Notas sobre teoria dos números (3)

Fonte: livros do L. Lóvasz e Kenneth Rosen (ref. completa na página)

Centro de Informática
Universidade Federal de Pernambuco

2007.1 / CIn-UFPE

Motivação

- Uma senhora estava caminhando para um mercado quando um cavalo se bateu com a sua cesta de ovos. O cavaleiro queria pagar os danos e perguntou para a senhora quantos ovos haviam na cesta.
- Ela não se lembrava exatamente da quantidade, mas sabia que se tirasse os ovos da cesta de três em três, sobravam dois ovos. Se tirasse de 5 em 5, sobravam 3 ovos e de 7 em 7 sobravam 2.
- Qual seria a menor quantidade de ovos que ela poderia ter?
- Como formular esse problema usando a notação da aritmética modular?

Motivação

- Uma senhora estava caminhando para um mercado quando um cavalo se bateu com a sua cesta de ovos. O cavaleiro queria pagar os danos e perguntou para a senhora quantos ovos haviam na cesta.
- Ela não se lembrava exatamente da quantidade, mas sabia que se tirasse os ovos da cesta de três em três, sobravam dois ovos. Se tirasse de 5 em 5, sobravam 3 ovos e de 7 em 7 sobravam 2.
- Qual seria a menor quantidade de ovos que ela poderia ter?
- Como formular esse problema usando a notação da aritmética modular?

Motivação

- Uma senhora estava caminhando para um mercado quando um cavalo se bateu com a sua cesta de ovos. O cavaleiro queria pagar os danos e perguntou para a senhora quantos ovos haviam na cesta.
- Ela não se lembrava exatamente da quantidade, mas sabia que se tirasse os ovos da cesta de três em três, sobravam dois ovos. Se tirasse de 5 em 5, sobravam 3 ovos e de 7 em 7 sobravam 2.
- Qual seria a menor quantidade de ovos que ela poderia ter?
- Como formular esse problema usando a notação da aritmética modular?

Exemplo

No século um, o matemático chinês chamado Sun-Tsu se perguntou: Que número será esse de forma que quando dividido por 3, o resto é 2; quando dividido por 5, o resto é 3; e quando dividido por 7, o resto é 2?

A pergunta é: Qual é a solução para o seguinte sistema de congruências?

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

Teorema (Teorema chinês do resto)

Sejam $m_1, m_2, \ldots m_n$ inteiros positivos primos entre si. O sistema

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

possui uma única solução módulo $m = m_1.m_2.\ldots.m_n$. (Ou seja, existe uma solução x com $0 \leq x < m$, e todas as outras soluções são congruentes módulo m com essa solução).

- Como calcular x:
  - faça $m = m_1.m_2.\ldots.m_n$;
  - para $k = 1, 2, \ldots n$ faça $M_k = m/m_k$;
  - chame Y_k o inverso de M_k módulo m_k e calcule Y_k, Ou seja, $M_k.Y_k \equiv 1\ (mod\ m_k)$;
  - $x \equiv a_1 M_1 Y_1 + a_2 M_2 Y_2 + \ldots a_n M_n Y_n\ (mod\ m)$.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (\text{mod } 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (\text{mod } 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (\text{mod } 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (\text{mod } 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (\text{mod } 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (\text{mod } 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (\text{mod } 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (\text{mod } 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (mod\ 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (mod\ 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1$ (mod 5);
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1$ (mod 7);
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (\text{mod } 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (\text{mod } 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Quantos ovos o cavaleiro deve pagar?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois:
   - quero calcular i, de forma que $35.i \equiv 1\ (mod\ 3)$;
   - como $35 \equiv 2\ (mod\ 3)$, posso calcular $2.i \equiv 1\ (mod\ 3)$
   - logo $i = 2$, pois $2.2 \equiv 1\ (mod\ 3)$.
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (\text{mod } 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (\text{mod } 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 105) \equiv 233 \equiv 23\ (mod\ 105)$.

Resp. Pelo menos 23 ovos.

Outro exemplo

- Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?
- $x \equiv 1\ (mod\ 2)$ e $x \equiv 1\ (mod\ 3)$;
- $m = 6$, $M_1 = 3$ e $M_2 = 2$;
- Y_1 é o inverso de 3 mod 2, como $3 \equiv 1\ (mod\ 2) \rightarrow Y_1 \equiv 1\ (mod\ 2)$;
- Y_2 é o inverso de 2 mod 3, como 2 mod 3 = 2, logo $Y_2 \equiv 2$ (mod 3);
- $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
- $x \equiv 7\ (mod\ 6)$.

Outro exemplo

- Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?
- $x \equiv 1\ (mod\ 2)$ e $x \equiv 1\ (mod\ 3)$;
- $m = 6$, $M_1 = 3$ e $M_2 = 2$;
- Y_1 é o inverso de 3 mod 2, como $3 \equiv 1\ (mod\ 2) \rightarrow Y_1 \equiv 1\ (mod\ 2)$;
- Y_2 é o inverso de 2 mod 3, como 2 mod 3 = 2, logo $Y_2 \equiv 2\ (\text{mod } 3)$;
- $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
- $x \equiv 7\ (mod\ 6)$.

Outro exemplo

- Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?
- $x \equiv 1\ (mod\ 2)$ e $x \equiv 1\ (mod\ 3)$;
- $m = 6$, $M_1 = 3$ e $M_2 = 2$;
- Y_1 é o inverso de 3 mod 2, como $3 \equiv 1\ (mod\ 2) \rightarrow Y_1 \equiv 1\ (mod\ 2)$;
- Y_2 é o inverso de 2 mod 3, como 2 mod 3 = 2, logo $Y_2 \equiv 2\ (\text{mod } 3)$;
- $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
- $x \equiv 7\ (mod\ 6)$.

Outro exemplo

- Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?
- $x \equiv 1\ (mod\ 2)$ e $x \equiv 1\ (mod\ 3)$;
- $m = 6$, $M_1 = 3$ e $M_2 = 2$;
- Y_1 é o inverso de 3 mod 2, como $3 \equiv 1\ (mod\ 2) \rightarrow$ $Y_1 \equiv 1\ (mod\ 2)$;
- Y_2 é o inverso de 2 mod 3, como 2 mod 3 = 2, logo $Y_2 \equiv 2\ (mod\ 3)$;
- $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
- $x \equiv 7\ (mod\ 6)$.

Outro exemplo

- Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?
- $x \equiv 1\ (mod\ 2)$ e $x \equiv 1\ (mod\ 3)$;
- $m = 6$, $M_1 = 3$ e $M_2 = 2$;
- Y_1 é o inverso de 3 mod 2, como $3 \equiv 1\ (mod\ 2) \rightarrow Y_1 \equiv 1\ (mod\ 2)$;
- Y_2 é o inverso de 2 mod 3, como 2 mod 3 = 2, logo $Y_2 \equiv 2$ (mod 3);
- $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
- $x \equiv 7\ (mod\ 6)$.

Outro exemplo

- Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?
- $x \equiv 1\ (mod\ 2)$ e $x \equiv 1\ (mod\ 3)$;
- $m = 6$, $M_1 = 3$ e $M_2 = 2$;
- Y_1 é o inverso de 3 mod 2, como $3 \equiv 1\ (mod\ 2) \rightarrow Y_1 \equiv 1\ (mod\ 2)$;
- Y_2 é o inverso de 2 mod 3, como 2 mod 3 = 2, logo $Y_2 \equiv 2$ (mod 3);
- $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
- $x \equiv 7\ (mod\ 6)$.

Outro exemplo

- Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?
- $x \equiv 1\ (mod\ 2)$ e $x \equiv 1\ (mod\ 3)$;
- $m = 6$, $M_1 = 3$ e $M_2 = 2$;
- Y_1 é o inverso de 3 mod 2, como $3 \equiv 1\ (mod\ 2) \rightarrow$ $Y_1 \equiv 1\ (mod\ 2)$;
- Y_2 é o inverso de 2 mod 3, como 2 mod 3 = 2, logo $Y_2 \equiv 2$ (mod 3);
- $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
- $x \equiv 7\ (mod\ 6)$.

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos *n* congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos *n* congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos *n* congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos *n* congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos *n* congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos *n* congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos *n* congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos n congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

Entendendo a prova do teorema chinês do resto

- Se entendermos o resultado para um sistema com duas congruências podemos aplicar o mesmo raciocínio para o caso de termos n congruências.

$$x \equiv a_1 \ (mod\ m_1) \quad (1)$$
$$x \equiv a_2 \ (mod\ m_2) \quad (2)$$

- Temos que $m = m_1 \cdot m_2$, $M_1 = m_2$ e $M_2 = m_1$
- mdc(m_1, m_2)= 1 (3)
- De (3) temos $Y_1 m_2 \equiv 1 \ (mod\ m_1)$ (3.1)
- De (3) tb. temos $Y_2 m_1 \equiv 1 \ (mod\ m_2)$ (3.2)
- De (1): $x = a_1 + k \cdot m_1$ (4)
- Substituindo (4) em (2): $a_+ k m_1 \equiv a_2 \ (mod\ m_2)$
  $\rightarrow \ k m_1 \equiv a_2 - a_1 \ (mod\ m_2)$
- (3.2) diz que $Y_2 m_1 \equiv 1 \ (mod\ m_2)$, logo
  $k \equiv Y_2(a_2 - a_1) \ (mod\ m_2) \rightarrow k = Y_2(a_2 - a_1) + m_2 \cdot z$ (5)
- Substituindo (5) em (4): $x = a_1 + (Y_2(a_2 - a_1) + m_2 \cdot z) \cdot m_1$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1) \ (6.1)$
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2) \ (6.2)$
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- $x = a_1 + m_1 Y_2 a_2 - m_1 Y_2 a_1 + m_1 m_2 z$
- $x = a_1(1 - M_2 Y_2) + M_2 Y_2 a_2 \ mod \ m$
- Precisamos agora apenas provar que $(1 - M_2 Y_2) \equiv M_1 Y_1 \ (mod \ m)$ para chegar a $x = a_1 M_1 Y_1 + a_2 M_2 Y_2 \ (mod \ m)$
- (3.1) nos diz que $Y_1 M_1 \equiv 1 \ (mod \ m_1) \rightarrow m_1 | (1 - Y_1 M_1)$ (6.1)
- (3.2) nos diz que $Y_2 M_2 \equiv 1 \ (mod \ m_2) \rightarrow m_2 | (1 - Y_2 M_2)$ (6.2)
- Portanto temos $m_1 \cdot m_2 = (1 - Y_1 M_1) \cdot (1 - Y_2 M_2)$
- $m \cdot c_1 = 1 - M2Y2 - M_1 Y_1 + M_1 M_2 Y_1 Y_2$ veja: $M_1 M_2 = m$ e seja $Y_1 Y_2 = c_2$.
- $mc_1 - mc_2 = 1 - M_2 Y_2 - M_1 Y_1$
- $M_1 Y_1 = 1 - M_2 Y_2 + mc_2 - mc_1$
- $M_1 Y_1 = 1 - M2Y2 + m \cdot c$, considerando $c_2 - c_1 = c$
- Logo $M_1 Y_1 \equiv 1 - M_2 Y_2 \ (mod \ m)$

- Suponha que $m_1, m_2, \ldots m_n$ são inteiros primos entre si maiores ou iguais a 2.
- Como consequência do teorema Chinês do resto, é possível provar que um inteiro a com $0 \leq a < m$ pode ser unicamente representado pela n-tupla:
- $(a \ mod \ m_1, \ a \ mod \ m_2, \ldots, \ \ mod \ m_n)$

Exemplo Os pares usados para representar os inteiros não negativos menores que 12, onde o primeiro componente do par é o resto da divisão por 3 e o segundo é o resto da divisão por 4 são:

- $0 = (0,0) \quad 1 = (1,1) \quad 2 = (2,2) \quad 3 = (0,3)$
- $4 = (1,0) \quad 5 = (2,1) \quad 6 = (0,2) \quad 7 = (1,3)$
- $8 = (2,0) \quad 9 = (0,1) \quad 10 = (1,2) \quad 11 = (2,3)$

- Suponha que $m_1, m_2, \ldots m_n$ são inteiros primos entre si maiores ou iguais a 2.
- Como consequência do teorema Chinês do resto, é possível provar que um inteiro a com $0 \leq a < m$ pode ser unicamente representado pela n-tupla:
- $(a \bmod m_1, \ a \bmod m_2, \ldots, \ \bmod m_n)$

Exemplo Os pares usados para representar os inteiros não negativos menores que 12, onde o primeiro componente do par é o resto da divisão por 3 e o segundo é o resto da divisão por 4 são:

- $0 = (0,0) \quad 1 = (1,1) \quad 2 = (2,2) \quad 3 = (0,3)$
- $4 = (1,0) \quad 5 = (2,1) \quad 6 = (0,2) \quad 7 = (1,3)$
- $8 = (2,0) \quad 9 = (0,1) \quad 10 = (1,2) \quad 11 = (2,3)$

- Para realizar aritmética com inteiros grandes, escolhemos módulos $m_1, m_2, \ldots, m_n$, onde cada m_i é um inteiro maior que 2 e $mdc(m_i, m_j) = 1$, para $i \neq j$ e $m = m_1.m_2.\ldots.m_n$ é maior do que o resultado da operação aritmética que queremos realizar.
- Podemos então realizar as operações aritméticas sobre os componentes correspondentes das n-tuplas de restos.
- Em seguida, recuperamos o resultado da operação resolvendo o sistema de n congruências.

Exemplo No exemplo anterior representamos $5 = (2, 1)$ e $1 = (1, 1)$; calculamos $5 + 1$ da seguinte maneira:
$(2, 1) + (1, 1) = (3 \ mod \ 3, \ 2 \ mod \ 4) = (0, 2)$.

- Como encontramos que número é representado por $(0, 2)$?
- Solucionando o sistema $x \equiv 0 \ (mod \ 3) \ , x \equiv 2 \ (mod \ 4)$.
- $x \equiv 6 (mod \ 12)$

- Para realizar aritmética com inteiros grandes, escolhemos módulos $m_1, m_2, \ldots, m_n$, onde cada m_i é um inteiro maior que 2 e $mdc(m_i, m_j) = 1$, para $i \neq j$ e $m = m_1.m_2.\ldots.m_n$ é maior do que o resultado da operação aritmética que queremos realizar.
- Podemos então realizar as operações aritméticas sobre os componentes correspondentes das n-tuplas de restos.
- Em seguida, recuperamos o resultado da operação resolvendo o sistema de n congruências.

Exemplo No exemplo anterior representamos $5 = (2, 1)$ e $1 = (1, 1)$; calculamos $5 + 1$ da seguinte maneira:
$(2, 1) + (1, 1) = (3 \ mod \ 3, \ 2 \ mod \ 4) = (0, 2)$.

- Como encontramos que número é representado por $(0, 2)$?
- Solucionando o sistema $x \equiv 0 \ (mod \ 3)$, $x \equiv 2 \ (mod \ 4)$.
- $x \equiv 6 (mod \ 12)$

- Para realizar aritmética com inteiros grandes, escolhemos módulos $m_1, m_2, \ldots, m_n$, onde cada m_i é um inteiro maior que 2 e $mdc(m_i, m_j) = 1$, para $i \neq j$ e $m = m_1.m_2.\ldots.m_n$ é maior do que o resultado da operação aritmética que queremos realizar.
- Podemos então realizar as operações aritméticas sobre os componentes correspondentes das n-tuplas de restos.
- Em seguida, recuperamos o resultado da operação resolvendo o sistema de n congruências.

Exemplo No exemplo anterior representamos $5 = (2, 1)$ e $1 = (1, 1)$; calculamos $5 + 1$ da seguinte maneira:
$(2, 1) + (1, 1) = (3 \ mod \ 3, \ 2 \ mod \ 4) = (0, 2)$.

- Como encontramos que número é representado por $(0, 2)$?
- Solucionando o sistema $x \equiv 0 \ (mod \ 3)$, $x \equiv 2 \ (mod \ 4)$.
- $x \equiv 6 (mod \ 12)$

Vantagens do método

- É possível realizar aritmética com inteiros maiores do que a capacidade de um determinado computador;
- as computações entre os diferentes componentes das tuplas podem ser realizadas em paralelo.

Vantagens do método

- É possível realizar aritmética com inteiros maiores do que a capacidade de um determinado computador;
- as computações entre os diferentes componentes das tuplas podem ser realizadas em paralelo.

Mais um exemplo

- O números $99, 98, 97$ e 95 são primos entre si.
- O resultado de 99.98.97.95 é 89.403.930.
- Usando os resultados que acabamos de aprender, podemos realizar aritmética com números menores que 89.403.930, operando sobre números menores que 100.
- $123684 = (33, 8, 9, 89)$ e $413456 = (32, 92, 42, 16)$
- A soma deses números é
  $(65 \ mod \ 99, 100 \ mod \ 98, 51 \ mod \ 97.105 \ mod \ 95)$
  $= (65, 2, 51, 10)$
- Solucionando o sistema de congruências a única solução menor que 89.403.930 é 537.140. Esse é o único momento onde é feita aritmética com inteiros maiores que 100.

Mais um exemplo

- O números $99, 98, 97$ e 95 são primos entre si.
- O resultado de $99.98.97.95$ é $89.403.930$.
- Usando os resultados que acabamos de aprender, podemos realizar aritmética com números menores que $89.403.930$, operando sobre números menores que 100.
- $123684 = (33, 8, 9, 89)$ e $413456 = (32, 92, 42, 16)$
- A soma deses números é
  $(65 \ mod \ 99, 100 \ mod \ 98, 51 \ mod \ 97.105 \ mod \ 95)$
  $= (65, 2, 51, 10)$
- Solucionando o sistema de congruências a única solução menor que $89.403.930$ é 537.140. Esse é o único momento onde é feita aritmética com inteiros maiores que 100.

- Algoritmo de divisão baseado no seguinte ressultado:

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

- Crivo de Erastótenes (ou divisão por tentativa): lista-se todos os números ímpares de 3 à *n*. Selecionamos o primeiro número da lista (3) e cortamos todos os seus múltiplos, emguida fazemos o mesmo para o próximo número e assim pordiante. Todos os números não cortados são primos.
- Teste de Lucas-Lehmer: teste bastante eficiente usado para os primos *Mersenne*, que são da forma $2^p - 1$, onde *p* também é um primo. Atualmente os maiores primos conhecidos são primos Mersenne, por causa desse teste.

- Algoritmo de divisão baseado no seguinte ressultado:

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

- Crivo de Erastótenes (ou divisão por tentativa): lista-se todos os números ímpares de 3 à *n*. Selecionamos o primeiro número da lista (3) e cortamos todos os seus múltiplos, emguida fazemos o mesmo para o próximo número e assim pordiante. Todos os números não cortados são primos.
- Teste de Lucas-Lehmer: teste bastante eficiente usado para os primos *Mersenne*, que são da forma $2^p - 1$, onde p também é um primo. Atualmente os maiores primos conhecidos são primos Mersenne, por causa desse teste.

- Algoritmo de divisão baseado no seguinte ressultado:

Teorema

Se n é um número composto, então n possui um divisor primo menor ou igual a $\sqrt{n}$

- Crivo de Erastótenes (ou divisão por tentativa): lista-se todos os números ímpares de 3 à *n*. Selecionamos o primeiro número da lista (3) e cortamos todos os seus múltiplos, emguida fazemos o mesmo para o próximo número e assim pordiante. Todos os números não cortados são primos.
- Teste de Lucas-Lehmer: teste bastante eficiente usado para os primos *Mersenne*, que são da forma $2^p - 1$, onde *p* também é um primo. Atualmente os maiores primos conhecidos são primos Mersenne, por causa desse teste.

- Teste de Miller-Rabin: teste probabilístico baseado no pequeno teorema de Fermat.
- Teste de primalidade AKS (Agrawal-Kayal-Saxena): algoritmo determinístico em tempo polinomial. Resultado publicado por cientistas indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena em 06 de Agosto de 2002. *Pimes is P*.
    - Receberam o prêmio Gödel de 2006.

- Teste de Miller-Rabin: teste probabilístico baseado no pequeno teorema de Fermat.
- Teste de primalidade AKS (Agrawal-Kayal-Saxena): algoritmo determinístico em tempo polinomial. Resultado publicado por cientistas indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena em 06 de Agosto de 2002. *Pimes is P*.
  - Receberam o prêmio Gödel de 2006.

Teorema (O pequeno teorema de Fermat)

Se p é primo e a a é um inteiro não divisível por p, então $a^{p-1} \equiv 1 \pmod{p}$. Além disso, para todo inteiro a nós temos que $a^p \equiv a \pmod{p}$.

- Como consequência desse teorema, temos um método eficiente para o teste de primalidade.
- Entretanto, existem números compostos de forma que $n \mid 2^{n-1} - 1$. Esses números são chamados de pseudoprimos.

Exemplo

O inteiro 341 é um pseudoprimo pois $341 \mid 2^{340} - 1$

- Mas, felizmente os pseudoprimos são relativamente raros.
- Atualmente usa-se o **teste probabilístico de primalidade**, baseado nesse teorema.

Teorema (O pequeno teorema de Fermat)

Se p é primo e a a é um inteiro não divisível por p, então $a^{p-1} \equiv 1 \pmod{p}$. Além disso, para todo inteiro a nós temos que $a^p \equiv a \pmod{p}$.

- Como consequência desse teorema, temos um método eficiente para o teste de primalidade.
- Entretanto, existem números compostos de forma que $n \mid 2^{n-1} - 1$. Esses números são chamados de pseudoprimos.

Exemplo

O inteiro 341 é um pseudoprimo pois $341 \mid 2^{340} - 1$

- Mas, felizmente os pseudoprimos são relativamente raros.
- Atualmente usa-se o **teste probabilístico de primalidade**, baseado nesse teorema.

Teorema (O pequeno teorema de Fermat)

Se p é primo e a a é um inteiro não divisível por p, então $a^{p-1} \equiv 1 \pmod{p}$. *Além disso, para todo inteiro a nós temos que* $a^p \equiv a \pmod{p}$.

- Como consequência desse teorema, temos um método eficiente para o teste de primalidade.
- Entretanto, existem números compostos de forma que $n \mid 2^{n-1} - 1$. Esses números são chamados de pseudoprimos.

Exemplo

O inteiro 341 é um pseudoprimo pois $341 \mid 2^{340} - 1$

- Mas, felizmente os pseudoprimos são relativamente raros.
- Atualmente usa-se o **teste probabilístico de primalidade**, baseado nesse teorema.

Teorema (O pequeno teorema de Fermat)

Se p é primo e a a é um inteiro não divisível por p, então $a^{p-1} \equiv 1 \pmod{p}$. Além disso, para todo inteiro a nós temos que $a^p \equiv a \pmod{p}$.

- Como consequência desse teorema, temos um método eficiente para o teste de primalidade.
- Entretanto, existem números compostos de forma que $n \mid 2^{n-1} - 1$. Esses números são chamados de pseudoprimos.

Exemplo

O inteiro 341 é um pseudoprimo pois $341 \mid 2^{340} - 1$

- Mas, felizmente os pseudoprimos são relativamente raros.
- Atualmente usa-se o **teste probabilístico de primalidade**, baseado nesse teorema.

O sistema RSA

- Criposistema de chave pública
- 1976, três pesquisadores do M. I. T: Ron Rivest, Adi Shamir e Len Adleman
- Baseado em exponeciação modular, módulo o produto de dois primos.
- A chave de encriptação ́baseada no módulo de $n = p \cdot q$, onde p e q são primos grandes; e em um expoente e, que é primo entre si com $(p-1) \cdot (q-1)$.
- Para encontrar os dois primos grandes é usado o teste de primalidade probabilístico.

Encriptação

- As mensagens são traduzidas em sequências de inteiros. E subdivida em blocos de inteiros.
- O sistema transforma a cada bloco de inteiros M (que juntos representam o texto original) para uma mensagem C, que representa o texto cifrado ou a mensagem encriptada, usando a seguinte função:
  - $C \equiv M^e \ \mathbf{mod}\ n$

Encriptação

- As mensagens são traduzidas em sequências de inteiros. E subdivida em blocos de inteiros.
- O sistema transforma a cada bloco de inteiros M (que juntos representam o texto original) para uma mensagem C, que representa o texto cifrado ou a mensagem encriptada, usando a seguinte função:
  - $C \equiv M^e$ **mod** n

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 59$; e $e = 13$.Dessa forma, $n = 2537$.
- É possível observar também que o *mdc* de e e $(p-1)\cdot(q-1)$ é 1.
- Aa letras da palavra STOP são transformadas em números usando por exemplo, a sua posição no alfabeto:
  - 1819 1415
- Cada bloco é encriptado usando a função $C \equiv M^{13}$ **mod** 2537.
- Rapidamente é possível calcular 181913 **mod** $2537 = 2081$ e 1415^{13} **mod** $2537 = 2182$.
- A mensagem encriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 59$; e $e = 13$.Dessa forma, $n = 2537$.
- É possível observar também que o *mdc* de e e $(p-1)\cdot(q-1)$ é 1.
- Aa letras da palavra STOP são transformadas em números usando por exemplo, a sua posição no alfabeto:
  - 1819 1415
- Cada bloco é encriptado usando a função $C \equiv M^{13}$ **mod** 2537.
- Rapidamente é possível calcular 181913 **mod** $2537 = 2081$ e 1415^{13} **mod** $2537 = 2182$.
- A mensagem encriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 59$; e $e = 13$.Dessa forma, $n = 2537$.
- É possível observar também que o *mdc* de e e $(p-1)\cdot(q-1)$ é 1.
- Aa letras da palavra STOP são transformadas em números usando por exemplo, a sua posição no alfabeto:
  - 1819 1415
- Cada bloco é encriptado usando a função $C \equiv M^{13}$ **mod** 2537.
- Rapidamente é possível calcular 181913 **mod** $2537 = 2081$ e 1415^{13} **mod** $2537 = 2182$.
- A mensagem encriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 59$; e $e = 13$.Dessa forma, $n = 2537$.
- É possível observar também que o *mdc* de e e $(p-1)\cdot(q-1)$ é 1.
- Aa letras da palavra STOP são transformadas em números usando por exemplo, a sua posição no alfabeto:
  - 1819 1415
- Cada bloco é encriptado usando a função $C \equiv M^{13}$ **mod** 2537.
- Rapidamente é possível calcular 181913 **mod** $2537 = 2081$ e 1415^{13} **mod** $2537 = 2182$.
- A mensagem encriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 59$; e $e = 13$.Dessa forma, $n = 2537$.
- É possível observar também que o *mdc* de e e $(p-1)\cdot(q-1)$ é 1.
- Aa letras da palavra STOP são transformadas em números usando por exemplo, a sua posição no alfabeto:
  - 1819 1415
- Cada bloco é encriptado usando a função $C \equiv M^{13}$ **mod** 2537.
- Rapidamente é possível calcular 181913 **mod** $2537 = 2081$ e 1415^{13} **mod** $2537 = 2182$.
- A mensagem encriptada é 2081 2182.

Decriptação RSA

- O texto original pode ser recuperado usando a chave de decriptação d, que é um inverso de e módulo $(p-1)\cdot(q-1)$. Esse inverso sempre existe?
- $d \cdot e \equiv 1(\ mod\ ((p-1)\cdot(q-1))$. Logo existe um inteiro k de forma que $d \cdot e = 1 + k \cdot (p-1)\cdot(q-1)$. Logo:
- $C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$
- Pelo pequeno teorema de Fermat e assumindo que mdc(M,p) = mdc(M,q) = 1 (o que sempre ocorre, com raríssimas exceções), tem-se que:
- $M^{p-1} \equiv 1 \pmod{p}$ e $M^{q-1} \equiv 1 \pmod{q}$. Logo:
- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M(\ \mathrm{mod}\ p)$
- e $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M(\ \mathrm{mod}\ q)$
- Como o mdc de p e q é 1, e pelo TCR, temos que $C^d \equiv M \pmod{pq}$

Decriptação RSA

- O texto original pode ser recuperado usando a chave de decriptação d, que é um inverso de e módulo $(p-1)\cdot(q-1)$. Esse inverso sempre existe?
- $d \cdot e \equiv 1(\ mod\ ((p-1)\cdot(q-1))$. Logo existe um inteiro k de forma que $d \cdot e = 1 + k \cdot (p-1)\cdot(q-1)$. Logo:
- $C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$
- Pelo pequeno teorema de Fermat e assumindo que mdc(M,p) = mdc(M,q) = 1 (o que sempre ocorre, com raríssimas exceções), tem-se que:
- $M^{p-1} \equiv 1\ (\text{mod}\ p)$ e $M^{q-1} \equiv 1\ (\text{mod}\ q)$. Logo:
- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M(\ \text{mod}\ p)$
- e $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M(\ \text{mod}\ q)$
- Como o mdc de p e q é 1, e pelo TCR, temos que $C^d \equiv M$ mod pq)

Decriptação RSA

- O texto original pode ser recuperado usando a chave de decriptação d, que é um inverso de e módulo $(p-1)\cdot(q-1)$. Esse inverso sempre existe?
- $d \cdot e \equiv 1(\ mod\ ((p-1)\cdot(q-1))$. Logo existe um inteiro k de forma que $d \cdot e = 1 + k \cdot (p-1)\cdot(q-1)$. Logo:
- $C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$
- Pelo pequeno teorema de Fermat e assumindo que mdc(M,p) = mdc(M,q) = 1 (o que sempre ocorre, com raríssimas exceções), tem-se que:
- $M^{p-1} \equiv 1\ (\mathrm{mod}\ p)$ e $M^{q-1} \equiv 1\ (\mathrm{mod}\ q)$. Logo:
- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M(\ \mathrm{mod}\ p)$
- e $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M(\ \mathrm{mod}\ q)$
- Como o mdc de p e q é 1, e pelo TCR, temos que $C^d \equiv M$ mod pq)

Decriptação RSA

- O texto original pode ser recuperado usando a chave de decriptação d, que é um inverso de e módulo $(p-1)\cdot(q-1)$. Esse inverso sempre existe?
- $d \cdot e \equiv 1(\ mod\ ((p-1)\cdot(q-1))$. Logo existe um inteiro k de forma que $d \cdot e = 1 + k \cdot (p-1)\cdot(q-1)$. Logo:
- $C^d = (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$
- Pelo pequeno teorema de Fermat e assumindo que mdc(M,p) = mdc(M,q) = 1 (o que sempre ocorre, com raríssimas exceções), tem-se que:
- $M^{p-1} \equiv 1 \pmod{p}$ e $M^{q-1} \equiv 1 \pmod{q}$. Logo:
- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M(\ \mathrm{mod}\ p)$
- e $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M(\ \mathrm{mod}\ q)$
- Como o mdc de p e q é 1, e pelo TCR, temos que $C^d \equiv M \mod pq$)

Exemplo de decriptação

- Recebendo a mensagem 0981 0461, que foi encriptada do mesmo modo do exemplo anterior. Ou seja, $n = 43 \cdot 59 = 2537$ e expoente $e = 13$
- Primeiro passo é calcular d, o inverso de 13 módulo $42 \cdot 58 = 2436$.
- Para decriptar um bloco C de mensagem é preciso computar $C^{937} \bmod 2537$
- $0981^{937} \bmod 2537 = 0704$ e $0461^{937} \bmod 2537 = 115$
- A mensagem númerica é 0704 1115.
- o texto original é HELP

Exemplo de decriptação

- Recebendo a mensagem 0981 0461, que foi encriptada do mesmo modo do exemplo anterior. Ou seja, $n = 43 \cdot 59 = 2537$ e expoente $e = 13$
- Primeiro passo é calcular d, o inverso de 13 módulo $42 \cdot 58 = 2436$.
- Para decriptar um bloco C de mensagem é preciso computar $C^{937} \bmod 2537$
- $0981^{937} \bmod 2537 = 0704$ e $0461^{937} \bmod 2537 = 115$
- A mensagem númerica é 0704 1115.
- o texto original é HELP

Exemplo de decriptação

- Recebendo a mensagem 0981 0461, que foi encriptada do mesmo modo do exemplo anterior. Ou seja, $n = 43 \cdot 59 = 2537$ e expoente $e = 13$
- Primeiro passo é calcular d, o inverso de 13 módulo $42 \cdot 58 = 2436$.
- Para decriptar um bloco C de mensagem é preciso computar C^{937} mod 2537
- $0981^{937} \bmod 2537 = 0704$ e $0461^{937} \bmod 2537 = 115$
- A mensagem númerica é 0704 1115.
- o texto original é HELP

Exemplo de decriptação

- Recebendo a mensagem 0981 0461, que foi encriptada do mesmo modo do exemplo anterior. Ou seja, $n = 43 \cdot 59 = 2537$ e expoente $e = 13$
- Primeiro passo é calcular d, o inverso de 13 módulo $42 \cdot 58 = 2436$.
- Para decriptar um bloco C de mensagem é preciso computar C^{937} mod 2537
- 0981^{937} mod $2537 = 0704$ e 0461^{937} mod $2537 = 115$
- A mensagem númerica é 0704 1115.
- o texto original é HELP

Exemplo de decriptação

- Recebendo a mensagem 0981 0461, que foi encriptada do mesmo modo do exemplo anterior. Ou seja, $n = 43 \cdot 59 = 2537$ e expoente $e = 13$
- Primeiro passo é calcular d, o inverso de 13 módulo $42 \cdot 58 = 2436$.
- Para decriptar um bloco C de mensagem é preciso computar C^{937} mod 2537
- 0981^{937} mod $2537 = 0704$ e 0461^{937} mod $2537 = 115$
- A mensagem númerica é 0704 1115.
- o texto original é HELP

Exemplo de decriptação

- Recebendo a mensagem 0981 0461, que foi encriptada do mesmo modo do exemplo anterior. Ou seja, $n = 43 \cdot 59 = 2537$ e expoente $e = 13$
- Primeiro passo é calcular d, o inverso de 13 módulo $42 \cdot 58 = 2436$.
- Para decriptar um bloco C de mensagem é preciso computar C^{937} mod 2537
- 0981^{937} mod $2537 = 0704$ e 0461^{937} mod $2537 = 115$
- A mensagem númerica é 0704 1115.
- o texto original é HELP