INTEIROS E CONGRUÊNCIAS

1 A definição de quociente de dois inteiros a e b parte da igualdade a=qb+r com 0≤r<|b|. Tenha em atenção as funções do Excel:

QUOTIENT(a,b) - Returns the integer portion of a division.

MOD(a,b) - Returns the remainder after number is divided by divisor. The result has the same sign as divisor.

INT(x) - Rounds a number down to the nearest integer.

FLOOR(x,s) - Rounds number down, to the nearest multiple of s.

CEILING(x,s) - Returns number rounded up, to the nearest multiple of s.

Calcule:

a) O quociente (Q) e o resto (R) da divisão de 3958 por 18, -3958 por 18, 3958 por -18, -3958 por -18, usando as funções QUOTIENT e MOD e usando as definições da aula teórica.

b) Reconstrua o dividendo a partir de Q e de R em ambos os casos. O que pode concluir?

c) Proponha fórmulas no Excel para obter o quociente e o resto de acordo com as definições da aula teórica.

2 Obtenha a representação binária, octal e hexadecimal de 57483 (base 10).

3 Seja o número natural N, na base b, $(a_{n-1}\ldots a_0)_b$, com $a_{n-1}>0$.

a) Prove que $n-1=\lfloor \log_b N \rfloor$ e portanto N tem $1+\lfloor \log_b N \rfloor$ dígitos na base b.

b) Quantos dígitos tem 2^{64} na sua representação na base 10?

c) E 5 000 000 000 na base 2?

4 Mostre que 17369 e 5472 são primos entre si. Determine os inteiros *m* e *n* tais que 17369m+5472n=1.

5 Obtenha a decomposição em fatores primos de 21340 e de 88. Calcule o mdc e o mmc.

6 Obtenha a decomposição em fatores primos de 13331.

7 Máximo divisor comum.

a) Prove que, dados dois inteiros a e b, mdc(a,b)mmc(a,b)=|ab|.

b) Usando o resultado da alínea anterior, calcule o mdc(1575, 231) e o mmc(1575, 231).

8 Obtenha todos os inteiros x, 0≤x<n, que satisfazem as seguintes congruências

a) $3x \equiv 4 \ (mod\ 6)$

b) $4x \equiv 3 \ (mod\ 7)$

c) $2x \equiv 18 \ (mod\ 50)$

9 Calcule o inverso de 5 (mod 7) e de 500 (mod 8191).

10 Resolva o sistema de congruências

a) $\begin{cases} 2x+3y \equiv 4 \ (mod\ 5) \\ 4x-y \equiv 1 \ (mod\ 5) \end{cases}$

b) $\begin{cases} 3x + y \equiv 1 \ (mod\ 4) \\ 2x - 2y \equiv 2 \ (mod\ 4) \end{cases}$

11 Calcule o valor das seguintes expressões:

a) $(579)^{39}$ (mod 59).

b) 18^{8970} (mod 8971).

c) $18^{8971} + 18^{8974}$ (mod 8971).

12 Calcule, módulo p, a sequência c, 2c, …, (p-1)c para p=11 nos casos c=5 ou c=15. Calcule em cada caso c^{p-1}. Confronte com a demonstração do Pequeno Teorema de Fermat.

13 O código internacional dos livros ISBN (International Standard Book Number) tem 10 dígitos, o qual identifica o país de publicação, o editor e o livro propriamente dito nos primeiros 9 dígitos. O décimo é um dígito de verificação (check digit) que é calculado a partir dos outros de forma a que a seguinte congruência se verifique

$$a_1 + 2a_2 + 3a_3 + \cdots + 9a_9 + 10a_{10} \equiv 0 \ (mod\ 11)$$

No caso de a_{10}=10 escreve-se X.

Calcule o dígito de verificação para um novo livro cujos primeiros 9 dígitos são

0-13-602079. Qualquer alteração num único dígito dá erro na comparação com o dígito de verificação. Mude o 5º dígito de 0 para 9 e teste a correção do novo código.

14 O número de identificação fiscal em Portugal é constituído por 9 dígitos NIF=(a_1, a_2, …, a_9), sendo que o último é calculado de molde que NIF.w (mod 11) = 0, em que w=(9,8,7,6,5,4,3,2,1), isto é

$$9a_1 + 8a_2 + 7a_3 + \cdots + 2a_8 + a_9 \equiv 0 \ (mod\ 11)$$

No caso de a_9=10 escreve-se 0.

a) Verifique se o seguinte NIF está correto: 154584908.

b) Qual o dígito de verificação do NIF 50141319C?

15 Suponha que tem um processador só com inteiros de 8 bits mas que precisa de representar (e fazer operações…) com números maiores. Recorrendo ao teorema chinês dos restos, guarda em três bytes os seguintes números: 21, 48, 88, correspondendo, respetivamente aos restos da divisão do número x por 5^2, 7^2 e 11^2. Qual o número x?

16 Pretende-se montar um sistema de encriptação RSA para a receção de mensagens curtas. Para isso, escolhem-se dois primos p=127 e q=131. O número auxiliar é s=11.

a) No contexto de preparação da comunicação, calcule os números necessários à descodificação a e b, que são os inversos de s módulo (p-1) e (q-1) respetivamente.

b) Sendo a codificação dos carateres dados por a-01, b-02, …, obtenha o número correspondente à palavra “abrame”. Se for demasiado grande para as chaves escolhidas (r=pq=16637, s=11), segmente-o em dois blocos. Calcule o criptograma para enviar.

c) Desencripte o criptograma recebido, para verificação.