Matemática Concreta

Noções sobre Teoria dos Números
Parte 1

Dr. A. Riker
Universidade Federal do Pará (UFPA)
afr@ufpa.br

2021.PL03

Introdução

Parte 1:

- Indução Finita
- Divisibilidade

Parte 2:

- Números Primos
- Congruência

Introdução

- O conjunto dos números Inteiros é central para a matemática em computação. Portanto, queremos explorar a teoria dos números, um ramo importante da matemática preocupado com as propriedades dos inteiros.

Princípio da Indução Finita

- **Axioma de indução:** Seja A um subconjunto dos números naturais que possui as propriedades:
  i) $0 \in A$
  ii) $\forall a \in A => a + 1 \in A$
  Então, A contém todos os números naturais, ou seja, A = N.

Princípio da Indução Finita

- **Teorema do Princípio da Indução**
  Seja a $\in$ N e p(n) uma propriedade de n, a qual pode ser pensada como uma afirmação que envolve um número n dado. Suponha que:
  i) p(a) é verdadeira e
  ii) se p(n) é verdadeira => p(n + 1) é verdadeira, $\forall n \geq$ a.
  Então, p(n) é verdadeira para todo n $\geq$ a.

Princípio da Indução Finita

- **Método prático para Provar por Indução**
  i) Assumir que a hipótese é verdadeira;
  ii) Verificar se a hipótese produz um resultado verdade quando o passo zero é calculado;
  iii) Verificar se a hipótese produz um resultado verdade quando o passo n+1 é calculado;

Princípio da Indução Finita

Exemplo 1: Utilizando o Princípio de Indução Finita, podemos provar que o conjunto das partes de um conjunto A possui exatamente 2^n elementos, onde $n = n(A)$ é o número de elementos de A.

Consideremos inicialmente que $n = 0$, ou seja, o conjunto A é vazio, tem cardinalidade zero e possui apenas um subconjunto que é ele mesmo, desta forma temos que a afirmação é válida para $n = 0$.

$$2^0 = 1.$$

Tomemos como hipótese de indução que o conjunto A, contendo n elementos, possui 2^n subconjuntos.

Verificando o que acontece quando acrescentamos um elemento ao conjunto A, ou seja, consideramos o conjunto A' que possui $n + 1$ elementos. Os 2^n subconjuntos de A também são subconjuntos de A' e quando acrescentamos a cada subconjunto o novo elemento formamos outros 2^n subconjuntos que são diferentes dos primeiros 2^n. Estes são todos os subconjuntos de A', totalizando

$$2^n + 2^n = 2 \cdot 2^n = 2^{n+1} \text{ subconjuntos.}$$

Portanto a afirmação é válida para todo $n \in \mathrm{N}$.

Princípio da Indução Finita

Exemplo 2: Utilizando o Princípio de Indução Finita, provaremos a fórmula da soma dos n primeiros números naturais não nulos.

Sn = 1 + 2 + ...+ n, então $S_n = \frac{n\cdot(n+1)}{2}$

Verificando para $n = 1$, temos que

$S_1 = \frac{1\cdot(1+1)}{2} = \frac{2}{2} = 1$, verdade.

Supondo que a fórmula seja verdadeira para $n \in N^*$, ou seja, a hipótese de indução é que $S_n = \frac{n\cdot(n+1)}{2}$.

Para analisar o que ocorre para $n + 1$, adicionamos este número em ambos os lados da equação:

$$S_n + (n+1) = \frac{n\cdot(n+1)}{2} + (n+1)$$

$$S_{n+1} = \frac{n\cdot(n+1)+2\cdot(n+1)}{2}$$

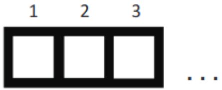
$$S_{n+1} = \frac{(n+1)\cdot(n+2)}{2}$$

$S_{n+1} = \frac{(n+1)\cdot[(n+1)+1]}{2} =$, verdadeira para $n + 1$.

Portanto, pelo Princípio de Indução, a fórmula é válida para todo $n \in N$.

Princípio da Indução Finita

Exemplo 3: Na construção de quadrados conjugados com palitos, necessitamos de quatro palitos para construir o primeiro quadrado, sete palitos para construir dois quadrados, como mostra a figura, ou seja, acrescentamos três palitos para cada novo quadrado.



Mostraremos que a fórmula $a_n = 3 \cdot n + 1$ define o número de palitos utilizados na construção de n quadrados.

Verificando a validade da fórmula para $n = 1$.

$a_1 = 3 \cdot 1 + 1 \Rightarrow a_1 = 4$, fórmula válida para $n = 1$.

Supondo a fórmula verdadeira para $n \in \mathbb{N}$, ou seja, $a_n = 3 \cdot n + 1$.

Para construir cada quadrado acrescentamos três palitos, assim,

$a_{n+1} = 3 \cdot n + 1 + 3$

$a_{n+1} = 3 \cdot (n + 1) + 1$

Donde se conclui que a fórmula é válida para todo $n \in \mathbb{N}$.

Divisibilidade

- Sejam a e b naturais, com a $\neq$ 0, dizemos que a divide b, e denotamos por a|b, se existe um natural c tal que b = a c.
- Podemos dizer que a é um divisor de b ou que b é um múltiplo de a. Caso a não divida b escrevemos a $\nmid$ b.
- De modo análogo, se a e b inteiros, com $a \neq 0$, escrevemos a|b, se b = $a.c$, para algum inteiro c.
  Exemplo: 2|0; 1|3; 3 5; 4|4.

Divisibilidade

- A prova por contradição é muito utilizada quando queremos verificar a propriedade de um único caso. Por exemplo:
- Demonstraremos que o número $5^{250} - 3$ não é divisível por 5.
- Suponha, por contradição, que $5|5^{250} - 3$. Então existe um número tal que:
  $5^{250} - 3 = 5.b$
  $3 = 5^{250} - 5.b$
  $3 = 5(5^{249} - b)$
  $5|3$, o que é absurdo!
- Concluímos que nossa suposição inicial é falsa, então $5 \nmid 5^{250} - 3$.

Divisibilidade

- **Algumas Propriedades**
  - $0 \mid 0$, pois, por exemplo, 0=7.0 e $7 \in N$.
  - Portanto é verdade $0 \mid 0$, mas notem que, particularmente, 0=1.0; 0=3.0; 0=27.0; 0=18745.0; ou seja, o número natural t tal que 0=t.0 claramente não é único!
  - Assim, não existe o quociente de 0 por 0 e portanto, neste contexto, $0 \mid 0$, mas o símbolo $\frac{0}{0}$ não está definido.
  - Devido à não unicidade tratada na observação anterior e ao fato de que 0a se, e somente se, a=0, é comum não trabalhar com o zero como divisor.
  - É comum admitir que todos os divisores considerados são diferentes de zero, mesmo que isso não seja explicitamente dito.

Divisibilidade

- **Algumas Propriedades**
  - Se $b \mid a$ e $b \neq 0$, então o número natural t tal que a=tb é único.
  - Com efeito, vamos considerar que exista outro número natural k tal que a=kb, neste caso, teríamos que kb=tb. Mas, estamos supondo $b \neq 0$; logo, cancelamos o b e obtemos, necessariamente, que k=t. Dessa forma, mesmo que quiséssemos "fabricar" um k diferente, isso não seria possível!

Divisibilidade

Propriedade 1: Se $a \mid b$ e $b \mid a$, então $a = b$.

Ocultar

Ocultar

• Para cada número natural não nulo a, o único número natural não nulo b que é, simultaneamente, múltiplo e divisor de a é o próprio a.

Se $a \mid b$ e $b \mid a$, então, por definição, existem números naturais t e k tais que $b = ta$ e $a = kb$.
Dessa forma, $a = k(ta) = (kt)a$. Mas $a \neq 0$; logo, de $a = (kt)a$, segue que $kt = 1$.
No entanto t e k são números naturais; portanto, $kt = 1$ só é possível se $k = t = 1$ e, assim, de $b = ta$ (ou $a = kb$) segue que $a = b$.

Divisibilidade

Propriedade 2: Se $a \mid b$ e $b \mid m$, então $a \mid m$.

Ocultar

Ocultar

- Divisor de divisor é divisor: se a é divisor de b e b é divisor de m, então a é divisor de m.
- Múltiplo de múltiplo é múltiplo: se m é múltiplo de b e b é múltiplo de a, então m é múltiplo de a.
- Essa propriedade é conhecida por ***transitividade da divisibilidade***.

Se $a \mid b$ e $b \mid m$, então, por definição, existem números naturais t e k de modo que $b = ta$ e $m = kb$.

Assim, temos que

$$m = k(ta) = (kt)a. \qquad (i)$$

Mas como t e k são números naturais, então $x = kt$ também será um número natural, já que o produto de dois números naturais é um número natural.

Dessa forma, por (i), temos que $m = xa$, com $x \in \mathbb{N}$. Portanto, por definição, $a \mid m$.

Divisibilidade

Propriedade 3: Se $a \mid m$ e $a \mid n$, então $a \mid m + n$.

Ocultar

Ocultar

• A soma de múltiplos é um múltiplo: se m e n são múltiplos de a, então a soma $m + n$ é também um múltiplo de a.
• Se a é divisor de m e de n, então a é divisor da soma $m + n$.

Se $a \mid m$ e $a \mid n$, então, por definição, existem números naturais t e k de modo que $m = ta$ e $n = ka$.
Assim, temos que
$m + n = ta + ka = (t + k)a. \qquad (i)$
Mas como t e k são números naturais, então $z = t + k$ também será um número natural, já que a soma de dois números naturais é um número natural.
Dessa forma, por (i), temos que $m + n = za$, com $z \in \mathbb{N}$.
Portanto, por definição, $a \mid m + n$.

Divisibilidade

Propriedade 4: Se $a \mid m$, então $a \mid mn$.

Ocultar

Ocultar

- Se a divide m, então a divide qualquer múltiplo de m.
- Se a é divisor de m, então a divide todo múltiplo de m.

Se $a \mid m$, então, por definição, existe um número natural k tal que $m = ka$. Então, para qualquer número natural n, temos que $mn = (ka)n = (kn)a$.
Dessa forma, se fizermos $kn = t$, então teremos que $mn = ta$, com $t \in \mathbb{N}$, e isso é suficiente para garantir que $a \mid mn$.

Divisibilidade

Propriedade 5: Se $a \mid m$ e $a \mid n$, então $a \mid xm + yn$, para quaisquer números naturais x e y.

Ocultar

Ocultar

• Se a é divisor de m e de n, então a é divisor da soma entre os produtos xm e yn, para quaisquer números naturais x e y.

Essa justificativa poderia ser feita a partir da definição de divisibilidade, como feito nas propriedades anteriores, mas vamos utilizar as **propriedades 3 e 4** para fazê-la.

Assim, suponhamos que a seja um divisor de m e de n.

Portanto, se x e y são números naturais, então, pela **propriedade 4**, temos que $a \mid xm$ e $a \mid yn$.

Como, agora, temos que $a \mid xm$ e $a \mid yn$, utilizamos a **propriedade 3** para concluir que a é divisor da soma entre xm e yn.

Assim, podemos afirmar que $a \mid xm + yn$, para $x, y \in \mathbb{N}$.

Divisibilidade

Existem algumas propriedades importantes de divisibilidade:
(i) Se $a|b$, então $a \leq b$;
(ii) Se $a|b$ e $a|c$, então $a|b+c$;
(iii) Se $a|b$, então $a|b.c$, para qualquer $c \in Z$;
(iv) Se $a|b$ e $b|c$, então $a|c$;
(v) Se p é um número primo e $p|ab$, com $mdc(a,b) = 1$, então $p|a$ ou $p|b$.

Observações: Juntando as propriedades (ii) e (iii), vemos que se $a|b$ e $a|c$, então $a|bx+cy$, para quaisquer x, $y \in Z$. Alguns problemas sobre divisibilidade vem disfarçados, pois quando se pergunta quando a fração $\frac{a}{b}$ é um inteiro é o mesmo que perguntar quando $a|b$.

Matemática Concreta

Noções sobre Teoria dos Números
Parte 1

Dr. A. Riker
Universidade Federal do Pará (UFPA)
afr@ufpa.br

2021.PL03