Departamento de Matemática da Universidade de Coimbra

Teoria dos Números

Exame final – 3 de Fevereiro de 2003

1. Sejam b e c inteiros não ambos nulos e seja $(b, c) = d$. Prove que, se um inteiro t for soma de um múltiplo de b com um múltiplo de c (isto é, se existirem inteiros x e y tais que $bx + cy = t$), então $d \mid t$.

2. Um número natural n tem como divisores primos apenas os números 2 e 5. Se dividirmos n por 25 obtemos um número inteiro cujo número de divisores é metade do número de divisores de n. Determine o menor valor que n pode tomar.

3. (a) Sendo m um número natural, defina sistema reduzido de resíduos módulo m.

   (b) Se $\{r_1, r_2, \ldots, r_k\}$ for um sistema reduzido de resíduos módulo m e a um inteiro tal que $(a, m) = 1$, prove que $\{ar_1, ar_2, \ldots, ar_k\}$ é um sistema reduzido de resíduos módulo m.

   (c) Enuncie e demonstre o Teorema de Euler (ou Grande Teorema de Fermat).

   se $(a,m) = 1$, $a^{\varphi(m)} \equiv 1 \pmod m$

4. Prove que $11 \cdot 31 \cdot 61 \mid 20^{15} - 1$.

5. Determine todos os inteiros u compreendidos entre 2000 e 3000 que satisfazem simultaneamente $5u \equiv 3 \pmod 4$, $3u \equiv 1 \pmod 5$ e $u \equiv 6 \pmod 7$.

6. Sejam a e b dois números naturais primos entre si, de paridades diferentes e com $a > b$. Ponhamos

$$x = a^2 - b^2\,, \quad y = 2ab\,, \quad z = a^2 + b^2\,.$$

   Prove que, então, (x, y, z) é um trio pitagórico primitivo.

   $(x,y,z) = 1$

Teoria dos Números

Resumo da resolução do exame de 3/2/2003

1. Como $d \mid b$ e $d \mid c$, tem-se que $d \mid bx + cy$.

2. Como os únicos divisores primos de n são 2 e 5, n é da forma $2^\alpha 5^\beta$, com $\alpha, \beta \in \mathbb{N}$. Daqui segue-se que o número de divisores de n é $(\alpha+1)(\beta+1)$

   Como ao dividirmos n por 25 obtemos um número inteiro, podemos afirmar que $\beta \geq 2$, tendo-se

   $$\frac{n}{25} = 2^\alpha 5^{\beta-2}.$$

   Daqui segue-se que o número de divisores de $\frac{n}{25}$ é $(\alpha+1)(\beta-1)$.

   Como este número é metade do número de divisores de n, temos que

   $$(\alpha+1)(\beta-1) = \frac{(\alpha+1)(\beta+1)}{2}$$

   donde se tira que $\beta = 3$. O menor valor possível para n obtém-se tomando $\alpha = 1$.

   O menor valor que n pode tomar satisfazendo as condições indicadas é então

   $$n = 2 \cdot 5^3 = 250.$$

3. Pergunta teórica directa.

4. Como 11, 31 e 61 são primos (bastaria serem primos dois a dois), o seu produto divide um número se e só se cada um deles divide esse número.

   Vejamos primeiro que $11 \mid 20^{15} - 1$. Como $20 \equiv -2 \pmod{11}$, tem-se $20^{15} \equiv -2^{15} \pmod{11}$. Como $2^5 \equiv -1 \pmod{11}$, tem-se $2^{15} \equiv -1 \pmod{11}$. Segue-se que $20^{15} \equiv 1 \pmod{11}$, c.q.d.

   Vejamos agora que $31 \mid 20^{15} - 1$. Como $31 \cdot 13 = 403$, tem-se $20^2 \equiv -3 \pmod{31}$, donde $20^{14} \equiv -3^7 \pmod{31}$. Como $3^3 \equiv -4 \pmod{31}$, tem-se $3^6 \equiv 16 \pmod{31}$. Segue-se que $20^{15} \equiv (-3) \cdot 10 \cdot 2 \cdot 3^6 \equiv -30 \equiv 1 \pmod{31}$, c.q.d.

   Alternativa: Como $20^3 \equiv 2 \pmod{31}$, tem-se $20^{15} \equiv 2^5 \pmod{31}$, e $2^5 \equiv 1 \pmod{31}$, c.q.d.

   Provemos finalmente que $61 \mid 20^{15} - 1$. Como $3^4 \equiv 20 \pmod{61}$, tem-se $20^{15} \equiv 3^{60} \pmod{61}$. Como $\varphi(61) = 60$, pelo Pequeno Teorema de Fermat tem-se $3^{60} \equiv 1 \pmod{61}$, c.q.d.

   Alternativa: Como $20^3 \equiv 9 \pmod{61}$, tem-se $20^{15} \equiv 9^5 \pmod{61}$. Ora $9^5 \equiv 1 \pmod{61}$, pelo que $20^{15} \equiv 1 \pmod{61}$, c.q.d.

5. A primeira observação é que não se pode aplicar directamente o teorema chinês dos resíduos, porque este só se refere a sistemas de congruências em que o coeficiente da incógnita é igual a 1.

Comecemos então por analisar separadamente as duas primeiras congruências.

Resolvendo-as, vemos que

$$5u \equiv 3 \pmod 4 \iff u \equiv 3 \pmod 4 \quad \text{e} \quad 3u \equiv 1 \pmod 5 \iff u \equiv 2 \pmod 5.$$

Interessam-nos assim os inteiros u que satisfazem simultaneamente

$$\begin{cases} u \equiv 3 \pmod 4 \\ u \equiv 2 \pmod 5 \\ u \equiv 6 \pmod 7 \end{cases}$$

A este sistema já se pode aplicar o teorema chinês dos resíduos (note-se que 4, 5 e 7 são primos dois a dois).

Ponhamos $m_1 = 4$, $m_2 = 5$, $m_3 = 7$ e $m = m_1m_2m_3 = 140$. Resolvendo as três congruências $\frac{m}{m_j}b_j \equiv 1 \pmod{m_j}$, $j = 1, 2, 3$, obtemos $b_1 = 3$, $b_2 = 2$ e $b_3 = 6$.

Uma solução comum das três congruências iniciais é então

$$\frac{m}{m_1}3b_1 + \frac{m}{m_2}2b_2 + \frac{m}{m_3}6b_3 = 1147.$$

O conjunto completo das soluções é a classe de congruência $[1147]_{140} = \{1147 + k.140 : k \in \mathbb{Z}\}$.

Entre 2000 e 3000 há exactamente sete soluções: 2127, 2267, 2407, 2547, 2687, 2827 e 2967.

6. x, y e z constituem um trio pitagórico se $x^2 + y^2 = z^2$. Verifiquemos se os números dados satisfazem essa condição:

$$x^2 + y^2 = (a^2 - b^2)^2 + (2ab)^2 = a^4 - 2a^2b^2 + b^4 + 4a^2b^2 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2.$$

Um trio pitagórico diz-se primitivo se os três números em causa forem primos entre si. Verifiquemos se os números dados satisfazem essa condição. Seja d o máximo divisor comum de x, y e z. Como $d \mid a^2 - b^2$ e $d \mid a^2 + b^2$, tem-se que $d \mid 2a^2$ e $d \mid 2b^2$. Logo, $d \mid 2(a^2, b^2)$. Como a e b são primos entre si, a^2 e b^2 também o são, pelo que $d \mid 2$. Mas d não pode ser igual a 2, porque d divide x e z e estes são ímpares. Logo, tem-se $d = 1$ e, portanto, x, y e z constituem um trio pitagórico primitivo.

Cotação:

1. 2
2. 3
3. (a) 1.5
   (b) 2
   (c) 2
4. 3.5
5. 3.5
6. 2.5