Introdução à Teoria dos Números

Exame - 23/11/2021

Atenção: justifique cuidadosamente todas as respostas
O exame consiste nas perguntas 1., 2., 3. e 4. e em duas das perguntas 5., 6. e 7.

1. Considere-se a sucessão definida por recorrência

$$x_1 = 2, \qquad x_{n+1} = x_n^2 - x_n + 1 \ \forall n \geq 1.$$

a) (1.5 valores) Provar, por indução, que $x_{n+1} = \prod_{k=1}^{n} x_k + 1$, para todo o $n \geq 1$.
Dados $m < n$, calcular $m.d.c.(x_m, x_n)$.

b) (1.5 valor) Determinar se 5 divide x_n para algum n.

Resolução: $x_2 = x_1^2 - x_1 + 1 = 2^2 - 2 + 1 = 3 = x_1 + 1$, e portanto a igualdade verifica-se para $n = 1$. Assumindo que ela se verifica para um dado n, então, pela definição,

$$x_{n+2} = x_{n+1}^2 - x_{n+1} + 1 = x_{n+1}\,(x_{n+1} - 1) + 1 =$$

pela hipótese de indução,

$$= x_{n+1}\left(\prod_{k=1}^{n} x_k + 1 - 1\right) + 1 = \prod_{k=1}^{n+1} x_k + 1,$$

completando assim o passo de indução.
A igualdade demonstrada prova que $m.d.c.(x_m, x_n) = 1$:

$$x_n = \prod_{k=1}^{n-1} x_k + 1 = x_m \prod_{1 \le k < n, k \neq m} x_k + 1.$$

Prova-se facilmente por indução que, para todo o $k \geq 1$,

$$x_{2k-1} \equiv 2 \mod 5 \qquad x_{2k} \equiv 3 \mod 5 :$$

para $k = 1$, temos

$$x_1 = 2, \qquad x_2 = 3;$$

e supondo que a propriedade se verifica para um k, temos

$$x_{2(k+1)-1} = x_{2k+1} = x_{2k}^2 - x_{2k} + 1 \equiv 3^2 - 3 + 1 \equiv 2 \mod 5,$$

e usando este resultado

$$x_{2(k+1)} = x_{2k+2} = x_{2k+1}^2 - x_{2k+1} + 1 \equiv 2^2 - 2 + 1 \equiv 3 \mod 5.$$

Portanto, 5 não divide nenhum dos termos da sucessão.

2. (2 valores) Justificar se as afirmações seguintes são verdadeiras ou falsas:

i) Para todos os inteiros a, b, $a^2 \mid b^3 \implies a \mid b$.

ii) Para todos os inteiros a, b, $a^3 \mid b^2 \implies a \mid b$.

Resolução: podemos assumir que a e b são positivos, uma vez que o sinal não afecta a relação de divisibilidade. Se

$$a = \prod_i p_i^{t_i}, \qquad b = \prod_i p_i^{s_i}$$

são as decomposições em factores primos dos dois inteiros, onde se assume, como habitualmente, que o expoente é zero se o primo respectivo não divide o inteiro em questão,

$$a \mid b \Leftrightarrow t_i \leq s_i \ \forall i.$$

Portanto

$$a^3 \mid b^2 \Leftrightarrow 3t_i \leq 2s_i \ \forall i \implies t_i \leq s_i \ \forall i \Leftrightarrow a \mid b.$$

O mesmo raciocínio sugere imediatamente que a outra afirmação é falsa, e basta dar um contra-exemplo: $8^2 = 4^3$ mas 8 não divide 4.

3.

a) (3 valores) Calcular as soluções $0 < x < 1755$ da equação

$$60x \equiv 105 \mod 1755.$$

b) (3 valores) Calcular as soluções $0 < x < 1755$ da equação

$$x^7 \equiv 2 \mod 1755.$$

Resolução: $1755 = 5{\times}27{\times}13$; portanto $m.d.c.(60, 1755) = 15$ que divide $105 = 15 \times 7$.
Assim a equação é equivalente a

$$4x \equiv 7 \mod 117 \Leftrightarrow x \equiv -29 \times 7 \Leftrightarrow 31 \mod 117,$$

e as soluções da equação original são

$$\{31{+}117k : 0 \leq k < 15\} = \{31, 148, 265, 382, 499, 616, 733, 850, 967, 1084, 12$$

Como $\phi(1755) = 4 \times 18 \times 12$ é primo com 7 (e 2 é primo com 1755) sabemos que a equação tem solução única módulo 1755. Vamos resolvê-la usando o Teorema Chinês dos Restos: a equação é equivalente ao sistema

$$\begin{cases} x^7 \equiv 2 \mod 5 \\ x^7 \equiv 2 \mod 27 \\ x^7 \equiv 2 \mod 13 \end{cases}.$$

Resolvendo cada uma das equações obtemos

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 11 \mod 27 \\ x \equiv 11 \mod 13 \end{cases}$$

que tem solução $x \equiv 713 \mod 1755$.

4. Sabendo que 10 é uma raiz primitiva módulo 109,

a) (2 valores) calcular as soluções $0 < x < 109$ da equação

$$x^{28} \equiv 9 \mod 109;$$

b) (2 valores) determinar, para cada $k \in \{7, 8, 9\}$, o número de $0 < b < 109$ para os quais a equação

$$x^k \equiv b \mod 109$$

tem soluções;

c) (1 valor) justificar se $5 \equiv 10^{16} \mod 109$ é raiz primitiva módulo 109.

Resolução: Pelo critério de Euler a equação tem $4 = m.d.c.(28, 108)$ soluções. Sendo 10 uma raiz primitiva,

sabemos que elas serão da forma $x \equiv 10^y$ onde y é solução da equação linear

$$28y \equiv c \mod 108,$$

e c é determinado, módulo 108, por $10^c \equiv 9 \mod 109$. Este valor pode ser facilmente deduzido de

$$9 \equiv -100 \equiv -10^2 \equiv 10^{56} \mod 109.$$

$28y \equiv 56 \mod 108 \Leftrightarrow 7y \equiv 14 \mod 27 \Leftrightarrow y \equiv 2 \mod 27.$

Temos portanto as soluções da equação original

$$\{10^2, 10^{29}, 10^{56}, 10^{83}\}.$$

Para determinar, como pedido, as soluções $0 < x < 109$, vemos primeiro que $10^2 \equiv 100 \equiv -9$ e que $10^{56} \equiv 9$; as outras duas soluções são igualmente simétricas uma da outra (se $a^{28} \equiv 9 \mod 109$ também $(-a)^{28} \equiv 9 \mod 109$), pelo que basta calcular por exemplo $10^{29} \equiv 30 \mod 109$, e concluímos que as soluções são

$$\{9, 100, 30, 79\}.$$

Como 7 é primo com 108, a equação $x^7 \equiv b \mod 109$ tem solução (única) para qualquer $0 < b < 109$, logo há 108 valores possíveis de b.
$m.d.c.(8, 108) = 4$, portanto a equação $x^8 \equiv b \mod 109$ (com $0 < b < 109$) tem soluções se e só se $b^{27} \equiv 1 \mod 109$ e esta última equação tem 27 soluções.
Do mesmo modo, como $m.d.c.(9, 108) = 9$, a equação $x^9 \equiv b \mod 109$ tem soluções se e só se $b^{12} \equiv 1 \mod 109$ e esta equação tem 12 soluções.

Sendo 10 raiz primitiva, 10^k é raiz primitiva se e só se $m.d.c.(k, 108) = 1$, portanto 5 não pode ser raiz primitiva.
Isso podia ser deduzido directamente notando que

$$5^{27} \equiv 10^{27\times 16} \equiv \left(10^{108}\right)^4 \equiv 1,$$

pelo que a ordem de 5 módulo 109 não é 108.

5. (2 valores) Considere-se a função

$$\psi(n) = \sum_{d|n} \phi(d),$$

onde d percorre os divisores positivos de n e ϕ designa a função de Euler.
Mostrar que ψ é multiplicativa: se n e m são primos entre si, $\psi(mn) = \psi(m)\psi(n)$, e deduzir que $\psi(n) = n$ para todo o $n \geq 1$.

Resolução: Como m e n são primos entre si, existe uma bijecção entre divisores d de mn e pares (d_1, d_2), onde d_1 é divisor de m e d_2 divisor de n: a cada par (d_1, d_2) deste tipo fazemos corresponder $d = d_1 d_2$ que é divisor de mn; esta função é injectiva porque os divisores de m são primos com os de n:

$$d_1 d_2 = d_1' d_2' \implies d_1 \mid d_1' \wedge d_1' \mid d_1;$$

e é também sobrejectiva: a sua inversa faz corresponder a cada divisor d de mn o par $(m.d.c.(d, m), m.d.c.(d, n))$.

Portanto

$$\psi(mn) = \sum_{d|mn} \phi(d) = \sum_{d_1|m,\, d_2|n} \phi(d_1 d_2) =$$

somando primeiro nos d_2 para cada d_1,

$$= \sum_{d_1|m} \left(\sum_{d_2|n} \phi(d_1 d_2) \right) =$$

porque d_1 e d_2 são primos entre si,

$$= \sum_{d_1|m} \left(\sum_{d_2|n} \phi(d_1)\phi(d_2) \right) = \sum_{d_1|m} \phi(d_1) \left(\sum_{d_2|n} \phi(d_2) \right) =$$

$$= \psi(n) sum_{d_1|m} \phi(d_1) = \psi(n)\psi(m).$$

6. (2 valores) Justificar que a equação $x^2 \equiv 5 \mod p$, com p primo, tem ou não soluções dependendo da classe de congruência de p módulo 20, e determinar para quais destas classes a equação tem soluções.

Resolução: Em primeiro lugar, há dois primos, o 2 e o 5, que são os únicos primos na sua classe congruência módulo 20. Para esses dois a equação tem obviamente solução.
Suponhamos agora que $p \neq 2, 5$. A equação ter solução módulo p significa que 5 é resíduo quadrático módulo p; usando o símbolo de Legendre, isso acontece se e só se $(5|p) = 1$. Pela Lei da Reciprocidade quadrática, uma vez que $5 \equiv 1 \mod 4$,

$$(5|p) = (p|5) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \mod 5 \\ -1 & \text{se } p \equiv \pm 2 \mod 5 \end{cases}$$

Como estes primos são ímpares podemos caracterizar os primos para os quais existe solução como aqueles que

pertencem às seguintes classes de congruência módulo 10:

$$1, 2, 5, 9.$$

Naturalmente, essas classes correspondem às classes de congruência módulo 20:

$$1, 2, 5, 9, 11, 19.$$

7. (2 valores) Justificar que, para todo o $k > 1$, as soluções da equação $x^6 \equiv 1 \mod 3^k$ são $\pm 1 + 3^{k-1}t$, com $0 \leq t \leq 2$.

Resolução: Note-se que, para $k > 1$, $\phi(3^k)$ é múltiplo de 6. Como existem raizes primitivas para 3^k, podemos aplicar o critério de Euler para concluir que a equação tem exactamente $6 = m.d.c.(6, \phi(3^k))$ soluções. Basta por isso verificar que

$$(\pm 1 + 3^{k-1}t)^6) = 1 + \sum_{j=1}^{6} \binom{6}{j} 3^{(k-1)j} t^j \equiv 1 \mod 3^k$$

para qualquer $0 \leq t \leq 2$.