Lista 4

Sistemas de Congruências Lineares

1. Resolva as seguintes sistemas de congruências lineares:

   a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$,

   b) $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod 7 \end{cases}$,

   c) $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}$.

2. Determine o menor inteiro a, maior que 100, tal que:

$$2 \mid a;\ 3 \mid (a+1);\ 4 \mid (a+2);\ 5 \mid (a+3);\ 6 \mid (a+4).$$

3. Se de uma cesta com ovos retiramos duas unidades por ver, sobra 1 ovo. O mesmo acontece se os ovos são retirados de 3 em 3, de 4 em 4, de 5 em 5, de 6 em 6. Mas não resta nehnum resto se retiramos 7 unidades cada vez. Qual é menor numero possivel de ovos na cesta?

Teoremas de Euler, Fermat e Wilson

4. Seja a um inteiro. Demonstre as afirmações abaixo.

   a) $a^{21} \equiv a \pmod{15}$ e $a^{21} \equiv a \pmod{15}$

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

   c) Se mdc$(a, 42) = 1$ então $3 \cdot 7 \cdot 8 \mid a^6 - 1$.

5. a) Sejam a, b inteiros e seja p um primo positivo tal que mdc$(a, p) = 1$. Mostre que $x = a^{p-2}b$ é solução da congruência $ax \equiv b \pmod p$.

   b) Resolva as congruências $6x \equiv 5 \pmod{11}$ e $3x \equiv 17 \pmod{29}$

6. a) Seja p um inteiro primo e sejam a, b inteiros arbitrarios. Mostre que se $a^p \equiv b^p \pmod p$ então $a \equiv b \pmod p$.

   b) Seja $p > 2$ um primo. Mostre que

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod p.$$

7. Mostre que $2^8 \equiv 1 \pmod{17}$ e que $2^{16} \equiv 1 \pmod{17}$.

8. Sejam p um primo e a um inteiro tal que $p \nmid a$. Prove que

   a) se $p > 2, a^{\frac{p-1}{2}} \equiv 1 \pmod p$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod p$;

   b) o menor inteiro positivo e tal que $a^e \equiv 1 \pmod p$ é divisor de $p - 1$;

c) se e é o inteiro acima de x é um inteiro tal que $a^x \equiv 1 \pmod{p}$ então $e \mid x$.

9. a) Sejam p, q primos distintos e impares tais que $(p-1) \mid (q-1)$. Mostre que se $\text{mdc}(a, pq) = 1$ então $a^{q-1} \equiv 1 \pmod{pq}$.

   b) Seja a um inteiro. Prove que $a^{37} \equiv a \pmod{1729}$; $a^{79} \equiv a \pmod{158}$.

10. Sejam a um inteiro e n um inteiro positivo tais que $\text{mdc}(a, n) = \text{mdc}(a-1, n) = 1$. Prove que

$$1 + a + \cdots + a^{\varphi(n)+1} \equiv 0 \pmod{n}.$$

11. Sejam m, n inteiros positivos relativamente primos. Prove que

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

12. Determine o resto de divição de a por b nos casos

    a) $a = 15!$ e $b = 17$.

    b) $a = 2 \cdot (26)!$ e $b = 29$.

13. Reúna os inteiros $2, 3, \ldots, 21$ em pares (a, b) tais que $ab \equiv 1 \pmod{23}$.

14. Mostre que $18! \equiv -1(\mod 437)$.

15. Encontre o resto de divição $5! \cdot 25!$ por 31.