Departamento de Matemática da Universidade de Coimbra

Exame de Teoria dos Números

Licenciatura em Matemática

16 de Janeiro de 2004 Duração: 2h30m

Não é permitido o uso de calculadoras. Justifique resumidamente todas as afirmações que efectuar. Não escreva a lápis nem a vermelho. Qualquer tentativa de fraude será punida com o anulamento da prova.

---

1. Prove que:
   (a) Se a, b e c são inteiros tais que $a \mid bc$ e $(a,b) = 1$ então $a \mid c$;
   (b) Se um número primo divide um produto de números inteiros então divide, pelo menos, um dos factores.
2. Determine o inteiro positivo que é múltiplo de 7, termina em 00 e tem 18 divisores positivos.
3. Calcule o resto da divisão inteira de $1^4 + 2^4 + 3^4 + \cdots + 41^4 + 42^4$ por 5.
4. Sabendo que 2 é uma raíz primitiva módulo 13, resolva a congruência $x^9 \equiv 12 \pmod{13}$.
5. (a) Sendo φ a função de Euler diga como se define $\varphi(n)$, para $n \in \mathbb{N}$.
   (b) Prove que, para p primo e $k \in \mathbb{N}$, $\varphi\left(p^k\right) = p^k - p^{k-1}$.
6. Para assistir a uma representação teatral cada adulto pagou 1,80€ e cada criança pagou 0,80€ . O total da receita foi 90€ . Sabe-se que assistiram à representação mais adultos do que crianças e que o número de crianças era superior a 20.
   (a) Escreva uma equação Diofantina cuja resolução permita obter o número de adultos e o número de crianças que assistiram à representação.
   (b) Resolvendo a equação escrita em (a) determine o número de pessoas que assistiram à representação. (Se não respondeu à alínea (a), determine as soluções naturais de
   $$24\,x + 10\,y = 300$$
   que verificam $x > y$ e $y > 5$).

Cotação :

1. 4 valores
2. 3 valores
3. 3 valores
4. 3 valores
5. 3 valores
6. 4 valores

Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução do Exame da Época Normal

16 de Janeiro de 2004 Duração: 2h30m

---

1. (4 valores)
(a) Sejam a, b e c inteiros tais que $(a,b)=1$ e $a \mid bc$. De $(a,b)=1$ sabe-se que existem inteiros x e y tais que $1=ax+by$. Multiplicando ambos os membros desta igualdade por c obtém-se $c=acx+bcy$. Por hipótese $a \mid bc$ e, portanto, também $a \mid bcy$. É claro que $a \mid acx$, concluindo-se assim que $a \mid acx+bcy$, isto é, $a \mid c$.

(b) A demonstração será feita por indução no número de factores do produto. Seja p um número primo e, para $n \geq 2$ número natural, designe-se por $P(n)$ a afirmação

"*Se p divide um produto de n inteiros então p divide, pelo menos, um deles*".

Verifique-se que $P(2)$ é verdadeira. Sejam $a_1, a_2 \in \mathbb{Z}$ e suponha-se que $p \mid a_1a_2$. Se $p \mid a_1$ nada mais há a provar. Se $p \nmid a_1$ então, (porque p é primo os seus únicos divisores positivos são 1 e p), $(p,a_1)=1$ e, usando o resultado da alínea (a), conclui-se que $p \mid a_2$. Assim, de $p \mid a_1a_2$, resulta que $p \mid a_1$ ou $p \mid a_2$, isto é, a afirmação $P(2)$ é verdadeira.

Seja $k \in \mathbb{N}$, arbitrário e suponha-se que $P(k)$ é verdadeira, isto é, suponha-se que "*se p divide um produto de k inteiros então p divide, pelo menos, um deles*" (hipótese de indução).

Considerem-se $a_1, a_2, \ldots, a_k, a_{k+1} \in \mathbb{Z}$ tais que $p \mid a_1a_2\cdots a_ka_{k+1}$ e seja $b=a_1a_2\cdots a_k$. Então $p \mid ba_{k+1}$ e, usando o facto de $P(2)$ ser verdadeira, conclui-se que $p \mid b$ ou $p \mid a_{k+1}$. Se $p \mid a_{k+1}$ nada mais há a provar. Se $p \nmid a_{k+1}$ então $p \mid b$, isto é, $p \mid a_1a_2\cdots a_k$ e, da hipótese de indução, resulta que p divide, pelo menos, um dos inteiros, $a_1, a_2, \ldots, a_k$. Em ambos os casos, o facto de p dividir $a_1a_2\cdots a_ka_{k+1}$ implica que p divide, pelo menos, um dos factores $a_1, a_2, \ldots, a_k, a_{k+1}$. Mostrou-se assim que $P(k+1)$ é verdadeira. O método de indução matemática permite concluir que a afirmação $P(n)$ é verdadeira, para todo o número natural $n \geq 2$. Uma vez que o primo p é arbitrário obtém-se o resultado.

---

2. (3 valores)
Designe-se por n o inteiro positivo procurado e seja $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ a decomposição canónica de n, isto é, $r \in \mathbb{N}$, $p_1, p_2, \ldots, p_r$ são números primos distintos dois a dois e $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$. O número de divisores positivos de n é

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)\,.$$

Uma vez que 7 é primo, n é múltiplo de 7 se e só se um dos primos $p_1, \ldots, p_r$ for igual a 7. Por outro lado, n termina em 00 se e só se $100=2^2\times 5^2$ divide n, isto é, se e só se os primos 2 e 5 figuram na decomposição canónica de n com expoentes superiores ou iguais a 2. Assim, os inteiros positivos múltiplos de 7 e que terminam em 00 são todos aqueles com uma decomposição canónica da forma $n=2^{\alpha_1}5^{\alpha_2}7^{\alpha_3}p_4^{\alpha_4}\cdots p_r^{\alpha_r}$, onde $\alpha_1, \alpha_2 \geq 2$. Então

$\alpha_1 + 1 \geq 3$, $\alpha_2 + 1 \geq 3$ e $\alpha_i + 1 \geq 2$ para $i = 3, \ldots r$, donde

$$\begin{aligned} \tau(n) = 18 &\Leftrightarrow (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1) = 2 \times 3^2 \\ &\Leftrightarrow \begin{cases} r = 3 \\ \alpha_1 = 2 \\ \alpha_2 = 2 \\ \alpha_3 = 1\,. \end{cases} \end{aligned}$$

O número procurado é $n = 2^2 \times 5^2 \times 7 = 700$.

---

3. (3 valores)
Uma vez que 5 é primo, por aplicação do Teorema de Fermat, sabe-se que, para $a \in \mathbb{Z}$ tal que $5 \nmid a$, $a^4 \equiv 1 \pmod 5$. Obviamente que se $5 \mid a$ então $5 \mid a^4$ e portanto $a^4 \equiv 0 \pmod 5$.

Uma vez que $42 = 5 \times 8 + 2$, em $1, 2, \ldots, 42$ há exactamente 8 múltiplos de 5 ($1 \times 5, 2 \times 5, \ldots, 8 \times 5$) e os restantes 34 números são primos com 5.

Então na soma $1^4 + 2^4 + 3^4 + \cdots + 41^4 + 42^4$ há 8 parcelas congruentes com 0 módulo 5 e as restantes 34 são congruentes com 1 módulo 5, obtendo-se que

$$1^4 + 2^4 + 3^4 + \cdots + 41^4 + 42^4 \equiv 34 \pmod 5 \equiv 4 \pmod 5\,.$$

Assim, o resto da divisão inteira de $1^4 + 2^4 + 3^4 + \cdots + 41^4 + 42^4$ por 5 é 4.

---

4. (3 valores)
Comece-se por verificar que a congruência $x^9 \equiv 12 \pmod{13}$ tem soluções. O número 13 é primo e $12^{\frac{13-1}{(9,13-1)}} = 12^{\frac{12}{3}} = 12^4 \equiv (-1)^4 \pmod{13} \equiv 1 \pmod{13}$, o que permite concluir que existem exactamente $(9, 13-1) = 3$ classes de congruência módulo 13 cujos elementos verificam a congruência dada. Determinem-se essas classes.

Uma vez que 2 é uma raíz primitiva módulo 13, o conjunto $\{2, 2^2, \ldots, 2^{12}\}$ é um sistema reduzido de resíduos módulo 13. Assim, porque 12 é primo com 13, existe um e um só $k \in \{1, 2, \ldots, 12\}$ tal que $2^k \equiv 12 \pmod{13}$. De $2^1 \equiv 2 \pmod{13}$, $2^2 \equiv 4 \pmod{13}$, $2^3 \equiv 8 \pmod{13}$, $2^4 = 16 \equiv 3 \pmod{13}$, $2^5 \equiv 6 \pmod{13}$ e $2^6 \equiv 12 \pmod{13}$, conclui-se que $k = 6$.

Se $x \in \mathbb{Z}$ verifica a congruência dada então $(x, 13) = 1$ e portanto existe um e um só $i \in \{1, 2, \ldots, 12\}$ tal que $x \equiv 2^i \pmod{13}$. Logo,

$$\begin{aligned} x^9 \equiv 12 \pmod{13} &\Leftrightarrow 2^{9i} \equiv 2^6 \pmod{13} \\ &\Leftrightarrow 2^{9i} - 2^6 \equiv 0 \pmod{13} \\ &\Leftrightarrow 2^6\left(2^{9i-6} - 1\right) \equiv 0 \pmod{13} \\ &\Leftrightarrow 2^6 \equiv 0 \pmod{13} \vee 2^{9i-6} - 1 \equiv 0 \pmod{13} \\ &\Leftrightarrow 2^{9i-6} \equiv 1 \pmod{13}\,, \end{aligned}$$

onde, na penúltima equivalência, se usou o facto de 13 ser primo e, na última, se usou o facto de 2 e 13 serem primos entre si. Uma vez que a ordem de 2 módulo 13 é 12 (2 é uma raíz primitiva módulo 13),

$$2^{9i-6} \equiv 1 \pmod{13} \Leftrightarrow 9i - 6 \equiv 0 \pmod{12}$$

$$\begin{aligned}
&\Leftrightarrow \quad 9i \equiv 6 \,(\mathrm{mod}\, 12)\\
&\Leftrightarrow \quad 3i \equiv 2 \,(\mathrm{mod}\, 4)\\
&\Leftrightarrow \quad -i \equiv 2 \,(\mathrm{mod}\, 4)\\
&\Leftrightarrow \quad i \equiv -2 \,(\mathrm{mod}\, 4)\\
&\Leftrightarrow \quad i \equiv 2 \,(\mathrm{mod}\, 4)\,.
\end{aligned}$$

Os inteiros que satisfazem a congruência $i \equiv 2 \,(\mathrm{mod}\, 4)$ são todos os inteiros pertencentes a $[2]_4$. Esta classe de congruência módulo 4 é união de três classes de congruência módulo 12, $[2]_{12}$, $[2+4]_{12} = [6]_{12}$ e $[2+8]_{12} = [10]_{12}$.

Então as soluções de $x^9 \equiv 12 \,(\mathrm{mod}\, 13)$ são as 3 classes de congruência módulo 13 $[2^2]_{13} = [4]_{13}$, $[2^6]_{13} = [12]_{13}$ e $[2^{10}]_{13} = [2^6 2^2 2^2]_{13} = [-1 \times 4 \times 4]_{13} = [10]_{13}$.

---

5. (3 valores)
(a) Para $n \in \mathbb{N}$, $\varphi(n)$ é o número de elementos de qualquer sistema reduzido de resíduos módulo n, isto é, $\varphi(n)$ é o número de elementos de $\{1, 2, \ldots, n\}$ que são primos com n.

(b) Para p primo e $k \in \mathbb{N}$, $\varphi\left(p^k\right)$ é o número de elementos de $\{1, 2, \ldots, p^k - 1, p^k\}$ que são primos com p^k, ou seja, é a diferença entre o número de elementos de $\{1, 2, \ldots, p^k - 1, p^k\}$ (que é p^k) e o número de elementos de $\{1, 2, \ldots, p^k - 1, p^k\}$ que <u>não</u> são primos com p^k. Sendo p primo, os divisores positivos de p^k são as potências de base p e expoente pertencente a $\{0, 1, \ldots, k\}$. Então os inteiros de $\{1, 2, \ldots, p^k - 1, p^k\}$ que não são primos com p^k são precisamente os que são múltiplos de p, ou seja, $p, 2p, \ldots, p^{k-1}p$. Uma vez que estes inteiros são p^{k-1}, obtém-se que $\varphi\left(p^k\right) = p^k - p^{k-1}$.

---

6. (4 valores)
(a) Designem-se por x e y, respectivamente, o número de adultos e de crianças, que assistiram à representação. Então $1,8\,x + 0,8\,y = 90$. Multiplicando ambos os membros desta equação por 10 obtém-se a equação equivalente

$$18\,x + 8\,y = 900\,. \tag{1}$$

Assim, o número de adultos e o número de crianças que assistiram à representação formam um par, (x, y), de números naturais que verificam a equação Diofantina linear (1) e, além disso, satisfazem $x > y > 20$.

(b) Resolva-se a equação (1). Uma vez que $(18, 8) = 2$ e $2 \mid 900$, a equação (1) tem soluções inteiras. Atendendo a que $18\,x + 8\,y = 900 \Leftrightarrow 9\,x + 4\,y = 450$, vai resolver-se a equação

$$9\,x + 4\,y = 450\,. \tag{2}$$

De $1 = 9 \times 1 + 4(-2)$ resulta que $450 = 9 \times 450 + 4(-900)$ e portanto $x_0 = 450$ e $y_0 = -900$ são inteiros que verificam (2). Sejam x_1 e y_1 inteiros tais que $9\,x_1 + 4\,y_1 = 450$. De $9\,x_1 + 4\,y_1 = 9\,x_0 + 4\,y_0 \Leftrightarrow 9(x_1 - x_0) = 4(y_0 - y_1)$, porque $(9, 4) = 1$, conclui-se que $4 \mid x_1 - x_0$ e $9 \mid y_0 - y_1$, isto é, existem $q, t \in \mathbb{Z}$ tais que $x_1 = x_0 + 4q$ e $y_1 = y_0 - 9t$. Mas

$$\begin{aligned}
9\,x_1 + 4\,y_1 = 450 \quad &\Leftrightarrow \quad 9\,x_0 + 36q + 4\,y_0 - 36t = 450\\
&\Leftrightarrow \quad 450 + 36q - 36t = 450\\
&\Leftrightarrow \quad q = t
\end{aligned}$$

e portanto as soluções inteiras de (2) são dadas por

$$\begin{cases} x = x_0 + 4q = 450 + 4q \\ y = y_0 - 9q = -900 - 9q \end{cases}, \quad q \in \mathbb{Z}\,.$$

Uma vez que

$$\begin{cases} x > 0 \\ y > 0 \\ x > y \\ y > 20 \end{cases} \Leftrightarrow \begin{cases} x > y \\ y > 20 \end{cases},$$

basta procurar as soluções de (2) que verificam $x > y$ e $y > 20$.

Sejam $x = 450 + 4q$ e $y = -900 - 9q$, com $q \in \mathbb{Z}$.

$$x > y \Leftrightarrow 450 + 4q > -900 - 9q \Leftrightarrow 13q > -1350 \Leftrightarrow q > -\frac{1350}{13}\,.$$

Atendendo a que $1350 = 103 \times 13 + 11$, $-\frac{1350}{13} = -103 - \frac{11}{13}$ e portanto, para q inteiro, $q > -\frac{1350}{13} \Leftrightarrow q \geq -103$. Analogamente, sendo q inteiro,

$$y > 20 \Leftrightarrow -900 - 9q > 20 \Leftrightarrow q < -\frac{920}{9} \Leftrightarrow q < -102 - \frac{2}{9} \Leftrightarrow q \leq -103\,.$$

Conjugando as duas desigualdades obtém-se $q = -103$, $x = 450+4(-103) = 450-412 = 38$ e $y = -900-9(-103) = -900+927 = 27$. Assistiram à representação 65 pessoas, 38 adultos e 27 crianças.

Resolução de (b) para quem não respondeu a (a) Resolva-se a equação $24\,x+10\,y = 300$. Uma vez que $(24, 10) = 2$ e $2 \mid 300$ esta equação tem soluções inteiras. Atendendo a que $24\,x + 10\,y = 300 \Leftrightarrow 12\,x + 5\,y = 150$, vai resolver-se a equação

$$12\,x + 5\,y = 150\,. \tag{3}$$

De $1 = 12(-2) + 5 \times 5$ resulta que $150 = 12(-300) + 5 \times 750$ e portanto $x_0 = -300$ e $y_0 = 750$ são inteiros que verificam (3). Sejam x_1 e y_1 inteiros tais que $12\,x_1 + 5\,y_1 = 150$. De $12\,x_1 + 5\,y_1 = 12\,x_0 + 5\,y_0 \Leftrightarrow 12(x_1 - x_0) = 5(y_0 - y_1)$, porque $(12, 5) = 1$, conclui-se que $5 \mid x_1 - x_0$ e $12 \mid y_0 - y_1$, isto é, existem $q, t \in \mathbb{Z}$ tais que $x_1 = x_0 + 5q$ e $y_1 = y_0 - 12t$. Mas

$$\begin{aligned} 12\,x_1 + 5\,y_1 = 150 &\Leftrightarrow 12\,x_0 + 60q + 5\,y_0 - 60t = 150 \\ &\Leftrightarrow 150 + 60q - 60t = 150 \\ &\Leftrightarrow q = t \end{aligned}$$

e portanto as soluções inteiras de (3) são dadas por

$$\begin{cases} x = x_0 + 5q = -300 + 5q \\ y = y_0 - 12q = 750 - 12q \end{cases}, \quad q \in \mathbb{Z}\,.$$

Uma vez que

$$\begin{cases} x > 0 \\ y > 0 \\ x > y \\ y > 5 \end{cases} \Leftrightarrow \begin{cases} x > y \\ y > 5 \end{cases},$$

basta procurar as soluções de (3) que verificam $x > y$ e $y > 5$.

Sejam $x = -300 + 5q$ e $y = 750 - 12q$, com $q \in \mathbb{Z}$.

$$x > y \Leftrightarrow -300 + 5q > 750 - 12q \Leftrightarrow 17q > 1050 \Leftrightarrow q > \frac{1050}{17}\,.$$

Atendendo a que $1050 = 61 \times 17 + 13$, $\frac{1050}{17} = 61 + \frac{13}{17}$ e portanto, para q inteiro, $q > \frac{1050}{17} \Leftrightarrow q \geq 62$. Analogamente, sendo q inteiro,

$$y > 5 \Leftrightarrow 750 - 12q > 5 \Leftrightarrow q < \frac{745}{12} \Leftrightarrow q < 62 + \frac{1}{12} \Leftrightarrow q \leq 62\,.$$

Conjugando as duas desigualdades obtém-se $q = 62$, $x = -300 + 5 \times 62 = -300 + 310 = 10$ e $y = 750 - 12 \times 62 = 750 - 744 = 6$.