Álgebra 1

Lista 07

(Congruência Módulo m)

7.1. (Gavetas de Dirichlet) Se $x_1, \ldots, x_m$ são inteiros, demostre que a soma de um certo subconjunto de $\{x_1, \ldots, x_m\}$ é um múltiplo de m.

(Dica: Considere as distintas classes módulo m dentre as determinadas por $0, x, x_1 + x_2, \ldots, x_1 + \ldots + x_m$)

7.2. (Quadrados perfeitos II). Verifique que cada quadrado perfeito é congruente a $0, 1,$ ou $4 \pmod 8$.

7.3. (Teorema Chinês dos Restos I). Dados inteiros a e b, verifique que uma condição necessária e suficiente para que o par de congruências $x \equiv a \pmod m$, $x \equiv b \pmod n$ possua uma solução é que $a \equiv b \pmod d$, onde $d = \text{m.d.c}(m, n)$. Se $d = 1$, verifique que a solução é única módulo mn.

7.4. (Polinômios e divisibilidade). Se $f(X)$ é um polinômio com coeficientes inteiros e se $x \equiv y \pmod m$, verifique que $f(x) \equiv f(y) \pmod m$. Obtenha critérios de divisibilidade por 9 e por 11.

7.5. (Módulo composto). Se m e n são inteiros positivos relativamente primos, e $f(X)$ é um polinômio com coeficientes inteiros, demonstre que a congruência $f(x) \equiv 0 \pmod{mn}$ possui uma solução se, e somente se, $f(x) \equiv 0 \pmod m$ e $f(x) \equiv 0 \pmod n$ ambas possuem soluções.
(Dica: use o Teorema Chinês dos Restos e o Exercício 7.4.)

7.6. (Levantamento de Hensel). Sejam p um primo e $f(X)$ um polinômio com coeficientes inteiros. Suponha que $f(a) \equiv 0 \pmod{p^k}$ para algum inteiro $k > 0$. Prove que as seguintes condições são equivalentes:

(i) $f(a + tp^k) \equiv 0 \pmod{p^{k+1}}$ para algum t;

(ii) $Df(a)t \equiv -\frac{f(a)}{p^k} \pmod p$ para algum t;

(iii) ou $Df(a) \not\equiv 0 \pmod p$ ou $f(a) \equiv 0 \pmod{p^{k+1}}$.

7.7. (Relação de equivalência). Para x e y inteiros > 0, escreva $x \sim y$ se $\frac{y}{x}$ é uma potência de 2; prove que isso é uma relação de equivalência, e que $x \sim y$ se, e somente se, os divisores ímpares de x são os mesmos de y.