Introdução à Teoria dos Números

Exame - 15/11/2022

Atenção: justifique cuidadosamente todas as respostas
O exame consiste em duas das perguntas 1., 2. e 3. e duas das perguntas 4. 5. e 6.
Cada pergunta tem a cotação de 2 valores.

1. Dados inteiros a, b, c, mostrar que

$$mmc(a, mdc(b, c)) = mdc(mmc(a, b), mmc(a, c)).$$

Resolução: Se

$$a = \prod_i p_i^{k_i}, \qquad b = \prod_i p_i^{j_i}, \qquad c = \prod_i p_i^{m_i},$$

onde o produto é sobre todos os primos, com a convenção de que, por exemplo, $k_i = 0$ se p_i não divide a, a igualdade do enunciado equivale a mostrar que, para todo o i,

$$\max(k_i, \min(j_i, m_i)) = \min(\max(k_i, j_i), \max(k_i, m_i)),$$

ou seja, omitindo o índice i da notação, que para quaisquer naturais k, j e m

$$\max(k, \min(j, m)) = \min(\max(k, j), \max(k, m)).$$

Suponhamos, sem perda de generalidade, que $j \leq m$; então o lado esquerdo é $\max(k, j)$; por outro lado, $\max(k, j) \leq$

$\max(k, m)$: caso contrário teríamos ou $\max(k, j) = k > m = \max(k, m)$ que é uma contradição, ou $\max(k, j) = j > \max(k, m)$ contrariando a hipótese.
Portanto temos igualdade entre as duas expressões.

2. Calcular o inteiro $0 < a < 2000$ que satisfaz

$$a \equiv 3^{999} \mod 2000.$$

Resolução: usando o Teorema Chinês dos Restos, queremos resolver, com $0 < a < 2000$,

$$\begin{cases} a \equiv 3^{999} & \mod 2^4 \\ a \equiv 3^{999} & \mod 5^3 \end{cases} \Leftrightarrow \begin{cases} a \equiv 3^{7} & \mod 2^4 \\ a \equiv 3^{99} & \mod 5^3 \end{cases}$$

aplicando o Teorema de Euler.
A primeira equação é equivalente a

$$3a \equiv 1 \mod 2^4 \Leftrightarrow a \equiv 11 \mod 2^4;$$

do mesmo modo, a segunda equação é equivalente a

$$3a \equiv 1 \mod 5^3 \Leftrightarrow a \equiv 42 \mod 5^3.$$

Ou seja, a equação original é equivalente a $3a \equiv 1 \mod 2000$; resolvendo esta equação ou o sistema

$$\begin{cases} a \equiv 11 & \mod 2^4 \\ a \equiv 42 & \mod 5^3 \end{cases}$$

obtemos $a \equiv 667 \mod 2000$.

3. Para que inteiros n é que $\phi(n) \equiv 2 \mod 4$?

Resolução: A condição significa que $\phi(n)$ é divisível por 2 mas não por 2^2. Portanto n não pode ser diviível por mais do que um factor primo ímpar. Uma solução é $n = 4$; qualquer outra solução terá que ser da forma p^k ou $2p^k$; como nesse caso $\phi(n) = p^{k-1}(p-1)$, deduzimos que p é um primo congruente com 3 módulo 4 (caso contrário, $p - 1 \equiv 0 \mod 4$).
Reciprocamente, qualquer inteiro daquela forma satisfaz a condição, porque $p^k \equiv \pm 1 \mod 4$ e $p - 1 \equiv 2 \mod 4$ e, portanto, $\phi(2p^k) \equiv 2 \mod 4$.

4. Sabendo que 1987 é primo, que 3 é raiz primitiva módulo 1987, e que $2 \equiv 3^{109} \mod 1987$, determinar quantas soluções tem a equação

$$32x^{111} + 1 \equiv 0 \mod 1987.$$

Resolução: Como 109 é primo com 1986, concluímos que 2 também é raiz primitiva módulo 1987. A equação fica equivalente a

$$2^{5+111y} \equiv 2^{993} \mod 1987,$$

ou seja

$$5 + 111y \equiv 993 \mod 1986;$$

mas $mdc(1986, 111) = 3$ que não divide 988 pelo que a equação não em soluções.

5. 4993 é primo; determinar se a equação

$$19x^2 \equiv 2455 \mod 4993$$

tem ou não solução.
Sugestão : usar a Lei da Reciprocidade Quadrática; não é necessário calcular o inverso de 19 módulo 4993.

Resolução:

A equação é equivalente a $x^2 \equiv 2455a \mod 4993$ onde a é o inverso de 19 módulo 4993. Como a é resíduo quadrático se e só e 19 for, basta calcular $(19|4993)$ e $(2455|4993) = (5|4993)(491|4993)$. A equação terá (duas) soluções se e só se

$$(19|4993)(2455|4993) = 1.$$

Quanto ao primeiro factor, e notando que $4993 \equiv 1 \mod 4$,

$$(19|4993) = (4993|19) = (15|19) = (3|19)(5|19) = -(19|3)(19|5) = -(1|3)(4|$$

Por outro lado,

$$(5|4993) = (4993|5) = (3|5) = -1$$

e

$$(491|4993) = (4993|491) = (83|491) = -(491|83) = -(76|83) =$$

$$= -(4|83)(19|83) = -(19|83) = (83|19) = (7|19) = -(19|7) = -(5|7) = 1,$$

e portanto $(2455|4993) = -1$.
Deduzimos que a equação tem soluções.

6. Seja p um primo congruente com 1 módulo 4 e d um inteiro ímpar tal que $d \mid (p-1)$.
Mostrar que d é resíduo quadrático módulo p.

Resolução: Seja q um factor primo de d, o que implica $p \equiv 1 \mod q$. Temos

$$(q|p) = (p|q) = (1|q) = 1.$$

Se $d = \prod_{i=1}^{r} q_i^{k_i}$, temos

$$(d|p) = \prod_{i=1}^{r} (q_i^{k_i}|p) = \prod_{i=1}^{r} (q_i|p) = 1.$$