Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 8

Equações lineares módulo n e o teorema chinês dos restos

1 Equações Lineares Módulo m

Se $\operatorname{mdc}(a, m) = 1$, como a é invertível módulo m, a equação

$$ax \equiv b \pmod{m},$$

tem solução única módulo m, dada por $x \equiv a^{\varphi(m)-1}b \pmod{m}$ (utilizando o teorema de Euler-Fermat para encontrar o inverso de $\overline{a} \in \mathbb{Z}/(m)$). Assim, todas as soluções da equação acima são da forma $x = a^{\varphi(m)-1}b + km$ onde $k \in \mathbb{Z}$. No caso geral, se $\operatorname{mdc}(a, m) = d > 1$ temos que

$$ax \equiv b \pmod{m} \implies ax \equiv b \pmod{d} \iff b \equiv 0 \pmod{d}.$$

Logo uma condição necessária para que a congruência linear $ax \equiv b \pmod{m}$ tenha solução é que $d \mid b$. Esta condição é também suficiente, já que escrevendo $a = da'$, $b = db'$ e $m = dm'$, temos que

$$ax \equiv b \pmod{m} \iff a'x \equiv b' \pmod{m'}.$$

Como $\operatorname{mdc}(a', m') = 1$, há uma única solução $(a')^{\varphi(m')-1}b'$ módulo m', isto é, há d soluções distintas módulo m, a saber $x \equiv (a')^{\varphi(m')-1}b' + km' \pmod{m}$ com $0 \le k < d$. Note ainda que como resolver $ax \equiv b \pmod{m}$ é equivalente a resolver a equação diofantina linear $ax + my = b$, poderíamos também ter utilizado o teorema de Bachet-Bézout e o algoritmo de Euclides para encontrar as soluções desta congruência linear como no exemplo **??**. Resumimos esta discussão na seguinte

Proposição 1. *A congruência linear*

$$ax \equiv b \pmod{m}$$

admite solução se, e somente se, $\operatorname{mdc}(a, m) \mid b$. *Neste caso, há exatamente* $\operatorname{mdc}(a, m)$ *soluções distintas módulo* m.

Agora queremos encontrar condições para que um sistema de congruências lineares tenha solução. O seguinte teorema nos garante a existência de tais soluções.

Teorema 2 (Teorema Chinês dos Restos)**.** *Se $b_1, b_2, \ldots, b_k$ são inteiros quaisquer e $a_1, a_2, \ldots, a_k$ são primos relativos dois a dois, o sistema de equações*

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

admite solução, que é única módulo $A = a_1 a_2 \ldots a_k$.

Demonstração. Daremos duas provas do teorema chinês dos restos. Para a primeira, consideremos os números $M_i = \frac{A}{a_i}$. Como $\mathrm{mdc}(a_i, M_i) = 1$, logo existe X_i tal que $M_i X_i \equiv 1 \pmod{a_i}$. Note que se $j \neq i$ então M_j é múltiplo de a_i e portanto $M_j X_j \equiv 0 \pmod{a_i}$. Assim, temos que

$$x_0 = M_1 X_1 b_1 + M_2 X_2 b_2 + \cdots + M_k X_k b_k$$

é solução do sistema de equações, pois $x_0 \equiv M_i X_i b_i \equiv b_i \pmod{a_i}$. Além disso, se x_1 é outra solução, então $x_0 \equiv x_1 \pmod{a_i} \iff a_i \mid x_0 - x_1$ para todo a_i, e como os a_i's são dois a dois primos, temos que $A \mid x_0 - x_1 \iff x_0 \equiv x_1 \pmod{A}$, mostrando a unicidade módulo A.

Para a segunda prova, considere o mapa natural

$$\begin{aligned} f \colon \mathbb{Z}/(A) &\to \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_k) \\ b \bmod A &\mapsto (b \bmod a_1, b \bmod a_2, \ldots, b \bmod a_k). \end{aligned}$$

Note que este mapa está bem definido, isto é, o valor de $f(b \bmod A)$ independe da escolha do representante da classe de $b \bmod A$, pois quaisquer dois representantes diferem de um múltiplo de A, que tem imagem $(0 \bmod a_1, \ldots, 0 \bmod a_k)$ no produto $\mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_k)$. Observemos agora que o teorema chinês dos restos é equivalente a mostrar que f é uma bijeção: o fato de f ser sobrejetor corresponde à existência da solução do sistema, enquanto que o fato de f ser injetor corresponde à unicidade módulo A. Como o domínio e o contradomínio de f têm mesmo tamanho (ambos têm A elementos), para mostrar que f é uma bijeção basta mostrarmos que f é injetora. Suponha que $f(b_1 \bmod A) = f(b_2 \bmod A)$, então $b_1 \equiv b_2 \pmod{a_i}$ para todo i, e como na primeira demonstração temos que isto implica $b_1 \equiv b_2 \pmod{A}$, o que encerra a prova. $\square$

Observação 3. *Como* $\mathrm{mdc}(b, a_1 a_2 \ldots a_k) = 1 \iff \mathrm{mdc}(b, a_j) = 1, \forall j \leq k$, *a bijeção f definida na segunda prova do teorema anterior satisfaz $f((\mathbb{Z}/(A))^\times) = (\mathbb{Z}/(a_1))^\times \times (\mathbb{Z}/(a_2))^\times \times \cdots \times (\mathbb{Z}/(a_k))^\times$.*

Em particular, isso nos dá uma nova prova de que
$\varphi(a_1 a_2 \ldots a_k) = \varphi(a_1)\varphi(a_2)\ldots\varphi(a_k)$ *sempre que* $\mathrm{mdc}(a_i, a_j) = 1, \forall i \neq j$.

Por exemplo, para $k = 2$, $a_1 = 3$ e $a_2 = 5$, temos a seguinte tabela, que mostra, para cada i e j com $0 \leq i < 3$ e $0 \leq j < 5$, a única solução x com $0 \leq x < 3 \cdot 5 = 15$ tal que $x \equiv i \pmod 3$ e $x \equiv j \pmod 5$:

	0 mod 5	1 mod 5	2 mod 5	3 mod 5	4 mod 5
0 mod 3	0	6	12	3	9
1 mod 3	10	1	7	13	4
2 mod 3	5	11	2	8	14

Vejamos algumas aplicações.

Exemplo 4. *Um inteiro é* livre de quadrados *se ele não é divisível pelo quadrado de nenhum número inteiro maior do que 1. Demonstrar que existem intervalos arbitrariamente grandes de inteiros consecutivos, nenhum dos quais é livre de quadrados.*

Solução: Seja n um número natural qualquer. Sejam $p_1, \ldots, p_n$ primos distintos. O teorema chinês dos restos nos garante que o sistema

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2} \\ x &\equiv -2 \pmod{p_2^2} \\ &\vdots \\ x &\equiv -n \pmod{p_n^2} \end{aligned}$$

tem solução. Se x_0 é uma solução positiva do sistema, então cada um dos números $x_0+1, x_0+2, \ldots, x_0+n$ é divisível pelo quadrado de um inteiro maior do que 1, logo nenhum deles é livre de quadrados. $\square$

Exemplo 5. *Seja $P(x)$ um polinômio não constante com coeficientes inteiros. Demonstrar que para todo inteiro n, existe um inteiro i tal que*

$$P(i), P(i+1), P(i+2), \ldots, P(i+n)$$

são números compostos.

Solução: Demonstraremos primeiro o seguinte

Lema 6. *Seja $P(x)$ um polinômio não constante com coeficientes inteiros. Para todo par de inteiros k, i, tem-se que $P(i) \mid P(k\,P(i) + i)$.*

Demonstração. Dado que $(kP(i)+i)^n \equiv i^n \pmod{P(i)}$ para todo n inteiro não negativo, é fácil ver que $P(kP(i)+i) \equiv P(i) \equiv 0 \pmod{P(i)}$. $\square$

Suponhamos por contradição que a sequência $P(i), P(i+1), \ldots, P(i+n)$ contém um número primo para cada i. Então a sequência $\{P(i)\}_{i \geq 1}$ assume infinitos valores primos. Consideremos os $n+1$ primos distintos $P(i_0), P(i_1), \ldots, P(i_n)$.

Pelo teorema chinês dos restos segue que existem infinitas soluções x do sistema de equações

$$\begin{aligned} x &\equiv i_0 \pmod{P(i_0)} \\ x &\equiv i_1 - 1 \pmod{P(i_1)} \\ x &\equiv i_2 - 2 \pmod{P(i_2)} \\ &\vdots \\ x &\equiv i_n - n \pmod{P(i_n)} \end{aligned}$$

onde, se x_0 é uma solução, então $x = x_0 + k(P(i_0) \cdots P(i_n))$ também é solução para todo $k \geq 0$. Assim, pelo lema anterior, podemos dizer que $P(x), P(x+1), \dots, P(x+n)$ são números compostos quando k é suficientemente grande, múltiplos respectivamente de $P(i_0), P(i_1), \dots, P(i_n)$. $\square$

Exemplo 7. *Uma* potência não trivial *é um número da forma m^k, onde m, k são inteiros maiores do que ou iguais a 2. Dado $n \in \mathbb{N}$, prove que existe um conjunto $A \subset \mathbb{N}$ com n elementos tal que para todo subconjunto $B \subset A$ não vazio, $\sum\limits_{x \in B} x$ é uma potência não trivial. Em outras palavras, se $A = \{x_1, x_2, \dots, x_n\}$ então todas as somas $x_1, x_2, \dots, x_n$, $x_1+x_2, x_1+x_3, \dots, x_{n-1}+x_n$, $\dots$, $x_1+x_2+\cdots+x_n$ são potências não triviais.*

Solução: Vamos provar a existência de um tal conjunto por indução em n. Para $n = 1$, $A = \{4\}$ é solução e, para $n = 2$, $A = \{9, 16\}$ é solução. Suponha agora que $A = \{x_1, \dots, x_n\}$ é um conjunto com n elementos e para todo $B \subset A$, $B \neq \emptyset$, $\sum\limits_{x \in B} x = m_B^{k_B}$. Vamos mostrar que existe $c \in \mathbb{N}$ tal que o conjunto $\tilde{A} = \{cx_1, cx_2, \dots, cx_n, c\}$ satisfaz o enunciado. Seja $\lambda = \text{mmc}\{k_B \mid B \subset A, B \neq \emptyset\}$, o mínimo múltiplo comum de todos os expoentes k_B. Para cada $B \subset A$, $B \neq \emptyset$, associamos um número primo $p_B > \lambda$, de forma que $B_1 \neq B_2$ implica $p_{B_1} \neq p_{B_2}$. Pelo teorema chinês dos restos existe um natural r_B com

$$\begin{aligned} r_B &\equiv 0 \pmod{p_X} \text{ para todo subconjunto } X \subset A,\ X \neq B \\ \lambda \cdot r_B &\equiv -1 \pmod{p_B}. \end{aligned}$$

(λ é invertível módulo p_B). Tomemos

$$c = \prod_{\substack{X \subset A \\ X \neq \emptyset}} (1 + m_X^{k_X})^{\lambda r_X}$$

e vamos mostrar que $\tilde{A} = \{cx_1, cx_2, \dots, cx_n, c\}$ continua a satisfazer as condições do enunciado.

Dado $B' \subset \{cx_1, cx_2, \dots, cx_n\}$, temos que $B' = \{cx \mid x \in B\}$ para algum $B \subset A$. Como c é uma potência λ-ésima, c também é uma potência k_B-ésima, portanto, $\sum_{x \in B'} x = cm_B^{k_B}$ será uma potência k_B-ésima para todo $B' \neq \emptyset$. Além disso, para subconjuntos de $\tilde{A}$ da forma $B' \cup \{c\}$, temos

$$\sum_{x \in B' \cup \{c\}} x = c \cdot (1 + m_B^{k_B}) = \Big(\prod_{\substack{X \subset A \\ X \neq \emptyset, B}} (1 + m_X^{k_X})^{\lambda r_X} \Big) (1 + m_B^{k_B})^{\lambda r_B + 1},$$

que é uma potência p_B-ésima, pois $\lambda r_B + 1$ e r_X $(X \neq B)$ são múltiplos de p_B. □

Problemas Propostos

Problema 8. *Resolver as equações lineares*

(a) $7x \equiv 12 \pmod{127}$

(b) $12x \equiv 5 \pmod{122}$

(c) $40x \equiv 64 \pmod{256}$

Problema 9. *Resolver o sistema de congruências lineares*

$$\begin{aligned} x &\equiv 0 \pmod{7} \\ x &\equiv 1 \pmod{12} \\ x &\equiv -5 \pmod{17} \end{aligned}$$

Problema 10. *Determine um valor de* s *tal que* $1024s \equiv 1 \pmod{2011}$ *e calcule o resto da divisão de* 2^{2000} *por* 2011.

Problema 11. *Um inteiro positivo* n *é chamado de* auto-replicante *se os últimos dígitos de* n^2 *formam o número* n. *Por exemplo,* 25 *é auto-replicante pois* $25^2 = 625$. *Determine todos os números auto-replicantes com exatamente 4 dígitos.*

Problema 12. *Sejam* $a, n \in \mathbb{N}_{>0}$ *e considere a sequência* (x_k) *definida por* $x_1 = a$, $x_{k+1} = a^{x_k}$ *para todo* $k \in \mathbb{N}$. *Demonstrar que existe* $N \in \mathbb{N}$ *tal que* $x_{k+1} \equiv x_k \pmod{n}$ *para todo* $k \geq N$.

Problema 13. *Demonstrar que o sistema de equações*

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

tem solução se, e só se, para todo i *e* j, $\mathrm{mdc}(a_i, a_j) \mid (b_i - b_j)$. *(No caso particular em que* $\mathrm{mdc}(a_i, a_j) = 1$, *o problema se reduz ao teorema chinês dos restos).*

Problema 14. *Demonstrar que, para* k *e* n *números naturais, é possível encontrar* k *números consecutivos, cada um dos quais tem ao menos* n *divisores primos diferentes.*

Problema 15. *Demonstrar que se a, b e c são três inteiros diferentes, então existem infinitos valores de n para os quais $a+n$, $b+n$ e $c+n$ são primos relativos.*

Problema 16. *Demonstrar que para todo inteiro positivo m e todo número par $2k$, este último pode ser escrito como a diferença de dois inteiros positivos, cada um dos quais é primo relativo com m.*

Problema 17. *Demonstrar que existem progressões aritméticas de comprimento arbitrário formadas por inteiros positivos tais que cada termo é a potência de um inteiro positivo com expoente maior do que* 1.

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.