Teoria dos números I
Divisibilidade e aritmética modular

André Gustavo dos Santos[1]

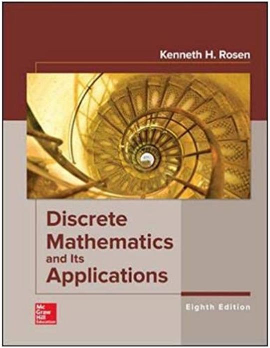
[1] Departamento de Informática
Universidade Federal de Viçosa

INF230 - 2021/1

Conteúdo

UFV

Os slides seguintes são baseados nas seções 4.1 e 4.2.4 do livro texto da disciplina:



ROSEN, Kenneth H.
Discrete mathematics and its applications.
McGraw-Hill Education, 8th edition, 2018

Introdução

- **Teoria dos números** é o ramo da matemática dedicado ao estudo dos números inteiros e suas propriedades
- Há vários conceitos importantes na teoria dos números usados na computação
- Nesta aula falaremos apenas de divisibilidade e aritmética modular
- Depois veremos números primos, distribuição de primos, algumas questões em aberto, além de MDC e do teorema fundamental da aritmética
- Em seguida, congruências lineares e solução de sistemas de congruências pelo teorema chinês do resto
- Por fim, aplicações na computação: geração de números pseudoaleatórios, dígito verificador e criptografia de chave pública

"*Mathematics is the queen of the sciences, and the theory of numbers is the queen of mathematics.*" – Gauss

Divisibilidade

- Um inteiro dividido por outro inteiro ($\neq 0$) pode produzir ou não um resultado inteiro
- Por exemplo, $12/4 = 3$ é um número inteiro, mas $11/4 = 2.75$ não

- Mas em teoria dos números trabalhamos apenas com números inteiros.
- A divisão de um número inteiro por um inteiro positivo produz um quociente e um resto
- Trabalhar com esses restos nos leva à aritmética modular, importante na matemática e usada em várias áreas da computação

Divisão

Definição

Se a e b são inteiros com $a \neq 0$, dizemos que *a divide b* se há um inteiro c tal que $b = ac$ (ou, de forma equivalente, se $\frac{b}{a}$ é um inteiro).

Quando a divide b dizemos que a é um *fator* (ou *divisor*) de b, e que b é um *múltiplo* de a.

A notação $a|b$ indica que a divide b. Usamos $a \not| b$ quando a não divide b.

Obs.: podemos expressar a|b com quantificadores, como $\exists c(ac = b)$ *no domínio dos inteiros.*

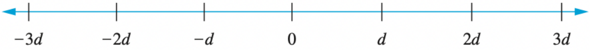
Determine se $3|7$ e se $3|12$

Temos que $3|12$ pois $12 = 3 \cdot 4$. Ou, de forma equivalente, $12/3 = 4$.
Mas $3 \not| 7$ pois não existe inteiro c tal que $7 = 3c$, ou seja, $7/3$ não é um número inteiro.

UFV

Divisão

A figura abaixo representa os inteiros divisíveis por um inteiro positivo d:



Sejam n e d inteiros positivos. Quantos inteiros positivos $\leq n$ são divisíveis por d?

- Os inteiros positivos divisíveis por n são da forma dk, sendo k um inteiro positivo.
- A quantidade deles $\leq n$ são a quantidade de valores k tal que $0 < dk \leq n$.
- Que é o mesmo que $0 < k \leq \lfloor \frac{n}{d} \rfloor$.
- Portanto, há $\lfloor \frac{n}{d} \rfloor$ inteiros positivos até n divisíveis por d.

Divisão

Teorema 1

Sejam a, b, c inteiros, com $a \neq 0$. Então

1. se $a|b$ e $a|c$, então $a|(b+c)$;
2. se $a|b$, então $a|bc$ para todo inteiro c;
3. se $a|b$ e $b|c$, então $a|c$.

Prova (do item 1)

- Se $a|b$ então $b = ak$ para algum inteiro k; se $a|c$ então $c = aj$ para algum inteiro j;
- Então $b + c = ak + aj = a(k + j)$; logo $a|(b+c)$ pois $b + c = ar$, para o inteiro $r = k + j$.

Corolário 1

Se a, b, c são inteiros, com $a \neq 0$, tais que $a|b$ e $a|c$, então $a|mb + nc$ para quaisquer m, n inteiros.

Prova

- Pelo item 2 do teorema 1, se $a|b$ então $a|bm$ para todo inteiro m; analogamente, $a|cn$
- Pelo item 1 do teorema 1, se $a|bm$ e $a|cn$, então $a|bm + cn$.

Algoritmo de Divisão

Teorema 2 - Algoritmo de Divisão

Seja a um inteiro e d um inteiro positivo. Então há números inteiros q e r, únicos, com $0 \leq r < d$, tal que $a = dq + r$.

Obs: o teorema 2 não é realmente um algoritmo, mas esse é seu nome tradicional.

Definição

Na equação do algoritmo da divisão, d é chamado *divisor*, a é chamado *dividendo*, q é o *quociente* e r é o *resto*. A notação abaixo é usada para expressar quociente e resto:

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

*Obs: temos que a **div** $d = \lfloor a/d \rfloor$ e a **mod** $d = a - d\lfloor a/d \rfloor$.*

Exemplos

Qual o quociente e qual o resto quando 101 é dividido por 11?

Temos que $101 = 11 \cdot 9 + 2$; o quociente é $9 = 101$ **div** 11 e o resto é $2 = 101$ **mod** 11

Qual o quociente e qual o resto quando -11 é dividido por 3?

O quociente é $-4 = -11$ **div** 3 e o resto é $1 = -11$ **mod** 3

Obs: note que, apesar de $-11 = 3(-3) - 2$, o resto não é -2, pois não pode ser negativo ($r = -2$ não satisfaz $0 \leq r < 3$).

Implementação

- Linguagens de programação têm operadores para cálculo do resto:
  - `mod` – BASIC e Maple (também em Excel e SQL)
  - `%` – C, C++, Java e Python
  - `rem` – Ada e Lisp
- Cuidado ao usá-los!
  - alguns deles retornam $a - d\lceil a/d \rceil$ em vez de $a \textbf{ mod } d = a - d\lfloor a/d \rfloor$ quando $a < 0$
  - e alguns são definidos também para $m < 0$ (e até para $m = 0$)

Aritmética modular

- Em algumas situações precisamos apenas do resto de um número inteiro quando é dividido por um determinado número inteiro positivo
- Exemplo: que horas serão daqui a 50 horas?
- Como frequentemente precisamos só do resto, há notações especiais para eles
- Já vimos que $a \ \mathbf{mod} \ m$ representa o resto da divisão de a por m
- A notação de congruência a seguir é usada para indicar que dois inteiros possuem o mesmo resto quando divididos por um inteiro positivo m

Congruência

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 $a \equiv b \pmod{m}$ para indicar isso. Se a e b não são congruentes módulo m, escrevemos $a \not\equiv b (\text{mod } m)$.

- Embora as notações $a \equiv b \pmod{m}$ e $a \bmod m = b$ incluam "mod", representam coisas diferentes
  - $a \equiv b \pmod{m}$ é uma relação no conjunto de inteiros
  - $a \ \textbf{mod} \ m = b$ é uma função nesse conjunto
- Entretanto, existe uma estreita conexão entre elas, dada pelo teorema a seguir

Teorema 3

Sejam a e b números inteiros e m um inteiro positivo. Então $a \equiv b \pmod{m}$ se e somente se $a \bmod m = b \bmod m$.

UFV

Exemplos

17 é congruente a 5 módulo 6?

Sim, pois 6 divide $17 - 5 = 12$. Logo, $17 \equiv 5 \pmod{6}$.

Outra forma: sim, pois 17 *e* 5 *deixam o mesmo resto,* 5*, quando divididos por* 6*.*

24 e 4 são congruentes módulo 6?

Não, pois 6 não divide $24 - 14 = 10$. Logo, $24 \not\equiv 14 \pmod{6}$.

Outra forma: não, pois 24 *e* 14 *deixam restos diferentes quando divididos por* 6 *(*0 *e* 2*).*

Congruência

Teorema 4

Seja m um inteiro positivo. Os inteiros a e b são congruentes módulo m se e somente se existe um inteiro k tal que $a = b + km$.

Prova

- ($\rightarrow$) Se a e b são congruentes módulo m, então $m|(a - b)$.
  Logo, existe um inteiro k tal que $a - b = km$, então $a = b + km$.
- ($\leftarrow$) Se existe um inteiro k tal que $a = b + km$, então $a - b = km$.
  Logo, $m|(a - b)$, então $a \equiv b (\text{mod } m)$.

Classe de congruência

- O conjunto de todos os inteiros congruentes a um inteiro a módulo m forma uma classe de congruência.
- É possível mostrar que há m classes de congruência disjuntas módulo m e que a união de todas elas é o conjunto de números inteiros.

Adição e multiplicação

- O teorema a seguir mostra que adição e multiplicação preservam congruência

Teorema 5

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

Exemplo

Temos que $7 \equiv 2 (\text{mod } 5)$ e $11 \equiv 1 (\text{mod } 5)$. Então:

- $18 = 7 + 11 \equiv 2 + 1 = 3 (\text{mod } 5)$
- $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 (\text{mod } 5)$

Calcule o valor de $(19^3 \text{ mod } 31)^4 \text{ mod } 23$

- $19^3 \text{ mod } 31 = (19 \cdot 19 \cdot 19) \text{ mod } 31 = 6859 \text{ mod } 31 = 8$
- $8^4 \text{ mod } 23 = (8 \cdot 8 \cdot 8 \cdot 8) \text{ mod } 23) = 4096 \text{ mod } 23 = 2$

Adição e multiplicação

Corolário (do teorema 5)

Seja m um inteiro positivo. Se a e b são inteiros, então

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

e

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Calcule o valor de $(19^3 \bmod 31)^4 \bmod 23$

- $$\begin{aligned} 19^3 \bmod 31 &= (((19 \cdot 19) \bmod 31) \cdot 19) \bmod 31 \\ &= ((361 \bmod 31) \cdot 19) \bmod 31 \\ &= (20 \cdot 19) \bmod 31 \\ &= 380 \bmod 31 = 8 \end{aligned}$$
- $$\begin{aligned} 8^4 \bmod 23 &= (((8 \cdot 8) \bmod 23) \cdot 8) \bmod 23) \cdot 8) \bmod 23 \\ &= ((((64 \bmod 23) \cdot 8) \bmod 23) \cdot 8) \bmod 23 \\ &= (((18 \cdot 8) \bmod 23) \cdot 8) \bmod 23 \\ &= ((144 \bmod 23) \cdot 8) \bmod 23 \\ &= (6 \cdot 8) \bmod 23 \\ &= 48 \bmod 23 = 2. \end{aligned}$$

Obs.: no slide anterior o cálculo foi feito sem calcular mod a cada passo; valores intermediários poderiam ficar muito grandes, causando overflow para expoentes altos.

Cuidado!

- Muito cuidado ao trabalhar com congruências
- Algumas propriedades que podemos pensar ser verdadeiras não são válidas
- Por exemplo, se $ac \equiv bc (\text{mod } m)$ a congruência $a \equiv b (\text{mod } m)$ pode ser falsa
- E se $a \equiv b (\text{mod } m)$ e $c \equiv d (\text{mod } m)$, a congruência $a^c \equiv b^d (\text{mod } m)$ pode ser falsa

Aritmética módulo *m*

- Podemos definir operações aritméticas em $\mathbb{Z}_m$, o conjunto de inteiros não negativos menores que m, ou seja, $\{0, 1, \ldots, m-1\}$.
- A adição, denotada por $+_m$, é definida como

$$a +_m b = (a + b) \bmod m$$

- E a multiplicação, denotada por $\cdot_m$, é definida como

$$a \cdot_m b = (a \cdot b) \bmod m$$

Encontre o valor de $7 +_{11} 9$ e $7 \cdot_{11} 9$ em $\mathbb{Z}_{11}$

- $7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

UFV

Propriedades

As operações $+_m$ e $\cdot_m$ satisfazem muitas das propriedades da adição e da multiplicação comuns. Em particular:

- Fechamento: se a e b pertencem a $\mathbb{Z}_m$, então $a +_m b$ e $a \cdot_m b$ também pertencem a $\mathbb{Z}_m$
- Associatividade: se a, b e c pertencem a $\mathbb{Z}_m$, então $(a +_m b) +_m c = a +_m (b +_m c)$ e $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$
- Comutatividade: se a e b pertencem a $\mathbb{Z}_m$, então $a +_m b = b +_m a$ e $a \cdot_m b = b \cdot_m a$
- Elemento neutro: 0 e 1 são elementos neutros da adição e multiplicação módulo m, respectivamente. Assim, se $a \in \mathbb{Z}_m$, então $a +_m 0 = a$ e $a \cdot_m 1 = a$
- Oposto: Se $a \neq 0$ pertence a $\mathbb{Z}_m$, $m - a$ é seu oposto (inverso aditivo) módulo m, e 0 é seu próprio oposto. Ou seja, $a +_m (m - a) = 0$ e $0 +_m 0 = 0$
- Distributividade: se a, b e c pertencem a $\mathbb{Z}_m$, então $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ e $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Obs.: não foi incluída propriedade de inverso multiplicativo, pois nem sempre existe módulo m

Potenciação modular - motivação

- Em criptografia é importante encontrar $b^n \bmod m$ de forma eficiente em tempo e espaço, ou seja, rapidamente e sem gastar muita memória.
- É impraticável calcular b^n primeiro e só depois achar o resto por m, pois para n grande b^n fica gigantesco, necessitando muita memória para armazenamento

Calcule $3^{106} \bmod 47$

- $3^{106} \bmod 47 = 375710212613636260325580163599137907799836383538729 \bmod 47 = 14$

Potenciação modular - motivação

- Pelas propriedades da multiplicação na aritmética modular, podemos calcular $b^n \bmod m$ calculando sucessivamente $b^k \bmod m$ para $k = 1, 2, \ldots, m$, já que $b^{k+1} \bmod m = b(b^k \bmod m) \bmod m$
- Com esta ideia evitamos que o valor cresça muito (pois fazemos mod m a cada multiplicação), mas ainda fazemos $n - 1$ multiplicações.

Calcule $3^{106} \bmod 47$

- $3^1 \bmod 47 = 3$
- $3^2 \bmod 47 = 3 \cdot 3 \bmod 47 = 9 \bmod 47 = 9$
- $3^3 \bmod 47 = 3 \cdot 9 \bmod 47 = 27 \bmod 47 = 27$
- $3^4 \bmod 47 = 3 \cdot 27 \bmod 47 = 81 \bmod 47 = 34$
- $3^5 \bmod 47 = 3 \cdot 34 \bmod 47 = 102 \bmod 47 = 8$
- $3^6 \bmod 47 = 3 \cdot 8 \bmod 47 = 24 \bmod 47 = 24$
- $3^7 \bmod 47 = 3 \cdot 24 \bmod 47 = 72 \bmod 47 = 25$
- ...
- $3^{106} \bmod 47 = \ldots$

Potenciação modular - algoritmo

Queremos calcular $b^n \bmod m$

- Seja $(a_{k-1} \dots a_1 a_0)_2$ a representação binária de n
- Então $n = 2^{k-1} a_{k-1} + \cdots + 2^1 a_1 + 2^0 a_0$
- Note que $b^n = b^{2^{k-1} a_{k-1} + \cdots + 2^1 a_1 + 2^0 a_0} = b^{2^{k-1} a_{k-1}} \cdot \ldots \cdot b^{2^1 a_1} \cdot b^{2^0 a_0}$
- Calculamos somente $b, b^2, b^4, \ldots, b^{k-1}$ e multiplicamos os b^{2^i} quando $a_i = 1$

Calcule $3^{106} \bmod 47$

- $106 = 1101010_2 = 2^6 + 2^5 + 2^3 + 2^1$
- $3^1 \bmod 47 = 3$
- $3^2 \bmod 47 = 3 \cdot 3 \bmod 47 = 9 \bmod 47 = 9$
- $3^4 \bmod 47 = 9 \cdot 9 \bmod 47 = 81 \bmod 47 = 34$
- $3^8 \bmod 47 = 34 \cdot 34 \bmod 47 = 1156 \bmod 47 = 28$
- $3^{16} \bmod 47 = 28 \cdot 28 \bmod 47 = 102 \bmod 47 = 32$
- $3^{32} \bmod 47 = 32 \cdot 32 \bmod 47 = 1024 \bmod 47 = 37$
- $3^{64} \bmod 47 = 37 \cdot 37 \bmod 47 = 1369 \bmod 47 = 6$
- $3^{106} = 3^{2^6+2^5+2^3+2^1} = 3^{64} 3^{32} 3^8 3^2 = 6 \cdot_{47} 37 \cdot_{47} 28 \cdot_{47} 9 = 34 \cdot_{47} 28 \cdot_{47} 9 = 12 \cdot_{47} 9 = 14$

- São $\mathcal{O}(log_2 n)$ operações, eficiente no tempo.
- Reduzindo o resultado mod m a cada multiplicação, eficiente no espaço.