Algebra I Lista 4 para ser entregue dia 29/05

1) Sejam a, b, n, m em $\mathbb{N}$ com $n, m > 1$.

Mostre que o sistema

$x \equiv a \pmod{n}$
$x \equiv b \pmod{m}$

possui solução $\Leftrightarrow$ $a \equiv b \pmod{mdc(n,m)}$

A lem disso no caso de haver solução ela é única modulo $m.n$.

2) Sejam $p, a \in \mathbb{N}$ p primo, $p > 2$, $p \nmid a$.

Se $x^2 \equiv a \pmod{p}$ tem solução $x_0 \in I = \{0, 1, \ldots, p-1\}$ então $p - x_0$ também é solução e estas são as únicas em I.

3) Sejam a, p em $\mathbb{N}$, p um primo impar $p \nmid a$.

a) Se $x^2 \equiv a \pmod{p}$ não tem solução então $(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$ e
Se $x^2 \equiv a \pmod{p}$ tem solução então.
$(p-1)! + a^{\frac{p-1}{2}} \equiv 0 \mod p$.

4) Seja p primo ímpar e $p \nmid a$, $a \in \mathbb{N}$. Prove que

i) $p \mid a^{\frac{p-1}{2}} - 1 \iff x^2 \underset{p}{\equiv} a$ tem solução

ii) $p \mid a^{\frac{p-1}{2}} + 1 \iff x^2 \underset{p}{\equiv} a$ não tem solução

5) Se p é um primo ímpar então os numeros $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ são dois a dois não congruentes modulo p e representam todos os quadrados módulo p

6) Determinar os numeros entre 1 e 1200 que tem restos 1, 2, 6 quando divididos respectivamente por 9, 11 e 13.

7) Sejam a um inteiro Provar que

a) $a^{21} \equiv a \ (15)$, $a^7 \equiv a \ (42)$

b) Se $mdc(a, 35) = 1$ então $a^{12} \equiv 1 \ (35)$

c) Se $mdc(a, 42) = 1$ então $3.7.8 \mid a^6 - 1$.

8) Prove que para quaisquer inteiros a, b e p com $p > 1$ vale a implicação

$$a^p \equiv b^p \ (p) \implies a \equiv b \ (p).$$