Teorema 5.1.6. Sejam a,b,c números inteiros. Então:

(i) se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$;

(ii) se $a \mid b$ então $a \mid bc$ para todo inteiro c;

(iii) se $a \mid b$ e $b \mid c$, então $a \mid c$;

(iv) se $a \mid b$ e $a \mid c$, então $a \mid (bm + cn)$ para todo $m \in \mathbb{Z}$ e para todo $n \in \mathbb{Z}$.

(i) Suponha que $a|b$ e $a|c$. Então, por definição, temos $b = ak$, $k \in \mathbb{Z}$, e $c = ak$, $k \in \mathbb{Z}$.

Cuidado! $b = ak$ e $c = ak$ então $b = c$.

(i) Suponha que $a|b$ e $a|c$. Então, por definição, temos $b = ak$, $k \in \mathbb{Z}$, e $c = al$, $l \in \mathbb{Z}$. Logo,

$$b + c = ak + al = a(k+l) \iff b + c = an,$$

onde $n = k + l \in \mathbb{Z}$. Segue que $a|(b+c)$. $\blacksquare$

Teorema 5.1.7. Sejam a,d números inteiros, $d > 0$. Existem números inteiros únicos q,$r \in \mathbb{Z}$ com $0 \leq r < d$ tais que $a = dq + r$.

Definição 5.1.8. Sejam a,d números inteiros, $d > 0$ e sejam q,$r \in \mathbb{Z}$ tais que $0 \leq r < d$ e $a = dq + r$. Dizemos que q e r são respectivamente o quociente e o resto da divisão de a por d e escrevemos

$$q = a \text{ div } d \quad \text{e} \quad r = a \bmod d.$$

Exemplo 5.1.9. Sejam $a = 14$ e $d = 3$.

Determine q = a div d. Determine r = a mod d.

Temos $14 = 3 \cdot 4 + 2$, logo $q = 14 \text{ div } 3 = 4$ e $r = 14 \bmod 3 = 2$.

$14 \% 3 = 2$

Exemplo 5.1.10. Sejam $a = 30$ e $d = 5$.

Determine q = a div d. Determine r = a mod d.

Temos $30 = 5 \cdot 6 + 0$, logo $q = 30 \text{ div } 5 = 6$ e $r = 30 \bmod 5 = 0$.

Exemplo 5.1.11. Vejamos agora um exemplo envolvendo um inteiro negativo. Considere $a = -21$ e $d = 4$.

Temos $-21 = 4 \cdot (-5) + (-1)$, mas devemos ter $a = dq + r$ com $0 \leq r < d$, então

$$-21 = 4 \cdot (-6) + 3$$

e $-21 \text{ div } 4 = -6$ e $-21 \bmod 4 = 3$.

Definição 5.1.13. Sejam a,b,m inteiros, $m > 0$. Dizemos que a é congruente a b módulo m se $m \mid (a - b)$. Escrevemos nesse caso $a \equiv b \pmod{m}$.

Exercício 5.1.15. Determine se as congruências abaixo são verdadeiras ou falsas.

(i) $15 \equiv 2 \pmod{7}$.

(ii) $20 \equiv 6 \pmod{7}$.

(iii) $20 \equiv -1 \pmod{7}$.

(iv) $32 \equiv 4 \pmod{10}$.

(i) $7 \mid (15-2) \iff 7 \mid 13$, falso.

(ii) $7 \mid (20-6) \iff 7 \mid 14$, verdadeiro.

(iii) $7 \mid (20-(-1)) \iff 7 \mid 21$, verdadeiro.

(iv) $10 \mid (32-4) \iff 10 \mid 28$, falso.

Exercício 5.1.16. Calcule as reduções abaixo sabendo que $\underline{a \mod m}$ deve ser um inteiro entre 0 e $m - 1$.

resto da divisão de a por m

(i) $15 \mod 3$.

(ii) $-4 \mod 5$.

(iii) $22 \mod 10$.

(iv) $-1 \mod 8$.

(i) $15 = 3 \cdot 5 + 0 \Rightarrow 15 \mod 3 = 0$

(ii) $-4 = 5 \cdot (-1) + 1 \Rightarrow -4 \mod 5 = 1$ $\longrightarrow$ $-4 \mod 5 \in \{0, 1, 2, 3, 4\}$.

(iii) $22 = 10 \cdot 2 + 2 \Rightarrow 22 \mod 10 = 2$

(iv) $-1 = 8 \cdot (-1) + 7 \Rightarrow -1 \mod 8 = 7$

Teorema 5.1.14. Sejam a,b,m inteiros, $m > 0$. Então $a \equiv b \pmod{m}$ se e somente se $a \bmod m = b \bmod m$.

restos $r_1 = r_2$ $m \mid (a-b)$

Exemplo. Sejam $a = 20$, $b = 14$ e $m = 6$.

Temos $20 = 6 \cdot 3 + 2$ e $14 = 6 \cdot 2 + 2$, logo $20 \bmod 6 = 2$ e $14 \bmod 6 = 2$. Então $20 \bmod 6 = 14 \bmod 6$ e $20 \equiv 14 \pmod{6}$ pois $6 \mid (20-14)$.

Demonstração.

($\Leftarrow$) Suponha que $a, b, m \in \mathbb{Z}$, $m > 0$, tais que $a \bmod m = b \bmod m$. Devemos provar que $a \equiv b \pmod{m}$.

Temos $a = mq_1 + r_1$ e $b = mq_2 + r_2$, onde $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ e $0 \leq r_1 \leq m-1$, $0 \leq r_2 \leq m-1$. Como $a \bmod m = b \bmod m$, temos $r_1 = r_2$. Devemos provar que $a \equiv b \pmod{m}$, isto é, $m \mid (a-b)$. Segue que

$$a - b = mq_1 + r_1 - (mq_2 + r_2) = mq_1 - mq_2 + \cancel{r_1} - \cancel{r_2}$$

$$\Leftrightarrow a - b = m(q_1 - q_2),$$

isto é, $a - b = mk$, onde $k = q_1 - q_2 \in \mathbb{Z}$. Isto prova que $a \equiv b \pmod{m}$. ∎

Teorema 5.1.14. Sejam a,b,m inteiros, $m > 0$. Então $a \equiv b \pmod m$ se e somente se $a \bmod m = b \bmod m$.

($\Rightarrow$) Temos $a = mq_1 + r_1$ e $b = mq_2 + r_2$, onde $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ e $0 \leq r_1 \leq m-1$, $0 \leq r_2 \leq m-1$. Suponha que $a \equiv b \pmod m$, isto é, $m \mid (a-b)$. Devemos provar que $a \bmod m = b \bmod m$, isto é, $r_1 = r_2$.

Como $m \mid (a-b)$ temos $a-b = mk$, onde $k \in \mathbb{Z}$. Logo,

$$a-b = mk = (mq_1 + r_1) - (mq_2 + r_2),$$

$$a-b = mk = mq_1 - mq_2 + r_1 - r_2,$$

$$a-b = mk = m(q_1 - q_2) + r_1 - r_2,$$

portanto

$$r_1 - r_2 = mk - m(q_1 - q_2) \Leftrightarrow r_1 - r_2 = m(k - q_1 + q_2).$$

Segue que m divide $r_1 - r_2$. Note que, como

$$0 \leq r_1 \leq m-1, \quad 0 \leq r_2 \leq m-1,$$

temos $-(m-1) \leq r_1 - r_2 \leq m-1$, onde $r_1 - r_2$ é múltiplo de m, logo $r_1 - r_2 = 0$ e $r_1 = r_2$, como gostaríamos. ∎

divisões por 5

$0 \leq r_1 \leq 4$

$0 \leq r_2 \leq 4$ e $r_1 - r_2$ é múltiplo de 5 $\Rightarrow r_1 - r_2 = 0$

$-4 \leq r_1 - r_2 \leq 4$

Teorema 5.1.17. Seja m um inteiro positivo. Dois números inteiros a e b satisfazem $a \equiv b \pmod{m}$ se e somente se $a = b + km$ para algum inteiro k.

$m | (a-b)$

Teorema 5.1.18. Sejam m um inteiro positivo e a,b inteiros tais que $a \equiv b \pmod{m}$. Se $c \equiv d \pmod{m}$ então

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ac \equiv bd \pmod{m}$.

$a \equiv b \pmod{7}$ $\quad$ $c \equiv d \pmod{7}$

Sejam $m = 7$, $a = 23$, $b = 2$, $c = 90$, $d = 6$.

(i) $23 + 90 \equiv 2 + 6 \pmod{7}$

(ii) $23 - 90 \equiv 2 - 6 \pmod{7}$

(iii) $23 \cdot 90 \equiv 2 \cdot 6 \pmod{7}$

Corolário 5.1.19. Seja m um inteiro positivo. Se $a \equiv b \pmod{m}$ e $c \in \mathbb{Z}$, então

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Corolário 5.1.20. Seja m um inteiro positivo. Sejam A,B números inteiros e sejam $a = A \bmod m$ e $b = B \bmod m$. Então

(i) $A + B \equiv a + b \pmod{m}$,

(ii) $A - B \equiv a - b \pmod{m}$,

(iii) $AB \equiv ab \pmod{m}$.

Definição 5.2.1. Seja p um número inteiro maior que 1. Dizemos que p é *número primo* se os únicos inteiros que dividem p são 1 e p. Se n é um inteiro positivo maior que 1 e n não é primo, dizemos que n é um *número composto*.

Exercício 5.2.2. Determine se os números abaixo são primos ou compostos.

(i) $n = 8$

(ii) $n = 7$

(iii) $n = 11$

(iv) $n = 12$

(i) $n=8$ é composto pois $2|8$.

(ii) $n=7$ é primo.

(iii) $n=11$ é primo.

(iv) $n=12$ é composto pois $2|6$.

Teorema 5.2.3 (Teorema Fundamental da Aritmética). Todo número inteiro positivo $n > 1$ pode ser escrito como um número primo ou como o produto de dois ou mais número primos. Além disso, n é escrito como produto de números primos de maneira única a menos da ordem em que os números primos no produto.

Exemplo: Número inteiro composto.

$n = 12$ é composto: temos $12 = 2 \cdot 2 \cdot 3$.

Exemplo: Número inteiro primo.

$n = 7$ é primo.

Podemos enunciar o Teorema Fundamental da Aritmética de uma maneira equivalente: todo número inteiro positivo n pode ser escrito como

$$n = p_1^{l_1} \cdot p_2^{l_2} \cdots p_s^{l_s},$$

onde $p_1, p_2, \ldots, p_s$ são primos e $l_1 \geq 1, l_2 \geq 1, \ldots, l_s \geq 1$.

$$n = 12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3^1$$

Teorema 5.2.6. Seja n um número inteiro. Se n é um número composto, então existe um fator primo de n menor ou igual a $\sqrt{n}$.

Seja n um inteiro composto. Então pelo Teorema 5.2.3 sabemos que $n = p_1 \cdot p_2 \cdots p_s$, onde $p_1, p_2, \ldots, p_s$ são números primos. Suponha, por contradição, que todos os fatores primos de n são maiores que $\sqrt{n}$, isto é, $p_1 > \sqrt{n}, p_2 > \sqrt{n}, \ldots, p_s > \sqrt{n}$. Então $p_1 \cdot p_2 \cdots p_s > \sqrt{n} \cdot \sqrt{n} \cdots \sqrt{n} > n$, logo

$n = p_1 \cdots p_s > n$, um absurdo. Segue que a hipótese $p_1 > \sqrt{n}, p_2 > \sqrt{n}, \ldots, p_s > \sqrt{n}$ é falsa e portanto existe $p_i \leq \sqrt{n}$ para algum $1 \leq i \leq s$. ■

Teorema 5.2.6. Seja n um número inteiro. Se n é um número composto, então existe um fator primo de n menor ou igual a $\sqrt{n}$.

p

q

Sabemos que $p \to q$ é equivalente a $\sim q \to \sim p$.

Corolário 5.2.7. Seja n um número inteiro. Se não existe um fator primo de n menor ou igual a $\sqrt{n}$, então n é um número primo.

Exemplo 5.2.8. Prove que 97 é primo.

Usar o Corolário 5.2.7 com $n = 97$.

Temos $\sqrt{81} = 9$ e $\sqrt{100} = 10$, logo $9 < \sqrt{97} < 10$. Verificamos os primos 2, 3, 5, 7:

- $97 \bmod 2 = 1$,
- $97 \bmod 3 = 1$,
- $97 \bmod 5 = 2$,
- $97 \bmod 7 = 6$.

Como 97 não é divisível por $p = 2, 3, 5$ ou 7, temos que 97 é primo.

Podemos utilizar a fatoração em números primos para encontrar os divisores de um número. Seja n um número inteiro positivo e seja $n = p_1^{e_1} \cdots p_s^{e_s}$ a sua fatoração em números primos. Podemos escrever os divisores de n como

$$n = p_1^{\ell_1} \cdots p_s^{\ell_s},$$

onde $0 \leq \ell_1 \leq e_1, \ldots, 0 \leq \ell_s \leq e_s$.

Exemplo 5.2.9. Considere o número inteiro $n = 18$. A fatoração de n em números primos é

Temos $n = 18 = 2^1 \cdot 3^2$, então os divisores de 18 são

$2^0 \cdot 3^0 = 1$, $\quad 2^0 \cdot 3^1 = 3$, $\quad 2^0 \cdot 3^2 = 9$,

$2^1 \cdot 3^0 = 2$, $\quad 2^1 \cdot 3^1 = 6$, $\quad 2^1 \cdot 3^2 = 18$.

Teorema 5.2.10. Existem infinitos números primos.

Suponha, por contradição, que existe um número finito de primos e sejam eles $p_1, p_2, \ldots, p_s$. Considere o número $n = p_1 p_2 p_3 \cdots p_s + 1$.

Note que se n for composto então $p_i | n$ para algum primo $p_i \in \{p_1, \ldots, p_s\}$. Então

$p_i | n$ e $p_i | p_1 \cdots p_s$, logo $p_i | (n - p_1 \cdots p_s) \iff p_i | 1$, impossível pois p_i é primo. Então n não é divisível por nenhum número primo, logo n é primo. Mas $n \neq p_i$ para todo i, uma contradição. Concluímos que existe um número infinito de primos. ∎

Definição 5.3.1. Sejam a,b números inteiros não-nulos. O maior número inteiro d tal que $d \mid a$ e $d \mid b$ é dito o *máximo divisor comum* de a e b; escrevemos $d = \mathrm{mdc}(a,b)$.

Exemplo 5.3.2. Sejam $a = 12$ e $b = 15$.

Divisores de a: $\{1, 2, 3, 4, 6, 12\}$.

Divisores de b: $\{1, 3, 5, 15\}$.

$\Rightarrow \mathrm{mdc}(12, 15) = 3$.

Exemplo 5.3.3. Considere os números inteiros $a = 18$ e $b = 54$.

Divisores de a: $\{1, 2, 3, 6, 9, 18\}$.

Divisores de b: $\{1, 2, 3, 6, 9, 18, 27, 54\}$.

$\Rightarrow \mathrm{mdc}(18, 54) = 18$, pois 18 divide 54.

O máximo divisor comum de dois inteiros pode ser encontrado utilizando o método do Exemplo 5.2.9: fatoramos os inteiros em números primos e escolhemos, para cada númer primo, o menor expoente que aparece na fatoração de um deles. Mais precisamente, se

$$a = p_1^{e_1} \cdots p_s^{e_s} \quad \text{e} \quad b = p_1^{f_1} \cdots p_s^{f_s},$$

então

$$\text{mdc}(a,b) = p_1^{l_1} \cdots p_s^{l_s} \quad \text{onde } l_i = \min\{e_i, f_i\},$$

para $i = 1, \ldots, s$.

Exemplo 5.3.4. Sejam $a = 50$ e $b = 30$.

Temos $a = 2 \cdot 5^2$ e $b = 2 \cdot 3 \cdot 5$, então escrevemos

$$a = 2^1 \cdot 3^0 \cdot 5^2 \quad \text{e} \quad b = 2^1 \cdot 3^1 \cdot 5^1$$

e concluímos que $\text{mdc}(50,30) = 2^1 \cdot 3^0 \cdot 5^1 = 10$.

Definição 5.3.5. Sejam a,b números inteiros não-nulos. Se $\text{mdc}(a,b) = 1$ dizemos que a e b são *relativamente primos* ou *primos entre si.*

Definição 5.3.6. Dizemos que números inteiros $a_1, a_2, \ldots, a_n$ são *pares relativamente primos* ou *primos entre si dois a dois* se $\text{mdc}(a_i, a_j) = 1$ para todo i,j tal que $1 \leq i < j \leq n$.

Exemplo 5.3.7. Sejam $a_1 = 5$, $a_2 = 4$ e $a_3 = 6$.

5 e 4 são relativamente primos pois $\text{mdc}(4,5) = 1$.

4 e 6 não são relativamente primos pois $\text{mdc}(4,6) = 2$.

Definição 5.3.8. Sejam a,b números inteiros positivos. O menor inteiro positivo M que é múltiplo de a e b é dito o *mínimo múltiplo comum* de a e b; escrevemos $M = \text{mmc}(a,b)$.

O mínimo múltiplo comum de dois inteiros pode ser determinado como no Exemplo 5.3.4, mas para o mmc escolhemos o maior expoente que aparece na fatoração de cada inteiro.

Exemplo 5.3.9. Sejam $a = 50$ e $b = 30$. Vimos no Exemplo 5.3.4

Temos $a = 2 \cdot 5^2$ e $b = 2 \cdot 3 \cdot 5$, então escrevemos

$$a = 2^1 \cdot 3^0 \cdot 5^2 \quad \text{e} \quad b = 2^1 \cdot 3^1 \cdot 5^1$$

e concluímos que $\text{mmc}(50,30) = 2^1 \cdot 3^1 \cdot 5^2 = 150$

Teorema 5.3.10. Sejam a,b números inteiros positivos. Então $ab = \text{mdc}(a,b) \cdot \text{mmc}(a,b)$.

Indução

A *indução matemática* é uma forma de argumento para fornecer demonstrações de teoremas que são válidos para números inteiros. Considere uma declaração da forma $\forall n P(n)$, onde o domínio de discurso é o conjunto dos números inteiros positivos $\{1,2,3,\ldots\}$. A demonstração de um tal teorema por indução matemática tem duas partes:

(i) demonstração de que $P(\cdot)$ é verdadeira para o menor inteiro do conjunto, nesse caso $P(1)$;

(ii) demonstração de que $P(k) \rightarrow P(k+1)$ para todo inteiro positivo k.

O item (i) acima é chamado de *passo base* e o item (ii) é chamado de *passo de indução.*

Vejamos agora por que estes dois passos provam que $\forall n P(n)$ é verdadeira. $n \in \{1, 2, \ldots\}$

Para, por exemplo $n = 5$, temos

$P(1) \Rightarrow P(1)$ é verdadeiro

$k = 1 \Rightarrow$

Exemplo 6.1.1. Forneça uma demonstração por indução matemática do teorema a seguir: se n é um inteiro positivo, então

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}. \tag{6.2}$$

Seja $P(n)$ a afirmação $1+2+3+\cdots+n = \frac{n(n+1)}{2}$.

O domínio do teorema é o conjunto

(i) demonstração de que $P(\cdot)$ é verdadeira para o menor inteiro do conjunto, nesse caso $P(1)$;

(ii) demonstração de que $P(k) \to P(k+1)$ para todo inteiro positivo k.

(i) Passo base: para $n =$

(ii) Passo de indução. Devemos provar que $P(k) \to P(k+1)$ para todo $k \geq 1$. Supomos que $P(k)$ é verdadeiro:

Devemos provar que $P(k+1)$ é verdadeiro:

Temos

Exemplo 6.1.2. Prove que, para n um inteiro positivo,

$$1 + 3 + \cdots + (2n - 1) = n^2. \tag{6.5}$$

Exemplo 6.1.3. Sejam a,r números reais, $r \neq 1$. Prove a fórmula para a soma de um número finito dos termos de uma progressão geométrica: para $n \geq 0$ temos

$$\sum_{j=0}^{n} ar^j = \overset{a}{\cancel{1}} + ar + ar^2 + \cdots + ar^n = a\frac{r^{n+1} - 1}{r - 1}. \tag{6.6}$$

Exemplo 6.1.5. Prove que $n^3 - n$ é divisível por 3 para todo inteiro positivo n.

Exemplo 6.1.4. Prove que $n < 2^n$ para todo inteiro n positivo.

Exemplo 6.1.2. Prove que, para n um inteiro positivo,

$$1 + 3 + \cdots + (2n - 1) = n^2. \tag{6.5}$$

Seja $P(n)$ a afirmação

O domínio do teorema é o conjunto

(i) demonstração de que $P(\cdot)$ é verdadeira para o menor inteiro do conjunto, nesse caso $P(1)$;

(ii) demonstração de que $P(k) \to P(k+1)$ para todo inteiro positivo k.

(i) Passo base: para $n =$

(ii) Passo de indução. Devemos provar que $P(k) \to P(k+1)$ para todo $k \geq 1$. Supomos que $P(k)$ é verdadeiro:

Devemos provar que $P(k+1)$ é verdadeiro:

Temos

Exemplo 6.1.3. Sejam a,r números reais, $r \neq 1$. Prove a fórmula para a soma de um número finito dos termos de uma progressão geométrica: para $n \geq 0$ temos

$$\sum_{j=0}^{n} ar^j = \overset{a}{\cancel{1}} + ar + ar^2 + \cdots + ar^n = a\frac{r^{n+1}-1}{r-1}. \tag{6.6}$$

Seja $P(n)$ a afirmação

O domínio do teorema é o conjunto

(i) demonstração de que $P(\cdot)$ é verdadeira para o menor inteiro do conjunto, nesse caso $P(1)$;

(ii) demonstração de que $P(k) \to P(k+1)$ para todo inteiro positivo k.

(i) Passo base: para $n =$

(ii) Passo de indução. Devemos provar que $P(k) \to P(k+1)$ para todo $k \geq 1$. Supomos que $P(k)$ é verdadeiro:

⋮

Devemos provar que $P(k+1)$ é verdadeiro: