Notas sobre teoria dos números (2)

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

Centro de Informática
Universidade Federal de Pernambuco

2007.1 / CIn-UFPE

Definição (Maior divisor comum)

Sejam a e b inteiros de forma que apenas um dels pode ser zero. O maior inteiro d de foram que $d \mid a$ e $d \mid b$ é chamado de maior divisor comum de a e b, denotado por $mdc(a, b)$.

- Uma maneira de encontrar o mdc de dois núemros é encontrar a fatoração prima desses números. Portanto sejam as fatorações de a e b dadas como a seguir:
  - $a = p_1^{a1} p_2^{a2} \dots p_n^{an}$
  - $b = p_1^{b1} p_2^{b2} \dots p_n^{bn}$
- $mdc(a, b) = p_1^{min(a1,b1)}, p_2^{min(a_2,b_2)} \dots p_n^{min(an,bn)}$

Definição (primos entre si)

Os inteiros a e b são primos entre si se seu mdc é 1.

Definição (primos entre si dois a dois)

Os inteiros $a_1, a_2, \ldots a_n$ são primos entre si dois a dois se $mdc(a_i, a_j) = 1$ para $1 \leq i < j \leq n$.

Definição (o menor múltiplo comum)

O menor múltiplo comum de dois inteiros positivos a e b é o menor inteiro positivo que é divisível pelos dois, a e b. O menor múltiplo comum é denotado por $mmc(a, b)$.

- $mmc(a, b) = p_1^{max(a1,b1)}, p_2^{max(a_2,b_2)} \ldots p_n^{max(an,bn)}$

Exemplo

Prove que se a e b são inteiros postivos então $ab = mdc(a, b).mmc(a, b)$

Definição

Sejam a e b inteiros positivos. Nós denotamos a **mod** *m como o resto quando a é dividido por m.*

- Temos que 15 **mod** 12 = 3 **mod** 12, que é igual a 3.
- Usamos uma notação para indicar que dois inteiros possuem o mesmo resto quando divididos por um inteiro positivo *m*.

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m *se m divide $a - b$. Usamos a notação $a \equiv b(mod\ m)$ para indicar que a é congruente a b módulo m. Se a e b não são congruentes módulo m, escrevemos $a \not\equiv b\ (mod\ m)$. Quando $a \equiv b\ (mod\ m)$, temos que a **mod** $m = b$ **mod** m.*

- Dizemos que $a \equiv b(mod\ m)$ se e somente se a **mod** m = b **mod** m.

Exemplo $7 \equiv 2(mod\ 5)$

- **Você pode provar que se $a \equiv b\ (mod\ m)$ então $m|(a - b)$.**

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m *se m divide* $a - b$. *Usamos a notação* $a \equiv b(mod\ m)$ *para indicar que a é congruente a b módulo m. Se a e b não são congruentes módulo m, escrevemos* $a \not\equiv b\ (mod\ m)$. *Quando* $a \equiv b\ (mod\ m)$, *temos que* $a\ \mathbf{mod}\ \ m = b\ \mathbf{mod}\ m$.

- Dizemos que $a \equiv b(mod\ m)$ se e somente se a **mod** m = b **mod** m.

Exemplo $7 \equiv 2(mod\ 5)$

- **Você pode provar que se** $a \equiv b\ (mod\ m)$ **então** $m|(a - b)$.

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m *se m divide* $a - b$. *Usamos a notação* $a \equiv b(mod\ m)$ *para indicar que a é congruente a b módulo m. Se a e b não são congruentes módulo m, escrevemos* $a \not\equiv b\ (mod\ m)$. *Quando* $a \equiv b\ (mod\ m)$, *temos que* $a \textbf{ mod } m = b \textbf{ mod } m$.

- Dizemos que $a \equiv b(mod\ m)$ se e somente se a **mod** m = b **mod** m**.**

Exemplo $7 \equiv 2(mod\ 5)$

- **Você pode provar que se** $a \equiv b\ (mod\ m)$ **então** $m|(a - b)$**.**

Teorema

Seja m um inteiro positivo. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$.

Algumas aplicações de congruência

- Funções Hashing: $h(k) = k \ mod \ n$;
- Números pseudorandômicos:
- $x_{n+1} = (ax_n + c) \ mod \ m$.
- x_0 é chamado de semente, a multiplicador e c incremento, onde todos devem ser menores que m, e c e x_0 devem ser maiores ou iguais a zero; e a maior ou igual a 2.

Exemplo $m = 9$, $a = 7$, $c = 4$ e $x_0 = 3$, temos a sequência:

- $$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8...$$

- Criptografia: cifra de deslocamento: $f(x) = (x + 3) \ mod \ 26$.

Algumas aplicações de congruência

- Funções Hashing: $h(k) = k \ mod \ n$;
- Números pseudorandômicos:
- $x_{n+1} = (ax_n + c) \ mod \ m$.
- x_0 é chamado de semente, a multiplicador e c incremento, onde todos devem ser menores que m, e c e x_0 devem ser maiores ou iguais a zero; e a maior ou igual a 2.

Exemplo $m = 9$, $a = 7$, $c = 4$ e $x_0 = 3$, temos a sequência:

- $$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8...$$

- Criptografia: cifra de deslocamento: $f(x) = (x + 3) \ mod \ 26$.

Algumas aplicações de congruência

- Funções Hashing: $h(k) = k\ mod\ n$;
- Números pseudorandômicos:
- $x_{n+1} = (ax_n + c)\ mod\ m$.
- x_0 é chamado de semente, a multiplicador e c incremento, onde todos devem ser menores que m, e c e x_0 devem ser maiores ou iguais a zero; e a maior ou igual a 2.

Exemplo $m = 9$, $a = 7$, $c = 4$ e $x_0 = 3$, temos a sequência:

- $$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8...$$

- Criptografia: cifra de deslocamento: $f(x) = (x + 3)\ mod\ 26$.

Algumas aplicações de congruência

- Funções Hashing: $h(k) = k \ mod \ n$;
- Números pseudorandômicos:
- $x_{n+1} = (ax_n + c) \ mod \ m$.
- x_0 é chamado de semente, a multiplicador e c incremento, onde todos devem ser menores que m, e c e x_0 devem ser maiores ou iguais a zero; e a maior ou igual a 2.

Exemplo $m = 9$, $a = 7$, $c = 4$ e $x_0 = 3$, temos a sequência:

- $$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8...$$
- Criptografia: cifra de deslocamento: $f(x) = (x + 3) \ mod \ 26$.

Algumas aplicações de congruência

- Funções Hashing: $h(k) = k\ mod\ n$;
- Números pseudorandômicos:
- $x_{n+1} = (ax_n + c)\ mod\ m$.
- x_0 é chamado de semente, a multiplicador e c incremento, onde todos devem ser menores que m, e c e x_0 devem ser maiores ou iguais a zero; e a maior ou igual a 2.

Exemplo $m = 9$, $a = 7$, $c = 4$ e $x_0 = 3$, temos a sequência:

- $$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8...$$

- Criptografia: cifra de deslocamento:
  $f(x) = (x + 3)\ mod\ 26$.

O Algoritmo de Euclides

- O máximo divisor comum de dois inteiros positivos pode ser encontrado usando-se as suas fatorações primas. Mas esse método é ineficiente para inteiros grandes.
- O algoritmo de Euclides calcula o *mdc* de dois inteiros de modo eficiente, sem encontrar suas fatorações primas.
- Ele é baseado em alguns resultados simples, que podemos provar.

O Algoritmo de Euclides

- O máximo divisor comum de dois inteiros positivos pode ser encontrado usando-se as suas fatorações primas. Mas esse método é ineficiente para inteiros grandes.
- O algoritmo de Euclides calcula o *mdc* de dois inteiros de modo eficiente, sem encontrar suas fatorações primas.
- Ele é baseado em alguns resultados simples, que podemos provar.

O Algoritmo de Euclides

- O máximo divisor comum de dois inteiros positivos pode ser encontrado usando-se as suas fatorações primas. Mas esse método é ineficiente para inteiros grandes.
- O algoritmo de Euclides calcula o *mdc* de dois inteiros de modo eficiente, sem encontrar suas fatorações primas.
- Ele é baseado em alguns resultados simples, que podemos provar.

O Algoritmo de Euclides

1. Prove que $mdc(a, b) = mdc(a, b - a)$.
2. Seja r o resto se dividirmos b por a. Então prove que $mdc(a, b) = mdc(a, r)$.

O Algoritmo de Euclides

1. Prove que $mdc(a, b) = mdc(a, b - a)$.
2. Seja r o resto se dividirmos b por a. Então prove que $mdc(a, b) = mdc(a, r)$.

O Algoritmo de Euclides

Suponha que nos são dados dois inteiros positivos a e b, e desejamos achar seu máximo divisor comum.

1. Se $a > b$ então trocamos a por b e vice-versa.
2. Se $a > 0$, dividimos b por a, para obter um resto r. Substituimos b por r e retornamos ao passo 1.
3. Senão (se $a = 0$), retornamos b como o m.d.c. e paramos.

O Algoritmo de Euclides: exemplos

- $mdc(300, 18) = mdc(12, 18) = mdc(12, 6) = mdc(6, 0) = 6$
- E o mdc de 101 e 100?
- $mdc(101, 100) = mdc(1, 100) = mdc(1, 0) = 1$
- $mdc(89, 55)$?
- $mdc(89, 55) = mdc(34, 55) = mdc(34, 21) = mdc(13, 21) = mdc(13, 8)$
  $= mdc(5, 8) = mdc(5, 3) = mdc(2, 3) = mdc(2, 1) = mdc(1, 0) = 1$

O Algoritmo de Euclides: exemplos

- $mdc(300, 18) = mdc(12, 18) = mdc(12, 6) = mdc(6, 0) = 6$
- E o mdc de 101 e 100?
- $mdc(101, 100) = mdc(1, 100) = mdc(1, 0) = 1$
- $mdc(89, 55)$?
- $mdc(89, 55) = mdc(34, 55) = mdc(34, 21) = mdc(13, 21) = mdc(13, 8) = mdc(5, 8) = mdc(5, 3) = mdc(2, 3) = mdc(2, 1) = mdc(1, 0) = 1$

O Algoritmo de Euclides: exemplos

- $mdc(300, 18) = mdc(12, 18) = mdc(12, 6) = mdc(6, 0) = 6$
- E o mdc de 101 e 100?
- $mdc(101, 100) = mdc(1, 100) = mdc(1, 0) = 1$
- $mdc(89, 55)$?
- $mdc(89, 55) = mdc(34, 55) = mdc(34, 21) = mdc(13, 21) = mdc(13, 8) = mdc(5, 8) = mdc(5, 3) = mdc(2, 3) = mdc(2, 1) = mdc(1, 0) = 1$

O Algoritmo de Euclides: exemplos

- $mdc(300, 18) = mdc(12, 18) = mdc(12, 6) = mdc(6, 0) = 6$
- E o mdc de 101 e 100?
- $mdc(101, 100) = mdc(1, 100) = mdc(1, 0) = 1$
- $mdc(89, 55)$?
- $mdc(89, 55) = mdc(34, 55) = mdc(34, 21) = mdc(13, 21) = mdc(13, 8) = mdc(5, 8) = mdc(5, 3) = mdc(2, 3) = mdc(2, 1) = mdc(1, 0) = 1$

O Algoritmo de Euclides: exemplos

- $mdc(300, 18) = mdc(12, 18) = mdc(12, 6) = mdc(6, 0) = 6$
- E o mdc de 101 e 100?
- $mdc(101, 100) = mdc(1, 100) = mdc(1, 0) = 1$
- $mdc(89, 55)$?
- $mdc(89, 55) = mdc(34, 55) = mdc(34, 21) = mdc(13, 21) = mdc(13, 8)$
  $= mdc(5, 8) = mdc(5, 3) = mdc(2, 3) = mdc(2, 1) = mdc(1, 0) = 1$

- Qual o resultado de quinta-feira + sexta-feira?
- Vamos fazer a seguinte associação:

0	1	2	3	4	5	6
Dom	Seg	Ter	Qua	Qui	Sex	Sáb

- Assim, a pergunta pode ser formulada da seguinte maneira:

$$\text{Qual o resultado de } (4+5) \ mod \ 7?$$

Daí a resposta é terça-feira.

- Qual o resultado de quinta-feira + sexta-feira?
- Vamos fazer a seguinte associação:

0	1	2	3	4	5	6
Dom	Seg	Ter	Qua	Qui	Sex	Sáb

- Assim, a pergunta pode ser formulada da seguinte maneira:

  Qual o resultado de $(4 + 5)$ *mod* 7?

  Daí a resposta é terça-feira.

- Qual o resultado de quinta-feira + sexta-feira?
- Vamos fazer a seguinte associação:

0	1	2	3	4	5	6
Dom	Seg	Ter	Qua	Qui	Sex	Sáb

- Assim, a pergunta pode ser formulada da seguinte maneira:

$$\text{Qual o resultado de } (4 + 5) \textit{ mod } 7?$$

Daí a resposta é terça-feira.

De modo semelhante, podemos facilmente calcular:

a) Quinta-feira.Sexta-feira;

Resp. Quinta-feira.Sexta-feira $\rightarrow (4.5)\ mod\ 7 = 6 =$ Sábado;

b) (Sábado)^2;

Resp. $(6)^2\ mod\ 7 = 36\ mod\ 7 = 1 =$ Segunda-feira;

c) Segunda-feira - Sábado.

Resp. $(1 - 6)\ mod\ 7 = -5\ mod\ 7 = 2 =$ Terça-feira.

De modo semelhante, podemos facilmente calcular:

a) Quinta-feira.Sexta-feira;

Resp. Quinta-feira.Sexta-feira $\rightarrow (4.5)$ *mod* $7 = 6 =$ Sábado;

b) (Sábado)^2;

Resp. $(6)^2$ *mod* $7 = 36$ *mod* $7 = 1 =$ Segunda-feira;

c) Segunda-feira - Sábado.

Resp. $(1 - 6)$ *mod* $7 = -5$ *mod* $7 = 2 =$ Terça-feira.

De modo semelhante, podemos facilmente calcular:

a) Quinta-feira.Sexta-feira;

Resp. Quinta-feira.Sexta-feira $\rightarrow (4.5)$ *mod* $7 = 6 =$ Sábado;

b) (Sábado)^2;

Resp. $(6)^2$ *mod* $7 = 36$ *mod* $7 = 1 =$ Segunda-feira;

c) Segunda-feira - Sábado.

Resp. $(1 - 6)$ *mod* $7 = -5$ *mod* $7 = 2 =$ Terça-feira.

Propriedades

1) Comutatividade:
   1. Seg + Sex = Sex + Seg. ($(a+b)$ *mod* m $=(b+a)$ *mod* m);
   2. Ter.Qui = Qui.Terc;
2) Associatividade:
   1. (Seg + Ter) + Qui = Seg + (Ter + Qui);
   2. (Sex.Ter).Qua = Sex.(Ter.Qua).

Propriedades

1) Comutatividade:
   1. Seg + Sex = Sex + Seg. ($(a+b)$ *mod* m $= (b+a)$ *mod* m);
   2. Ter.Qui = Qui.Terc;

2) Associatividade:
   1. (Seg + Ter) + Qui = Seg + (Ter + Qui);
   2. (Sex.Ter).Qua = Sex.(Ter.Qua).

Propriedades

3) Elemento neutro da adição:
   1. Seg + Dom = Seg; Ter + Dom = Ter. O “Dom” é o zero.

4) Elemento neutro da multiplicação:
   1. Seg.Ter = Ter; Qua.Seg = Qua. “Seg” funciona como um.

5) Subtração é o inverso da soma:
   1. (Seg + Ter) - Seg = Ter.

Propriedades

3) Elemento neutro da adição:
   1. Seg + Dom = Seg; Ter + Dom = Ter. O “Dom” é o zero.
4) Elemento neutro da multiplicação:
   1. Seg.Ter = Ter; Qua.Seg = Qua. “Seg” funciona como um.
5) Subtração é o inverso da soma:
   1. (Seg + Ter) - Seg = Ter.

Propriedades

3) Elemento neutro da adição:
    1. Seg + Dom = Seg; Ter + Dom = Ter. O “Dom” é o zero.
4) Elemento neutro da multiplicação:
    1. Seg.Ter = Ter; Qua.Seg = Qua. “Seg” funciona como um.
5) Subtração é o inverso da soma:
    1. (Seg + Ter) - Seg = Ter.

E a divisão ?

- Em alguns casos ela é óbvia. Sab/Ter = Qua. Temos Ter.Qua = Sab.
- Entretanto, Ter/Qua?
- Na aritmética usual isso seria $\frac{2}{3}$, que não é um inteiro. Dessa forma, os racionais foram introduzidos. Mas será que devemos introduzir *dias da semana fracionários*? Veremos que a resposta é não.

E a divisão ?

- Em alguns casos ela é óbvia. Sab/Ter = Qua. Temos Ter.Qua = Sab.
- Entretanto, Ter/Qua?
- Na aritmética usual isso seria $\frac{2}{3}$, que não é um inteiro. Dessa forma, os racionais foram introduzidos. Mas será que devemos introduzir *dias da semana fracionários*? Veremos que a resposta é não.

E a divisão ?

- Em alguns casos ela é óbvia. Sab/Ter = Qua. Temos Ter.Qua = Sab.
- Entretanto, Ter/Qua?
- Na aritmética usual isso seria $\frac{2}{3}$, que não é um inteiro. Dessa forma, os racionais foram introduzidos. Mas será que devemos introduzir *dias da semana fracionários*? Veremos que a resposta é não.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x.Qua = Ter$
- A resposta é $x = Qua$, Qua.Qua = Ter, pois $3.3 \equiv 2\ (mod\ 7)$.
- Na realidade solucionamos a **congruência linear** $x.3 \equiv 2\ mod\ 7$.
- Como encontrar uma solução para o caso geral $ax \equiv b\ (mod\ m)$?
- Além disso, temos que $14 \equiv 8\ (mod\ 6)$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4\ (mod\ 6)$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x.Qua = Ter$
- A resposta é $x = Qua$, Qua.Qua = Ter, pois $3.3 \equiv 2\ (mod\ 7)$.
- Na realidade solucionamos a **congruência linear** $x.3 \equiv 2\ mod\ 7$.
- Como encontrar uma solução para o caso geral $ax \equiv b\ (mod\ m)$?
- Além disso, temos que $14 \equiv 8\ (mod\ 6)$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4\ (mod\ 6)$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x.Qua = Ter$
- A resposta é $x = Qua$, Qua.Qua = Ter, pois $3.3 \equiv 2 \ (mod\ 7)$.
- Na realidade solucionamos a **congruência linear** $x.3 \equiv 2 \ mod\ 7$.
- Como encontrar uma solução para o caso geral $ax \equiv b \ (mod\ m)$?
- Além disso, temos que $14 \equiv 8 \ (mod\ 6)$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4 \ (mod\ 6)$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x.Qua = Ter$
- A resposta é $x = Qua$, Qua.Qua = Ter, pois $3.3 \equiv 2\ (mod\ 7)$.
- Na realidade solucionamos a **congruência linear** $x.3 \equiv 2\ mod\ 7$.
- Como encontrar uma solução para o caso geral $ax \equiv b\ (mod\ m)$?
- Além disso, temos que $14 \equiv 8\ (mod\ 6)$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4\ (mod\ 6)$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x.Qua = Ter$
- A resposta é $x = Qua$, Qua.Qua = Ter, pois $3.3 \equiv 2\ (mod\ 7)$.
- Na realidade solucionamos a **congruência linear** $x.3 \equiv 2\ mod\ 7$.
- Como encontrar uma solução para o caso geral $ax \equiv b\ (mod\ m)$?
- Além disso, temos que $14 \equiv 8\ (mod\ 6)$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4\ (mod\ 6)$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x.Qua = Ter$
- A resposta é $x = Qua$, Qua.Qua = Ter, pois $3.3 \equiv 2\ (mod\ 7)$.
- Na realidade solucionamos a **congruência linear** $x.3 \equiv 2\ mod\ 7$.
- Como encontrar uma solução para o caso geral $ax \equiv b\ (mod\ m)$?
- Além disso, temos que $14 \equiv 8\ (mod\ 6)$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4\ (mod\ 6)$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x.Qua = Ter$
- A resposta é $x = Qua$, Qua.Qua = Ter, pois $3.3 \equiv 2\ (mod\ 7)$.
- Na realidade solucionamos a **congruência linear** $x.3 \equiv 2\ mod\ 7$.
- Como encontrar uma solução para o caso geral $ax \equiv b\ (mod\ m)$?
- Além disso, temos que $14 \equiv 8\ (mod\ 6)$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4\ (mod\ 6)$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Alguns Resultados

Teorema (pg. 137)

Se a e b são inteiros positivos, então existem inteiros s e t de forma que mdc(a,b)= sa+tb.

- Isso quer dizer que o mdc de a e b pode ser escrito como uma **combinação linear** com coeficientes inteiros de a e b.
- Para encontrar a **combinação linear** de dois inteiros que seja igual ao seu mdc usamos o algoritmo de Euclides.

Alguns Resultados

Teorema (pg. 137)

Se a e b são inteiros positivos, então existem inteiros s e t de forma que mdc(a,b)= sa+tb.

- Isso quer dizer que o mdc de a e b pode ser escrito como uma **combinação linear** com coeficientes inteiros de a e b.
- Para encontrar a **combinação linear** de dois inteiros que seja igual ao seu mdc usamos o algoritmo de Euclides.

Alguns Resultados

Exemplo

Expresse o mdc(300,18) = 6 como uma combinação linear de 300 e 18.
Vimos que mdc(300,18) = mdc(12,18) = mdc(12,6) = mdc (6,0) = 6:

1. *300 = 18.16 + 12* $\rightarrow$ **12 = 300 -18.16**
2. *18 = 12.1 + 6* $\rightarrow$ **6 = 18-12**
3. *12 = 6.2 + 0*

Logo, 6=18 -(300 - 18.16) $\rightarrow$ *6 = 18 - 300 + 18.16* $\rightarrow$ **6 = 17.18 - 300**.

Outro exemplo

- Expresse o mdc(252,198) como uma combinação linear de 252 e 198 .
- mdc(252,198) = mdc (198, 54) = mdc (54, 36) = mdc(36, 18) = mdc (18, 0) = 18).
  1. 252 = 198.1 + 54
  2. 198 = 54.3 + 36
  3. 54 = 36.1 + 18
  4. 36 = 18.2 + 0
- Assim,
  1. 54 = 252 - 198
  2. 36 = 198 - 3.54
  3. 18 = 54 -36
- Logo, 18 = (252 - 198) - (198 - 3. 54) = 252 - 2.198 + 3.(252 - 198) = **4. 252 - 5.198**.

Outro exemplo

- Expresse o mdc(252,198) como uma combinação linear de 252 e 198 .
- mdc(252,198) = mdc (198, 54) = mdc (54, 36) = mdc(36, 18) = mdc (18, 0) = 18).
  1. 252 = 198.1 + 54
  2. 198 = 54.3 + 36
  3. 54 = 36.1 + 18
  4. 36 = 18.2 + 0
- Assim,
  1. 54 = 252 - 198
  2. 36 = 198 - 3.54
  3. 18 = 54 -36
- Logo, 18 = (252 - 198) - (198 - 3. 54) = 252 - 2.198 + 3.(252 - 198) = **4. 252 - 5.198.**

Outro exemplo

- Expresse o mdc(252,198) como uma combinação linear de 252 e 198 .
- mdc(252,198) = mdc (198, 54) = mdc (54, 36) = mdc(36, 18) = mdc (18, 0) = 18).
  1. 252 = 198.1 + 54
  2. 198 = 54.3 + 36
  3. 54 = 36.1 + 18
  4. 36 = 18.2 + 0
- Assim,
  1. 54 = 252 - 198
  2. 36 = 198 - 3.54
  3. 18 = 54 -36
- Logo, 18 = (252 - 198) - (198 - 3. 54) = 252 - 2.198 + 3.(252 - 198) = **4. 252 - 5.198.**

Outro exemplo

- Expresse o mdc(252,198) como uma combinação linear de 252 e 198 .
- mdc(252,198) = mdc (198, 54) = mdc (54, 36) = mdc(36, 18) = mdc (18, 0) = 18).
  1. 252 = 198.1 + 54
  2. 198 = 54.3 + 36
  3. 54 = 36.1 + 18
  4. 36 = 18.2 + 0
- Assim,
  1. 54 = 252 - 198
  2. 36 = 198 - 3.54
  3. 18 = 54 -36
- Logo, 18 = (252 - 198) - (198 - 3. 54) = 252 - 2.198 + 3.(252 - 198) = **4. 252 - 5.198**.

Lema (pg. 138)

Se a, b e c são inteiros positivos de forma que a e b são primos entre si e $a \mid bc$ então $a \mid c$.

Prova

1. a e b são primos entre si $\rightarrow$ mdc(a,b) = 1;
2. sa + tb = 1;
3. sac + tbc = c;
4. Se $a \mid bc \rightarrow a \mid tbc$;
5. Como $a \mid sac$ e $a \mid tbc$ então $a \mid (sac + tbc)$, logo $a \mid c$

Lema (pg. 138)

Se a, b e c são inteiros positivos de forma que a e b são primos entre si e $a \mid bc$ então $a \mid c$.

Prova

1. a e b são primos entre si $\rightarrow$ mdc(a,b) = 1;
2. sa + tb = 1;
3. sac + tbc = c;
4. Se $a \mid bc \rightarrow a \mid tbc$;
5. Como $a \mid sac$ e $a \mid tbc$ então $a \mid (sac + tbc)$, logo $a \mid c$

Lema (pg. 138)

Se a, b e c são inteiros positivos de forma que a e b são primos entre si e $a \mid bc$ então $a \mid c$.

Prova

1. a e b são primos entre si $\rightarrow$ mdc(a,b) = 1;
2. sa + tb = 1;
3. sac + tbc = c;
4. Se $a \mid bc \rightarrow a \mid tbc$;
5. Como $a \mid sac$ e $a \mid tbc$ então $a \mid (sac + tbc)$, logo $a \mid c$

Lema (pg. 138)

Se a, b e c são inteiros positivos de forma que a e b são primos entre si e $a \mid bc$ então $a \mid c$.

Prova

1. a e b são primos entre si $\rightarrow$ mdc(a,b) = 1;
2. sa + tb = 1;
3. sac + tbc = c;
4. Se $a \mid bc \rightarrow\ a \mid tbc$;
5. Como $a \mid sac$ e $a \mid tbc$ então $a \mid (sac + tbc)$, logo $a \mid c$

Lema (pg. 138)

Se a, b e c são inteiros positivos de forma que a e b são primos entre si e a $|$ bc então a $|$ c.

Prova

1. a e b são primos entre si $\rightarrow$ mdc(a,b) = 1;
2. sa + tb = 1;
3. sac + tbc = c;
4. Se $a \mid bc \rightarrow a \mid tbc$;
5. Como $a \mid sac$ e $a \mid tbc$ então $a \mid (sac + tbc)$, logo $a \mid c$

Teorema (pg. 139)

Seja m um inteiro positivo e sejam a,b e c inteiros. Se $ac \equiv bc \pmod{m}$ *e c e m são primos entre si então* $a \equiv b \pmod{m}$.

Prova

1. $ac \equiv bc \pmod{m}$.
2. $m \mid (ac - bc)$
3. $m \mid c(a-b)$
4. Como mdc(m,c) = 1, pelo lema anterior $m \mid (a-b)$, logo $a \equiv b (mod\ m)$.

Teorema (pg. 139)

Seja m um inteiro positivo e sejam a,b e c inteiros. Se $ac \equiv bc \pmod{m}$ e c e m são primos entre si então $a \equiv b \pmod{m}$.

Prova

1. $ac \equiv bc \ (mod\ m)$.
2. $m \mid (ac - bc)$
3. $m \mid c(a - b)$
4. Como mdc(m,c) = 1, pelo lema anterior $m \mid (a - b)$, logo $a \equiv b(mod\ m)$.

Teorema (pg. 139)

Seja m um inteiro positivo e sejam a,b e c inteiros. Se $ac \equiv bc \pmod{m}$ e c e m são primos entre si então $a \equiv b \pmod{m}$.

Prova

1. $ac \equiv bc \pmod{m}$.
2. $m \mid (ac - bc)$
3. $m \mid c(a - b)$
4. Como mdc(m,c) = 1, pelo lema anterior $m \mid (a - b)$, logo $a \equiv b (mod\ m)$.

Teorema (pg. 139)

Seja m um inteiro positivo e sejam a,b e c inteiros. Se $ac \equiv bc \ (mod\ m)$ *e c e m são primos entre si então* $a \equiv b \ (mod\ m)$.

Prova

1. $ac \equiv bc \ (mod\ m)$.
2. $m \mid (ac - bc)$
3. $m \mid c(a - b)$
4. Como mdc(m,c) = 1, pelo lema anterior $m \mid (a - b)$, logo $a \equiv b (mod\ m)$.

- Na aritmética usual se temos $ax = b$, com $a \neq 0$, então x = b/a . Ou seja, multiplicando ambos os lados da equação pelo *inverso* de *a*, que é 1/a, temos como calcular x.
- De forma semelhante, na aritmética modular quando queremos a solução de $ax \equiv b \ (mod\ m)$, onde m é um inteiro positivo, e a e b são inteiros, precisamos calcular o **inverso de a módulo m.**
- Seja $\bar{a}$ um inteiro de forma que $\bar{a}.a \equiv 1 \ (mod\ m)$. Dizemos que $\bar{a}$ é um *inverso de a módulo m*.
- O seguinte teorema garante que o inverso de a módulo m existe se a e m são primos entre si.

- Na aritmética usual se temos $ax = b$, com $a \neq 0$, então x = b/a . Ou seja, multiplicando ambos os lados da equação pelo *inverso* de *a*, que é 1/a, temos como calcular x.
- De forma semelhante, na aritmética modular quando queremos a solução de $ax \equiv b \ (mod\ m)$, onde *m* é um inteiro positivo, e a e b são inteiros, precisamos calcular o **inverso de a módulo m**.
- Seja $\bar{a}$ um inteiro de forma que $\bar{a}.a \equiv 1 \ (mod\ m)$. Dizemos que $\bar{a}$ é um *inverso de a módulo m*.
- O seguinte teorema garante que o inverso de a módulo m existe se a e m são primos entre si.

- Na aritmética usual se temos $ax = b$, com $a \neq 0$, então x = b/a . Ou seja, multiplicando ambos os lados da equação pelo *inverso* de *a*, que é 1/a, temos como calcular x.
- De forma semelhante, na aritmética modular quando queremos a solução de $ax \equiv b \ (mod\ m)$, onde *m* é um inteiro positivo, e a e b são inteiros, precisamos calcular o **inverso de a módulo m**.
- Seja $\bar{a}$ um inteiro de forma que $\bar{a}.a \equiv 1 \ (mod\ m)$. Dizemos que $\bar{a}$ é um *inverso de a módulo m*.
- O seguinte teorema garante que o inverso de a módulo m existe se a e m são primos entre si.

- Na aritmética usual se temos $ax = b$, com $a \neq 0$, então x = b/a . Ou seja, multiplicando ambos os lados da equação pelo *inverso* de *a*, que é 1/a, temos como calcular x.
- De forma semelhante, na aritmética modular quando queremos a solução de $ax \equiv b \ (mod \ m)$, onde m é um inteiro positivo, e a e b são inteiros, precisamos calcular o **inverso de a módulo m**.
- Seja $\bar{a}$ um inteiro de forma que $\bar{a}.a \equiv 1 \ (mod \ m)$. Dizemos que $\bar{a}$ é um *inverso de a módulo m*.
- O seguinte teorema garante que o inverso de a módulo m existe se a e m são primos entre si.

Teorema (pg. 140)

Se a e m são inteiros primos entre si e $m > 1$, então o inverso de a módulo m existe. Além disso, esse inverso é único módulo m.

Prova

1. como mdc (a,m) = 1 $\rightarrow$ sa + tm = 1;
2. sa + tm $\equiv$ 1 (mod m);
3. tm $\equiv$ 0 (mod m);
4. sa $\equiv$ 1 (mod m).
5. s é o inverso de a módulo m.

Teorema (pg. 140)

Se a e m são inteiros primos entre si e $m > 1$, então o inverso de a módulo m existe. Além disso, esse inverso é único módulo m.

Prova

1. como mdc (a,m) = 1 $\rightarrow$ sa + tm = 1;
2. sa + tm $\equiv$ 1 (mod m);
3. tm $\equiv$ 0 (mod m);
4. sa $\equiv$ 1 (mod m).
5. s é o inverso de a módulo m.

Teorema (pg. 140)

Se a e m são inteiros primos entre si e $m > 1$, então o inverso de a módulo m existe. Além disso, esse inverso é único módulo m.

Prova

1. como mdc (a,m) = 1 $\rightarrow$ sa + tm = 1;
2. sa + tm $\equiv$ 1 (mod m);
3. tm $\equiv$ 0 (mod m);
4. sa $\equiv$ 1 (mod m).
5. s é o inverso de a módulo m.

Teorema (pg. 140)

Se a e m são inteiros primos entre si e $m > 1$, então o inverso de a módulo m existe. Além disso, esse inverso é único módulo m.

Prova

1. como mdc (a,m) = 1 $\rightarrow$ sa + tm = 1;
2. sa + tm $\equiv$ 1 (mod m);
3. tm $\equiv$ 0 (mod m);
4. sa $\equiv$ 1 (mod m).
5. s é o inverso de a módulo m.

Teorema (pg. 140)

Se a e m são inteiros primos entre si e $m > 1$, então o inverso de a módulo m existe. Além disso, esse inverso é único módulo m.

Prova

1. como mdc (a,m) = 1 $\rightarrow$ sa + tm = 1;
2. sa + tm $\equiv$ 1 (mod m);
3. tm $\equiv$ 0 (mod m);
4. sa $\equiv$ 1 (mod m).
5. s é o inverso de a módulo m.

Exemplos

Exemplo

Para calcular um inverso de 3 mod 7 usamos o algoritmo de Euclides.

$\bar{a}.3 \equiv 1 \; mod \; 7.$

$7 = 2.3 + 1 \rightarrow 1 = 7 - 2.3.$

Logo $\bar{a}$ *é -2, 5, 12, etc.*

- Encontre um inverso de 4 módulo 9.
- Ou seja, $4.x \equiv 1 \; (mod \; 9)$
- $9 = 2.4 + 1 \rightarrow 1 = 9 - 2.4$
- Resposta: -2, 7 , etc.

Exemplos

Exemplo

Para calcular um inverso de 3 mod 7 usamos o algoritmo de Euclides.

$\bar{a}.3 \equiv 1 \; mod \; 7.$

7 = 2.3 +1 $\rightarrow$ *1 = 7 -2.3.*

Logo ā é -2, 5, 12, etc.

- Encontre um inverso de 4 módulo 9.
- Ou seja, $4.x \equiv 1 \; (mod \; 9)$
- 9 = 2.4 + 1 $\rightarrow$ 1 = 9-2.4
- Resposta: -2, 7 , etc.

Exemplos

Exemplo

Para calcular um inverso de 3 mod 7 usamos o algoritmo de Euclides.

$\bar{a}.3 \equiv 1 \; mod \; 7.$

7 = 2.3 +1 $\rightarrow$ 1 = 7 -2.3.

Logo ā é -2, 5, 12, etc.

- Encontre um inverso de 4 módulo 9.
- Ou seja, $4.x \equiv 1 \; (mod \; 9)$
- 9 = 2.4 + 1 $\rightarrow$ 1 = 9-2.4
- Resposta: -2, 7 , etc.

Exemplos

Exemplo

Para calcular um inverso de 3 mod 7 usamos o algoritmo de Euclides.

$\bar{a}.3 \equiv 1 \; mod \; 7.$

7 = 2.3 +1 → 1 = 7 -2.3.

Logo ā é -2, 5, 12, etc.

- Encontre um inverso de 4 módulo 9.
- Ou seja, $4.x \equiv 1 \; (mod \; 9)$
- 9 = 2.4 + 1 → 1 = 9-2.4
- Resposta: -2, 7 , etc.

- Assim, para solucionar $ax \equiv b \ mod \ m$ fazemos os seguintes passos:
  1. encontramos $\bar{a}$
  2. como $\bar{a}.a \equiv 1 \ (mod \ m)$, multilpicamos ambos os lados da congruência por $\bar{a}$:
  3. $\bar{a}.a.x \equiv b.a \ (mod \ m)$;
  4. então temos $x \equiv b.\bar{a} \ (mod \ m)$

- Assim, para solucionar $ax \equiv b \ mod \ m$ fazemos os seguintes passos:
  1. encontramos $\bar{a}$
  2. como $\bar{a}.a \equiv 1 \ (mod \ m)$, multilpicamos ambos os lados da congruência por $\bar{a}$:
  3. $\bar{a}.a.x \equiv b.a \ (mod \ m)$;
  4. então temos $x \equiv b.\bar{a} \ (mod \ m)$

- Assim, para solucionar $ax \equiv b \; mod \; m$ fazemos os seguintes passos:
    1. encontramos $\bar{a}$
    2. como $\bar{a}.a \equiv 1 \; (mod \; m)$, multilpicamos ambos os lados da congruência por $\bar{a}$:
    3. $\bar{a}.a.x \equiv b.a \, (mod \; m)$;
    4. então temos $x \equiv b.\bar{a} \, (mod \; m)$

- Assim, para solucionar $ax \equiv b\ mod\ m$ fazemos os seguintes passos:
  1. encontramos $\bar{a}$
  2. como $\bar{a}.a \equiv 1\ (mod\ m)$, multilpicamos ambos os lados da congruência por $\bar{a}$:
  3. $\bar{a}.a.x \equiv b.a\ (mod\ m)$;
  4. então temos $x \equiv b.\bar{a}\ (mod\ m)$

Exemplos

Exemplo

Retomando o nosso exemplo: $x.3 \equiv 2(mod\ 7)$*:*
Vimos que um inverso de 3 mod 7 é 5. Daí $x \equiv 10\ mod\ 7 \rightarrow x \equiv 3\ mod\ 7$*.*

- $3x \equiv 4\ (mod\ 7)$?
- Vimos que 5 é um inverso de 3 mod 7.
- Assim, $x \equiv 20\ (mod\ 7)$, logo $x \equiv 6\ (mod\ 7)$.

Exemplos

Exemplo

Retomando o nosso exemplo: $x.3 \equiv 2(mod\ 7)$*:*
Vimos que um inverso de 3 mod 7 é 5. Daí $x \equiv 10\ mod\ 7 \rightarrow x \equiv 3\ mod\ 7$.

- $3x \equiv 4\ (mod\ 7)$?
- Vimos que 5 é um inverso de 3 mod 7.
- Assim, $x \equiv 20\ (mod\ 7)$, logo $x \equiv 6\ (mod\ 7)$.

Exemplos

Exemplo

Retomando o nosso exemplo: $x.3 \equiv 2(mod\ 7)$*:*
Vimos que um inverso de 3 mod 7 é 5. Daí $x \equiv 10\ mod\ 7 \rightarrow x \equiv 3\ mod\ 7$*.*

- $3x \equiv 4\ (mod\ 7)$?
- Vimos que 5 é um inverso de 3 mod 7.
- Assim, $x \equiv 20\ (mod\ 7)$, logo $x \equiv 6\ (mod\ 7)$.

Exemplos

Exemplo

Encontre x para $4x \equiv 5 \pmod 9$.

1. *O inverso de 4 mod 9 é -2, 7, etc.*
2. *Logo* $x \equiv 35 \pmod 9$ *ou* $x \equiv 8 \bmod 9$.

Exemplos

Exemplo

Encontre x para $4x \equiv 5 \pmod{9}$.

1. *O inverso de 4 mod 9 é -2, 7, etc.*
2. *Logo* $x \equiv 35 \pmod{9}$ *ou* $x \equiv 8 \ mod\ 9$.

- 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?

- 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?

- 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 $21 \equiv 1$ (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 $21 \equiv 1$ (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 $21 \equiv 1$ (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 $21 \equiv 1$ (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.

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 $Y_2 \equiv 2$ (m od 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 $Y_2 \equiv 2$ (m od 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 $Y_2 \equiv 2$ (m od 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 $Y_2 \equiv 2$ (m od 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 $Y_2 \equiv 2$ (m od 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 $Y_2 \equiv 2$ (m od 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 $Y_2 \equiv 2$ (m od 3);
- $x \equiv 1.3.1 + 1.2.2 \ (mod\ 6)$
- $x \equiv 7 \ (mod\ 6)$.

- 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:

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

- 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:
- $(a\ mod\ m_1,\ a\ mod\ m_2, \ldots,\ \ mod\ m_n)$

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:

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

- 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.

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:
  - $C \equiv M^e \ \mathbf{mod}\ n$

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 99$; 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 $C \equiv M^{13} \textbf{ mod } 2537$.
- Rapidamente é possível calcular 181913 **mod** $2537 = 2081$ e 1415^{13} **mod** $2537 = 2182$.
- A mensagem enpriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 99$; 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 enpriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 99$; 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 $C \equiv M^{13} \textbf{ mod } 2537$.
- Rapidamente é possível calcular $181913 \textbf{ mod } 2537 = 2081$ e $1415^{13} \textbf{ mod } 2537 = 2182$.
- A mensagem enpriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 99$; 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 $C \equiv M^{13} \textbf{ mod } 2537$.
- Rapidamente é possível calcular $181913 \textbf{ mod } 2537 = 2081$ e $1415^{13} \textbf{ mod } 2537 = 2182$.
- A mensagem enpriptada é 2081 2182.

Exemplo de encriptação RSA

- Seja a mensagem original a palavra STOP, onde $p = 43$ e $q = 99$; 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 $C \equiv M^{13} \textbf{ mod } 2537$.
- Rapidamente é possível calcular 181913 **mod** $2537 = 2081$ e 1415^{13} **mod** $2537 = 2182$.
- A mensagem enpriptada 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:
- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M(\text{ mod } p)$
- 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:
- $M^{p-1} \equiv 1 \text{ (mod } p)$ 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:
- $M^{p-1} \equiv 1 \pmod p$ e $M^{q-1} \equiv 1 \pmod q$. Logo:
- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M(\bmod p)$
- e $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M(\bmod q)$
- 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:
- $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M(\bmod p)$
- e $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M(\bmod q)$
- 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} 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 $C^{937} \bmod 2537$
- $0981^{937} \bmod 2537 = 0704$ 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 $C^{937} \bmod 2537$
- $0981^{937} \bmod 2537 = 0704$ 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} mod $2537 = 0704$ e 0461^{937} mod $2537 = 115$
- A mensagem númerica é 0704 1115.
- o texto original é HELP