Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 10

Congruências de Grau Superior

1 Congruências de Grau Superior

Dado um polinômio $f(x) \in \mathbb{Z}[x]$ e um número natural n, vamos estudar condições para que a congruência

$$f(x) \equiv 0 \pmod{n}$$

tenha solução. O primeiro resultado diz que basta considerar o caso em que $n = p^k$ é a potência de um primo p.

Proposição 1. *Suponhamos que $n = p_1^{k_1} \cdots p_l^{k_l}$ onde os p_j são primos distintos. Temos uma equivalência*

$$f(x) \equiv 0 \pmod{n} \iff \begin{cases} f(x) \equiv 0 \pmod{p_1^{k_1}} \\ \vdots \\ f(x) \equiv 0 \pmod{p_l^{k_l}} \end{cases}$$

de modo que $f(x) \equiv 0 \pmod{n}$ admite solução se, e somente se, $f(x) \equiv 0 \pmod{p_j^{k_j}}$ tem solução para cada j.

Demonstração. Como as potências $p_j^{k_j}$ são coprimas duas a duas, temos que n divide um inteiro M se, e só se, $p_j^{k_j} \mid M$ para cada j, o que demonstra a equivalência. Assim, a existência de solução para $f(x) \equiv 0 \pmod{n}$ implica a existência de solução para o sistema acima. Reciprocamente, se cada $f(x) \equiv 0 \pmod{p_j^{k_j}}$ tem uma solução $x \equiv a_j \pmod{p_j^{k_j}}$, pelo teorema chinês dos restos existe a tal que $a \equiv a_j \pmod{p_j^{k_j}}$ para todo j, de modo que $f(a) \equiv f(a_j) \equiv 0 \pmod{p_j^{k_j}}$ para todo j e logo $f(a) \equiv 0 \pmod{n}$ pela equivalência acima. Note em particular que o número de soluções distintas módulo n de $f(x) \equiv 0 \pmod{n}$ é igual ao produto do número de soluções módulo $p_j^{k_j}$ de $f(x) \equiv 0 \pmod{p_j^{k_j}}$. □

A próxima proposição indica como, a partir de uma solução de $f(x) \equiv 0 \pmod{p^{k_0}}$, obter soluções para $f(x) \equiv 0 \pmod{p^k}$ para todo $k \geq k_0$. Para isso, precisamos da noção de *derivada* de um polinômio: se $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{j=0}^{n} a_j x^j$, definimos sua derivada $p'(x)$ como sendo o polinômio $p'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 = \sum_{j=1}^{n} j a_j x^{j-1}$. Note que, se $p(x) \in \mathbb{Z}[x]$, então $p'(x) \in \mathbb{Z}[x]$.

Proposição 2 (Lema de Hensel). *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio, p um número primo. Seja $a \in \mathbb{Z}$ tal que $f(a) \equiv 0 \pmod{p^{k_0}}$ e cuja maior potência p^{l_0} de p com $p^{l_0} \mid f'(a)$ satisfaz $0 \leq 2l_0 < k_0$. Então existe uma sequência de inteiros $(a_k)_{k \geq k_0}$ com*

$$a_{k_0} = a, \quad a_{k+1} \equiv a_k \pmod{p^{k-l_0}} \qquad e$$
$$f(a_k) \equiv 0 \pmod{p^k} \text{ para todo } k \geq k_0.$$

Em particular, se existe um inteiro a tal que $f(a) \equiv 0 \pmod{p}$ mas $f'(a) \not\equiv 0 \pmod{p}$ então $f(x) \equiv 0 \pmod{p^k}$ admite solução para todo $k \in \mathbb{N}$.

Demonstração. Construímos a sequência indutivamente. Seja $k \geq k_0$ e suponha por indução que $p^k \mid f(a_k)$, ou seja, $f(a_k) = r_k p^k$ para um certo $r_k \in \mathbb{Z}$ e $p^{l_0} \mid f'(a_k)$ mas $p^{l_0+1} \nmid f'(a_k)$, ou seja, $f'(a_k) = s_k p^{l_0}$ onde $p \nmid s_k$. Estamos procurando um número da forma $a_{k+1} = a_k + t_k p^{k-l_0}$, com $t_k \in \mathbb{Z}$, que satisfaz $p^{k+1} \mid f(a_{k+1})$, $p^{l_0} \mid f'(a_{k+1})$ mas $p^{l_0+1} \nmid f'(a_{k+1})$.

Para cada $r \in \mathbb{N}$, temos

$$(a_k + t_k p^{k-l_0})^r = a_k^r + t_k r a_k^{r-1} p^{k-l_0} + \sum_{j=2}^{k} \binom{r}{j} a_k^{r-j} p^{j(k-l_0)} \equiv$$

$$\equiv a_k^r + t_k r a_k^{r-1} p^{k-l_0} \pmod{p^{k+1}},$$

pois a hipótese $0 \leq 2l_0 < k_0$ implica $2(k-l_0) \geq k+1$. Se $f(x) = \sum_{r=0}^{n} c_r x^r$, multiplicando a congruência acima por c_r e somando, de $r = 0$ até n, obtemos

$$f(a_{k+1}) = f(a_k + t_k p^{k-l_0}) = \sum_{r=0}^{n} c_r a_k^r + t_k \sum_{r=0}^{n} r a_k^{r-1} p^{k-l_0} =$$
$$= f(a_k) + t_k f'(a_k) p^{k-l_0} = r_k p^k + s_k t_k p^k \pmod{p^{k+1}}.$$

Logo para que $p^{k+1} \mid f(a_{k+1})$ devemos encontrar t_k tal que $r_k + s_k t_k \equiv 0 \pmod{p}$, o que é possível pois s_k é invertível módulo p. Finalmente, temos que

$$f'(a_{k+1}) \equiv f'(a_k) = s_k p^{l_0} \pmod{p^{k-l_0}}$$
$$\implies \begin{cases} f'(a_{k+1}) & \equiv 0 \pmod{p^{l_0}} \\ f'(a_{k+1}) & \not\equiv 0 \pmod{p^{l_0+1}} \end{cases}$$

o que completa a indução. □

Observemos que a condição sobre a derivada de f no lema de Hensel é necessária. Para isto, consideremos $f(x) = x^m + 3$ com $m \geq 2$, $a = 0$ e $p = 3$. Assim, temos que $f(0) = 3 \equiv 0 \pmod 3$, mas $f'(0) = 0$ é divisível por potências arbitrariamente grandes de 3, logo $f(x)$ não satisfaz a segunda hipótese da proposição. E de fato, se $b \in \mathbb{Z}$ e $f(b) = b^m + 3 \equiv 0 \pmod 3$ então $b \equiv 0 \pmod 3$, donde $b^m \equiv 0 \pmod 9$ e $f(b) = b^m + 3 \equiv 3 \pmod 9$, o que mostra que nenhuma raiz módulo 3 "levanta" para uma raiz módulo 9.

Agora vamos nos concentrar em equações módulo p. Para o próximo resultado, necessitamos de um

Lema 3. *Seja p um primo. Então*

$$1^k + 2^k + \cdots + (p-1)^k \bmod p = \begin{cases} 0 & \text{se } (p-1) \nmid k, \\ p-1 & \text{se } (p-1) \mid k. \end{cases}$$

Demonstração. Se $(p-1) \mid k$, temos que cada termo da soma acima é congruente a 1 módulo p e o resultado segue. Suponha agora que $(p-1) \nmid k$ e seja g uma raiz primitiva módulo p. Temos portanto

$$1^k + 2^k + \cdots + (p-1)^k \equiv 1 + g^k + g^{2k} + \cdots + g^{(p-2)k} \pmod p$$

Sendo $S = 1 + g^k + g^{2k} + \cdots + g^{(p-2)k}$, multiplicando por g^k e observando que $g^{(p-1)k} \equiv 1 \pmod p$ temos

$$\begin{aligned} & g^k S \equiv g^k + g^{2k} + \cdots + g^{(p-1)k} \pmod p \\ \iff & g^k S \equiv S \pmod p \iff (g^k - 1)S \equiv 0 \pmod p \end{aligned}$$

Como g é uma raiz primitiva e $(p-1) \nmid k$ temos que $g^k - 1 \not\equiv 0 \pmod p$, ou seja, $g^k - 1$ é invertível módulo p e portanto $S \equiv 0 \pmod p$, o que encerra a prova. □

Teorema 4 (Chevalley-Warning)**.** *Seja p um primo e sejam*

$$f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$$

polinômios em n variáveis com coeficientes inteiros tais que $f_i(0, \ldots, 0) \equiv 0 \pmod p$ para todo $i \leq k$. Suponha que $\sum_{1 \leq i \leq k} \deg(f_i) < n$. Então a quantidade de "pontos" em

$$A = \{(x_1, \ldots, x_n) \in (\mathbb{Z}/p\mathbb{Z})^n \mid f_i(x_1, \ldots, x_n) = \overline{0} \quad \forall i = 1, \ldots, k\}$$

é um múltiplo de p. Em particular, existem pontos $(x_1, \ldots, x_n) \neq (\overline{0}, \ldots, \overline{0})$ em $(\mathbb{Z}/p\mathbb{Z})^n$ tais que $f_i(x_1, \ldots, x_n) = \overline{0}$ para todo i.

Demonstração. Usaremos o lema anterior para determinar $|A| \bmod p$. Para isso, notemos que pelo teorema de Euler-Fermat $f_j(x_1, \ldots, x_n) \not\equiv 0 \pmod p \iff f_j(x_1, \ldots, x_n)^{p-1} \equiv 1 \pmod p$. Definamos

$$g(x_1, \ldots, x_n) = \prod_{1 \leq j \leq k} \big(1 - f_j(x_1, \ldots, x_n)^{p-1}\big).$$

Observemos que $g(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ se, e somente se, existe j tal que $f_j(x_1, \ldots, x_n) \not\equiv 0 \pmod{p}$. Por outro lado, se $f_j(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ para todo j então $g(x_1, \ldots, x_n) \equiv 1 \pmod{p}$, portanto

$$\sum_{(x_1,\ldots,x_n)\in(\mathbb{Z}/p\mathbb{Z})^n} g(x_1, \ldots, x_n) \equiv |A| \pmod{p}.$$

Notemos agora que $\deg(g) \leq \sum_{1\leq j\leq k}(p-1)\deg(f_j) < (p-1)n$. Portanto cada monômio $cx_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ de g é tal que $\sum_{1\leq j\leq n} i_j < (p-1)n$, donde pelo Princípio da Casa dos Pombos sempre existe algum r com $0 \leq i_r < p-1$. Assim, pelo lema anterior, $\sum_{x_r\in\mathbb{Z}/p\mathbb{Z}} x_r^{i_r} \equiv 0 \pmod{p}$ donde

$$\begin{aligned}\sum_{(x_1,\ldots,x_n)\in(\mathbb{Z}/p\mathbb{Z})^n} cx_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} &\equiv c\sum_{x_1\in\mathbb{Z}/p\mathbb{Z}} x_1^{i_1}\sum_{x_2\in\mathbb{Z}/p\mathbb{Z}} x_2^{i_2}\cdots\sum_{x_n\in\mathbb{Z}/p\mathbb{Z}} x_n^{i_n}\\ &\equiv 0 \pmod{p}\end{aligned}$$

Isso mostra que $\sum_{(x_1,\ldots,x_n)\in(\mathbb{Z}/p\mathbb{Z})^n} g(x_1, \ldots, x_n) \equiv 0 \pmod{p}$ e, portanto, $|A|$ é múltiplo de p. Como $(\overline{0}, \overline{0}, \ldots, \overline{0}) \in A$, há pelo menos $p-1$ outros pontos nesse conjunto, o que prova o teorema.

□

Como aplicação, provemos o seguinte resultado, devido a Erdős, Ginzburg e Ziv.

Proposição 5. *Seja n um inteiro positivo. Dados inteiros $x_1, \ldots, x_{2n-1}$ existem $1 \leq i_1 < i_2 < \cdots < i_n \leq 2n-1$ tais que $x_{i_1}+x_{i_2}+\cdots+x_{i_n}$ é divisível por n.*

Demonstração. Mostremos primeiro que se o resultado vale para m e para n então vale para mn. Sejam $x_1, x_2, \ldots, x_{2mn-1} \in \mathbb{Z}$. Por hipótese temos que, para cada subconjunto A de $\{1, 2, \ldots, 2mn-1\}$ com $2n-1$ elementos, existe um subconjunto $B \subset A$ com n elementos tal que $\sum_{i\in B} x_i$ é divisível por n. Assim, construímos B_j indutivamente para todo $1 \leq j \leq 2m-1$, seguindo os seguintes passos

- Escolhemos um subconjunto A_j de $\{1, 2, \ldots, 2mn-1\} \setminus \bigcup_{k<j} B_k$ com $2n-1$ elementos.
- De A_j escolhemos um subconjunto B_j com n elementos tal que $\sum_{i\in B_j} x_i$ é divisível por n.

Observemos que se $j \leq 2m-1$ então

$$\begin{aligned}\left|\{1, 2, \ldots, 2mn-1\} \setminus \bigcup_{k<j} B_j\right| &= 2mn-1-(j-1)n\\ &\geq 2mn-1-(2m-2)n = 2n-1,\end{aligned}$$

o que garante a construção até $j = 2m-1$. Definamos agora os inteiros $y_j = \frac{1}{n}\sum_{i\in B_j} x_i$ para $1 \leq j \leq 2m-1$. De novo por hipótese, existe um subconjunto

de índices $C \subset \{1, \ldots, 2m-1\}$ com m elementos tal que $\sum_{j \in C} y_j$ é divisível por m e portanto

$$\sum_{j \in C} \sum_{i \in B_j} x_i = n \sum_{j \in C} y_j$$

é uma soma com $|C||B_j| = mn$ somandos que é divisível por mn.

Assim, basta provar a proposição para n primo. Para isso, consideremos os polinômios

$$f_1(x_1, \ldots, x_{2n-1}) = x_1^{n-1} + x_2^{n-1} + \cdots + x_{2n-1}^{n-1} \qquad \text{e}$$
$$f_2(x_1, \ldots, x_{2n-1}) = a_1 x_1^{n-1} + a_2 x_2^{n-1} + \cdots + a_{2n-1} x_{2n-1}^{n-1}$$

onde $a_1, \ldots, a_{2n-1}$ são os inteiros dados. A soma dos graus de f_1 e f_2 é $2(n-1) < 2n-1$. Pelo teorema de Chevalley-Warning, existem $x_1, \ldots, x_{2n-1} \in \mathbb{Z}/(n)$ não todos nulos com

$$f_1(x_1, \ldots, x_{2n-1}) \equiv f_2(x_1, \ldots, x_{2n-1}) \equiv 0 \pmod{n}.$$

Como $x^{n-1} \equiv 1 \pmod{n}$ para todo $x \in (\mathbb{Z}/(n))^\times$, $f_1(x_1, \ldots, x_{2n-1}) \equiv 0 \pmod{n}$ implica que existem exatamente n valores $i \leq 2n-1$ com $x_i \not\equiv 0 \pmod{n}$. Sejam $1 \leq i_1 < i_2 < \cdots < i_n \leq 2n-1$ tais valores de i, como $x_{i_s}^{n-1} \equiv 1 \pmod{n}$ para todo $s \leq n$ temos que

$$a_1 x_1^{n-1} + a_2 x_2^{n-1} + \cdots + a_{2n-1} x_{2n-1}^{n-1} \equiv a_{i_1} + a_{i_2} + \cdots + a_{i_n} \pmod{n},$$

pois $x_j \equiv 0 \pmod{n}$ se $j \neq i_s$ para todo $s \leq n$. Assim, $a_{i_1} + a_{i_2} + \cdots + a_{i_n}$ é divisível por n, o que prova o resultado. □

Problemas Propostos

Problema 6 (OBM2007). *Para quantos inteiros c, $-2007 \leq c \leq 2007$, existe um inteiro x tal que $x^2 + c$ é múltiplo de 2^{2007}?*

Problema 7. *Seja p um primo e seja n tal que $p^k \nmid n$. Demonstrar: se a equação $y^n \equiv a \pmod{p^k}$ tem solução com $\mathrm{mdc}(y, p) = 1$, então para todo $m > k$ a equação $y^n \equiv a \pmod{p^m}$ possui solução.*

Problema 8. *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio, p um número primo, a um inteiro tal que $f(a) \equiv 0 \pmod{p}$ mas $f'(a) \not\equiv 0 \pmod{p}$ e k um inteiro positivo. Prove que, se a_k é um inteiro tal que $a_k \equiv a \pmod{p}$ e $f(a_k) \equiv 0 \pmod{p^k}$, então, tomando b tal que $b \equiv a_k - f(a_k) \cdot f'(a_k)^{-1} \pmod{p^{2k}}$, então $f(b) \equiv 0 \pmod{p^{2k}}$.*

Problema 9. *Seja p um primo ímpar, a um inteiro e n um inteiro positivo. Sejam α e β inteiros não negativos, com $\alpha > 0$. Prove:*

(a) Se p^β e p^α são as maiores potências de p que dividem n e $a-1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência de p que divide $a^n - 1$ (atenção, p deve dividir $a-1$ pois $\alpha > 0$! Mas note que p não precisa dividir n)

(b) Se n é ímpar e p^β e p^α são as maiores potências de p que dividem n e $a+1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência de p que divide a^n+1 (mesma ressalva do item (i)).

Problema 10. *Sejam a um inteiro e n um inteiro positivo. Sejam α e β inteiros não negativos, com $\alpha, \beta > 0$. Prove:*

(a) Se n é ímpar e 2^α é a maior potência de 2 que divide $a-1$ então 2^α é também a maior potência de 2 que divide a^n-1.

(b) Se $a \equiv 1 \pmod 4$ e 2^β e 2^α são as maiores potências de 2 que dividem n e $a-1$ respectivamente então $2^{\alpha+\beta}$ é a maior potência de 2 que divide a^n-1.

(c) Se $a \equiv 3 \pmod 4$ e 2^β e 2^α são as maiores potências de 2 que dividem n e $a+1$ respectivamente então $2^{\alpha+\beta}$ é a maior potência de 2 que divide a^n-1.

(d) Se n é ímpar e 2^α é a maior potência de 2 que divide $a+1$ então 2^α é também a maior potência de 2 que divide a^n+1.

Problema 11. *Encontre todos os inteiros não negativos x e y tais que*

$$7^y - 2 \cdot 3^x = 1$$

Problema 12. *Seja p um número primo e n, k e $a = p^t a_1$ números naturais tais que $\mathrm{mdc}(p, a_1) = 1$. Prove: a congruência $x^n \equiv a \pmod{p^k}$ tem solução se, e só se, $k \leq t$ ou*

$$k > t, \quad n \mid t \quad e \quad a_1^{\frac{p^{k-1}(p-1)}{\mathrm{mdc}(n, p^{k-1}(p-1))}} \equiv 1 \pmod{p^{k-t}}.$$

Problema 13 (Irlanda 1997)**.** *Seja A um subconjunto de $\{1, 2, \ldots 2n-1\}$ com n elementos. Prove que A contém uma potência de 2 ou dois elementos distintos cuja soma é uma potência de 2.*

Problema 14 (Romênia 1996)**.** *Determinar o maior inteiro positivo n com a seguinte propriedade: existem inteiros não negativos $x_1, \ldots, x_n$ tais que, para toda sequência $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ de elementos de $\{-1, 0, 1\}$, não todos zero, o número*

$$\epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_n x_n$$

não é divisível por n^3.

Problema 15 (Erdős)**.** *Mostrar que todo número inteiro positivo pode ser expresso como soma de números da forma $2^a 3^b$ de modo que nenhum termo é divisível por outro.*

Problema 16 (Romênia 1998)**.** *Mostrar que para todo $n \geq 2$ existe um subconjunto S de $\{1, 2, \ldots, n\}$ com no máximo $2\lfloor\sqrt{n}\rfloor + 1$ elementos tal que todo número natural menor do que n pode ser representado como diferença de dois elementos de S.*

Dicas e Soluções

Em breve.

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.