CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS - CEFET

Departamento de Matemática

Uma Pequena Introdução à Teoria dos números e Criptografia RSA

Belo Horizonte, 2026

Conteúdo

1 Introdução

Estas notas têm como objetivo apresentar os conceitos fundamentais de Teoria dos Números e de Teoria de Grupos necessários para a compreensão do funcionamento do sistema criptográfico RSA. Não se pretende desenvolver uma abordagem completa dessas áreas da Matemática, mas sim reunir os resultados essenciais que servirão de base para o estudo do algoritmo.

Ao longo do texto, são abordados tópicos como divisibilidade, algoritmo da divisão euclidiana, máximo divisor comum, aritmética modular, o Pequeno Teorema de Fermat e conceitos básicos de grupos. Esses conteúdos constituem o mínimo necessário para compreender a geração de chaves, o processo de cifragem e decifragem, bem como a justificativa matemática da corretude do RSA.

O material foi organizado de forma gradual, buscando conciliar o rigor matemático com uma apresentação acessível, de modo que o leitor possa acompanhar os fundamentos teóricos antes de estudar os aspectos computacionais e criptográficos do algoritmo RSA.

2 Teoria dos números

2.1 Números inteiros

Para entender como funciona a criptografia RSA precisamos entender um pouco sobre teoria dos Números. Nessa seção começaremos descrevendo o conjunto dos números naturais e inteiros e o conceito de divisão de números inteiros.

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

é o conjunto dos números naturais.

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

é o conjunto dos números inteiros.

Dados $a, b \in \mathbb{Z}$, dizemos que a divide b, ou que a é um divisor de b, e denotamos por

$$a \mid b$$

se existir $c \in \mathbb{Z}$ tal que

$$b = a \cdot c.$$

Caso contrário, a não divide b, e denotamos por $a \not\mid b$.

Exemplo 1. a) $2 \mid 26$, pois $26 = 2 \cdot 13$

b) 5 não divide 26, pois não existe $c \in \mathbb{Z}$ tal que $26 = 5 \cdot c$.

c) $-13 \mid 26$, pois $26 = (-13) \cdot (-2)$.

Definição 1. Um número natural n é dito um número primo, se $n \neq 1$ e os únicos divisores naturais de n são 1 e n.

Exemplo 2. a) 5 é um número primo.

b) 12 não é primo, pois além de 1 e 12 como divisores de 12, temos:

$$3 \mid 12, \qquad 4 \mid 12, \qquad 6 \mid 12.$$

2.2 Teorema Fundamental da Aritmética

Teorema 2.1 (**Teorema Fundamental da Aritmética**)**.** Todo número natural maior que 1 ou é primo ou pode ser escrito, de modo único (a menos da ordem dos fatores), como produto de números primos.

Demonstração. Para cada número natural $n > 1$, existem duas possibilidades:

1) n é primo;

2) n não é primo.

- Se n for primo, já temos uma decomposição em fatores primos.
- Se n não for primo, então existem naturais a, b tais que

$$1 < a < n, \qquad 1 < b < n,$$

e

$$n = a \cdot b.$$

Se a e b forem primos, terminamos. Caso contrário, repetimos o processo para qualquer fator que não seja primo. Como os fatores obtidos são sempre menores que n, esse procedimento não pode continuar indefinidamente. Após um número finito de etapas, obtemos uma escrita de n como produto de números primos.

Portanto, todo número natural maior que 1 pode ser escrito como produto de primos. **(Unicidade)** Resta mostrar que essa decomposição é única, exceto pela ordem dos fatores.

Suponha que

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

em que todos os p_i e q_j são primos.

Como p_1 divide o produto $q_1 q_2 \cdots q_s$, pelo Lema de Euclides, p_1 deve dividir algum dos fatores q_j. Como q_j é primo, segue que

$$p_1 = q_j.$$

Reordenando os fatores, podemos supor que $p_1 = q_1$. Cancelando esse fator em ambos os lados, obtemos

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Repetindo o argumento sucessivamente, concluímos que

$$r = s$$

e, após uma reordenação dos fatores,

$$p_i = q_i, \qquad i = 1, \ldots, r.$$

Logo, a decomposição de um número natural maior que 1 em fatores primos é única, a menos da ordem dos fatores.

□

Exemplo 3.

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2.$$

Observe que as três decomposições diferem apenas pela ordem dos fatores.

2.3 Divisão Euclidiana

Teorema 2.2. Sejam a e b dois números inteiros, com $b \neq 0$. Então existem únicos inteiros q e r tais que

$$a = bq + r,$$

com

$$0 \leq r < |b|.$$

Os números q e r são chamados, respectivamente, de **quociente** e **resto** da divisão de a por b.

Exemplo 4. Dividindo 28 por 5, obtemos

$$28 = 5 \cdot 5 + 3.$$

Assim,

$$a = 28, \qquad b = 5, \qquad q = 5, \qquad r = 3.$$

Note que

$$0 \leq 3 < 5,$$

como exige o teorema.

Exemplo 5. Efetuando a divisão euclidiana de -46 por 7, procuramos inteiros q e r tais que

$$-46 = 7q + r, \qquad 0 \leq r < 7.$$

Temos

$$-46 = 7(-7) + 3.$$

Logo,

$$q = -7 \quad \text{e} \quad r = 3.$$

Lema 1 (**Lema de Euclides**). Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então

$$p \mid a \quad \text{ou} \quad p \mid b.$$

Teorema 2.3 (**Teorema de Euclides**). Existem infinitos números primos.

Demonstração. Faremos uma demonstração por absurdo.

Suponha que existam apenas finitos números primos, a saber,

$$p_1, p_2, \ldots, p_k.$$

Considere o número

$$N = p_1 p_2 \cdots p_k + 1.$$

Observe que, para cada $i = 1, \ldots, k$,

$$N = p_1 p_2 \cdots p_k + 1 \equiv 1 \pmod{p_i}.$$

Logo,

$$p_i \nmid N$$

para todo $i = 1, \ldots, k$.

Portanto, N não é divisível por nenhum dos primos da lista. Como todo número maior que 1 é primo ou possui um divisor primo (Teorema Fundamental da Aritmética), concluímos que:

- ou N é primo;
- ou N possui um divisor primo que não pertence à lista $p_1, p_2, \ldots, p_k$.

Em ambos os casos obtemos um primo que não estava na lista inicial, o que contradiz a hipótese de que todos os primos já haviam sido enumerados.

Logo, existem infinitos números primos.

□

2.4 Restos possíveis na divisão por n

Dado um número natural n, ao efetuarmos a divisão euclidiana de um inteiro por n, os únicos restos possíveis são

$$0, 1, 2, \ldots, n-1.$$

Exemplo 6. Os únicos restos possíveis na divisão por 4 são

$$0,\ 1,\ 2,\ \text{e}\ 3.$$

Consequentemente, todo número inteiro pode ser escrito em uma das seguintes formas:

$$4k,$$

$$4k+1,$$

$$4k+2,$$

$$4k+3,$$

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

Exemplo 7 (Quadrados perfeitos módulo 4). Mostremos que todo quadrado perfeito deixa resto 0 ou 1 quando dividido por 4.

Como qualquer inteiro a é da forma $4k$, $4k+1$, $4k+2$ ou $4k+3$, analisamos os quatro casos.

Caso 1: $a = 4k$

$$a^2 = (4k)^2 = 16k^2 = 4(4k^2).$$

Portanto, a^2 deixa resto 0 na divisão por 4.

Caso 2: $a = 4k+1$

$$a^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1.$$

Logo, a^2 deixa resto 1 na divisão por 4.

Caso 3: $a = 4k+2$

$$a^2 = (4k+2)^2 = 16k^2 + 16k + 4 = 4(4k^2 + 4k + 1).$$

Portanto, a^2 deixa resto 0 na divisão por 4.

Caso 4: $a = 4k + 3$

$$a^2 = (4k + 3)^2 = 16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1.$$

Logo, a^2 deixa resto 1 na divisão por 4.

Concluímos que todo quadrado perfeito é da forma

$$4k \quad \text{ou} \quad 4k + 1.$$

Em particular, se um número deixa resto 2 ou 3 quando dividido por 4, então ele não pode ser um quadrado perfeito.

2.5 Aritmética dos Restos

Observe que, ao somar um número da forma $4k + 2$ com um número da forma $4q + 3$, obtemos

$$(4k + 2) + (4q + 3) = 4(k + q) + 5 = 4(k + q) + 4 + 1 = 4(k + q + 1) + 1.$$

Portanto, a soma deixa resto 1 na divisão por 4.

De maneira semelhante, o resto da divisão por 4 de um produto pode ser determinado pelos restos dos fatores.

Por exemplo,

$$(4k + 2)(4q + 3) = 16kq + 12k + 8q + 6.$$

Colocando 4 em evidência,

$$(4k + 2)(4q + 3) = 4(4kq + 3k + 2q + 1) + 2.$$

Assim, o produto deixa resto 2 na divisão por 4.

Seja m um número natural. Dizemos que dois números inteiros são congruentes módulo m, e escrevemos

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

se a e b deixam o mesmo resto na divisão por m.

Exemplo 8.

$$39 \equiv 10 \pmod{29} \quad \text{ou} \quad 29 \mid 39 - 10$$

$$29 \equiv 11 \pmod{6} \quad \text{ou} \quad 6 \mid 29 - 11$$

$$38 \not\equiv 15 \pmod 3 \quad \text{ou} \quad 3 \text{ não divide } 38 - 15$$

Uma forma equivalente de definir é

$$a \equiv b \pmod m, \text{ se, e somente se, } m \mid (a - b)$$

Dado $m \in \mathbb{N}$, os números inteiros podem ser separados em classes quanto ao seu resto na divisão por m. Haverão m classes:

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}$$

em que,

$$\overline{0} = \{\ldots, -m, 0, m, 2m, \ldots\}$$

$$\overline{1} = \{\ldots, -m+1, 1, m+1, 2m+1, \ldots\}$$

$$\vdots$$

$$\overline{m-1} = \{\ldots, -m-1, -1, m-1, 2m-1, 3m-1, \ldots\}$$

Dadas as classes módulo, podemos definir uma soma e um produto (que na verdade são as operações herdadas de $\mathbb{Z}$).

Exemplo 9. Módulo 4, temos as classes $\overline{0}, \overline{1}, \overline{2}, \overline{3}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Exercício 1. Faça as tabelas de $+$ e $\cdot$ para as classes módulo 6, módulo 7 e módulo 12.

Propriedade

A relação $a \equiv b \pmod{m}$ tem as seguintes propriedades:

1. (*Reflexiva*) $a \equiv a \pmod{m}$
2. (*Simétrica*) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$
3. (*Transitiva*) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$

Uma relação com estas 3 propriedades é uma relação de equivalência.
Dado n, vamos denotar por $\mathbb{Z}_n$ o conjunto das classes de equivalência módulo n.

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \quad \text{em que} \quad \overline{a} = \{a + kn \mid k \in \mathbb{Z}\}$$

Geralmente representamos $\overline{a}$ usando o menor a natural possível, isto não é necessário.
Em $\mathbb{Z}_{15}$ temos que, $\overline{2} = \overline{17}$ pois

$$\overline{2} \cdot \overline{7} = \overline{14} \quad \text{e} \quad \overline{17} \cdot \overline{12} = \overline{14}$$

Exemplo 10. Calcule o resto na divisão por 7 de 10^{135}.

Primeiramente observemos o que acontece com as classes das potências de 10.

$$10 \equiv 3 \pmod{7} \quad \text{ou} \quad \overline{10} = \overline{3}$$

$$\overline{10} = \overline{3}$$

$$\overline{10}^2 = \overline{10} \cdot \overline{10} = \overline{3} \cdot \overline{3} = \overline{9} = \overline{2}$$

$$\overline{10}^3 = \overline{10} \cdot \overline{10} \cdot \overline{10} = \overline{2} \cdot \overline{3} = \overline{6}$$

$$\overline{10}^4 = \overline{10}^3 \cdot \overline{10} = \overline{6} \cdot \overline{3} = \overline{4}$$

$$\overline{10}^5 = \overline{10}^4 \cdot \overline{10} = \overline{4} \cdot \overline{3} = \overline{5}$$

$$\overline{10}^6 = \overline{5} \cdot \overline{3} = \overline{1}$$

$$\overline{10}^7 = \overline{3}$$

$$\overline{10}^8 = \overline{2}$$

Como $\overline{10}^6 = \overline{1}$ e $135 = 22 \cdot 6 + 3$:

$$10^{135} = (10^6)^{22} \cdot 10^3 \equiv 1^{22} \cdot 10^3 \pmod{7}$$

$$1^{22} \cdot 10^3 = \overline{10}^3 = \overline{6}$$

Logo $10^{135} \equiv 6 \pmod 7$ e, portanto, o resto é 6.

Exemplo 11. Encontre o resto na divisão de 3^{64} por 31.

$$3^2 \equiv 9 \pmod{31}$$

$$3^3 \equiv 27 \pmod{31} \quad \text{ou} \quad 3^3 \equiv -4 \pmod{31}$$

Como $64 = 3 \cdot 21 + 1$:

$$3^{64} = 3^{3\cdot 21+1} = 3^{3\cdot 21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv -4^{21} \cdot 3 \pmod{31}$$

$$\equiv -2^{42} \cdot 3 \pmod{31}$$

Como $2^5 = 32 \equiv 1 \pmod{31}$, então:

$$-(2^{42}) \cdot 3 \equiv -2^2 \cdot 3 \equiv -12 \equiv 19 \pmod{31}$$

Exemplo 12. Calcule o resto de 6^{35} na divisão por 16.

$$6^4 = 2^4 \cdot 3^4 = 16 \cdot 8^4 \equiv 0 \pmod{16}$$

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

Inverso

Dado $\overline{a} \in \mathbb{Z}_n$, dizemos que $\overline{b} \in \mathbb{Z}_n$ é um inverso de $\overline{a}$ se

$$\overline{a} \cdot \overline{b} = \overline{1}$$

Exemplo 13. Em $\mathbb{Z}_4$, temos que, $\overline{1} \cdot \overline{1} = \overline{1}$ e $\overline{3} \cdot \overline{3} = \overline{1}$

Exemplo 14. Em $\mathbb{Z}_7$

$$\overline{1} \cdot \overline{1} = \overline{1} \Rightarrow \overline{1} \text{ é inverso de } \overline{1}$$
$$\overline{2} \cdot \overline{4} = \overline{1} \Rightarrow \overline{4} \text{ é inverso de } \overline{2}$$
$$\overline{3} \cdot \overline{5} = \overline{1} \Rightarrow \overline{5} \text{ é inverso de } \overline{3}$$
$$\overline{6} \cdot \overline{6} = \overline{1} \Rightarrow \overline{6} \text{ é inverso de } \overline{6}$$

2.6 Máximo Divisor Comum

Lema 2. Dados a, b inteiros, então mdc$(a, b) =$ mdc$(a, b + a)$.

Exemplo 15.

$$\text{mdc}(30, 24) = \text{mdc}(30 - 24, 24) = \text{mdc}(6, 24) = \text{mdc}(6, 0) = 6$$

Algoritmo de Euclides

Dados $a, b \in \mathbb{Z}$, para encontrar mdc(a, b) basta fazer:

$$a = q_1 \cdot b + r_1$$

$$\text{mdc}(a, b) = \text{mdc}(a - q_1 b, b) = \text{mdc}(r_1, b) = \text{mdc}(b, r_1)$$

Continuando o processo:

$$b = q_2 \cdot r_1 + r_2$$

$$\vdots$$

$$r_{n-2} = q_n \cdot r_{n-1} + r_n \quad \text{onde } r_n = 0$$

Então:

$$\text{mdc}(a, b) = \text{mdc}(r_{n-1}, 0) = r_{n-1}$$

Exemplo 16.

$$\text{mdc}(51, 6) = \text{mdc}(45, 6) = \ldots = \text{mdc}(3, 6) = 3$$

Exemplo 17.

$$\text{mdc}(154, 30) = \text{mdc}(30, 4) = \text{mdc}(4, 2) = 2$$

As divisões sucessivas correspondentes são:

154	30	30	4	4	2
4	5	2	7	0	2

Exemplo 18. Vamos calcular o mdc de 10 e 25 usando o algoritmo de Euclides.

$$25 = 2 \cdot 10 + 5$$

$$10 = 2 \cdot 5 + 0$$

Logo,

$$\text{mdc}(25, 10) = \text{mdc}(10, 5) = \text{mdc}(5, 0) = 5.$$

Além disso,

$$10 = 5 \cdot 2 + 0$$

$$25 = 2 \cdot 10 + 5$$

Substituindo, obtemos

$$5 = 1 \cdot 25 - 2 \cdot 10.$$

Teorema 2.4. O mdc(a, b) é o menor natural que pode ser escrito na forma $k_1 a + k_2 b$, com $k_1, k_2 \in \mathbb{Z}$.

Dois números a e b são ditos primos entre si, ou coprimos, se

$$\text{mdc}(a, b) = 1.$$

Pelo teorema anterior, a e b são primos entre si se, e somente se, existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$k_1 a + k_2 b = 1.$$

Exemplo 19. Aplicando o algoritmo de Euclides:

$$1000 = 76 \cdot 13 + 12$$

$$13 = 1 \cdot 12 + 1$$

$$12 = 12 \cdot 1 + 0$$

Logo,

$$\text{mdc}(1000, 13) = \text{mdc}(13, 12) = \text{mdc}(12, 1) = 1.$$

Além disso,

$$1 = 1 \cdot 13 - 1 \cdot 12$$

e

$$12 = 1000 - 76 \cdot 13.$$

Substituindo,

$$1 = 13 - (1000 - 76 \cdot 13)$$

$$1 = 13 - 1000 + 76 \cdot 13$$

$$1 = 77 \cdot 13 - 1000.$$

Assim,

$$k_1 = 77 \qquad \text{e} \qquad k_2 = -1.$$

Em $\mathbb{Z}_n$, nem todo elemento possui inverso multiplicativo.

Exemplo 20. Em $\mathbb{Z}_6$, a classe $\overline{2}$ não possui inverso.

Se

$$\overline{a}\,\overline{b} = \overline{1} \quad \text{em } \mathbb{Z}_n,$$

então existem inteiros k e q tais que

$$(a + kn)(b + qn) = 1 + rn.$$

Desenvolvendo,

$$ab + (aq + kb + kqn)n = 1 + rn.$$

Portanto,

$$ab + \ell n = 1$$

para algum $\ell \in \mathbb{Z}$. Assim,

$$\text{mdc}(a, n) = 1 \qquad \text{e} \qquad \text{mdc}(b, n) = 1.$$

Em $\mathbb{Z}_6$, as únicas classes coprimas com 6 são

$$\overline{1} \quad \text{e} \quad \overline{5}.$$

De fato,

$$\overline{1} \cdot \overline{1} = \overline{1}$$

e

$$\overline{5} \cdot \overline{5} = \overline{1}.$$

Exemplo 21. Em $\mathbb{Z}_8$, temos

$$\overline{1},\ \overline{3},\ \overline{5},\ \overline{7}.$$

Além disso,

$$\overline{1} \cdot \overline{1} = \overline{1},$$

$$\overline{3} \cdot \overline{3} = \overline{1},$$

$$\overline{5} \cdot \overline{5} = \overline{1},$$

$$\overline{7} \cdot \overline{7} = \overline{1}.$$

Em $\mathbb{Z}_{10}$, as classes inversíveis são

$$\overline{1},\ \overline{3},\ \overline{7},\ \overline{9}.$$

De fato,

$$\overline{1} \cdot \overline{1} = \overline{1},$$

$$\overline{3} \cdot \overline{7} = \overline{1},$$

$$\overline{9} \cdot \overline{9} = \overline{1}.$$

Se a classe $\overline{a} \in \mathbb{Z}_n$ não possui inverso e $0 < a < n$ com

$$\text{mdc}(a, n) \neq 1,$$

então

$$\left(\frac{n}{\text{mdc}(a, n)} \right) \overline{a} = \overline{0}.$$

Logo, todo elemento de $\mathbb{Z}_n$ que não possui inverso multiplicativo é um divisor de zero.

Isto é, existem classes não nulas $\overline{a}$ e $\overline{b}$ tais que

$$\overline{a}\,\overline{b} = \overline{0}.$$

Em $\mathbb{Z}_n$, não necessariamente vale a lei do cancelamento, pois nem toda classe possui inverso.

Exemplo 22. Em $\mathbb{Z}_{10}$,

$$\overline{8} \cdot \overline{6} = \overline{8} \cdot \overline{1} = \overline{8},$$

mas

$$\overline{6} \neq \overline{1}.$$

Em $\mathbb{Z}_p$, onde p é primo, a única classe que não possui inverso é

$$\overline{0}.$$

2.7 Pequeno Teorema de Fermat

Teorema 2.5 (Pequeno Teorema de Fermat)**.** Seja a um inteiro e p um número primo. Então

$$a^p \equiv a \pmod{p}.$$

Exemplo 23.

$$10^{13} \equiv 10 \pmod{13}.$$

Lema 3 (Sonho do Calouro)**.** Seja p um número primo e $a, b \in \mathbb{Z}$. Então

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

Demonstração.

Pelo binômio de Newton,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k.$$

Ou seja,

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p.$$

Como p divide

$$\binom{p}{k} \qquad (1 \leq k \leq p-1),$$

segue que todos os termos intermediários são múltiplos de p. Portanto,

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

□

Demonstração do Pequeno Teorema de Fermat
Vamos fixar o primo p e demonstrar por indução em a.
Caso inicial:

$$1^p \equiv 1 \pmod{p}.$$

Hipótese de indução: Suponha que o teorema seja válido para a

$$a^p \equiv a \pmod{p}.$$

Passo indutivo: Mostremos que vale para $a+1$
Pelo lema,

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

Pela hipótese de indução,

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

Logo, a propriedade vale para $a+1$, concluindo a demonstração por indução.

□

Teorema 2.6 (Pequeno Teorema de Fermat (Versão 2))**.** Seja p um primo e a um inteiro não divisível por p. Então,

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

Exemplo 24. Encontre o resto da divisão de $2^{54\,326\,751}$ por 13.

$$54\,326\,751 = 12 \cdot 4\,527\,229 + 3.$$

Pelo Pequeno Teorema de Fermat,

$$2^{12} \equiv 1 \pmod{13}.$$

Assim,

$$2^{54\,326\,751} = 2^{12 \cdot 4\,527\,229 + 3} = \left(2^{12}\right)^{4\,527\,229} \cdot 2^3 \equiv 1^{4\,527\,229} \cdot 2^3 \pmod{13}.$$

Logo,

$$2^{54\,326\,751} \equiv 8 \pmod{13}.$$

Portanto, o resto da divisão de $2^{54\,326\,751}$ por 13 é

$$\boxed{8}.$$

3 Grupos

Um grupo é um conjunto G munido de uma operação $\star$ que associa a cada par de elementos $a, b \in G$ um elemento $a \star b \in G$, satisfazendo as seguintes propriedades:

1. **(Associatividade)** Para quaisquer $a, b, c \in G$,

$$(a \star b) \star c = a \star (b \star c).$$

2. **(Elemento neutro)** Existe $e \in G$ tal que, para todo $a \in G$,

$$a \star e = e \star a = a.$$

3. **(Elemento inverso)** Para todo $a \in G$, existe $a^{-1} \in G$ tal que

$$a \star a^{-1} = a^{-1} \star a = e.$$

Exemplo 25. a) $(\mathbb{Z}, +)$ é um grupo.

b) $(\mathbb{N}, +)$ não é um grupo, pois não possui inverso.

c) $(\mathbb{Q}, +)$ é um grupo.

d) $(\mathbb{Q}^*, \cdot)$ é um grupo.

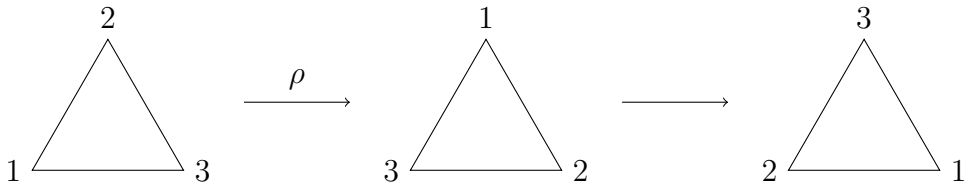
e) $(\mathbb{R}^3, +)$ é um grupo.

f) $(\mathbb{R}^3, \times)$ não é um grupo, pois não possui elemento neutro e a associatividade não é válida.

3.1 Grupo das Simetrias de um Triângulo Equilátero

Considere um triângulo equilátero com vértices rotulados por $1, 2, 3$.

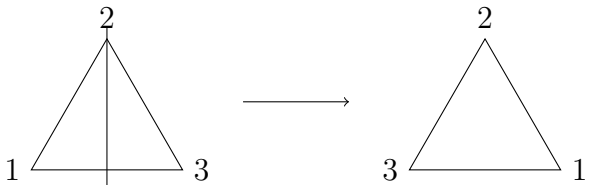
Rotação ρ de 120°



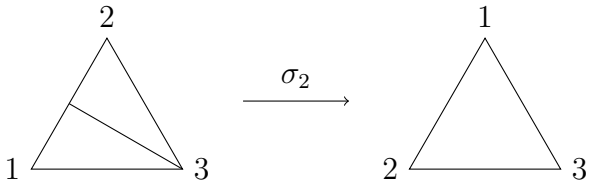
Observamos que

$$\rho^2 = \text{rotação de } 240^\circ, \qquad \rho^3 = e.$$

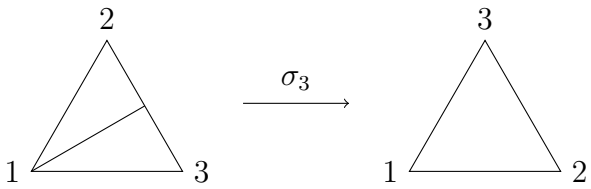
Reflexão σ_1



$\sigma_2 = \rho\sigma_1$



$\sigma_3 = \rho^2\sigma_1$



O conjunto das simetrias do triângulo equilátero é

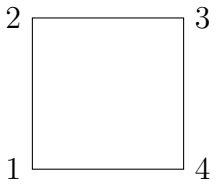
$$D_3 = \{e, \rho, \rho^2, \sigma_1, \sigma_2, \sigma_3\},$$

e forma um grupo com a composição de funções.

Tabela de composição

$\circ$	e	ρ	ρ^2	σ_1	σ_2	σ_3
e	e	ρ	ρ^2	σ_1	σ_2	σ_3
ρ	ρ	ρ^2	e	σ_2	σ_3	σ_1
ρ^2	ρ^2	e	ρ	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	e	ρ^2	ρ
σ_2	σ_2	σ_1	σ_3	ρ	e	ρ^2
σ_3	σ_3	σ_2	σ_1	ρ^2	ρ	e

Exercício 2. Montar a tabela das simetrias de um quadrado.



Exemplo 26. a) O conjunto das matrizes $m \times n$, com a operação de soma, é um grupo.

b) O conjunto das matrizes quadradas invertíveis de ordem n, com a multiplicação de matrizes, forma um grupo multiplicativo.

3.2 Grupos Aritméticos

O subconjunto dos elementos invertíveis de $\mathbb{Z}_n$ forma um grupo com relação à multiplicação.

Exemplo 27.

$$\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \ldots, \overline{9}\}.$$

Os elementos invertíveis de $\mathbb{Z}_{10}$ são

$$U_{10} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}.$$

Note que, se $a, b \in \mathbb{Z}_n$ são invertíveis, então ab também é invertível, pois

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Definição 2. O conjunto U_n é chamado de **grupo aritmético**.

O número de elementos de U_n é denotado por

$$\varphi(n).$$

Definição 3. A função $\varphi(n)$ é chamada de **função de Euler** (ou **função totiente de Euler**).

Em outras palavras, $\varphi(n)$ é a quantidade de inteiros positivos menores que n e que são coprimos com n.

Teorema 3.1. Se m e n são inteiros positivos tais que mdc$(m, n) = 1$, então

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n)$$

Vamos encontrar então uma fórmula para $\phi(n)$.

Se n tem a decomposição como produto de primos

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$$

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

$$\phi(n) = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

Exemplo 28. $\phi(120) = \phi(2^3 \cdot 3 \cdot 5)$
$= (2^3 - 2^2)(3 - 1)(5 - 1)$
$= 4 \cdot 2 \cdot 4 = 32$

$$\phi(120) = 120 \left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 32$$

3.3 Subgrupos

Seja $(G, \star)$ um grupo. Um subgrupo de G é um subconjunto $H \subseteq G$ tal que $(H, \star)$ é um grupo.

Exemplo 29. a) $(\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Q}, +)$

b) $(\mathbb{Z}^*, +)$ não é subgrupo de $(\mathbb{Q}^*, \cdot)$
(operação é diferente)

c) $(\mathbb{Z}^*, \cdot)$ não é subgrupo de $(\mathbb{Q}^*, \cdot)$, pois os elementos de $\mathbb{Z}^*$ não têm inverso multiplicativo e todos os elementos de $\mathbb{Q}^*$ têm inverso multiplicativo.

Todo grupo $(G, \star)$ tem pelo menos dois subgrupos: $(\{e\}, \star)$ e $(G, \star)$, sendo $\{e\}$ o elemento neutro de G.

Exemplo 30. $(\mathbb{Z}_{13}^*, \cdot) = \mathcal{U}(13)$ é um grupo. E $\{\overline{1}, \overline{3}, \overline{9}\}$ é um subgrupo de $\mathcal{U}(13)$, pois é fechado, associativo e o neutro está em $\{\overline{1}, \overline{3}, \overline{9}\}$.

$\overline{1} \cdot \overline{1} = \overline{1}$
$\overline{1} \cdot \overline{3} = \overline{3}$
$\overline{1} \cdot \overline{9} = \overline{9}$
$\overline{3} \cdot \overline{3} = \overline{9}$
$\overline{3} \cdot \overline{9} = \overline{27} = \overline{1}$

Definição 4. Ordem do grupo = n° de elementos.

Teorema 3.2. Em um grupo finito, a ordem de qualquer subgrupo divide a ordem do grupo.

Exemplo 31. No cubo mágico, o número de configurações possíveis é

$$2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11.$$

Além disso,

$$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$$

corresponde à ordem do maior subgrupo cíclico do grupo do cubo mágico.

Se k divide a ordem de G, não necessariamente existe um subgrupo de G de ordem k.

3.4 Subgrupos cíclicos

Seja $(G, \star)$ um grupo finito. Escrevemos:

$$a^k = \underbrace{a \star a \star \cdots \star a}_{k \text{ vezes}}$$

Considere o conjunto:

$$\{e, a, a^2, a^3, a^4, \dots\}$$

como G é finito, este conjunto também é finito.

Se $a^m = a^n$, então multiplicando por a^{-m} ambos os lados da igualdade, obtemos:

$$e = a^{n-m}$$

Se k é o menor natural tal que $a^k = e$, então o conjunto é um subgrupo de G de ordem k. E dizemos que k é a ordem do elemento a.

Exemplo 32. Em $\mathcal{U}(13)$, temos que

$\overline{3} = \overline{3}$
$\overline{3}^2 = \overline{9}$
$\overline{3}^3 = \overline{1}$

Sabemos que $\{\overline{1}, \overline{3}, \overline{9}\}$ é um subgrupo de $\mathcal{U}(13)$ de ordem 3. A ordem do $\overline{3}$ é 3.

E qual a ordem de $\overline{7}$ em $\mathcal{U}(13)$? Observe que:

$\overline{7} = \overline{7}$
$\overline{7}^2 = \overline{10}$
$\overline{7}^3 = \overline{5}$
$\overline{7}^4 = \overline{9}$
$\overline{7}^5 = \overline{11}$
$\overline{7}^6 = \overline{12}$
$\overline{7}^7 = \overline{6}$
$\overline{7}^8 = \overline{3}$
$\overline{7}^9 = \overline{8}$
$\overline{7}^{10} = \overline{4}$
$\overline{7}^{11} = \overline{2}$
$\overline{7}^{12} = \overline{1}$

A ordem do elemento $\overline{7}$ é 12.

Um subgrupo da forma $\{1, a, a^2, \dots\}$ é chamado **subgrupo cíclico** (gerado por a).
Se G é um subgrupo cíclico de G, dizemos que G é um **grupo cíclico**.

Exemplo 33. O grupo das simetrias de um triângulo não é cíclico.

Exemplo 34. No cubo mágico, o número de configurações possíveis é

$$2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11.$$

Além disso,

$$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$$

corresponde à ordem do maior subgrupo cíclico do grupo do cubo mágico.

Teorema 3.3 (Teorema da raiz primitiva:)**.** Se p é um número primo, $\mathcal{U}(p)$ é um grupo cíclico.

Exercício 3. Encontre um elemento em $\mathbb{Z}_{29}^* = \{1, 2, \ldots, 28\}$ que gera o grupo todo.

Teorema 3.4 (Teorema de Euler)**.** Sejam $n > 0$ e a dois números inteiros. Se mdc$(a, n) = 1$, então:

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

Demonstração. Como mdc$(a, n) = 1$, $\overline{a} \in \mathcal{U}(n)$. Logo, a ordem de $\overline{a}$ divide a ordem de $\mathcal{U}(n) = \phi(n)$.

Logo:

$$\overline{a}^{\,\phi(n)} = \overline{a}^{\,k \cdot q} = (\overline{a}^{\,k})^q = \overline{1}^{\,q} = 1$$

(em que k é a ordem de $\overline{a}$), ou seja,

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{c.q.d.}$$

□

Exemplo 35. Se $n = 12$, então

$$\phi(12) = 4$$

$$35^4 \equiv 1 \pmod{12}$$

Teorema 3.5 (Teorema de Wilson)**.** Se p é primo:

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

Demonstração. Dado $a \in \mathbb{Z}$, se p é primo, $(\mathbb{Z}_p^*, \cdot) = \mathcal{U}(p)$ é um grupo de ordem $p - 1$. Considere $a \in \mathbb{Z}_p^*$, $\overline{a}^{-1} \in \mathbb{Z}_p^*$.

Se $\overline{a}^{\,-1} \neq \overline{a}$, então $\overline{a}$ e $\overline{a}^{\,-1}$ aparecem em $\overline{1} \cdot \overline{2} \cdot \overline{3} \ldots \overline{p-1}$ e podemos cancelar $\overline{a}$ e $\overline{a}^{\,-1}$. Logo, $(p-1)!$ é o produto de classes de $\overline{a}$ tais que $\overline{a} = \overline{a}^{\,-1}$.

Se $\overline{a}^{\,2} \equiv 1 \pmod{p}$, então

$$a^2 - 1 \equiv 0 \pmod{p}$$

$$(a+1)(a-1) \equiv 0 \pmod{p}$$

$$(a+1)(a-1) = k \cdot p$$

Se $a \in \{1, 2, \ldots, p-1\}$, então:

$$a = 1 \quad \text{ou} \quad a = p - 1$$

Portanto, em $\overline{1} \cdot \overline{2} \cdot \overline{3} \ldots \overline{p-1}$, após o cancelamento temos:

$$\overline{1} \cdot (\overline{p-1}) \equiv \overline{p-1}$$

Assim:

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

□

4 Criptografia RSA

O método RSA lida com algoritmos computacionais utilizando a chave pública e foi inventado em 1978 por Ronald Rivest, Adi Shamir e Leonard Adleman que na época trabalhavam na MASSACHUSSETS INSTITUTE OF TECHNOLOGIC (M.I.T.). Atualmente, o RSA é o método mais usado em aplicações comerciais.

A chave de codificação do RSA é essencialmente constituída por $n = pq$, em que p e q são primos grandes. A pré-codificação inicia-se com a escolha de p, q e um inteiro e de forma que mdc$(e, \phi(n)) = 1$. O par (n, e) é feito público. Cada letra da mensagem deve ser colocado em correspondência biunívoca com um número de dois algarismos. Analogamente, ao espaço entre as palavras deve corresponder um número, também de dois algarismos e diferente dos demais. Após transformar a mensagem é obtida uma seqüência de números, a qual é preciso separar adequadamente em blocos de modo que cada bloco M satisfaça a condição $M^{\phi(n)} \equiv 1 \pmod{n}$ (**Teorema de Euler para** M **e** n).

Denotaremos o bloco como M_i, onde $i = 1, 2, \ldots, k$. A codificação é feita de forma que cada bloco codificado seja o resto da divisão de M_i^e por n, ou seja, devemos calcular $C(M)$ de forma que $M_i^e \equiv C(M) \pmod{n}$.

O processo de decodificação é feito através da determinação de um número inteiro positivo d tal que $ed \equiv 1 \pmod{\phi(n)}$. Essa congruência é facilmente calculada pelo **Algoritmo Euclidiano Estendido**.

Como um exemplo, vamos codificar a mensagem **"penso logo existo"**. Primeiro, com ajuda da tabela abaixo, vamos converter as letras em números.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
S	T	U	V	W	Y	X	Z	_									
28	29	30	31	32	33	34	35	99									

Assim, para a nossa mensagem, obtemos a seqüência:

$$25 - 142 - 32 - 82 - 49 - 92 - 124 - 2 - 62 - 49 - 9 - 14 - 3 - 31 - 82 - 8 - 29 - 24.$$

Escolhemos $n = 11 \cdot 13 = 143$ e $e = 17$. Calculando a ordem de n através da função

de Euler obtemos:

$$\phi(143) = \phi(11) \cdot \phi(13) = 10 \cdot 12 = 120.$$

Desta forma, cada bloco é codificado. Por exemplo, vamos codificar o bloco 25 da mensagem:

$$25^{17} \equiv (25^3)^5 \cdot 25^2 \equiv (38)^5 \cdot 53 \equiv 12 \cdot 53 \equiv 64 \pmod{143}.$$

Assim $C(25) = 64$. Repetindo o processo para todos os blocos obtemos a mensagem cifrada abaixo:

$$64 - 142 - 54 - 36 - 69 - 27 - 141 - 84 - 17 - 69 - 81 - 53 - 9 - 70 - 36 - 112 - 610 - 7.$$

Para decifrar a mensagem devemos determinar d, resolvendo a equação diofantina $17d + y120 = 1$. Neste caso resulta $d = 113$. Tomando o primeiro bloco acima como exemplo temos:

$$64^{113} \equiv (64^4)^{28} \cdot 64 \equiv 27^{28} \cdot 64 \equiv (27^5)^5 \cdot 27^3 \cdot 64 \equiv 1^5 \cdot 92 \cdot 64 \equiv 25 \pmod{143}.$$

Repetindo este processo com cada bloco, obtemos a seqüência inicial e, portanto, a mensagem que foi enviada inicialmente.

Para ajudar a criptografar e descriptografar os blocos, podemos usar a calculadora de blocos do RSA disponível em: https://criptocefet.com.br/cifras/calculadora-rsa.html

O RSA é um método de chave pública, pois o par (n, e) é acessível a qualquer usuário. Na prática, só podemos achar d se soubermos a ordem $\phi(n)$ e e. Desta forma, é preciso fatorar n, e se este número for muito grande, isto se torna um problema extremamente complexo. Existem algoritmos probabilísticos de fatoração de números (o *NFS-Number Field Sieve*, e suas variantes, o *QS-Quadratic Sieve*, etc) eficientes, em alguns casos, mas ainda estudam-se métodos determinísticos de fatoração em tempo não exponencial, pois fatorar um número inteiro composto n, muito grande, implica muito tempo e custos computacionais altos. Assim, podemos afirmar que o método é seguro.

Referências

[1] COUTINHO, S. C. *Números Inteiros e Criptografia*. 2. ed. Rio de Janeiro: IMPA, 2003. (Série de Computação e Matemática).

[2] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. 3. ed. Rio de Janeiro: IMPA, 2005.

[3] CRIPTOCEFET. Disponível em: https://criptocefet.com.br/index.html. Acesso em: 29 jun. 2026.