Departamento de Matemática da Universidade de Coimbra

Exame de Recurso de Teoria dos Números

Licenciatura em Matemática

6 de Fevereiro 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. Sejam a e b números naturais tais que $[a,b] = [a^2,b]$. Prove que $a^2 \mid b$.

2. Prove que, para $m \in \mathbb{N}$ e $a,x,y \in \mathbb{Z}$, se tem
$$ax \equiv ay \,(\mathrm{mod}\, m) \Leftrightarrow x \equiv y \,\left(\mathrm{mod}\, \frac{m}{(a,m)}\right).$$

3. Mostre que $30 \mid (2004^{2004} - 1998^{2004})$.

4. Numa turma com menos de 30 alunos foram efectuados trabalhos de grupo em 3 aulas das disciplinas de Português, Matemática e Biologia. Em todas as 3 aulas estiveram os mesmos alunos. Na aula de Português havia vários grupos de 4 alunos e 2 grupos de 3 alunos. Na aula de Matemática todos os grupos tinham 3 alunos, excepto um que tinha 2 alunos. Finalmente, na aula de Biologia todos os grupos tinham 5 alunos, excepto um que tinha 6 alunos.

   (a) Escreva um sistema de congruências cuja resolução permita obter o número de alunos presentes nas 3 aulas.

   (b) Determinando todas as soluções do sistema escrito em (a), obtenha o número de alunos que estiveram nas 3 aulas. (Se não respondeu à alínea (a), determine todas as soluções do sistema formado pelas congruências $x \equiv 1 \,(\mathrm{mod}\, 3)$, $x \equiv 3 \,(\mathrm{mod}\, 5)$ e $x \equiv 4 \,(\mathrm{mod}\, 7)$ e, de entre estas, a menor solução positiva).

5. Sejam m um número natural e a um inteiro primo com m.

   (a) Defina ordem de a módulo m.

   (b) Prove que, para $k \in \mathbb{N}$, $a^k \equiv 1 \,(\mathrm{mod}\, m)$ se e só se k é múltiplo da ordem de a módulo m.

6. Determine todos os inteiros positivos que têm exactamente 6 divisores positivos, sendo a soma destes divisores igual a 39.

7. Seja p um número primo ímpar. Determine, em função de p, as medidas dos lados de todos os triângulos rectângulos cujos lados têm como medidas números naturais primos entre si e em que um dos catetos mede p cm.

Cotação :

1. 2,5 valores
2. 3,5 valores
3. 2,5 valores
4. 3,5 valores
5. 3,5 valores
6. 2 valores
7 2,5 valores

Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução do Exame da Época de Recurso

6 de Fevereiro de 2004 Duração: 2h30m

---

1. (2,5 valores)
Sejam $p_1, p_2, \ldots, p_r$ todos os números primos (distintos dois a dois) que dividem a ou b. Isto é, $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ onde, para $i = 1, 2, \ldots, r$, $\alpha_i, \beta_i \in \mathbb{N}_0$ e $\alpha_i \neq 0$ ou $\beta_i \neq 0$. Então $[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_r^{\max\{\alpha_r,\beta_r\}}$ e, atendendo a que $a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$, $[a^2, b] = p_1^{\max\{2\alpha_1,\beta_1\}} p_2^{\max\{2\alpha_2,\beta_2\}} \cdots p_r^{\max\{2\alpha_r,\beta_r\}}$. Por hipótese $[a^2, b] = [a, b]$, isto é,

$$\max\{2\alpha_i, \beta_i\} = \max\{\alpha_i, \beta_i\}, \quad i = 1, 2, \ldots, r\,.$$

Pretende provar-se que $a^2 \mid b$, ou seja, que $2\alpha_i \leq \beta_i$, para $i = 1, 2, \ldots, r$. Suponha-se que existe $i \in \{1, 2, \ldots, r\}$ tal que $2\alpha_i > \beta_i$. Então

$$2\alpha_i = \max\{2\alpha_i, \beta_i\} = \max\{\alpha_i, \beta_i\}$$

e portanto $2\alpha_i = \alpha_i$ ou $2\alpha_i = \beta_i$. No primeiro caso tem-se $\alpha_i = 0$. Assim, em qualquer um dos casos conclui-se que $2\alpha_i \leq \beta_i$, o que contradiz a suposição feita. Então tem-se que $2\alpha_i \leq \beta_i$, para $i = 1, 2, \ldots, r$ e portanto $a^2 \mid b$.

---

2. (3,5 valores)
Sejam $m \in \mathbb{N}$ e $a, x, y \in \mathbb{Z}$.

$$\begin{aligned} ax \equiv ay \,(\mathrm{mod}\, m) &\Leftrightarrow m \mid (ax - ay) \\ &\Leftrightarrow \exists q \in \mathbb{Z} : ax - ay = qm \\ &\Leftrightarrow \exists q \in \mathbb{Z} : a(x - y) = qm\,. \end{aligned}$$

Seja $d = (a, m)$. Existem $q_1, q_2 \in \mathbb{Z}$ tais que $a = q_1 d$, $m = q_2 d$ e $(q_1, q_2) = 1$. Então (porque $d \neq 0$)

$$\begin{aligned} ax \equiv ay \,(\mathrm{mod}\, m) &\Leftrightarrow \exists q \in \mathbb{Z} : q_1 d(x - y) = q q_2 d \\ &\Leftrightarrow \exists q \in \mathbb{Z} : q_1(x - y) = q q_2 \\ &\Leftrightarrow q_2 \mid q_1(x - y)\,. \end{aligned}$$

Uma vez que q_1 e q_2 são primos entre si, $q_2 \mid q_1(x-y) \Leftrightarrow q_2 \mid (x-y)$ e portanto

$$\begin{aligned} ax \equiv ay \,(\mathrm{mod}\, m) &\Leftrightarrow q_2 \mid (x-y) \\ &\Leftrightarrow x \equiv y \,(\mathrm{mod}\, q_2) \\ &\Leftrightarrow x \equiv y \left(\mathrm{mod}\, \frac{m}{(a,m)}\right) . \end{aligned}$$

---

3. (2,5 valores)
Atendendo a que 2, 3 e 5 são primos dois a dois,

$$30 \mid \left(2004^{2004} - 1998^{2004}\right) \Leftrightarrow \begin{cases} 2 \mid (2004^{2004} - 1998^{2004}) \\ 3 \mid (2004^{2004} - 1998^{2004}) \\ 5 \mid (2004^{2004} - 1998^{2004}) \end{cases} .$$

Uma vez que 2004 e 1998 são pares e o produto e a soma de números pares são pares, conclui-se que $2 \mid (2004^{2004} - 1998^{2004})$.

De $2004 = 3 \times 668$ resulta que $2004 \equiv 0 \,(\mathrm{mod}\, 3)$ e portanto $2004^{2004} \equiv 0^{2004} \,(\mathrm{mod}\, 3) \equiv 0 \,(\mathrm{mod}\, 3)$. Analogamente, de $1998 = 3 \times 666$ conclui-se que $1998^{2004} \equiv 0 \,(\mathrm{mod}\, 3)$. Então $2004^{2004} - 1998^{2004} \equiv 0 \,(\mathrm{mod}\, 3)$, ou seja, $3 \mid (2004^{2004} - 1998^{2004})$.

De $2004 = 5 \times 40 + 4$, e porque 5 é primo, conclui-se que $(2004, 5) = 1$. Aplicando o Teorema de Fermat obtém-se que $2004^4 \equiv 1 \,(\mathrm{mod}\, 5)$. Então

$$2004^{2004} = \left(2004^4\right)^{501} \equiv 1^{501} \,(\mathrm{mod}\, 5) \equiv 1 \,(\mathrm{mod}\, 5) .$$

Uma vez que também $(1998, 5) = 1$ ($1998 = 5 \times 399 + 3$), aplicando novamente o Teorema de Fermat, obtém-se que

$$1998^{2004} = \left(1998^4\right)^{501} \equiv 1^{501} \,(\mathrm{mod}\, 5) \equiv 1 \,(\mathrm{mod}\, 5) .$$

Então $2004^{2004} - 1998^{2004} \equiv 1 - 1 \,(\mathrm{mod}\, 5) \equiv 0 \,(\mathrm{mod}\, 5)$, ou seja, $5 \mid (2004^{2004} - 1998^{2004})$.

Provou-se assim que 2, 3 e 5 são divisores de $2004^{2004} - 1998^{2004}$ e portanto, pelo afirmado inicialmente, também 30 divide $2004^{2004} - 1998^{2004}$.

---

4. (3,5 valores)
(a) Designe-se por x o número de alunos presentes nas 3 aulas em causa. Seja m o número de grupos que, na aula de Português, tinha 4 alunos. Então $x = 4m + 6$ e portanto $x \equiv 6 \,(\mathrm{mod}\, 4)$, ou seja, $x \equiv 2 \,(\mathrm{mod}\, 4)$. Seja n o número de grupos que, na aula de Matemática, tinha 3 alunos. Então $x = 3n + 2$ e portanto $x \equiv 2 \,(\mathrm{mod}\, 3)$. Finalmente, sendo k o número de grupos que, na aula de Biologia tinha 5 alunos, tem-se $x = 5k + 6$ e portanto $x \equiv 6 \,(\mathrm{mod}\, 5)$, ou ainda, $x \equiv 1 \,(\mathrm{mod}\, 5)$.

Então o número de alunos é solução de

$$\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 . \end{cases} \tag{1}$$

Uma vez que 3, 4 e 5 são primos dois a dois, o Teorema chinês dos resíduos garante que este sistema tem solução, sendo o conjunto das soluções uma classe de congruência módulo $4 \times 3 \times 5 = 60$.

(b) Resolvam-se as congruências auxiliares $\frac{60}{4} b_1 \equiv 1 \pmod 4$, $\frac{60}{3} b_2 \equiv 1 \pmod 3$ e $\frac{60}{5} b_3 \equiv 1 \pmod 5$.

$\frac{60}{4} b_1 \equiv 1 \pmod 4 \Leftrightarrow 15b_1 \equiv 1 \pmod 4 \Leftrightarrow -b_1 \equiv 1 \pmod 4 \Leftrightarrow b_1 \equiv -1 \pmod 4$
$\Leftrightarrow b_1 \equiv 3 \pmod 4$

$\frac{60}{3} b_2 \equiv 1 \pmod 3 \Leftrightarrow 20b_2 \equiv 1 \pmod 3 \Leftrightarrow -b_2 \equiv 1 \pmod 3 \Leftrightarrow b_2 \equiv -1 \pmod 3$
$\Leftrightarrow b_2 \equiv 2 \pmod 3$

$\frac{60}{5} b_3 \equiv 1 \pmod 5 \Leftrightarrow 12b_3 \equiv 1 \pmod 5 \Leftrightarrow 2b_3 \equiv 1 \pmod 5$.

Uma vez que $1 = 3 \times 2 + (-1) \times 5$, $2 \times 3 \equiv 1 \pmod 5$, logo $2b_3 \equiv 1 \pmod 5 \Leftrightarrow b_3 \equiv 3 \pmod 5$. Considerem-se $b_1 = 3$, $b_2 = 2$ e $b_3 = 3$.

Então $2 \times \frac{60}{4} b_1 + 2 \times \frac{60}{3} b_2 + 1 \times \frac{60}{5} b_3 = 2 \times 15 \times 3 + 2 \times 20 \times 2 + 12 \times 3 = 206$ é uma solução de (1) e portanto (Teorema chinês dos resíduos) o conjunto das soluções de (1) é $[206]_{60} = [26]_{60} = \{26 + 60k : k \in \mathbb{Z}\}$. Sabendo que o número de alunos da turma em causa é inferior a 30, conclui-se que nas 3 aulas estiveram 26 alunos.

Resolução de (b) para quem não respondeu a (a)

Pretende-se reolver o sistema

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 . \end{cases} \tag{2}$$

Uma vez que 3, 5 e 7 são primos dois a dois, o Teorema chinês dos resíduos garante que o conjunto das soluções deste sistema é uma classe de congruência módulo $3 \times 5 \times 7 = 105$.

Resolvam-se as congruências auxiliares $\frac{105}{3} b_1 \equiv 1 \pmod 3$, $\frac{105}{5} b_2 \equiv 1 \pmod 5$ e $\frac{105}{7} b_3 \equiv 1 \pmod 7$.

$\frac{105}{3} b_1 \equiv 1 \pmod 3 \Leftrightarrow 35b_1 \equiv 1 \pmod 3 \Leftrightarrow -b_1 \equiv 1 \pmod 3 \Leftrightarrow b_1 \equiv -1 \pmod 3$
$\Leftrightarrow b_1 \equiv 2 \pmod 3$

$\frac{105}{5} b_2 \equiv 1 \pmod 5 \Leftrightarrow 21b_2 \equiv 1 \pmod 5 \Leftrightarrow b_2 \equiv 1 \pmod 5$

$\frac{105}{7} b_3 \equiv 1 \pmod 7 \Leftrightarrow 15b_3 \equiv 1 \pmod 7 \Leftrightarrow b_3 \equiv 1 \pmod 7$.

Considerem-se $b_1 = 2$, $b_2 = 1$ e $b_3 = 1$.

Então $1 \times \frac{105}{3}\, b_1 + 3 \times \frac{105}{5}\, b_2 + 4 \times \frac{105}{7}\, b_3 = 1 \times 35 \times 2 + 3 \times 21 \times 1 + 4 \times 15 \times 1 = 193$ é uma solução de (2) e portanto (Teorema chinês dos resíduos) o conjunto das soluções de (2) é $[193]_{105} = [88]_{105} = \{88 + 105k : k \in \mathbb{Z}\}$. A menor solução positiva de (2) é 88.

---

5. (3,5 valores)

(a) Sendo a primo com m, pelo Teorema de Euler, $a^{\varphi(m)} \equiv 1 \,(\mathrm{mod}\, m)$. Então o conjunto dos números naturais, k, para os quais $a^k \equiv 1 \,(\mathrm{mod}\, m)$, é não vazio e, pelo princípio de boa ordenação, tem um mínimo. A ordem de a módulo m é esse mínimo, ou seja, é o menor número natural, k, que verifica $a^k \equiv 1 \,(\mathrm{mod}\, m)$.

(b) Seja h a ordem de a módulo m e considere-se $k \in \mathbb{N}$. Suponha-se que $a^k \equiv 1 \,(\mathrm{mod}\, m)$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{N}_0$ tais que $k = qh + r$ e $r < h$.

Então $a^k = a^{qh+r} = \left(a^h\right)^q a^r$. Sendo h a ordem de a módulo m, $a^h \equiv 1 \,(\mathrm{mod}\, m)$ e portanto $a^k \equiv 1^q\, a^r \,(\mathrm{mod}\, m) \equiv a^r \,(\mathrm{mod}\, m)$. Da hipótese resulta que $a^r \equiv 1 \,(\mathrm{mod}\, m)$, com $r \in \mathbb{N}_0$ e $r < h$. Atendendo à definição de ordem de a módulo m, terá de ser $r = 0$ e portanto $h \mid k$.

Reciprocamente suponha-se que $h \mid k$. Então existe $q \in \mathbb{N}$ tal que $k = qh$ e portanto $a^k = \left(a^h\right)^q \equiv 1^q \,(\mathrm{mod}\, m) \equiv 1 \,(\mathrm{mod}\, m)$.

---

6. (2 valores)

Seja n um inteiro positivo com decomposição canónica $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ ($p_1, p_2, \ldots, p_r$ são números primos distintos dois a dois e $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$). Suponha-se que $p_1, p_2, \ldots, p_r$ estão ordenados de modo a que $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r$.

O número de divisores positivos de n é $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$.

Então n tem 6 divisores positivos se e só se

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1) = 6 = 2 \times 3\,. \tag{3}$$

Uma vez que 2 e 3 são primos e, para $i = 1, 2, \ldots, r$, $\alpha_i + 1 \geq 2$, (3) é equivalente a

$$\left\{ \begin{array}{l} r = 1 \\ \alpha_1 + 1 = 6 \end{array} \right. \vee \left\{ \begin{array}{l} r = 2 \\ \alpha_1 + 1 = 3 \\ \alpha_2 + 1 = 2 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} r = 1 \\ \alpha_1 = 5 \end{array} \right. \vee \left\{ \begin{array}{l} r = 2 \\ \alpha_1 = 2 \\ \alpha_2 = 1 \end{array} \right. .$$

Assim um inteiro positivo tem 6 divisores positivos se e só se é de uma das forma p_1^5 ou $p_1^2 p_2$, com p_1, p_2 primos distintos.

Suponha-se que $n = p_1^5$, com p_1 primo. Será possível escolher p_1 de modo a que a soma dos divisores positivos de p_1^5 seja 39? Sendo p_1 primo, a soma dos divisores positivos de p_1^5 é

$\sigma(p_1^5) = 1+p_1+p_1^2+p_1^3+p_1^4+p_1^5$. Para $p_1 = 2$, $\sigma(2^5) = 1+2+2^2+2^3+2^4+2^5 > 39$, logo, para qualquer primo $p_1 > 2$, também $\sigma(p_1^5) = 1+p_1+p_1^2+p_1^3+p_1^4+p_1^5 > 1+2+2^2+2^3+2^4+2^5 > 39$. Não há nenhum inteiro da forma p_1^5, com p_1 primo, tal que $\sigma(p_1^5) = 39$.

Suponha-se agora que $n = p_1^2 p_2$, com p_1, p_2 primos distintos. Uma vez que a função σ é multiplicativa, $\sigma(n) = 39 \Leftrightarrow \sigma(p_1^2)\,\sigma(p_2) = 39 \Leftrightarrow (1 + p_1 + p_1^2)(1 + p_2) = 39 = 3 \times 13$. Atendendo a que 3 e 13 são primos, $1 + p_2 \geq 3$ e $1 + p_2 \neq 13$ (porque 12 não é primo),

$$\left(1 + p_1 + p_1^2\right)(1 + p_2) = 3 \times 13 \Leftrightarrow 1 + p_1 + p_1^2 = 13 \wedge 1 + p_2 = 3 \Leftrightarrow p_1 = 3 \wedge p_2 = 2\,.$$

Assim, há um e um só inteiro positivo nas condições do enunciado, $n = 3^2 \times 2 = 18$.

---

7. (2,5 valores)

Designem-se por x, y e z as medidas dos lados de um triângulo rectângulo nas condições do enunciado, sendo x e y as medidas dos catetos e z a medida da hipotenusa. Então (x, y, z) é um trio pitagórico primitivo e portanto x é par ou y é par. Suponha-se que y é par. Uma vez que p é ímpar terá de ser $x = p$. Além disso, existem $a, b \in \mathbb{N}$ primos entre si e de paridades distintas, tais que $a > b$, $x = a^2 - b^2$, $y = 2ab$ e $z = a^2 + b^2$. Então $p = a^2 - b^2 = (a - b)(a + b)$. Sendo p primo, os seus únicos divisores positivos são 1 e p. Uma vez que $a - b$ e $a + b$ são positivos e $a - b < a + b$ terá de ser

$$\left\{ \begin{array}{l} a - b = 1 \\ a + b = p \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} a = 1 + b \\ 1 + 2b = p \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} a = \frac{p+1}{2} \\ b = \frac{p-1}{2} \end{array} \right. .$$

Observe-se que a e b nestas condições são de facto de paridades diferentes porque a sua soma é igual a p que é ímpar. Além disso, de $1 = a+(-1)\times b$ conclui-se ainda que $(a, b) = 1$. Então $x = p$, $y = 2ab = \frac{(p+1)(p-1)}{2} = \frac{p^2-1}{2}$ e $z = a^2 + b^2 = \frac{p^2+2p+1}{4} + \frac{p^2-2p+1}{4} = \frac{p^2+1}{2}$.