*Duração: 45m* **Teste 3A** 26/11/08

SOLUÇÕES

---

1. Determine o valor lógico das seguintes afirmações.

| | V | F |
|---|---|---|
| (a) $3456 \bmod 23 = 1111 \bmod 23$. | | × |
| (b) $\text{mdc}(2 \times 3 \times 5 \times 7, 2^2 \times 3 \times 5) = 60$. | | × |
| (c) Se $p$ e $q$ são primos e $2 < p < q$, então $p \equiv_2 q$. | × | |
| (d) Se $p$ é um inteiro tal que $p > 1$, $((p\|a) \wedge (p\|b)) \Rightarrow a + b$ é primo. | | × |

2. (a) Usando o algoritmo de Euclides, calcule $\text{mdc}(29, 22)$ (apresente os diversos passos do algoritmo).

R.:

$$29 = 22 \times 1 + 7$$

$$22 = 7 \times 3 + \boxed{1}$$

$$7 = 1 \times 7 + 0$$

Portanto, $\text{mdc}(29, 22) = 1$.

(b) Determine inteiros $r$ e $s$ tais que $1 = 29r + 22s$.

R.: $r = -3$ e $s = 4$.

(c) Determine todas as soluções inteiras da congruência linear $22x \equiv_{29} 1$.

R.: $x \in \{4 + 29k \mid k \in \mathbb{Z}\}$.

(d) Descodifique a mensagem

$$*\text{PIBE}*\smile\text{D}\smile\text{W@P}$$

que foi encriptada utilizando o alfabeto da figura e a função $f(p) = (22p + 25) \bmod 29$ (Nota: o símbolo $\smile$ indica um espaço em branco).

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | X | Y | Z | W | $*$ | @ | $\smile$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ | $\updownarrow$ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |

R.: ESTUDEM$\smile$MAIS

---

RESOLUÇÃO

1. (a) $3456 = 23 \times 150 + 6$ pelo que $3456 \bmod 23 = 6$; por outro lado, $1111 = 23 \times 48 + 7$ donde $1111 \bmod 23 = 7$.

   (b) $\mathrm{mdc}(2 \times 3 \times 5 \times 7, 2^2 \times 3 \times 5) = 2 \times 3 \times 5 = 30$.

   (c) Se $p$ e $q$ são primos maiores do que 2 então são, em particular, números ímpares. Portanto, $p \equiv_2 1$ e $q \equiv_2 1$ pelo que $p \equiv_2 q$.

   (d) Se $p|a$ e $p|b$ então $a = k_1 p$ e $b = k_2 p$ para algum par de inteiros $k_1, k_2$. Logo $a + b = (k_1 + k_2)p$, o que mostra que $a+b$ não é necessariamente um número primo (por exemplo: para $p = 4$, $a = 8$ e $b = 12$ tem-se $a + b = 20$ que não é primo).

2. (a) O mdc é o último resto não nulo da sequência de divisões inteiras no algoritmo de Euclides.

   (b) Da alínea anterior sabemos que

$$\boxed{\begin{array}{c} 29 = 22 \times 1 + 7 \\ \\ 22 = 7 \times 3 + \boxed{1} \\ \\ 7 = 1 \times 7 + 0 \end{array}}$$

   Assim, da penúltima divisão tiramos $\boxed{1} = 22 + 7 \times (-3) \quad (*)$.

   Em seguida tiramos da primeira divisão efectuada que 7 é igual a $29 + 22 \times (-1)$. Substituindo em $(*)$ obtemos

$$\boxed{1} = 22 + 7 \times (-3) = 22 + (29 + 22 \times (-1)) \times (-3) = 29 \times (-3) + 22 \times 4.$$

   (c) Como $1 = 29 \times (-3) + 22 \times 4$ (alínea anterior), podemos concluir que $1 \equiv_{29} 22 \times 4$. Portanto, $x = 4$ é solução da congruência dada. Imediatamente, todas as soluções são da forma $x = 4 + 29k$ para $k \in \mathbb{Z}$.

   (d) `Cálculo da função de desencriptação (inversa de` $f$`):`

$$\boxed{\begin{array}{rcl} f(p) = (22p + 25) \bmod 29 & \Leftrightarrow & f(p) \equiv_{29} (22p + 25) \\ & \Leftrightarrow & f(p) + 4 \equiv_{29} 22p \\ & \Leftrightarrow & 4 \times (f(p) + 4) \equiv_{29} 4 \times 22p \\ & \Leftrightarrow & 4 \times (f(p) + 4) \equiv_{29} p \\ & \Leftrightarrow & p = 4(f(p) + 4) \bmod 29. \end{array}}$$

   Portanto, a função inversa de $f$ é a função $g$ definida por $g(q) = 4(q + 4) \bmod 29$. Assim:

   $g(*) = g(26) = 4(26 + 4) \bmod 29 = (4 \times 30) \bmod 29 = (4 \times 1) \bmod 29 = 4 =$E.

   $g(\mathrm{P}) = g(15) = 4(15 + 4) \bmod 29 = (4 \times 19) \bmod 29 = 18 =$S.

   $g(\mathrm{I}) = g(8) = 4(8 + 4) \bmod 29 = (4 \times 12) \bmod 29 = 19 =$T.

   $g(\mathrm{B}) = g(1) = 4(1 + 4) \bmod 29 = (4 \times 5) \bmod 29 = 20 =$U.

   $g(\mathrm{E}) = g(4) = 4(4 + 4) \bmod 29 = (4 \times 8) \bmod 29 = 32 \bmod 29 = 3 =$D.

   $g(*) =$E.

   $g(\smile) = g(28) = 4(28 + 4) \bmod 29 = (4 \times 32) \bmod 29 = (4 \times 3) \bmod 29 = 12 =$M.

   $g(\mathrm{D}) = g(3) = 4(3 + 4) \bmod 29 = (4 \times 7) \bmod 29 = 28 = \smile$.

$g(\smile) =$M.

$g(\mathrm{W}) = g(25) = 4(25+4) \bmod 29 = (4 \times 29) \bmod 29 = 0 =$A.

$g(@) = g(27) = 4(27+4) \bmod 29 = (4 \times 31) \bmod 29 = (4 \times 2) \bmod 29 = 8 =$I.

$g(\mathrm{P}) =$S.

As resoluções dos restantes testes são análogas.

---

## SOLUÇÕES

### TESTE 3B

1(a)
$$\begin{array}{|c|}\hline 29 = 11 \times 2 + 7 \\ 11 = 7 \times 1 + 4 \\ 7 = 4 \times 1 + 3 \\ 4 = 3 \times 1 + \boxed{1} \\ 3 = 1 \times 3 + 0 \\ \hline \end{array}$$

(b) $r = -3, s = 8$

(c) $8 + 29k$ $(k \in \mathbb{Z})$

(d) $g(q) = 8(q+1) \bmod 29$. PRATIQUEM$\smile$MAIS

2(a) F

(b) V

(c) V

(d) V

### TESTE 3C

1(a) F

(b) F

(c) V

(d) V

2(a)
$$\begin{array}{|c|}\hline 29 = 22 \times 1 + 7 \\ 22 = 7 \times 3 + \boxed{1} \\ 7 = 1 \times 7 + 0 \\ \hline \end{array}$$

(b) $r = -3, s = 4$

(c) $4 + 29k$ $(k \in \mathbb{Z})$

(d) $g(q) = 4(q+4) \bmod 29$. ESTUDEM$\smile$MAIS

### TESTE 3D

1(a)
$$\begin{array}{|c|}\hline 29 = 11 \times 2 + 7 \\ 11 = 7 \times 1 + 4 \\ 7 = 4 \times 1 + 3 \\ 4 = 3 \times 1 + \boxed{1} \\ 3 = 1 \times 3 + 0 \\ \hline \end{array}$$

(b) $r = -3, s = 8$

(c) $8 + 29k$ $(k \in \mathbb{Z})$

(d) $g(q) = 8(q+1) \bmod 29$. PRATIQUEM$\smile$MAIS

2(a) F

(b) V

(c) V

(d) V