1 Congruências, critérios de divisibilidade e restos, congruências e somas, congruências e produtos

Em encontros anteriores, discutimos o conceito de restos. Observamos que, ao resolver muitos problemas sobre divisibilidade, trabalhamos, na maioria das vezes, não com o numero propriamente dito, mas com o resto da divisão por algum numero fixo.

É natural, portanto, a seguinte definição: dizemos que os inteiros a e b são congruentes módulo m, se eles tem o mesmo resto quando divididos por m. Neste caso, escrevemos $a \equiv b \pmod{m}$.

Por exemplo, $9 \equiv 29 \pmod{10}$, $1 \equiv 3 \pmod{2}$, $16 \equiv 9 \pmod{7}$, $3 \equiv 0 \pmod{3}$, $2n+1 \equiv 1 \pmod{n}$. Note que A é divisível por m se e somente se $A \equiv 0 \pmod{m}$.

1. Prove que $a \equiv b \pmod{m}$ se e somente se $a-b$ é divisível por m.
   Solução. Se $a \equiv b \pmod{m}$, seja r o resto comum da divisão de a ou b por m. Temos:
   $$a = mk_1 + r,\ b = mk_2 + r.$$
   Logo $a - b = m(k_1 - k_2)$ é divisível por m.
   Reciprocamente, se $a-b$ for divisível por m, dividimos a e b por m com resto. Temos $a = mk_1 + r_1$, $b = mk_2 + r_2$. Então $a - b = m(k_1 - k_2) + r_1 - r_2$, é, por hipótese, divisível por m. Portanto, $r_1 - r_2$ é divisível por m. Como $|r_1 - r_2| < m$, temos $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$.

2. Prove que:
   (a) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \pm c \equiv b \pm d \pmod{m}$.
   (b) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.
   (c) Se $a \equiv b \pmod{m}$ e $ac \equiv d \pmod{m}$, então $bc \equiv d \pmod{m}$.
   (d) Se $a \equiv b \pmod{m}$ e c um inteiro qualquer, então $ac \equiv bc \pmod{m}$.
   (e) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.
   (f) Se $ax \equiv ab \pmod{m}$ e a e m forem primos entres si, então $x \equiv b \pmod{m}$.
   Solução. Sabemos que m divide $ax - ab$, ou seja, existe k inteiro tal que: $ax - ab = a(x-b) = mk$, então $m|a(x-b)$, como m e a são primos entre si, então $m|(x-b) \Rightarrow x \equiv b \pmod{m}$.
   Observação. $2 \cdot 6 \equiv 2 \cdot 4 \pmod{4}$, mas $6 \not\equiv 4 \pmod{4}$, pois 4 e 2 não são primos entre si.

3. Verifique quais afirmações abaixo são falsas:
   (a) $98 \equiv 0 \pmod{7}$
   (b) $5 + 8 + 3 \equiv 6 \pmod{6}$
   (c) $-2 \equiv 2 \pmod{8}$
   (d) $11^2 \equiv 1 \pmod{3}$
   (e) $16 \equiv -4 \pmod{5}$

4. Ache o resto da divisão por, 7, 9, 11 e 13 do numero 3215529.
   Solução. Observemos que: $3215529 = 3 \cdot 10^6 + 2 \cdot 10^5 + 1 \cdot 10^4 + 5 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10^1 + 9$.

   $3 \cdot 10^6 + 2 \cdot 10^5 + 1 \cdot 10^4 + 5 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10^1 + 9 \equiv 3 \cdot 3^6 + 2 \cdot 3^5 + 1 \cdot 3^4 + 5 \cdot 3^3 + 5 \cdot 3^2 + 2 \cdot 3^1 + 2 = 3 \cdot 9^3 + 6 \cdot 9^2 + 1 \cdot 9^2 + 5 \cdot 27 + 5 \cdot 9 + 2 \cdot 3 + 2 \equiv 3 \cdot 2^3 + (-1) \cdot 2^2 + 1 \cdot 2^2 + 5 \cdot (-1) + 5 \cdot 2 + 6 + 2 \equiv 24 - 4 + 4 - 5 + 10 + 6 + 2 = 37 \equiv 2 \pmod{7}$

   $3 \cdot 10^6 + 2 \cdot 10^5 + 1 \cdot 10^4 + 5 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10^1 + 9 \equiv 3 \cdot 1^6 + 2 \cdot 1^5 + 1 \cdot 1^4 + 5 \cdot 1^3 + 5 \cdot 1^2 + 2 \cdot 1^1 + 9 \equiv 27 \equiv 0 \pmod{9}$

   $3 \cdot (-1)^6 + 2 \cdot (-1)^5 + 1 \cdot (-1)^4 + 5 \cdot (-1)^3 + 5 \cdot (-1)^2 + 2 \cdot (-1)^1 + 9 \equiv 3 - 2 + 1 - 5 + 5 - 2 + 9 = 9 \pmod{11}$

   $3 \cdot 10^6 + 2 \cdot 10^5 + 1 \cdot 10^4 + 5 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10^1 + 9 \equiv 3 \cdot (-3)^6 + 2 \cdot (-3)^5 + 1 \cdot (-3)^4 + 5 \cdot (-3)^3 + 5 \cdot (-3)^2 + 2 \cdot (-3)^1 + 9 = 3 \cdot 9^3 - 2 \cdot 27 \cdot 9 + 1 \cdot 81 - 5 \cdot 27 + 5 \cdot 9 - 2 \cdot 3 + 9 \equiv 27 \cdot 81 - 2 \cdot 1 \cdot 9 + 1 \cdot 3 - 5 \cdot 1 + 45 - 6 + 9 \equiv 1 \cdot 3 - 18 + 3 - 5 + 6 - 6 + 9 = -8 \equiv 5 \pmod{13}$

5. Deduza critérios de divisibilidade dos números: 2, 3, 4, 5, 9, 11.

6. Ache o resto da divisão por 7 dos seguintes números: $2^{5345}, 2^{3765839}, 2^{10^{10}}$

7. Determine o resto da divisão por 5 do numero: $45769834^{532} \times 63876^{1654} + 87987545^{1345874} - 95973434$.

8. Encontre o resto da divisão de 8^{900} por 29.

9. Encontre o resto da divisão de $11^{13} + 17^{19}$ por 7.

10. Encontre os restos de $1234^{1234} + 12345^{123} - 123456^{1234}$ por 12.

11. Prove que todo quadrado perfeito deixa resto 0, 1 ou 4 por 8.

12. Mostre que $n^5 - 5n^3 + 4n$ é divisível por 120.
Solução. Temos que:
$n^5 - 5n^3 + 4n = n(n^4 - 5n^2 + 4) = n(n^2 - 1)(n^2 - 4) = n(n-1)(n+1)(n-2)(n+2) = (n+2)(n+1)n(n-1)(n-2)$

Teremos que entre 5 números inteiros consecutivos:
Pelo menos 2 serão múltiplos de 2, pelo menos 1 será múltiplo de 3, pelo menos 1 será múltiplo de 4, um será múltiplo de 5

Um desses múltiplos de 2 será o tal número múltiplo de 4. Logo o produto desses números será múltiplo de $2 \cdot 3 \cdot 4 \cdot 5 = 120$.

13. Mostre que $143^6 + 91^{10} + 77^{12} - 1$ é múltiplo de 1001.
Solução. Como o numero 1001 é muito grande para analisar todos os possíveis restos, analisamos então os restos de seus fatores, pois se um numero é múltiplo de 1001 obrigatoriamente tem que ser múltiplo de seus fatores:

$$\begin{array}{c|c} 1001 & 7 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array}$$

agora analisamos os restos por 7, 11 e 13:
$143^6 + 91^{10} + 77^{12} - 1 \equiv 3^6 + 0^{10} + 0^{12} - 1 \equiv 9^3 - 1 \equiv 2^3 - 1 \equiv 0 \pmod 7$
$143^6 + 91^{10} + 77^{12} - 1 \equiv 0^6 + 3^{10} + 0^{12} - 1 \equiv 9^5 - 1 \equiv (-2)^5 - 1 \equiv -32 - 1 \equiv 0 \pmod{11}$
$143^6 + 91^{10} + 77^{12} - 1 \equiv 0^6 + 0^{10} + (-1)^{12} - 1 \equiv 1 - 1 \equiv 0 \pmod{13}$
Então $143^6 + 91^{10} + 77^{12} - 1$ deixa resto 0 pelos fatores de 1001, ou seja é múltiplo de 1001.

14. Usando congruências, prove que $30^{99} + 61^{99}$ é divisível por 31.

15. Prove que $300^{3000} - 1$ é divisível por 1001.

16. Existe um número natural n tal que $n^2 + n + 1$ é divisível por 1955?
Dica. Analise quais são os valores que $n^2 + n + 1$ tomam levando em conta o resto de n por 5.

17. Mostre que 19 nunca divide um número da forma $4n^2 + 4$.

18. Prove que $n^3 + 2$ não é divisível por 9, qualquer que seja o inteiro n.

19. Mostre que a equação diofantina $x^2 + y^2 + z^2 = 8w + 7$ não possui soluções $x,\ y,\ z,\ w$ inteiros.
Dica. Reduza a equação Módulo 8 e mostre que $x_0^2 + y_0^2 + z_0^2 \equiv 7 \pmod 8$ nunca ocorre.

20. Foi calculada a soma dos algarismos do número 2^{100}, depois foi calculada a soma dos algarismos do número resultante, e assim por diante, até sobrar um único algarismo. Qual é este algarismo?
Dica. Considere o critério de divisibilidade por 9.

21. Mostre que, para todo $n \in \mathbb{N}$,

   (a) 7 divide $3^{2n+1} + 2^{n+2}$.
   (b) 9 divide $10^n + 3 \times 4^{n+2} + 5$.
   (c) 24 divide $2 \times 7^n + 3 \times 5^n - 5$.
   (d) 35 divide $3^{6n} - 2^{6n}$
   (e) 64 divide $7^{2n} + 16n - 1$.

22. $x^n - y^n$ é divisível por $x - y$ para todos naturais x e y, $x \neq y$ e $n > 0$.
Solução. Temos que; $x \equiv y \pmod{x-y} \Rightarrow x^n \equiv y^n \pmod{x-y}$. Então, segundo a definição de congruência, $x^n - y^n$ é divisível por $x - y$, sendo $n \in \mathbb{N}$.

23. Seja p um número primo e suponha que a e b são inteiros arbitrários. Prove que $(a+b)^p \equiv (a^p + b^p) \pmod{p}$.
Dica. Utilise o "Pequeno" Teorema de Fermat.

24. Prove que $p^2 - 1$ é divisível por 24 se p for um número primo maior do que 3.

25. Prove que $p^2 - q^2$ é divisível por 24 se p e q forem números primos maiores do que 3.

26. Usando congruências, encontre o resto da divisão do número $10^{10} + 10^{100} + 10^{1000} + \cdots + 10^{10.000.000.000}$ por 7.
Dica. Utilise o "Pequeno" Teorema de Fermat.

2 Respostas

3. As afirmações falsas são: (b) e (c).

6. $2^{5345}, 2^{3765839}, 2^{10^{10}}$ por 7 deixam resto 4, 4, 2 respectivamente

7. Resto 2

8. Resto 7

9. Resto 0

10. Resto 1

26. Resto 5