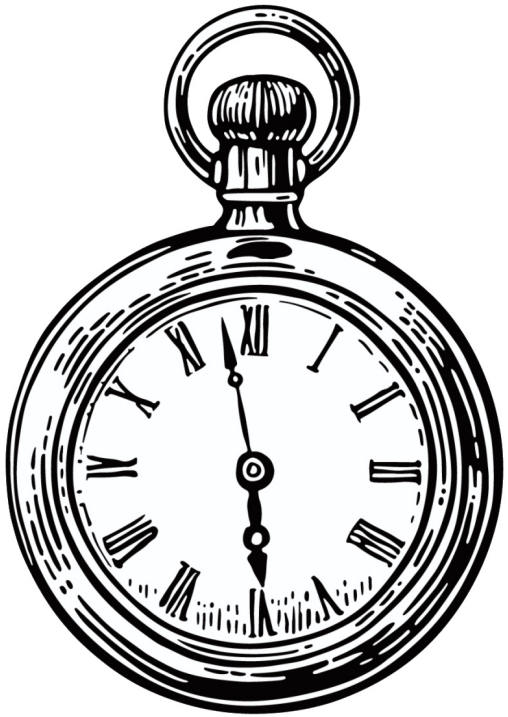
CiberSegurança

Módulo 1 - 02 ARITMÉTICA MODULAR

MEET, MEIC, MEIM

2021–2022



A aritmética do relógio

Seja n um número inteiro positivo. Dizemos que a é **congruente** com b módulo n, e escrevemos $a \equiv b (\mathrm{mod}\, n)$, se n divide $a - b$.
O inteiro n diz-se **módulo da congruência**.

Exemplos:

1. Todos os números pares são congruentes com 0 módulo 2. Todos os números ímpares são congruentes com 1 módulo 2.
2. Na relação de congruência módulo 5 tem-se, por exemplo, que:

$$-1 \equiv 4 (\mathrm{mod}\, 5), \quad 0 \equiv 10 (\mathrm{mod}\, 5), \quad 3 \equiv -2 (\mathrm{mod}\, 5) \ldots$$

3. Em geral, na relação de congruência módulo n, tem-se que

$$n \equiv 0 (\mathrm{mod}\, n) \quad \text{e} \quad n - 1 \equiv -1 (\mathrm{mod}\, n)$$

Seja n um número inteiro positivo. Tem-se que a e b são congruentes se e só se o seu resto da divisão inteira por n coincide, isto é, se

$$a = p \cdot n + r \quad \text{e} \quad b = q \cdot n + r$$

Em particular, todo o número inteiro é congruente módulo n com um e um só elemento do conjunto:

$$\{0, 1, \cdots, n-1\}$$

Exemplos:

1. Todo o número inteiro é congruente módulo 5 com um e um só elemento do conjunto:
$$\{0, 1, 2, 3, 4\}$$
2. Todo o número inteiro é congruente módulo 8 com um e um só elemento do conjunto:
$$\{0, 1, 2, 3, 4, 5, 6, 7\}$$

Seja n um inteiro positivo. A relação de congruência módulo n é uma *relação de equivalência*, isto é, para todos os $a, b, c \in \mathbf{Z}$, tem-se que:

- $a \equiv a (\mathrm{mod}\, n)$; *(reflexividade)*
- Se $a \equiv b (\mathrm{mod}\, n)$ então $b \equiv a \mathrm{mod}\, (n)$; *(simetria)*
- Se $a \equiv b (\mathrm{mod}\, n)$ e $b \equiv c (\mathrm{mod}\, n)$ então $a \equiv c (\mathrm{mod}\, n)$ *(transitividade)*

A **classe de congruência** de a módulo n, que denotamos por

$$a(\bmod n)$$

é o conjunto de todos os números inteiros congruentes com a módulo n.

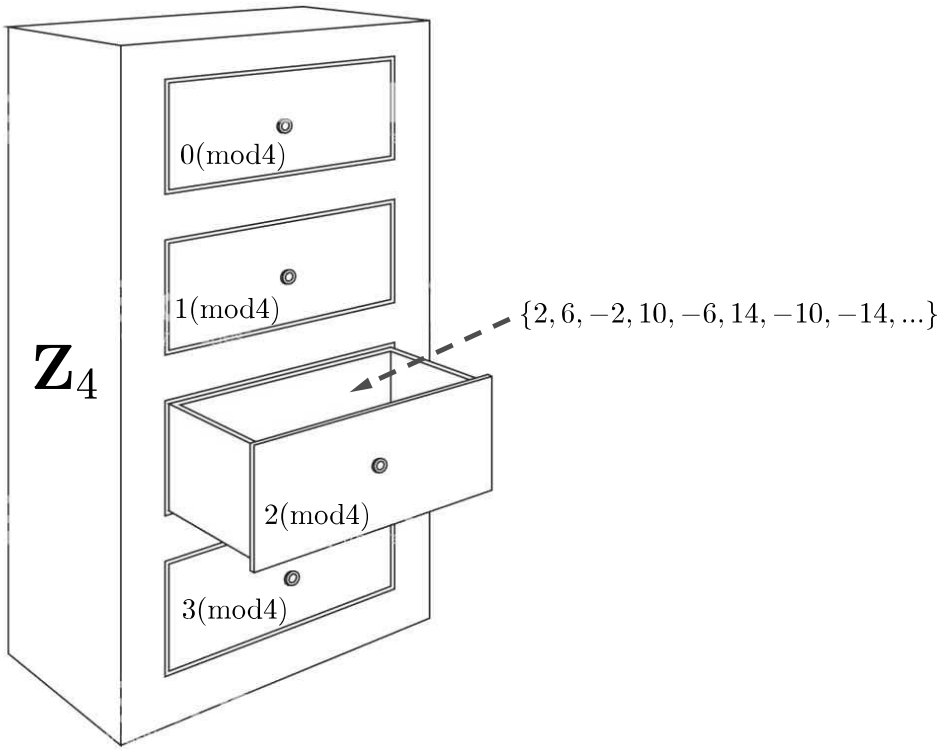
Exemplos:

1. $1(\bmod 2)$ é o conjunto dos números ímpares, $0(\bmod 2)$ é o conjunto dos números pares;
2. $2(\bmod 5) = \{\cdots -13, -8, -3, 2, 7, 12, 17 \ldots\}$;
3. $0(\bmod n) = \{\cdots -4n, -3n, -2n, -n, 0, n, 2n, 3n, 4n \ldots\}$;
4. $k(\bmod n) =$
   $\{\ldots k-4n, k-3n, k-2n, k-n, k, k+n, k+2n, k+3n, k+4n \ldots\}$

$\rightsquigarrow$ Sim, a notação é confusa ...

$b \equiv a(\bmod n)$ é equivalente a $b \in a(\bmod n)$

O conjunto cujos elementos são as classes de congruência módulo n denota-se por $\mathbf{Z}_n$.



Cada classe de congruência contém infinitos números inteiros, pelo que há infinitas possibilidades de descrever o conjunto $\mathbf{Z}_n$.

1. $\mathbf{Z}_2 = \{0(\bmod 2), 1(\bmod 2)\} = \{-6(\bmod 2), 1(\bmod 2)\} = \ldots$
2. $\mathbf{Z}_5 = \{0(\bmod 5), 1(\bmod 5), 2(\bmod 5), 3(\bmod 5), 4(\bmod 5)\}$
   $= \{10(\bmod 5), -4(\bmod 5), 7(\bmod 5), 8(\bmod 5), -1(\bmod 5)\} = \ldots$

Uma escolha natural para as classes de congruência são os restos da divisão inteira por n:

$$\mathbf{Z}_n = \{0(\bmod n), 1(\bmod n), \cdots, (n-1)(\bmod n)\}$$

ou, simplificando ainda mais, **quando não há ambigüidade no módulo n da congruência**:

$$\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$$

1. $\mathbf{Z}_2 = \{0(\mathrm{mod}\,2), 1(\mathrm{mod}\,2)\} = \{0, 1\}$
2. $\mathbf{Z}_4 = \{0(\mathrm{mod}\,4), 1(\mathrm{mod}\,4), 2(\mathrm{mod}\,4), 3(\mathrm{mod}\,4)\} = \{0, 1, 2, 3\}$
3. $\mathbf{Z}_5 = \{0(\mathrm{mod}\,5), 1(\mathrm{mod}\,5), 2(\mathrm{mod}\,5), 3(\mathrm{mod}\,5), 4(\mathrm{mod}\,5)\} = \{0, 1, 2, 3, 4\}$
4. No caso de $\mathbf{Z}_{16}$ é frequente também usar a notação hexadecimal:

$$\mathbf{Z}_{16} = \{0(\mathrm{mod}\,16), 1(\mathrm{mod}\,16), 2(\mathrm{mod}\,16), 3(\mathrm{mod}\,16), \ldots, 15(\mathrm{mod}\,16)\}$$

$$= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f\}$$

$\rightsquigarrow$ Outra notação frequente é aquela que usa o elemento da classe de congruência com valor absoluto mais pequeno:

$$\mathbf{Z}_3 = \{0, 1, -1\}, \quad \mathbf{Z}_4 = \{0, 1, 2, -1\}, \quad \mathbf{Z}_5 = \{0, 1, 2, -2, -1\} \ldots$$

A relação de congruência é **compatível** com as operações de adição e multiplicação de número inteiros, isto é, se n é um número inteiro positivo, e

$$a \equiv (a' \bmod n) \text{ e } b \equiv (b' \bmod n)$$

então:

1. $a + b \equiv a' + b' (\bmod n)$;
2. $a \cdot b \equiv a' \cdot b' (\bmod n)$.

$\rightsquigarrow$ **Em particular para cada inteiro positivo n, é possível definir corretamente em $\mathbf{Z}_n$ operações de adição e multiplicação.**

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Adição e multiplicação em $\mathbf{Z}_2 = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Observe-se que se trata, de facto, das operações lógicas XOR e AND:

XOR	0	1
0	0	1
1	1	0

AND	0	1
0	0	0
1	0	1

Adição e multiplicação em $\mathbf{Z}_3 = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\rightsquigarrow$ Em criptografia é usada com muita frequência (p.e. RSA, ECC) aritmética modular com o módulo um número primo $n = p$ ou um produto de dois números primos $n = p \cdot q$, com primos muito grandes e também aritmética módulo 2^n (usada em blocos de n *bits*)

Propriedades das operações em $\mathbf{Z}_n$

$\mathbf{Z}_n$ hereda as "boas" propriedades das operações em $\mathbf{Z}$:

1. A adição $+$ é comutativa, associativa e com elemento neutro, que é a classe de congruência do 0:

$$0(\bmod n) = n(\bmod n) = 2n(\bmod n)...$$

2. Cada classe de congruência $a(\bmod n)$ tem um elemento simétrico para a adição:

$$(-a)(\bmod n) = (n-a)(\bmod n) = ...$$

3. A multiplicação $\cdot$ é comutativa, associativa, distributiva relativamente à adição, e com elemento neutro, que é a classe de congruência do 1:

$$1(\bmod n) = n+1(\bmod n) = ...$$

Em $\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$:

- o simétrico de 4 para adição é 3:

$$3 + 4 = 7 \equiv 0 (\mathrm{mod}\, 7)$$

- o simétrico de 6 para adição é 1:

$$6 + 1 = 7 \equiv 0 (\mathrm{mod}\, 7)$$

- tem-se que $5 \cdot 4 = 6$,

$$5 \cdot 4 = 20 \equiv 6 (\mathrm{mod}\, 7)$$

- o quadrado de 4 é 4, isto é $4^2 = 2$,

$$4^2 = 16 \equiv 2 (\mathrm{mod}\, 7)$$

- tem-se que $3 \cdot 5 = 1$ em $\mathbf{Z}_7$,

$$3 \cdot 5 = 15 \equiv 1 (\mathrm{mod}\, 7)$$

Identificando o alfabeto standard com os inteiros módulo 26

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

a cifra de César é simplesmente a adição 3 mod 26:

Texto limpo	a	z	a	n	g	a	d	e	c	e	s	a	r
	0	25	0	13	6	0	3	4	2	4	18	0	17
	3	2	3	16	9	3	6	7	5	7	21	3	20
Texto cifrado	D	C	D	Q	J	D	G	H	F	H	V	D	U

Cada alfabeto de deslocação da *Tabula Reta* de Trithemius consiste simplesmente em adicionar o valor, módulo 26, da **letra chave**.
Por exemplo, o alfabeto da substituição definida pelo alfabeto **M**:

	a	b	c	d	e	f	g	h	i	j	k	l	m
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y

	n	o	p	q	r	s	t	u	v	w	x	y	z
M	Z	A	B	C	D	E	F	G	H	I	J	K	L

corresponde a adicionar 12, módulo 26:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
12	13	14	15	16	17	18	19	20	21	22	23	24
M	N	O	P	Q	R	S	T	U	V	W	X	Y

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25
25	0	1	2	3	4	5	6	7	8	9	10	11
Z	A	B	C	D	E	F	G	H	I	J	K	L

Outros módulos que aparecem frequentemente em criptografia (AES, funções *hash*) são as potências de 2 porque os conjuntos $\mathbf{Z}_{2^n}$ podem identificar-se com as sequências (*arrays*) de n bits.

Para cada $0 \leq k < 2^n$, identificamos a classe $k(\mathrm{mod}\, 2^n)$ com a representação binária de k usando um *array* de n-bits.

Exemplos:

1. $\mathbf{Z}_2 = \{0, 1\}$;
2. $\mathbf{Z}_4 = \mathbf{Z}_{2^2} = \{0, 1, 2, 3\} = \{00, 01, 10, 11\}$
3. $\mathbf{Z}_8 = \mathbf{Z}_{2^3} = \{0, 1, 2, 3, 4, 5, 6, 7\} = \{000, 001, 010, 011, 100, 101, 110, 111\}$
4. $\mathbf{Z}_{16} = \mathbf{Z}_{2^4} = \{0, 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15\}$

   $= \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$

$\boxplus_n$: a adição módulo 2^n

A adição módulo 2^n, quando realizada entre *arrays* de n *bits*, será denotada por $\boxplus_n$.

Exemplos:

- $101 \boxplus_3 101 = 010$, (adição módulo $2^3 = 8$);
  $(5 + 5 = 2 \bmod 2^3)$
- $1011 \boxplus_4 0101 = 0000$, (adição módulo $2^4 = 16$);
  $(11 + 5 = 0 \bmod 2^4)$
- $10 \boxplus_2 11 = 01$ (adição módulo $2^2 = 4$).
  $(2 + 3 = 1 \bmod 2^2)$

Combinações de operações do tipo $\boxplus_n$

Os *arrays* de *bits* podem subdivir-se em blocos de diferentes tamanhos e combinar operações módulo 2^n, para n diferentes, sendo que, (abusando ligeiramente da notação), a subdivisão em blocos mais pequenos é subentendida.

Por exemplo:

- $1011 \boxplus_4 0101 = 0000$ é a operação módulo $2^4 = 16$ (11+5=0)
- $1011 \boxplus_2 0101$ consiste em subdivir em blocos de 2-*bits* e operar módulo 2^2, bloco a bloco:

$$\begin{array}{c|c} 10 & 11 \\ 01 & 01 \\ \hline 11 & 00 \end{array} \quad \text{visto que} \quad \begin{array}{c|c} 2 & 3 \\ 1 & 1 \\ \hline 3 & 0 \end{array} \quad \text{(mod 4 em cada sub-bloco)}$$

- $1011 \boxplus_1 0101$ consiste em sub-dividir em blocos de 1 *bit*, ou seja, trata-se do *bitwise* XOR,

$$1011 \boxplus_1 0101 = 1011 \oplus 0101 = 1110$$

Sejam N, M os números naturais representados, respetivamente, pelos *arrays* de n-bits $b_n b_{n-1} \cdots b_1 b_0$ e $c_n c_{n-1} \cdots c_1 c_0$ (com $b_k, c_k \in \{0, 1\}$).

Tem-se que:

$$\begin{aligned} N &= b_{n-1}2^{n-1} \cdots + b_2 2^2 + b_1 2 + b_0 \\ M &= c_{n-1}2^{n-1} \cdots + c_2 2^2 + c_1 2 + c_0 \end{aligned}$$

Para calcular $M + N$, observamos que se $b_k = c_k = 1$, então $2 \cdot 2^k = 2^{k+1}$ (*vai um*, exceto no caso $b_{n-1} = c_{n-1} = 1$, porque $2^n = 0 \bmod (2^n)$).

Exemplo: $1110 \boxplus_4 0101 = 0011$

1					$1 \cdot 2^3$					
1	1	1	0	$\equiv$	$1 \cdot 2^3$	$+1 \cdot 2^2$	$+1 \cdot 2$	$+0$	$\equiv$	14
0	1	0	1	$\equiv$	$0 \cdot 2^3$	$+1 \cdot 2^2$	$+0 \cdot 2$	$+1$	$\equiv$	5
0	0	1	1	$\equiv$	$0 \cdot 2^3$	$+0 \cdot 2^2$	$+1 \cdot 2$	$+1$	$\equiv$	3

Outras operações em *arrays* de *n-bits*

Para além da adição $\boxplus_n$, são usadas frequentemente em criptografia as seguintes operações em *arrays* de *n-bits*:

- o *bitwise XOR*, designado por $\oplus$;
- o *bitwise OR*, designado por $\vee$;
- o *bitwise AND*, designado por $\wedge$;
- o complemento *bitwise*, designado por $\neg$;
- os *shift* e as rotações de n bits, à esquerda e à direita.

Exemplos: operações em arrays de 4-bits (*nibbles*)

- $0011 \oplus 0101 = 0110$;
- $0011 \vee 0101 = 0111$
- $0011 \wedge 0101 = 0001$
- $\neg 0011 = 1100$;
- $0011 \boxplus_4 0101 = 1000$, (adição $\mod 2^4$);
- $0011 \boxplus_2 0101 = 0100$, (adição mód 2^2, sub-blocos de 2 *bits*);
- *shift* à esquerda de dois *bits*: $1011 \rightsquigarrow 1100$;
- *rotação* à esquerda de dois *bits*:$1011 \rightsquigarrow 1110$.

Seja n um inteiro positivo. Um elemento $a \in \mathbf{Z}_n$ diz-se **invertível** (módulo n), se existe $b \in \mathbf{Z}_n$ tal que:

$$a \cdot b \equiv 1 (\mathrm{mod}\, n)$$

Se $a \in \mathbf{Z}_n$ é invertível, então o elemento $b \in \mathbf{Z}_n$ tal que $a \cdot b \equiv 1 (\mathrm{mod}\, n)$ é único, designa-se por a^{-1} e diz-se **inverso módulo** n de a.

O conjunto dos elementos invertíveis em $\mathbf{Z}_n$ denota-se por $\mathbf{Z}_n^*$.

Exemplo: Tem-se que

$$3 \cdot 2 = 1 \,\mathrm{mod}\, 5$$

por tanto, 3 é invertível módulo 5 e o seu inverso, módulo 5, é 2.

Exemplos: inversos módulo 2 e 3

Em $\mathbf{Z}_2$ e $\mathbf{Z}_3$, todos os elementos não nulos possuem inverso, isto é, são invertíveis.

Multiplicação em $\mathbf{Z}_2$

$\cdot$	0	1
0	0	0
1	0	1

Multiplicação em $\mathbf{Z}_3$

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Em particular,

$$\mathbf{Z}_2^* = \{1\}, \quad \mathbf{Z}_3^* = \{1, 2\}$$

Exemplos: inversos módulo 4

Recorde-se a tabela da multiplicação em $\mathbf{Z}_4$:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Em $\mathbf{Z}_4$, como mostra a tabela da multiplicação, não existe b tal que

$$2 \cdot b \equiv 1 (\mathrm{mod}\, 4)$$

Por outras palavras **2 não é invertível módulo 4**.
Em particular,

$$\mathbf{Z}_4^* = \{1, 3\}$$

Observe-se também que, por exemplo, 3 é invertível módulo 4 e é o seu próprio inverso ...

Exemplos: inversos módulo n

Todos os elementos de $\mathbf{Z}_n$ possuem um elemento simétrico para a adição, no entanto, a existência de inversos multiplicativos em $\mathbf{Z}_n$ depende muito do módulo n considerado:

	$\mathbf{Z}_2$	$\mathbf{Z}_3$	$\mathbf{Z}_4$	$\mathbf{Z}_5$	$\mathbf{Z}_6$	$\mathbf{Z}_7$	$\mathbf{Z}_8$	$\mathbf{Z}_9$	$\mathbf{Z}_{10}$	$\mathbf{Z}_{11}$
♯**Elementos invertíveis**	1	2	2	4	2	6	4	6	4	10

$\rightsquigarrow$ **Esta falta de regularidade é o motivo principal das muitas aplicações da aritmética modular em criptografia.**

Caracterização de elementos invertíveis módulo n

Seja n um inteiro positivo. Dado $a \in \mathbf{Z}_n$, tem-se que a é invertível (módulo n) se e só se a e n são **primos entre si**, isto é, se e só se

$$\gcd(a, n) = 1$$

$\rightsquigarrow$ **Em particular, se p é um número primo, então todos os elementos não nulos de $\mathbf{Z}_p$ são invertíveis.**

Nota: $\gcd(a, b)$ significa *"greatest common divisor"*, isto é, o máximo divisor comum entre os dois números inteiros a e n.

- Dados dois números inteiros a e b existe um inteiro positivo d, chamado **máximo divisor comum** que divide a a e a b e tal que todo outro divisor de a e b divide também a d;
- Um número inteiro $p > 1$ diz-se **primo** se os únicos divisores positivos são 1 e p, caso contrário diz-se **composto**.
- Dois números inteiros positivos dizem-se **primos entre sim** quando o seu máximo divisor comum é 1.
- **(Teorema Fundamental da Aritmética)** Todo número inteiro positivo se escreve de modo único (exceto a ordem dos fatores) como um produto de números primos;

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

1. Em $\mathbf{Z}_{14}$, os elementos invertíveis são 1, 3, 5, 9, 11, 13, ou seja,

$$\mathbf{Z}_{14}^{*} = \{1, 3, 5, 9, 11, 13\}$$

   Por exemplo, $3 \cdot 5 = 15 \equiv 1 (\mathrm{mod}\, 14)$, ou seja, módulo 14 tem-se que $3^{-1} = 5$.

2. Os elementos invertíveis em $\mathbf{Z}_{128}$ são as classes de congruência dos números ímpares.

3. Todos os elementos não nulos de $\mathbf{Z}_{43}$ são invertíveis, porque para todo $x \in \{2, 3, \cdots, 42\}$, como 43 é um número primo, verifica-se que $g.c.d.(x, 43) = 1$.

O Lema de Bézout

Dados inteiros não nulos, a e b, existem inteiros n e m tais que

$$an + bm = \gcd(a, b)$$

Verificando-se ainda:

- os inteiros da forma $ax + by$ são precisamente os múltiplos do $\gcd(a, b)$;
- existem x, y tais que $ax + by = 1$ se e só se a e b são primos entre si.

Pelo Lema de Bezout, a e n são primos entre si se e só se existem inteiros x, y tais que

$$ax + ny = 1$$

Os inteiros x, y são por vezes chamados **coeficientes de Bezout**.

Qual a relação do Lema de Bezout com o cálculo de inversos módulo n?

$$\gcd(a, n) = 1 \implies \exists x, y \in \mathbf{Z} : ax + yn = 1 \implies ax = 1 - yn$$

$$\implies ax \equiv 1 (\mathrm{mod}\, n)$$

Por outras palavras, x é o inverso de a módulo n.

Como se calculam então os coeficientes de Bezout?

Dados inteiros positivos, a, b, com $a > b$, o algoritmo de Euclides consiste em realizar divisões sucessivas até obter resto nulo, mais precisamente :

$$\begin{array}{rcll} a & = & q_0 b + r_0 & (r_0 < b) \\ b & = & q_1 r_0 + r_1 & (r_1 < r_0) \\ r_0 & = & q_2 r_1 + r_2 & (r_2 < r_1) \\ \vdots & & \vdots & \\ r_{k-2} & = & q_k r_{k-1} + r_k & (r_{k+1} < r_k) \\ r_{k-1} & = & q_{k+1} r_k + 0 & \end{array}$$

Observe-se que, a partir do último resto não nulo, e substituindo nas divisões anteriores de modo ascendente, obtém-se uma expressão do tipo

$$r_k = ax + by$$

$\rightsquigarrow$ **O Algoritmo de Euclides permite calcular os coeficientes de Bezout**

A apresentação dos cálculos do algoritmo de Euclides de modo a obter facilmente os coeficientes de Bezout costuma designar-se por **Algoritmo Estendido de Euclides**.

O algoritmo estendido de Euclides consiste na construção indutiva de quatro sucessões (q_n), (r_n), (x_n) e (y_n), onde

$$\begin{array}{lll} r_0 = a, & r_1 = b, & r_{n+1} = r_{n-1} - q_n r_n, \quad \text{e} \quad 0 \leq r_{n+1} < |r_n| \\ x_0 = 1, & x_1 = 0, & x_{n+1} = x_{n-1} - q_n x_n \\ y_0 = 0, & y_1 = 1, & y_{n+1} = y_{n-1} - q_n y_n \\ & q_1 = a//b & q_{n+1} = r_n//r_{n+1} \end{array}$$

O algoritmo termina quando $r_{n+1} = 0$, sendo r_n o máximo comun divisor de a e b e x_n, y_n os coeficientes de Bezout.

$\rightsquigarrow$ O cálculo do inverso de a módulo b precisa só de r_n, q_n e x_n.

Exemplo : a e b co-primos

Sejam $a = 12$ e $b = 7$. As sucessões do algoritmo estendido de Euclides são:

n	q_n	r_n	x_n	y_n
0	–	12	1	0
1	1	7	0	1
2	1	5	1	-1
3	2	2	-1	2
4	0	1	3	-5

Como $r_4 = 1$, não é preciso continuar o algoritmo ($r_5 = 0$), verificándose:

$$\gcd(7, 12) = r_4 = 1, \quad r_4 = ax_4 + by_4,$$

ou seja

$$1 = 12 \times (3) + 7 \times (-5) +$$

Em particular: $7^{-1} = (-5) \bmod 12 = 7 \bmod 12$ e $12^{-1} = 3 \bmod 7$.

Sejam $a = 28$ e $b = 16$. As sucessões do algoritmo estendido de Euclides são:

n	q_n	r_n	x_n	y_n
0	0	28	1	0
1	0	16	0	1
2	1	12	1	-1
3	1	4	-1	2
4	–	0	–	–

Como $r_4 = 0$, não é preciso continuar o algoritmo, verificándose:

$$\gcd(28, 16) = r_3 = 4, \quad r_3 = ax_3 + by_3,$$

$$4 = 28 \times (-1) + 16 \times (2)$$

Em particular, como 28 e 16 não são coprimos, 28 não é invertível módulo 16 e 16 não é invertível módulo 28.

O sistema de **cifra Afim** consiste em :

- o alfabeto é $\mathbf{Z}_{26}$ (identificado com o alfabeto minúsculo em texto limpo e com o alfabeto maiúsculo no texto cifrado);
- o espaço de chaves $\mathcal{K}$ consiste em todos os pares (a, b), com $a, b \in \mathbf{Z}_{26}$ e a invertível módulo 26:

$$\mathcal{K} = \mathbf{Z}_{26}^* \times \mathbf{Z}_{26} \qquad (12 \cdot 26 = 312 \text{ chaves});$$

- a transformação de cifragem e_k para $k = (a, b)$ está definida por

$$c_k(x) = ax + b$$

- a transformação de decifragem d_k para $k = (a, b)$ está definida por

$$d_k(y) = a^{-1}y - a^{-1}b$$

Exemplos:

1. A cifra Afim com parámetros $(a, b) = (3, 2)$ verifica

Texto limpo	*c*	*i*	*f*	*r*	*a*	*a*	*f*	*i*	*m*
	2	8	5	17	0	0	5	8	12
	8	0	17	1	2	2	17	0	12
Texto cifrado	*J*	*B*	*S*	*C*	*D*	*D*	*S*	*B*	*N*

2. A cifra de César, e todas as cifras da *Tabula Reta* são cifras afins do tipo $(a, b) = (1, b)$ (com $b = 3$ no caso da cifra de César);
3. A cifra Atbash, é um caso particular da cifra afim, com $(a, b) = (-1, 25)$:

$$e(x) = (-x + 25) \bmod 26$$

$\rightsquigarrow$ É um cifra de substituição mono-alfabética, pode ser cripto-analisada usando análise de frequências

$\rightsquigarrow$ É possível adaptar a ideia para cifrar **blocos de letras** no lugar de letras individualmente, e obter uma cifra resistente ao análise de frequências (simétrica).

Por exemplo, identificar os blocos de 4 letras

$$AAAA, AAAB, AAAC, \ldots, AAAZ, AABA, AABB, \ldots, ZZZY, ZZZZ$$

com os elementos $0, 1, \ldots, 26^4$ e realizar uma cifra afim módulo $26^4 = 456976$.

Em matemática são usadas diferentes terminologias para descrever os conjuntos munidos de operações, em função das propriedades que as operações verificam.

Estruturas que aparecem frequentemente em criptografia:

- **grupo** : conjunto munido de uma operação associativa, com elemento neutro e tal que todo o elemento possui simétrico diz-se um **grupo**.
  Se a operação é também comutativa, o grupo diz-se **comutativo** ou **abeliano**.
- **anel**: conjunto munidos de duas operações, denotadas em geral por $+$ e $\cdot$, verificando que:
  1. a operação $+$ é comutativa, associativa, com elemento neutro, denotado por 0, e tal que existe simétrico para todo o elemento;
  2. a operação $\cdot$ é associativa, com elemento neutro 1;
  3. a operação $\cdot$ é distributiva relativamente à primeira;

  Se a operação $\cdot$ é também comutativa, então dizemos que é um **anel comutativo**.
- **corpo**: um anel munido de duas operações $+$ e $\cdot$, e tal que todo o elemento diferente do 0 admite um elemento inverso para a segunda operação $\cdot$.

Exemplos de estruturas algébricas

1. São grupos (abelianos): $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{Q}^*, \cdot)$, $(\mathbf{R}, +)$, $(\mathbf{R}^+, \cdot)$, $(\mathbf{R}_n[x], +)$ ...
2. Não são grupos: $(\mathbf{N}, +)$, $(\mathbf{Z}^*, \cdot)$, $(\mathbf{R}, \cdot)$, $(\mathbf{R}_n[x], \cdot)$....
3. São anéis (comutativos): $(\mathbf{Z}, +, \cdot)$, $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}_n[x], +, \cdot)$ ...
4. Os conjuntos de matrizes quadradas (com coeficientes inteiros, racionais, reais, complexos ...) munidos das operações usuais de adição e multiplicação de matrizes são anéis não comutativos.
5. São corpos: $(\mathbf{Q}, +, \cdot)$,$(\mathbf{R}, +, \cdot)$, $(\mathbf{C}, +, \cdot)$. Um exemplo de corpo não comutativo é o corpo dos quaterniões $\mathbf{H}$.
6. Não são corpos: $(\mathbf{Z}, +, \cdot)$, $(\mathbf{R}_n[x], +, \cdot)$

$\rightsquigarrow$ A notação $\mathbf{K}_n[x]$ representa o conjunto dos polinómios na variável x, de grau inferior ou igual a n, e coeficientes no anel $\mathbf{K}$.