Congruência Modular

F. Manso

junho, 2026

$$a \equiv b \pmod{n} \iff n \mid a - b$$

Sumário

1 O que é Congruência Modular?

Congruência modular é uma relação de equivalência entre dois inteiros a e b que deixam o mesmo resto quando divididos por um inteiro n. Então, dizemos que a é congruente a b módulo n e denotamos

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

Adota-se n como um inteiro estritamente maior que 1.

Dizer que é uma relação de equivalência significa que a relação, no conjunto dos inteiros, é:

1. **Reflexiva:** $a \equiv a \pmod{n}$;
2. **Simétrica:** $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$;
3. **Transitiva:** se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$.

Essa relação de equivalência dá origem às *classes de equivalência módulo* n, que particionam o conjunto dos inteiros em conjuntos disjuntos; ou seja, cada número inteiro, sob a relação de equivalência módulo n, pertence a uma e somente uma classe de equivalência.

n dá origem a n classes de equivalência que vão do zero até $n-1$. Denotamos cada classe de equivalência como $[x]$ ou $\bar{x}$. Quando reunimos todas essas classes de equivalência num novo conjunto, criamos o chamado *conjunto quociente*, denotado por $\mathbb{Z}/n\mathbb{Z}$ ou simplesmente $\mathbb{Z}_n$. Por exemplo:

$$\mathbb{Z}_3 = \{[0],[1],[2]\} \quad \text{ou} \quad \mathbb{Z}_3 = \{\bar{0},\bar{1},\bar{2}\}.$$

No dia a dia utilizamos as classes de equivalência módulo 12 e nem percebemos. Quando usamos 15 horas e 3 horas da tarde para representar o mesmo horário, estamos dizendo que $15 \equiv 3 \pmod{12}$.

2 Propriedades da Congruência Modular

2.1 As três propriedades que definem relação de equivalência

1) **Reflexiva:** $a \equiv a \pmod{n}$

2) **Simétrica:** $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

3) **Transitiva:** se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$

2.2 Compatibilidade com as operações aritméticas

Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

1) $a + c \equiv b + d \pmod{n}$

2) $a - c \equiv b - d \pmod{n}$

3) $a \cdot c \equiv b \cdot d \pmod{n}$

2.3 Compatibilidade com potenciação

Se $a \equiv b \pmod{n}$, então

$$a^k \equiv b^k \pmod{n}, \quad \forall\, k \in \mathbb{Z}_{>0}.$$

2.4 Compatibilidade parcial com a divisão

Se $a \cdot c \equiv b \cdot c \pmod{n}$, então:

1) $a \equiv b \pmod{\frac{n}{\mathrm{MDC}(c,n)}}$

2) $a \equiv b \pmod{n} \iff \mathrm{MDC}(c,n) = 1$. Em particular, se p é primo: $a \equiv b \pmod{p}$.

2.5 Mudança de módulo

- Se $a \equiv b \pmod{n}$ e $d \mid n$ (d divide n), então $a \equiv b \pmod{d}$.
- Se $a \equiv b \pmod{n}$, então $a \cdot n \equiv b \cdot n \pmod{n \cdot n}$.

2.6 Existência de inverso multiplicativo

O inverso multiplicativo de a módulo n é o inteiro a^{-1} tal que

$$a \cdot a^{-1} \equiv 1 \pmod{n}.$$

Existe a^{-1} se e somente se $\mathrm{MDC}(a,n) = 1$.

Se n é primo (p), todas as classes de equivalência módulo p possuem inverso a^{-1}, e $\mathbb{Z}_p$ é um corpo finito.

3 Algoritmo de Euclides para o Cálculo de MDC(a,b)

Seja $a, b \in \mathbb{Z}$ com $a > b$. Então:

	q_0	q_1	q_2	$\cdots$	q_{n-1}	q_n
a, b	r_0	r_1	r_2	$\cdots$	$\mathrm{MDC}(a,b)$	0

onde:

$$
\begin{aligned}
q_0 &= \text{parte inteira da divisão de } a \text{ por } b,\\
r_0 &= \text{resto da divisão de } a \text{ por } b,\\
q_1 &= \text{parte inteira da divisão de } b \text{ por } r_0,\\
r_1 &= \text{resto da divisão de } b \text{ por } r_0,\\
q_2 &= \text{parte inteira da divisão de } r_0 \text{ por } r_1,\\
r_2 &= \text{resto da divisão de } r_0 \text{ por } r_1,\\
&\vdots
\end{aligned}
$$

O algoritmo converge para $\mathrm{MDC}(a,b)$ igual a r_{n-1}, o resto da divisão de r_{n-3} por r_{n-2}. Essa é a penúltima divisão do algoritmo. A última, r_{n-2}/r_{n-1}, levará a q_n e resto $r_n = 0$.

Exemplo 1.

$$
\mathrm{MDC}(91,35): \quad \begin{array}{c|cccc} & 2 & 1 & 1 & 2 \\ \hline 91,\ 35 & 21 & 14 & \boxed{7} & 0 \end{array} \quad \Rightarrow \quad \mathrm{MDC}(91,35) = 7.
$$

4 Algoritmo para o Cálculo do Inverso Multiplicativo a^{-1} Módulo n, Baseado no Algoritmo de Euclides para o Cálculo de $\mathrm{MDC}(n,a)$

$$
a \cdot a^{-1} \equiv 1 \pmod{n}, \quad n > a.
$$

Condição de existência: $\mathrm{MDC}(n,a) = 1$.

$$
\begin{array}{c|ccccccc} & q_0 & q_1 & q_2 & \cdots & q_{n-1} & q_n \\ \hline n,\ a & r_0 & r_1 & r_2 & \cdots & 1 & 0 \end{array}
$$

$$
a^{-1} \bmod n = d_0 = r_{n-3} - q_{n-1}; \quad d_0 = \frac{r_{n-4} - q_{n-2}}{r_{n-2}}
$$

$$
d_1 = \frac{d_0(r_{n-6} - q_{n-4})}{r_{n-4}}, \quad d_2 = \frac{d_1(r_{n-8} - q_{n-6})}{r_{n-6}}, \quad \cdots \quad (n{-}1 \text{ IMPAR})
$$

$$
d_i = \frac{d_0(r_{n-5} - q_{n-3})}{r_{n-3}}, \quad \cdots \quad (n{-}1 \text{ PAR})
$$

Fórmula final:

$$
a^{-1} = \frac{d_k(n - q_0)}{r_0} \quad \text{se } n{-}1 \text{ for ÍMPAR}
$$

$$
a^{-1} = \frac{d_k(a - q_1)}{r_1} \quad \text{se } n{-}1 \text{ for PAR}
$$

Exemplo 2. $n = 83$, $a = 13$. *Calcular* a^{-1}.

$$
\begin{array}{c|ccccc} & 6 & 2 & 1 & 1 & 2 \\ \hline 83,\ 13 & 5 & 3 & 2 & 1 & 0 \end{array} \qquad n - 1 = 3 \ \textit{(ÍMPAR)}
$$

$$
d_0 = \frac{5-1}{2} = \frac{4}{2} = 2, \qquad d_1 = a^{-1} = \frac{2 \times 83 - 6}{5} = \frac{160}{5} = 32.
$$

Verificação: $a \cdot a^{-1} \equiv 1 \pmod{n}$*:*

$$13 \times 32 = 416 \equiv 1 \pmod{83}.\checkmark$$

Portanto, $a^{-1} \equiv 32 \pmod{83}$*, ou seja,* 32 *é o inverso multiplicativo de* 13 *módulo* 83*.*

Exemplo 3. $n = 179$*,* $a = 37$*. Calcular* a^{-1}*.*

	4	1	5	6
179, 37	31	6	1	0

$n - 1 = 2$ *(PAR)*

$$d_0 = \frac{31-5}{1} = 26, \qquad d_1 = a^{-1} = \frac{26 \times 179 - 4}{31} = \frac{4650}{31} = 150.$$

Verificação:

$$37 \times 150 = 5550 \equiv 1 \pmod{179}.\checkmark$$

Portanto, $a^{-1} \equiv 150 \pmod{179}$*.*

5 Teorema de Bézout

Se MDC$(a, b) = d$, então existem dois inteiros x e y tais que

$$ax + by = d.$$

Se MDC$(a, b) = 1$, segue que $ax + by = 1$.

Aplicado a MDC(n, a): $nx + ay = 1$, donde

$$y = a^{-1} \bmod n, \qquad x = \frac{ay - 1}{-n}.$$

Exemplo 4. $n = 83$*,* $a = 13$*,* $a^{-1} = 32$*:*

$$y = 32, \qquad x = \frac{13 \times 32 - 1}{-83} = -5.$$

Verificação:

$$83 \times (-5) + 13 \times 32 = -415 + 416 = 1.\checkmark$$

6 Função Totiente de Euler $\phi(n)$

A função totiente de Euler, $\phi(n)$, é uma função aritmética que conta quantos números inteiros positivos menores ou iguais a n são coprimos com n.

Exemplo 5. $\phi(10) = 4$*: inteiros positivos menores ou iguais a* 10 *são* $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$*. Desses 10 valores, apenas* $1, 3, 7$ *e* 9 *são coprimos com* 10*, portanto* $\phi(10) = 4$*.*

Se n é primo, $\phi(p) = p - 1$.

6.1 Fórmula para o cálculo de $\phi(n)$

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1),$$

onde p_k é um fator primo na fatoração prima de n e α_k o expoente desse fator primo.

Exemplo 6. *$\phi(10)$: $10 = 2^1 \times 5^1$, logo*

$$\phi(10) = 2^{1-1}(2-1) \cdot 5^{1-1}(5-1) = 2^0 \cdot 1 \cdot 5^0 \cdot 4 = 1 \cdot 4 = 4.$$

Exemplo 7.

$$\phi(17) = 17^{1-1}(17-1) = 17^0 \cdot 16 = 16 = p - 1.$$

6.2 Teorema de Euler

Se $\text{MDC}(n, a) = 1$, então

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

Exemplo 8. *$n = 10$, $a = 7$, $\text{MDC}(10, 7) = 1$, $\phi(10) = 4$:*

$$7^4 \equiv 1 \pmod{10}, \qquad 8401 \equiv 1 \pmod{10}.\checkmark$$

6.3 Pequeno Teorema de Fermat

Se $n = p$ (primo), então

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

Como $\phi(p) = p - 1$, o Pequeno Teorema de Fermat é um caso particular do Teorema de Euler, ou seja, o Teorema de Euler generaliza o Pequeno Teorema de Fermat para n não primos.

7 Sistema Completo e Sistema Reduzido de Resíduos Módulo n

Um **sistema completo de resíduo módulo** n é o conjunto das n classes de equivalência módulo n indo de $[0]$ até $[n-1]$. Por padrão, utilizamos o representante da classe menor que n.

Exemplo 9. *$n = 10$: sistema completo de resíduo módulo 10:*

$$[0], [1], [2], [3], [4], [5], [6], [7], [8], [9].$$

Por padrão: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.

Um **sistema reduzido de resíduo módulo** n é o conjunto das classes de equivalência que são coprimas com n.

Exemplo 10. *$n = 10$: sistema reduzido de resíduo módulo 10:*

$$[1], [3], [7], [9].$$

Por padrão: $1, 3, 7, 9$.

8 Teorema de Wilson

$$(p-1)! \equiv -1 \pmod{p}, \quad p \text{ primo.}$$

Exemplo 11. *$p = 7$:* $6! \equiv -1 \pmod 7$, *i.e.,* $720 \equiv -1 \pmod 7$. ✓

Se n é par e $n+1$ é um número primo, então

$$\frac{n!}{(n)} = 2k + \frac{2}{n+1}, \quad k \in \mathbb{Z}_{>0}.$$

Em termos de congruência:

$$(n-1)! \equiv 1 \pmod{n+1}.$$

9 Sistema Linear de Congruência Modular

$$x \equiv a \pmod b \quad \text{e} \quad x \equiv c \pmod d.$$

Condição necessária e suficiente: $\text{MDC}(d, b) = j$ divide $(c - a)$.
Infinitas soluções:

$$x = \left[\left(\frac{b}{d}\right)^{-1} \pmod{\frac{d}{j}}\right] \cdot \frac{b}{j} \cdot (c-a) + a \pm \frac{b}{j} \cdot \frac{d}{j} \cdot w, \quad w \in \mathbb{Z}.$$

Se $j = \text{MDC}(d, b) = 1$:

$$x = \left(b^{-1} \bmod d\right) \cdot b \cdot (c-a) + a \pm b \cdot d \cdot w, \quad w \in \mathbb{Z}.$$

Exemplo 12. *Sistema:* $x \equiv 3 \pmod 7$ *e* $x \equiv 17 \pmod{46}$.
Dados: $a = 3$, $b = 7$, $c = 17$, $d = 46$.
Algoritmo de Euclides para $b^{-1} \bmod d$*:*

	6	1	1	3
46, 7	4	3	1	0

$$\frac{4-1}{1} = 3, \qquad b^{-1} \bmod d = \frac{46 \times 3 - 6}{4} = \frac{132}{4} = 33.$$

$$c - a = 17 - 3 = 14.$$

$$x = (33 \cdot 7 \cdot 14 + 3) \pm 7 \cdot 46 \cdot w = 3239 \pm 322\, w.$$

Para w*:* $\dfrac{3239}{322} = 10 + \dfrac{17}{322}$*, logo* $x = 17 \pm 322\, w$.

Portanto, $x \equiv 17 \pmod{322}$ *são as infinitas soluções para o sistema, e* 17 *é o menor valor inteiro positivo.*

10 Mapa de Congruência Módulo n e Regra Geral de Divisibilidade

Seja k um número natural na base 10. Então temos:

$$k = d_0 \times 10^0 + d_1 \times 10^1 + d_2 \times 10^2 + \cdots + d_n \times 10^n.$$

10.1 Mapa de congruência mod 7

$$
\begin{aligned}
1 \times 10^0 &= 1 \equiv 1 \pmod 7 \\
1 \times 10^1 &= 1 \times 10 = 10 \equiv 3 \pmod 7 \\
1 \times 10^2 &= 3 \times 10 = 30 \equiv 2 \pmod 7 \\
1 \times 10^3 &= 2 \times 10 = 20 \equiv 6 \equiv -1 \pmod 7 \\
1 \times 10^4 &= 6 \times 10 = 60 \equiv 4 \equiv -3 \pmod 7 \\
1 \times 10^5 &= 4 \times 10 = 40 \equiv 5 \equiv -2 \pmod 7 \\
1 \times 10^6 &= 5 \times 10 = 50 \equiv 1 \pmod 7 \quad \text{(ciclo)}
\end{aligned}
$$

Então, podemos reescrever k mod 7 como:

$$k \bmod 7 = 1 \cdot d_0 + 3 \cdot d_1 + 2 \cdot d_2 + (-1) \cdot d_3 + (-3) \cdot d_4 + (-2) \cdot d_5 + 1 \cdot d_6 + 3 \cdot d_7 + \cdots$$

Exemplo 13. *Seja $k = 87$. Queremos saber se 7 divide 87.*
$87 = 7 \times 10^0 + 8 \times 10^1$.
Em módulo 7: $1 \times 7 + 3 \times 8 = 7 + 24 = 31 = 1 \times 10 + 3 \times 3 = 10 + 9 = 1 \times 0 + 3 \times 1 = 3$.
Portanto, 7 não divide 87 porque deixa resto 3 na divisão (de fato, $87 = 12 \times 7 + 3$*).*

Exemplo 14. *Queremos saber se 13 divide 1911.*
Mapa de congruência módulo 13:

$$
\begin{aligned}
1 &\equiv 1 \pmod{13} \\
10 &\equiv 10 \pmod{13} \\
100 &\equiv 9 \pmod{13} \\
1000 &\equiv 12 \equiv -1 \pmod{13} \\
10000 &\equiv 3 \equiv -10 \pmod{13} \\
100000 &\equiv 4 \equiv -9 \pmod{13} \\
1000000 &\equiv 1 \pmod{13} \quad \textit{(ciclo)}
\end{aligned}
$$

Então $1911 \bmod 13 = 1 \times 1 + 1 \times 10 + 9 \times 9 + 1 \times (-1) = 1 + 10 + 81 - 1 = 91$.
$91 = (-12) \times 1 + 10 \times 7 = -12 + 70 = 78 = 1 \times 8 + (-3) \times 7 = 8 - 21 = -13$.
Observamos que 91, 78 *e* -13 *deixam resto zero na divisão por 13, portanto 1911 também deixará resto zero na divisão por 13, o que permite concluir que 13 divide 1911. De fato,* $1911 = 13 \times 147$.

Agora consideremos os mapas de congruência módulos 3 e 2:
Módulo 3:

$$
\begin{aligned}
1 &\equiv 1 \pmod 3 \\
10 &\equiv 1 \pmod 3 \quad \text{(ciclo)}
\end{aligned}
$$

Módulo 2:

$$
\begin{aligned}
1 \times 10^0 &= 1 \equiv 1 \pmod 2 \\
1 \times 10^1 &= 10 \equiv 0 \pmod 2 \\
1 \times 10^2 &= 0 \times 10 = 0 \pmod 2 \\
&\vdots \\
1 \times 10^k &\equiv 0 \pmod 2
\end{aligned}
$$

Esses dois mapas explicam as regras de divisibilidade por 3 e por 2: n é divisível por 3 se a soma dos seus dígitos é divisível por 3; n é divisível por 2 se o dígito da unidade é par.

11 Módulo 9 – Um Módulo Especial no Sistema de Numeração Posicional de Base 10

Sistema completo de resíduos módulo 10:

$$\mathrm{SCR}_{10} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}.$$

Mapa de congruência módulo 9:

$$10^0 = 1 \equiv 1 \pmod 9$$
$$10^1 = 1 \times 10 = 10 \equiv 1 \pmod 9 \quad \text{(ciclo)}$$

Isso permite utilizar mod 9 nos algoritmos de adição, subtração, multiplicação, divisão e potenciação para verificar se a operação foi efetuada corretamente.

11.1 Operações verificadas por mod 9

1. **Adição:** $p_1 + p_2 = S$ (p: parcela; S: soma)
2. **Subtração:** $p_1 + (-p_2) = d$ (p: parcela; d: diferença)
3. **Multiplicação:** $F_1 \times F_2 = P$ (F: fator; P: produto)
4. **Divisão euclidiana:** $d = D \times q + r$ (d: dividendo; D: divisor; r: resto)
5. **Potenciação:** $a^k = P$ (a: base; k: expoente; P: potência)

Exemplo 15. $37 + 45 = 82$. *Em mod 9:* $(3+7)+(4+5) = (8+2)$, *ou seja,* $10+9 = 10$*;* $1+0 = 1$*;* $1 = 1$. *Operação efetuada corretamente.*

Exemplo 16. $45-37 = 45+(-37) = 8$. *Em mod 9:* $(4+5)+(-3-7) = (9 \equiv 0)+(-10 \equiv -1 \equiv 8) = 8$*;* $8 = 8$. *Operação efetuada corretamente.*

Exemplo 17. $37 \times 45 = 1665$. *Em mod 9:* $(3+7) \times (4+5) = 10 \times 9 = (10 \equiv 1) \times (9 \equiv 0) = 1 \times 0 = 0$*;* $0 = 0$. *Operação efetuada corretamente.*

Exemplo 18. $\dfrac{45}{37} = 1$ *com resto* 8*;* $45 = 37 \times 1 + 8$. *Em mod 9:* $(4+5) = (3+7) \times 1 + 8$*;* $9 \equiv 0 = (10 \equiv 1) \times 1 + 8 = 9 \equiv 0$*;* $0 = 0$. *Operação efetuada corretamente.*

Exemplo 19. $37^3 = 50653$. *Em mod 9:* $(3+7)^3 = 10^3 \equiv 1^3 = 1$*;* $1 = 1$. *Operação efetuada corretamente.*

12 Tabuada com Padrão $n \equiv d_0 \pmod{10}$ e Acréscimo $+a$ ou $+a+1$

Observação: todo n é congruente ao dígito da unidade módulo 10.

Se $a = 0$, temos a tabuada do 1 ($1 \equiv 1 \pmod{10}$):

$$\begin{array}{ccc} & 1 \times 1 = 01 & \\ & 1 \times 2 = 02 & \\ & 1 \times 3 = 03 & \\ 1 \times 4 = 04 & 1 \times 5 = 05 & 1 \times 6 = 06 \\ 1 \times 7 = 07 & 1 \times 8 = 08 & 1 \times 9 = 09 \ (9 \equiv 0 \pmod{9}) \end{array}$$

Soma-se $a = 0$ à medida que avançamos.

Se $a = 1$, temos a tabuada do 11 ($11 \equiv 1 \pmod{10}$):

$$\begin{array}{ccc} & 11 \times 1 = 11 & \\ & 11 \times 2 = 22 & \\ & 11 \times 3 = 33 & \\ 11 \times 4 = 44 & 11 \times 5 = 55 & 11 \times 6 = 66 \\ 11 \times 7 = 77 & 11 \times 8 = 88 & 11 \times 9 = 99 \ (99 \equiv 0 \pmod{9}) \end{array}$$

Soma-se $a = 1$ à medida que avançamos.

Para $n \equiv 9 \pmod{10}$: padrão com acréscimo $+(a+1)$, $a = 9$:

$$\begin{array}{ccc} & 9 \times 1 = 09 & \\ & 9 \times 2 = 18 & \\ & 9 \times 3 = 27 & \\ 9 \times 4 = 36 & 9 \times 5 = 45 & 9 \times 6 = 54 \\ 9 \times 7 = 63 & 9 \times 8 = 72 & 9 \times 9 = 81 \ (81 \equiv 0 \pmod{9}) \end{array}$$

Soma-se $a + 1 = 10$ à medida que avançamos.

Para $n \equiv 3 \pmod{10}$: padrão com acréscimo $+a$ ou $+(a+1)$ alternados:

$$\begin{array}{ccc} & 3 \times 1 = 03 & \\ & 3 \times 2 = 06 & \\ & 3 \times 3 = 09 & \\ 3 \times 4 = 12 & 3 \times 5 = 15 & 3 \times 6 = 18 \\ 3 \times 7 = 21 & 3 \times 8 = 24 & 3 \times 9 = 27 \equiv 0 \pmod{9}) \end{array}$$

Se $a = 1$: tabuada do 13:

$$\begin{array}{ccc} & 13 & \\ & 26 & \\ & 39 & \\ \boxed{52} & 65 & 78 \\ \boxed{91} & 104 & 117 \equiv 0 \pmod{9}) \end{array}$$

Quadro completo de padrões $n \equiv d_0 \pmod{10}$ e acréscimos $+a$ ou $+a+1$:

Assinalamos com $\square$ as posições em que o acréscimo muda do padrão $+a$ para $+a+1$ ou de $+a+1$ para $+a$.

Os padrões devem ser construídos aos pares a e b de modo que $a+b=10$. Se $a<b$, por padrão a tem acréscimo $+a$ e b tem acréscimo $+a+1$.

$n \equiv 1 \pmod{10}$

	1		
	2		$+a$
	3		
4	5	6	
7	8	9	

$n \equiv 9 \pmod{10}$

	9		
	8		$+(a+1)$
	7		
6	5	4	
3	2	1	

$n \equiv 3 \pmod{10}$

	3		
	6		$+a$
	9		
$\boxed{2}$	5	8	$\square+(a+1)$
$\boxed{1}$	4	7	

$n \equiv 7 \pmod{10}$

	7		
	4		$+(a+1)$
	1		
$\boxed{8}$	5	2	$\square+a$
$\boxed{9}$	6	3	

$n \equiv 2 \pmod{10}$

	2		
	4		$+a$
	6		
8	$\boxed{0}$	2	$\square+(a+1)$
4	6	8	

$n \equiv 8 \pmod{10}$

	8		
	6		$+(a+1)$
	4		
2	0	$\boxed{8}$	$\square+a$
6	4	2	

$n \equiv 4 \pmod{10}$

	4		
	8		$+a$
	$\boxed{2}$		
6	$\boxed{0}$	4	$\square+(a+1)$
8	$\boxed{2}$	6	

$n \equiv 6 \pmod{10}$

	6		
	2		$+(a+1)$
	$\boxed{8}$		
4	0	$\boxed{6}$	$\square+a$
2	$\boxed{8}$	4	

$n \equiv 5 \pmod{10}$

	5		
	0		$+(a+1)$
	$\boxed{5}$		
0	$\boxed{5}$	0	$\square+a$
$\boxed{5}$	0	$\boxed{5}$	

Exemplo 20. *Queremos construir a tabuada do 86.*

$86 \equiv 6 \pmod{10}$, $a=8$, $a+1=9$.

Tabuada do 86:

$$86,\ 172,\ \boxed{258},\ 344,\ 430,\ \boxed{516},\ 602,\ \boxed{688},\ 774 \equiv 0 \pmod{9}.$$

Portanto, $86 \times 3 = 258$ *e* $86 \times 9 = 774$.

13 Algoritmo de Divisão via Inverso Multiplicativo de D Módulo 10

Divisão euclidiana: $d = D \cdot q + r$, com $D^{-1} \pmod{10}$.

Temos $D^{-1}(d - r) = D \cdot D^{-1} \cdot q \pmod{10}$; como $D \cdot D^{-1} \equiv 1 \pmod{10}$:

$$D^{-1}(d - r) \equiv 1 \cdot q \equiv q \pmod{10}.$$

Exemplo 21. $n = 1911$, $D = 7$; $D^{-1} \bmod 10 = 3$.

$$\begin{aligned} d = 1911, \quad r = 580, \quad q = 873. \\ 1 - 0 = 1 \times 3 = 3. \\ 11 - 2 = 9 \times 3 = 27 \equiv 7 \pmod{10}. \\ 9 - 5 = 4 \times 3 = 12 \equiv 2 \pmod{10}. \end{aligned}$$

14 Dígitos de Verificação do CPF via Mod 11

O CPF é composto por 11 dígitos, sendo o 9º dígito o que indica a região da emissão do documento.

9º dígito:

- 1: DF, GO, MT, MS, TO
- 2: AM, PA, RR, AP, AC, RO
- 3: CE, MA, PI
- 4: PB, PE, AL, RN
- 5: BA, SE
- 6: MG
- 7: RJ, ES
- 8: SP
- 9: PR, SC
- 0: RS

Os dois últimos dígitos são dígitos verificadores e podem ser calculados via mod 11 com o seguinte algoritmo. Os exemplos a seguir referem-se ao mesmo CPF, 509 539 316, calculando-se o 10º e o 11º dígitos verificadores.

10º dígito:

Exemplo 22.

5	0	9	5	3	9	3	1	6
↓	↓	↓	↓	↓	↓	↓	↓	↓
×1	×2	×3	×4	×5	×6	×7	×8	×9

$$
\begin{aligned}
1 \times 5 &= 5 \equiv 5 \pmod{11} \\
2 \times 0 &= 0 + 5 = 5 \equiv 5 \pmod{11} \\
3 \times 9 &= 27 + 5 = 32 \equiv 10 \pmod{11} \\
4 \times 5 &= 20 + 10 = 30 \equiv 8 \pmod{11} \\
5 \times 3 &= 15 + 8 = 23 \equiv 1 \pmod{11} \\
6 \times 9 &= 54 + 1 = 55 \equiv 0 \pmod{11} \\
7 \times 3 &= 21 + 0 = 21 \equiv 10 \pmod{11} \\
8 \times 1 &= 8 + 10 = 18 \equiv 7 \pmod{11} \\
9 \times 6 &= 54 + 7 = 61 \equiv \boxed{6} \pmod{11}
\end{aligned}
$$

Portanto, o 10^o *dígito verificador é* **6**, *e o CPF parcial torna-se:*

$$509.539.316\text{-}\boxed{6}$$

11º dígito:

Exemplo 23. *Para o* 11^o *dígito, utiliza-se o número de 10 dígitos* 5095393166, *multiplicando cada algarismo (da esquerda para a direita) pelos pesos* $1, 2, 3, \ldots, 10$ *e tomando o resultado módulo 11.*

$$
\begin{array}{cccccccccc}
5 & 0 & 9 & 5 & 3 & 9 & 3 & 1 & 6 & 6 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\times 1 & \times 2 & \times 3 & \times 4 & \times 5 & \times 6 & \times 7 & \times 8 & \times 9 & \times 10
\end{array}
$$

$$
\begin{aligned}
1 \times 5 &= 5 \equiv 5 \pmod{11} \\
2 \times 0 &= 0 + 5 = 5 \equiv 5 \pmod{11} \\
3 \times 9 &= 27 + 5 = 32 \equiv 10 \pmod{11} \\
4 \times 5 &= 20 + 10 = 30 \equiv 8 \pmod{11} \\
5 \times 3 &= 15 + 8 = 23 \equiv 1 \pmod{11} \\
6 \times 9 &= 54 + 1 = 55 \equiv 0 \pmod{11} \\
7 \times 3 &= 21 + 0 = 21 \equiv 10 \pmod{11} \\
8 \times 1 &= 8 + 10 = 18 \equiv 7 \pmod{11} \\
9 \times 6 &= 54 + 7 = 61 \equiv 6 \pmod{11} \\
10 \times 6 &= 60 + 6 = 66 \equiv \boxed{0} \pmod{11}
\end{aligned}
$$

Portanto, o 11^o *dígito verificador é* **0**, *e o CPF completo torna-se:*

$$509.539.316\text{-}60$$

Resultado final: ***509.539.316-60****.*

15 Calendário Permanente a Partir de Janeiro de 1900

15.1 Tabela de meses

Valor	Meses
0	Outubro, Janeiro (ano não bissexto)
1	Maio
2	Agosto, Fevereiro (ano bissexto)
3	Março, Novembro, Fevereiro (ano não bissexto)
4	Junho
5	Setembro, Dezembro
6	Abril, Julho, Janeiro (ano bissexto)

15.2 Calendário padrão

S	D	S	T	Q	Q	S
0	1	2	3	4	5	6

15.3 Cálculos para obtenção do valor k

1. $x = \text{ANO} - 1 \equiv i \pmod 4$
2. $y = \dfrac{1}{4}(x - i)$
3. $(x + y) \equiv j \pmod 7$
4. $k = j$ (ano não bissexto); $k = j + 1$ (ano bissexto)

Exemplo 24. *Construir o calendário de Junho de 2026.*
2026 é um ano não bissexto. Tabela: Junho $= 4$.
Atualiza o calendário padrão para:

Q	*Q*	*S*	*S*	*D*	*S*	*T*
0	*1*	*2*	*3*	*4*	*5*	*6*

Cálculos para o valor de k:

1. $x = 2026 - 1 = 2025 \equiv 1 \pmod 4$
2. $y = \frac{1}{4}(2025 - 1) = \frac{1}{4}(2024) = 506$
3. $x + y = 2025 + 506 = 2531 \equiv 4 \pmod 7$
4. $k = 4$

Atualiza o calendário para:

D	*S*	*T*	*Q*	*Q*	*S*	*S*
0	$\boxed{4}$	*2*	*3*	*4*	*5*	*6*

Então temos Junho de 2026:

S	*T*	*Q*	*Q*	*S*	*S*	*D*
1	*2*	*3*	*4*	*5*	*6*	*7*
8	$\boxed{9}$	*10*	*11*	*12*	*13*	*14*
15	*16*	*17*	*18*	*19*	*20*	*21*
22	*23*	*24*	*25*	*26*	*27*	*28*
29	*30*					

09/06/2026: Terça-Feira.

Exemplo 25. *Queremos saber o dia da semana para a data 06/12/1964.*
Ano: 1964 (ano bissexto). Tabela: Dezembro $= 5$.
Atualiza o calendário padrão para:

Q	*S*	*S*	*D*	*S*	*T*	*Q*
0	*1*	*2*	*3*	*4*	*5*	*6*

Cálculos para o valor de k*:*

1. $x = 1964 - 1 = 1963 \equiv 3 \pmod 4$
2. $y = \frac{1}{4}(1963 - 3) = \frac{1}{4}(1960) = 490$
3. $x + y = 1963 + 490 = 2453 \equiv 3 \pmod 7$
4. $k = 3 + 1 = 4$ *(bissexto)*

Atualiza o calendário para:

S	*T*	*Q*	*Q*	*S*	*S*	*D*
0	$\boxed{4}$	*2*	*3*	*4*	*5*	*6*

Dezembro de 1964:

T	*Q*	*Q*	*S*	*S*	*D*	*S*
1	*2*	*3*	*4*	*5*	$\boxed{6}$	*7*
8	*9*	*10*	*11*	*12*	*13*	*14*
15	*16*	*17*	*18*	*19*	*20*	*21*
22	*23*	*24*	*25*	*26*	*27*	*28*
29	*30*	*31*				

06/12/1964: Domingo.

16 Exercícios Clássicos de Congruência Modular

Exercício 1

Qual é o resto da divisão de 2^{100} por 3?
$\phi(3) = 2$. Pelo Teorema de Euler: $2^{\phi(3)} = 2^2 \equiv 1 \pmod 3$.

$$2^{100} = (2^2)^{50} \equiv 1^{50} \equiv 1 \pmod 3; \qquad 2^{100} \equiv 1 \pmod 3.$$

Portanto, o resto da divisão de 2^{100} por 3 é **1**.

Exercício 2

Qual é o algarismo das unidades (o último dígito) do número 7^{2026}?

Seja $n = d_0 \times 10^0 + d_1 \times 10^1 + \cdots + d_m \times 10^n$. Então $n \equiv d_0 \pmod{10}$, $\forall n \in \mathbb{N}$.

$\phi(10) = 4$. Pelo Teorema de Euler: $7^{\phi(10)} = 7^4 \equiv 1 \pmod{10}$.

$$\frac{2026}{4} = 506 \text{ com resto } 2.$$

$$7^{2026} = 7^{2024} \cdot 7^2 = (7^4)^{506} \cdot 49 \equiv 1^{506} \cdot 49 \equiv 49 \equiv 9 \pmod{10}.$$

Portanto, o algarismo das unidades de 7^{2026} é **9**.

Exercício 3

Um bando de piratas encontrou uma arca cheia de moedas de ouro. Quando tentaram dividir as moedas igualmente por 5 piratas, sobraram 2 moedas. No dia seguinte, após uma briga onde dois piratas fugiram, tentaram dividir as mesmas moedas igualmente pelos 3 piratas restantes e sobrou 1 moeda. Qual o menor número possível de moedas que a arca continha?

Sistema:

$$x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}.$$

Dados: $a = 1$, $b = 3$, $c = 2$, $d = 5$.

$b^{-1} \bmod d = 3^{-1} \bmod 5 = 2$ (pois $3 \times 2 = 6 \equiv 1 \pmod{5}$).

$(c - a) = (2 - 1) = 1$.

$$x = b^{-1} \bmod d \cdot b \cdot (c - a) + a \pm b \cdot d \cdot w = 2 \times 3 \times 1 + 1 \pm 3 \times 5 \times w = 7 \pm 15w.$$

Para $w = 0$: $x = 7$ moedas.

Verificação: $7 \equiv 1 \pmod{3}$; $7 \equiv 2 \pmod{5}$. ✓

O menor número possível de moedas na arca é **7**.

Exercício 4

Encontrar os dois últimos dígitos do número 9^{1002}.

$\phi(100) = \phi(2^2 \times 5^2) = 2^1(2-1) \cdot 5^1(5-1) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$.

$$\frac{1002}{40} = 25 \text{ com resto } 2.$$

$$9^{1002} = (9^{40})^{25} \cdot 9^2 \equiv 1^{25} \cdot 81 \equiv 81 \pmod{100}.$$

Portanto, os dois últimos dígitos do número 9^{1002} são **8** e **1**.

Exercício 5

Prove que o número $n^7 - n$ é divisível por 42 para qualquer inteiro positivo n.

$42 = 2 \times 3 \times 7$. Precisamos mostrar que $n^7 - n$ é divisível por 2, 3 e 7.

7 é primo. Pelo Pequeno Teorema de Fermat: $n^6 \equiv 1 \pmod{7}$, logo $n^7 \equiv n \pmod{7}$, portanto $n^7 - n \equiv 0 \pmod{7}$, e 7 divide $n^7 - n$.

Fatorando:

$$n^7 - n = n(n^3 - 1)(n^3 + 1), \quad n^3 - 1 = (n-1)(n)(n+1).$$

$$n^7 - n = (n)(n-1)(n)(n+1)(n^3+1) = n(n-1)(n)(n+1)(n^3+1).$$

$(n-1)(n)(n+1)$ é o produto de 3 inteiros consecutivos, portanto divisível por 3, logo 3 divide $n^7 - n$.

Agora só precisamos mostrar que $n^7 - n$ é par:

$$n^7 - n = n(n^3 - 1)(n^3 + 1).$$

Se n é par, então 2 divide $n^7 - n$. Se n é ímpar, tanto $n^3 - 1$ quanto $n^3 + 1$ são pares, e o produto entre 2 pares é par, e o produto entre um ímpar (n) e um par $(n^3 - 1)(n^3 + 1))$ é par. Logo 2 divide $n^7 - n$. Isso conclui a prova. □

Exercício 6

Uma editora quer embalar livros em caixas. Se usarem caixas que levam exatamente 11 livros, sobram 4 livros fora. Se usarem caixas que levam 17 livros, falta exatamente 1 livro para preencher a última caixa (ou seja, sobram 16 livros). Sabendo que o estoque está entre 100 e 300 livros, qual o número exato de livros?

Sistema:

$$x \equiv 4 \pmod{11}, \quad x \equiv 16 \pmod{17}.$$

Dados: $a = 4$, $b = 11$, $c = 16$, $d = 17$. $(c - a) = 16 - 4 = 12$.

Algoritmo de Euclides para $b^{-1} \bmod d = 11^{-1} \bmod 17$:

	1	1	1	5
17, 11	6	5	1	0

$$\frac{6-1}{1} = 5, \qquad b^{-1} \bmod d = \frac{17 \times 5 - 1}{6} = \frac{84}{6} = 14.$$

$$x = [b^{-1} \bmod d] \cdot b \cdot (c-a) + a \pm b \cdot d \cdot w = 14 \times 11 \times 12 + 4 \pm 11 \times 17 \times w = 1852 \pm 187\, w.$$

$$\frac{1852}{187} = 9 + \text{resto } 169 \quad \Rightarrow \quad x = 169 \pm 187\, w.$$

Para $w = 0$: $x = 169$. Como $100 \leq 169 \leq 300$, o número exato de livros no estoque é **169**.