Restos e divisores

Sejam a um número inteiro e $m > 1$ um número natural. Usando o algoritmo da divisão Euclideana, podemos escrever a na forma $mq + r$, de forma única, onde q é um inteiro e $r \in \{0, 1, \ldots, m-1\}$. O número r é o *resto da divisão de* a *por* m. Alternativamente, r diz-se o valor de a *módulo* m e denota-se $(a \mod m)$. Se b é um outro inteiro, dizemos que a *é congruente com* b *módulo* m se a e b têm o mesmo resto quando divididos por m, ou seja, se $(a \mod m) = (b \mod m)$. Nota que isto é equivalente a ter-se que m divide $a - b$, ou ainda, que existe um inteiro x tal que $a = mx + b$. Quando a e b são congruentes módulo m, escrevemos $(a \equiv b \mod m)$.

1. Mostra que: se $(a_1 \equiv b_1 \mod m)$ e $(a_2 \equiv b_2 \mod m)$ então $(a_1 + a_2 \equiv b_1 + b_2 \mod m)$ e $(a_1a_2 \equiv b_1b_2 \mod m)$.

2. **Algoritmo de Euclides**

   (a) Mostra que $\mathrm{mdc}(a, b) = \begin{cases} a, & \text{se } b = 0; \\ \mathrm{mdc}(b,\ a \mod b), & \text{caso contrário.} \end{cases}$

   O algoritmo de Euclides é um procedimento que, usando esta propriedade, nos permite calcular o máximo divisor comum entre dois inteiros. Explicitamente, se $b \neq 0$, toma-se $r_{-1} = a$ e $r_0 = |b|$ e, no i-ésimo passo, calculam-se os únicos inteiros q_i e r_i tais que $r_{i-2} = r_{i-1}q_i + r_i$ e $0 \leq r_i < r_{i-1}$. O algoritmo termina quando se obtém $r_k = 0$ e, nesse caso, temos que $\mathrm{mdc}(a, b) = r_{k-1}$.

   (b) Explica porque é que o algoritmo de Euclides termina sempre e calcula corretamente o máximo divisor comum de a e b.

   (c) Usa o algoritmo de Euclides para calcular o máximo divisor comum entre 70 e 130.

3. **Teorema de Bézout**

   O Teorema de Bézout diz-nos que $\mathrm{mdc}(a, b)$ pode ser escrito como combinação linear de a e b, isto é, que existem inteiros x, y tais que $\mathrm{mdc}(a, b) = ax + by$.

   Considera o conjunto $S = \{ax + by \mid x, y \in \mathbb{Z}\}$.

   (a) Mostra que o conjunto S contém pelo menos um inteiro positivo.

   (b) Seja $d = ax_0 + by_0$ o menor inteiro positivo do conjunto S, para certos $x_0, y_0 \in \mathbb{Z}$. Mostra que d é o máximo divisor comum de a e b.

   (c) Em geral, podemos usar o algoritmo de Euclides para escrever $\mathrm{mdc}(a, b)$ como combinação linear de a e b. Explica como.

4. Mostra que a equação $(ax \equiv b \mod m)$ tem solução em x se e só se o máximo divisor comum de a e m divide b.

Um *inverso módulo m de a* é um inteiro x tal que $(ax \equiv 1 \mod m)$. Nota que, pela questão anterior, um tal x existe se e só se a e m forem primos entre si (ou *coprimos*). Além disso, pelo Teorema de Bézout, se a e m são primos entre si, ou seja, se $\operatorname{mdc}(a, b) = 1$, então podemos escrever $1 = ax_0 + my_0$ para certos inteiros x_0, y_0. Em particular, temos $(ax_0 \equiv 1 \mod m)$.

5. Calcula:

   (a) o inverso de 4 módulo 25,

   (b) o inverso de 13 módulo 7.

O seguinte resultado pode ser útil na abordagem a diversos problemas olímpicos.

Teorema Chinês dos Restos

Sejam $m_1, \ldots, m_k$ números inteiros positivos, coprimos dois a dois, e sejam $a_1, \ldots, a_k$ números inteiros. Então, existe um inteiro x tal que

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \ldots \\ x \equiv a_k \mod m_k \end{cases}$$

Além disso, módulo $m_1 m_2 \ldots m_k$, tal x é único e é dado por

$$a_1 \,\widehat{m}_1\, n_1 + a_2 \,\widehat{m}_2\, n_2 + \cdots + a_k \,\widehat{m}_k\, n_k \mod m_1 m_2 \ldots m_k,$$

onde, para $i \in \{1, 2, \ldots, k\}$, $\widehat{m}_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$ e n_i é o inverso de $\widehat{m}_i$ módulo m_i.

6. Calcula os últimos dois algarismos de 2023^{2023}.

7. **(AIME II 2012)** Sejam n e p inteiros positivos. Dizemos que n é p-seguro se a diferença entre n e qualquer múltiplo de p é, em valor absoluto, maior que 2. Por exemplo, os números 10-seguros são $3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \ldots$. Quantos inteiros positivos menores ou iguais a 10000 são simultaneamente 7-seguros, 11-seguros e 13-seguros?