Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 6

Congruências I

Definição 1. *Dizemos que os inteiros a e b são congrentes módulo m se eles deixam o mesmo resto quando divididos por m. Denotaremos isso por $a \equiv b \pmod{m}$.*

Por exemplo, $7 \equiv 2 \pmod{5}$, $9 \equiv 3 \pmod{6}$, $37 \equiv 7 \pmod{10}$ mas $5 \not\equiv 3 \pmod{4}$. Veja que $a \equiv b \pmod{m}$ se, e somente se, $m \mid a - b$.

Teorema 2. *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

i) $a + c \equiv b + d \pmod{m}$

ii) $a - c \equiv b - d \pmod{m}$

iii) $ka \equiv kb \pmod{m}$ $\forall k \in \mathbb{Z}$

iv) $ac \equiv bd \pmod{m}$

v) $a^k \equiv b^k \pmod{m}$ $\forall k \in \mathbb{N}$

vi) Se $mdc(k, m) = d$, então $ka \equiv kb \pmod{m} \Leftrightarrow a \equiv b \pmod{m/d}$

Demonstração. Sejam q_1 e q_2 tais que:

$$\begin{aligned} a - b &= q_1 m \\ c - d &= q_2 m \end{aligned}$$

Então, $(a + c) - (b + d) = (q_1 + q_2)m$. Logo, $a + c$ e $b + d$ deixam o mesmo resto por m e consequentemente $a + c \equiv b + d \pmod{m}$. Usando que $a - b \pmod{a}^k - b^k$ e que $m \mid a - b$, concluímos que $m \pmod{a}^k - b^k$. Os demais itens serão deixados para o leitor.

Em termos práticos, podemos realizar quase todas as operações elementares envolvendo igualdade de inteiros. Uma das diferenças cruciais é a operação de divisão como mostra o último item do teorema anterior.

Exemplo 3. *Calcule o resto de* 4^{100} *por 3.*

Como $4 \equiv 1 \pmod 3$, temos $4^{100} \equiv 1^{100} = 1 \pmod 3$.

Exemplo 4. *Calcule o resto de* 4^{100} *por 5.*

Como $4 \equiv -1 \pmod 5$, temos $4^{100} \equiv (-1)^{100} = 1 \pmod 5$.

Exemplo 5. *Calcule o resto de* 4^{100} *por 7.*

Você deve ter percebido que encontrar relações do tipo $a \equiv \pm 1 \pmod m$ podem simplificar bastante o cálculo de $a^k \pmod m$. Procuremos alguma relação como essa para 4 e 7. Veja que:

$$4^0 \equiv 1 \pmod 7, 4^1 \equiv 4 \pmod 7, 4^2 \equiv 2 \pmod 7, 4^3 \equiv 1 \pmod 7.$$

Assim,

$$4^{99} = (4^3)^{33} \equiv 1^{33} = 1 \pmod 7.$$

Como $4^3 \equiv 1 \pmod 7$, os restos das potências de 4 na divisão por 7 se repetem periodicamente de 3 em 3 pois $4^{3k+r} \equiv 4^{3k} \cdot 4^r \equiv 4^r \pmod 7$.

Exemplo 6. *Qual o resto de* $36^{36} + 41^{41}$ *na divisão por* 77*?*

Inicialmente devemos perceber que existe uma relação entre os números do problema: $36 + 41 = 77$. Assim:

$$\begin{aligned} -36 &\equiv 41 \pmod{77}, \\ (-36)^{41} &\equiv 41^{41} \pmod{77}, \\ 36^{36}(1 - 36^5) &\equiv 36^{36} + 41^{41} \pmod{77}. \end{aligned}$$

Nosso próximo passo é encontrar o resto de 36^5 na divisão por 77. Como $36 \equiv 1 \pmod 7$, $36^5 \equiv 1 \pmod 7$. Além disso, $36 \equiv 3 \pmod 1)1$ produzindo $36^5 \equiv 3^5 \equiv 1 \pmod 1)1$. Como $mdc(7, 11) = 1$ e ambos dividem $36^5 - 1$, podemos concluir que $77 \mid 36^5 - 1$. Logo, $36^{36} + 41^{41}$ deixa resto 0 na divisão por 77.

Exemplo 7. *Prove que* $p^2 - 1$ *é divisível por 24 se* p *é um primo maior que 3.*

Se p é um primo maior que 3, $p \equiv \pm 1 \pmod 3$ e $p \equiv 1 \pmod 2$. Daí, $p^2 \equiv 1 \pmod 3$. Além disso, se $p = 2k + 1$, segue que $p^2 = 4k(k + 1) + 1 \equiv 1 \pmod 8$ pois $k(k + 1)$ é par. Como $mdc(8, 3) = 1$ e ambos dividem $p^2 - 1$, segue que $24 \mid p^2 - 1$.

Exemplo 8. *(OCM-2001) Achar o menor natural* n *tal que 2001 é a soma dos quadrados de* n *inteiros*

Podemos concluir da solução do problema anterior que todo todo inteiro ímpar ao quadrado deixa resto 1 por 8. Usemos isso para estimar o valor de n. Sejam $x_1, x_2, \ldots, x_n$ inteiros ímpares tais que:

$$x_1^2 + x_2^2 + \ldots x_n^2 = 2001.$$

Analisando a congruência módulo 8, obtemos:

$$\begin{aligned} x_1^2 + x_2^2 + \ldots x_n^2 &= 2001 \pmod 8 \\ 1 + 1 + \ldots + 1 &\equiv 1 \pmod 8 \\ n &\equiv 1 \pmod 8 \end{aligned}$$

Como 2001 não é quadrado perfeito, não podemos ter $n = 1$. O próximo candidado para n seria $1 + 8 = 9$. Se exibirmos um exemplo para $n = 9$, teremos achado o valor mínimo. Veja que:

$$2001 = 43^2 + 11^2 + 5^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2.$$

Exemplo 9. *(IMO) Seja $s(n)$ a soma dos dígitos de n. Se $N = 4444^{4444}$, $A = s(N)$ e $B = s(A)$. Quanto vale $s(B)$?*

Pelo critério de divisibilidade por 9, $N \equiv A \equiv B \pmod 9$. Inicialmente calculemos o resto de N por 9. Como $4444 \equiv 16 \equiv 7 \pmod 9$, precisamos encontrar $7^{4444} \pmod 9$. Seguindo os métodos dos primeiros exemplos, seria interessante encontrarmos um inteiro r tal que $7^r \equiv \pm 1 \pmod 9$. O menor inteiro positivo com essa propriedade é $r = 3$. Como $4444 = 1481 \cdot 3 + 1$, temos:

$$7^{4444} \equiv 7^{1481 \cdot 3 + 1} \equiv (7^3)^{1481} \cdot 7 \equiv 7 \pmod 9.$$

Nosso próximo passo é estimar o valor de $s(B)$. Como $N = 4444^{4444} < 10^{5 \cdot 4444}$, $A = s(N) \leq 5 \cdot 4444 \cdot 9 = 199980$. Além disso, $B = s(A) \leq 1 + 9 \cdot 5 = 46$ e $s(B) \leq 12$. O único inteiro menor ou igual a 12 com resto 7 por 9 é o próprio 7, daí $s(B) = 7$.

Exemplo 10. *Prove que $11^{n+2} + 12^{2n+1}$ é divisível por 133 para qualquer natural n.*

Duas relações que podemos extrair dos números envolvidos são: $144 - 11 = 133$ e $133 - 12 = 121$. Assim:

$$\begin{aligned} 144 &\equiv 11 \pmod{133}, \\ 12^2 &\equiv 11 \pmod{133}, \\ 12^{2n} &\equiv 11^n \pmod{133}, \\ 12^{2n+1} &\equiv 11^n \cdot 12 \pmod{133}, \\ 12^{2n+1} &\equiv 11^n \cdot (-121) + 133 \cdot 11^n \pmod{133}, \\ 12^{2n+1} &\equiv -11^{n+2} \pmod{133}. \end{aligned}$$

Exemplo 11. *Prove que $n^5 + 4n$ é divisível por 5 para todo inteiro n*

Inicialmente note que $n^5 + 4n = n(n^4 + 4)$. Se $n \equiv 0 \pmod 5$, não há o que fazer. Se $n \equiv \pm 1 \pmod 5$, $n^4 + 4 \equiv 1 + 4 = 0 \pmod 5$. Finalmente, se $n \equiv \pm 2 \pmod 5$, $n^2 \equiv 4 \equiv -1 \pmod 5$ e consequentemente $n^4 + 4 \equiv 1 + 4 = 0 \pmod 5$.

Exemplo 12. *Seja $n > 6$ um inteiro positivo tal que $n - 1$ e $n + 1$ são primos. Mostre que $n^2(n^2 + 16)$ é divisível por 720. A recíproca é verdadeira?*

Veja que n é da forma $6k$, pois $n-1$ e $n+1$ são primos maiores que 3, portanto da forma $6k-1$ e $6k+1$, respectivamente. Logo,

$$n^2(n^2+16) = 144(9k^4+4k^2).$$

Resta provar que $9k^4+4k^2$ é um múltiplo de 5. Vamos analisar a igualdade acima módulo 5.

i) Se $k \equiv 0, 2$ ou $3 \pmod 5$, temos $9k^4+4k^2 \equiv 0 \pmod 5$;

ii) Se $k \equiv 1 \pmod 5 \Rightarrow n \equiv 1 \pmod 5$, temos $n-1 \equiv 0 \pmod 5$, um absurdo;

iii) Se $k \equiv 4 \pmod 5 \Rightarrow n \equiv 4 \pmod 5$, temos $n+1 \equiv 0 \pmod 5$, novamente um absurdo.

Isso conclui a demonstração. A recíproca não é verdadeira. Basta tomar, por exemplo, $n = 90$.

Problemas Propostos

Problema 13. *Determine o resto de $2^{20}-1$ na divisão por 41.*

Problema 14. *Qual o resto de $1^{2000}+2^{2000}+\ldots+2000^{2000}$ na divisão por 7?*

Problema 15. *Qual o resto na divisão de $2^{70}+3^{70}$ por 13?*

Problema 16. *Qual o resto de 3^{200} por 100?*

Problema 17. *(Estônia 2000) Determine todos os possíveis restos da divisão do quadrado de um número primo com o 120 por 120.*

Problema 18. *Qual o último dígito de 777^{777}?*

Exemplo 19. *Prove que $2222^{5555}+5555^{2222}$ é divisível por 7.*

Problema 20. *Prove que o número n^3+2n é divisível por 3 para todo natural n.*

Problema 21. *Prove que n^2+1 não é divisível por 3 para nenhum n inteiro.*

Problema 22. *Prove que n^3+2 não é divisível por 9 para nenhum n inteiro.*

Problema 23. *Prove que p^2-q^2 é divisível por 24 se p e q são primos maiores que 3.*

Problema 24. *Prove que se $2n+1$ e $3n+1$ são ambos quadrados perfeitos, então n é divisível por 40.*

Problema 25. *Se n é ímpar, prove que $7|2^{2n+1}+3^{n+2}$.*

Problema 26. *Seja $d(n)$ a soma dos dígitos de n. Suponha que $n+d(n)+d(d(n)) = 1995$. Quais os possíveis restos da divisão de n por 9?*

Problema 27. *Prove que não existem inteiros positivos $x_1, x_2, \ldots, x_{14}$ tais que:*

$$x_1^4+x_2^4+\ldots+x_{14}^4 = 1599.$$

Problema 28. *Escreva uma única congruência que é equivalente ao par de congruências* $x \equiv 1 \pmod 4$ *e* $x \equiv 2 \pmod 3$.

Problema 29. *Prove que* $20^{15} - 1$ *é divisível por* $11 \cdot 31 \cdot 61$

Problema 30. *(Alemanha 1997) Determine todos os primos p para os quais o sistema*

$$p + 1 = 2x^2$$
$$p^2 + 1 = 2y^2$$

tem uma solução nos inteiros x, y.

Problema 31. *Mostre que se n divide um número de Fibonacci então ele dividirá uma infinidade.*

Dicas e Soluções

13. Veja que

$$\begin{aligned} 2^5 = 32 &\equiv -9 \pmod{41} \Rightarrow \\ 2^{10} \equiv 81 &\equiv -1 \pmod{42} \Rightarrow \\ 2^{20} &\equiv 1 \pmod{41}. \end{aligned}$$

Assim, o resto procurado é zero.

14. Como $i^{2000} \equiv (i + 7k)^{2000} \pmod 7$, podemos simplificar o problema calculando primeiramente o valor de:

$$1^{2000} + 2^{2000} + 3^{2000} + 4^{2000} + 5^{2000} + 6^{2000} + 7^{2000} \pmod 7.$$

Outra observação importante que simplificará o cálculo é perceber que $2^3 \equiv 1 \pmod 7$. Assim,

$$2^{3k} \equiv 1 \pmod 7, 2^{3k+1} \equiv 2 \pmod 7, \text{ e } 2^{3k+2} \equiv 4 \pmod 7.$$

Usando isso e o fato de que 2000 é par, temos:

$$\begin{aligned} 1^{2000} + 2^{2000} + 3^{2000} + 4^{2000} + 5^{2000} + 6^{2000} + 7^{2000} &\equiv \\ 1^{2000} + 2^{2000} + (-4)^{2000} + 4^{2000} + (-2)^{2000} + (-1)^{2000} + 0^{2000} &\equiv \\ &\equiv 1 + 4 + 2 + 2 + 4 + 1 + 0 \\ &\equiv 0 \pmod 7. \end{aligned}$$

Dentre os primeiros 2000 naturais consecutivos, podemos formar 285 grupos de 7 números consecutivos cuja soma é múltipla de 7, em virtude da soma anterior. Os cinco números restantes possuem como resto na divisão por 7 o número:

$$\begin{aligned} 1996^{2000} + 1997^{2000} + 1998^{2000} + 1999^{2000} + 2000^{2000} &\equiv 1 + 4 + 2 + 2 + 4 \\ &\equiv 6 \pmod 7. \end{aligned}$$

Assim, o resto da soma na divisão por 7 é 6.

15. Inicialmente é interessante buscarmos alguma relação entre os números envolvidos no problema. Como $13 = 4 + 9$, podemos escrever:

$$\begin{aligned} 9 &\equiv -4 \pmod{13} \Rightarrow \\ 9^{35} &\equiv (-4)^{35} \pmod{13} \Rightarrow \\ 3^{70} + 2^{70} &\equiv 0 \pmod{13}. \end{aligned}$$

17. Use a fatoração $120 = 3 \cdot 5 \cdot 2^3$ e analise a congruência módulo 3, 5 e 8 separadamente.

18. Se n não é múltiplo de 3, sabemos que $n^2 \equiv 1 \pmod 3$. Assim $n^2 + 2 \equiv 0 \pmod 3$. Se n é múltiplo de 3, $n \equiv 0 \pmod 3$. Em qualquer caso, $n(n^2 + 2) \equiv 0 \pmod 3$.

19. Basta repetir a análise do problema anterior

20. Podemos montar uma tabela de congruências na divisão por 9:

n	0	1	2	3	4	5	6	7	8
n^3	0	1	8	0	1	8	0	1	8

Como nenhum cubo perfeito diexa resto 7 na divisão por 9, $n^3 + 2 \not\equiv 0 \pmod 9$.

23. Proceda como no exemplo 7.

25.

$$\begin{aligned} 2^{2n+1} + 3^{n+2} &\equiv 4^n \cdot 2 + 3^n \cdot 9 \\ &\equiv (-3)^n \cdot 2 + 3^n \cdot 2 \\ &\equiv 0 \pmod 7. \end{aligned}$$

26. Seja r o resto na divisão por 9 de n. Pelo critério de divisibilidade por 9, temos:

$$n + d(n) + d(d(n)) \equiv 3r \equiv 1995 \pmod 9.$$

Assim, $r \equiv 2 \pmod 3$ (Pela propriedade *vi* do teorema 2). Além disso,

$$\begin{aligned} n &\leq 1995 \Rightarrow \\ d(n) &\leq 27 = d(1989) \Rightarrow \\ d(d(n)) &\leq 10 = d(19). \end{aligned}$$

Consequentemente, $n \geq 1995 - d(n) - d(d(n)) \geq 1958$. Basta procurarmos nos conjunto $\{1958, 1959, \ldots, 1995\}$ os inteiros que deixam resto 2 por 3 e que satisfazem a equação do problema. Nesse conjunto, apena o inteiro 1967 cumpre essas condições.

27. Estudando a congruência módulo 16, podemos mostrar que $x^4 \equiv 0$ ou $1 \pmod 1)6$. Assim, a soma

$$x_1^4 + x_2^4 + \ldots + x_{14}^4$$

é congruente a um dos números do conjunto $\{0, 1, \ldots, 14\}$ m odulo 16 enquanto que $1599 \equiv 15 \pmod{16}$. Um absurdo.

28. $x \equiv 5 \pmod{12}$.

30. Suponha sem perda de generalidade que $x, y \geq 0$. Como $p+1$ é par, $p \neq 2$. Além disso,

$$2x^2 \equiv 1 \equiv 2y^2 \pmod{p}$$

e consequentente, usando que p é ímpar, $x \equiv \pm y \pmod{p}$. Como $x < y < p$, temos

$$p^2 + 1 = 2(p-x)^2 = 2p^2 - 4px + p + 1,$$

de modo que $p = 4x - 1, 2x^2 = 4x$. Podemos concluir que x é 0 ou 2 e que a única possibilidade para p é $p = 7$.

31. Em virtude da fórmula recursiva da sequência de Fibonacci, é possível mostrarmos que os restos de seus termos na divisão por qualquer número formam uma sequência periódica.

Referências

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

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

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

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

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