Introdução à Aritmética Modular

George Darmiton da Cunha Cavalcanti
CIn - UFPE

Introdução

- Em alguns problemas o interesse se concentra no resto da divisão entre dois números, por exemplo
  - Que horas serão daqui a 50 horas?
  - Nesse caso, nosso interesse reside no resto da divisão entre 50 e 24 horas.

- Para esses casos, existe uma notação própria para indicar quando dois inteiros possuem o mesmo resto, quando divididos por um inteiro positivo.

Definição

- Se ***a*** e ***b*** são inteiros e ***m*** é um inteiro positivo, então ***a*** é ***congruente*** com ***b modulo m*** se ***m*** divide ***a–b***.

- Notação
  - ***a≡b (mod m)***
  - Para indicar que ***a*** é congruente com ***b*** módulo ***m***

Exemplo

Ache o menor inteiro não negativo que é congruente módulo 8, para os seguintes números:

(a) 379	3
(b) 695	7
(c) -578	6
(d) -285	3

Exemplo

Determine se 17 é congruente com 5 módulo 6 e se 24 e 14 são congruentes módulo 6.

Dado que 6 divide 17-5 = 12, podemos dizer que $17 \equiv 5 \pmod 6$.

Enquanto que 24-14 = 10 não é divisível por 6, podemos relatar que $24 \not\equiv 14 \pmod 6$

Exemplo

Se $x \equiv 1 \ (\textbf{mod}\ 3)$, encontre uma expressão para x na forma x = _____.

$x = 3k + 1, k = 0, \pm 1, \pm 2, \pm 3, \ldots$

Teorema

Sejam ***a*** e ***b*** dois inteiros, e **m** um inteiro positivo. Então ***a≡b (mod m)*** se e somente se ***a mod m = b mod m***

Exemplo

Ache os números entre 1 e 100 que são congruentes a 6 módulo 13.

$1 \leq x \leq 100$ e $x \equiv 6$ (**mod** 13)

6+0=6 6+13=19 19+13=32 ...

6, 19, 32, 45, 58, 71, 84, 97

Exemplo

Ache os números entre -50 e 50 que são congruentes a 21 módulo 12.

$-50 \leq x \leq 50$ e $x \equiv 21$ (**mod** 12)

21+0=21 21+12=33 33+12=45

21-12=9 9-12=-3 ...

-39, -27, -15, -3, 9, 21, 33, 46

Teorema

Seja ***m*** um inteiro positivo. Os inteiros ***a*** e ***b*** são congruentes módulo ***m*** se e somente se existe um inteiro ***k*** de forma que $a = b + km$.

Classe de congruência de *a módulo m*

É definida como o conjunto de todos os inteiros congruentes com ***a*** módulo ***m***.

Exemplo

Classe de congruência *módulo m*

Se *m=3*, então existem três classes que contém o mesmo resto

$\overline{0}$ = {..., -9, -6, -3, 0, 3, 6, 9, ...}
$\overline{1}$ = {..., -8, -5, -2, 1, 4, 7, 10, ...}
$\overline{2}$ = {..., -7, -4, -1, 2, 5, 8, 11, ...}

Exemplo

Classe de congruência *módulo m*

Os elementos da classe $\bar{0}$ são da forma

3k

Os elementos da classe $\bar{1}$ são da forma

3k+1

Os elementos da classe $\bar{2}$ são da forma

3k+2

Exemplo

Quantas classes de congruência é possível construir quando ***m*** for igual a:

a) 12?

b) 35?

c) n?

Teorema

Seja *m* um inteiro positivo. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ então

$a+c \equiv b+d \pmod{m}$ e $ac \equiv bd \pmod{m}$

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

Exemplo

Se $7 \equiv 2 \pmod 5$ e $11 \equiv 1 \pmod 5$, então pelo teorema anterior

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$$

$$77 = 7 \times 11 \equiv 2 \times 1 = 2 \pmod 5$$

Aplicações de Congruência

- Endereçamento de memória
- Geração de números pseudo-aleatórios
- Criptografia

Exemplo
Endereçamento de memória

- O computador da faculdade mantém registros de todos os estudantes.
- Como endereçar os registros a fim de recuperar as informações dos estudantes?

- Para acessar os registros uma chave é necessária.
- Uma função *h(k)* mapeia uma posição de memória para um registro que possui chave *k*.

Exemplo
Endereçamento de memória

- Uma função comum para realizar essa tarefa pode ser
  - ***h(k) = k mod m***

- Sabendo que ***m*** é o número de posições de memória disponíveis

- Supondo que ***m*** = 111
- h(064212848) = 064212848 ***mod*** 111 = 14
- h(037149212) = 037149212 ***mod*** 111 = 65

- Problemas de colisões
- h(107405723) = 107405723 ***mod*** 111 = 14

Exemplo
Geração de números pseudo-aleatórios

É possível gerar um seqüência de números pseudo-aleatórios $\{x_n\}$ com $0 \leq x_n < m$ para todo n com

$$x_{n+1} = (ax_n + c) \bmod m$$

$2 \leq a < m$ $\quad$ $0 \leq c < m$ $\quad$ $0 \leq x_0 < m$

Exemplo
Geração de números pseudo-aleatórios

$m = 9, \quad a = 7, \quad c = 4 \quad \text{e} \quad x_0 = 3$

$$
\begin{aligned}
x_1 &= 7x_0 + 4 = 7 \cdot 3 + 4 = 25 \bmod 9 = 7,\\
x_2 &= 7x_1 + 4 = 7 \cdot 7 + 4 = 53 \bmod 9 = 8,\\
x_3 &= 7x_2 + 4 = 7 \cdot 8 + 4 = 60 \bmod 9 = 6,\\
x_4 &= 7x_3 + 4 = 7 \cdot 6 + 4 = 46 \bmod 9 = 1,\\
x_5 &= 7x_4 + 4 = 7 \cdot 1 + 4 = 11 \bmod 9 = 2,\\
x_6 &= 7x_5 + 4 = 7 \cdot 2 + 4 = 18 \bmod 9 = 0,\\
x_7 &= 7x_6 + 4 = 7 \cdot 0 + 4 = 4 \bmod 9 = 4,\\
x_8 &= 7x_7 + 4 = 7 \cdot 4 + 4 = 32 \bmod 9 = 5,\\
x_9 &= 7x_8 + 4 = 7 \cdot 5 + 4 = 39 \bmod 9 = 3.
\end{aligned}
$$

A seqüência gerada é: 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,...

Exemplo
Geração de números pseudo-aleatórios

A seqüência apresentada contém nove números diferentes antes de se repetir.

Supondo ***c=0***, o gerador multiplicativo de forma que $m = 2^{31}-1$ e $a = 16.807$ gerará $2^{31}-2$ números antes de repetir.

Exemplo
Criptografia

- Expressar a encriptação de *Julio Cesar* como um processo matemático.
- Cada letra será representada por um número
  - A por 0; K por 10 e Z por 25.

- $f(p) = (p+3)$ **mod** 26

- $p \leq 25, f(p) \in \{0,1,2,...,25\}$

Exemplo
Criptografia

Qual é a mensagem secreta produzida pela mensagem?

- MEET YOU IN THE PARK

Primeiro passo

- Trocar letras por números
- 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

Segundo passo

- Trocar cada número *p* por $f(p) = (p+3)$ ***mod*** *26*
- 15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13

Terceiro passo

- Trocar cada número *p* por uma letra
- PHHW BRX LQ WKH SDUN

Exemplo
Criptografia

Para recuperar a mensagem original é necessária a função inversa de *f*, f^{-1}

$f^{-1}(p) = (p-3)$ **mod** 26.

De maneira geral,

$f(p) = (p+k)$ **mod** 26. *(codificador)*

$f^{-1}(p) = (p-k)$ **mod** 26. *(decodificador)*

Exemplo

- Livros são identificados por um número ISBN (*International Standard Book Number*), um código de 10 dígitos $x_1x_2...x_{10}$. Esses números identificam a linguagem, a editora, o número do livro e um dígito de verificação.

- Esse dígito de verificação é selecionado de forma que $\Sigma_{i=1:10}\, ix_i \equiv 0$ (***mod*** *11)*

- Os primeiros 9 dígitos são 0-07-053965. Qual é o dígito verificador para esse livro?