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

Sejam x, y e z números inteiros positivos tais que $x^2 + y^2 = z^2$.

(a) Prove que x e y não podem ser ambos ímpares.

(b) Se y é ímpar, prove que $4|x$.

Solução

(a) Suponhamos que x e y são simultaneamente ímpares, isto é, $x = 2r + 1$ e $y = 2s + 1$ com $r, s \in \mathbb{N}$. Então $x^2 + y^2 = 4(r^2 + s^2 + r + s) + 2 = 4k + 2$ é um número par. Logo $z^2 = x^2 + y^2$ é par e consequentemente z é par, ou seja, $z = 2n$ com $n \in \mathbb{N}$. Mas isto acarreta $4n^2 = 4k + 2$ e portanto $2n^2 = 2k + 1$. Absurdo, não podemos ter par igual a ímpar.

(b) Pelo item (a) se y é ímpar, então x é par. Como $z^2 = x^2 + y^2$ e $x^2 + y^2$ é ímpar então z é ímpar. Sejam n, m e t em $\mathbb{N}$ tais que $x = 2n$, $y = 2m + 1$ e $z = 2s + 1$. Devemos provar que n é par. De fato,

$$x^2 + y^2 = z^2 \Rightarrow 4n^2 + 4m^2 + 4m + 1 = 4s^2 + 4s + 1 \Rightarrow n^2 + m^2 + m = s^2 + s$$

Portanto, $n^2 = (s^2 + s) - (m^2 + m)$, ou seja, n^2 é par e consequentemente n é par.

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

(a) Sejam a, b, c números inteiros. Se $a|c$, $b|c$ e $(a, b) = 1$, prove que $ab|c$.

(b) Se p e q são números primos p, $q \geqslant 5$, prove que $24|p^2 - q^2$.

Solução

(a) A hipótese $(a, b) = 1$, nos assegura que existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = 1$. Multiplicando a igualdade por c, temos $cax_0 + cby_0 = c$. Como $a|c$ e $b|c$, existem inteiros c_1 e c_2 tais que $c = c_1a$ e $c = c_2b$. Substituindo, temos que $c_2bax_0 + c_1aby_0 = ab(c_1x_0 + c_2y_0) = c$. Portanto, $ab|c$.

(b) Pelo item (a), basta provar que $2^3|(p - q)(p + q)$ e $3|(p - q)(p + q)$.

(i) Provemos que $2^3|(p - q)(p + q)$

Suponhamos $p \geqslant 5$ primo. Segue que p é da forma $4k + 1$ ou da forma $4k + 3$. Como $(4k + 1)^2 = 16k^2 + 8k + 1$ e $(4k + 3)^2 = 8k^2 + 24k + 8 + 1$, em qualquer caso, temos que p^2 é da forma $8k + 1$.

Portanto, se $p \geqslant 5$ e $q \geqslant 5$ são primos, então $p^2 = 8k + 1$ e $q^2 = 8t + 1$, logo 8 divide $p^2 - q^2 = 8(k - t)$.

(ii) Provemos que $3|p^2 - q^2$.

Como p e q são primos maiores ou iguais a cinco, então $p = 3n_1 + 1$ ou $p = 3n_2 + 2$ e $q = 3m_1 + 1$ ou $q = 3m_2 + 2$. Em qualquer caso, $p^2 = 3n + 1$ e $q^2 = 3m + 1$. Portanto $p^2 - q^2 = 3(n + m)$, ou seja, $3|p^2 - q^2$.

(i) Solução alternativa

Como p e q são ímpares, $p+q$ e $p-q$ são pares, ou seja, $p+q=2n$ e $p-q=2m$. Resta mostrar que n ou m é par. Somando, temos $2p=2(n+m)$, isto é, $p=n+m$. Portanto, n e m não podem ser ambos ímpares, caso contrário p seria par. Portanto $2^3|p^2-q^2$.

Questão 03 **[2,00 pts ::: (a)=1,00 pt; (b)=1,00 pt]**

Para $n \in \mathbb{N}$, designaremos por $\varphi(n)$ a *função fi de Euler*.

(a) Se p é um número primo e r um número natural, prove que

$$\varphi(p^r) = p^r\left(1-\frac{1}{p}\right).$$

(b) Se n é um número par tal que $\varphi(n)=\dfrac{n}{2}$. Prove que $n=2^r$, para algum $r \geqslant 1$.

Solução

(a) De 1 até p^r existem p^r números naturais. Para obter $\varphi(p^r)$ devemos excluir, desses, os números que não são primos com p^r, ou seja, todos os múltiplos de p, que são precisamente $p, 2p, 3p, \ldots, p^{r-1}p$, cujo número é p^{r-1}. Portanto

$$\varphi(p^r) = p^r - p^{r-1} = p^r\left(1-\frac{1}{p}\right)$$

(b) O número n é da forma $n=2^r q$, sendo $r \geq 1$ e $(2^r, q)=1$. Como a função φ é multiplicativa, $\varphi(n)=\varphi(2^r)\varphi(q)=2^{r-1}\varphi(q)$. Por hipótese $\varphi(n)=\dfrac{n}{2}=2^{r-1}q$. Portanto, $2^{r-1}\varphi(q)=2^{r-1}q$, o que acarreta $\varphi(q)=q$. Como o único número com a propriedade que $\varphi(q)=q$ é o número 1, então $n=2^r$.

Questão 04 **[2,00 pts ::: (a)=1,00 pt; (b)=1,00 pt]**

(a) Sejam $a, m, n \in \mathbb{Z}$, com $m>1$, $n \geq 0$ e $(a,m)=1$. Mostre que $a^n \equiv 1 \bmod m$ se, e somente se, $\mathrm{ord}_m(a)$ divide n.

(b) Sejam p, q primos. Mostre que, se $2^p \equiv 1 \bmod q$, então $q \equiv 1 \bmod p$.

Definição: $\mathrm{ord}_m(a) := \min\{i \in \mathbb{N} \quad | \quad a^i \equiv 1 \bmod m\}$

Solução

(a) Suponha que $\mathrm{ord}_m(a) \mid n$, isto é, $n = \mathrm{ord}_m(a)\cdot q$, com $q \in \mathbb{Z}$. Assim,

$$a^n = a^{\mathrm{ord}_m(a)\cdot q} = (a^{\mathrm{ord}_m(a)})^q \equiv 1^q \equiv 1 \bmod m$$

Reciprocamente, suponha que $a^n \equiv 1 \bmod m$. Pela divisão euclidiana, podemos escrever $n = \mathrm{ord}_m(a)\cdot q + r$, onde $0 \leq r < \mathrm{ord}_m(a)$. Então,

$$1 \equiv a^n \equiv a^{\mathrm{ord}_m(a)q+r} \equiv (a^{\mathrm{ord}_m(a)})^q a^r \equiv a^r \bmod m$$

Como $\mathrm{ord}_m(a)$ é o menor expoente natural i tal $a^i \equiv 1 \bmod m$ e $0 \leq r < \mathrm{ord}_m(a)$, concluimos que $r=0$. Portanto, $\mathrm{ord}_m(a) \mid n$.

(b) Suponha, então, que $2^p \equiv 1 \bmod q$. Como

$\text{ord}_q(2) \neq 1$ e, pelo item (a), $\text{ord}_q(2) \mid p$, concluimos que $\text{ord}_q(2) = p$.

Por outro lado, observando que q é necessariamente ímpar, pelo pequeno Teorema de Fermat, temos que

$2^{q-1} \equiv 1 \bmod q$, logo $\text{ord}_q(2) = p \mid q-1$.

Portanto, $q \equiv 1 \bmod p$.

Questão 05 **[2,00 pts]**

Se $p > 3$ e os números p e $p+2$ são números naturais primos, mostre que $2p + 2 \equiv 0 \bmod 12$.

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,

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

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