Duração: 30m **Teste 3A** 21/11/07

SOLUÇÕES

A segunda questão é de escolha múltipla; uma resposta certa terá a cotação máxima que lhe for atribuída e uma resposta errada perderá metade dessa cotação (desde que a nota do teste permaneça não negativa).

---

1. Considere o algoritmo seguinte que permite calcular o valor da função *soma* em cada inteiro positivo n dado.

   `procedure` *soma* (n: inteiro positivo)
   $soma := 0$ {valor inicial da soma}
   `for` $i := 1$ `to` n
      `for` $j := 1$ `to` i
         $soma := soma + 1$;

   (a) Calcule $soma(6)$. R.: 21

   (b) Determine $soma(n)$. R.: $\dfrac{n^2+n}{2}$

2. Determine o valor lógico das seguintes afirmações.

	V	F
(a) $2131 \bmod 19 = 1903 \bmod 19 = 1$.		×
(b) $147 \equiv_{75} -3$.	×	
(c) Se p é primo e $p \mid ab \Rightarrow (p \mid a)$ ou $(p \mid b)$.	×	
(d) Seja $\phi(n)$ o número de inteiros positivos menores que n que são primos com n. Então $\phi(11) < \phi(16)$.		×

3. Descodifique a mensagem "DMDCPQO", que foi encriptada com a função

$$f(p) = (3p+3) \bmod 23,$$

identificando as 23 letras do alfabeto pelos inteiros $0, 1, 2, \ldots, 22$ (como mostra a figura).

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

R.: ATAQUEM

RESOLUÇÃO

1(a) Como o valor incial da variável *soma* é 0, e em cada passo dos dois ciclos do algoritmo, este valor cresce uma unidade, então

$$soma(6) = \sum_{i=1}^{6}\sum_{j=1}^{i} 1 = \sum_{i=1}^{6} i = 1+2+3+4+5+6 = 21.$$

(b) De modo análogo, usando a fórmula para a soma dos primeiros n naturais obtida nas aulas,

$$soma(n) = \sum_{i=1}^{n}\sum_{j=1}^{i} 1 = 1+2+3+\cdots+n = \frac{n^2+n}{2}.$$

2(a) É falsa porque, como $1903 = 100 \times 19 + 3$, então $1903 \bmod 19 = 3$.

(b) É verdadeira pois $147 \bmod 75 = 72$ e $-3 \bmod 75$ também é igual a 72 (ou, equivalentemente, porque $147 - (-3) = 150$ é múltiplo de 75).

(c) É claramente verdadeira: se considerarmos as factorizações primas de a e b, o seu produto ab, sendo divisível por p, terá que conter o factor p entre ele; logo, necessariamente, ou p aparece na factorização prima de a (o que significa que $p \mid a$) ou aparece na de b (o que significa que $p \mid b$).

(d) Como 11 é primo, qualquer inteiro positivo $a < n$ é primo com n, pelo que $\phi(11) = 10$. Por outro lado, como $16 = 2^4$, então entre os inteiros positivos inferiores a 16 só os números ímpares são primos com 16. Portanto, só os números 1, 3, 5, 7, 9, 11, 13 e 15 são primos com 16. Logo $\phi(16) = 8 < \phi(11)$ e a afirmação é falsa.

3) Pela definição da função f de codificação, $f(A) = f(0) = 3 \bmod 23 = 3 = D$. Portanto, a primeira letra na palavra original é o A. Analogamente, $f(B) = f(1) = 6 \bmod 23 = 6 = G$, $f(C) = f(2) = 9 \bmod 23 = 9 = J$, etc. Observando, nesta sequência, que a codificação da letra seguinte avança três posições no alfabeto, obtemos imediatamente a tabela

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z
$f\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
$\boxed{\text{D}}$	G	J	N	$\boxed{\text{Q}}$	T	X	B	E	H	L	$\boxed{\text{O}}$	R	U	Z	$\boxed{\text{C}}$	F	I	$\boxed{\text{M}}$	$\boxed{\text{P}}$	S	V	A

Portanto, descodificando pela correspondência inversa de f obtemos DMDCPQO→ATAQUEM.

Outra resolução: Conhecemos a função de codificação f, mas para descodificar uma palavra precisamos de conhecer a função inversa de f; calculemo-la, isto é, dado $f(p) = (3p+3) \bmod 23$ determinemos o valor original p:

$$\begin{aligned}
f(p) \bmod 23 = (3p+3) \bmod 23 \quad &\Leftrightarrow \quad f(p) \equiv_{23} 3p+3 \\
&\Leftrightarrow \quad f(p) - 3 \equiv_{23} 3p \\
&\Leftrightarrow \quad 8(f(p)-3) \equiv_{23} 24p \\
&\Leftrightarrow \quad 8(f(p)-3) \equiv_{23} p \\
&\Leftrightarrow \quad p = 8(f(p)-3) \bmod 23.
\end{aligned}$$

Portanto, se $f(p) = q$, o valor original $p = f^{-1}(q)$ pode ser recuperado pela identidade

$$f^{-1}(q) = 8(q-3) \bmod 23.$$

Podemos agora calcular imediatamente a palavra original:

$$
\begin{aligned}
&f^{-1}(D) = f^{-1}(3) = 8(3-3) \bmod 23 = 0 = A\\
&f^{-1}(M) = f^{-1}(11) = 8(11-3) \bmod 23 = 18 = T\\
&f^{-1}(C) = f^{-1}(2) = 8(2-3) \bmod 23 = 15 = Q\\
&f^{-1}(P) = f^{-1}(14) = 8(14-3) \bmod 23 = 19 = U\\
&f^{-1}(Q) = f^{-1}(15) = 8(15-3) \bmod 23 = 4 = E\\
&f^{-1}(O) = f^{-1}(13) = 8(13-3) \bmod 23 = 11 = M
\end{aligned}
$$

As resoluções dos restantes testes são análogas.

SOLUÇÕES

TESTE 3B

1(a) 28

(b) $\dfrac{n^2+n}{2}$

2(a)		×
(b)	×	
(c)		×
(d)	×	

3) EMPATEM

TESTE 3C

1(a) 21

(b) $\dfrac{n^2+n}{2}$

2(a)		×
(b)	×	
(c)		×
(d)	×	

3) DEFENDAM

TESTE 3D

1(a) 21

(b) $\dfrac{n^2+n}{2}$

2(a)	×	
(b)		×
(c)	×	
(d)		×

3) ESTUDEM
