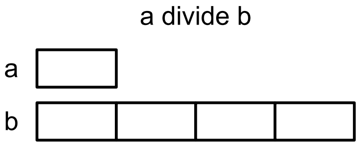
Fundamentos: Algoritmos, Inteiros e Matrizes

Centro de Informática
UFPE

Inteiros e Divisão

- Sejam a e b inteiros, com $a \neq 0$.
- a divide b se existe um inteiro c, tal que $b = ac$.

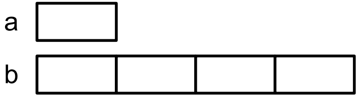


Por exemplo, a = 3, b = 12

Inteiros e Divisão

- Sejam a e b inteiros, com $a \neq 0$.
- a divide b se existe um inteiro c, tal que $b = ac$.
- Exemplo. 5 divide 10, pois existe um inteiro $c = 2$, tal que $10 = 5 \cdot 2$.
- Exemplo. 5 não divide 11, pois não existe um inteiro c, tal que $11 = 5c$.

a divide b



Por exemplo, a = 3, b = 12

Inteiros e Divisão

- Quando a divide b, dizemos que
  - a é um *fator* de b.
  - b é um *múltiplo* de a.
- Notação: $a \mid b$
- Formalmente: $a \mid b \;\equiv\; \exists c(b = ac)$, no domínio dos inteiros.
- $a \not| \; b$ denota que a não divide b.

Inteiros e Divisão

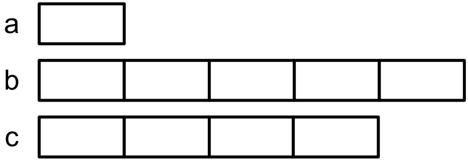
Exercícios

- $5 \mid 13$?
- $13 \mid 5$?
- $84 \mid 252$?
- $3 \mid -9$?
- $2 \mid 12345678$?

Inteiros e Divisão

Teorema.

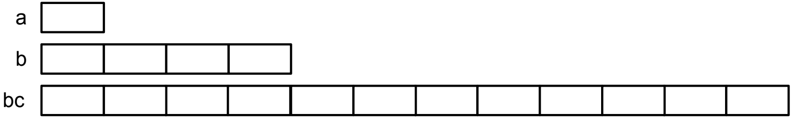
- Sejam a, b, c inteiros.
- Se $(a \mid b)$ e $(a \mid c)$, então $(a \mid (b + c))$.



Inteiros e Divisão

Teorema.

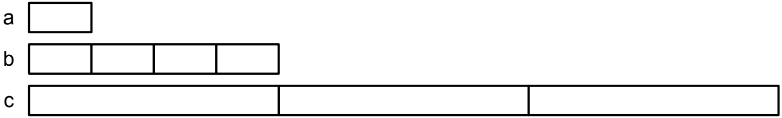
- Sejam a, b, c inteiros.
- Se $(a \mid b)$, então $(a \mid bc)$, para todo inteiro c.



Inteiros e Divisão

Teorema.

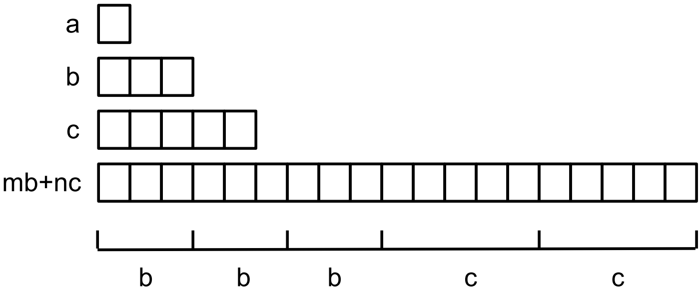
- Sejam a, b, c inteiros.
- Se $(a \mid b)$ e $(b \mid c)$, então $a \mid c$.



Inteiros e Divisão

Teorema.

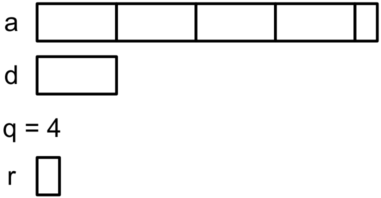
- Sejam a, b, c inteiros.
- Se $(a \mid b)$ e $(a \mid c)$, então $a \mid (mb + nc)$, para m e n inteiros.



Inteiros e Divisão

O Algoritmo da Divisão

- Seja a um inteiro e d um inteiro positivo.
- Então, existem inteiros q e r únicos, com $0 \leq r < d$, tal que $a = dq + r$
- d é o divisor, a é o dividendo, q é o quociente e r é o resto.
- Atenção: o divisor é sempre positivo e o resto é sempre maior ou igual a zero.

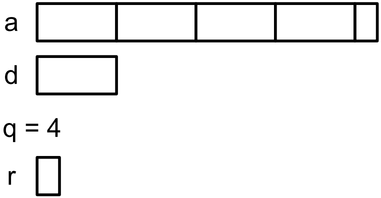


Inteiros e Divisão

O Algoritmo da Divisão

Notação.

- $q = a \textbf{ div } d$
- $r = a \textbf{ mod } d$



Inteiros e Divisão
O Algoritmo da Divisão

Exemplos.

- $32 \textbf{ div } 5 = 6$.
- $32 \textbf{ mod } 5 = 2$.

Inteiros e Divisão

O Algoritmo da Divisão

Exercícios. Calcule:

- 21 **div** 3.
- 21 **mod** 3.
- 1 **div** 9.
- 1 **mod** 9.
- 0 **div** 5325.
- 0 **mod** 5325.

Inteiros e Divisão

O Algoritmo da Divisão

- E quanto à divisão -10 **div** 3?
- No mundo dos reais: $-10/3 = -3,333..$
- Divisão de inteiros: -10 **div** $3 = -4$
- Por que -10 **div** $3 \neq -3$?
  Dica. Calcule o resto para $q = -3$ e verifique se ele é positivo ou negativo.

Inteiros e Divisão

O Algoritmo da Divisão

- Divisão de números negativos requer mais cuidado:

$$a \textbf{ div } d = \lfloor a/d \rfloor$$

Lembre-se: $a \in Z$ e $d > 0$.

Inteiros e Divisão

O Algoritmo da Divisão

Procedimento para calcular $q = a \textbf{ div } d$ e $r = a \textbf{ mod } d$

1. Calcule a/d (divisão de reais)
2. Calcule $q = \lfloor a/d \rfloor$
3. Calcule o resto usando $a = d \cdot q + r$

Inteiros e Divisão

O Algoritmo da Divisão

Exemplo.

1. $-10/3 = -3,333...$
2. $q = \lfloor -10/3 \rfloor = \lfloor -3,333... \rfloor = -4$
3. Se $-10 = 3 \cdot (-4) + r$, então $r = 2$

Inteiros e Divisão

O Algoritmo da Divisão

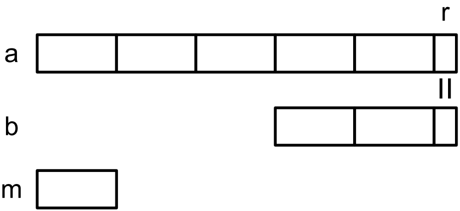
Exercícios. Calcule:

- -2002 **div** 87.
- -2002 **mod** 87.

Inteiros e Divisão

Aritmética Modular

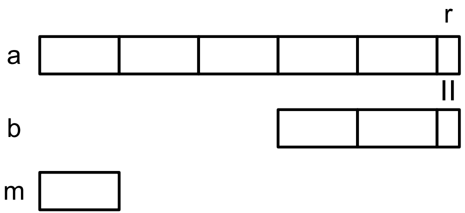
- Sejam a e b inteiros e m um inteiro positivo.
- a *é congruente a* b *módulo* m se m divide $a - b$.
- Notação: $a \equiv b \ (mod \ m)$.



Inteiros e Divisão
Aritmética Modular

Teorema.

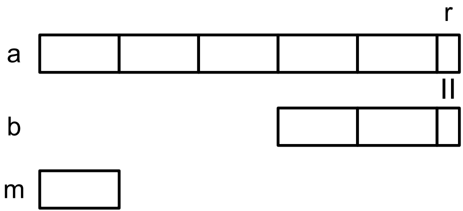
- Sejam a e b inteiros e m um inteiro positivo.
- $a \equiv b \ (mod \ m)$ se, e somente se, $(a \ \mathbf{mod} \ m) = (b \ \mathbf{mod} \ m)$.



Inteiros e Divisão

Aritmética Modular

- Sejam a e b inteiros e m um inteiro positivo.
- $a \equiv b \ (mod \ m)$ se, e somente se, $(a \ \mathbf{mod} \ m) = (b \ \mathbf{mod} \ m)$.
- Exemplo. 42 é congruente a 7 módulo 5.



Inteiros e Divisão

Aritmética Modular

Exercício.

- Quais destes são congruentes?

  a) $13 \equiv 5 \ (mod\ 8)$
  b) $13 \equiv 5 \ (mod\ 3)$
  c) $12 \equiv 30 \ (mod\ 15)$
  d) $8 \equiv 10 \ (mod\ 2)$
  e) $76 \equiv 33 \ (mod\ 43)$

- Encontre pelo menos 3 outros números congruentes a 42 módulo 5.

Inteiros e Divisão

Aritmética Modular

- O operador de congruência modular é comutativo e transitivo.
- $(a \equiv b \pmod{m}) \equiv (b \equiv a \pmod{m})$
- $(a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \rightarrow (a \equiv c \pmod{m})$

Inteiros e Divisão

Aritmética Modular

- O operador de congruência modular é comutativo e transitivo.
- $(a \equiv b\ (mod\ \ m)) \ \equiv \ (b \equiv a\ (mod\ \ m))$
- $(a \equiv b\ (mod\ \ m)) \wedge (b \equiv c\ (mod\ \ m)) \rightarrow (a \equiv c\ (mod\ \ m))$
- Exemplo.

$$(5 \equiv 11\ (mod\ 3)) \ = \ (11 \equiv 5\ (mod\ 3))$$

- Exemplo.

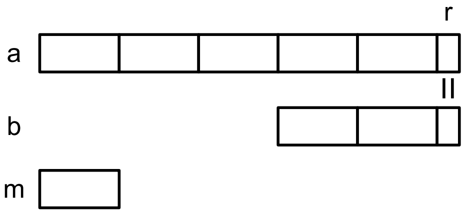
$$(5 \equiv 11\ (mod\ 3)) \wedge (11 \equiv 17\ (mod\ 3)) \rightarrow (5 \equiv 17\ (mod\ 3))$$

Inteiros e Divisão

Aritmética Modular

Teorema.

- Seja m um inteiro positivo.
- $a \equiv b \ (mod \ m)$ se, e somente se, existe um k tal que $a = b + km$.

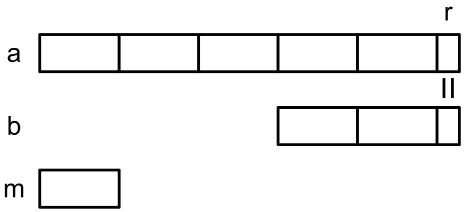


Inteiros e Divisão

Aritmética Modular

Teorema.

- Seja m um inteiro positivo.
- $a \equiv b \pmod{m}$ se, e somente se, existe um k tal que $a = b + km$.
- Qual o valor de k na figura abaixo?

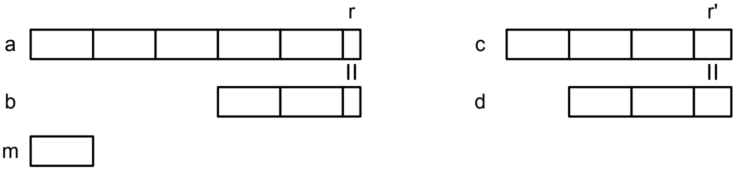


Inteiros e Divisão

Aritmética Modular

Teorema.

- Seja m um inteiro positivo.
- Suponha $a \equiv b \ (mod \ m)$ e $c \equiv d \ (mod \ m)$.
- Então,
  $a + c \equiv b + d \ (mod \ m)$ e
  $ac \equiv bd \ (mod \ m)$

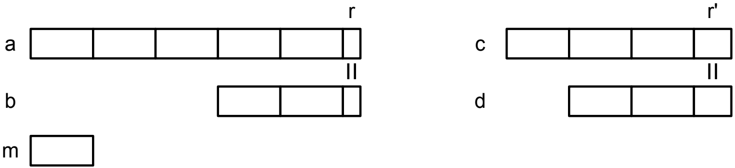


Inteiros e Divisão

Aritmética Modular

Exemplo.

- Sabemos que $13 \equiv 8 \ (\textit{mod}\ 5)$ e $11 \equiv 6 \ (\textit{mod}\ 5)$.
- Pelo teorema, $(13 + 11) \equiv (8 + 6) \ (\textit{mod}\ 5)$.
- E também: $(13 \cdot 11) \equiv (8 \cdot 6) \ (\textit{mod}\ 5)$.



Inteiros e Divisão

Aritmética Modular

Caso particular do teorema.

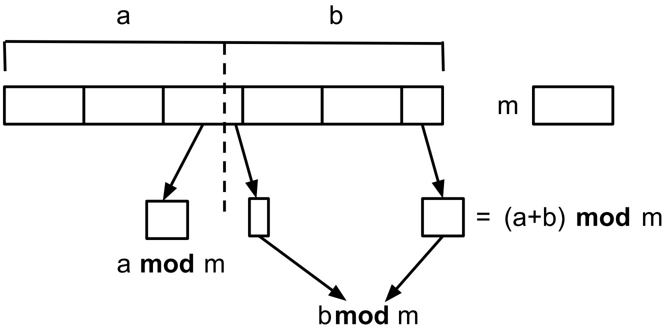
- Sabemos que $x \equiv x \pmod{m}$.
- Pelo teorema, podemos sempre somar ou multiplicar os 2 lados de uma equivalência por um número.
- Exemplo. $13 \equiv 8 \ (mod\ 5)$.
  Como temos que $3 \equiv 3 \ (mod\ 5)$,
  $(13 + 3) \equiv (8 + 3) \ (mod\ 5)$ e
  $(13 \cdot 3) \equiv (8 \cdot 3) \ (mod\ 5)$.

Inteiros e Divisão

Aritmética Modular

Teorema.

- Sejam m um inteiro positivo e a e b inteiros. Então:
- $(a+b)$ **mod** $m = ((a$ **mod** $m) + (b$ **mod** $m))$ **mod** m
- ab **mod** $m = ((a$ **mod** $m)(b$ **mod** $m))$ **mod** m



Inteiros e Divisão

Aplicações de Congruências: *hashing*

- Suponha que temos que armazenar o CPF e nome das pessoas:

123456789-38	Pelé
322766292-60	Maradona
123263420-34	Zico
969603020-52	Kuki
632523234-63	Ronaldo
639570309-23	Kaká

- Armazenar o CPF na íntegra pode ser ineficiente.
- Por exemplo, encontrar o dono do CPF "639570309-23" pode ser demorado pelo tamanho do número.

Inteiros e Divisão

Aplicações de Congruências: *hashing*

- Uma solução é utilizar uma função h que mapeia um número longo (como o CPF) para um número curto.
- Por exemplo. $h(63957030923) = 123$.
- O computador poderia então procurar por 123 (mais rápido) ao invés de procurar por 63957030923.
- A função h é chamada de função de *hash*.

Inteiros e Divisão

Aplicações de Congruências: *hashing*

- Suponha a função $h(k) = k \textbf{ mod } 200$.

138	Pelé
60	Maradona
34	Zico
52	Kuki
63	Ronaldo
123	Kaká

Inteiros e Divisão

Aplicações de Congruências: *hashing*

- Suponha a função $h(k) = k \textbf{ mod } 200$.

138	Pelé
60	Maradona
34	Zico
52	Kuki
63	Ronaldo
123	Kaká

- Problema: E se Romário, CPF "625234132-63", for cadastrado? Note que $h(62523413263) = 63$.

Inteiros e Divisão

Aplicações de Congruências: *hashing*

- Suponha a função $h(k) = k \textbf{ mod } 200$.

138	Pelé
60	Maradona
34	Zico
52	Kuki
63	Ronaldo
123	Kaká

- Problema: E se Romário, CPF "625234132-63", for cadastrado? Note que $h(62523413263) = 63$.
- Este evento chama-se *colisão*. Existem muitas políticas para resolução de colisão.

Inteiros e Divisão

Aplicações de Congruências: números aleatórios

- Um teste de *stress* em um celular é feito da seguinte forma:
  1. Conecte o celular em um computador.
  2. Faça o computador enviar sinais de pressionamento de teclas ao celular.
  3. Verifique se o celular travou. Se sim, envie o problema aos programadores e reinicie o celular.
  4. Volte ao passo 2.

Inteiros e Divisão

Aplicações de Congruências: números aleatórios

- Um teste de *stress* em um celular é feito da seguinte forma:
  1. Conecte o celular em um computador.
  2. Faça o computador enviar sinais de pressionamento de teclas ao celular.
  3. Verifique se o celular travou. Se sim, envie o problema aos programadores e reinicie o celular.
  4. Volte ao passo 2.
- Que teclas o computador escolhe para pressionar?
- No teste de *stress*, escolhemos teclas aleatoriamente.
- Em simulações, é muito comum precisarmos gerar números aleatoreamente.

Inteiros e Divisão

Aplicações de Congruências: números aleatórios

- Como fazer um computador sortear números?
- Se um programa de computador gera números, estes números não podem ser verdadeiramente aleatórios, pois são gerados de forma previsível.
- Chamamos números que são gerados de forma sistemática e *parecem* aleatórios de *pseudo aleatórios*.

Inteiros e Divisão

Aplicações de Congruências: números aleatórios

- Sejam os inteiros m (módulo), a (multiplicador), c (incremento) e x_0 (semente).
- $2 \leq a < m$, $0 \leq c < m$ e $0 \leq x_0 < m$.
- Sequência de números x_i:

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

Inteiros e Divisão

Aplicações de Congruências: números aleatórios

Exemplo.

- Seja $x_0 = 2$.
- Seja $x_{n+1} = (3x_n + 4) \textbf{ mod } 5$.

$x_0 = 2$
$x_1 = (3x_0 + 4) \textbf{ mod } 5 = (3 \cdot 2 + 4) \textbf{ mod } 5 = 10 \textbf{ mod } 5 = 0$
$x_2 = (3x_1 + 4) \textbf{ mod } 5 = (3 \cdot 0 + 4) \textbf{ mod } 5 = 4 \textbf{ mod } 5 = 4$

Exercício. Calcule x_3, x_4, x_5, x_6, x_7 e x_8.

Inteiros e Divisão

Aplicações de Congruências: criptografia

- Dada a mensagem “Náutico Campeão”, como enviar sem que um espião possa entender?
- Precisamos de uma função invertível f que embaralhe as letras.
- $f($“Náutico Campeão”$) =$“@36kagni35*7sKL320”.
- O destinatário, conhecedor de f^{-1}, faria $f^{-1}($“@36kagni35*7sKL320”$) =$“Náutico Campeão”;

Inteiros e Divisão

Aplicações de Congruências: criptografia

- Júlio César utilizava um método de criptografia simples.
- Cada letra era substituída pela letra 3 posições adiante.
- 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
- "A" vira "D", "B" vira "E", ..., "X" vira "A", etc.
- Exercício. Como ficaria "Náutico Campeão" criptografado?
- Exercício. Qual a função f?
  Dica: faça com que f mapeie uma letra na outra (não a frase toda). Assuma que as letras são modeladas como números: A=0, B=1, C=2, ..., Z=25.

Inteiros e Divisão

Aplicações de Congruências: criptografia

- 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
- "Náutico Campeão" vira "QDXWLFR FDPSHDR".
- Para cada letra, aplicar $f(p) = (p + 3) \textbf{ mod } 26$, onde A=0, B=1, C=2, D=3, ...
- Exercício. Qual a função f^{-1}?

Exercícios recomendados

Seção 3.4

- Fazer todos
- Os de prova de teorema são opcionais
- Discrete Mathematics and Its Applications
  Kenneth Rosen, 6a edição

Primos

- Um inteiro positivo p maior que 1 é *primo* se seus únicos fatores positivos são 1 e p.
- Exemplos: 2, 3, 5, 7, 11, etc.

Primos

- Um inteiro maior que 1 não-primo é chamado de *composto*.
- Ou seja, n é composto se existe um inteiro $1 < a < n$ tal que $a \mid n$.
- Exemplos: 4, 6, 8, 9, 10, etc.

Primos

Teorema Fundamental da Aritmética.

- Todo inteiro maior que 1 pode ser escrito unicamente como um primo ou um produto de primos.
- Os fatores são descritos em ordem não decrescente.
- Exemplos.
  $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  $11 = 11$
  $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37.$
  $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

http://www.datapointed.net/visualizations/math/factorization/animated-diagrams/

Primos

Teorema.

- Se n é um inteiro composto, então n tem um divisor primo $d \leq \sqrt{n}$.
- Exemplo. Seja n o inteiro composto 30. Então, n possui um divisor primo $d \leq \sqrt{30}$. Note que 2 é divisor primo de 30 e menor ou igual que $\sqrt{30} = 5,477$.

Primos

Primalidade

- Um dos grandes desafios da computação é descobrir se n é um número primo ou não.

Primos

Primalidade

- Um dos grandes desafios da computação é descobrir se n é um número primo ou não.
- O teorema anterior diz:
  Se n é um inteiro composto, então n tem um divisor primo $d \leq \sqrt{n}$.

Primos

Primalidade

- Um dos grandes desafios da computação é descobrir se n é um número primo ou não.
- O teorema anterior diz:
  Se n é um inteiro composto, então n tem um divisor primo $d \leq \sqrt{n}$.
- Sabemos que $p \rightarrow q \equiv \neg q \rightarrow \neg p$.

Primos

Primalidade

- Um dos grandes desafios da computação é descobrir se n é um número primo ou não.
- O teorema anterior diz:
  Se n é um inteiro composto, então n tem um divisor primo $d \leq \sqrt{n}$.
- Sabemos que $p \rightarrow q \equiv \neg q \rightarrow \neg p$.
- Ou seja, se n *não* tem divisor primo $d \leq \sqrt{n}$, então n *não* é composto.
- Ou: se n *não* tem divisor primo $d \leq \sqrt{n}$, então n é primo.

Primos

Primalidade

- Teorema. Se n *não* tem divisor primo $d \leq \sqrt{n}$, então n é primo.
- Este teorema poupa-nos trabalho. Para saber se n é primo, não precisamos testar se n é divisível pelos *números* $2, 3, 4, 5, 6, 7, 8, \ldots, n-1$.
- Apenas testamos se n é divísivel pelos *primos* $2, 3, 5, 7, 11, 13, \ldots, \sqrt{n}$.
- Exercício. Usando o teorema acima, mostre que 97 é primo (sabendo que $\sqrt{97} = 9,8$).

Primos

Fatoração

- Como fatorar o número n?
- Qual o algoritmo que fatora 105 em $3 \cdot 5 \cdot 7$?

Primos

Fatoração: “algoritmo” ineficiente para $n = 105$.

- $105 \textbf{ mod } 2 = 0$? Não! Teste com o próximo primo...
- $105 \textbf{ mod } 3 = 0$? Sim! 3 é um fator.
  Faça $n = 105 \textbf{ div } 3 = 35$ e recomece dividindo por 3.
- $35 \textbf{ mod } 3 = 0$? Não!
- $35 \textbf{ mod } 5 = 0$? Sim! 5 é um fator.
  Faça $n = 35 \textbf{ div } 5 = 7$ e recomece dividindo por 5.
- $7 \textbf{ mod } 5 = 0$? Não!
- $7 \textbf{ mod } 7 = 0$? Sim! 7 é um fator.
  Como $7 \textbf{ div } 7 = 1$, o algoritmo termina.

Primos

Fatoração: "algoritmo" ineficiente para $n = 105$.

- $105 \textbf{ mod } 2 = 0$? Não! Teste com o próximo primo...
- $105 \textbf{ mod } 3 = 0$? Sim! 3 é um fator.
  Faça $n = 105 \textbf{ div } 3 = 35$ e recomece dividindo por 3.
- $35 \textbf{ mod } 3 = 0$? Não!
- $35 \textbf{ mod } 5 = 0$? Sim! 5 é um fator.
  Faça $n = 35 \textbf{ div } 5 = 7$ e recomece dividindo por 5.
- $7 \textbf{ mod } 5 = 0$? Não!
- $7 \textbf{ mod } 7 = 0$? Sim! 7 é um fator.
  Como $7 \textbf{ div } 7 = 1$, o algoritmo termina.
- Não precisávamos testar $7 \textbf{ mod } 5$ e $7 \textbf{ mod } 7$, pois $\sqrt{7} = 2,6$. Se 7 não tem divisor primo $\leq 2,6$, então 7 é primo.

Primos

Fatoração

input: n

```
primo := 2;
while (primo ≤ √n) {
    if (n mod primo == 0) {
        print(primo);
        n := n  div primo;
    }
    else {
        primo := prox_primo(primo);
    }
}
print(n);
```

Exercício: ache os fatores de $n = 1617$ usando o algoritmo acima.

Primos

Teorema.

- Existem infinitos números primos.

Prova.

- Suponha que os primos são *finitos*: p_1, p_2, ..., p_n.
- Seja $Q = p_1 p_2 \dots p_n + 1$
- Escolha um primo qualquer da lista, digamos p_j.
- Note que p_j não divide Q.
  - Por que não?
  - Porque, se p_j divide Q, ele também divide o número $Q - p_1 p_2 \dots p_n$.
  - Mas, o número $Q - p_1 p_2 \dots p_n = 1$ (definição de Q).
  - E 1 não é divisível por nenhum primo.
- Portanto, nenhum primo da lista p_1, p_2, ..., p_n divide Q.
- Ou seja, Q é primo e não pertence à lista inicial de todos os primos!
- Provamos por contradição que existem infinitos primos.

Primos

Curiosidade

- Existe um interesse em achar números primos grandes.
- Os maiores primos encontrados seguem o padrão $2^p - 1$, onde p é primo.
- Estes primos são chamados de primos de Mersenne.
- 25 de janeiro de 2013: $2^{57.885.161} - 1$ (17.425.170 de dígitos)
- *Great Internet Mersenne Prime Search*: `http://www.mersenne.org`

Primos

Teorema do Número Primo

- Seja $\pi(x)$ o número de primos existentes menores ou iguais a x.
- Exemplo. $\pi(10) = 4$, pois existem 4 primos menores ou iguais a 10: 2, 3, 5 e 7.
- Não sabemos como calcular $\pi(x)$, mas temos uma *aproximação*.
- $\pi(x)$ é *aproximadamente* $x/(\mathit{ln}\ x)$, quando x tende ao infinito.
- Provado em 1896 por Jacques Hadamard e Charles-Jean-Gustave-Nicholas de la Valleé-Poussin

Primos

Teorema do Número Primo

- $\pi(x)$ é *aproximadamente* $x/(\ln x)$, quando x tende ao infinito.
- Exercício. Qual a probabilidade *aproximada* de escolhermos um número n entre 1 e x tal que n seja primo?

Primos

Teorema do Número Primo

- $\pi(x)$ é *aproximadamente* $x/(ln\ x)$, quando x tende ao infinito.
- Exercício. Qual a probabilidade *aproximada* de escolhermos um número n entre 1 e x tal que n seja primo?
- Como temos aproximadamente $x/(ln\ x)$ números primos entre 1 e x, a chance de escolher um número destes entre x possibilidades é

$$\frac{x/(ln\ x)}{x} = \frac{1}{ln\ x}$$

Máximo Divisor Comum

- Sejam a e b inteiros.
- Assuma que $a \neq 0$ ou $b \neq 0$ (ou ambos).
- O maior inteiro d tal que $(d \mid a)$ e $(d \mid b)$ é o *Máximo Divisor Comum* de a e b.
- Notação: $mdc(a, b)$

Máximo Divisor Comum

Exemplo

- Qual o mdc(16,20)?
- Os divisores de 16 são: 1, 2, 4, 8 e 16.
- Os divisores de 20 são: 1, 2, 4, 5, 10 e 20.
- Os divisores comuns são: 1, 2 e 4.
- O máximo divisor comum é 4.

Máximo Divisor Comum

Exercício

- Qual o mdc(100,80)?

Máximo Divisor Comum

- Os inteiros a e b são *primos relativos* se o $mdc(a, b) = 1$.
- Exemplo. $mdc(7, 8) = 1$.
- Exercício. Quais dos pares abaixo são primos relativos?
  a) $(10, 43)$
  b) $(53, 12)$
  c) $(56, 20)$
  d) $(2^{57.885.161} - 1, 2^{57.885.161} - 1)$

Máximo Divisor Comum

- Os inteiros a_1, a_2, a_3, ..., a_n são primos relativos 2 a 2 se o $mdc(a_i, a_j) = 1$, para $1 \leq i < j \leq n$.
- Exemplo. 10, 43, 11, $2^{57.885.161} - 1$

Máximo Divisor Comum

- Podemos achar o $mdc(a, b)$ através da fatoração.
- Temos que fatorar a e b numa forma padrão (ou forma normal):
- $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$
- $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$

Máximo Divisor Comum

- Podemos achar o $mdc(a, b)$ através da fatoração.
- Temos que fatorar a e b numa forma padrão (ou forma normal):
- $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$
- $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$
- Exemplo. Sejam $a = 10$ e $b = 12$.
  $a = 2 \cdot 5$
  $b = 2 \cdot 2 \cdot 3$.
- Na forma normal:
  $a = 2^1 \cdot 3^0 \cdot 5^1$
  $b = 2^2 \cdot 3^1 \cdot 5^0$
- Qual o $mdc(a, b)$?

Máximo Divisor Comum

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

Máximo Divisor Comum

- Sejam $a = 10$ e $b = 12$
- $a = 2^1 \cdot 3^0 \cdot 5^1$
  $b = 2^2 \cdot 3^1 \cdot 5^0$
- $mdc(a, b) = 2^{min(1,2)} \cdot 3^{min(0,1)} \cdot 5^{min(1,0)}$
- Ou seja, $mdc(a, b) = 2^1 \cdot 3^0 \cdot 5^0 \;=\; 2$

Máximo Divisor Comum

Exercício.

- Sejam $a = 52$ e $b = 36$.
- Use a fatoração de a e b e calcule o $mdc(a, b)$.

Mínimo Múltiplo Comum

- Sejam a e b inteiros positivos.
- O *mínimo múltiplo comum* de a e b ou $mmc(a, b)$ é o menor inteiro positivo que é divisível por a e b.
- A fatoração também pode ser utilizada para calcularmos o *mmc*.
- Seja $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$
- Seja $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$
- $mmc(a, b) = p_1^{max(a_1, b_1)} p_2^{max(a_2, b_2)} \dots p_n^{max(a_n, b_n)}$

Mínimo Múltiplo Comum

Exemplo.

- Sejam $a = 8$ e $b = 10$.
- $a = 2 \cdot 2 \cdot 2$
- $b = 2 \cdot 5$
- Normalizando:
  $a = 2^3 \cdot 5^0$
  $b = 2^1 \cdot 5^1$
- $mmc(a, b) = 2^{max(3,1)} \cdot 5^{max(0,1)} = 2^3 \cdot 5^1 = 40$

Mínimo Múltiplo Comum

Exercício.

- Sejam $a = 12$ e $b = 15$.
- Ache o $mmc(a, b)$ utilizando fatoração.

Exercícios recomendados

Seção 3.5

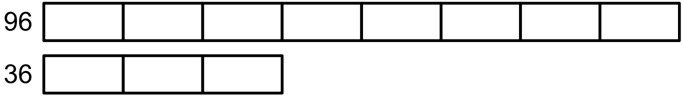
- Fazer todos
- Os de prova de teorema são opcionais
- Discrete Mathematics and Its Applications
  Kenneth Rosen, 6a edição

Algoritmo de Euclides

- Euclides propôs um algoritmo para calcular o *mdc*.
- O algoritmo de Euclides é mais eficiente que a técnica da fatoração.

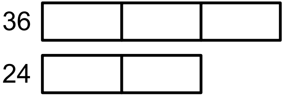
Algoritmo de Euclides

- Suponha que queremos calcular $mdc(96, 36)$.
- Dividindo 96 por 36, temos: $96 = 36 \cdot 2 + 24$.
- Note que
  - Um divisor de 96 e 36 também é divisor de 24.
  - Um divisor de 36 e 24 também é divisor de 96.
- Ou seja, um divisor de $(96, 36)$ também é divisor de $(36, 24)$
- Portanto, o $mdc(96, 36) = mdc(36, 24)$.



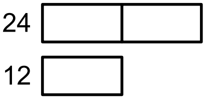
Algoritmo de Euclides

- Podemos então reduzir o problema de calcular o $mdc(96, 36)$ no problema de calcular o $mdc(36, 24)$.
- Ao dividir 36 por 24, temos $36 = 24 \cdot 1 + 12$.
- Nosso problema agora é reduzido ao do $mdc(24, 12)$.



Algoritmo de Euclides

- Dividindo 24 por 12, temos $24 = 12 \cdot 2 + 0$.
- Portanto, 12 divide 24.
- O $mdc(24, 12) = 12$.
- E também o $mdc(24, 12) = mdc(36, 24) = mdc(96, 36) = 12$



Algoritmo de Euclides

Resumindo: para calcular o $mdc(96, 36)$, fazemos:

$$\begin{aligned} 96 &= 36 \cdot 2 + 24 \\ 36 &= 24 \cdot 1 + 12 \leftarrow mdc \\ 24 &= 12 \cdot 2 + 0 \end{aligned}$$

O algoritmo finaliza quando o resto é 0. O $mdc(96, 36)$ é 12.

Algoritmo de Euclides

Lema

- Sejam a, b, q e r inteiros.
- Se $a = bq + r$,
  então $mdc(a, b) = mdc(b, r)$.

Algoritmo de Euclides

Exercício. Use o algoritmo de Euclides para calcular

- $mdc(16, 36)$
- $mdc(156, 64)$
- $mdc(320, 168)$

Algoritmo de Euclides

```
procedure mdc(a, b:  positive integers)
   x = a;
   y = b;
   while y ≠ 0 {
     r = x  mod y;
     x = y;
     y = r;
   }
```

- Ao término do laço, como sabemos qual é o $mdc(a, b)$?
- Para 2 números $m < n$, qual a diferença em executar `mdc(m,n)` e `mdc(n,m)`?

Congruências Lineares

Inverso de a módulo m

- $\bar{a}$ é o *inverso* de a módulo m se, e somente se, $\bar{a}a \equiv 1 \ (mod \ \ m)$.
- Exemplo. O inverso de 3 módulo 7 é -2, pois

$$(-2 \cdot 3) \equiv 1 \ (mod \ 7)$$

- Exercício. Calcule $-6 \ \mathbf{mod} \ 7$.

Congruências Lineares

Inverso de a módulo m

Mas, nem sempre $\overline{a}$ existe!

Teorema.

- Se a e m são primos relativos, então $\overline{a}$ existe.
- E mais: $\overline{a}$ é único (módulo m).
- Ou seja, existe um único $0 < \overline{a} < m$ e todos outros inversos são congruentes a $\overline{a}$ módulo m.

Congruências Lineares

Inverso de a módulo m

Como calcular $\overline{a}$, o inverso de a módulo m?

- Primeiro, certifique-se que $\overline{a}$ existe. Ou seja, verifique se $mdc(a, m) = 1$.
- Descubra s e t tal que $1 = sa + tm$.
  - Existe um procedimento para se resolver esta equação.
- s é o inverso de a módulo m.

Congruências Lineares

Inverso de a módulo m

Como calcular s e t, tal que $1 = sa + tm$?

- Primeiro passo: faça o Algoritmo de Euclides iniciando com a divisão de a por m e verifique se $mdc(a, m) = 1$.

Congruências Lineares

Inverso de a módulo m

Exemplo. Cálculo do inverso de 55 módulo 34.

- Primeiro passo: faça o Algoritmo de Euclides iniciando com a divisão de 55 por 34 e verifique se $mdc(55, 34) = 1$.

$$
\begin{aligned}
55 &= 34 \cdot 1 + 21 \\
34 &= 21 \cdot 1 + 13 \\
21 &= 13 \cdot 1 + 8 \\
13 &= 8 \cdot 1 + 5 \\
8 &= 5 \cdot 1 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \leftarrow mdc \\
2 &= 1 \cdot 2 + 0
\end{aligned}
$$

O $mdc(55, 34) = 1$. Portanto, $\overline{a}$ existe.

Congruências Lineares

Inverso de a módulo m

Como calcular s e t, tal que $1 = sa + tm$?

- Segundo passo: enumere cada equação gerada pelo Algoritmo de Euclides.

Congruências Lineares

Inverso de a módulo m

Exemplo. Cálculo do inverso de 55 módulo 34.

- Segundo passo: enumere cada equação gerada pelo Algoritmo de Euclides.

$$
\begin{aligned}
55 &= 34 \cdot 1 + 21 & (1)\\
34 &= 21 \cdot 1 + 13 & (2)\\
21 &= 13 \cdot 1 + 8 & (3)\\
13 &= 8 \cdot 1 + 5 & (4)\\
8 &= 5 \cdot 1 + 3 & (5)\\
5 &= 3 \cdot 1 + 2 & (6)\\
3 &= 2 \cdot 1 + 1 & (7)\\
2 &= 1 \cdot 2 + 0 & (8)
\end{aligned}
$$

Congruências Lineares

Inverso de a módulo m

Como calcular s e t, tal que $1 = sa + tm$?

- Terceiro passo: isole o 1 da penúltima equação.

Congruências Lineares

Inverso de *a* módulo *m*

Exemplo. Cálculo do inverso de 55 módulo 34.

- Terceiro passo: isole o resto 1 da penúltima equação.

O penúltimo passo é:

$$3 = 2 \cdot 1 + 1 \quad (7)$$

Isolando o 1, temos:

$$1 = 3 - 2 \cdot 1$$

Congruências Lineares

Inverso de a módulo m

Como calcular s e t, tal que $1 = sa + tm$?

- Quarto passo: substitua na equação o valor do resto da equação de cima. Repita até chegar na equação $1 = sa + tm$
- **Muito importante**: **não** simplifique os números que aparecem à esquerda da igualdade. Chamaremos estes números de *indestrutíveis*.

Congruências Lineares

Inverso de a módulo m

Exemplo. Cálculo do inverso de 55 módulo 34.

- Quarto passo: substitua na equação o valor do resto da equação de cima. Repita até chegar na equação $1 = s55 + t34$

Antes de começarmos a substituição, veja em vermelho os números indestrutíveis:

$$
\begin{aligned}
55 &= 34 \cdot 1 + 21 && (1)\\
34 &= 21 \cdot 1 + 13 && (2)\\
21 &= 13 \cdot 1 + 8 && (3)\\
13 &= 8 \cdot 1 + 5 && (4)\\
8 &= 5 \cdot 1 + 3 && (5)\\
5 &= 3 \cdot 1 + 2 && (6)\\
3 &= 2 \cdot 1 + 1 && (7)
\end{aligned}
$$

Congruências Lineares

Inverso de *a* módulo *m*

Exemplo. Cálculo do inverso de 55 módulo 34.

- Quarto passo: substitua na equação o valor do resto da equação de cima.

Os indestrutíveis estão em vermelho.

$$
\begin{array}{lll}
1 & = 3 - 2 \cdot 1 & [1] \\
 & = 3 - (5 - 3) & [\text{Subst. } (6)] \\
 & = 3 - 5 + 3 & [\text{Aritmética}] \\
 & = 2 \cdot 3 - 5 & [\text{Aritmética}] \\
 & \quad \textit{O truque é não simplificar } 2 \cdot 3 & \\
 & = 2(8 - 5) - 5 & [\text{Subst. } (5)] \\
 & = 2 \cdot 8 - 2 \cdot 5 - 5 & [\text{Aritmética}] \\
 & = 2 \cdot 8 - 3 \cdot 5 & [\text{Aritmética}]
\end{array}
$$

...

Congruências Lineares

Inverso de a módulo m

$$
\begin{aligned}
1 &= 2\cdot 8 - 3\cdot 5 && \text{[Continuação]}\\
&= 2\cdot 8 - 3\cdot(13-8) && \text{[Subst. (4)]}\\
&= 2\cdot 8 - 3\cdot 13 + 3\cdot 8 && \text{[Aritmética]}\\
&= 5\cdot 8 - 3\cdot 13 && \text{[Aritmética]}\\
&= 5\cdot(21-13) - 3\cdot 13 && \text{[Subst. (3)]}\\
&= 5\cdot 21 - 5\cdot 13 - 3\cdot 13 && \text{[Aritmética]}\\
&= 5\cdot 21 - 8\cdot 13 && \text{[Aritmética]}\\
&= 5\cdot 21 - 8\cdot(34-21) && \text{[Subst. (2)]}\\
&= 5\cdot 21 - 8\cdot 34 + 8\cdot 21 && \text{[Aritmética]}\\
&= 13\cdot 21 - 8\cdot 34 && \text{[Aritmética]}\\
&= 13\cdot(55-34) - 8\cdot 34 && \text{[Subst. (1)]}\\
&= 13\cdot 55 - 13\cdot 34 - 8\cdot 34 && \text{[Aritmética]}\\
&= 13\cdot 55 - 21\cdot 34 && \text{[Aritmética]}
\end{aligned}
$$

Congruências Lineares

Inverso de a módulo m

Como calcular s e t, tal que $1 = sa + tm$?

- Quinto passo: verifique se s é de fato $\overline{a}$. Ou seja, verifique se $\overline{a}a \equiv 1 \ (mod \ \ m)$

Congruências Lineares

Inverso de a módulo m

Exemplo. Cálculo do inverso de 55 módulo 34.

- Quinto passo: verifique se 13 é de fato $\overline{55}$. Ou seja, verifique se $(13 \cdot 55) \equiv 1 \ (mod\ 34)$
- Calculamos primeiro o quociente:

$$(13 \cdot 55) \ \mathbf{div} \ 34 \ = \ \lfloor 715/34 \rfloor \ = \ \lfloor 21.02 \rfloor \ = \ 21$$

- Agora, usamos a equação $a = bq + r$ para achar o resto:

$$715 = 34 \cdot 21 + r \ \therefore \ r = 715 - 714 \ \therefore \ r = 1$$

- Como o resto é 1, verificamos que nossos cálculos estavam corretos e, portanto, 13 é o inverso de 55 módulo 34.

Congruências Lineares

Inverso de a módulo m

Exercício.

- Calcule o inverso de
  a) 35 módulo 11.
  b) 43 módulo 15.
  c) 15 módulo 43.

Verifique se seu cálculo está correto.

Congruências Lineares

Inverso de a módulo m

Por que isso funciona?
Seja a premissa $1 = sa + tm$. Concluímos que $s = \overline{a}$.

1. $1 = sa + tm$	[Premissa]
2. $1 \equiv 1 \ (mod \ \ m)$	[Def. $\equiv (mod \ \ m)$]
3. $sa + tm \equiv 1 \ (mod \ \ m)$	[Subst (1) em (2)]
4. $tm \equiv 0 \ (mod \ \ m)$	[Def. $\equiv (mod \ \ m)$]
5. $-tm \equiv 0 \ (mod \ \ m)$	[Mult (4) por -1]
6. $sa \equiv 1 \ (mod \ \ m)$	[Soma (3) e (5)]
7. $s = \overline{a}$	[Def. $\overline{a}$]

Congruências Lineares

- Sejam $a, b \in Z$ inteiros e $m \in Z^+$.
- Um congruência linear é uma equação do tipo

$$ax \equiv b \ (mod \ \ m)$$

- Como resolver essa equação?

Congruências Lineares

Para resolver a equação $ax \equiv b \pmod{m}$:

- Encontre o inverso de a módulo m, $\bar{a}$.
- Calcule $\bar{a}b$.
- A solução é $x \equiv \bar{a}b \pmod{m}$.

Congruências Lineares

Exemplo.

- Seja a equivalência $35x \equiv 4 \ (mod\ 3)$.
- O inverso de 35 módulo 3 é -1.
- $\bar{a}b = (-1) \cdot 4$
- Então, a solução é $x \equiv -4 \ (mod\ 3)$.

Congruências Lineares

Exercício.

- Calcule a solução de
  a) $3x \equiv 2 \ (mod\ 7)$.
  b) $5x \equiv \ 2 \ (mod\ 34)$
  c) $74x \equiv \ 5 \ (mod\ 33)$

Congruências Lineares

Por que isso funciona?

Premissas: $ax \equiv b \ (mod\ \ m)$ e $\overline{a}$ existe.
Conclusão: $x \equiv \overline{a}b \ (mod\ \ m)$.

1. $ax \equiv b \ (mod\ \ m)$ [Premissa]
2. $\overline{a}ax \equiv \overline{a}b \ (mod\ \ m)$ [Mult. (1) por $\overline{a}$]
3. $\overline{a}a \equiv 1 \ (mod\ \ m)$ [Premissa e def. $\overline{a}$]
4. $\overline{a}ax \equiv x \ (mod\ \ m)$ [Mult. (3) por x]
5. $x \equiv \overline{a}ax \ (mod\ \ m)$ [Comutatividade em (4)]
6. $x \equiv \overline{a}b \ (mod\ \ m)$ [Transitividade em (5) e (2)]

Teorema Chinês do Resto

O que é, o que é?

- Quando dividido por 3, dá resto 2.
- Quando dividido por 5, dá resto 3.
- Quando dividido por 7, dá resto 2.

Teorema Chinês do Resto

O que é, o que é?

- Quando dividido por 3, dá resto 2.
- Quando dividido por 5, dá resto 3.
- Quando dividido por 7, dá resto 2.
- Resposta: 23 (módulo 105)
- Que outro número é também solução para esse problema?

Teorema Chinês do Resto

O que é, o que é?

- $x \equiv 2 \ (mod \ 3)$
- $x \equiv 3 \ (mod \ 5)$
- $x \equiv 2 \ (mod \ 7)$

Teorema Chinês do Resto

- Sejam m_1, m_2, ..., m_n primos relativos 2 a 2.
- Sejam a_1, a_2, ..., a_n inteiros.
- O sistema de congruências

$$
\begin{aligned}
x &\equiv a_1 \; (mod \;\; m_1) \\
x &\equiv a_2 \; (mod \;\; m_2) \\
&\vdots \\
x &\equiv a_n \; (mod \;\; m_n)
\end{aligned}
$$

  tem solução única (módulo $m = m_1 m_2 \dots m_n$).
- Ou seja, existe uma solução x, $0 \leq x < m$ e, todas as demais soluções y são $x \equiv y \; (mod \;\; m)$.

Teorema Chinês do Resto

Como resolver esse sistema?

- Seja $m = m_1 m_2 \ldots m_n$.
- Seja $M_k = m/m_k$. Ou seja, M_k é m sem o termo m_k.
- Calcule y_k, o inverso de M_k módulo m_k.
- A solução é $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$.

Teorema Chinês do Resto

Por que isso funciona?

Vamos provar que $a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \equiv a_1 \pmod{m_1}$.

1. $M_1 y_1 \equiv 1 \pmod{m_1}$ [Premissa]
2. $a_1 M_1 y_1 \equiv a_1 \pmod{m_1}$ [Mult 2 lados de (1) por a_1]
3. $M_2 \equiv 0 \pmod{m_1}$ [Def. $\equiv \pmod{m_1}$ e $M_2 = m_1 m_3$]
4. $M_3 \equiv 0 \pmod{m_1}$ [Def. $\equiv \pmod{m_1}$ e $M_3 = m_1 m_2$]
5. $a_2 M_2 y_2 \equiv 0 \pmod{m_1}$ [Mult 2 lados de (3) por $a_2 y_2$]
6. $a_3 M_3 y_3 \equiv 0 \pmod{m_1}$ [Mult 2 lados de (4) por $a_3 y_3$]
7. $a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \equiv a_1 \pmod{m_1}$ [(2)+(5)+(6)]

Teorema Chinês do Resto

Por que isso funciona?

De forma similar ao slide anterior, podemos provar que

$$a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \equiv a_2 \ (mod \ \ m_2)$$
$$a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \equiv a_3 \ (mod \ \ m_3)$$

Assim como, para provar para mais de 3 equações, o raciocínio é o mesmo.

Teorema Chinês do Resto

Exemplo. Seja o sistema

$$
\begin{aligned}
x &\equiv 2 \ (mod\ 3) \\
x &\equiv 3 \ (mod\ 5) \\
x &\equiv 2 \ (mod\ 7)
\end{aligned}
$$

- Como 3, 5 e 7 são primos relativos 2 a 2, podemos usar o Teorema Chinês do Resto.
- $M_1 = (3 \cdot 5 \cdot 7)/3 = 35$, $M_2 = 21$ e $M_3 = 15$.
- $y_1 = -1$ (inverso de 35 módulo 3)
- $y_2 = 1$ (inverso de 21 módulo 5)
- $y_3 = 1$ (inverso de 15 módulo 7)
- A solução é

$$x = (2 \cdot 35 \cdot -1) + (3 \cdot 21 \cdot 1) + (2 \cdot 15 \cdot 1) = 23$$

Teorema Chinês do Resto

Exercício.

$$x \equiv 2 \ (mod \ 3)$$
$$x \equiv 1 \ (mod \ 4)$$
$$x \equiv 3 \ (mod \ 5)$$

Pseudoprimos

Pequeno Teorema de Fermat

- Se p é primo e a não é divisível por p, então $a^{p-1} \equiv 1\ (mod\ \ p)$
- Exemplo. 11 é primo e 30 não é divisível por 11. $30^{10} = 590.490.000.000.000$. $590.490.000.000.000 \textbf{ mod } 11 = 1$.

Pseudoprimos

Pequeno Teorema de Fermat

- Outra variação do teorema.
- Se p é um número primo, então, para todo inteiro a, $a^p \equiv a \ (mod \ p)$.
- Exemplo. 2^{11} **mod** $11 = 2$ **mod** $11 = 2$.

Pseudoprimos

Primalidade

- Dado um n, como saber se ele é primo?
- Sabemos que, se n não tem divisor primo $d \leq \sqrt{n}$, então n é primo.

Pseudoprimos

Primalidade

- Dado um n, como saber se ele é primo?
- Sabemos que, se n não tem divisor primo $d \leq \sqrt{n}$, então n é primo.
- Ou seja, temos que encontrar todos os primos menores que $\sqrt{n}$ e testar se estes primos dividem n. Se nenhum deles divide n, então n é primo.

Pseudoprimos

Primalidade

- Dado um n, como saber se ele é primo?
- Sabemos que, se n não tem divisor primo $d \leq \sqrt{n}$, então n é primo.
- Ou seja, temos que encontrar todos os primos menores que $\sqrt{n}$ e testar se estes primos dividem n. Se nenhum deles divide n, então n é primo.
- Existem formas mais eficientes para testar primalidade.

Pseudoprimos

Primalidade

- Pelo Pequeno Teorema de Fermat
  Se n é primo (e 2 não é divisível por n), então
  $2^{n-1} \equiv 1 \ (mod \ n)$

Pseudoprimos

Primalidade

- Pelo Pequeno Teorema de Fermat
  Se n é primo (e 2 não é divisível por n), então
  $2^{n-1} \equiv 1 \pmod{n}$
- Infelizmente, o converso não é verdade.
  Ou seja, se $2^{n-1} \equiv 1 \pmod{n}$, então n pode ser primo ou pode ser composto.

Pseudoprimos

Primalidade

- Pelo Pequeno Teorema de Fermat
  Se n é primo (e 2 não é divisível por n), então
  $2^{n-1} \equiv 1 \ (mod \ \ n)$
- Infelizmente, o converso não é verdade.
  Ou seja, se $2^{n-1} \equiv 1 \ (mod \ \ n)$, então n pode ser primo ou pode ser composto.
- Resumindo: em tese, este teorema não serve para teste de primalidade. Ou serve?

Pseudoprimos

Primalidade

- Na verdade, se $2^{n-1} \equiv 1 \ (mod \ n)$, então há uma grande chance de n ser primo.

Pseudoprimos

Primalidade

- Na verdade, se $2^{n-1} \equiv 1 \ (mod \ n)$, então há uma grande chance de n ser primo.
- Existem muito mais primos que satisfazem $2^{n-1} \equiv 1 \ (mod \ n)$ do que compostos que satisfazem esta congruência.

Pseudoprimos

Primalidade

- Na verdade, se $2^{n-1} \equiv 1 \ (mod \ n)$, então há uma grande chance de n ser primo.
- Existem muito mais primos que satisfazem $2^{n-1} \equiv 1 \ (mod \ n)$ do que compostos que satisfazem esta congruência.
- "Muito mais" significa:
  Existem 455.052.512 de primos menores que 10^{10}.
  E apenas 14.884 compostos que satisfazem a congruência

Pseudoprimos

Primalidade

- Na verdade, se $2^{n-1} \equiv 1 \ (mod \ n)$, então há uma grande chance de n ser primo.
- Existem muito mais primos que satisfazem $2^{n-1} \equiv 1 \ (mod \ n)$ do que compostos que satisfazem esta congruência.
- "Muito mais" significa:
  Existem 455.052.512 de primos menores que 10^{10}.
  E apenas 14.884 compostos que satisfazem a congruência
- Estes compostos são chamados de pseudoprimos.

Pseudoprimos

- Seja b um inteiro positivo.
- Se n é um inteiro composto e $b^{n-1} \equiv 1 \ (mod \ n)$, então n é chamado de *pseudoprimo na base b*.

Pseudoprimos

Resumindo

- Se n satisfaz $b^{n-1} \equiv\ 1\ (mod\ \ n)$, então n é primo ou é pseudoprimo
  Apesar de sabermos que há grandes chances de ser primo, não temos 100% de certeza.
- Se n não satisfaz esta congruência, então n é composto.

Pseudoprimos

Teste de Primalidade

- $2^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- $3^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- $\vdots$
- ${b_m}^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)

Pseudoprimos

Teste de Primalidade

- $2^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- $3^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- $\vdots$
- ${b_m}^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- Se n passar em todas as bases que testamos, então, ainda não temos uma conclusão.

  Existem números compostos que passam em todas as bases. São chamados de números de Carmichael.

Pseudoprimos

Teste de Primalidade

- $2^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- $3^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- $\vdots$
- ${b_m}^{n-1} \equiv 1 \ (mod \ n)$? Se sim, continue. Senão, pare (n é composto)
- Se n passar em todas as bases que testamos, então, ainda não temos uma conclusão.
  Existem números compostos que passam em todas as bases. São chamados de números de Carmichael.
- Para casos difíceis, temos que usar outros algoritmos (que são probabilísticos: o algoritmo submete n a uma série de testes e, a probabilidade de n ser composto e passar em todos os testes é quase zero.)

Criptografia de Chave Pública

- Qualquer pessoa pode enviar uma mensagem para qualquer outra sem precisar combinar previamente como criptografar a mensagem.
- Uma pessoa deixa pública uma chave (números) a ser usada para criptografar a mensagem.
- Outra pessoa utiliza esta chave para criptografar a mensagem.
- Apenas o destinatário sabe como decriptografar (usando uma chave privada).

Criptografia de Chave Pública

- O algoritmo utiliza-se de 2 primos grandes (tipicamente com 200 dígitos cada) multiplicados um pelo outro.
- O resultado é um número de 400 dígitos.
- Para quebrar o código, deve-se fatorar um número de 400 dígitos.
- Hoje, o melhor algoritmo de fatoração leva 2 bilhões de anos para fatorar.

Criptografia de Chave Pública

- Chave pública: n e e, onde n é o produto dos primos p e q
- Função para criptografar: $C = M^e \textbf{ mod } n$
- Chave privada: d, onde d é o inverso de e módulo $(p-1)(q-1)$
- Função para decriptografar: $M = C^d \textbf{ mod } n$

Criptografia de Chave Pública

- Chave pública: n e e, onde n é o produto dos primos p e q
- Função para criptografar: $C = M^e \textbf{ mod } n$
- Chave privada: d, onde d é o inverso de e módulo $(p-1)(q-1)$
- Função para decriptografar: $M = C^d \textbf{ mod } n$
- Exemplo:
  Sejam $n = 2537$, $e = 13$ e $M = 3$.
  Então $C = 3^{13} \textbf{ mod } 2537 = 1087$.
  Sejam $d = 937$. Então $M = 1087^{937} \textbf{ mod } 2537 = 3$.
  Neste exemplo, usamos $p = 43$ e $q = 59$.

Criptografia de Chave Pública

- Chave pública: n e e, onde n é o produto dos primos p e q
- Função para criptografar: $C = M^e \textbf{ mod } n$
- Chave privada: d, onde d é o inverso de e módulo $(p-1)(q-1)$
- Função para decriptografar: $M = C^d \textbf{ mod } n$
- Exemplo:
  Sejam $n = 2537$, $e = 13$ e $M = 3$.
  Então $C = 3^{13} \textbf{ mod } 2537 = 1087$.
  Sejam $d = 937$. Então $M = 1087^{937} \textbf{ mod } 2537 = 3$.
  Neste exemplo, usamos $p = 43$ e $q = 59$.
- Mais detalhes: Seção 3.7 de *Discrete Mathematics*
- História da criptografia: *The Code Book* de Simon Singh.