Questão 01 **[2,00 pts ::: (a)=1,00 pt; (b)=1,00 pt]**

(a) Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Mostre que $a - b$ divide $a^n - b^n$.

(b) Seja n um número natural. Mostre que, se $2^n - 1$ é primo então n é primo.

Solução

(a) Vamos provar usando indução sobre n.

A afirmação é verdadeira para $n = 1$, pois $a - b$ divide $a - b$.

Suponhamos, agora, que $a - b \mid a^n - b^n$. Temos que

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a - b)a^n + b(a^n - b^n)$$

Como $a - b \mid a - b$ e, por hipótese, $a - b \mid a^n - b^n$, decorre da igualdade acima que

$$a - b \mid a^{n+1} - b^{n+1}$$

Portanto, a afirmação é válida para todo n natural.

(b) Suponhamos que n não é primo. Temos que $n = a \cdot b$, com $1 < a < n$ e $1 < b < n$. Como pelo item (a), $2^a - 1$ divide $(2^a)^b - 1 = 2^n - 1$, onde $2^a - 1 \neq 1$ e $2^a - 1 \neq 2^n - 1$, concluímos que $2^n - 1$ é composto.

Portanto, se $2^n - 1$ é primo então n é primo.

Questão 02 **[2,00 pts ::: (a)=1,00 pt; (b)=1,00 pt]**

(a) Mostre que se n é um número ímpar, então $1 + 2 + 3 + \cdots + (n - 1) \equiv 0 (\mathrm{mod}\, n)$.

(b) Mostre que se n é um número par, então $1 + 2 + 3 + \cdots + (n - 1) \not\equiv 0 (\mathrm{mod}\, n)$.

Solução

Primeiro observe que $1 + 2 + 3 + \cdots + (n - 1) = \dfrac{(n - 1)n}{2}$.

(a) Se n é ímpar, então $(n - 1)$ é par e $\dfrac{(n - 1)}{2}$ é um número inteiro. Assim, $n \mid 1 + 2 + 3 + \cdots + (n - 1)$, portanto $1 + 2 + 3 + \cdots + (n - 1) \equiv 0 (\mathrm{mod}\, n)$.

(b) Se n é par, então $n = 2k$, para algum $k \in \mathbb{N}$. Logo $\dfrac{(n - 1)n}{2} = (n - 1)k$. Como $(n, n - 1) = 1$ e $k < n$ segue que $n \nmid (n - 1)k$, portanto

$1 + 2 + 3 + \cdots + (n - 1) \not\equiv 0 (\mathrm{mod}\, n)$.

Questão 03 **[2,00 pts]**

Um palíndromo é um número que, escrito da direita para a esquerda ou da esquerda para a direita, o resultado é o mesmo (por exemplo, 373 e 521125 são palíndromos). Prove que todo palíndromo com um número par de algarismos é divísivel por 11.

Solução

Considere a representação decimal de um palíndromo a com um número par de algarismos.

Assim, $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ e
$a = a_0 10^n + a_1 10^{n-1} + \cdots + a_{n-1}10 + a_n$, com n ímpar.

Usando a congruência módulo 11 e o fato de que $10 \equiv -1 \bmod 11$, temos que
$a \equiv a_0 - a_1 + \cdots + a_{n-1} - a_n \bmod 11$ e $a \equiv a_n - a_{n-1} + \cdots + a_1 - a_0 \bmod 11$.

Somando as duas congruências, obtemos $2a \equiv 0 \bmod 11$, e como $(2, 11) = 1$, $a \equiv 0 \bmod 11$.

Portanto a é divisível por 11.

Questão 04 **[2,00 pts]**

Se $p > 3$ e os números p e $p + 2$ são primos, mostre que $12 \mid 2p + 2$.

Solução

Ao dividir um inteiro p por 12 os possíveis restos são: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11. Se $p > 3$ é um número primo, então não ocorrem o seguintes restos: 0, 2, 3, 4, 6, 8, 9 e 10, pois isto acarretaria que p é divisível por 2 ou 3. Como $p + 2$ também é primo os restos 1 ou 7 também não podem ocorrer.

De fato,

$$p = 12k_1 + 1 \Rightarrow p + 2 = 12k_1 + 3 \Rightarrow 3|p + 2.$$
$$p = 12k_2 + 7 \Rightarrow p + 2 = 12k_1 + 9 \Rightarrow 3|p + 2.$$

Portanto $p = 12k_3 + 5$ ou $p = 12k_4 + 11$. Nestes dois casos,

$$2p + 2 = 24k_3 + 12 \Rightarrow 12|2p + 2.$$
$$2p + 2 = 24k_4 + 24 \Rightarrow 12|2p + 2.$$

Questão 05 **[2,00 pts ::: (a)=1,00 pt; (b)=1,00 pt]**

Seja $m > 1$ um número inteiro.

(a) Mostre que um elemento $[a] \in \mathbb{Z}_m$ é invertível se, e somente se, $(a, m) = 1$.

(b) Mostre que o anel $\mathbb{Z}_m$ é corpo se, e somente se, m é primo.

Solução

(a) Se $[a]$ é invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $1 = [a] \cdot [b] = [a \cdot b]$. Logo $a \cdot b \equiv 1 \bmod m$, isto é, existe $t \in \mathbb{Z}$ tal que $a \cdot b - 1 = t \cdot m$ ou $a \cdot b - t \cdot m = 1$. Portanto $(a, m) = 1$.
Reciprocamente, se $(a, m) = 1$, então existem x, $y \in \mathbb{Z}$ tal que $a \cdot x + m \cdot y = 1$. Logo, $[1] = [a \cdot x + m \cdot y] = [a \cdot x] + [m \cdot y] = [a] \cdot [x] + [0] = [a] \cdot [x]$, ou seja, $[a]$ é invertível.

(b) Se m é primo, então $(a, m) = 1$ para todo $1 \leq a \leq m - 1$. Pelo item a), os elementos $[1], [2], \ldots, [m-1]$ são invertíveis e $\mathbb{Z}_m$ é corpo.
Reciprocamente, se m não é primo, existem inteiros $1 < a$, $b < m$ tal que $m = a \cdot b$. Assim, $[0] = [m] = [a] \cdot [b]$ com $[a] \neq 0$ e $[b] \neq 0$. Ou seja, $[a]$ e $[b]$ não são elementos invertíveis e $\mathbb{Z}_m$ não é corpo.