Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 11

O Teorema Chinês dos Restos

Iremos estudar um antigo teorema descoberto pelos chineses no início século $XIII$. Comecemos recordando um lema da aula 06:

Lema 1. *Se $mdc(a, m) = 1$, então existe um inteiro x tal que:*

$$ax \equiv 1 \pmod{m}.$$

Tal inteiro é único módulo m. Se $mdc(a, m) > 1$, não existe x satisfazendo tal equação.

Demonstração. Pelo teorema de Bachet-Bézout, existem inteiros x e y tais que $ax+my = 1$. Analisando essa congruência módulo m, obtemos $ax \equiv 1 \pmod{m}$. Se y é outro inteiro que satisfaz a mesma congruência, temos $ax \equiv ay \pmod{m}$. Pelo primeiro lema, $x \equiv y \pmod{m}$. Se $d = mdc(a, m) > 1$, não podemos ter $d \mid m$ e $m \mid ax - 1$ pois $d \nmid ax - 1$.

Exemplo 2. *Encontre x inteiro tal que:*

$$\begin{aligned} x &\equiv 1 \pmod{11}; \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

A primeira congruência nos diz que $x = 11k+1$ para algum $k \in \mathbb{Z}$. Sejam q e r o quociente e o resto da divisão de k por 7, respectivamente. Assim, $k = 7q + r$ e $x = 77q + 11r + 1$. Para x satisfazer a segunda congruência, devemos encontrar $r \in \{0, 1, 2, 3, 4, 5, 6\}$ tal que $11r + 1 \equiv 2 \pmod{7}$, ou seja, $4r \equiv 1 \pmod{7}$. Como o inverso de 4 (mod 7) é 2, obtemos $r = 2$ e $x = 77q + 23$. Veja que para qualquer q inteiro, tal x é solução do sistema de congruências.

Exemplo 3. *Encontre x inteiro tal que:*

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

Pelo exemplo anterior, para x satisfazer as duas primeiras equações, devemos ter $x = 77q+23$. Dividindo q por 5, obtemos $q = 5l+s$ com $0 \leq s < 5$. Daí, $x = 385l+77s+23$. Para satisfazer a última congruência, devemos ter $77s + 23 \equiv 4 \pmod 5$, ou seja, $2s \equiv 1 \pmod 5$. Como 3 é o inverso de 2 (mod 5), $s = 3$ e consequentemente $x = 385l + 254$.

Perceba que nos dois exemplos anteriores, o problema foi reduzido à encontrarmos o inverso de um inteiro. No último exemplo, a solução geral possui a forma: $x = 11 \cdot 7 \cdot 5l+231+22+1$. Essencialmente, o trabalho de encontrar esses inversos foi possível pois os inteiros 5, 7 e 11 são primos entre si dois a dois.

Veremos agora um mecanismo levemente diferente para resolver tais sistemas equações.

Teorema 4. *(***Teorema Chinês dos Restos***) Sejam $m_1, m_2, \ldots, m_r$, inteiros positivos primos entre si, dois a dois, e sejam $a_1, a_2, \ldots, a_r$; r inteiros quaisquer. Então, o sistema de conguências:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

admite uma solução x. Além disso, as soluções são únicas módulo $m = m_1 m_2 \ldots m_r$.

Demonstração. Escrevendo $m = m_1 m_2 \ldots m_r$, vemos que $\dfrac{m}{m_j}$ é um inteiro e $mdc\left(\dfrac{m}{m_j}, m_j\right) = 1$. Então, pelo lema inicial, para cada j, existe um inteiro b_j tal que $\left(\dfrac{m}{m_j}\right) b_j \equiv 1 \pmod{m_j}$. Claramente $\left(\dfrac{m}{m_j}\right) b_j \equiv 0 \pmod{m_i}$ para $i \neq j$. Definamos

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \ldots + \frac{m}{m_r} b_r a_r$$

Consideremos x_0 módulo m_i: $x_0 \equiv \dfrac{m}{m_i} b_j a_j \equiv a_i \pmod{m_i}$. Logo, x_0 é uma solução do nosso sistema. Se x_0 e x_1 também o são, podemos escrever $x_0 \equiv x_1 \pmod{m_i}$ para cada i. Como $mdc(m_i, m_j) = 1$, para $i \neq j$, pbtemos $x_0 \equiv x_1 \pmod m$.

Observação 5. *Se cada uma das equações do sistema anterior fosse do tipo $b_i x \equiv a_i \pmod m)_i$, com $mdc(b_i, m) = 1$, ainda poderíamos usá-lo. Bastaria reescrever $b_i x \equiv a_i \pmod m)_i$ como $x \equiv \overline{b_i} a_i \pmod m)_i$, onde $\overline{b_i}$ é o inverso de $b_i \pmod m)_i$.*

Exemplo 6. *Encontre o menor inteiro positivo x tal que $x \equiv 5 \pmod 7$, $x \equiv 7 \pmod{11}$ e $x \equiv 3 \pmod{13}$.*

Usando o teorema anterior com $m_1 = 5, m_2 = 7, m_3 = 11, a_1 = 5, a_2 = 7$ *e* $a_3 = 3$ podemos achar $x \equiv 887 \pmod{1001} = 7.11.13$. Como a solução é única módulo m, isso significa que, dentre os números $1, 2, \cdots, 1001$ a menor solução positiva é 887.

Exemplo 7. *(OBM 2009) Sejam m e n dois inteiros positivos primos entre si. O Teorema Chinês dos Restos afirma que, dados inteiros i e j com $0 \leq i < m$ e $o \leq j < n$, existe exatamente um inteiro a, com $0 \leq a < mn$, tal que o resto da divisão de a por m é igual a i e o resto da divisão de a por n é igual a j. Por exemplo, para $m = 3$ e $n = 7$, temos que 19 é o único número que deixa restos 1 e 5 quando dividido por 3 e 7, respectivamente. Assim, na tabela a seguir, cada número de 0 a 20 aparecerá exatamente uma vez.*

	0	*1*	*2*	*3*	*4*	*5*	*6*
0		A				B	
1				C			D
2		E			F		

Qual a soma dos números das casas com as letras A, B, C, D, E e F?

Usando o teorema chinês dos restos, podemos encontrar $A = 15, B = 12, C = 10, D = 13, E = 8$ e $F = 11$. Assim, $A + B + C + D + E + F = 69$.

Exemplo 8. *(Estônia 2000) Determine todos os restos possíveis da divisão do quadrado de um número primo com 120 por 120.*

Seja n tal que $mdc(n, 120) = 1$. Como $120 = 3 \cdot 5 \cdot 8$, temos que $n \not\equiv 0 \pmod 3$, $\pmod 5$ $\pmod 2$. Daí, $n^2 \equiv 1 \pmod 3$, $n^2 \equiv 1 \pmod 8$ e $n^2 \equiv 1$ ou $4 \pmod 5$. Sendo assim, n^2 satisfaz o sistema:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 8 \\ x &\equiv \pm 1 \pmod 5 \end{aligned}$$

cujas soluções são $x \equiv 1 \pmod{120}$ e $x \equiv 49 \pmod{120}$.

Aconselhamos ao leitor a resolução de alguns exemplos numéricos até adquirir prática com o algoritmo usado para encontrar x_0. Provamos, no teorema passado, que todas as soluções daquele sistema de congruências são os termos de uma $P.A$ de razão m. Geralmente usaremos aquele teorema apenas para garantir que um sistema de congruências admite uma solução. Os próximos exemplos podem deixar isso mais claro.

Exemplo 9. *Para cada número natural n, existe uma sequência arbitrariamente longa de números natu rais consecutivos, cada um deles sendo divisível por uma s-ésima potência de um número natural maior que 1.*

Demonstração. Dado $m \in \mathbb{N}$, considere o conjunto $\{p_1, p_2, \ldots, p_m\}$ de primos distintos. Como $mdc(p_i^s, p_j^s) = 1$, então pelo teorema 3, existe x tal que $x \equiv -i \pmod{p_i^s}$ para $i = 1, 2, \ldots m$. Cada um dos números do conjunto $\{x + 1, x + 2, \ldots, x + m\}$ é divisível por um número da forma p_i^s.

Exemplo 10. *(USAMO 1986)*

(a) Existem 14 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 11$?

(b) Existem 21 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 13$?

Demonstração. (a) Não. Suponha que existam tais inteiros. Da nossa lista de 14 inteiros consecutivos, 7 são números pares. Vamos observar os ímpares: $a, a+2, a+4, a+6, a+8, a+10$ e $a+12$. Podemos ter no máximo três deles divisíveis por 3, dois por 5, um por 7 e um por 11. Veja que $3+2+1+1=7$. Pelo Princípio da Casa dos Pombos, cada um desses ímpares é divisível por exatamente um primo do conjunto $\{3,5,7,11\}$. Além disso, note que os múltiplos de 3 só podem ser $\{a, a+6, a+12\}$. Dois dos números restantes em $(a+2, a+4, a+8,$ e $a+10)$ são divisíveis por 5. Mas isso é impossível. (b) Sim. Como os números $\{210, 11, 13\}$ são primos entre si, dois a dois, pelo teorema 3 existe um inteiro positivo $n > 10$ tal que:

$$\begin{aligned} n &\equiv 0(\bmod 210 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot) \\ n &\equiv 1(\bmod 11) \\ n &\equiv -1(\bmod 13) \end{aligned}$$

Veja que o conjunto $\{n-10, n-9, \ldots, n+9, n+10\}$ satisfaz as condições do item (b).

Exemplo 11. *Sejam a e b inteiros positivos tais que, para qualquer n natural, $a^n+n \mid b^n+n$. Prove que $a=b$.*

Seja p um primo maior que a e b. Então $mdc(p,a) = mdc(p,b) = 1$. Como $mdc(p, p-1) = 1$, existe um inteiro positivo n tal que $n \equiv 1 \pmod{p-1}$ e $n \equiv -a \pmod{p}$. Pelo teorema de Fermat, $a^n + n \equiv 0 \pmod{\ }$ e $b^n + n \equiv b - a \pmod{p}$. Assim, $p \mid |b-a|$. Como $|b-a| < p$, segue que $|b-a| = 0$ e $a = b$.

Exemplo 12. *(Olimpíada Nórdica 1998)*

(a) Para quais inteiros positivos n existe um sequência $x_1, x_2, \ldots, x_n$ contendo cada um dos inteiros $1, 2, \ldots, n$ exatamente uma vez, e tal que k divide $x_1 + x_2 + \cdots + x_k$ para $k = 1, 2, \cdots, n$?

(b) Existe uma sequência infinita $x_1, x_2, \ldots$ contendo todo inteiro positivo exatamente uma vez, e tal que para cada inteiro positivo k, k divide $x_1 + x_2 + \cdots + x_k$?

a) Suponha que n é um inteiro que satisfaz o enunciado. Naturalmente n divide a soma:

$$x_1 + x_2 + \ldots x_n = \frac{n(n+1)}{2}.$$

Daí, $\dfrac{n+1}{2}$ é um inteiro e n deve ser ímpar. Seja $m = \dfrac{n+1}{2}$. Usando que

$$(n-1) \mid x_1 + x_2 + \ldots x_{n-1} = mn - x_n,$$

temos $x_n \equiv m \pmod{n-1}$ se $n \geq 3$ e, consequentemente, $x_n = m$. Repetindo a mesma análise para $n-2$ no lugar de $n-1$, obtemos $x_{n-1} = m$ para $n \geq 5$. Como não podem existir dois termos iguais, temos um absurdo. Analisando os casos quando $n \leq 4$, encontramos $n = 1$ e $n = 3$ como únicas soluções.

b) Iremos construir a sequência indutivamente. Suponha que já tenhamos definido os termos $x_1, x_2, \ldots, x_n$ satisfazendo a condição $k \mid x_1 + x_2 \ldots x_k$ para todo $k \leq n$. Seja m o menor inteiro positivo que ainda não apareceu na sequência. Pelo Teorema Chinês dos Restos, existe x tal que $x \equiv -(x_1 + x_2 + \ldots + x_n) \pmod{n+1}$ e $x \equiv -(x_1 + x_2 + \ldots + x_n) - m \pmod{n+2}$. Escolha l, inteiro positivo, tal que $l > x_1, x_2, \ldots, x_n, m$ e $l \equiv x \pmod{(n+1)(n+2)}$. Defina $x_{n+1} = l$ e $x_{n+2} = m$. Veja que a condição $k \mid x_1 + x_2 \ldots x_k$ agora é verdadeira para todo $k \leq n+2$. Para o início, basta definir $x_1 = 1$.

Exemplo 13. *(Olimpíada de São Petesburgo 1990) Dado um polinômio $F(x)$ com coeficientes inteiros, tal que, para cada inteiro n, o valor de $F(n)$ é divisível por pelo menos um dos inteiros $a_1, a_2, \cdots, a_m$. Prove que podemos encontrar um índice k tal que $F(n)$ é divisível por a_k para cada inteiro positivo n.*

Demonstração. Suponha que não exista tal índice. Para cada índice k ($k = 1, 2, \ldots, m$), existe um inteiro x_k tal que $F(x_k)$ não é divisível por a_k. Assim, existem números $d_k = p_k^{\alpha_k}$(onde p_k são números primos), tais que d_k divide a_k mas não divide $F(x_k)$. Se existem potências do mesmo primo entre esses números, podemos apagar aquelas repetidas deixando apenas uma que tem expoente mínimo. Caso $F(x)$ não seja divisível por uma potência apagada, não será pela potência que tem expoente mínimo. Essas deleções garatem que nossa nova coleção $d_1, d_2, \ldots, d_j$ de potências de primos contenham apenas inteiros primos entre si, dois a dois. Pelo teorema chinês dos restos, exite um inteiro N tal que $N \equiv x_k \pmod{d}_k$, para $k \in \{1, 2, \ldots, j\}$. Suponhamos que $d_k \mid F(N)$. Sabemos que $x - y \mid F(x) - F(y)$ e consequentemente $N - x_k \mid F(N) - F(x_k)$. Como $d_k \mid N - x_k$, devemos ter $d_k \mid F(x_k)$. Uma contradição! Logo, $F(N)$ não é divisível por nenhum d_k e isso contradiz a hipótese sobre os a_i.

Problemas Propostos

Problema 14. *Encontre o menor inteiro positivo (com a exceção de $x = 1$) que satisfaça o seguinte sistema de congruências:*

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{7} \end{aligned}$$

Problema 15. *Encontre todas as soluções do sistema:*

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 2 \end{aligned}$$

Problema 16. *Encontre todos os inteiros que deixam restos* $1, 2$ *e* 3 *quando divididos por* $3, 4$ *e* 5*, respectivamente.*

Problema 17. *Encontre todas as soluções do sistema:*

$$\begin{aligned} 3x &\equiv 1 \pmod 4 \\ 2x &\equiv 1 \pmod 3 \\ 4x &\equiv 5 \pmod 7 \end{aligned}$$

Problema 18. *Encontre todas as soluções das congruências:*

a) $20x \equiv 4 \pmod{30}$.

b) $20x \equiv 30 \pmod 4$.

c) $353x \equiv 254 \pmod{400}$.

Problema 19. *Se* a *é escolhido ao acaso no conjunto* $\{1, 2, 3, \ldots, 14\}$ *e* b *é escolhido ao acaso no conjunto* $\{1, 2, \ldots, 15\}$*, qual a probabilidade de que a equação* $ax \equiv b \pmod{15}$ *possua pelo menos uma solução?*

Problema 20. *Sejam* a *e* b *inteiros tais que* $mdc(a, b) = 1$ *e* $c > 0$*. Prove que existe um inteiro* x *tal que* $mdc(a + bx, c) = 1$.

Problema 21. *Existem* n *inteiros consecutivos tal que cada um contém um fator primo repetido* k *vezes?*

Problema 22. *Seja* n *um número natural arbitrário. Prove que existe um par de naturais* (a, b) *tais que* $mdc(a + r, b + s) > 1 \ \forall \ r, s = 1, 2, \ldots, n$.

Problema 23. *Um ponto* $(x, y) \in Z^2$ *é legal se* $mdc(x, y) = 1$*. Prove ou disprove: Dado um inteiro positivo* n*, existe um ponto* $(a, b) \in Z^2$ *cuja distância a todo ponto legal e pelo menos* n*?*

Problema 24. *Sejam* $m_o, m_1, ..., m_r$ *inteiros positivos que são primos entre si, dois a dois. Mostre que existem* $r+1$ *inteiros consecutivos* $s, s+1, ..., s+r$ *tal que* m_i *divide* $s+i$ *para* $i = 0, 1, ..., r$.

Problema 25. *(Romênia 1995) Seja* $f : \mathbb{N} - \{0, 1\} \to \mathbb{N}$ *definida por* $f(n) = mmc[1, 2, ..., n]$*. Prove que para todo* $n \geq 2$*, existem* n *números consecutivos para os quais* f *é constante.*

Problema 26. *(OBM 2005) Dados os inteiros positivos a, c e o inteiro b, prove que existe um inteiro positivo x tal que $a^x + x \equiv b \pmod{c}$.*

Problema 27. *(Cone Sul 2003) Demonstrar que existe uma sequência de inteiros positivos $x_1, x_2, \ldots$ que satisfaz as duas condições seguintes:*

(a) contém exatamente uma vez cada um dos inteiros positivos,

(b) a soma parcial $x_1 + x_2 + \ldots x_n$ é divisível por n^n.

Problema 28. *(República Tcheca e Eslovaca 1997) Mostre que existe uma sequência crescente $\{a_n\}_{n=1}^{\infty}$ de números naturais tais que para $k \geq 0$, a sequência $\{a_n + k\}$ contém um número finito de primos.*

Problema 29. *Considere o inteiro $c \geq 1$ e a sequência definida por $a_1 = c$ e $a_{i+1} = c^{a_i}$. Mostre que esta sequência se torna eventualmente constante quando a reduzimos módulo n para algum inteiro positivo n (isto significa que $a_m \equiv a_j \pmod{n}$ se $m \geq j$).*

Problema 30. *(Coréia 1999) Encontre todos os inteiros n tais que $2^n - 1$ é um múltiplo de 3 e $\dfrac{2^n - 1}{3}$ é um divisor de $4m^2 + 1$ para algum inteiro m.*

Problema 31. *(OBM 2006) Prove que, para todo inteiro $n \leq 2$, o número de matrizes quadradas 2×2 com entradas inteiras e pertencentes ao conjunto $\{0, 1, 2, \ldots, n-1\}$ que têm determinante da forma $kn + 1$ para algum k inteiro é dado por*

$$\prod_{\substack{p \text{ primo} \\ p \mid n}} \left(1 - \frac{1}{p^2}\right).$$

Problema 32. *Encontre todos os subconjuntos $S \subset \mathbb{Z}_+$ tais que todas as somas de uma quantidade finita de elementos de S(com possíveis repetições de elementos) são números compostos.*

Problema 33. *Existe algum natural n para o qual existem $n - 1$ progressões aritméticas com razões $2, 3, \ldots, n$ tais que qualquer natural está em pelo menos uma das progressões?*

Problema 34. *Seja $P(X)$ um polinômio com coeficientes inteiros e k é um inteior qualquer. Prove que existe um inteiro m tal que $P(m)$ tem pelo menos k fatores primos distintos.*

Acompanhe as dicussões dos problemas propostos no fórum do POTI:
www.poti.impa.br/forum/

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.

[2] E. Carneiro, O. Campos and F. Paiva, Olimpíadas Cearenses de Matemática 1981-2005 (Níveis Júnior e Senior), Ed. Realce, 2005.

[3] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, Treinamento Cone Sul 2008. Fortaleza, Ed. Realce, 2010.

[4] D. Fomin, A. Kirichenko, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, MA, 1994.

[5] D. Fomin, S. Genkin and I. Itenberg, Mathematical Circles, Mathematical Words, Vol. 7, American Mathematical Society, Boston, MA, 1966.

[6] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers.