Introdução à Aritmética Modular

Carlos Alex

12 de novembro de 2021

Nessa aula iremos começar uma introdução à aritmética modular, um tópico da Teoria dos Números. Precisamos recordar de alguns conceitos antes:

(I) DIVISIBILIDADE

Dados dois inteiros a e b, com "a" diferente de 0, dizemos que a divide b ou que a é um divisor de b ou ainda que b é um múltiplo de a e escrevemos "a | b" se o r obtido pelo algoritmo de divisão aplicado à a e b é 0, ou seja, se b = a.q para algum inteiro q.

Exemplos:
Veja que 3 | 18, já que 18 = 3.6, mas 3 não divide 26, pois 26 = 2.13. Também, 7 | 56, pois 56 = 7.8, daí, 8 | 56 também. Para todo n pertencente aos naturais n | 6n, pois 6n = 2.3.n e 3 | 3n + 3, pois 3n + 3 = 3.(n + 1). Da mesma forma $m + 1 \mid m^2 - 1$ para todo m pertencente aos inteiros, pois $m^2 - 1 = (m + 1).(m - 1)$.
Propriedades :

(I) Se d | a, então $d \leq a$.

(II) Se d | a, então d | a.c, para qualquer $c \in \mathbb{Z}$.

(III) Se a | b e a | c, então a | b + c. Logo, se d | a e d | b, então d | ax + by, para quaisquer x e y pertencentes a Z.

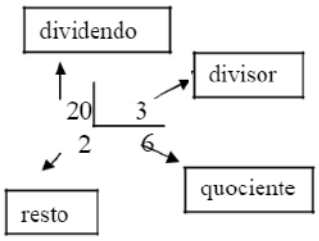
(IV) Se a | b e b | c, então a | c (transitividade)

Obs.: Veja que alguns problemas de divisibilidade podem vir disfarçados, pois já que ocorre de b ser múltiplo de a sempre que a | b, então provar que a | b é o mesmo que provar que $\frac{b}{a}$ é um número inteiro.

Teorema: Se p é um número primo e p | a.b, então p | a ou p | b.

(II) ALGORITMO DA DIVISÃO

Em uma divisão temos:



Chegamos no seguinte algoritmo:

$$D = d \cdot q + r$$

(III) ARITMÉTICA MODULAR

Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que a é congruente a b módulo m se e somente se m divide a diferença a - b.

Em outros termos, a é congruente a b módulo m se e somente se existe um inteiro k tal que $a - b = k.m$

Com a notação

$$a \equiv b\ (\mathrm{mod.}\, m)$$

indica-se que a é congruente a b módulo m. Portanto simbolicamente:

$$a \equiv b\ (\mathrm{mod.}\, m) \leftrightarrow m \mid (a - b)$$

ou seja:

$$a \equiv b\ (\mathrm{mod.}\, m) \leftrightarrow \exists\, k \in z \mid a - b = k.m$$

assim por exemplo:

$$3 \equiv 24\ (\mathrm{mod.}\, 7), \text{porque } 7 \mid (3 - 24)$$

$$-31 \equiv 11\ (\mathrm{mod.}\, 6), \text{porque } 6 \mid (-31 - 11)$$

$$-15 \equiv -63\ (\mathrm{mod.}\, 8), \text{porque } 8 \mid (-15 - (-63))$$

Se m não divide a diferença a – b, então diz-se que a é incongruente a b módulo m, o que se indica pela notação:

$$25 \not\equiv 12\ (\mathrm{mod.}\, 7), \text{porque } 7 \nmid (25 - 12)$$

$$-21 \not\equiv (\mathrm{mod.}\, 5), \text{porque } 5 \nmid (-21 - 10)$$

$$16 \equiv 9\ (\mathrm{mod.}\, 4) \text{ porque } 4 \nmid (16 - 9)$$

Note-se que dois inteiros quaisquer são congruentes módulo 1, enquanto que dois inteiros são congruentes módulo 2 se ambos são pares ou se ambos são ímpares.

Em particular, se $a \equiv 0\ (\mathrm{mod.}\, m)$ se e somente se o módulo m divide a (m|a)

PROPRIEDADES

(**I**) $a \equiv a\ (\mathrm{mod.}\, m)$

(**II**) se $a \equiv b\ (\mathrm{mod.}\, m)$, então $b \equiv a\ (\mathrm{mod.}\, m)$

(**III**) se a $\equiv$ b (mod. m) e se b $\equiv$ c (mod. m) , então a $\equiv$ c (mod. m)

(**IV**) Se a $\equiv$ b (mod. m) e se n | m , com n $>$ 0 , *então* $a \equiv b\ (mod.n)$

(**V**)Se a $\equiv$ b (mod. m)e se c $>$ 0, *então* $ac \equiv bc$ (mod. mc)

(**VI**)Se a $\equiv$ b (mod. m)e se a, b e m são todos divisíveis pelo inteiro d $>$ 0, *então* $a/d \equiv b/d\ (mod.m/d)$

divisíveis pelo inteiro d $>$ 0, *então* a/d

(**VII**)Se a $\equiv$ b (mod. m)e se c $\equiv$ d (mod. m), então a + c $\equiv$ b + c (mod. m)e ac $\equiv$ bd (mod. m)

(**VIII**) Se $\equiv$ b (mod. m), então a + c $\equiv$ b + c $(mod\ m)$ e ac $\equiv$ bc (mod. m)

(**IX**) Se a $\equiv$ b (mod m), então $a^n \equiv b^n$(mod m) para todo inteiro positivo n.

Pequeno Teorema de Fermat

$\rightarrow p / a^p - a;\ a \in Z\ e\ p\ primo.$

$\rightarrow a^p \equiv a\ (\text{mod}\ p)$

$\rightarrow p\ não\ divide\ a \Rightarrow p / a^{p-1} - 1$

$\rightarrow p\ não\ divide\ a \Rightarrow a^{p-1} \equiv 1(\text{mod}\ p)$

Alguns problemas

Parte 1

01. Qual é o maior inteiro positivo n tal que n + 10 divide $n^3 + 100$?

02. Prove que não existe nenhum inteiro tal que 4 | n² + 2.

03 Qual é o resto que uma potência ímpar de 2 deixa por 3?

04. (OBM) Quantos pares ordenados de inteiros positivos existem tais que $\frac{2014}{a^2+b^2}$ é inteiro?

05. (OBM) Qual é a maior potência de 2 que divide $2011^{2012} - 1$?

06. Quantos são os inteiros positivos n tais que n + 3 | n² + 7?

07. Mostre que se 7 | 3a + 2b, então 7 | 4a – 2b.

08. Mostre que se 3 | a + 7b, então 3 | a + b.

10. Encontre todos os inteiros positivos n tais que n + 2009 divide n² + 2009 e n + 2010 divide n² + 2010.

11. Mostre que se 17 | 3a + 2b então 17 | 10a + b.

12. (OBM) Para quantos inteiros *n* o número $\frac{n}{100-n}$ é também inteiro?

13. (OBM) Determine o número de inteiros positivos n menores que 100 de modo que a fração 8n+5/5n+8 não seja irredutível. Uma fração é chamada de irredutível quando o máximo divisor comum (MDC) entre o seu numerador e o seu denominador é igual a 1.

14. (Maio) Encontre todos os pares de números inteiros positivos (a, b) tais que 8b + 1 é múltiplo de a e 8a + 1 é múltiplo de b.

15. (IMO1959). Mostre que a fração 21n + 4/ 14n + 3 é irredutível para todo n natural.

16 (OBM) Para quantos inteiros positivos m o número $\frac{2004}{m^2-2}$ é um inteiro positivo?

Parte 2

17. Verifique as alternativas e marque (V) Verdadeiro ou (F) Falso:

(**a**)( ) $91 \equiv 0\ (\text{mod}.7)$
(**b**)( ) $3 + 5 + 7 \equiv 5\ (\text{mod}.10)$
(**c**)( ) $-2 \equiv -2\ (\text{mod}.8)$
(**d**)( ) $11^2 \equiv 1\ (\text{mod}.3)$
(**e**)( ) $17 \equiv 9\ (\text{mod}.2)$
(**f**)( ) $42 \equiv -8\ (\text{mod}.10)$
(**g**)( ) $x \equiv 3\ (\text{mod}.5) \rightarrow x \in \{\ldots, -7, -2, 3, 8, 13, \ldots\}$

18. Sabendo que $1066 \equiv 1776\ (\text{mod}.m)$, achar todos os possíveis valores do módulo m.

19. Achar todos os inteiros x tais que $0 \leq x < 15\ e$

$3x \equiv 6\ (\text{mod}.15)$

20. Achar todos os inteiros x tais que $1 \leq x \leq 100$ e $x \equiv 7\ (\text{mod}.17)$

21. Sabendo que $k \equiv 2 \pmod{4}$, mostrar que $6k + 5 \equiv 3 \pmod{4}$

22. Mostrar, mediante um exemplo, que $a^2 \equiv b^2 \pmod{m}$ não implica $a \equiv b \pmod{m}$

23. Mostrar que todo primo (exceto 2) é congruente módulo 4 a 1 ou 3.

24. Mostrar que $11^{10} \equiv 1 \pmod{100}$.

25. Mostrar que 41 divide $2^{20} - 1$.

26. Determine o resto de 5^{21} *por* 127 .

27. Determine o resto de 2^{20} *por* 11.

28. Determine o resto de $13^6 - 2^{25} \cdot 5^{15}$ *por* 3

29. Achar os restos das divisões de 2^{50} e 41^{65} por 7.

30. Sejam $a, p \in \mathrm{N}$, com p primo. Mostre que se $a^2 \equiv 1 (\mathrm{mod}\ p)$, então $a \equiv 1 (\mathrm{mod}\ p)$ ou $a \equiv -1 (\mathrm{mod}\ p)$

31. (OBM) Prove que existem infinitos inteiros positivos *n* tais que

$$\frac{5^{n-2} - 1}{n}$$

é um inteiro.

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

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

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

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

36. Escreva uma única congruência que é equivalente ao par de congruências $x \equiv 1 \pmod{4}$ e $x \equiv 2 \pmod{3}$.

37. Qual o resto de 3^{200} por 100?

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

39. Prove que $p^2 - q^2$ é divisível por 24 se p e q são primos maiores que 3.

40. Prove que $n^2 + 1$ não é divisível por 3 para nenhum n inteiro.

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

ANOTAÇÕES