Questão 01 **[2,00 pts]**

As ternas de números inteiros positivos (x, y, z), com $(x, y) = 1$, que satisfazem a equação $x^2 + y^2 = z^2$ são denominadas *ternas pitagóricas primitivas* e o triângulo retângulo de catetos x e y e hipotenusa z é chamado um *triângulo pitagórico primitivo*. Um resultado bastante conhecido é:

"As ternas pitagóricas primitivas (x, y, z) são da forma $x = a^2 - b^2, y = 2ab, z = a^2 + b^2$ com a, b números inteiros positivos com $a > b$."

Use o resultado acima para provar que se x e y são os catetos de um triângulo pitagórico primitivo, então a área desse triângulo é um múltiplo de 6.

Solução

Temos que a área do triângulo é dada por $A = \frac{x \cdot y}{2}$, onde

$x = a^2 - b^2, y = 2ab$, logo $A = (a^2 - b^2)ab$, com $a > b > 0$.

Se a e b são impares então $a^2 - b^2$ é par, caso contrário, temos a ou b é par.

Portanto $A = (a^2 - b^2)ab$ é sempre par.

Por outro lado, qualquer inteiro é da forma $3k, 3k + 1$ ou $3k + 2$, com $k \in \mathbb{Z}$.

Se $x = 3k + 1$ ou $3k + 2$ temos que $x^2 = 3t + 1$, com $k, t \in \mathbb{Z}$.

Se a e b não são múltiplos de 3 temos que $a^2 - b^2 = 3t_1 + 1 - 3t_2 - 1 = 3(t_1 - t_2)$, caso contrário, a ou b é múltiplo de 3.

Portanto $A = (a^2 - b^2)ab$ é sempre múltiplo de 3.

Como A é múltiplo de 2 e de 3 concluimos que A é múltiplo de 6.

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

Uma pessoa recebeu 91 reais em notas de 2 e 5 reais.

(a) Qual é o número máximo de notas que ela pode ter recebido? E qual é o número mínimo?

(b) O número de notas recebidas de 2 reais pode ter sido igual ao número de notas de 5 reais?

Solução

(a) Indicando por x o número de notas de 2 reais e por y o número de notas de 5 reais temos que

$$2x + 5y = 91$$

Resolvendo a equação diofantina, encontramos a solução minimal $x = 3$ e $y = 17$ e a solução em $\mathbb{N}$ é dada por

$$\begin{cases} x = & 3 + 5t \\ y = & 17 - 2t \end{cases}$$

onde $0 \leq t \leq 8$.

Como $x + y = 20 + 3t$, o número máximo de notas é igual a 44 e o número mínimo é igual a 20.

(b) Temos que $x = y$ quando $t = 2$, obtendo $x = y = 13$.

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

Dados a, b, $m \in \mathbb{Z}$, com $m > 1$.

a) Prove que: a congruência $aX \equiv b \bmod m$ possui solução se, e somente se, $(a, m)|b$.

b) Resolva a congruência $6X \equiv 15 \bmod 21$.

Solução

a) Suponha que a congruência $aX \equiv b \bmod m$ tenha uma solução x_0, isto é, $m|ax_0 - b$, o que equivale à existência de y tal que $ax_0 - b = my$. Portanto a equação diofantina $aX - mY = b$ possui solução. Logo $(a, m)|b$.
Reciprocamente, suponha que $(a, m)|b$. Logo a equação diofantina $aX - mY = b$ admite uma solução x_0 e y_0. Ou seja, $ax_0 = b + my_0$ e consequentemente, x_0 é solução da congruência $aX \equiv b \bmod m$.

b) Como $(6, 21) = 3$ e $3|15$, então a congruência $6X \equiv 15 \bmod 21$ tem três soluções módulo 21. Por inspeção $x_0 = 6$ é uma solução da congruência. Portanto 6, 13 e 20, são as três soluções não congruentes. Logo todas as soluções são dadas por

$$\{6 + 21t | t \in \mathbb{Z}\} \cup \{13 + 21s | s \in \mathbb{Z}\} \cup \{20 + 21r | r \in \mathbb{Z}\}$$

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

(a) Dado um número primo p, prove que p divide $a^p - a$, para todo $a \in \mathbb{Z}$.

(b) Sejam p um número primo e a e b números inteiros. Mostre que

$$(a + b)^p \equiv a^p + b^p \mod p$$

Solução

(a) Se $p = 2$, temos que $a^2 - a = a(a - 1)$ é par e assim 2 divide $a^2 - a$.
Suponhamos p ímpar. Nesse caso, como
$(-a)^p - (-a) = -(a^p - a)$ basta provar o resultado para $a \geq 0$. Vamos provar usando indução sobre a.
O resultado vale para $a = 0$ pois p divide 0.
Supondo o resultado válido para a, provaremos para $a + 1$.
Pela fórmula do Binômio de Newton,

$$(a + 1)^p - (a + 1) = a^p - a + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$$

Usando a hipótese de indução e o fato que $\binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a$ é divisível po p, concluimos que p divide $(a+1)^p - (a+1)$.

(b) Temos que, para todo $a \in \mathbb{Z}$, $a^p \equiv a \mod p$, pois p divide $a^p - a$.
Daí,

$$(a + b)^p \equiv a + b \equiv a^p + b^p \mod p$$

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

Seja $p \geq 3$ um número primo e $b \in \mathbb{N}$. Prove que:

a) $b^p + (p-1)!b \equiv 0 \bmod p$

b) $(p-1)! \equiv (p-1) \bmod (1+2+3+\cdots+(p-1))$

Solução

a) Pelo Pequeno Teorema de Fermat $b^p \equiv b \bmod p$. Pelo Teorema de Wilson, tem-se $(p-1)! \equiv -1 \bmod p$, que acarreta $(p-1)!b \equiv -b \bmod p$. Somando as duas congruências , obtemos

$$b^p + (p-1)!b \equiv (b-b) \bmod p \equiv 0 \bmod p$$

b) Note que, $1+2+\cdots+(p-1) = \dfrac{p(p-1)}{2}$. Como $(p, \dfrac{p-1}{2}) = 1$ é suficiente provar a congruência dada módulo p e módulo $\dfrac{p-1}{2}$. Pelo teorema de Wilson tem-se $(p-1)! \equiv -1 \bmod p$, que acarreta $(p-1)! \equiv (p-1) \bmod p$.
Agora, $(p-1)!-(p-1) = (p-1)((p-2)!-1)$. Como $\dfrac{p-1}{2} | (p-1)$, então $\dfrac{p-1}{2} | ((p-1)! - (p-1))$, ou seja, $(p-1)! \equiv (p-1) \bmod \dfrac{p-1}{2}$.