Achando um módulo de resolver o problema!

(versão compacta)

Gabriella Morgado - morgado.gabriella.s@gmail.com

27ª Semana Olímpica (2024) - Nível 1

1 Breves considerações sobre o material

Esta é a versão compacta do material, sem dicas, soluções, motivações para os conceitos, etc. Caso queira conferir a versão completa, ela deve ser postada no Google Classroom da Semana Olímpica e no site da OBM. Caso não encontre a versão completa do material por algum motivo ou caso tenha alguma dúvida, pode enviar um e-mail para o meu endereço morgado.gabriella.s@gmail.com!

2 Divisibilidade

Primeiramente, lembremos do algoritmo de divisão: dados a e m inteiros, $m \neq 0$, existem q e r únicos inteiros tais que $a = mq + r$ e $0 \leq r \leq (m-1)$.

Dizemos que $m|a$ (lê-se "m divide a") se a deixa resto 0 na divisão por m ou, equivalentemente, $a = mq$, para algum q inteiro. E temos as seguintes propriedades, para a, b, c, $m \neq 0$ inteiros:

(i) $m|0$, $1|m$ e $m|m$;

(ii) $m|1 \implies m = \pm 1$;

(iii) $m|a$ e $b|c \implies mb|ac$;

(iv) $m|a$ e $a|m \implies a = \pm m$;

(v) Se $m|a$ e $m|b$, então $m|(ax + by)$, para quaisquer a e b inteiros. Em particular, temos $m|(a+b)$ e $m|(a-b)$;

(vi) Se a e b deixam um mesmo resto r por m, então $m|(a-b)$;

(vii) Se $m|a$, então $a = 0$ ou $|m| \leq |a|$;

(viii) Se $m|a$ e $a|b$, então $m|b$;

(ix) Se $m|a$, então $m|ka$, para todo k inteiro;

(x) Se $m|ab$ e $mdc(m,b) = 1$, então $m|a$. Em particular, para p primo, se $p|ab$, então $p|a$ ou $p|b$;

(xi) Se $m|(a-b)$, então $m|(a^k - b^k)$ para todo k inteiro positivo;

(xii) Se $m|(a+b)$, então $m|(a^k + b^k)$ para todo k inteiro positivo ímpar.

3 Congruências

Uma forma de facilitar a manipulação de expressões envolvendo divisibilidade é com o uso das congruências.

Dizemos que $a \equiv b (\text{mod } m)$ (lê-se "a é côngruo a b módulo m" ou "a é congruente a b módulo m") para $m > 1$, a, b inteiros quando:

(i) a e b deixam o mesmo resto por m;

(ii) $m|(a - b)$.

Mostre que (i) e (ii) são equivalentes! E, temos ainda, algumas propriedades. Suponhamos que, para $m > 0$, a, b, c, d inteiros, tenhamos $a \equiv b (\text{mod } m)$ e $c \equiv d (\text{mod } m)$. Seja ainda um inteiro q com $mdc(q, m) = D > 0$. Então,

(i) $a + c \equiv b + d (\text{mod } m)$. Em particular, $a + c \equiv b + c (\text{mod } m)$;

(ii) $a - c \equiv b - d (\text{mod } m)$ Em particular $a - c \equiv b - c (\text{mod } m)$;

(iii) $ac \equiv bd (\text{mod } m)$. Em particular, $ac \equiv bc (\text{mod } m)$;

(iv) $a^k \equiv b^k (\text{mod } m)$, para todo $k \in \mathbb{Z}_{>0}$;

(v) $qa \equiv qb (\text{mod } m) \iff a \equiv b (\text{mod } \frac{m}{D})$. Em particular, se $mdc(q, m) = 1$, $qa \equiv qb (\text{mod } m) \iff a \equiv b (\text{mod } m)$.

Informalmente, podemos somar, subtrair, multiplicar e elevar "dos dois lados". Também podemos dividir ou "cortar" "dos dois lados", mas com o cuidado de observar o mdc do módulo e do fator.

4 Teoremas

Existem alguns teoremas famosos envolvendo divisibilidade e congruências que enunciaremos sem a demonstração. Caso queira ver a prova desses teoremas, você pode checar uma referência como [1].

(Teorema de Báchet-Bézout) Dados a, b inteiros não ambos nulos, existem x, y inteiros tais que

$$ax + by = mdc(a, b).$$

(Soluções para equações diofantinas lineares) Dados a, b, c inteiros, a e b não ambos nulos, a equação

$$ax + by = c$$

tem solução (x, y) nos inteiros se, e só se, $mdc(a, b) = d \mid c$. Mais que isso, sendo (x', y') uma solução, existem infinitas soluções, que são unicamente os elementos do conjunto $\{(x, y) = (x' + \frac{b}{d}t, y' - \frac{a}{d}t), \text{ para } t \in \mathbb{Z}\}$. Note que essa é uma generalização do teorema de Bachét-Bézout.

(Teorema de Wilson) Se p é primo, então

$$(p - 1)! \equiv -1 \pmod{p}.$$

E, reciprocamente, se n é inteiro positivo tal que $(n-1)! \equiv -1 \pmod{n}$, então n é primo.

(Pequeno Teorema de Fermat) Para a inteiro não nulo e p primo tal que $p \nmid a$, temos

$$a^{p-1} \equiv 1 \pmod{p}.$$

Existe, ainda uma outra versão, que não precisa da suposição de a e p coprimos. Sendo a inteiro e p primo. temos

$$a^p \equiv a \pmod{p}.$$

(Teorema de Euler) Para a inteiro não nulo e coprimo com o inteiro $m > 0$, temos

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

sendo ϕ a função phi de Euler, tal que $\phi(n)$ é a quantidade de inteiros positivos coprimos com n e menores que n. Note que $\phi(p) = p - 1$ para p primo. Daí, o teorema de Euler é uma generalização do pequeno teorema de Fermat.

(Teorema Chinês dos Restos) Sejam $n_1, \ldots, n_k$ inteiros maiores que 1. Seja N o produto dos n_i. Se os n_i são coprimos dois a dois e $a_1, \ldots, a_k$ são inteiros tais que temos o sistema

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_k}. \end{cases}$$

Esse sistema tem uma solução e quaisquer duas soluções, digamos x_1 e x_2, são tais que $x_1 \equiv x_2 \pmod{N}$. Isto é, a solução é única módulo N.

5 Problemas resolvidos

1. Prove que $7 \mid (2222^{5555} + 5555^{2222})$.

2. (Olimpíada de Maio 2001) Encontre todos os naturais a e b tais que $a \mid (b+1)$ e $b \mid (a+1)$.

3. Mostre que, para n ímpar, $n | 1^n + 2^n + \cdots + (n-1)^n$.

4. (Leningrado 1989) Seja A um natural maior que 1 e seja B um natural divisor de $A^2 + 1$. Prove que, se $B - A > 0$, então $B - A > \sqrt{A}$.

5. (Rússia 2001) Encontre todos os primos p e q tais que $p + q = (p - q)^3$.

6 Problemas

1. Determine o resto de 5^{200} por 3.

2. Mostre que $mdc(n, n+1) = 1$ para todo n inteiro.

3. Prove os seguintes critérios de divisibilidade:
(a) Um número é par se, e só se, seu dígito das unidades é par.
(b) Um número é múltiplo de 5 se, e só se, seu dígito das unidades é 0 ou 5.
(c) Um número é múltiplo de 10 se, e só se, seu dígito das unidades é 0.
(d) Um número é múltiplo de 3 se, e só se, a soma de seus dígitos é divisível por 3.
(e) Um número é múltiplo de 9 se, e só se, a soma de seus dígitos é divisível por 9.
(f) Um número é múltiplo de 11 se, e só se, a soma de seus dígitos em posições pares menos a soma de seus dígitos em posições ímpares é divisível por 11. Por exemplo, 121 é múltiplo de 11, porque $1 + 1 - 2 = 0 \equiv 0 \pmod{11}$.

4. (Sonho de todo estudante) Prove que, para todo p primo, vale $(a+b)^p \equiv a + b \pmod{p}$.

5. Mostre que existem infinitos números inteiros que não podem ser escritos como a soma de três cubos perfeitos.

6. Encontre todas as soluções inteiras de $x^3 - 117y^3 = 5$.

7. (OMCPLP 2019, adaptado) Determine o menor inteiro positivo k tal que existem k inteiros $x_1, x_2, \ldots x_k$ tais que $x_1^5 + x_2^5 + \cdots + x_k^5 = 2018$.

8. (IMO 1964)
(a) Ache todos os inteiros n tais que $7|2^n - 1$.
(b) Prove que não existe $n \in \mathbb{N}$, tal que $7|2^n + 1$.

9. Sejam a, a' inteiros. Dizemos que a' é inverso de $a \pmod{n}$ se $aa' \equiv 1 \pmod{n}$. Mostre que a tem inverso $\pmod{n}$ se, e somente se, $mdc(a, n) = 1$. Mostre ainda que tal inverso deve ser único $\pmod{n}$, isto é, se a'' é um inteiro tal que $aa' \equiv aa'' \equiv 1 \pmod{n}$, então $a' \equiv a'' \pmod{n}$.

10. Prove que, se p é primo tal que $p \equiv 3 \pmod{4}$, então, se $p \mid (a^2 + b^2)$, segue que $p|a$ e $p|b$.

11. (OBM 2000) É possível encontrar duas potências de 2 distintas e com o mesmo número de algarismos tais que uma possa ser obtida através de uma reordenação dos dígitos da outra?

12. (IMO 1975) Sejam $N = 4444^{4444}$ e $s(n)$ a soma dos algarismos de n. Determinemos A e B como $A = s(N)$ e $B = s(A)$. Qual é o valor de $s(B)$?

13. (Rússia 1997) Encontre todas as soluções inteiras de $(x^2 - y^2)^2 = 1 + 16y$.

14. (São Petersburgo 2016) Seja $(a_n)_{n\in\mathbb{Z}_{>0}}$ uma sequência de inteiros tal que $(m+n)|(a_m+a_n)$, para quaisquer m, n inteiros positivos. Prove que $n|a_n$, para todo n inteiro positivo.

15. (Romênia JBMO TST 2021) Encontre todos os pares de inteiros positivos (x, y) tais que $x \leq y$ e $\frac{(x+y)(xy-1)}{zy+1} = p$, sendo p primo.

16. (Canadá Júnior 2021) De quantas maneiras podemos permutar os n primeiros inteiros positivos de modo que, para todo $k \in \{1, 2, \dots n\}$, os primeiros k inteiros da permutação sejam incongruentes dois a dois módulo k?

17. (TM2 2023) Definimos a sequência $(a_n)_{n\in\mathbb{N}}$ de forma recursiva, onde os termos iniciais são $a_1 = 12$ e $a_2 = 24$, e, para $n \geq 3$, temos $a_n = a_{n-2} + 14$.
(a) O número 2023 aparece na sequência?
(b) Mostre que não existem quadrados perfeitos nessa sequência.

18. (USAJMO 2022) Para quais inteiros positivos m, existem uma P.A. $(a_n)_{n\in\mathbb{Z}_{>0}}$ e uma P.G. $(g_n)_{n\in\mathbb{Z}_{>0}}$ tais que as seguintes propriedades são ambas satisfeitas?
(a) $m|(a_n - g_n), \forall n \in \mathbb{Z}_{>0}$;
(b) $m \nmid (a_2 - a_1)$.

19. (IMO 2005) Determine todos os inteiros positivos coprimos com todos os termos da sequência $(a_n)_{n\in\mathbb{N}}$ dada por $a_n = 2^n + 3^n + 6^n - 1$.

20. (OBM 2005) Sejam n e k inteiros positivos, k ímpar. Prove que $(1 + 2 + \cdots + n)|(1^k + 2^k + \cdots + n^k)$.

21. (Cazaquistão 2018) Seja S o conjunto $S = \{xy(x + y)|x, y \in \mathbb{Z}_{>0}\}$. Seja n natural tal que exista um a natural que satisfaça $a + 2^k \in S, \forall k \in \{1, 2, \dots n\}$. Encontre o maior tal n possível.

22. (JBMO Shortlist 2021) Encontre todos os inteiros positivos a, b, c tais que $ab + 1$, $bc + 1$ e $ca + 1$ são iguais a fatoriais de inteiros positivos.

23. (OBM 2009) Mostre que existe um inteiro positivo n_0 com a seguinte propriedade: para qualquer inteiro $n \geq n_0$, é possível particionar um cubo em n cubos menores.

24. (Rússia 1995) Existe uma sequência de inteiros positivos na qual todos os inteiros positivos aparecem exatamente uma vez cada e a soma dos k primeiros termos é divisível por k, para todo k inteiro positivo?

25. (IMO 2023) Determine todos os inteiros positivos compostos $n > 1$ com a seguinte propriedade: sendo $1 = d_1 < d_2 < \cdots < d_k = n$ todos os divisores positivos de n, então $d_i \mid (d_{i+1} + d_{i+2}), \forall i \in \{1, 2, \dots k - 2\}$.

Referências

[1] José Plínio de Oliveira Santos. *Introdução à Teoria dos Números*. IMPA, 3rd edition, 2020.