Introdução à Teoria dos Números

Exame - 30/10/2025

Justifique cuidadosamente todas as respostas
O exame consiste nas perguntas 1, 2, 3 e 4 e uma das perguntas 5 e 6

1. Dados inteiros x e y, justificar que

a) (1.0) $\text{mdc}(x, y) = 1 \Leftrightarrow \text{mdc}(x + y, xy) = 1$;

b) (2.0) $(x + y) \mid xy$ se e só se $(x + y) \mid d^2$, onde $d = \text{mdc}(x, y)$.

Resolução: Para a alínea a), seja p um primo; claramente, se $p \mid x$ e $p \mid y$ então $p \mid (x + y)$ e $p \mid xy$ e portanto

$$\text{mdc}(x + y, xy) = 1 \implies \text{mdc}(x, y) = 1.$$

Reciprocamente, se $p \mid xy$, então $p \mid x$ ou $p \mid y$; mas nesse caso, se $p \mid (x + y)$ então $p \mid x$ e $p \mid y$; e portanto temos também a outra implicação.

Uma das implicações da alínea b) é também evidente: se $(x+y) \mid d^2$,então $x + y$ divide também xy que é múltiplo de d^2. Quanto à outra implicação , podemos usar a alínea anterior: como mdc $\left(\frac{x}{d}, \frac{y}{d}\right) = 1$, também

$$\text{mdc}\left(\left(\frac{x}{d} + \frac{y}{d}\right), \left(\frac{x}{d}\frac{y}{d}\right)\right) = 1.$$

Ora

$$(x + y) \mid xy \Leftrightarrow \left(\frac{x}{d} + \frac{y}{d}\right) \mid \left(\frac{x}{d}\frac{y}{d}\right) d,$$

e portanto, se a soma do lado esquerdo divide aquele produto e é primo com o primeiro factor tem que dividir o segundo factor d; e

$$\left(\frac{x}{d} + \frac{y}{d}\right) \mid d \Leftrightarrow (x + y) \mid d^2.$$

2. (3.0) Seja m par e $a_1, \cdots, a_m$ e $b_1, \cdots, b_m$ dois sistemas completos de representantes das classes de congruência módulo m.
Justificar que

$$a_1 + b_1, \cdots, a_m + b_m$$

nunca é um sistema completo de representantes das classes de congruência módulo m.
Sugestão: determinar o inteiro $0 \leq S < m$ que satisfaz

$$S \equiv \sum_{i=1}^{m} a_i \mod m.$$

Resolução: Notamos que

$$\sum_{i=1}^{m} a_i \equiv \sum_{k=1}^{m} k \mod m.$$

Esta última soma é igual a $\frac{m(m+1)}{2}$; e esta soma é

$$\begin{cases} \frac{m}{2}(m+1) \equiv \frac{m}{2} \mod m & \text{se } m \text{ é par} \\ \\ m\frac{m+1}{2} \equiv 0 \mod m & \text{se } m \text{ é ímpar} \end{cases}$$

Em particular, se m é par, a soma dos elementos de um sistema completo de representantes das classes de congruência módulo m é congruente com $m/2$; e portanto

$$\sum_{i=1}^{m}(a_i + b_i) = \sum_{i=1}^{m} a_i + \sum_{i=1}^{m} b_i \equiv 2 \times \frac{m}{2} \equiv 0 \mod m$$

donde se conclui que a família dos $a_i + b_i$ não pode ser um sistema completo de representantes das classes de congruência módulo m.

3. Sabendo que $527 = 17 \times 31$,

a) (3.0)) determinar para quantos $0 < b < 527$, primos com 527, a equação $x^{12} \equiv b \mod 527$ tem soluções;

b) (2.0)) determinar para que inteiros $m > 0$ existe algum k tal que o número de soluções da equação $x^k \equiv 1 \mod 527$ é m.

Resolução: a) as classes de congruência b, primas com 527, para as quais a equação $x^{12} \equiv b \mod 527$ tem solução correspondem, pelo Teorema Chinês dos Restos, aos pares de classes $b_1 \mod 17, b_2 \mod 31$, primas com os respectivos módulos, para os quais o sistema

$$\begin{cases} x^{12} \equiv b_1 \mod 17 \\ x^{12} \equiv b_2 \mod 31 \end{cases}$$

tem soluções.
Como $\text{mdc}(17-1, 12) = 4$, a primeira equação tem, por aplicação do Critério de Euler, 4 soluções, caso $b_1^{\frac{17-1}{4}} \equiv 1 \mod 17$ (e nenhuma solução caso contrário) e o mesmo critério mostra que há 4 classes módulo 17 (primas com 17), para as quais a primeira equação do sistema tem soluções.
O mesmo raciocínio mostra que há 5 classes b_2 módulo 31(primas com 31) para as quais a segunda equação tem soluções.
O Teorema Chinês dos Restos implica que existem $20 = 4 \times 5$ classes módulo 527, primas com o módulo, para as quais a equação inicial tem soluções.

b) mais uma vez pelo Teorema Chinês dos Restos, dado um k, a equação $x^k \equiv 1 \mod 527$ tem $m_1 \times m_2$ soluções onde

$$m_1 = \text{mdc}(k, 16), \qquad m_2 = \text{mdc}(k, 30).$$

Se $m_1 = 1$, m_2 pode tomar qualquer um dos valores $1, 3, 5, 15$; já se $m_1 = 2^k$, com $2 \leq k \leq 4$, m_2 poderá tomar qualquer um dos valores $2, 6, 10, 30$.
Na tabela seguinte apresentam-se os possíveis valores de $m = m_1 \times m_2$ e de um valor de k correspondente (o que não era pedido na pergunta):

$$
\begin{array}{rrrr rrrr}
1 = & 1\times 1 & k = & 1, & 3 = & 1\times 3 & k = & 3,\\
4 = & 2\times 2 & k = & 2, & 5 = & 1\times 5 & k = & 5,\\
8 = & 4\times 2 & k = & 4, & 12 = & 2\times 6 & k = & 12,\\
15 = & 1\times 15 & k = & 15, & 16 = & 8\times 2 & k = & 8,\\
24 = & 4\times 6 & k = & 12, & 32 = & 16\times 2 & k = & 16,\\
40 = & 4\times 10 & k = & 20, & 48 = & 8\times 6 & k = & 24,\\
80 = & 8\times 10 & k = & 40, & 96 = & 16\times 6 & k = & 48,\\
120 = & 4\times 30 & k = & 60, & 160 = & 16\times 10 & k = & 80,\\
240 = & 8\times 30 & k = & 120, & 480 = & 16\times 30 & k = & 240
\end{array}
$$

4. Seja $f(x) = x^2 + 5x + 7$.

a) (2.0) Justificar que a equação $f(x) \equiv 0 \mod 19$ tem duas soluções (não é necessário calculá-las).

b) (2.0) Quantas soluções tem a equação $f(x) \equiv 0 \mod 19^4$?

c) (2.0) Caracterizar os primos p para os quais a equação $f(x) \equiv 0 \mod p$ tem duas soluções.

Resolução: a) o discriminante do polinómio $f(x)$ é $5^2 - 4\times 7 = -3$; temos que verificar se -3 é resíduo quadrático módulo 19. Pela Lei da Reciprocidade Quadrática, $(-3|19) = (-1|19)(3|19)$ pela propriedade de multiplicatividade do símbolo de Legendre, $= -(3|19)$ porque $19 \equiv 3 \mod 4$, $= (19|3)$ porque 19 e 3 são ambos congruentes com 3 módulo 4; como $(19|3) = (3\times 6+1|3) = (1|3) = 1$, concluímos que -3 é resíduo quadrático e portanto a equação tem de facto duas soluções.
b) $f'(x) = 2x + 5$ só se anula módulo 19 para $x \equiv 7 \mod 19$, mas $f(7) \not\equiv 0 \mod 19$. Portanto f' não se anula, módulo 19, em nenhuma das soluções a e b da equação $f(x) \equiv 0 \mod 19$ e o Lema de Hensel garante que existem, para qualquer $k > 0$ve portanto também para $k = 4$, exactamente duas soluções a_k e b_k de $f(x) \equiv 0 \mod 19^k$, sendo $a_k \equiv a$ e $b_k \equiv b$, módulo 19.
c) se $p = 2$ verificamos directamente que a equação não tem soluções. Usamos

a Lei da Reciprocidade Quadrática para determinar para que primos ímpares p, o discriminante -3 é resíduo quadrático. Se $p = 3$ verificamos igualmente que a equação tem uma única solução $x \equiv 2 \mod 3$. Para $p > 3$ temos dois casos: se $p \equiv 1 \mod 4$

$$(-3|p) = (-1|p)(3|p) = (3|p) = (p|3),$$

enquanto que se $p \equiv 3 \mod 4$

$$(-3|p) = (-1|p)(3|p) = -(3|p) = (p|3).$$

Como $(p|3) = 1 \Leftrightarrow p \equiv 1 \mod 3$, deduzimos que a equação $f(x) \equiv 0 \mod p$ tem duas soluções se e só se p é um primo ímpar congruente com 1 módulo 3.

5. (3.0) Sejam $p_1 < p_2 < \cdots < p_m$ os primeiros m primos, $P = \prod_{j=1}^{m} p_j$ e, para cada $1 \leq k \leq m$, $n_k = \frac{P(p_k-1)}{p_k}$.
Mostrar que $\phi(n_k)$ não depende de k.

Resolução: sabemos que

$$\phi(n_k) = \prod_{j \neq k} (p_j - 1)\phi(p_k - 1);$$

ora $p_k - 1 = \prod_{j=1}^{k-1} p_j^{\alpha_j}$, onde os expoentes α_j são não negativos e dependem também de k; mas, em qualquer caso,

$$\phi(n_k) = \phi\left(\prod_{j<k} p_j^{1+\alpha_j} \prod_{j>k} p_j\right) = \prod_{j<k} p_j^{\alpha_j}(p_j - 1) \prod_{j>k} (p_j - 1) = \prod_{j=1}^{m} (p_j - 1).$$

Podemos chegar ao resultado de forma mais directa notando que, para qualquer $M = \prod_i p_i^{k_i}$ (com $k_i > 0$),

$$\phi(M) = \prod_i (p_i^{k_i} - p_i^{k-i-1}) = \prod_i p_i^{k_i}(p_i - 1) = M \prod_{p|M} \left(1 - \frac{1}{p}\right).$$

Logo, como n_k é divisível exactamente pelos p_i com $i \neq k$,

$$\phi(n_k) = n_k \prod_{i \neq k} \left(1 - \frac{1}{p_i}\right) = (p_k - 1) \prod_{i \neq k} p_i \left(1 - \frac{1}{p_i}\right) = \prod_i (p_i - 1)$$

6.

a) (1.0) Determinar para que valores de $m > 0$ é que $2^m + 1$ é resíduo quadrático módulo 5.

b) (2.0) Seja $m \equiv 0 \mod 4$ e $n = 2^m + 1$. Mostrar que n é primo se e só se $5^{\frac{n-1}{2}} \equiv -1 \mod n$.

Sugestão : se p é um factor primo de n, calcular $\mathrm{ord}_p(5)$.

Resolução: a) o símbolo de Legendre $(2^m + 1|5)$ só depende do valor de m módulo 4, uma vez que $2^{m+4k} \equiv 2^m \mod 5$. Verificamos que

$$(2^1 + 1|5) = -1; (2^2 + 1|5) = 0; (2^3 + 1|5) = 1; (2^4 + 1|5) = -1.$$

Portanto, $2^m + 1$ é resíduo quadrático módulo 5 se e só se $m \equiv 3 \mod 4$.
Nota: a resposta $m \equiv 2$ ou $3 \mod 4$ também seria aceitável.
b) suponhamos que $n = 2^m + 1$ é primo; então

$$5^{\frac{n-1}{2}} \equiv (5|n) \mod n;$$

mas $(5|n) = (n|5)$ (porque $5 \equiv 1 \mod 4) = -1$ pela alínea anterior ($m \equiv 0 \mod 4$).
Suponhamos agora que $n = 2^{4t} + 1$ e $5^{2^{4t-1}} = 5^{\frac{n-1}{2}} \equiv -1 \mod n$; isso implica que $\mathrm{ord}_n(5) = 2^{4t} = n - 1$: temos necessariamente $\mathrm{ord}_n(5) \mid 2^{4t}$ e portanto $\mathrm{ord}_n(5) = 2^k$, mas não pode ser $k < 4t$ pois caso contrário

$$-1 \equiv 5^{2^{4t-1}} = \left(5^{2^k}\right)^{2^{4t-1-k}} \equiv 1,$$

uma contradição.
Mas $\mathrm{ord}_n(5) = n - 1$ implica que n é primo: se p é um factor primo de n, pelo mesmo raciocínio $\mathrm{ord}_p(5) = 2^{4t} = n - 1$ e temos

$$n - 1 = \mathrm{ord}_p(5) \leq p - 1 \leq n - 1,$$

ou seja, $p = n$.