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. Resolva as seguintes sistemas de congruências lineares:

   a) $\begin{cases} 4x \equiv 3 \pmod 7 \\ 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases}$,

   b) $\begin{cases} 3x \equiv 5 \pmod 2 \\ x \equiv -3 \pmod 5 \\ 4x \equiv 7 \pmod 9 \end{cases}$.

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

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

4. Se de uma cesta com ovos retiramos duas unidades por vez, 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 nenhum resto se retiramos 7 unidades cada vez. Qual é menor numero possível de ovos na cesta?

Teoremas de Euler, Fermat e Wilson

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

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

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

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

6. a) Sejam a, b inteiros e seja p um primo positivo tal que $\text{mdc}(a, p) = 1$. 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 $3x \equiv 17 \pmod{29}$

7. Encontre o resto de divisão de

   a) 5^{14} por 7.

b) 5^{100} por 11.

c) 15^{175} por 11.

d) 31^{200} por 28.

e) $2^{7^{2002}}$ por 352.

8. Encontre dois ultimos digitos do

a) 2^{999};

b) 3^{999};

c) 5^{2020};

d) 7^{2019};

e) 123^{2010};

f) 557^{2012};

9. a) Seja p um inteiro primo e sejam a, b inteiros arbitrários. Mostre que se $a^p \equiv b^p \pmod{p}$ então $a \equiv b \pmod{p}$.

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

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

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

11. 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 $e \mid x$.

12. 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 $a^{37} \equiv a \pmod{1729}$; $a^{79} \equiv a \pmod{158}$.

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

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

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

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

15. Determine o resto da divisão de a por b nos casos

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

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

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

17. Mostre que $18! \equiv -1 \pmod{437}$.

18. Encontre o resto de divisão de

a) $5! \cdot 25!$ por 31;

b) $97!$ por 101;

c) $65!$ por 71;

d) $53!$ por 61;

e) $149!$ por 139;

19. Resolve

a) $\varphi(n) = n/3$.

b) $\varphi(2x) = \varphi(3x)$.

c) $\varphi(x) = 2$.

d) $\varphi(x) = 2x/3$.

e) $\varphi(x) = 6$.

20. Mostre que para todo n temos

a) $\varphi(4n) = 2\varphi(2n)$;

b) $\varphi(4n + 2) = \varphi(2n + 1)$;