INE5403 - Fundamentos de Matemática Discreta para a Computação

2) Números Inteiros

- Divisão nos Inteiros
- Números Primos
- Inteiros e Algoritmos
- Aplicações

Divisão nos Números Inteiros

- Este tópico está relacionado à *Teoria de Números*.
  - Números inteiros e suas propriedades.

- Veremos conceitos básicos de Teoria de Números:
  - divisibilidade, mdcs 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.
  - <u>Exemplo</u>: 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

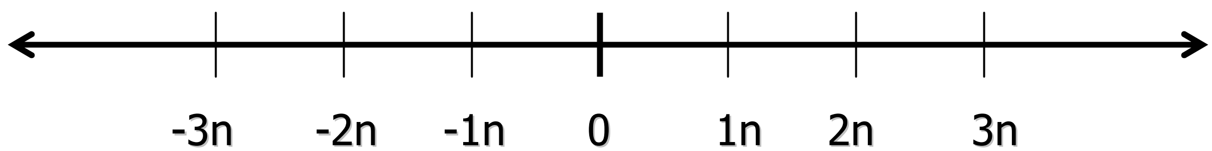
  - a *divide* b é denotado por $a \mid b$

  - escrevemos $a \nmid b$ se a *não divide* b

  - <u>Exemplo</u>: $3 \nmid 7$ 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

<u>Teorema</u> (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

<u>Teorema Fundamental da Aritmética</u>:

"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:

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

$$641 = 641$$

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

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 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, $n=a.b$, sendo a e b inteiros positivos > 1
- note que: ou $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$
  (senão ocorreria $a.b > \sqrt{n} . \sqrt{n} = n$)
- 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: 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).

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

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).

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: $7007 = 7^2.11.13$

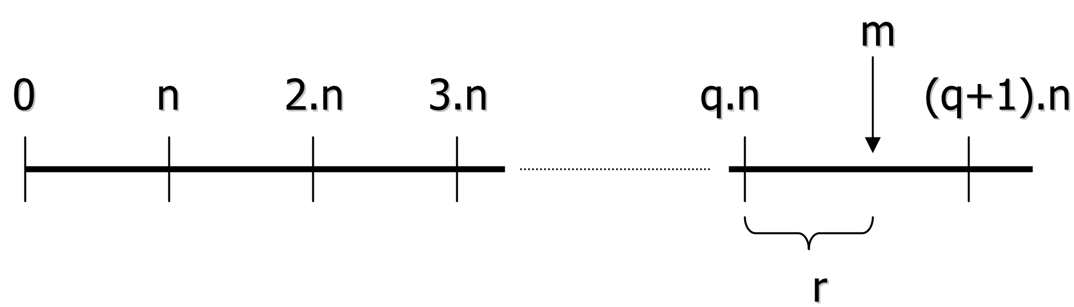
Algoritmo para a divisão de inteiros

- 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:

$$\mathbf{m = q.n + r}$$

Algoritmo para a divisão de inteiros

- Se m não é múltiplo de n, a sua localização na reta dos múltiplos de n é dada por:
  - 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:

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

- 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 <u>*divisível*</u> 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.
- O maior inteiro d tal que $d|a$ e $d|b$ é chamado de **máximo divisor comum** de a e b e é denotado MDC(a,b).
- Em notação matemática:

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

- 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**: MDC(24,36) = max{1,2,3,4,6,12} = 12
  MDC(17,22) = max{1} = 1

Máximo Divisor Comum

- O MDC(a,b) tem algumas propriedades interessantes:
  - ele pode ser escrito como uma combinação de a e b
  - não é apenas “maior do que” todos os outros divisores:
    - é sempre um múltiplo de cada um deles

Máximo Divisor Comum

- **Teorema**: Se d é o MDC(a,b), então:

  (a) $d = s.a + t.b$ para alguns inteiros s e t

  (b) se c é qualquer outro divisor de a e b, então $c \mid d$

- **Prova**:
  - Seja x o menor inteiro positivo que pode ser escrito como $s.a+t.b$
  - Seja c um divisor comum de a e de b
  - Já que $c|a$ e $c|b$, então $c|x$
    - de modo que $c \leq x$
  - Se pudermos provar que x é um divisor comum de a e de b:
    - ele será o maior divisor comum de a e de b.

Máximo Divisor Comum

- **Teorema**:

  (a) MDC(a,b) = d = s.a + t.b

  (b) d é divisível por qualquer outro divisor de a e b

- **Prova (cont.)**:
  - Sabemos que: $a = q.x+r$, para $0 \leq r < x$
    - Então: $r = a-q.x = a-q.(s.a + t.b)$

      $= a-q.s.a-q.t.b = (1-q.s).a + (-q.t).b$
  - Se r não for 0, então:
    - já que r<x,
    - e já que r é a soma de um múltiplo de a e um de b,

    teremos uma contradição para:
    - "x é o menor positivo que é a soma de múltiplos de a e de b"
  - Portanto, r deve ser zero e x|a
  - Do mesmo modo, mostra-se que x|b. □

Máximo Divisor Comum

- Conseqüência:
  - Sejam a, b e d $\in Z^+$
  - O inteiro d é o MDC de a e de b sse:
    - $d|a$ e $d|b$
    - sempre que $c|a$ e $c|b$, então $c|d$.

Máximo Divisor Comum

- **Exemplo**: os divisores comuns de 12 e de 30 são:
    - 1, 2, 3 e 6
  - De modo que:
    - MDC(12,30)=6 e $6=1.30+(-2).12$

Máximo Divisor Comum

- **Exemplo**: note que MDC(17,95)=1
    - pois 17 é primo e $17 \nmid 95$
  - Pode-se verificar, então, que:
    - $1 = 28.17 + (-5).95$

Máximo Divisor Comum

- Se MDC(a,b)=1, dizemos que os inteiros a e b são ***relativamente primos***.
- **Exemplo**: 17 e 22 são primos entre si pois MDC(17,22)=1.

- Os inteiros $a_1,a_2,\ldots,a_n$ são ***relativamente primos aos pares*** se $MDC(a_i,a_j)=1$, para $1 \leq i < j \leq n$.
- **Exemplo**: Verifique se são relativamente primos aos pares os inteiros 10,17 e 21 e também os inteiros 10,19 e 24.
- **Solução**:
  - MDC(10,17)=1, MDC(10,21)=1 e MDC(17,21)=1 √
  - Como 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:

$$\boxed{a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}} \qquad \boxed{b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}}$$

  - 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:

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

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

$$\begin{cases} 60=2^2.3^1.5^1 \\ 18=2^1.3^2 \end{cases} \rightarrow \quad MDC(60,18)=2^1.3^1.5^0=6$$

Cálculo do MDC (algoritmo de Euclides)

Exemplo: calcule o MDC(91,287).

- Dividir 287 por 91, obtendo: $287 = 91.3 + 14$

  - note que todo divisor de 91 e 287 deve ser divisor de:

    $287 - 91.3 = 14$

Cálculo do MDC (algoritmo de Euclides)

Exemplo: calcule o MDC(91,287).

- Dividir 287 por 91, obtendo: $287 = 91.3 + 14$

  - note que todo divisor de 91 e 287 deve ser divisor de:
    $287 - 91.3 = 14$
  - por outro lado, todo divisor de 91 e 14 deve ser divisor de:
    $287 = 91.3 + 14$

Cálculo do MDC (algoritmo de Euclides)

Exemplo: calcule o MDC(91,287).

- Dividir 287 por 91, obtendo: 287 = 91.3 + 14

  - note que todo divisor de 91 e 287 deve ser divisor de:
    287 - 91.3 = 14

  - por outro lado, todo divisor de 91 e 14 deve ser divisor de:
    287 = 91.3 + 14

  - logo, {287,91 e 14} têm os mesmos divisores e:
    MDC(91,287) = MDC(91,14)

Cálculo do MDC (algoritmo de Euclides)

Exemplo: calcule o MDC(91,287).

- Dividir 287 por 91, obtendo: $287 = 91.3 + 14$

  - note que todo divisor de 91 e 287 deve ser divisor de:
    $287 - 91.3 = 14$
  - por outro lado, todo divisor de 91 e 14 deve ser divisor de:
    $287 = 91.3 + 14$
  - logo, {287,91 e 14} têm os mesmos divisores e:
    $MDC(91,287) = MDC(91,14)$

- Próximo passo: dividir 91 por 14, obtendo: $91=14.6+7$

Cálculo do MDC (algoritmo de Euclides)

Exemplo: calcule o MDC(91,287).

- Dividir 287 por 91, obtendo: $287 = 91.3 + 14$

  - note que todo divisor de 91 e 287 deve ser divisor de:
    $287 - 91.3 = 14$
  - por outro lado, todo divisor de 91 e 14 deve ser divisor de:
    $287 = 91.3 + 14$
  - logo, {287,91 e 14} têm os mesmos divisores e:
    MDC(91,287) = MDC(91,14)

- Próximo passo: dividir 91 por 14, obtendo: $91=14.6+7$
- Em seguida: $14 = 7.2$
- Como 7 divide 14, segue que MDC(14,7)=7

Cálculo do MDC (algoritmo de Euclides)

Exemplo: calcule o MDC(91,287).

- Dividir 287 por 91, obtendo: $287 = 91.3 + 14$

  - note que todo divisor de 91 e 287 deve ser divisor de:
    $287 - 91.3 = 14$
  - por outro lado, todo divisor de 91 e 14 deve ser divisor de:
    $287 = 91.3 + 14$
  - logo, {287,91 e 14} têm os mesmos divisores e:
    MDC(91,287) = MDC(91,14)

- Próximo passo: dividir 91 por 14, obtendo: $91=14.6+7$
- Em seguida: $14 = 7.2$
- Como 7 divide 14, segue que MDC(14,7)=7
- Logo MDC(287,91)= MDC(91,14)= 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:

$$662 = 414 \times 1 + 248$$
$$414 = 248 \times 1 + 166$$
$$248 = 166 \times 1 + 82$$
$$166 = 82 \times 2 + 2$$
$$82 = 2 \times 41$$

- Logo, MDC(662,414)=2, pois 2 é o último resto não-nulo.

Cálculo do MDC

- **Exemplo**: Sejam a=190 e b=34. Então:

  190 = 5.34 + 20

  34 = 1.20 + 14

  20 = 1.20 + 14

  20 = 1.14 + 6

  14 = 2.6 + 2

  6 = 3.2 + 0

  – De modo que: MDC(190,34) = 2

O algoritmo de Euclides

- Em pseudocódigo:

```
function MDC(a,b)
x:=a
y:=b
while y ≠ 0
    r:=x mod y
    x:=y
    y:=r
end

{MDC(a,b) é o valor de x}
```

Máximo Divisor Comum

- **Nota**: o próprio algoritmo de Euclides pode ser adaptado para fornecer os valores de s e t para:
    - $d = s.a + t.b = MDC(a,b)$

Máximo Divisor Comum

- **Exemplo**: Sejam a=190 e b=34. Então:

$$
\begin{aligned}
MDC(190,34) = 2 &= 14 - 2.(6) \\
&= 14 - 2.[20 - 1.(14)] \\
&= 3.(14) - 2.(20) \\
&= 3.[34 - 1.(20)] - 2.(20) \\
&= 3.(34) - 5.(190 - 5.34) \\
&= 28.(34) - 5.(190)
\end{aligned}
$$

- Portanto: s=-5 e t=28

Máximo Divisor Comum

- **Teorema**: se a e b $\in$ Z^+, e se b>a, então:

  $$MDC(a,b) = MDC(b,b\pm a)$$

- **Prova**:
  - Se c divide a e b, também divide $b\pm a$
  - Já que: $a = b - (b-a) = -b + (b+a)$, temos que:
    - um divisor comum de b e $b\pm a$ também divide a e b
  - Então, uma vez que a e b possuem os mesmos divisores comuns que b e $b\pm a$:
    - eles devem o mesmo máximo divisor comum $\square$

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 MMC(a,b).

- Em notação matemática:
  $$MMC(a,b)=\min\{k \mid a|k \wedge b|k\}$$

- **Exemplo**:
  MMC(12,18)=36

Método para o cálculo do MMC:

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

$$\boxed{a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}} \qquad \boxed{b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}}$$

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

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

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

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

$$\begin{cases} 95256 = 2^3.3^5.7^2 \\ 432 = 2^4.3^3 \end{cases} \rightarrow \quad MMC(95256,432) = 2^4.3^5.7^2$$

MDC e MMC

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

  $$a.b = MDC(a,b) \;.\; MMC(a,b)$$

  Prova: ?

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

  Solução: $540 = 2^2.3^3.5^1$

  $504 = 2^3.3^2.7^1$

  $MDC(2^2.3^3.5^1,2^3.3^2.7^1)= 2^2.3^2.5^0.7^0=36$

  $MMC(2^2.3^3.5^1,2^3.3^2.7^1)= 2^3.3^3.5^1.7^1=7560$

  $540.504 = 272140 = 36x7560$ √

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.

  - <u>Exemplo</u>: 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* ***mod*** *m* o resto que é obtido quando a é dividido por m.

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

- **Exemplo**: 17 mod 5 = 2 $(17 = 3\times5 + 2)$
  -133 mod 9 = 2 $(-133 = -15\times9 + 2)$
  2001 mod 101 = 82 $(2001=19\times101 + 82)$

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 $\mathbf{a \equiv b \pmod{m}}$

  – 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:

$6|(17-5)$, 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

$$\mathbf{a = b + k.m}$$

Prova:

1) se $a \equiv b \pmod m$, então $m|(a-b)$
   $\Rightarrow$ 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

$$b=a+s.m \quad \text{e} \quad d=c+t.m$$

- $b+d = (a+s.m) + (c+t.m) = (a+c) + (s+t).m$

  $\Rightarrow\ a+c \equiv b+d \pmod{m}\ \surd$

- $b.d = (a+s.m).(c+t.m) = a.c + (a.t + c.s + stm).m$

  $\Rightarrow\ a.c \equiv b.d \pmod{m}\ \surd$

Aritmética modular e congruência

- **Exemplo**: Como $7 \equiv 2 \pmod 5$ e $11 = 1 \pmod 5$, o teorema anterior garante que:

  - $7 + 11 \equiv 2 + 1 \pmod 5$, ou seja,
    $18 \equiv 3 \pmod 5$

  - $7.11 \equiv 2.1 \pmod 5$, 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 "descriptografar" 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 $m_1, m_2, \ldots, m_n$ 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 $m_1, m_2, \ldots, m_n$.

- Ou seja, podemos representar a por:

  $$(a \bmod m_1,\ a \bmod m_2,\ \ldots,\ a \bmod m_n)$$

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:

$$x \equiv 65 \pmod{99}$$
$$x \equiv 2 \pmod{98}$$
$$x \equiv 51 \pmod{97}$$
$$x \equiv 10 \pmod{95} \qquad x=?$$