9 · 3 MOD 26 = 1

27 MOD 26 → 27 | 26
26 1
1

Exercícios P1.

01. Não vi como faz e não quero perder tempo.

02. Multiplique 2432 (7) por 263 (7)

```
      1
      3 2  1
    2 1 1
   ¹2 4 3 2 (7)
      2 6 3 (7)
  ¹1 ²0 ¹6 2 6
 ¹2 1 5 5 5
 5 1 6 4
 1 0 4 6 2 0 6
```

9 | 7 — 7, 1, 2
13 | 7 — 7, 1, 6
7 | 7 — 7, 1, 0
12 | 7 — 7, 1, 5
19 | 7 — 14, 2, 5
26 | 7 — 21, 3, 5
15 | 7 — 14, 2, 1
8 | 7 — 7, 1, 1
16 | 7 — 14, 2, 2
13 | 7 — 7, 1, 6

03. Multiplique 34524 (6) por 45 (6)

```
   2 3 3 1 2
   3 4 4 2 3
     3 4 5 2 4 (6)
           4 5 (6)
 ¹3 1 ¹0 3 1 2
 2 3 1 3 4 4
 3 0 2 4 1 5 2
```

20 | 6 — 18, 3, 2
13 | 6 — 12, 2, 1
27 | 6 — 24, 4, 3
24 | 6 — 24, 4, 0
19 | 6 — 18, 3, 1
16 | 6 — 12, 2, 4
10 | 6 — 6, 1, 4
21 | 6 — 18, 3, 3
19 | 6 — 18, 3, 1
15 | 6 — 12, 2, 3
7 | 6 — 6, 1, 1
6 | 6 — 6, 1, 0

___/___/___

H L K i Fs

5) B B

J P O L I (26)

T C C (26)

B T F^B C^B W Q

B T F C W Q

H A J O G W

H B D M O V M Q

7) Calcular 23^{-1} mod 61

1º MDC (23, 61) →

61	23^2	15^1	8^1	7^1	1^2
15	8	7	1	0	

⇒ 1

2º → 1º eq = $61 = 23 \cdot 2 + 15$

2º = $23 = 15 \cdot 1 + 8$

3º = $15 = 8 \cdot 1 + 7$

4º = $8 = 7 \cdot 1 + 1$

3º → $\boxed{1 = 8 - 1 \cdot 7}$ - 4º

Substituir o resto na 3º ($7 = 15 - 1 \cdot 8$)

$1 = 8 - 1 \cdot (15 - 1 \cdot 8)$

$1 = 8 - 1 \cdot 15 + 1 \cdot 8 = 1 = 2 \cdot 8 - 1 \cdot 15$ DOIS TERMOS

Subst. resto da equ. 2º ($8 = 23 - 15 \cdot 1$)

$1 = 2 \cdot (23 - 15 \cdot 1) - 1 \cdot 15$

$1 = 2 \cdot 23 - 3 \cdot 15$

Sub. resto da eq. 1º ($15 = 61 - 23 \cdot 2$)

$1 = 2 \cdot 23 - 3 \cdot (61 - 2 \cdot 23)$

$1 = 2 \cdot 23 - \cancel{3 \cdot 61} + 6 \cdot 23$

$1 = 2 \cdot 23 + 6 \cdot 23$

$\boxed{1 = 8 \cdot 23}$

Logo, 23^{-1} mod 61 = 8

61 / 1 / 0

$1 = 23 \cdot ?$

$1 = a \cdot a^{-1}$

$a \cdot a^{-1} = 1 \rightarrow 23 \cdot 8$ MOD 61 = 1

184 | 61

1 | 3

8 ✓

PROVA DO RESULTADO

$\cancel{3 \cdot 61}$ pois está por cima do módulo

IPOG INSPIRANDO Vidas

Lista: 1, ~~2~~, ~~3~~, ~~4~~, ~~5~~, ~~6~~, 14, 15

6- Calcular 9^{-1} mod 53

MDC (9, 53)

53	9^5	8^1	1^8	$\Rightarrow 1$
8	1	0		

1° $53 = 5 \cdot 9 + 8$

2° $9 = 1 \cdot 8 + 1$

$1 = 9 - 1 \cdot 8$

1° $8 = 53 - 5 \cdot 9$

$1 = 9 - 1 \cdot (53 - 5 \cdot 9)$

$1 = 9 - 1 \cdot \overset{=0}{53} + 5 \cdot 9$

$1 = 6 \cdot 9$, Logo, 9^{-1} mod $53 = 6$

$54 \,|\!\underline{\;53\;}$

$\underline{53}$ $\quad 1$

1

Calcular 7^{-1} mod 53

MDC (53, 7)

53	7^7	4^1	3^1	1^3	$\Rightarrow 1$
4	3	1	0		

$1^{\circ} \rightarrow$ $53 = 7 \cdot 7 + 4$

$2^{\circ} \rightarrow$ $7 = 1 \cdot 4 + 3$

$3^{\circ} \rightarrow$ $4 = 1 \cdot 3 + 1$

$4^{\circ} \rightarrow$ $3 = 3 \cdot 1 + 0$ → Resto 0 foda-se

$\boxed{1 = 4 - 1 \cdot 3}$

$3 = 7 - 1 \cdot 4$

$1 = 4 - 1 \cdot (7 - 1 \cdot 4) \Rightarrow 1 = 4 - 1 \cdot 7 + 1 \cdot 4 \Rightarrow \boxed{1 = 2 \cdot 4 - 1 \cdot 7}$

$4 = 53 - 7 \cdot 7$

$1 = 2(53 - 7 \cdot 7) - 1 \cdot 7 \Rightarrow 1 = 2 \cdot 53 + \underbrace{14 \cdot 7 - 1 \cdot 7}_{(14 - (-1)) \cdot 7} = \boxed{1 = 2 \cdot 53 - 7 \cdot 15}$

$-15 + 53 = \underline{38}$, 7^{-1} mod $53 = 38$

www.ipog.edu.br

IPOG
INSPIRANDO Vidas

Calcular $11^{-1} \bmod 53$

MDC(53, 11)

53	11^4	9^1	2^4	1^2
	9	2	1	0

$53 = 4 \cdot 11 + 9 \longrightarrow 9 = 53 - 4 \cdot 11$

$11 = 1 \cdot 9 + 2 \rightarrow 2 = 11 - 1 \cdot 9$

$9 = 4 \cdot 2 + 1$

$\boxed{1 = 9 - 4 \cdot 2}$

$(1+4) \cdot 9$

$1 = 9 - 4(11 - 1 \cdot 9) = 1 = 9 - 4 \cdot 11 + 4 \cdot 9 = \boxed{1 = 5 \cdot 9 - 4 \cdot 11}$

$1 = 5 \cdot (53 - 4 \cdot 11) - 4 \cdot 11$

$1 = 5 \cdot 53 + 5 \cdot (-4 \cdot 11) - 4 \cdot 11$

$1 = 5 \cdot 53 - 20 \cdot 11 - 4 \cdot 11$

$1 = 5 \cdot 53 - 24 \cdot 11$

$53 - 24 = 29$

$29 \cdot 11 = 319 \mid 53$; 318 ; 6 ; 1

Calcular $17^{-1} \bmod 53$

MDC(53, 17) =

53	17^3	2^8	1^2
	2	1	0

$53 = 3 \cdot 17 + 2$

$17 = 8 \cdot 2 + 1$

$\boxed{1 = 17 - 8 \cdot 2}$ $\quad 2 = 53 - 3 \cdot 17$

$1 = 17 - 8(53 - 3 \cdot 17)$

$1 = 17 - 8 \cdot 53 + 24 \cdot 17$

$1 = 25 \cdot 17 - 8 \cdot 53$

$17^{-1} \bmod 53 = 25$

$25 \cdot 17 = 425 \mid 53$; 424 ; 8 ; 1

Calcular $25^{-1} \bmod 53$

53	25^2	3^8	1^3
	3	1	0

$53 = 2 \cdot 25 + 3$

$25 = 8 \cdot 3 + 1 \quad \rightarrow 3 = 53 - 2 \cdot 25$

$\boxed{1 = 25 - 8 \cdot 3} \rightarrow 1 = 25 - 8(53 - 2 \cdot 25)$

$1 = 25 - 8 \cdot 53 + 16 \cdot 25$

$1 = 17 \cdot 25 - 8 \cdot 53$

$425 \mid 53$; 424 ; 8 ; 1

Logo = 17

4- Dividir $4051_{(7)}$ por $436_{(7)}$

$$
\begin{array}{r|l}
4051_{(7)} & 436_{(7)} \\
-3621_{(7)} & 6 \\
\hline
130 &
\end{array}
$$

Div = 6, resto 130

1436
2
1205

3436
5
3152

01- Traduzir a palavra representada em ASCII

01000011 - 01010010 - 01001001 - 01010000 - 01010100 - 01001111 -
67 C   82 R   73 I   80 P   84 T   79 O

- 01000111 - 01010010 - 01000001 - 01000110 - 01001001 - 01000001
71 G   82 R   65 A   70 F   73 I   65 A

0	1	0	0	0	0	1	1	= 67 = C
128	64	32	16	8	4	2	1	

0	1	0	1	0	0	1	0	= 82 = R
128	64	32	16	8	4	2	1	

07- Calcular $23^{-1} \bmod 61$ Já feita !!

MDC(61, 23) =

	23^2	15^1	8^1	7^1	1^7
61	23	15	8	7	1
15	8	7	1	0	

$61 = 2 \cdot 23 + 15 \quad (15 = 61 - 2 \cdot 23)\ 1°$

$23 = 1 \cdot 15 + 8 \quad (8 = 23 - 1 \cdot 15)\ 2°$

$15 = 1 \cdot 8 + 7 \quad (7 = 15 - 1 \cdot 8)\ 3°$

$8 = 1 \cdot 7 + 1 \to \boxed{1 = 8 - 1 \cdot 7}\ 4°$

$4°$ e $3°$: $1 = 8 - 1 \cdot (15 - 1 \cdot 8)$

$\boxed{1 = 8 - 15 + 1 \cdot 8} \to 4°$ e $2°$

$1 = 8 - 15 + 1 \cdot (23 - 1 \cdot 15) \Rightarrow \boxed{1 = 8 - 15 + 23 - 1 \cdot 15}$

$4°$ e $1°$ $\to 1 = 8 - 15 + 23 - 1 \cdot (61 - 2 \cdot 23)$

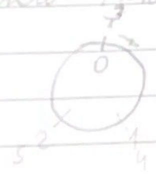
$1 = 16 - 1 \cdot 61 + 2 \cdot 23$

$1 = 2 \cdot 8 - 2 \cdot 23$

$23^{-1} \bmod 61 = 8$

08- Qual é a diferença entre aritmética modular e aritmética comum?

Na aritmética modular, os números "retrocedem" quando atin-
gem um certo valor, o módulo. Por exemplo, 7 mod 3 seria
1, enquanto 9 mod 3 seria 0



09. Encontre o $\phi(n)$ para todos os n's inteiros de 130 a 140.

$\phi(130) = $

130	2
65	5
13	13
1	

$(2^1 - 2^0) \cdot (5^1 - 5^0) \cdot (13^1 - 13^0)$

$2 - 1 \cdot 5 - 1 \cdot 13 - 1$

$1 \cdot 4 \cdot 12 = \underline{48}$

$\phi(131) = 131$ é primo $\rightarrow 131^1 - 131^0 = \underline{130}$

$\phi(132) = $

132	2
66	2
33	3
11	11
1	

$(2^2 - 2^1) \cdot (3^1 - 3^0) \cdot (11^1 - 11^0)$

$4 - 2 \cdot 3 - 1 \cdot 11 - 1$

$2 \cdot 2 \cdot 10 = \underline{40}$

$\phi(133) = $

133	7
19	19
1	

$\rightarrow (7^1 - 7^0) \cdot (19^1 - 19^0)$

$7 - 1 \cdot 19 - 1 = \underline{108}$

$\phi(134) = $

134	2
67	67
1	

$\rightarrow (2^1 - 2^0) \cdot (67^1 - 67^0)$

$2 - 1 \quad 67 - 1 = \underline{66}$

$\phi(135) = $

135	3
45	3
15	3
5	5
1	

$\rightarrow (3^3 - 3^2) \cdot (5^1 - 5^0)$

$27 - 9 \cdot 5 - 1$

$18 \cdot 4 = \underline{72}$

__/__/__

$$\phi(136) = \begin{array}{r|l} 136 & 2 \\ 68 & 2 \\ 34 & 2 \\ 17 & 17 \\ 1 & \end{array} \quad \rightarrow (2^3 - 2^2) \cdot (17^1 - 17^0)$$

$$8 - 4 \cdot 17 - 1 = \underline{64}$$

$\phi(137) = 137$ é primo logo $137^1 - 137^0 = \underline{136}$

$$\phi(138) = \begin{array}{r|l} 138 & 2 \\ 69 & 3 \\ 23 & 23 \\ 1 & \end{array} \quad (2^1 - 2^0) \cdot (3^1 - 3^0) \cdot (23^1 - 23^0)$$

$$2 - 1 \cdot 3 - 1 \cdot 23 - 1 = \underline{44}$$

$\phi(139) = 139$ é primo, logo $\underline{138}$

$$\phi(140) = \begin{array}{r|l} 140 & 2 \\ 70 & 2 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \quad (2^2 - 2^1) \cdot (5^1 - 5^0) \cdot (7^1 - 7^0)$$

$$4 - 2 \cdot 5 - 1 \cdot 7 - 1 = \underline{48}$$

10) MDC (437, 393) por Euclides e fatoração

$$(437, 393) = \begin{array}{c|c|c|c|c|c|c} 437 & 393^1 & 44^8 & 41^1 & 3^{13} & 2^1 & 1^2 \\ \hline 44 & 41 & 3 & 2 & 1 & 0 & \end{array} = 1$$

Fatoração $\rightarrow$ 437 . 393 | Não há fatores primos em comum, assim o MDC = $\underline{1}$

Primo $\quad$ 3 · 131

11_ 13^{28} mod 29

$a^{p-1} \equiv 1 \pmod{p}$ PEQUENO Fermat

$13^{28} \equiv 1 \pmod{29}$ $\quad$ p = 29 que é primo e 13 não divisível p/ 29

Logo: 13^{28} mod $29 = 1$

p-1

NÃO é primo

11^{33} mod 34 EXPONENCIAÇÃO

$b_5 b_4 \ldots b_0$ ... DEPOIS DO 0

Expoente para binário = 33 = 100001 (K=5)

d	K	i	b_i	a
d=1	5	5	$b_5=1$	11
d=1·1				
d=11·1 MOD 4=11				
d=11·11 MOD 34=19		4	$b_4=0$	
d=19·19 MOD 34=21		3	$b_3=0$	
d=21·21 MOD 34=33		2	$b_2=0$	
d=33·33 MOD 34=1		1	$b_1=0$	
d=1·1		0	$b_0=1$	
d=1·11=11				

$\boxed{\text{Logo } 11^{33} \text{ MOD } 34 = 11}$

12- Com o teorema de Fermat, encontre 3^{303} mod 11.

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

$p=11,\ a=3 \longrightarrow 3^{10} \equiv 1 \pmod{11}$

$3^{303} = 3^{10} \cdot 3^{10} \cdot 3^{3}$

$3^{30} \cdot 3^{3}$ mod 11

27 mod 11 = 5

13- a) MDC(32, 28) =

32	28 [1]	4 [7]
4	0	

= 4

b) MDC(187, 381) =

381	187 [2]	7 [26]	5 [1]	2 [2]	1 [2]
7	5	2	1	0	

= 1

c) MDC(841, 173).

841	173 [4]	149 [1]	24 [6]	5 [4]	4 [1]	1 [4]
149	24	5	4	1	0	

= 1

___/___/___

14- 160^{-1} mod 841

MDC (841, 160) =

841	160^5	41^3	37^1	4^9	1^4
41	37	4	1	0	

$841 = 5 \cdot 160 + 41 \quad (41 = 841 - 5 \cdot 160)$

$160 = 3 \cdot 41 + 37 \quad (\overline{37} = 160 - 3 \cdot 41)$

$41 = 1 \cdot 37 + 4 \quad (\underline{\overline{4}} = 41 - 1 \cdot 37)$

$37 = 9 \cdot 4 + 1$

$\hookrightarrow \boxed{1 = 37 - 9 \cdot \underline{4}}$

$1 = 37 - 9 \cdot (41 - 1 \cdot 37)$

$1 = 37 - 9 \cdot 41 + 9 \cdot 37 \rightarrow 1 = 37 \cdot 1 + 37 \cdot 9 - 9 \cdot 41$

$1 = 37 \cdot (1 + 9) - 9 \cdot 41$

$\boxed{1 = \underline{37} \cdot 10 - 9 \cdot 41}$

$1 = 10 \cdot (160 - 3 \cdot 41) - 9 \cdot 41$

$1 = 10 \cdot 160 - 10 \cdot 3 \cdot 41 - 9 \cdot 41 \rightarrow 1 = 10 \cdot 160 - 30 \cdot 41 - 9 \cdot 41$

$1 = 10 \cdot 160 - (30 + 9) \cdot 41$

$\boxed{1 = 10 \cdot 160 - 39 \cdot \underline{41}}$

$1 = 10 \cdot 160 - 39 \cdot (841 - 5 \cdot 160)$

$1 = 10 \cdot 160 - 39 \cdot 841 + 39 \cdot 5 \cdot 160 \rightarrow 1 = 10 \cdot 160 + 195 \cdot 160 - 39 \cdot 841$

$1 = (195 + 10) \cdot 160 - 39 \cdot 841$

$\boxed{1 = 205 \cdot 160 - 39 \cdot 841}$

$\hookrightarrow 160^{-1} \bmod 841 = \underline{205}$

15- 1234^{-1} mod 4321

4321	1234^3	619^1	615^1	4^{153}	3^1
619	615	4	3	1	

$4321 = 1234 \cdot 3 + 619$

$1234 = 619 \cdot 1 + 615$

$619 = 615 \cdot 1 + 4$

$615 = 4 \cdot 153 + 3$

$4 = 3 \cdot 1 + 1$

www.ipog.edu.br

IPOG
INSPIRANDO Vidas

___/___/___

Feito no Quadro pelo Professor

$1 = 4 - 1 \cdot (615 - 4 \cdot 153)$

$1 = 4 \cdot 154 - 615$

$1 = 154(619 - 615 \cdot 1) - 615$

$1 = 154 \cdot 619 - 155 \cdot 615$

$1 = 154 \cdot 619 - 155 \cdot (1234 - 619 \cdot 1)$

$1 = 309 \cdot 619 - 155 \cdot 1234$

$1 = 309 \cdot (4321 - 1234 \cdot 3) - 155 \cdot 1234$

$1 = 309 \cdot 4321 - 1082 \cdot 1234$

$\boxed{1 = 4321 \cdot 309 - 1234 \cdot 1082}$

$-1082 + 4321 = \underline{3239}$

16 - a) $7x \equiv 6 \mod 19$

$x \equiv 6 \cdot \underbrace{7^{-1} \bmod 19}$

19	7^2	5^1	2^2
5	2	1	

$19 = 2 \cdot 7 + 5 \rightarrow \underline{5} = 19 - 2 \cdot 7$

$7 = 1 \cdot 5 + 2 \rightarrow \underline{2} = 7 - 1 \cdot 5$

$5 = 2 \cdot 2 + 1 \rightarrow 1 = 5 - 2 \cdot \underline{2}$

$1 = 5 - 2(7 - 1 \cdot 5) \Rightarrow 1 = 5 - 2 \cdot 7 + 2 \cdot 1 \cdot 5$

$1 = 1 \cdot 5 + 2 \cdot 5 - 2 \cdot 7 \Rightarrow 1 = 3 \cdot \underline{5} - 2 \cdot 7$

$1 = 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7$

$1 = 3 \cdot 19 - 3 \cdot 2 \cdot 7 - 2 \cdot 7 \Rightarrow 1 = 3 \cdot 19 - 6 \cdot 7 - 2 \cdot 7$

$\Rightarrow 1 = -8 \cdot 7 + 3 \cdot 19$

$19 - 8 = \underline{11}$

$(11 \cdot 7)x \equiv 11 \cdot 6 \bmod 19$

$x \equiv 66 \bmod 19$

$66 \div 19 \cong 3$

$66 - (3 \cdot 19) = \boxed{x = 9}$

www.ipog.edu.br

IPOG
INSPIRANDO Vidas

b. $6x \equiv 4 \mod 13$

$x \equiv 4 \cdot 6^{-1} \mod 13$

$$\begin{array}{c|c} 13 & 6^{2} \\ 1 & \end{array}$$

$13 = 2 \cdot 6 + 1$

$1 = 13 - 2 \cdot 6$

$-2 + 13 = \underline{11}$

$6^{-1} \mod 13 = \underline{11}$

$x \equiv 4 \cdot 11 \mod 13$

$x \equiv 44 \mod 13$

$$\begin{array}{r|l} 44 & 13 \\ \underline{39} & 3 \\ 5 & \end{array}$$

$\Rightarrow \underline{x = 5}$

C. $9x \equiv 3 \mod 17$

$x = 3 \cdot 9^{-1} \mod 17$

$$\begin{array}{c|c|c} 17 & 9^{1} & 8^{1} \\ \hline 8 & 1 & \end{array}$$

$17 = 1 \cdot 9 + 8 \rightarrow 8 = 17 - 1 \cdot 9$

$9 = 1 \cdot 8 + 1$

$\hookrightarrow 1 = 9 - 1 \cdot 8$

$1 = 9 - 1 \cdot (17 - 1 \cdot 9)$

$1 = 9 - 1 \cdot 17 + 1 \cdot 9$

$1 = 2 \cdot 9 - 1 \cdot 17$

$x = 2$

$9x \equiv 3 \mod 17$

$\hookrightarrow (9 \cdot 2)\, x \equiv 3 \mod 17$ por 2

$18x \equiv \underbrace{2 \cdot 3}_{} \mod 17$

$6 \mod 17$

$18 \equiv 1 \mod 17$

$\underline{x = 6}$

$$\begin{array}{r|l} 17 & 6 \\ \underline{16} & 3 \\ 1 & \end{array}$$

D. $12x \equiv 10 \mod 23$

$x = 10 \cdot 12^{-1} \mod 23$

$$\begin{array}{c|c|c} 23 & 12^{1} & 11^{1} \\ 11 & 1 & \end{array} \begin{cases} 23 = 1 \cdot 12 + 11 \\ 12 = 1 \cdot 11 + 1 \end{cases}$$

$1 = 12 - 1 \cdot 11 \rightarrow 1 = 12 - 1 \cdot (23 - 1 \cdot 12)$

$1 = 12 - 1 \cdot 23 + 1 \cdot 12$

$1 = 2 \cdot 12 - 1 \cdot 23$

$\hookrightarrow 12^{-1} \mod 23 = 2$

$x = 10 \cdot 2 \mod 23$

$x = 20 \mod 23$

$\rightarrow x = 20$

www.ipog.edu.br

IPOG INSPIRANDO Vidas