *Números Primos: Mistérios e recordes.* Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2001.

Índice geral