

# INE5403 - Fundamentos de Matemática Discreta para a Computação

## 2) Fundamentos

2.1) Conjuntos e Sub-conjuntos

2.2) **Números Inteiros**

2.3) Funções

2.4) Seqüências e Somas

2.5) Crescimento de Funções

# Divisão nos Números Inteiros

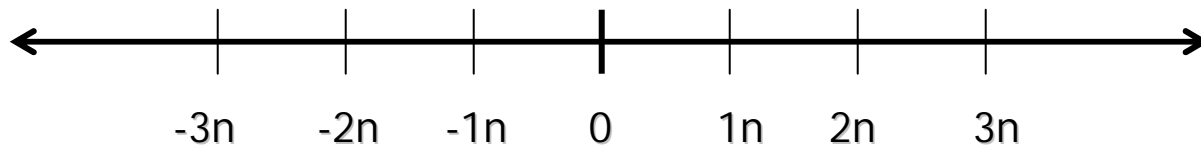
- Este tópico está relacionado à Teoria de Números.
  - Números inteiros e suas propriedades.
- Veremos conceitos básicos de Teoria de Números, incluindo divisibilidade, máximos divisores comuns e aritmética modular.
- Noções básicas: divisibilidade e números primos.
- Aplicações de aritmética modular:
  - geração de números pseudo-aleatórios
  - alocações de memória computacional
  - criptografia

# Divisão nos inteiros

- Quando um inteiro é dividido por um 2º inteiro não-nulo, o quociente pode ou não ser um inteiro.
  - Exemplo:  $12/3 = 4$  é um inteiro  
 $11/4 = 2.75$  não é
- Se a e b são inteiros com  $a \neq 0$ , dizemos que a ***divide*** b se existe um inteiro c tal que  $b=a.c$ 
  - quando a divide b, dizemos que a é um fator de b e que b é um múltiplo de a
  - a divide b é denotado por  $a \mid b$
  - escrevemos  $a \nmid b$  se a não divide b
  - Exemplo:  $3 \nmid 7$  e  $3 \mid 12$

# Divisão nos inteiros

- **Ilustração**: inteiros divisíveis pelo inteiro positivo  $n$ :



# Divisão nos inteiros

**Teorema**: Sejam  $a$ ,  $b$  e  $c$  números inteiros. Então:

1. Se  $a|b$  e  $a|c$ , então  $a|(b+c)$ .

Exemplo:  $7|14$  e  $7|21$ , então  $7|35$

2. Se  $a|b$ , então  $a|b.c$ , para qualquer inteiro  $c$ .

Exemplo:  $3|6$ , então  $3|54$

3. Se  $a|b$  e  $b|c$ , então  $a|c$ .

Exemplo:  $5|15$  e  $15|45$ , então  $5|45$

# Divisão nos inteiros

## Teorema (cont.):

Prova de 1: “se  $a|b$  e  $a|c$  então  $a|(b+c)$ ”.

- Se  $a|b$  e  $a|c$ , então, da definição de divisibilidade, existem inteiros  $s$  e  $t$  tais que  $b=a.s$  e  $c=a.t$
- Portanto:  $b+c = a.s + a.t = a.(s+t)$
- Logo:  $a$  divide  $b+c$  □

# Números primos

- Um inteiro positivo  $> 1$  é chamado de ***primo*** se os únicos fatores positivos de  $p$  são 1 e  $p$ .
  - um inteiro positivo  $> 1$  que não é *primo* é chamado de *composto*.

Exemplo: 7 é primo (fatores 1 e 7)

9 é composto (divisível por 3)

- Utilidade dos números primos: servem de ***base*** para a construção de números inteiros.

# Números primos

## Teorema Fundamental da Aritmética:

“Todo inteiro positivo  $n$  pode ser escrito de maneira única como o *produto de números primos*, onde os fatores primos são escritos em ordem crescente de grandeza”.

- **Exemplo:** as fatorações de 100, 641, 999 e 1024 em números primos são dadas por:

$$100 = 2.2.5.5 = 2^2 5^2$$

$$641 = 641$$

$$999 = 3.3.3.37 = 3^3 37$$

*Note que o fator primo pode aparecer mais do que uma vez*



# Números primos

- É frequentemente importante mostrar que um dado inteiro é primo.
  - por exemplo, em Criptografia números primos grandes são usados em alguns métodos para tornar secretas as mensagens.
- Como fazer?
- Um procedimento para mostrar que um dado inteiro é primo é baseado no teorema a seguir.

# Números primos

**Teorema:** "Se  $n$  é um inteiro composto, então  $n$  tem um divisor primo  $\leq \sqrt{n}$ ".

**Prova:**

- se  $n$  é composto, ele tem um fator  $1 < a < n$
- logo,  $n = a \cdot b$ , sendo  $a$  e  $b$  inteiros positivos  $> 1$
- note que: ou  $a \leq \sqrt{n}$  ou  $b \leq \sqrt{n}$   
(senão ocorreria  $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$ )
- ou seja: com certeza,  $n$  tem pelo menos um divisor positivo que não excede  $\sqrt{n}$
- por sua vez, este divisor ou é primo ou, pelo Teor. Fund. da Aritmética, tem um divisor primo.
- em ambos os casos fica garantido que  $n$  tem que ter um divisor primo  $\leq \sqrt{n}$

# Números primos

- Conclusão: o teorema mostra que um inteiro é primo se ele não for divisível por nenhum primo  $\leq$  à sua raiz quadrada.

- **Exemplo:** Mostre que 101 é primo.

## **Solução:**

- os únicos primos que não excedem  $\sqrt{101}$  são 2,3,5 e 7
  - como 101 não é divisível por nenhum deles (o quociente não é inteiro), 101 é primo.
- Pelo que foi visto até agora, sabe-se que todo inteiro tem uma *fatoração* em números primos.
  - Procedimento para obter os fatores?

# Fatoração em primos

1. Comece dividindo  $n$  por sucessivos primos, a partir de 2
  - se  $n$  tiver um fator primo, um fator primo  $\leq \sqrt{n}$  deve ser encontrado
  - se nenhum primo  $\leq \sqrt{n}$  for encontrado,  $n$  é ele próprio primo (FIM).
2. Se um fator primo  $p$  for encontrado, fatore  $n/p$ 
  - note que  $n/p$  não tem fatores primos  $< p$
3. Se  $n/p$  não tiver um fator primo que seja  $\geq p$  e  $\leq \sqrt{n/p}$ , ele mesmo é primo (FIM).
4. Senão,  $n/p$  deverá ter o seu fator primo  $q$ :
  - procure a fatoração de  $n/(p.q)$
5. Repetir o procedimento até que a fatoração tenha sido reduzida a um primo.

# Fatoração em primos

**Exemplo:** Encontre a fatoração de 7007.

**Solução:** Realizar divisões com primos sucessivos:

1. 7 divide 7007, pois  $7007/7 = 1001$
2. 7 divide também 1001, pois  $1001/7 = 143$
3. Continuamos dividindo 143 por primos sucessivos (*podemos começar por 7*):
  - o 7 não divide 143, mas o próximo primo, 11, divide:  $143/11 = 13$
  - como 13 é primo, o procedimento está completo.
4. Logo:  $7007 = 7^2 \cdot 11 \cdot 13$

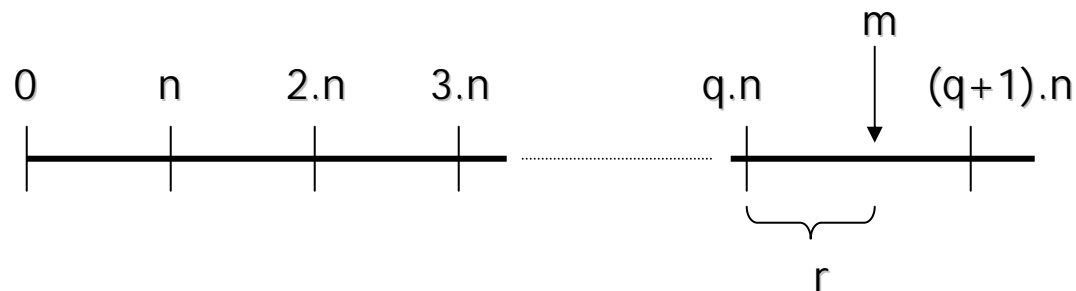
# Algoritmo para a divisão de inteiros

- Um inteiro pode ou não ser divisível por outro.
- Quando um inteiro é dividido por um inteiro positivo, sempre há um *quociente* e um *resto*.
- **O algoritmo da divisão:** sejam  $m$  um inteiro e  $n$  um inteiro positivo. Então há inteiros únicos  $q$  e  $r$ , com  $(0 \leq r < n)$ , tais que:

$$m = q.n + r$$

# Algoritmo para a divisão de inteiros

- Ilustração: se  $m$  não é múltiplo de  $n$ , a sua localização na reta dos múltiplos de  $n$  é:
  - seja  $q.n$  o 1º múltiplo de  $n$  à esquerda de  $m$ :



- então  $r$  é a distância de  $q.n$  até  $m$ , de modo que:

$$0 \leq r < n \quad \text{e} \quad m = q.n + r$$

**Definição:**  $n$  é o divisor,  $m$  é o dividendo,  $q$  é o quociente e  $r$  é o resto.

# Algoritmo para a divisão de inteiros

- **Exemplo:** quais são o quociente e o resto quando 101 é dividido por 11?
- **Solução:**  $101 = 11 \times 9 + 2$      $q=9$      $r=2$
- **Exemplo:** quais são o quociente e o resto quando -11 é dividido por 3?
- **Solução:**  $-11 = 3 \times (-4) + 1$
- **Questão:** por que não se pode escrever:  
 $-11 = 3 \times (-5) + 4$  ?    *ou:*  
 $-11 = 3 \times (-3) - 2$  ?
- Note que o inteiro  $m$  é divisível por  $n$  se e somente se o resto é zero quando  $m$  é dividido por  $n$ .



# Máximo Divisor Comum

- É o maior inteiro que divide 2 inteiros ao mesmo tempo.

**Definição:** Sejam  $a$  e  $b$  inteiros, com pelo menos um dos dois não-nulo. O maior inteiro  $d$  tal que  $d|a$  e  $d|b$  é chamado de máximo divisor comum de  $a$  e  $b$  e é denotado  $\text{MDC}(a,b)$ .

- Em notação matemática:

$$\text{MDC}(a,b) = \max\{d \mid d|a \wedge d|b\}$$

- Uma forma de encontrar o MDC de 2 inteiros é encontrar todos os divisores positivos comuns de ambos os inteiros e pegar o maior.
- Exemplo:  $\text{MDC}(24,36) = \max\{1,2,3,4,6,12\} = 12$   
 $\text{MDC}(17,22) = \max\{1\} = 1$

# Máximo Divisor Comum

- Os inteiros  $a$  e  $b$  são *primos entre si* se o seu máximo divisor comum é igual a 1.
- **Exemplo:** 17 e 22 são primos entre si pois  $\text{MDC}(17,22)=1$ .
- Os inteiros  $a_1, a_2, \dots, a_n$  são *2 a 2 primos entre si* se  $\text{MDC}(a_i, a_j)=1$ , para  $1 \leq i < j \leq n$ .
- **Exemplo:** Verifique se são 2 a 2 primos entre si os inteiros 10, 17 e 21 e também os inteiros 10, 19 e 24.
- **Solução:**
  - $\text{MDC}(10,17)=1$ ,  $\text{MDC}(10,21)=1$  e  $\text{MDC}(17,21)=1$  ✓
  - Como  $\text{MDC}(10,24)=2 > 1$ , os inteiros 10, 19 e 24 *não são* 2 a 2 primos entre si.

# Método para o cálculo do MDC:

- Pode-se utilizar as fatorações em números primos dos inteiros positivos  $a$  e  $b$ :

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

- onde os  $p_i$ 's são os primos que são fatores de  $a$  e/ou  $b$  (os mesmos)

- Então o  $MDC(a,b)$  pode ser calculado como:

$$MDC(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

- **Exemplo:**  $MDC(60,18)=?$

$$\begin{cases} 60=2^2 \cdot 3^1 \cdot 5^1 \\ 18=2^1 \cdot 3^2 \end{cases}$$

$$\rightarrow MDC(60,18)=2^1 \cdot 3^1 \cdot 5^0=6$$

# Cálculo do MDC (algoritmo de Euclides)

**Exemplo:** calcule o  $\text{MDC}(91,287)$ .

- Dividir 287 por 91, obtendo:  $287 = 91 \cdot 3 + 14$ 
  - note que todo divisor de 91 e 287 deve ser divisor de:  
 $287 - 91 \cdot 3 = 14$
  - por outro lado, todo divisor de 91 e 14 deve ser divisor de:  
 $287 = 91 \cdot 3 + 14$
  - logo,  $\{287, 91 \text{ e } 14\}$  têm os mesmos divisores e:  
 $\text{MDC}(91,287) = \text{MDC}(91,14)$
- Próximo passo: dividir 91 por 14, obtendo:  $91 = 14 \cdot 6 + 7$
- Em seguida:  $14 = 7 \cdot 2$
- Como 7 divide 14, segue que  $\text{MDC}(14,7) = 7$
- Logo  $\text{MDC}(287,91) = \text{MDC}(91,14) = \text{MDC}(14,7) = 7$  .

# Cálculo do MDC (algoritmo de Euclides)

- **Resumo:**
  - aplicar o algoritmo da divisão sucessivas vezes
  - o MDC procurado é o último resto não-nulo das divisões
- **Exemplo:** Encontre o MDC de 414 e 662 usando o algoritmo de Euclides.

**Solução:**

$$\begin{aligned}662 &= 414 \times 1 + 248 \\414 &= 248 \times 1 + 166 \\248 &= 166 \times 1 + 82 \\166 &= 82 \times 2 + 2 \\82 &= 2 \times 41\end{aligned}$$

- Logo,  $\text{MDC}(662,414)=2$ , pois 2 é o último resto não-nulo.

# O algoritmo de Euclides

- Em pseudocódigo:

```
function MDC(a,b)
```

```
  x:=a
```

```
  y:=b
```

```
  while y  $\neq$  0
```

```
    r:=x mod y
```

```
    x:=y
```

```
    y:=r
```

```
  end
```

```
{MDC(a,b) é o valor de x}
```

# Mínimo Múltiplo Comum

- O **mínimo múltiplo comum** dos inteiros positivos  $a$  e  $b$  é o menor inteiro positivo que é divisível tanto por  $a$  como por  $b$ .
  - É denotado por  $\text{MMC}(a,b)$ .

- Em notação matemática:

$$\text{MMC}(a,b) = \min\{k \mid a|k \wedge b|k\}$$

- **Exemplo:**

$$\text{MMC}(12,18) = 36$$

# Método para o cálculo do MMC:

- Também pode vir das fatorações em números primos dos inteiros positivos a e b:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

onde os  $p_i$ 's são fatores de a e/ou b (os mesmos primos).

- Então o MMC(a,b) pode ser calculado como:

$$MMC(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}$$

- **Exemplo:**  $MMC(95256,432)=?$

$$\begin{cases} 95256 = 2^3 \cdot 3^5 \cdot 7^2 \\ 432 = 2^4 \cdot 3^3 \end{cases} \rightarrow MMC(95256,432) = 2^4 \cdot 3^5 \cdot 7^2$$



# MDC e MMC

- **Teorema:** Sejam a e b inteiros positivos. Então:

$$a \cdot b = \text{MDC}(a,b) \cdot \text{MMC}(a,b)$$

**Prova:** ?

- **Exemplo:** Sejam  $a=540$ ,  $b=504$

**Solução:**  $540 = 2^2 \cdot 3^3 \cdot 5^1$

$$504 = 2^3 \cdot 3^2 \cdot 7^1$$

$$\text{MDC}(2^2 \cdot 3^3 \cdot 5^1, 2^3 \cdot 3^2 \cdot 7^1) = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 = 36$$

$$\text{MMC}(2^2 \cdot 3^3 \cdot 5^1, 2^3 \cdot 3^2 \cdot 7^1) = 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^1 = 7560$$

$$540 \cdot 504 = 272140 = 36 \times 7560 \quad \checkmark$$

# Aritmética Modular

- Em muitas situações estamos interessados apenas no resto da divisão de um inteiro por outro.
- Por exemplo, quando perguntamos “que horas serão daqui a 50 horas”, o que nos interessa é apenas o resto quando “50 + hora atual” é dividido por 24.
  - Exemplo: hora atual = 20:00  
hora daqui a 50 horas = resto de  $70/24 = 22:00$
- Como o que nos interessa em muitas situações são apenas os restos, temos notações especiais para eles.

# Aritmética modular

- Seja  $a$  um inteiro e  $m$  um inteiro positivo. Denota-se por  $a \bmod m$  o resto que é obtido quando  $a$  é dividido por  $m$ .

– segue desta definição que  $a \bmod m$  é o inteiro  $r$  tal que  $a = q \cdot m + r$  e  $0 \leq r < m$

- **Exemplo:**

$17 \bmod 5 = 2$	$(17 = 3 \times 5 + 2)$
$-133 \bmod 9 = 2$	$(-133 = -15 \times 9 + 2)$
$2001 \bmod 101 = 82$	$(2001 = 19 \times 101 + 82)$

# Aritmética modular e congruência

- Existe também uma notação para indicar que 2 inteiros têm o mesmo resto quando divididos por um mesmo inteiro  $m$ .

- Se  $a$  e  $b$  são inteiros e  $m$  é um inteiro positivo, então  $a$  é dito ser *congruente a  $b$  módulo  $m$*  se  $m$  divide  $a-b$  ( $m|(a-b)$ ).

- usa-se a notação  $a \equiv b \pmod{m}$

- se  $a$  e  $b$  *não são* congruentes módulo  $m$ , escreve-se:  
 $a \not\equiv b \pmod{m}$

- Observe que  $a \equiv b \pmod{m}$  se e somente se:  
 $a \bmod m = b \bmod m$

# Aritmética modular e congruência

- **Exemplo:** Determine se 17 é congruente a 5 módulo 6 e também se 24 e 14 são congruentes módulo 6.

## Solução:

$6 \mid (17-5)$ , pois  $17-5 = 12$ , logo:  $17 \equiv 5 \pmod{6}$

$24-14=10$ , mas  $6$  *não divide* 10, logo:  $24 \not\equiv 14 \pmod{6}$

- Os teoremas a seguir indicam maneiras úteis de se trabalhar com congruências.

# Aritmética modular e congruência

- **Teorema:** Seja  $m$  um inteiro positivo. Os inteiros  $a$  e  $b$  são *congruentes módulo  $m$*  se e somente se existe um inteiro  $k$  tal que

$$a = b + k.m$$

**Prova:**

- 1) se  $a \equiv b \pmod{m}$ , então  $m \mid (a-b)$   
 $\Rightarrow$  existe um inteiro  $k$  tal que  $a-b=k.m$   
 $\Rightarrow a=b+k.m$

- 2) conversamente:

- se existe um inteiro  $k$  tal que  $a=b+k.m$ , então  $k.m=b-a$   
 $\Rightarrow m$  divide  $a-b$   
 $\Rightarrow a \equiv b \pmod{m}$

# Aritmética modular e congruência

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

$$\begin{cases} a+c \equiv b+d \pmod{m} \\ a.c \equiv b.d \pmod{m} \end{cases}$$

**Prova:** como  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ , há inteiros  $s$  e  $t$  com  
 $b = a + s.m$  e  $d = c + t.m$

- $b+d = (a+s.m) + (c+t.m) = (a+c) + (s+t).m$   
 $\Rightarrow a+c \equiv b+d \pmod{m} \quad \checkmark$
- $b.d = (a+s.m).(c+t.m) = a.c + (a.t + c.s + stm).m$   
 $\Rightarrow a.c \equiv b.d \pmod{m} \quad \checkmark$

# Aritmética modular e congruência

- **Exemplo:** Como  $7 \equiv 2 \pmod{5}$  e  $11 \equiv 1 \pmod{5}$ , o teorema anterior garante que:
  - $7 + 11 \equiv 2 + 1 \pmod{5}$ , ou seja,  
 $18 \equiv 3 \pmod{5}$
  - $7 \cdot 11 \equiv 2 \cdot 1 \pmod{5}$ , ou seja,  
 $77 \equiv 2 \pmod{5}$



# Aplicações da aritmética modular

- Criptologia: há um grande número de técnicas baseadas em aritmética modular para criptografar blocos de letras.
- Uma das mais antigas é o chamado “cifrador de César”:  
a b c d e f g h i j k l m n o p q r s t u v w x y z  
d e f g h i j k l m n o p q r s t u v w x y z a b c
- Para expressar este processo matematicamente, atribui-se um número inteiro entre 0 e 25 para cada letra:  
- por exemplo, substitui-se “a” por 0, “k” por 10, ...
- O cifrador de César pode ser representada pela função:  
$$f(p) = (p + 3) \bmod 26$$
  
onde  $p$  é um inteiro entre 0 e 25.

# Aplicações da aritmética modular

- **Exemplo:** Use o cifrador de César para criptografar a mensagem "REUNIAO NO SAGUAO DO CTC".

1) Primeiro substituir letras por números:

"17 4 20 13 8 0 14 13 14 18 0 6 20 0 14 3 14 2 19 2"

2) Substituir estes números usando  $f(p) = (p+3) \bmod 26$ :

"20 7 23 16 11 3 17 16 17 21 3 9 23 3 17 6 17 5 22 5"

3) O que fornece a seguinte mensagem criptografada:

"UHXQLDRQRVDJXDRGRFWF"

4) Para "decriptografar" esta mensagem, basta atribuir números de 0 a 25 às letras e substituir estes números por:

$$f^{-1}(p) = (p-3) \bmod 26$$

# Aplicações da aritmética modular

## Aritmética computacional com números grandes:

- Sejam  $m_1, m_2, \dots, m_n$  primos 2 a 2 e seja  $m$  o seu produto.
- Pode-se mostrar que qualquer inteiro  $a$ , com  $0 \leq a < m$  pode ser representado de maneira única apenas com os restos das suas divisões por  $m_1, m_2, \dots, m_n$ .
- Ou seja, podemos representar  $a$  por:  
( $a \bmod m_1, a \bmod m_2, \dots, a \bmod m_n$ )

# Aplicações da aritmética modular

- **Exemplo:** Suponha que em um certo processador é muito mais rápido realizar cálculos com inteiros  $< 100$  do que com inteiros maiores.
- Podemos nos restringir a cálculos com inteiros  $< 100$  utilizando aritmética modular com os restos destes inteiros módulo 99, 98, 97 e 95 (primos 2 a 2 entre si).
  - isto nos permitiria representar qualquer inteiro entre 0 e  $99 \times 98 \times 97 \times 95 (= 89403930)$ .

# Aplicações da aritmética modular

- **Exemplo (continuação):**
- Exemplo numérico:
  - 123684 pode ser representado por  $(33,8,9,89)$
  - 413456 pode ser representado por  $(32,92,42,16)$
- Se quisermos obter a soma "123684 + 413456", é só somar as suas componentes:
  - "123684+ 413456" pode ser representado por:  
 $(33,8,9,89) + (32,92,42,16) = (65,2,51,10)$
- Podemos continuar sempre com aritmética modular.
  - para recuperar o resultado, temos que resolver:  
 $x \equiv 65 \pmod{99}$   
 $x \equiv 2 \pmod{98}$   
 $x \equiv 51 \pmod{97}$   
 $x \equiv 10 \pmod{95}$                        $x=?$