Introdução à Teoria dos Números

Exame - 06/11/2023

Justifique cuidadosamente todas as respostas.

1.(2.0) Determinar os pares não ordenados $\{x, y\}$ de inteiros positivos que satisfazem as duas condições

$$gcd(x, y) = 60, \qquad lcm(x, y) = 12600 = 2^3 \times 3^2 \times 5^2 \times 7.$$

Resolução : para qualquer par de inteiros nessas condições, temos que $x/60$ e $y/60$ são o primos entre si e

$$\frac{x}{60}\frac{y}{60} = 2 \times 3 \times 5 \times 7.$$

Portanto os pares x, y correspondem aos oito modos (não ordenados) de factorizar $2 \times 3 \times 5 \times 7$.

1	$2 \times 3 \times 5 \times 7$	$x = 2^2 \times 3 \times 5$	$y = 2^3 \times 3^2 \times 5^2 \times 7$
2	$3 \times 5 \times 7$	$x = 2^3 \times 3 \times 5$	$y = 2^2 \times 3^2 \times 5^2 \times 7$
3	$2 \times 5 \times 7$	$x = 2^2 \times 3^2 \times 5$	$y = 2^3 \times 3 \times 5^2 \times 7$
5	$2 \times 3 \times 7$	$x = 2^2 \times 3 \times 5^2$	$y = 2^3 \times 3^2 \times 5 \times 7$
7	$2 \times 3 \times 5$	$x = 2^2 \times 3 \times 5 \times 7$	$y = 2^3 \times 3^2 \times 5^2$
2×3	5×7	$x = 2^3 \times 3^2 \times 5$	$y = 2^2 \times 3 \times 5^2 \times 7$
2×5	3×7	$x = 2^3 \times 3 \times 5^2$	$y = 2^2 \times 3^2 \times 5 \times 7$
2×7	3×5	$x = 2^3 \times 3 \times 5 \times 7$	$y = 2^2 \times 3^2 \times 5^2$

2. (2.0) Prove que se $n > 1$ os inteiros

$$n^4 + n^2 + 1, \qquad 1 + 10^{2n-1}$$

não são primos.

Resolução : o primeiro caso deduz-se por aplicação da fórmula do binómio, uma vez que

$$n^4 + n^2 + 1 = (n^2 + 1)^2 - n^2 = (n^2 + n + 1)(n^2 - n + 1),$$

e que, para $n > 1$, ambos os factores são maiores que 1. O segundo caso pode ser justificado usando congruências módulo 11:

$$1 + 10^{2n-1} \equiv 1 + (-1)^{2n-1} \equiv 0 \mod 11.$$

Nota: a primeira parte deste problema tinha, sem uma sugestão, um grau de dificuldade superior ao prependido, nesta parte do exame. Essa foi uma das razões para uma alteração no critério de avaliação do exame.

3. Um inteiro é livre de quadrados se for o produto de primos distintos.

a) (2.0) Determine três inteiros consecutivos, nenhum dos quais é livre de quadrados.

b) (1.0) Justifique que, para todo o inteiro positivo m existem m inteiros consecutivos, nenhum dos quais é livre de quadrados.

Resolução : na primeira alínea basta aplicar o Teorema Chinês dos Restos a, por exemplo

$$\begin{cases} x \equiv 0 & \mod 4 \\ x + 1 \equiv 0 & \mod 9 \\ x + 2 \equiv 0 & \mod 25 \end{cases}$$

que tem solução $x \equiv 548$ módulo $4 \times 9 \times 25$; portanto os inteiros $548, 549, 550$ não são livres de quadrados.
Naturalmente, qualquer outra escolha de três módulos co-primos dois a dois e cada um deles divisível por um quadrado daria exemplos com a mesma propriedade.
Na segunda alínea, basta justificar que se escolhermos primos distintos $p_1, \cdots, p_m$ e aplicarmos o Teorema Chinês dos Restos ao sistema com equações

$$x + i \equiv p_i^2,$$

obtemos m inteiros consecutivos não livres de quadrados.

4. a) (3.0) Sabendo que 3 é uma raiz primitiva módulo 43 e que

$$3^{12} \equiv 4 \mod 43,$$

determine o número de soluções $0 < x < 43$ de cada uma das equações seguintes:

$$x^{23} \equiv 4 \mod 43, \qquad x^{36} \equiv 4 \mod 43, \qquad x^{35} \equiv 4 \mod 43.$$

4. b) (3.0) Para quantos valores de $0 < k < 42$ é que a equação $x^k \equiv 4 \mod 43$

i) tem exactamente uma solução?

ii) tem exactamente três soluções?

4. c) (2.0) Para quantos $0 < b < 43$ é que a equação

$$x^{35} \equiv b \mod 43$$

tem soluções?

Resolução : em a), uma vez que 23 é primo com $\phi(43) = 42$, a equação $x^{23} \equiv 4 \mod 43$ tem uma solução única, módulo 43.
A informação dada implica que a equação $x^{36} \equiv 4 \mod 43$ se pode escrever como

$$3^{36y} \equiv 3^{12} \mod 43,$$

que por sua vez é equivalente a $36y \equiv 12 \mod 42$. Esta tem seis soluções, uma vez que $mdc(36, 42) = 6$ divide 12. Portanto aquela equação tem seis soluções, módulo 43.
Finalmente, o mesmo raciocínio implica que a equação $x^{35} \equiv 4 \mod 43$ é equivalente a $35y \equiv 12 \mod 42$, que não tem soluções, uma vez que $mdc(35, 42) = 7$ não divide 12.

b) A equação $x^k \equiv 4 \mod 43$ é equivalente a

$$ky \equiv 12 \mod 42;$$

esta terá uma única solução se e só se $mdc(k, 42) = 1$; logo existem

$$\phi(42) = \phi(7)\phi(3)\phi(2) = 12$$

valores de $0 < k < 42$ nessas condições.
A equação terá exactamente três soluções se e só se $mdc(k, 42) = 3$, uma vez que 3 divide 12; existem portanto $\phi(14) = 6$ valores de k que estão em bijecção com os valores de $0 < k/3 < 14$ primos com 14.

c) Pelo critério de Euler, $x^{35} \equiv b \mod 43$ tem $7 = mdc(35, 42)$ soluções se $b^6 \equiv 1 \mod 43$ (e nenhuma solução

caso contrário). Ora esta última equação tem seis soluções, de novo por aplicação do critério de Euler.

5. a) (1.5) Determine, usando a Leida Reciprocidade Quadrática, para que primos p é que -3 é um resíduo quadrático.

5. b) (1.5) Mostrar que existem infinitos primos congruentes com 1 módulo 3.
Sugestão: se $p_1, \cdots, p_m$ são primos congruentes com 1 módulo 3, considerar um factor primo de

$$(p_1 \cdots p_m)^2 + 3.$$

Resolução : em primeiro lugar, -3 é resíduo quadrático módulo 2, obviamente. E evidentemente $x^2 equiv - 3 \mod 3$ tem uma única solução.
Quanto aos outros primos, temos $(-3|p) = (-1|p)(3|p)$; e

$$(-1|p) = \begin{cases} 1 & \text{se } p \equiv 1 \mod 4 \\ -1 & \text{se } p \equiv -1 \mod 4 \end{cases}$$

Pela Lei da Reciprocidade Quadrática,

$$(3|p) = \begin{cases} (p|3) & \text{se } p \equiv 1 \mod 4 \\ -(p|3) & \text{se } p \equiv -1 \mod 4 \end{cases}$$

Juntqando os dois resultados, concluímos que $(-3|p) = (p|3)$ para todo o primo ímpar.
Por outro lado, verifica-se directamente, ou pelo critério de Euler que

$$(p|3) = \begin{cases} 1 & \text{se } p \equiv 1 \mod 3 \\ -1 & \text{se } p \equiv 2 \mod 3 \end{cases}$$

Portanto os primos para os quais -3 é resíduo quadrático são 2 e os primos ímpares congruentes com 1 módulo 3.

b) Se $p_1, \cdots, p_m$ são quaisquer primos congruentes com 1 módulo 3, seja q um factor primo ímpar de $N = (p_1 \cdots p_m)^2 + 3$; note-se que, uma vez que $N \equiv 1 \mod 3$, $q \neq 3$. Temos então

$$(p_1 \cdots p_m)^2 \equiv -3 \mod q,$$

ou seja, -3 é resíduo quadrático módulo q e portanto $q \equiv 1 \mod 3$; como $q \neq p_i$ (caso contrário $q|3$), aquele conjunto não contém todos os primos congruentes com 1 módulo 3 e portanto esse conjunto não é finito.

6. (2.0) Seja $n > 1$ um inteiro ímpar. Mostrar que existe um inteiro a tal que $a^{n-1} \equiv 1 \mod n$, mas $a^{\frac{n-1}{d}} \not\equiv 1 \mod n$, para qualquer divisor $d > 1$ de $n - 1$, se e só se n é primo.

Resolução : se n é primo, evidentemente existe um a com ordem $n - 1$ (uma raiz primitiva) que satisfaz as condições enunciadas.
Resta provar a recíproca; vamos mostrar que se n não é primo, então nenhum a satisfaz aquelas condições: suponhamos que $n = \prod j p_j^{k_j}$, e que existe a tal que $a^{n-1} \equiv 1 \mod n$. Se designarmos por t a ordem de a módulo n, temos que $t|(n-1)$ mas também $t|\phi(n)$; logo $t|mdc(n-1, \phi(n))$ que é estritamente menor que $n - 1$. Portanto $t = (n-1)/d$ para algum $d > 1$ e a condição do enunciado não se verifica.