Universidade de Brasília
Faculdade do Gama

Matemática Discreta 2

Prof. Dr. Glauco Vitor Pedrosa

UnB Gama
O novo endereço da tecnologia

Congruências

- Sejam $\underline{a}$ e $\underline{b}$ dois inteiros quaisquer e seja $|\underline{m}| > 1$.
- Dizemos que *a é congruente a b módulo m* se o resto da divisão de *a* por *m* for igual ao resto da divisão de *b* por *m*
- Exemplo:

$3 \equiv 24 \pmod 7$

$13 \equiv 1 \pmod 6$

$15 \equiv -6 \pmod 7$

mod de dividendo negativo

- Como encontrar o mod de **dividendo negativo**?
- Exemplo:

a) -5 (mod 4)

Faça: 5 (mod 4) = 1, então subtraia 4 – 1 = 3

b) -50 (mod 7)

Faça: 50 (mod 7) = 1, então subtraia 7 – 1 = 6

c) -48 (mod 3)

Faça: 48 (mod 3) = 0, **<u>não faça nada!</u>**

d) -51 (mod 7)

Faça: 51 (mod 7) = 2, então subtraia 7 – 2 = 5

e) -121 (mod 50)

Faça: 121 (mod 50) = 21, então subtraia 50 - 21 = 29

mod de divisor negativo

- Como encontrar o mod de **divisor negativo**?
- Exemplo:

a) 5 (mod -4)

Faça: 5 (mod 4) = 1, então some – 4 + 1 = -3

b) 50 (mod -7)

Faça: 50 (mod 7) = 1, então some -7 +1 = -6

c) 48 (mod -3)

Faça: 48 (mod 3) = 0, **não faça nada!**

d) 51 (mod -7)

Faça: 51 (mod 7) = 2, então some -7 + 2 = -5

e) 121 (mod -50)

Faça: 121 (mod 50) = 21, então some -50 + 21 = -29

mod de números negativos

- **Regra geral:**

$-a \pmod{m} = m - (a \pmod{m})$

$a \pmod{-m} = -m + (a \pmod{m})$

$-a \pmod{-m} = -(a \pmod{m})$

Importante!!

- Exceção quando $(a \pmod{m}) = 0$, então não faça nada.

Exercício

- Julgue V ou F as seguintes sentenças

a) $7 \equiv 5 \pmod{2}$ **verdadeira**

b) $19 \equiv -5 \pmod{3}$ **verdadeira**

c) $-19 \equiv 5 \pmod{3}$ **verdadeira**

d) $9 \equiv -13 \pmod{-5}$ **falsa**

e) $-10 \equiv -17 \pmod{-7}$ **verdadeira**

Exercício

- Encontre todos os valores de n entre 1 e 100 que sejam congruentes a 6 mod 13

$$\mathbf{n \equiv 6 \bmod 13 \quad tal\ que \quad 1 \leq n \leq 100}$$

Resposta:

n = {6, 19, 32, 45, 58, 71, 84, 97}

Congruências

- Proposição:

Se $a \equiv b \pmod{m}$ *então* $m \mid (a-b)$

- Exemplo:

$3 \equiv 24 \pmod{7}$, então $7 \mid (3-24)$

$-31 \equiv 11 \pmod{6}$, então $6 \mid (-31-11)$

$-15 \equiv -63 \pmod{8}$, então $8 \mid (-15-(-63))$

Congruências

- Proposição:

Se a ≡ b (mod m) $então$ m | (a-b)

- Demonstração:

Se a ≡ b (mod m) , então

$$a = mq_1 + r_1$$

$$b = mq_2 + r_2$$

a ≡ b (mod m), então $r_1 = r_2$

$(a-b) = mq_1 + r_1 - mq_2 - r_2 = m(q_1 - q_2)$

Incongruências

- Se $m \nmid (a-b)$, então diz-se que *a é incongruente a b módulo m*, o que se indica pela notação:

$$a \not\equiv b \pmod{m}$$

Exemplos:

- $25 \not\equiv 12 \pmod{7}$, porque $7 \nmid (25-12)$
- $-21 \not\equiv 10 \pmod{5}$, porque $5 \nmid (-21-10)$

Exercício

- Mostrar que:

Se $n \equiv 7 \pmod{12}$, então $n \equiv 3 \pmod{4}$

Demonstração:

- Se $n \equiv 3 \pmod{4}$, então $4 \mid (n-3)$, ou seja, $(n-3) = 4k$
- Se $n \equiv 7 \pmod{12}$, então $12 \mid (n-7)$, ou seja, $(n-7) = 12k$

$$n-7 = 12k$$

$$n-7+4 = 12k+4$$

$$n-3 = 4(3k+1)$$

Propriedades

1. $a \equiv a \pmod{m}$ **(reflexiva)**
2. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$ **(simétrica)**
3. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ então $a \equiv c \pmod{m}$ **(transitiva)**

Exercício

- Achar o menor inteiro positiva que representa a soma:

a) (5 + 3 + 2 + 1 + 8) mod 7

Resposta: 5

b) (2 + 3 – 1 + 7 – 2) mod 4

Resposta. 1

c) (2 . 3 . 5 . 7 . 121) mod 4

Resposta. 2

d) $(3^2 + 5^{10})$ mod 4

Resposta. 2

Exercício

- Encontre o resto da divisão de 2^{56} por 7

Temos que

- $2^1 \equiv 2 \bmod 7$
- $2^2 \equiv 4 \bmod 7$
- $2^3 \equiv 1 \bmod 7$
- $2^4 \equiv 2 \bmod 7$
- $2^5 \equiv 4 \bmod 7$
- $2^6 \equiv 1 \bmod 7$

- Dessa forma, podemos reescrever:
  $2^{56} = 2^2 . 2^{54} = 2^2 . (2^3)^{18} = 4.1 =$ **4**

Exercício

- Encontre o resto da divisão de 2^{56} por 11

- Temos que
- $2^1 \equiv 2 \bmod 11$
- $2^2 \equiv 4 \bmod 11$
- $2^3 \equiv 8 \bmod 11$
- $2^4 \equiv 5 \bmod 11$
- $2^5 \equiv 10 \bmod 11$
- $2^6 \equiv 9 \bmod 11$
- $2^7 \equiv 7 \bmod 11$
- $2^8 \equiv 3 \bmod 11$
- $2^9 \equiv 6 \bmod 11$
- $2^{10} \equiv 1 \bmod 11$

- Temos que $2^{56} = 2^6 . 2^{50} = 2^6 . (2^{10})^5 = 9.1 = 9$

Exercício

- Encontre o resto da divisão de 3^8 por 13

- Temos que
- $3^1 \equiv 3 \bmod 13$
- $3^2 \equiv 9 \bmod 13$
- $3^3 \equiv 1 \bmod 13$

- Logo, temos que $3^8 = 3^3 . 3^3 . 3^2 = 1.1.9 = 9$

Exercício

- Sabendo-se que $k \equiv 1 \bmod 4$, mostrar que:

$6k + 5 \equiv 3 \bmod 4$

Solução:

Se $k \equiv 1 \pmod 4$ então $k = 4n + 1$

$6k + 5 = 6(4n + 1) + 5 = 24n + 6 + 5 = 24n + 8 + 3 =$

$\mathbf{4(6n + 2) + 3}$

Temos que $6k + 5$ deixa resto 3 na divisão por 4.

Portanto: $6k + 5 \equiv 3 \bmod 4$

Exercício

- Mostrar que:

$a)\ 41 \mid 2^{20} - 1$

$b)\ 89 \mid 2^{44} - 1$

$c)\ 97 \mid 2^{48} - 1$

Exercício

- Para verificar se o número de um CPF é válido, fazemos os seguintes cálculos

Suponha que o CPF seja dado por:

$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 v_1 v_2$

1° passo: verificar se

$v_1 = 11 - ((\sum_{i=1}^{9}(11 - i) * a_i) \bmod 11)$

Se o resultado da subtração for maior que 9, o dígito verificador é ZERO

2° passo: verificar se

$v_2 = 11 - (((\sum_{i=1}^{9}(12 - i) * a_i) + (v_1 * 2)) \bmod 11)$

Se o resultado da subtração for maior que 9, o dígito verificador é ZERO