Notas sobre teoria dos números - Aritmática Modular (2)

Anjolina Grisi de Oliveira

1 Introdução à Aritmética modular

Definição 1 *Sejam a e b inteiros positivos. Nós denotamos a* **mod m como o resto quando** *a* **é dividido por** *m*.

Definição 2 *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* $a \equiv b(modm)$ *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** $b = b$ **mod** m.

Teorema 1 *Seja m um inteiro positivo. Se* $a \equiv b \ (mod\ m)$ *e* $c \equiv d \ (mod\ m)$, *então* $a + c \equiv b + d \ (mod\ m)$ *e* $ac \equiv bd \ (mod\ m)$.

2 Adição, Subtração e Multiplicação

- 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.

- De modo semelhante, podemos facilmente calcular:

  a) Quinta-feira.Sexta-feira;
  b) (Sábado)^2;
  c) Segunda-feira - Sábado.

  a) Quinta-feira.Sexta-feira $\rightarrow$ $(4.5)\ mod\ 7 = 6 =$ Sábado;
  b) (Sábado)$^2 \rightarrow (6)^2\ mod\ 7 = 36\ mod\ 7 = 1 =$ Segunda-feira;
  c) Segunda-feira - Sábado $\rightarrow$ $(1 - 6)\ mod\ 7 = -5\ mod\ 7 = 2 =$ Terça-feira.

3 Propriedades

De modo semelhante à aritmética com inteiros, na aritmética modular temos as seguintes propriedades:

1. Comutatividade:
   (a) Seg + Sex = Sex + Seg. $((a + b)\ mod\ m\ = (b + a)\ mod\ m)$;
   (b) Ter.Qui = Qui.Terc;
2. Associatividade:
   (a) (Seg + Ter) + Qui = Seg + (Ter + Qui);
   (b) (Sex.Ter).Qua = Sex.(Ter.Qua).
3. Elemento neutro da adição:
   (a) Seg + Dom = Seg; Ter + Dom = Ter. O "Dom" é o zero.
4. Elemento neutro da multiplicação:
   (a) Seg.Ter = Ter; Qua.Seg = Qua. "Seg" funciona como um.
5. Subtração é o inverso da soma:
   (a) (Seg + Ter) - Seg = Ter.

4 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.
  - $\frac{Ter}{Qua} = x$
  - $x.Qua = Ter$
  - 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.

5 Alguns Resultados

Teorema 2 (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.

Exemplo 1 *Expresse o mdc(300,18) = 6 como uma combinaç ao 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* → **12 = 300 -18.16**
2. *18 = 12.1 + 6* → **6 = 18-12**
3. *12 = 6.2 + 0*

Logo, 6=18 -(300 - 18.16) → *6 = 18 - 300 + 18.16* → **6 = 17.18 - 300**.

Exemplo 2 *Expresse p 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*

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 1 (pg. 138) *Se a, b e c são inteiros positivos de forma que a e b são primos entre si e a | bc entào a | c.*

Prova

1. a e b sào primos entre si → 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 $a \mid 9sac + tbc)$, logo $a \mid c$

Teorema 3 (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 $a \equiv b(mod\ m)$.

6 Resolvendo Congruência Linear

- 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, precismoas 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 4 (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 → sa + tm = 1;
2. sa + tm ≡ 1 (mod m);

3. tm $\equiv 0$ (mod m);

4. sa $\equiv 1$ (mod m).

5. s é o inverso de a módulo m.

Exemplo 3 *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.*

Exemplo 4 *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.

- 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 $x \equiv b.\bar{a}\ (mod\ m)$

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

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

Exemplo 7 *Encontre* x *para* $4x \equiv 5\ (mod\ 9)$*.*

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

7 Teorema Chinês do Resto

Exemplo 8 *No século um, o matemático chinês chamado Sun-Tsu se perguntou: Que núemro 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 5 (Teorema chinês do resto, pg142) *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, $M_k.Y_k \equiv 1 \ (mod\ m_k)$;
  - $x \equiv a_1 M_1 Y_1 + a_2 M_2 Y_2 + \ldots a_n M_n Y_n \ (mod\ m)$.

Exemplo 9 *Vamos solucionar o exemplo 8.*

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* $35 \equiv 2 \ (mod\ 3)$*;*
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. $x \equiv 2.35.2 + 3.21.1 + 2.15.1 \ (mod\ 106) \equiv 233 \equiv 23 \ (mod\ 105)$.

Exemplo 10 *Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?*

1. $x \equiv 1\ (mod\ 2)$ *e* $x \equiv 1\ (mod\ 3)$*;*
2. $m = 6$*,* $M_1 = 3$ *e* $M_2 = 2$*;*
3. Y_1 *é o inverso de 3 mod 2, como* $3\ \equiv 1\ (mod\ 2) \rightarrow Y_1 \equiv 1\ (mod\ 2)$*;*
4. Y_2 *é o inverso de 2 mod 3, como 2 mod 3 = 2, logo* $Y_2 \equiv 2\ (mod\ 3)$*;*
5. $x\ \equiv\ 1.3.1 + 1.2.2\ (mod\ 6)$
6. $x\ \equiv\ 7\ (mod\ 6)$.