

Inteiros

Inteiros.

Congruência.

Referência: Discrete Mathematics with Graph Theory
Edgar Goodaire e Michael Parmenter, 3rd ed 2006
Capítulo: 4

Números reais

- ❑ A relação binária \leq em \mathbb{R} é uma ordem parcial
 - Reflexiva, antissimétrica, transitiva
- ❑ Propriedades da adição e multiplicação de reais ($a, b, c \in \mathbb{R}$)
 - (**fecho**) $a+b$ e ab são números reais
 - (**comutatividade**) $a+b = b+a$ e $ab = ba$
 - (**associatividade**) $(a+b)+c = a+(b+c)$ e $(ab)c = a(bc)$
 - (**elemento neutro**) $a+0 = a$ e $a \cdot 1 = a$
 - (**distributividade**) $a(b+c) = ab+ac$ e $(a+b)c = ac+bc$
 - (**inverso aditivo**) $a+(-a) = 0$
 - (**inverso multiplicativo**) $a \left(\frac{1}{a}\right) = 1$ se $a \neq 0$
 - $a \leq b$ implica $a+c \leq b+c$
 - $a \leq b$ e $c \geq 0$ implica que $ac \leq bc$
 - $a \leq b$ e $c \leq 0$ implica que $ac \geq bc$

A subtração define-se como
 $a-b = a+(-b)$

Princípio da boa ordenação

❑ Muitos conjuntos de reais não têm mínimo

– Não existe o menor real positivo

– $\min\left\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right\} = ?$

❑ Este problema não ocorre nos naturais

Princípio da boa ordenação. Todo o conjunto não vazio de números naturais tem um elemento mínimo.

❑ As propriedades dos reais podem ser transpostas para os inteiros

– O conjunto dos naturais é fechado para a adição? Multiplicação? Subtração?

– O conjunto dos inteiros ímpares é fechado para a adição?

Algoritmo da divisão

❑ Divisão

❑ $\frac{58}{17} = 3 + \frac{7}{17}$

$\frac{58}{17} = 2 + \frac{24}{17}$

❑ $\frac{a}{b} = q + \frac{r}{b}$

$a = qb + r$

Menor dos múltiplos de b
maiores que a (existe!)
 $0 \leq r = a - qb < b$



❑ **Teorema:** sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Então existem inteiros únicos q e r , com $0 \leq r < |b|$, tal que $a = qb + r$.

- q – quociente
- r – resto

Exemplo

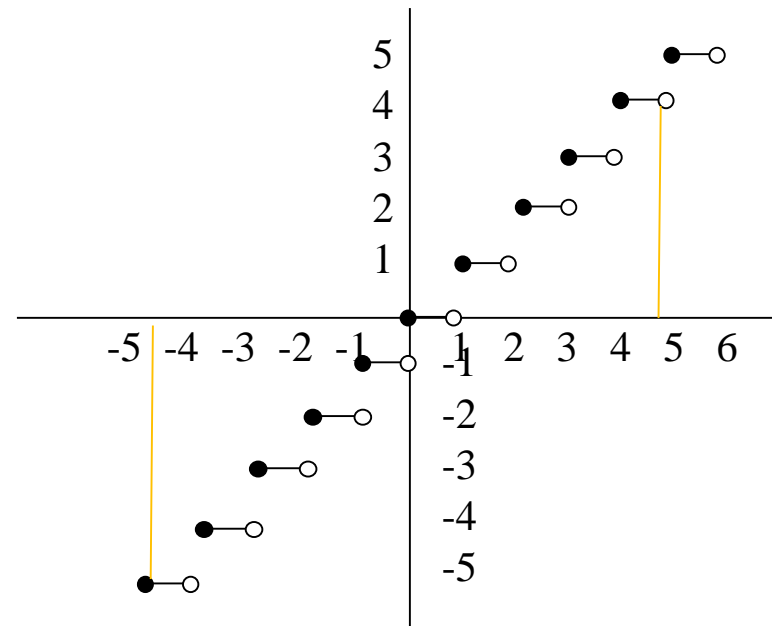
$$\square a = qb + r, \quad 0 \leq r < |b|$$

$$\square 19 = 4(4) + 3$$

$$\square -19 = -5(4) + 1$$

$$\square 19 = -4(-4) + 3$$

$$\square -19 = 5(-4) + 1$$



Função chão.

$$\square \text{Proposição: } q = \begin{cases} \left\lfloor \frac{a}{b} \right\rfloor & \text{se } b > 0 \\ \left\lceil \frac{a}{b} \right\rceil & \text{se } b < 0 \end{cases}$$

$$\frac{19}{4} = 4.75$$

Representação de naturais

□ Representação habitual é base 10

$$- 2159 = 2 * 10^3 + 1 * 10^2 + 5 * 10^1 + 9 * 10^0 = (2159)_{10}$$

$$(a_{n-1}a_{n-2} \dots a_0)_b = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \dots + a_1b + a_0$$

$$\square N = \underbrace{((a_{n-1}b + a_{n-2})b + \dots + a_1)b + a_0}_{q_0}$$

$$\begin{array}{ccccccc} N & \lfloor b & & & & & \\ a_0 & q_0 & \lfloor b & & & & \\ & a_1 & q_1 & \dots & \lfloor b & & \\ & & & a_{n-2} & a_{n-1} & & \end{array}$$

$$\begin{array}{ccccccc} 2159 & \lfloor 8 & & & & & \\ 7 & 269 & \lfloor 8 & & & & \\ & 5 & 33 & \lfloor 8 & & & \\ & & 1 & 4 & & & \end{array}$$

$$(4157)_8$$

Numeração binária e hexadecimal

❑ Representação base 2 ou binária

$$\begin{aligned} - (2159)_{10} &= 1 * 2^{11} + 0 * 2^{10} + 0 * 2^9 + 0 * 2^8 + 0 * 2^7 + 1 * 2^6 \\ &+ 1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0 = \\ &= (100001101111)_2 \end{aligned}$$

❑ Base 16 ou hexadecimal necessita de 16 símbolos

- 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

$$- (2159)_{10} = 8 * 16^2 + 6 * 16^1 + 15 * 16^0 = (86F)_{16}$$

❑ Passar da binária para a hexadecimal

- 1000 0110 1111

- 8 6 F

Divisibilidade

- ❑ **Definição:** dados a e b inteiros com $b \neq 0$, diz-se que b é um divisor ou um fator de a e que a é divisível por b se e só se $a = qb$ para algum inteiro q .
 - Escreve-se $b|a$ e lê-se “b divide a”
- ❑ Para todo o n , $1|n$ e para $n \neq 0$, $n|0$
- ❑ **Proposição:** Sejam a, b, c inteiros tais que $c|a$ e $c|b$. Então $c|(xa + yb)$ para quaisquer inteiros x e y .
- ❑ **Prova:** dado que $c|a$, $a = q_1c$, q_1 inteiro, e dado que $c|b$, $b = q_2c$, q_2 inteiro. Então $xa + yb = xq_1c + yq_2c = (q_1x + q_2y)c$. Como $(q_1x + q_2y)$ é um inteiro então $c|(xa + yb)$
- ❑ A relação binária em \mathbb{N} $a|b$ é ordem parcial e $(\mathbb{N}, |)$ um cpo

Máximo divisor comum

❑ **Definição:** Sejam a e b inteiros não simultaneamente iguais a 0. Um inteiro g é o máximo divisor comum de a e b , $g = \text{mdc}(a, b)$, se $g|a$ e $g|b$ e qualquer c tal que $c|a$ e $c|b$ implica $c \leq g$.

❑ Ex: Considere os números 238 e 68

$$\text{divisores}238 = \{1, 2, 7, 14, 17, 34, 119, 238\}$$

$$\text{divisores}68 = \{1, 2, 4, 17, 34, 68\}$$

$$\text{divisoresComuns} = \{1, 2, 17, 34\}$$

$$\text{mdc}(238, 68) = 34$$

Lema

□ **Lema:** se $a = qb + r$ para inteiros a, b, q, r então
 $\text{mdc}(a, b) = \text{mdc}(b, r)$

– Como $238 = 3(68) + 34$, $\text{mdc}(238, 68) = \text{mdc}(68, 34) = 34$
porque $68 = 2(34) + 0$

□ **Prova:** Seja $g_1 = \text{mdc}(a, b)$ e $g_2 = \text{mdc}(b, r)$.

Como $g_2 | b$ e $g_2 | r$ então $g_2 | (qb + r)$, isto é, $g_2 | a$. Então g_2 é um divisor comum de a e de b e, como g_1 é o maior divisor comum de a e de b , $g_2 \leq g_1$.

Por outro lado, como $g_1 | a$ e $g_1 | b$ temos que $g_1 | (a - qb)$, isto é, $g_1 | r$. Então g_1 é um divisor comum de b e de r e, como g_2 é o maior divisor comum de b e de r , $g_1 \leq g_2$. Portanto, $g_1 = g_2$ e $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Algoritmo de Euclides

❑ Sejam a e b números naturais com $b < a$. Para calcular $\text{mdc}(a, b)$ fazer

❑ $a = q_1 b + r_1, \quad 0 \leq r_1 < b$

❑ Se $r_1 \neq 0$ $b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1$

❑ Se $r_2 \neq 0$ $r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2$

❑ Se $r_k \neq 0$ $r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad 0 \leq r_{k+1} < r_k$

❑ Se $r_{k+1} = 0$, $\text{mdc}(r_{k-1}, r_k) = r_k = \text{mdc}(a, b)$.

– Ex: $\text{mdc}(630, 196) = 14$

– $630 = 3(196) + 42 \quad 42 = 630 - 3(196) = a - 3b$

– $196 = 4(42) + 28 \quad 28 = 196 - 4(42) = b - 4r_1 = b - 4(a - 3b) = -4a + 13b$

– $42 = 1(28) + 14 \quad 14 = 42 - 28 = r_1 - r_2 = (a - 3b) - (-4a + 13b) = 5a - 16b$

– $28 = 2(14) + 0$

Obtenção de $\text{mdc}(a,b)=ma+nb$

Apresentando as três equações anteriores $r = ma+nb$ em forma tabular, antecedidas das duas linhas para a e para b

	r	a	b	q
a	630	1	0	
b	196	0	1	3
r₁	42	1	-3	4
r₂	28	-4	13	1
r₃	14	5	-16	2
r₄	0			

$$q_k = \text{quotient}(r_{k-1}, r_k)$$

$$3 = \text{quotient}(630, 196)$$

$$(42, 1, -3) = (630, 1, 0) - 3(196, 0, 1)$$

$$\text{linha}_k = \text{linha}_{k-2} - q_{k-1} \text{linha}_{k-1}$$

Como $r_4=0$,

$$\text{mdc}(630, 196) = r_3 = 14 = 5(630) + (-16)(196)$$

Propriedades do mdc

- ❑ **Definição:** Dois inteiros a e b , $a \neq 0$ $b \neq 0$, são primos entre si se $\text{mdc}(a,b)=1$
- ❑ **Teorema:** O máximo divisor comum dos inteiros a e b é uma combinação linear inteira de a e b , $g=\text{mdc}(a,b) = ma+nb$.
 - $\text{mdc}(630,196)=14=5a-16b=5(630)-16(196)$
- ❑ **Corolário:** Sejam x,a,b inteiros tais que $x|ab$. Se x e a forem primos entre si, então $x|b$.
- ❑ **Corolário:** o $\text{mdc}(a,b)$ é divisível por qualquer divisor comum de a e b .
- ❑ Recordando que $(\mathbb{N},|)$ é um cpo, verifica-se que
 - $a \wedge b = \text{mdc}(a,b)$ ínfimo

Mínimo múltiplo comum

- ❑ **Definição:** Se a e b forem inteiros não nulos, dizemos que l é o mínimo múltiplo comum de a e b , $l = mmc(a, b)$, se e só se l for um inteiro positivo que satisfaça
 - $a|l, b|l$ e,
 - Se m for um inteiro positivo tal que $a|m$ e $b|m$ então $l \leq m$.
- Ex: $mmc(630, -196) = 630 * 196 / 14 = 8820$
- ❑ Ainda no cpo $(\mathbb{N}, |)$, verifica-se que
 - ❑ $a \vee b = mmc(a, b)$ supremo
- ❑ O cpo $(\mathbb{N}, |)$ é um reticulado
- ❑ O conjunto dos divisores de um número natural é um reticulado
 - Ex: $A = \{d \in \mathbb{N} \mid d|30\} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

Números primos

- ❑ **Definição:** um número natural $p \geq 2$ é um **primo** se e só se os únicos números naturais que dividem p forem p e 1 . Um número natural $n > 1$ que não seja primo é **composto**.
 - n é composto se $n=ab$, com $1 < a, b < n$
 - 1 não é primo nem composto
 - Há $\frac{1}{4}$ de números primos de 1 a 100
 - $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$
 - Alguns primos grandes: $2^{756839}-1$, $2^{859433}-1$
- ❑ **Lema:** Dado qualquer número natural $n > 1$, existe um primo p tal que $p|n$.

Primos

- ❑ **Teorema:** há um número infinito de primos.
 - Prova por contradição: se o número de primos for finito p_1, p_2, \dots, p_t , seja $n = (p_1 p_2 \dots p_t) + 1$. Pelo lema, n é divisível por um primo, p_i . Como $p_1 p_2 \dots p_t$ também é divisível por p_i , $n - p_1 p_2 \dots p_t = 1$ é divisível por p_i , o que é uma contradição.
- ❑ Como determinar se um número é primo?
 - Os pares são múltiplos de 2
 - Os números cujos algarismos somados são múltiplos de 3 são divisíveis por 3
 - Os números terminados em 0 ou 5 são múltiplos de 5
- ❑ **Lema:** se um número natural $n > 1$ não é primo, então é divisível por um primo $p \leq \sqrt{n}$

Crivo de Eratóstenes

- ❑ Para encontrar todos os primos até n
 - Listar todos os inteiros de 2 a n
 - Marcar 2 e cortar todos os múltiplos de 2; idem para 3, 5, ...
 - Marcar o próximo número não marcado ou cortado e cortar os múltiplos até todos os números até \sqrt{n} estarem marcados ou cortados

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	

Decomposição em números primos

- ❑ **Teorema Fundamental da Aritmética:** cada número natural $n \geq 2$ pode ser escrito $n = p_1 p_2 \dots p_r$ como um produto único de números primos ou, agrupando os primos iguais, na forma $n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ do produto de potências de s primos distintos, em que os primos e as potências são únicos.
- ❑ Ex: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$
- ❑ $1176 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 = 2^3 3^1 7^2$
- ❑ **Definição:** os fatores primos de um inteiro $n \geq 2$ são os números primos que dividem n ; a multiplicidade de um fator primo p de n é o maior α tal que $p^\alpha | n$.

Divisibilidade

❑ $a = 9$ $b = 77$ $ab = 693$

❑ $c = 21$

❑ $c \nmid a$ $c \nmid b$ $c \mid ab$ $21 \mid 693$ $693 = 33 \cdot 21$

❑ Esta situação de um número não dividir nenhum dos fatores mas dividir o produto não pode acontecer se o número for primo!

– Fica evidente se se explicitar a decomposição em números primos

❑ $a = 3 \cdot 3$ $b = 7 \cdot 11$ $c = 3 \cdot 7$

❑ $ab = (3 \cdot 3)(7 \cdot 11) = 3(3 \cdot 7)11 = 3 \cdot c \cdot 11$

❑ Se c fosse um número primo tinha que dividir a ou b

Unicidade da decomposição

❑ **Proposição:** se um primo p divide o produto $a_1 a_2 \dots a_k$ de inteiros, então p divide um dos a_i .

❑ **Unicidade da decomposição em fatores primos**

- Prova: Assuma-se que um número natural $n > 1$ pode ser fatorizado em números primos de duas maneiras diferentes

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$$

- Cancelem-se os fatores iguais nas duas expressões; obtém-se um produto de primos igual a 1 (absurdo) ou uma equação da mesma forma sem fatores repetidos nas duas expressões
- Como $p_1 | p_1 p_2 \dots p_k$ então $p_1 | q_1 q_2 \dots q_l$. Pela proposição acima, $p_1 | q_j$ para um dos primos q_j . Como tanto p_1 como q_j são primos, isto força $p_1 = q_j$
- Mas isso contradiz a não existência de primos comuns, pelo que não podem existir duas fatorizações diferentes

Decomposição do mdc

❑ Exercício: qual a decomposição em números primos do $\text{mdc}(a,b)$?

❑ Resposta

- Pelo Teorema Fundamental da Aritmética, a e b podem exprimir-se na forma

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \qquad b = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

- Sendo assim

$$\text{mdc}(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_r^{\min(\alpha_r, \beta_r)}$$

Casos especiais

❑ Primos de Mersenne

- São números da forma $2^p - 1$
- Verificar com p até 16
- Mersenne indicou a lista: 2,3,5,7,13,17,19,31,67,127,257
- Mais tarde corrigiu-se: 2,3,5,7,13,17,19,31,61,89,107,127.
- Conjetura-se que haja relação entre p ser primo e $2^p - 1$ ser primo
 - Se p não for primo $2^p - 1$ também não é; o inverso não é sempre verdade
- O 39º primo de Mersenne ($p=13466917$) foi encontrado em 2001, após dois anos e meio a testar 100000 candidatos numa rede de 200000 PCs
- Não se sabe se há um número infinito de primos de Mersenne

Mais casos especiais

❑ Primos de Fermat

- $2^{2^n} + 1$
- São primos para $n=0, 1, 2, 3, 4$ (para $n=5$ é divisível por 641)
- Há mais do que cinco destes primos?

❑ Qual a regra para obter o número primo seguinte?

- Não há regra conhecida
- Os números primos são muito rebeldes... e essenciais!
- É possível encontrar dois primos consecutivos com um intervalo arbitrariamente grande.
 - $D!+2$ é divisível por 2, $D!+3$ por 3, ..., $D!+D$ por D .
 - Entre $D!+1$ e $D!+D$ não há primos

Qual a densidade de primos?

❑ Teorema dos **números primos**

- Seja $\pi(x)$ o número de primos $p \leq x$
- Valor aproximado: $\pi(x) \sim \frac{x}{\ln x}$
- $\pi(100) \sim \frac{100}{\ln 100} = 21.7$ De facto, 25

❑ Observação

- Todos estes cálculos usam números que ultrapassam a gama de inteiros das unidades aritméticas
- É necessário recorrer a bibliotecas de operações aritméticas sobre cadeias de algarismos de comprimento variável e elevado

Mais casos em aberto

- ❑ **Último Teorema de Fermat.** Para qualquer inteiro $n > 2$ a equação $a^n + b^n = c^n$ não tem solução inteira
 - Prova realizada só em 1994 por Andrew Wiles
- ❑ **Conjetura dos primos gémeos.** Existe um número infinito de números x tais que x e $x+2$ são primos?
 - 11 e 13, 41 e 43
 - não se sabe
- ❑ **Conjetura de Goldbach.** Podem todos os inteiros pares maiores que 2 ser escritos como a soma de dois primos?