MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

**Avaliação 3 - MA14 - 2015.2**

**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 $4|x$.

**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 $24|p^2 - q^2$.

**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 $r \geqslant 1$.

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

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

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

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

**Questão 05** **[ 2,00 pts ]**

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