DIVISORES, DIVISÃO E AFINS

MARCELO DIAS PASSOS

1. Divisores

Definição 1. *Sejam $a, b \in \mathbb{Z}$. Diremos que a **divide** b se, e somente se, existe $x \in \mathbb{Z}$ tal que $ax = b$. Neste caso, escreveremos $a|b$. Também falaremos: a é divisor de b, b é múltiplo de a ou b é divisível por a.*

Observamos imediatamente que todo inteiro é divisor de 0 e que 1 é divisor de todo inteiro.

Proposição 1. *A relação $|$ é reflexiva e transitiva.*

Demonstração. Para todo $x \in \mathbb{Z}$, $x|x$. Logo $|$ é relação reflexiva. Agora tomemos $x, y, z \in \mathbb{Z}$ tais que $x|y$ e $y|z$. Daí, existem $u, v \in \mathbb{Z}$ tais que $xu = y$ e $yv = z$. Logo $z = x(uv)$ e $x|z$. Provamos que $|$ é relação transitiva. □

Visto que $1|-1$ e $-1|1$, temos que $|$ **não** é antissimétrica (em $\mathbb{Z}$). Uma relação reflexiva e transitiva é chamada de **pré-ordem**. Portanto, $|$ é uma pré-ordem em $\mathbb{Z}$.

Para $a \in \mathbb{Z}$, temos que $a|-a$, $-a|a$, $a\big||a|$ e $|a|\big|a$. Para $a, b \in \mathbb{Z}$,

$$a|b \Leftrightarrow -a|b \Leftrightarrow a|-b \Leftrightarrow |a|\Big||b| \ .$$

Proposição 2. *Sejam $a, b \in \mathbb{N}$. Então $a|b$ se, e somente se, existe $x \in \mathbb{N}$ tal que $ax = b$.*

Demonstração. Caso $a = 0$, temos que $a|b$ se, e somente se, $b = 0$. Daí $a \cdot 1 = b$. Vamos supor que $a \neq 0$.

Suponhamos que $a|b$. Daí existe $x \in \mathbb{Z}$ tal que $ax = b$. Como $a > 0$, se $x < 0$, teríamos que $b = ax < 0$, um absurdo. Logo $x \in \mathbb{N}$. A recíproca é trivialmente verdadeira. □

Portanto, números naturais são divisíveis em $\mathbb{Z}$ se, e somente se, já o eram em $\mathbb{N}$.

Proposição 3. *Sejam $a, b \in \mathbb{Z}$. Então $a|b$ e $b|a$ se, e somente se, $|a| = |b|$.*

Demonstração. Se $|b| = |a|$, temos, pelo fatos já demonstrados, que $a|b$ e $b|a$.

Agora suponhamos que $a|b$ e $b|a$. Então $|a|\big||b|$ e $|b|\big||a|$. Como $|$ é antissimétrica em $\mathbb{N}$, $|b| = |a|$. □

Proposição 4. *Para $a, b, c \in \mathbb{Z}$, temos:*

(1) $a|ac$
(2) se $a|b$, então $ac|bc$,
(3) se $c \neq 0$ e $ac|bc$, então $a|b$, e
(4) se $a|b$ e $a|c$, então $a|b + c$.

Demonstração. (1) Pela definição.
(2) Se $a|b$, $ax = b$ para algum $x \in \mathbb{Z}$. Daí, $acx = bc$ e $ac|bc$.
(3) Suponhamos que $acx = bc$, para algum $x \in \mathbb{Z}$, e que $c \neq 0$. Como $\mathbb{Z}$ é domínio de integridade, $ax = b$ e $a|b$.
(4) Se $a|b$ e $a|c$, existem $x, y \in \mathbb{Z}$ tais que $ax = b$ e $ay = c$. Daí $b + c = a(x + y)$ e $a|b + c$.

□

Date: julho/agosto de 2013.

Proposição 5. *Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$ e $a|b$. Então $|a| \leq |b|$.*

Demonstração. Dado que $a|b$, temos que $|a||b|$ e existe $x \in \mathbb{N}$ tal que $|a|x = |b|$. Como $b \neq 0$, $x \neq 0$. Daí $|a| \leq |a|x = |b|$, pois $1 \leq x$. □

Para $x \in \mathbb{Z}$, sejam $D(x) = \{n \in \mathbb{Z} \colon n|x\}$ e $D^+(x) = \{n \in \mathbb{N} \colon n|x\}$.

Proposição 6. *Para $x \in \mathbb{Z}$, $D(x) = D(|x|)$. Se $x \neq 0$, $D(x)$ é limitado superiormente e inferiormente, e $\min D(x) = -|x|$ e $\max D(x) = |x|$.*

Demonstração. Por discussões anteriores, temos que $D(x) = D(|x|)$. Suponhamos $x \neq 0$ e fixemos $a \in D(x)$. Logo, pela proposição anterior, $|a| \leq |x|$, ou equivalentemente, $-|x| \leq a \leq |x|$. Como $-|x|, |x| \in D(x)$, temos que $\min D(x) = -|x|$ e $\max D(x) = |x|$. □

Dadas as propriedades dos inteiros que o fazem um anel e o fato que sua ordem (habitual) é compatível com a estrutura algébrica de $\mathbb{Z}$, muito pode ser definido e demonstrado para esses números.

2. Divisão Euclidiana

Definição 2. *Para $a \in \mathbb{Z}$, definimos $a\mathbb{Z} = \{x \in \mathbb{Z} \colon a|x\} = \{ay \colon y \in \mathbb{Z}\}$.*

Para $n \in \mathbb{Z}$, $n\mathbb{Z}$ é o conjunto dos múltiplos de n. Sendo assim, $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = (-1)\mathbb{Z} = \mathbb{Z}$, e para $n \in \mathbb{Z}$, $n\mathbb{Z} = (-n)\mathbb{Z} = |n|\mathbb{Z}$.

Proposição 7. *Para $a, b \in \mathbb{Z}$,*

(1) $a|b \quad \Leftrightarrow \quad b\mathbb{Z} \subseteq a\mathbb{Z}$, *e* *(2)* $a\mathbb{Z} = b\mathbb{Z} \quad \Leftrightarrow \quad |a| = |b|$.

Demonstração. (1) Suponhamos $a|b$ e seja $x \in b\mathbb{Z}$. Daí $b|x$. Como $|$ é transitiva, $a|x$ e $x \in a\mathbb{Z}$. Logo $b\mathbb{Z} \subseteq a\mathbb{Z}$. Agora, suponhamos $b\mathbb{Z} \subseteq a\mathbb{Z}$. Como $b \in b\mathbb{Z}$, $b \in a\mathbb{Z}$ e $a|b$.
(2) Imediato do item anterior e da proposição 3.

□

Proposição 8. *Para $n \in \mathbb{Z}^*$, $n\mathbb{Z}$ não é limitado superiormente nem inferiormente.*

Demonstração. Seja $k = |n|$ e temos que $1 \leq k$ e que $n\mathbb{Z} = k\mathbb{Z}$. Suponhamos que $k\mathbb{Z}$ seja limitado superiormente. Por resultado anterior, $k\mathbb{Z}$ admite máximo m. Sendo assim, $m = kx$, para algum $x \in \mathbb{Z}$. Sendo assim, $k(x+1) = kx + k = m + k \in k\mathbb{Z}$ e $k(x+1) > m$, um absurdo pois $m = \max k\mathbb{Z}$.

Agora tomemos $y \in \mathbb{Z}$. Como $n\mathbb{Z}$ não é limitado superiormente, existe $a \in n\mathbb{Z}$ tal que $-y < a$. Logo $-a < y$ e $-a \in n\mathbb{Z}$. Logo $n\mathbb{Z}$ não admite limitante inferior. □

A proposição anterior vai nos ajudar a demonstrar o teorema a seguir.

Teorema 9 (Divisão Euclidiana)**.** *Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$. Existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = bq + r \qquad e \qquad 0 \leq r < |b|.$$

Demonstração. Como $b \neq 0$, $b\mathbb{Z}$ é ilimitado inferiormente e superiormente. Logo $S = \{x \in b\mathbb{Z} \colon x \leq a\}$ é não vazio e limitado superiormente. Seja $m = \max S$. Como $m \in S$, $m \leq a$ e existe $r \in \mathbb{N}$ tal que $m + r = a$. Como $m \in b\mathbb{Z}$, $m = bq$, para algum $q \in \mathbb{Z}$.

Dado que $b\mathbb{Z} = |b|\mathbb{Z}$, $m = |b|q'$, para algum $q' \in \mathbb{Z}$. Dado que $q' < q' + 1$ e $0 < |b|$, temos que $m = |b|q < |b|(q' + 1)$ e $|b|(q' + 1) \in b\mathbb{Z}$. Logo $|b|(q' + 1) \notin S$ e $a < |b|(q' + 1)$. Sendo assim,

$$m + r = a < |b|(q' + 1) = |b|q' + |b| = m + |b|.$$

Logo $r < |b|$. Daí $a = bq + r$ e $0 \leq r < |b|$.

Suponhamos agora que $a = bu + v$, onde $0 \leq v < |b|$. Como bu e bq são comparáveis, podemos supor, sem perda de generalidade, que $bu \leq bq$. Daí $bq - bu \in \mathbb{N} \cap b\mathbb{Z}$. Também $bq - bu \in |b|\mathbb{Z}$ e $bq - bu = |b|t$, para algum $t \in \mathbb{N}$. Como $a = bq + r = bu + r$, temos que $v = bq - bu + r = |b|t + r$. Observamos que r, v, $|b|$ e t são todos números naturais. Seja $y = |b|t + v$. Pela divisão euclidiana em $\mathbb{N}$, temos que, na divisão de y por $|b|$, o quociente é t e o resto v Mas ao mesmo tempo $y = r \in \mathbb{N}$ e $r < |b|$, ou seja, na divisão de y por $|b|$, o quociente é 0 e o resto r. Sendo assim, $t = 0$ e $r = v$. Logo $q = u$, pois $b \neq 0$. □

Definição 3. *Os números q e r, estabelecidos no teorema anterior, são chamados de **quociente** e **resto** da divisão euclidiana de a por b.*

Observamos que a divisão (euclidiana) em $\mathbb{Z}$ estende a divisão de $\mathbb{N}$. Aliás, os exemplos a seguir vão mostrar como usar a divisão de $\mathbb{N}$ para determinar o quociente e o resto da divisão de $\mathbb{Z}$.

Exemplo 1. *Qual o quociente da divisão de 120 por -14? Temos que $120 = 14 \cdot 8 + 8$. Sendo assim, $120 = (-14) \cdot (-8) + 8$. Uma vez que $8 < 14 = |-14|$, temos que, na divisão pedida, o quociente é -8 e o resto é 8.*

Exemplo 2. *Qual o quociente da divisão de -120 por 14? Temos que $120 = 14 \cdot 8 + 8$. Sendo assim, $-120 = 14 \cdot (-8) - 8$. Observamos que -8 não pode resto dessa divisão, pois **não** é número natural. Por outro lado, podemos adicionar e subtrair 14 à expressão e obtemos*

$$-120 = 14 \cdot (-8) - 14 + 14 - 8 = 14 \cdot (-9) + 6.$$

Dado que $6 < 14$, o quociente é -9 e o resto é 6.

Exemplo 3. *Seja $a \in \mathbb{Z}$ que não é divisível por 3. Vejamos que a^2 tem resto 1 na divisão por 3. De fato, como $3 \nmid a$, $a = 3q + r$, onde $r \in \{1, 2\}$. Sendo assim,*

$$a^2 = (3q + r)^2 = 9q^2 + 6qr + r^2 = 3(3q^2 + 2qr) + r^2 \ .$$

Se $r = 1$, $a^2 = 3(3q^2 + 2qr) + 1$ e o resto da divisão por 3 é 1. Se $r = 2$, $a^2 = 3(3q^2 + 2qr) + 4 = 3(3q^2 + 2qr + 1) + 1$ e o resto da divisão por 3 também é 1.

Exercício 1. *Mostre, para $n \in \mathbb{Z}$, que n é par se, e somente se, n^2 é par.*

Exercício 2. *Mostre que $n(n + 1)$ é sempre par, para qualquer $n \in \mathbb{Z}$.*

Exercício 3. *Para $n \in \mathbb{Z}$, mostre que, se n é ímpar, então $8|n^2 - 1$.*

Exercício 4. *Mostre que, se a e b são inteiros e $a^2 + b^2$ é divisível por 3, então a e b são divisíveis por 3.*

Exercício 5. *Mostre que, se a e b são ambos ímpares, então $a^2 + b^2$ é divisível é par mas não é divisível por 4.*

Exercício 6. *Seja N um inteiro. Prove que N^2 dividido por 6 nunca deixa resto 2.*

Exercício 7. *Ache o quociente e o resto das divisões:*

(1) de 27 por 5 *(3) de -140 por -11* *(5) de -27 por -5* *(7) de -20390 por 25*
(2) de 38 por -7 *(4) de -14308 por 7* *(6) de 2013 por -12* *(8) de 143061 por 8*

Exercício 8. *O resto da divisão do inteiro N por 20 é 8. Qual é o resto da divisão de N por 5?*

Exercício 9. *Sejam $a, n \in \mathbb{N}$.*

(1) Mostre que existe $m \in \mathbb{N}$ tal que $(a+1)^n = ma + 1$.
(2) Mostre que, se $a > 1$, então existe $m \in \mathbb{N}$ tal que $(a-1)^{2n} = ma + 1$.
(3) Mostre que, se $a > 0$, então existe $m \in \mathbb{N}$ tal que $(a-1)^{2n+1} = ma - 1$.

Exercício 10. *Seja $n \in \mathbb{N}^*$. Mostre que o quadrado do produto de todos os divisores positivos de n é n^s, onde s é o número de divisores positivos de n.*

3. Subgrupos de $\mathbb{Z}$

Definição 4. *Seja $H \subseteq \mathbb{Z}$. Dizemos que H **é subgrupo** de $\mathbb{Z}$ se, e somente se:*

(1) $0 \in H$,
(2) $x + y \in H$, sempre que $x, y \in H$, e
(3) $-x \in H$, sempre que $x \in H$.

Neste caso, escreveremos $H \leq \mathbb{Z}$.

Observamos que $\{0\} \leq \mathbb{Z}$ e $\mathbb{Z} \leq \mathbb{Z}$. Vejamos que outros subconjuntos de $\mathbb{Z}$ são subgrupos de $\mathbb{Z}$.

Teorema 10. *Seja $n \in \mathbb{Z}$. Então $n\mathbb{Z} = \{nx \colon n \in \mathbb{Z}\} \leq \mathbb{Z}$.*

Demonstração. Temos que $0 = 0n$ e $0 \in n\mathbb{Z}$. Dados $a, b \in n\mathbb{Z}$, temos que $a = nx$ e $b = ny$, para $x, y \in \mathbb{Z}$. Logo $a + b = nx + ny = n(x + y) \in n\mathbb{Z}$. Ainda, se $x \in \mathbb{Z}$, $-(nx) = n(-x) \in n\mathbb{Z}$. Logo $n\mathbb{Z} \leq \mathbb{Z}$. □

Portanto $\{0\} = 0\mathbb{Z}$ e $1\mathbb{Z} = (-1)\mathbb{Z} = \mathbb{Z}$. Ainda, para $n \in \mathbb{Z}$, $n\mathbb{Z} = (-n)\mathbb{Z} = |n|\mathbb{Z}$. Demonstraremos resultados que provaram que esses são os únicos subgrupos de $\mathbb{Z}$.

Proposição 11. *Seja $H \leq \mathbb{Z}$. Então $nx \in H$, sempre que $n \in \mathbb{Z}$ e $x \in H$.*

Demonstração. Fixemos $x \in H$. Seja $I = \{n \in \mathbb{N} \colon nx \in H\}$. Como $0 \in H$, temos que $0 \in I$. Se $n \in I$, temos que $nx \in H$. Logo $(n+1)x = nx + x \in H$, pois $H \leq \mathbb{Z}$. Portanto $n + 1 \in I$. Pelo Princípio da Indução, temos que $I = \mathbb{N}$.

Tomemos $n \in \mathbb{N}$. Pelo demonstrado no parágrafo anterior, $nx \in H$. Sendo assim, $-nx = (-n)x \in H$. Concluímos que $mx \in H$, para qualquer $m \in \mathbb{Z}$. □

Corolário 12. *Se $H \leq \mathbb{Z}$, então $H = \mathbb{Z}$ se, e somente se, $1 \in H$ (ou $-1 \in H$).* □

O próximo resultado vai dar condição equivalente para que algum subconjunto não vazio seja subgrupo.

Proposição 13. *Seja $H \subseteq \mathbb{Z}$, não vazio. São equuivalentes:*

(1) H é subgrupo de $\mathbb{Z}$
(2) $x - y \in H$, sempre que $x, y \in H$.

Demonstração. Suponhamos que $H \leq \mathbb{Z}$ e sejam $x, y \in H$. Logo $-y \in H$ e $x - y = x + (-y) \in H$.

Agora provemos a recíproca. Suponhamos que $x - y \in H$, sempre $x, y \in H$. Dado que $H \neq \emptyset$, podemos fixar $z \in H$. Daí, $0 = z - z \in H$. Dado $x \in H$, temos que $-x = 0 - x \in H$. Dados $a, b \in H$, temos que $a + b = a - (-b) \in H$, pois que $-b \in H$. Sendo assim, $H \leq \mathbb{Z}$. □

Agora podemos demonstrar o próximo resultado.

Proposição 14. *Seja $H \leq \mathbb{Z}$. Então existe um único $n \in \mathbb{N}$ tal que $H = n\mathbb{Z}$.*

Demonstração. Caso $H = \{0\}$, temos que $H = 0\mathbb{Z}$. Suponhamos que $H \neq \{0\}$. Se $m \in H$, $|m| \in H$, pois que H é subgrupo. Logo $I = \{i \in H : i > 0\} \neq \emptyset$. Seja $n = \min I$.

Dado que $n \in H$, temos que $n\mathbb{Z} \subseteq H$, pela proposição 11. Agora tomemos $x \in H$. Como $n \neq 0$, pela divisão euclidiana, existem $q, r \in \mathbb{Z}$, tais que $x = nq + r$ e $0 \leq r < n$. Obsevamos que $r = x - nq$. Dado que $n\mathbb{Z} \subseteq H$, $x, nq \in H$ e $r \in H$. Caso $r > 0$, teríamos $r \in I$ e $r < \min I$, um absurdo. Logo $r = 0$ e $x = nq \in n\mathbb{Z}$.

Caso $n\mathbb{Z} = n'\mathbb{Z}$, para $n, n' \in \mathbb{N}$, temos que $n|n'$ e $n'|n$, o que só é possível se $n = n'$, por serem naturais. □

Definição 5. *Seja $H \leq \mathbb{Z}$. O natural determinado pelo teorema 14 é chamado de* ***gerador (natural) de*** *H.*

Proposição 15. *Sejam H e K subgrupos de $\mathbb{Z}$. Então $H + K = \{h + k : h \in H \wedge k \in K\}$. Também $H \cap K \leq \mathbb{Z}$.*

Demonstração. Uma vez que $0 \in H \cap K$, temos que $H \cup K \subseteq H + K$, logo $H + K \neq \emptyset$. Fixemos $x, y \in H + K$. Daí existem $h_1, h_2 \in H$ e $k_1, k_2 \in K$ tais que $x = h_1 + k_1$ e $y = h_2 + k_2$. Logo $x - y = (h_1 + k_1) - (h_2 + k_2) = (h_1 - h_2) + (k_1 - k_2) \in H + K$, dado que $h_1 - h_2 \in H$ e $k_1 - k_2 \in K$. Concluímos que $H + K \leq \mathbb{Z}$.

Já temos que $0 \in H \cap K$. Fixemos $x, y \in H \cap K$. Como $H \leq \mathbb{Z}$, temos que $x - y \in H$. Analogamente, $x - y \in K$. Logo $x - y \in H \cap K$. Concluímos que $H \cap K \leq \mathbb{Z}$. □

Corolário 16. *Nas mesmas condições da proposição anterior, $H + K$ é o menor subgrupo de $\mathbb{Z}$ que cobre H e K.*

Demonstração. Da fato, como $0 \in K$, temos que $h = h + 0 \in H + K$, para todo $h \in H$. Logo $H \subseteq H + K$. Analogamente $K \subseteq H + K$. Agora suponhamos que $J \leq \mathbb{Z}$ e $H \cup K \subseteq J$. Para $h \in H$ e $k \in K$ temos que $h, k \in J \leq \mathbb{Z}$, logo $h + k \in J$. Sendo assim, $H + K \subseteq J$. □

A construção da soma de subgrupos dá alternativa de como "cobrir" dois subgrupos, uma vez que a união de dois subgrupos quaisquer não é sempre subgrupo. Exemplo disso é $S = 2\mathbb{Z} \cup 3\mathbb{Z}$. Temos que $2, 3 \in S$ mas $5 = 2 + 3 \notin S$.

4. Máximo Divisor Comum

Dados $a, b \in \mathbb{Z}$, observamos que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ para um único $c \in \mathbb{N}$. Como $a \in a\mathbb{Z} \subseteq c\mathbb{Z}$, temos que $c|a$. Analogamente, $c|b$. Portanto é c **divisor comum**. Agora tomemos $d \in \mathbb{N}$, divisor comum a a e b. Como $c = ax + by$, algum $x, y \in \mathbb{Z}$, temos que $d|c$. Como a relação "|" é relação de ordem em $\mathbb{N}$, temos que c é o **"maior"** entre os divisores naturais comuns a a e b.

Definição 6. *Dados $a, b \in \mathbb{Z}$, o gerador de $a\mathbb{Z} + b\mathbb{Z}$ é chamado de* ***máximo divisor comum de*** *a **e** b, e será denotado por* $\mathrm{mdc}(a, b)$.

Vejamos algumas propriedades que ajudam no cálculo do máximo divisor comum de dois inteiros.

Teorema 17. *Sejam $a, b \in \mathbb{Z}$. Então:*

(1) $\mathrm{mdc}(a, b) = \mathrm{mdc}(|a|, |b|) = \mathrm{mdc}(b, a)$,

(2) $\mathrm{mdc}(a, 1) = 1$,

(3) $\mathrm{mdc}(a,b) = 0$ *se, e somente se,* $a = b = 0$*, e*
(4) $\mathrm{mdc}(a,b) = |a|$ *se, e somente se,* $a|b$*.*

Demonstração. (1) Observamos que $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + a\mathbb{Z} = |a|\mathbb{Z} + |b|\mathbb{Z}$.
(2) Temos que $a\mathbb{Z} + 1\mathbb{Z} = 1\mathbb{Z}$.
(3) Temos que $0\mathbb{Z} + 0\mathbb{Z} = \{0\} = 0\mathbb{Z}$. Logo $\mathrm{mdc}(0,0) = 0$. Por outro lado, se $\mathrm{mdc}(a,b) = 0$, $a, b \in a\mathbb{Z} + b\mathbb{Z} = 0\mathbb{Z} = \{0\}$. Logo $a = b = 0$.
(4) Observamos que

$$a\mathbb{Z} + b\mathbb{Z} = |a|\mathbb{Z} \Leftrightarrow b\mathbb{Z} \subseteq a\mathbb{Z} \Leftrightarrow a|b \ .$$

□

Proposição 18. *Sejam* $a, b \in \mathbb{Z}$*. Então* $D(\mathrm{mdc}(a,b)) = D(a) \cap D(b)$ *e, se* $a \neq 0$ *ou* $b \neq 0$*, então* $D(a) \cap D(b)$ *é limitado superiormente e* $\mathrm{mdc}(a,b) = \max\big(D(a) \cap D(b)\big)$*.*

Demonstração. Pelo já discutido, temos que $\mathrm{mdc}(a,b)$ divide a e divide b. Logo, se $x \in D(\mathrm{mdc}(a,b))$, temos que $x|a$ e $x|b$, ou seja, $x \in D(a) \cap D(b)$. Agora tomemos $x_0, y_0 \in \mathbb{Z}$ tais que $\mathrm{mdc}(a,b) = ax_0 + by_0$. Se $y \in D(a) \cap D(b)$, temos que $y|\mathrm{mdc}(a,b)$ e $y \in D(\mathrm{mdc}(a,b))$.

Suponhamos que $0 \notin \{a, b\}$. Logo $c = \mathrm{mdc}(a,b) > 0$. Sendo assim, $D(c)$ é limitado superiormente e $c = |c| = \max D(c) = \max D(a) \cap D(b)$. □

É por causa do último item do teorema anterior, que se costuma definir máximo divisor comum, como o máximo do conjunto $D(a) \cap D(b)$. Mas essa definição não pode ser usada para o caso de $a = b = 0$, pois neste caso, $D(0) \cap D(0) = \mathbb{Z}$, que não tem máximo.

O teorema anterior enuncia alguns casos no quais é muito simples calcular o máximo divisor comum de dois inteiros. Mas nos outros casos, como fazê-lo? Para números pequenos, é relativamente simples, por exemplo, $D(2) \cap D(3) = \{-1, 1\}$, logo $\mathrm{mdc}(2,3) = 1$. Se a e b forem ambos não nulos e muito grandes, pode ser dispendioso determinar $D(a) \cap D(b)$.

Lema 19 (Euclides)**.** *Sejam* $a, b, q \in \mathbb{Z}$*. Então* $\mathrm{mdc}(a,b) = \mathrm{mdc}(b, a + bq)$*. Em particular, se* $b \neq 0$ *e* r *é o resto da divisão euclidiana de* a *por* b*, então* $\mathrm{mdc}(a,b) = \mathrm{mdc}(b,r)$*.*

Demonstração. Seja $x \in b\mathbb{Z} + (a + bq)\mathbb{Z}$. Daí $x = bm + (a + bq)n$, para $m, n \in \mathbb{Z}$. Daí,

$$x = an + b(m + qn) \in a\mathbb{Z} + b\mathbb{Z} \ .$$

Portanto $b\mathbb{Z} + (a+bq)\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. Agora tomemos $y \in a\mathbb{Z} + b\mathbb{Z}$ e sejam $u, v \in \mathbb{Z}$ tais que $y = au + bv$. Sendo assim,

$$y = b(v - qu) + (a + bq)u \in b\mathbb{Z} + (a + bq)\mathbb{Z} \ .$$

Ou seja, $a\mathbb{Z} + b\mathbb{Z} \subseteq b\mathbb{Z} + (a+bq)\mathbb{Z}$. Concluímos que $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + (a+bq)\mathbb{Z}$ e $\mathrm{mdc}(a,b) = \mathrm{mdc}(b, a+bq)$.

Se $b \neq 0$ e r é o resto da divisão euclidiana de a por b, temos que existe $q \in \mathbb{Z}$ tal que $a = bq + r$. Logo $r = a - bq$. Pelo que já foi provado até agora, temos que $\mathrm{mdc}(a,b) = \mathrm{mdc}(b,r)$. □

Exemplo 4. *Sejam* $a = 120$ *e* $b = 21$*. Pelo teorema anterior, temos que* $\mathrm{mdc}(120, 21) = \mathrm{mdc}(21, 15)$*, pois* 15 *é o resto da divisão de* 120 *por* 21*. Por sua vez,* $\mathrm{mdc}(21, 15) = \mathrm{mdc}(15, 6) = \mathrm{mdc}(6, 3) = \mathrm{mdc}(3, 0) = 3$*, pois dividindo-se* 21 *por* 15 *obtemos resto* 6*, dividindo-se* 15 *por* 6 *obtemos resto* 3 *e dividindo-se* 6 *por* 3 *obtemos resto* 0*.*

Teorema 20 (Algoritmo de Euclides)**.** *Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$. Seja $(a_n)_{n\in\mathbb{N}}$, sequência de inteiros, construída por: $a_0 = a$, $a_1 = b$ e, para $n \in \mathbb{N}$,*

$$a_{n+2} = \begin{cases} \text{o resto da divisão de } a_n \text{ por } a_{n+1}, \text{ se } a_{n+1} \neq 0 \\ a_{n+1}, \text{ caso contrário.} \end{cases}$$

Então existe $m \in \mathbb{N}^*$ tal que $a_m \neq 0$, $a_m | a_{m-1}$ e $a_n = 0$, para todo natural $n \geq m+1$. Ainda $\mathrm{mdc}(a, b) = |a_m|$.

Demonstração. Se $a_i = 0$, para algum natural $i \geq 2$, podemos provar, por indução, que $a_n = 0$, para todo natural $n \geq i$.

Seja $S = \{|a_n| : n \in \mathbb{N}^* \text{ e } a_n \neq 0\}$. Como $a_1 = b \neq 0$, temos que $S \neq \emptyset$. Tomemos $k = \min S$ e seja $m \in \mathbb{N}^*$ tal que $k = |a_m|$. Daí $a_m \neq 0$ e a_{m+1} é resto de divisão de a_{m-1} por a_m. Se $a_{m+1} \neq 0$, então $0 < a_{m+1} < |a_m| = k = \min S$, um absurdo! Logo $a_{m+1} = 0$ e a_m divide a_{m-1}. Pela fato exposto no primeiro parágrafo, temos que $a_n = 0$, para todo $n \geq m+1$, natural.

Dado que $a_1 = b \neq 0$, temos que a_2 é o resto da divisão de $a_0 = a$ por $a_1 = b$. Pelo lema anterior, $\mathrm{mdc}(a, b) = \mathrm{mdc}(a_0, a_1) = \mathrm{mdc}(a_1, a_2)$. Seja $T = \{i \in \mathbb{N} : \mathrm{mdc}(a_i, a_{i+1}) = \mathrm{mdc}(a, b)\}$. Já temos que $0, 1 \in T$. Tomemos $n \geq m+1$, natural. Como $a_n = 0 = a_{n+1}$, então $\mathrm{mdc}(a_n, a_{n+1}) = 0$ e $n \notin T$, pois $b \neq 0$ e $\mathrm{mdc}(a, b) \neq 0$. Logo T é não vazio e limitado superiormente pelo natural m. Seja $k = \max T$. Daí $1 \leq k \leq m$. Suponhamos que $k < m$, ou seja, $k + 1 \leq m$. Como $a_m \neq 0$, temos que $a_{k+1} \neq 0$. Logo a_{k+2} é o resto da divisão de a_k por a_{k+1}. Pelo lema anterior $\mathrm{mdc}(a_{k+1}, a_{k+2}) = \mathrm{mdc}(a_k, a_{k+1}) = \mathrm{mdc}(a, b)$, dado que $k \in T$. Mas chegamos ao absurdo de $k+1$ ser elemento de T estritamente maior que o máximo de T. Portanto $k = m$ e $\mathrm{mdc}(a_m, a_{m+1}) = \mathrm{mdc}(a, b)$. Dado que $a_{m+1} = 0$, $\mathrm{mdc}(a, b) = |a_m|$. □

O teorema anterior mostra que no momento em que a_m é divisível por a_{m-1} e $a_m \neq 0$, obtemos o máximo divisor comum de a e b. Nesse momento podemos "parar" de fazer de divisão de a_n por a_{n+1}. Exatamente como procedemos no exemplo anterior.

Exercício 11. *Para cada par de números inteiros a e b, dados abaixo, determine o* $\mathrm{mdc}(a, b)$.
(1) 637 *e* 3887 *(2)* 7325 *e* 8485 *(3)* 648 *e* 1218 *(4)* 551 *e* 874

Exercício 12. *Seja $n \in \mathbb{N}$. Mostre que*
(1) $\mathrm{mdc}(n, 2n+1) = 1$ *(2)* $\mathrm{mdc}(n+1, n^2+n+1) = 1$ *(3)* $\mathrm{mdc}(2n+1, 9n+4) = 1$

Exercício 13. *Sejam $a, b, u, v \in \mathbb{Z}$ tais que $u|a$ e $v|b$. Mostre que* $\mathrm{mdc}(u, v) | \mathrm{mdc}(a, b)$.

Proposição 21. *Sejam $a, b, c \in \mathbb{Z}$. Então* $\mathrm{mdc}(ac, bc) = c \cdot \mathrm{mdc}(a, b)$.

Demonstração. Seja $d = \mathrm{mdc}(a, b)$. Dado que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, observamos que $ac\mathbb{Z} + bc\mathbb{Z} \subseteq cd\mathbb{Z}$. Fixemos $y \in cd\mathbb{Z}$ e $u \in \mathbb{Z}$ tal que $y = cdu$. Como $du \in d\mathbb{Z}$, existem $x_0, y_0 \in \mathbb{Z}$ tais que $du = ax_0 + by_0$. Logo $y = cdu = acx_0 + bcy_0 \in ac\mathbb{Z} + bc\mathbb{Z}$. □

Exercício 14. *Sejam $a, b \in \mathbb{Z}$ tais que* $\mathrm{mdc}(a, b) = 1$. *Mostre que $a+2b$ e $b+2a$ não são ambos nulos e que o* $\mathrm{mdc}(a+2b, b+2a)$ *é* 1 *ou* 3.

Exercício 15. *Sejam $a, b \in \mathbb{N}^*$ tais que $a < b$ e* $\mathrm{mdc}(a, b) = 1$.
(1) Mostre que $\mathrm{mdc}(b+a, b-a)$ *é* 1 *ou* 2.
(2) Mostre que $\mathrm{mdc}(a+b, a^2+b^2)$ *é* 1 *ou* 2.

Exercício 16. *Uma doceria tem em seu estoque* 150 *balas de côco e* 180 *de chocolate. Quantas balas de cada sabor deve colocar igualmente em caixas decoradas, sabendo-se que essas quantidades deverão ser as maiores possíveis?*

Exercício 17. *Sejam* $a, b, c \in \mathbb{Z}$. *Mostre que* $\mathrm{mdc}(a, \mathrm{mdc}(b, c)) = \mathrm{mdc}(\mathrm{mdc}(a, b), c)$.

Exercício 18. *Uma empresa de logística é composta de três áreas: administrativa, operacional e vendedores. A área administrativa é composta de 30 funcionários, a operacional de 48 e a de vendedores com 36 pessoas. Ao final do ano, a empresa realiza uma integração entre as três áreas, de modo que todos os funcionários participem ativamente. As equipes devem conter o mesmo número de funcionários de cada área e com o maior número possível. Determine quantos funcionários devem participar de cada equipe e o número possível de equipes.*

Exercício 19. *Uma indústria de tecidos fabrica retalhos de mesmo comprimento. Após realizarem os cortes necessários, verificou-se que duas peças restantes tinham as seguintes medidas: 156 centímetros e 234 centímetros. O gerente de produção ao ser informado das medidas, deu a ordem para que o funcionário cortasse o pano em partes iguais e de maior comprimento possível. Como ele poderá resolver essa situação?*

5. Teorema de Bachet-Bézout

Dada a maneira como definimos máximo divisor comum, temos:

Proposição 22 (Teorema de Bachet-Bézout)**.** *Sejam* $a, b \in \mathbb{Z}$. *Então existem* $x_0, y_0 \in \mathbb{Z}$ *tais que* $ax_0 + by_0 = \mathrm{mdc}(a, b)$.

Demonstração. Pois que $\mathrm{mdc}(a, b) \in a\mathbb{Z} + b\mathbb{Z}$. □

Corolário 23. *Sejam* $a, b \in \mathbb{Z}$. *Então* $\mathrm{mdc}(a, b) = 1$ *se, e somente se, existem* $x_0, y_0 \in \mathbb{Z}$ *tais que* $ax_0 + by_0 = 1$.

Demonstração. O teorema de Bachet-Bézout prova uma das implicações. Suponhamos que existam $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$. Sendo assim, $1 \in a\mathbb{Z} + b\mathbb{Z}$. Logo $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z}$ e $\mathrm{mdc}(a, b) = 1$. □

Corolário 24. *Sejam* $a, b \in \mathbb{Z}$ *tais que* $d = \mathrm{mdc}(a, b) \neq 0$. *Se* $a', b' \in \mathbb{Z}$ *são tais que* $a'd = a$ *e* $b'd = b$, *então* $\mathrm{mdc}(a', b') = 1$.

Demonstração. Sejam $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = d$. Logo $a'x_0 + b'y_0 = 1$ e $1 = \mathrm{mdc}(a', b')$. □

Definição 7. *Sejam* $x, y \in \mathbb{Z}$. *Dizemos que* x ***e*** y ***são primos entre si*** *(ou ainda,* ***relativamente primos****, ou* x ***é primo relativo a*** y*) se, e somente se,* $\mathrm{mdc}(x, y) = 1$.

Exercício 20. *Determine todos os elementos de* $\{0, \ldots, 17\}$ *que são primos relativos a* 18. *Quantos são?*

Corolário 25. *Sejam* $a, b, c \in \mathbb{Z}$ *tais que* $a|bc$ *e* $\mathrm{mdc}(a, b) = 1$. *Então* $a|c$.

Demonstração. Sejam $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = 1$. Logo $c = acx_0 + bcy_0$. Dado que $a|bc$, temos que $a|c$. □

Corolário 26. *Sejam* $a, b, c \in \mathbb{Z}$. *Então* $\mathrm{mdc}(a, b) = 1 = \mathrm{mdc}(a, c)$ *se, e somente se,* $\mathrm{mdc}(a, bc) = 1$.

Demonstração. Suponhamos que $\mathrm{mdc}(a, bc) = 1$. Pelo corolário 23, temos que $ax_0 + bcy_0 = 1$, para $x_0, y_0 \in \mathbb{Z}$. Daí $1 = ax_0 + b(cy_0) = ax_0 + c(by_0)$ e $\mathrm{mdc}(a, b) = 1 = \mathrm{mdc}(a, c)$.

Agora suponhamos que $\mathrm{mdc}(a, b) = 1 = \mathrm{mdc}(a, c)$. Podemos fixar $u_0, v_0 \in \mathbb{Z}$ tais que $au_0 + cv_0 = 1$. Sendo assim, $b = abu_0 + bcv_0 \in a\mathbb{Z} + bc\mathbb{Z} = (\mathrm{mdc}(a, bc))\mathbb{Z}$. Logo $\mathrm{mdc}(a, bc)|b$. Como $\mathrm{mdc}(a, bc)|a$, $\mathrm{mdc}(a, bc)|\mathrm{mdc}(a, b) = 1$ e $\mathrm{mdc}(a, bc) = 1$ □

Exercício 21. *Sejam $a, b, c, d \in \mathbb{Z}$. Mostre que*

$$\mathrm{mdc}(ac, bd) = 1 \quad \textit{se, e somente se,} \quad \mathrm{mdc}(a, b) = \mathrm{mdc}(a, d) = \mathrm{mdc}(b, c) = \mathrm{mdc}(c, d) = 1 \ .$$

Exercício 22. *Sejam $a, b \in \mathbb{Z}$ tais que a e b são primos entre si. Mostre que $\mathrm{mdc}(a^n, b^m) = 1$, para quaisquer $m, n \in \mathbb{N}$.*

Exercício 23. *Mostre que, se $a, b \in \mathbb{Z}$, então $\mathrm{mdc}(a^2, b^2) = (\mathrm{mdc}(a, b))^2$. Generalize e demonstre para $n \in \mathbb{N}^*$.*

Exercício 24. *Sejam $a, b, c \in \mathbb{Z}$ tais que a e b são primos entre si. Mostre que $\mathrm{mdc}(ac, b) = \mathrm{mdc}(c, b)$.*

Exercício 25. *Sejam $a, b, c, d \in \mathbb{Z}$ tais que $\mathrm{mdc}(a, b) = \mathrm{mdc}(c, d) = 1$. Mostre que $\mathrm{mdc}(ac, bd) = \mathrm{mdc}(a, d) \cdot \mathrm{mdc}(b, c)$.*

A próxima proposição vai, futuramente, auxilar-nos a determinar todos os divisores de um determinado números.

Proposição 27. *Sejam $a, b \in \mathbb{N}^*$ dois números distintos e primos entre si. Seja $f\colon D^+(a) \times D^+(b) \longrightarrow \mathbb{N}$ definida por*

$$f(m, n) = mn \ , \qquad \textit{para } (m, n) \in D^+(a) \times D^+(b).$$

A função f é injetora e $\mathrm{im(f)} = D^+(ab)$.

Demonstração. Dado que a e b são não nulos, temos que 0 não é elemento de $D^+(a)$ nem de $D^+(b)$. Portanto $0 \notin \mathrm{im(f)}$. Tomemos $(m_1, n_1), (m_2, n_2) \in D^+(a) \times D^+(b)$ tais que $f(m_1, n_1) = f(m_2, n_2)$. Dado que que $\mathrm{mdc}(a, b) = 1$, $\mathrm{mdc}(m_1, n_2) = 1 = \mathrm{mdc}(m_2, n_1)$, pelo exercício 13. Dado que $m_1|m_2n_1$, teremos que $m_1|m_2$. Por outro lado, $m_2|m_1n_1$ e teremos que $m_1|m_2$. Como $m_1, m_2 \in \mathbb{N}^*$, $m_1 = m_2$ e, consequentemente, $n_1 = n_2$. Acabamos de provar que f é injetora.

Se $x|a$ e $y|b$, temos que $xy|ab$. Logo $\mathrm{im(f)} \subseteq D^+(ab)$. Tomemos $z \in \mathbb{N}$, divisor de ab. Como $ab \neq 0$, $z \neq 0$. Seja $m = \mathrm{mdc}(z, a)$. Podemos fixar $u, v \in \mathbb{N}^*$ tais que $mu = z$ e $mv = a$. Pelo corolário 24, $\mathrm{mdc}(u, v) = 1$. Ainda, $mu|mvb$. Como $m \neq 0$, $u|vb$ e, por $\mathrm{mdc}(u, v) = 1$, $u|b$. Logo $u \in D^+(b)$. Daí $z = f(m, u) \in \mathrm{im(f)}$. □

Exemplo 5. *Um número natural é dito um **quadrado perfeito** se, e somente se, é quadrado de algum inteiro (ou de único natural). No exercício 23, vimos que máximo divisor comum de quadrados perfeitos é quadrado perfeito. É fácil ver que produto de quadrados perfeitos também o é. Suponhamos que $a, b \in \mathbb{N}$ são tais que $\mathrm{mdc}(a, b) = 1$ e ab é quadrado perfeito. Vejamos que a e b são quadrados perfeitos.*

Caso $a = 0$, teremos $b = 1$ e o resultado vale. Analogamente o resultado é válido, se $b = 0$. Suponhamos $a, b \in \mathbb{N}^*$. Seja $x \in \mathbb{N}^*$ tal que $x^2 = ab$. Daí, $x|ab$ e $x = cd$, para únicos $c \in D^+(a)$ e $d \in D^+(b)$. Fixemos $p, q \in \mathbb{N}^*$ tais que $cp = a$ e $dq = b$. Portanto

$$cpdq = ab = x^2 = c^2d^2 \quad \textit{e, consequentemente,} \quad pq = cd \ .$$

Mas $p \in D^+(a)$ e $q \in D^+(b)$ e $pq = x = cd$. Pela unicidade citada, $p = c$ e $q = d$. Logo $a = c^2$ e $b = d^2$.

Exercício 26. *Sejam $a, b \in \mathbb{N}$ tais que* $\mathrm{mdc}(a, b)$ *e ab são quadrados de números naturais. Mostre que a e b também o são.*

Dados $a, b \in \mathbb{Z}$, observamos que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, para um único $m \in \mathbb{N}$. Como $m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, temos que $a|m$ e $b|m$. Portanto é m **múltiplo comum**. Agora tomemos $d \in \mathbb{N}$, múltiplo comum a a e b. Daí $d \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ e $m|d$. Como a relação "|" é relação de ordem em $\mathbb{N}$, temos que m é o **"menor"** entre os múltiplos naturais comuns a a e b.

Definição 8. *Dados $a, b \in \mathbb{Z}$, o gerador de $a\mathbb{Z} \cap b\mathbb{Z}$ é chamado de* ***mínimo múltiplo comum de*** *a **e** b, e será denotado por* $\mathrm{mmc}(a, b)$.

Se $a, b \in \mathbb{Z}$, temos que $a\mathbb{Z} = |a|\mathbb{Z}$ e $b\mathbb{Z} = |b|\mathbb{Z}$, logo $\mathrm{mmc}(a, b) = \mathrm{mmc}(|a|, |b|)$.

Teorema 28. *Sejam $a, b \in \mathbb{Z}$. Então:*

(1) $\mathrm{mmc}(a, b) = \mathrm{mmc}(|a|, |b|) = \mathrm{mmc}(b, a)$,
(2) $\mathrm{mmc}(a, b) = 0$ *se, e somente se, $a = 0$ ou $b = 0$, e*
(3) $\mathrm{mmc}(a, b) = |a|$ *se, e somente, $b|a$.*

se $a \neq 0 \neq b$, então $m = \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*\right)$.

Demonstração. (1) Temos que $a\mathbb{Z} \cap b\mathbb{Z} = |a|\mathbb{Z} \cap |b|\mathbb{Z} = b\mathbb{Z} \cap a\mathbb{Z}$.
(2) Suponhamos que $\mathrm{mmc}(a, b) = 0$. Daí $ab \in a\mathbb{Z} \cap b\mathbb{Z} = \{0\}$. Logo $ab = 0$ e, por consequência, $a = 0$ ou $b = 0$. Agora, tomemos, sem perda de generalidade, $a = 0$. Daí $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} = \{0\} \cap b\mathbb{Z} = \{0\}$. Logo $\mathrm{mmc}(a, b) = 0$.
(3) Observamos que $a\mathbb{Z} \cap b\mathbb{Z} \subseteq a\mathbb{Z}$ se, e somente se, $a\mathbb{Z} \subseteq b\mathbb{Z}$, que, por sua vez, equivale a $b|a$.

□

Exercício 27. *Sejam $a, b, u, v \in \mathbb{Z}$ tais que $u|a$ e $v|b$. Mostre que* $\mathrm{mmc}(u, v)|\mathrm{mmc}(a, b)$.

Proposição 29. *Sejam $a, b \in \mathbb{Z}^*$. Então $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^* \neq \emptyset$ e* $\mathrm{mmc}(a, b) = \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*\right)$.

Demonstração. Se $a \neq 0 \neq b$, pelo teorema anterior, $m = \mathrm{mmc}(a, b) \neq 0$. Logo $m \in a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ e $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^* \neq \emptyset$. Sendo assim, $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^* = m\mathbb{Z} \cap \mathbb{N}^*$. Seja $x \in m\mathbb{Z} \cap \mathbb{N}^*$, logo $m|x$ e, como $m, x \in \mathbb{N}^*$, $m \leq x$, pela proposição 5. Logo $m = \min\left(m\mathbb{Z} \cap \mathbb{N}^*\right)$. □

Teorema 30. *Seja $a, b \in \mathbb{N}$. Então* $\mathrm{mmc}(a, b) \cdot \mathrm{mdc}(a, b) = ab$.

Demonstração. Se $ab = 0$, temos que $\mathrm{mmc}(a, b) = 0$ e vale o resultado. Podemos supor que $ab \neq 0$.
Sejam $d = \mathrm{mdc}(a, b)$, $m = \mathrm{mmc}(a, b)$ e $a', b' \in \mathbb{N}^*$ tais que $a'd = a$ e $b'd = b$. Temos que $md \neq 0$.

Temos que $ab' = a'db' = a'b \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Logo $m|ab'$. Como $m \in a\mathbb{Z} \cap b\mathbb{Z}$, existem $x, y \in \mathbb{N}$ tais que $ax = m = by$. Portanto $a'x = b'y$. Dado que $\mathrm{mdc}(a', b') = 1$ e $a'|b'y$, temos que $a'|y$ e $y = a'k$, para algum $k \in \mathbb{N}$. Logo $x = b'k$ e $m = ab'k$. Portanto $ab'|m$. Concluímos que $m = ab'$ e

$$\mathrm{mmc}(a, b) \cdot \mathrm{mdc}(a, b) = md = ab'd = ab \ .$$

□

Corolário 31. *Sejam $a, b \in \mathbb{Z}$. Então* $\mathrm{mmc}(a, b) \cdot \mathrm{mdc}(a, b) = |ab|$. □

Corolário 32. *Sejam $a, b \in \mathbb{Z}$, relativamente primos. Então* $\mathrm{mmc}(a, b) = |ab|$. □

Exercício 28. *Sejam $a, b, c \in \mathbb{Z}$ tais que $a|c$, $b|c$ e $\mathrm{mdc}(a, b) = 1$. Mostre que $ab|c$.*

Exercício 29. *Sejam $a, b, n \in \mathbb{Z}$ e suponha $n \geq 0$. Mostre que $\mathrm{mmc}(an, bn) = n \cdot \mathrm{mmc}(a, b)$.*

Exercício 30. *Sejam $m, a, a', b, b' \in \mathbb{N}^*$ tais que $m = aa' = bb'$. Mostre que $\mathrm{mmc}(a, b) = m$ se, e somente se, $\mathrm{mdc}(a', b') = 1$.*

Exercício 31. *Para cada par de números inteiros a e b, dados abaixo, determine o $\mathrm{mmc}(a, b)$.*
(1) 637 *e* 3887 *(2)* 7325 *e* 8485 *(3)* 648 *e* 1218 *(4)* 551 *e* 874

Exercício 32. *Sejam $a, b, c \in \mathbb{Z}$. Mostre que $\mathrm{mmc}(a, \mathrm{mmc}(b, c)) = \mathrm{mmc}(\mathrm{mmc}(a, b), c)$.*

Exercício 33. *Apresente e demonstre resultado análogo ao apresentado no exercício 25 para mmc.*

Exercício 34. *Três automóveis disputam uma corrida em uma pista circular. O mais rápido deles dá uma volta em* 10 *minutos, um outro leva* 15 *minutos e o terceiro e mais lento demora* 18 *minutos para dar um volta completa. No fim de quanto tempo os* 3 *automóveis voltarão a se encontrar no início da pista se eles partiram exatamente no mesmo instante?*

Exercício 35. *Três netas visitam sua avó, respectivamente, em intervalos de* 5 *dias, de* 7 *dias e de* 9 *dias. Se a última vez em que as três netas se encontraram na casa de sua avó foi no dia 26 de julho de 2012 (Dia dos Avós no Brasil), quando tornarão a se encontrar todas na casa da avó?*

Exercício 36. *Numa linha de produção, certo tipo de manutenção é feita na máquina A a cada 3 dias, na máquina B, a cada 4 dias, e na máquina C, a cada 6 dias. Se no dia 2 de dezembro foi feita a manutenção nas três máquinas, após quantos dias as máquinas receberão manutenção no mesmo dia.*

Exercício 37. *Um médico, ao prescrever uma receita, determina que três medicamentos sejam ingeridos pelo paciente de acordo com a seguinte escala de horários: remédio A, de 2 em 2 horas, remédio B, de 3 em 3 horas e remédio C, de 6 em 6 horas. Caso o paciente utilize os três remédios às 8 horas da manhã, qual será o próximo horário de ingestão dos mesmos?*

Vejamos outra propriedade entre máximo divisor comum e mínimo múltiplo comum.

Proposição 33. *Sejam $a, b, c \in \mathbb{Z}$. Então*

$$a\mathbb{Z} \cap \Big(b\mathbb{Z} + c\mathbb{Z}\Big) = \Big(a\mathbb{Z} \cap b\mathbb{Z}\Big) + \Big(a\mathbb{Z} \cap c\mathbb{Z}\Big).$$

Consequentemente, $\mathrm{mmc}(a, \mathrm{mdc}(b, c)) = \mathrm{mdc}(\mathrm{mmc}(a, b), \mathrm{mmc}(a, c))$.

Demonstração. Como

$$0\mathbb{Z} \cap \Big(b\mathbb{Z} + c\mathbb{Z}\Big) = \{0\} = \{0\} + \{0\} = \Big(0\mathbb{Z} \cap b\mathbb{Z}\Big) + \Big(0\mathbb{Z} \cap c\mathbb{Z}\Big),$$

o resultado vale para $a = 0$. Ainda, para $x \in \mathbb{Z}$,

$$a\mathbb{Z} \cap \Big(0\mathbb{Z} + x\mathbb{Z}\Big) = a\mathbb{Z} \cap x\mathbb{Z} = \{0\} + a\mathbb{Z} \cap x = \Big(a\mathbb{Z} \cap 0\Big) + \Big(a\mathbb{Z} \cap x\mathbb{Z}\Big)$$

e o resultado vale para $b = 0$ ou $c = 0$. Suponhamos daqui por diante que $abc \neq 0$.

Seja $z \in \Big(a\mathbb{Z} \cap b\mathbb{Z}\Big) + \Big(a\mathbb{Z} \cap c\mathbb{Z}\Big)$. Daí $z = u + v$, onde $u \in a\mathbb{Z} \cap b\mathbb{Z}$ e $v \in a\mathbb{Z} \cap c\mathbb{Z}$. Como $u, v \in a\mathbb{Z}$, $x = u + v \in a\mathbb{Z}$. Ainda, $x = u + v \in b\mathbb{Z} + c\mathbb{Z}$. Logo $x \in a\mathbb{Z} \cap \Big(b\mathbb{Z} + c\mathbb{Z}\Big)$.

Agora tomemos $y \in a\mathbb{Z} \cap \Big(b\mathbb{Z} + c\mathbb{Z}\Big)$. Temos que $d\mathbb{Z} = b\mathbb{Z} + c\mathbb{Z}$, onde $d = \text{mdc}(b, c)$. Daí, $y = ap = dq$, para $p, q \in \mathbb{Z}^*$. Pelo teorema de Bachet-Bézout, existem $t, w \in \mathbb{Z}$ tais que $d = bt + cw$. Seja $e = \text{mdc}(a, d)$. Daí $a = a'e$ e $d = d'e$, para $a', d' \in \mathbb{Z}^*$, e $\text{mdc}(a', d') = 1$. Sendo assim, $a'p = d'q$ e $a'|q$, já que $\text{mdc}(a', d') = 1$. Podemos fixar $r \in \mathbb{Z}$, tal que $a'r = q$. Como $e|d$ e $d|b$, temos que $e|b$. Portanto, $a = a'e|a'b$ e $bqt = ba'rt \in a\mathbb{Z} \cap b\mathbb{Z}$. Analogamente provamos que $cqw \in a\mathbb{Z} \cap c\mathbb{Z}$. Logo

$$y = dq = bqt + cqw \in \Big(a\mathbb{Z} \cap b\mathbb{Z}\Big) + \Big(a\mathbb{Z} \cap c\mathbb{Z}\Big).$$

Conclui-se que $a\mathbb{Z} \cap \Big(b\mathbb{Z} + c\mathbb{Z}\Big) = \Big(a\mathbb{Z} \cap b\mathbb{Z}\Big) + \Big(a\mathbb{Z} \cap c\mathbb{Z}\Big)$. □

Corolário 34. *Nas mesmas condições da proposição anterior,* $a\mathbb{Z} + \Big(b\mathbb{Z} \cap c\mathbb{Z}\Big) = \Big(a\mathbb{Z} + b\mathbb{Z}\Big) \cap \Big(a\mathbb{Z} + c\mathbb{Z}\Big)$. *Porconsequência,* $\text{mdc}(a, \text{mmc}(b, c)) = \text{mmc}(\text{mdc}(a, b), \text{mdc}(a, c))$.

Demonstração. Seja $x = \text{mdc}(a, b)$. Daí $a\mathbb{Z} + b\mathbb{Z} = x\mathbb{Z}$. Logo, pela proposição anterior,

$$\Big(a\mathbb{Z} + b\mathbb{Z}\Big) \cap \Big(a\mathbb{Z} + c\mathbb{Z}\Big) = x\mathbb{Z} \cap \Big(a\mathbb{Z} + c\mathbb{Z}\Big) = \Big(x\mathbb{Z} \cap a\mathbb{Z}\Big) + \Big(x\mathbb{Z} \cap c\mathbb{Z}\Big).$$

Por outro lado, $x\mathbb{Z} \cap a\mathbb{Z} = a\mathbb{Z}$, já que $a\mathbb{Z} \subseteq x\mathbb{Z}$. Ainda, pela proposição anterior

$$x\mathbb{Z} \cap c\mathbb{Z} = c\mathbb{Z} \cap x\mathbb{Z} = \Big(c\mathbb{Z} \cap a\mathbb{Z}\Big) + \Big(c\mathbb{Z} \cap b\mathbb{Z}\Big).$$

Sendo assim,

$$\Big(a\mathbb{Z} + b\mathbb{Z}\Big) \cap \Big(a\mathbb{Z} + c\mathbb{Z}\Big) = a\mathbb{Z} + \Big(\Big(c\mathbb{Z} \cap a\mathbb{Z}\Big) + \Big(c\mathbb{Z} \cap b\mathbb{Z}\Big)\Big).$$

Como $a\mathbb{Z} + \Big(c\mathbb{Z} \cap a\mathbb{Z}\Big) = a\mathbb{Z}$, pois $c\mathbb{Z} \cap a\mathbb{Z} \subseteq a\mathbb{Z}$, temos que

$$\Big(a\mathbb{Z} + b\mathbb{Z}\Big) \cap \Big(a\mathbb{Z} + c\mathbb{Z}\Big) = a\mathbb{Z} + \Big(c\mathbb{Z} \cap b\mathbb{Z}\Big).$$

□

6. Equações Diofantinas

Os resultados que estabelecemos até o momento sobre máximo divisor comum vão ajudar a garantir a existência de soluções para equações do tipo

$$ax + by = c\ ,$$

bem como nos ajudar a construção de soluções para as mesmas. Essas equações são chamadas de **Equações Diofantinas Lineares**.

Teorema 35. *Sejam* $a, b \in \mathbb{Z}$ *tais que* $d = \text{mdc}(a, b) \neq 0$. *Para* $c \in \mathbb{Z}$, *a equação* $ax + by = c$ *tem solução se, e somente se,* $d|c$.

Demonstração. Lembramos que $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Logo

$$\text{existem } x_0, y_0 \in \mathbb{Z} \text{ tais que } ax_0 + by_0 = c \quad \Leftrightarrow \quad c \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \quad \Leftrightarrow \quad d|c$$

□

Teorema 36. *Sejam $a, b \in \mathbb{Z}$ tais que $d = \text{mdc}(a, b) \neq 0$. Sejam $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = c$. Se $a', b' \in \mathbb{Z}$ são tais que $a'd = a$ e $b'd = b$, então*

$$ax + by = c \quad \textit{se, e somente se,} \quad \begin{cases} x = x_0 + b'k \\ y = y_0 - a'k \end{cases} \textit{, para algum } k \in \mathbb{Z}.$$

Demonstração. Suponhamos que $x, y \in \mathbb{Z}$ são tais que $ax + by = c$. Sendo assim, $ax + by = ax_0 + by_0$ e $a(x - x_0) = b(y_0 - y)$. Logo $a'(x - x_0) = b'(y_0 - y)$. Sem perda de generalidade, suponhamos que $b' \neq 0$. Daí $b' | a'(x - x_0)$ e, dado que $\text{mdc}(a', b') = 1$, temos que $b' | (x - x_0)$. Seja $k \in \mathbb{Z}$ tal que $x - x_0 = b'k$, ou seja, $x = x_0 + b'k$. Ainda $a'b'k = b'(y_0 - y)$. Como $b' \neq 0$, $a'k = y_0 - y$, ou equivalentemente, $y = y_0 - a'k$.

Seja $k \in \mathbb{Z}$, $x = x_0 + b'k$ e $y = y_0 - a'k$. Daí $a(x_0 + b'k) + b(y_0 - a'k) = ax_0 + ab'k + by_0 - ba'k = c + a'db' - b'da' = c$. □

Exemplo 6. *Resolvamos a equação $2x + 3y = 1$. Temos que*

$$2x + 3y = 1 \Leftrightarrow 2x + 3y = 3 - 2 \Leftrightarrow 2(x + 1) = 3(1 - y) \ .$$

Como $\text{mdc}(2, 3) = 1$, temos que $1 - y = 2k$, para algum $k \in \mathbb{Z}$. Daí $y = 1 - 2k$, enquanto $x = 3k - 1$.

No teorema e no exemplo vimos que foi necessário ter previamente em mãos uma solução da equação. Vejamos que podemos alterar o algoritmo de Euclides (teorema 20) para obter testemunha para a igualdade $ax + by = \text{mdc}(a, b)$, do Teorema de Bachet-Bézout. Essa testemunha pode gerar uma solução da equação diofantina $ax + by = c$, onde $\text{mdc}(a, b) | c$.

Proposição 37 (Algoritmo estendido de Euclides)**.** *Sejam $a, b \in \mathbb{Z}$ tais que $b \neq 0$. Sejam $(a_n)_{n \in \mathbb{N}}$, (q_n), (x_n) e (y_n), sequências de inteiros, construídas por: $a_0 = a$, $a_1 = b$, $q_0 = q_1 = x_1 = y_0 = 0$, $x_0 = y_1 = 1$ e, para $n \in \mathbb{N}$,*

(1) se $a_{n+1} \neq 0$,
  (a) seja q_{n+2} o quociente da divisão de a_n por a_{n+1},
  (b) seja a_{n+2} o resto da divisão de a_n por a_{n+1},
  (c) seja $x_{n+2} = x_n - q_{n+2}x_{n+1}$ e
  (d) seja $y_{n+2} = y_n - q_{n+2}y_{n+1}$;
(2) e, se $a_{n+1} = 0$, sejam $a_{n+2} = a_{n+1}$, $q_{n+2} = q_{n+1}$, $x_{n+2} = x_{n+1}$ e $y_{n+2} = y_{n+1}$.

Então $a_n = ax_n + by_n$, para todo $n \in \mathbb{N}$, e existe $m \in \mathbb{N}^*$, tal que $\text{mdc}(a, b) = ax_m + by_m$.

Demonstração. Seja $S = \{i \in \mathbb{N} \colon a_i \neq ax_i + by_i\}$ e suponhamos que $S \neq \emptyset$. Observamos que $ax_0 + by_0 = a \cdot 1 + b \cdot 0 = a = a_0$ e que $ax_1 + by_1 = a \cdot 0 + b \cdot 1 = b = a_1$. Portanto $0 \notin S$ e $1 \notin S$. Se $m = \min S$, então $m \geq 2$ e $m = k + 2$, para $k \in \mathbb{N}$. Daí, $k \notin S$ e $k + 1 \notin S$. Se $a_{k+1} = 0$, $a_{k+2} = a_{k+1}$, $x_{k+2} = x_{k+1}$ e $y_{k+2} = y_{k+1}$; portanto, $ax_{k+2} + by_{k+2} = ax_{k+1} + by_{k+1} = a_{k+1} = a_{k+2}$ e teríamos $k + 2 = m \notin S$, um absurdo! Sendo assim, $a_{k+1} \neq 0$. Neste caso $a_k = a_{k+1}q_{k+2} + a_{k+2}$. Nesse caso

$$ax_{k+2} + by_{k+2} = a\Big(x_k - q_{k+2}x_{k+1}\Big) + b\Big(y_k - q_{k+2}y_{k+1}\Big) = \big(ax_k + by_k\big) - q_{n+2}\big(ax_{k+1} + by_{k+1}\big).$$

Como $k \notin S$ e $k + 1 \notin S$, $a_k = ax_k + by_k$ e $a_{k+1} = ax_{k+1} + by_{k+1}$. Portanto,

$$ax_m + by_m = ax_{k+2} + by_{k+2} = a_k - q_{k+2}a_{k+1} = a_{k+2} = a_m$$

e $m \notin S$, um absurdo. Concluímos que $S = \emptyset$.

Observamos que a sequência (a_n) é construída exatamente da mesma maneira como no teorema 20. Logo que existe $m \in \mathbb{N}^*$, tal que $|a_m| = \text{mdc}(a, b)$. Sendo assim, $\text{mdc}(a, b) = ax_m + by_m$. □

Exemplo 7. *Retomemos o cálculo de* $\mathrm{mdc}(120, 21)$ *com o intuito de descobrir* $x, y \in \mathbb{Z}$ *tais que* $3 = 120x + 21y$*. Começamos por:*

n	a_n	q_n	x_n	y_n
0	120	0	1	0
1	21	0	0	1

Como $a_1 = 21 \neq 0$*, devemos efetuar a divisão de* 120 *por* 21*. Daí obtemos quociente* 5 *e resto* 15*. Logo* $a_2 = 15$ *e* $q_2 = 5$*. Sendo assim,* $x_2 = 1 - 5 \cdot 0 = 1$ *e* $y_2 = 0 - 5 \cdot 1 = -5$*. Acrescentamos mais uma linha à tabela anterior:*

n	a_n	q_n	x_n	y_n
0	120	0	1	0
1	21	0	0	1
2	15	5	1	-5

Dado que $a_2 \neq 0$*, devemos continuar efetuando divisão. Obtemos:*

n	a_n	q_n	x_n	y_n
0	120	0	1	0
1	21	0	0	1
2	15	5	1	-5
3	6	1	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-5) = 6$

Como $a_3 \neq 0$*, continuamos com a divisão e obtemos:*

n	a_n	q_n	x_n	y_n
0	120	0	1	0
1	21	0	0	1
2	15	5	1	-5
3	6	1	-1	6
4	3	2	$1 - 2 \cdot (-1) = 3$	$-5 - 2 \cdot 6 = -17$

Pelo algoritmo de Euclides (teorema 20), temos que $a_4 = 3 = \mathrm{mdc}(120, 21)$*, pois* $a_4 \neq 0$ *e* $a_4 | a_3$*. Pelo versão estendida desse algoritmo, temos que* $120 \cdot 3 + 21 \cdot (-17) = 360 - 357 = 3$*.*

Mas como usar essas testemunhas para achar uma solução de uma equação diofantina? Basta multiplicar por um número conveniente!

Exemplo 8. *Resolvamos a equação diofantina* $120x + 21y = 9$*. Já sabemos que* $3 = 120 \cdot 3 + 21 \cdot (-17)$*. Portanto* $9 = 3\big(120 \cdot 3 + 21 \cdot (-17)\big) = 120 \cdot 9 + 21 \cdot (-51)$*. Daí*

$$120x + 21y = 9 = 120 \cdot 9 + 21 \cdot (-51) \Leftrightarrow 120(x - 9) = 21(-y - 51) \Leftrightarrow 40(x - 9) = 7(-y - 51).$$

Dado que $\mathrm{mdc}(40, 7) = 1$ *e que* $7 | 40(x-9)$*, temos que* $x - 9 = 7k$*, para algum* $k \in \mathbb{Z}$*. Daí* $-y - 51 = 40k$*. Portanto* $120x + 21y = 9$ *se, e somente se,* $x = 9 + 7k$ *e* $y = -51 - 40k$*, para algum* $k \in \mathbb{Z}$*.*

Exercício 38. *Para cada par de números inteiros* a *e* b*, dados abaixo, determine o* $\mathrm{mdc}(a, b)$ *e números inteiros* m *e* n *tais que* $\mathrm{mdc}(a, b) = am + bn$*.*
(1) 637 *e* 3887 *(2)* 7325 *e* 8485 *(3)* 648 *e* 1218 *(4)* 551 *e* 874

Exercício 39. *Resolva as seguintes equações diofantinas:*

(1) $14x - 24y = 18$ *(2)* $3x + 45y = 20$ *(3)* $50x + 56y = 74$

Exercício 40. *Dispondo de* 100 *reais, quais são as quantias que se podem gastar comprando selos de* 5 *reais e* 7 *reais?*

Exercício 41. *Determine todos os múltiplos de* 11 *e de* 9 *cuja soma é igual a:*
(1) 79 *(2)* 80 *(3)* 270

Exercício 42. *Ache o menor múltiplo positivo de* 5 *que deixa resto* 2 *quando dividido por* 3 *e por* 4*.*

Exercício 43. *Uma pessoa dispõe de* 55 *reais para gastar em biscoitos dos tipos A e B que custam* 3 *e* 5 *reais, respectivamente. Qual o número máximo de biscoitos que pode comprar gastando todo os* 55*?*

Exercício 44. *Numa criação de coelhos e galinhas, contaram-se* 400 *pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?*

Exercício 45. *Subindo uma escada de dois em dois degraus, sobra um degrau. Subindo a mesma escada de três em três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que o seu número é múltiplo de* 7 *e está compreendido entre* 40 *e* 100*.*

7. Números primos

Definimos agora aqueles que tem papel fundamental em $\mathbb{Z}$.

Definição 9. *Seja $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Dizemos que p é **primo** se, e somente se, sempre que $p|ab$, para $a, b \in \mathbb{Z}$, $p|a$ ou $p|b$. Quando $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ não é primo, ele é dito **composto**.*

Portanto, mostrar que um número inteiro p, não nulo e não inversível, é primo é mostrar que vale a frase:

$$\forall a, b \in \mathbb{Z}(\ p|ab \Rightarrow p|a \vee p|b\ ).$$

Deve ficar bem claro que os números 0, -1 e 1 **não são primos, nem compostos!**

Exemplo 9. *Vejamos que* 2 *é primo. Sejam $a, b \in \mathbb{Z}$ tais que $2|ab$. Por divisão euclidiana, existem $q_1, q_2 \in \mathbb{Z}$ e $r, s \in \{0, 1\}$ tais que $a = 2q_1 + r$ e $b = 2q_2 + s$. Como $ab = (2q_1 + r)(2q_2 + s) = 4q_1q_2 + 2(q_1s + q_2r) + rs$, temos que $2|rs$. Uma vez que $rs \in \{0, 1\}$, temos que $rs = 0$. Daí, $r = 0$ ou $s = 0$. Logo $2|a$ ou $2|b$.*

Teorema 38. *Seja $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. São equivalentes:*

(1) p é primo e
(2) os únicos divisores de p são -1, 1, p e $-p$.

Demonstração. Suponhamos que p é primo e seja $a \in \mathbb{Z}$ tal que $a|p$. Fixemos $b \in \mathbb{Z}$ tal que $ab = p$. Logo $p|ab$. Dado que p é primo, $p|a$ ou $p|b$. Se $p|a$, temos que $|p| = |a|$, ou seja, $a \in \{-p, p\}$. Se $b|p$, temos que $|b| = |p|$, $b \in \{-p, p\}$ e, nesse caso, $a \in \{-1, 1\}$.

Agora suponhamos que $D(p) = \{-p, -1, 1, p\}$ e que $p|ab$, para $a, b \in \mathbb{Z}$. Seja $d = \text{mdc}(p, a)$. Como $d \in D^+(p) = \{1, |p|\}$, temos que $d = 1$ ou $d = |p|$. Se $d = |p|$, então $|p|\big|a$ e $p|a$. Se $d = 1$, temos que $p|b$. □

Logo temos que 3, 5, 7, 11, 13, 17 e 19 são todos números primos.

Corolário 39. *Seja $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Temos que p é primo se, e somente se, $|p|$ é primo.* □

Exercício 46. *Seja $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Mostre que p é composto se, e somente se, existe $a, b \in \mathbb{Z}$ tais que $1 < a \leq b < |p|$ e $ab = |p|$.*

Exercício 47. *Mostre que o único primo da forma $n^3 - 1$ é 7.*

Corolário 40. *Sejam $a \in \mathbb{Z}$ e $p \in \mathbb{N}$, primo. Então*

$$\mathrm{mdc}(p, a) = \begin{cases} p & , \text{ se } p|a \\ 1 & , \text{ se } p \nmid a \end{cases}$$

Demonstração. Temos que $\mathrm{mdc}(p, a) \in \{1, p\}$. Pelo teorema 17, temos que $\mathrm{mdc}(p, a) = p$ se, e somente se, $p|a$. □

Exercício 48. *Sejam $p \in \mathbb{N}$ um primo e $I \leq \mathbb{Z}$. Mostre que $I \subseteq p\mathbb{Z}$ ou $I + p\mathbb{Z} = \mathbb{Z}$.*

Corolário 41. *Sejam $p, q \in \mathbb{Z}$, primos tais que $|p| \neq |q|$. Então $\mathrm{mdc}(p, q) = 1$. Ainda, para $m, n \in \mathbb{N}$, $\mathrm{mdc}(p^m, q^n) = 1$.*

Demonstração. Basta observar que $D(p) \cap D(q) = \{-1, 1\}$. Para o resultado sobre potências, basta utilizar o resultado do exercício 22. □

Corolário 42. *Sejam $p, x, n \in \mathbb{Z}$ tais que $n > 0$ e p é primo. Se $p|x^n$, então $p|x$.*

Demonstração. Se $p \nmid x$, temos que $\mathrm{mdc}(p, x) = 1$. Pelo corolário anterior $\mathrm{mdc}(p, x^n) = 1$. Dado que $p|x^n$, temos que $\mathrm{mdc}(p, x^n) = |p|$, um absurdo pois $|p| \neq 1$. □

Proposição 43. *Sejam $n, p \in \mathbb{N}$ onde p é primo. Então $D^+(p^n) = \left\{p^i : i \in \mathbb{N} \wedge i \leq n\right\}$.*

Demonstração. Seja $S = \left\{n \in \mathbb{N} : D^+(p^n) = \left\{p^i : i \in \mathbb{N} \wedge i \leq n\right\}\right\}$. Temos que $0 \in S$ pois $p^0 = 1$ e $D^+(1) = \{1\}$. Suponhamos que $k \in S$. Já temos que $\left\{p^i : i \in \mathbb{N} \wedge i \leq k+1\right\} \subseteq D^+(p^{k+1})$. Seja $d \in \mathbb{N}$ tal que $d|p^{k+1}$. Fixemos $x \in \mathbb{N}$ tais que $dx = p^{k+1}$. Como $p|p^{k+1}$, temos que $p|dx$ e, consequentemente, $p|d$ ou $p|x$, pois p é primo. Se $p|d$, temos que $p = dq$, para $q \in \mathbb{N}$. Logo $p^{k+1} = dx = pqx$, $p^k = qx$ e $q|p^k$. Sendo assim, $q \in D^+(p^k)$ e, como $k \in S$, $q = p^i$, para $i \in \mathbb{N}$ tal que $i \leq k$. Daí $d = qp = p^{i+1}$ e $i + 1 \leq k + 1$. Caso $p|x$, então $x = py$ para algum $y \in \mathbb{N}$. Daí $p^{k+1} = dpy$ e $d|p^k$. Logo $d = p^i$ para algum $i \leq k$. Sendo assim, $D^+(p^{k+1}) \subseteq \left\{p^i : i \in \mathbb{N} \wedge i \leq k+1\right\}$ e $k + 1 \in S$. Pelo Princípio da Indução Finita, $S = \mathbb{N}$. □

Exemplo 10. *Sabemos que $36 = 2^2 \cdot 3^2$. Podemos usar a proposição 27 para determinar todos os divisores naturais de 36. Visto que $\mathrm{mdc}(2^2, 3^2) = 1$, pois $\mathrm{mdc}(2, 3) = 1$, temos que*

$$D^+(36) = \left\{mn : m \in D^+(2^2) \wedge n \in D^+(3^2)\right\}.$$

Pela proposição anterior, temos que $D^+(2^2) = \left\{2^0, 2^1, 2^2\right\} = \{1, 2, 4\}$, enquanto $D^+(3^2) = \{1, 3, 9\}$. Daí $D^+(36) = \{1, 3, 9, 2, 6, 18, 4, 12, 36\}$ e

$$D(36) = \{-36, -18, -12, -9, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 9, 12, 18, 36\}.$$

Exercício 49. *Sejam $p, \alpha \in \mathbb{N}$, onde p é primo. Determine o número de elementos de $D(p^\alpha)$.*

Exercício 50. *Determine todos de divisores de $D(p_1^{\alpha_1} \dots p_n^{\alpha_n})$, onde $2 \leq p_1 < \cdots < p_n$ são primos distintos e $\alpha_1, \dots, \alpha_n \in \mathbb{N}$. Quantos são?*

Proposição 44. *Seja $x \in \mathbb{Z} \setminus \{-1, 1\}$. Então x admite divisor primo.*

Demonstração. Como $x \notin \{-1, 1\}$, temos $D^+(x) \not\subseteq \{1\}$. Sejam $S = \{i \in D^+(x) \colon 1 < i\}$ e $p = \min S$. Seja $d \in \mathbb{N} \setminus \{1\}$ um divisor de p. Como $p \neq 0$, $1 < d$ e $d|x$, já que $d|p$ e $p|x$. Logo $d \in S$. Logo $p \leq d$. Mas $d \leq p$. Logo $d = p$. Mostramos que os únicos divisores naturais de p são 1 e p. Sendo assim, p é primo. □

Exercício 51. *Seja $a \in \mathbb{N} \setminus \{0, 1\}$. Mostre que o conjunto $\{a^i \colon i \in \mathbb{N}\}$ é ilimitado superiormente.*

Lema 45. *Sejam $x \in \mathbb{N} \setminus \{0, 1\}$ e $p \in \mathbb{N}$, um primo. Então existe $n \in \mathbb{N}$ tal que $p^n|x$ e $p^{n+1} \nmid x$.*

Demonstração. Fixemos $m \in \mathbb{N}$ tal que $|x| < p^m$. Seja $S = \{i \in \mathbb{N} \colon p^i \big| |x|\}$, que é não vazio pois $0 \in S$. Suponhamos que existe $i \in S$ tal que $i \geq m$. Como $p^i|x$, temos que $p^i \leq |x|$, pela proposição 5. Como $p^m|p^i$, pela mesma proposição 5, $p^m \leq p^i$. Daí $|x| < p^m \leq p^i \leq |x|$, um absurdo! Logo S é limitado superior por m. Seja $n = \max S$ e temos que $p^n|x$ mas $p^{n+1} \nmid x$. □

Teorema 46 (Teorema Fundamental da Aritmética)**.** *Seja $x \in \mathbb{N} \setminus \{0, 1\}$. Então:*

(1) existem $k \in \mathbb{N}^*$, $p_1, \ldots, p_k$, primos, e $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$, tais que

$$1 < p_1 < p_2 < \cdots < p_k \qquad e \qquad x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad .$$

(2) se $l \in \mathbb{N}^*$, $q_1, \ldots, q_l$, primos, e $\beta_1, \ldots, \beta_l \in \mathbb{N}^*$, são tais que $1 < q_1 < q_2 < \cdots < q_l$, e $x = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$, então $k = l$, $p_i = q_i$ e $\alpha_i = \beta_i$, para $i \in \{1, \ldots, k\}$.

Demonstração. Vamos provar o teorema por indução em x. Seja

$$S = \{x \in \mathbb{N} \colon 2 \leq x \text{ e vale o item 1 do teorema para } x\}.$$

Temos que 2 é primo e $2 = 2^1$; logo $2 \in S$. Suponhamos que $x \in \mathbb{N}$ é tal que $x \geq 2$ e $\{2, \ldots, x\} \subseteq S$. Seja $y = x + 1$. Pelo lemas anteriores, podemos fixar $p_1 = \min\{i \in \mathbb{N} \colon i \text{ é primo e } i|y\}$ e $n_1 \in \mathbb{N}^*$ tal que $p_1^{n_1}|y$ e $p_1^{n_1+1} \nmid y$. Seja $r \in \mathbb{N}^*$ tal que $p_1^{n_1} r = y$. Como $1 < p_1 \leq p_1^{n_1}$, temos que $r < y$. Caso $r = 1$, y satisfaz o item 1. Caso, $r \neq 1$, temos que $r \in \{2, \ldots, x\}$ e r satisfaz o item 1. Logo podemos fixar $m \in \mathbb{N}^*$, $r_1, \ldots, r_m$, primos, e $\gamma_1, \ldots, \gamma_m \in \mathbb{N}^*$, tais que

$$1 < r_1 < r_2 < \cdots < r_m \qquad \text{e} \qquad r = r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_m^{\gamma_m} \quad .$$

Temos que $r_i|y$ e $r_i \geq p_1$, para todo $i \in \{1, \ldots, m\}$, dado que $r_i|r$ e $r|y$. Como $p_1^{n_1+1} \nmid y$, $p_1 \nmid r$ e $p_1 < r_1$. Logo $y = p_1^{n_1} r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_m^{\gamma_m}$ e $p_1 < r_1 < r_2 < \cdots < r_m$. Consequentemente, y satisfaz o item 1 do teorema. Por PIF, $S = \{x \in \mathbb{N} \colon x \geq 2\}$.

Para provar que vale o item 2, suponhamos que $x \in S$, $k, l \in \mathbb{N}^*$, $p_1, \ldots, p_k, q_1, \ldots, q_l$, primos, $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l \in \mathbb{N}^*$, são tais que

$$1 < p_1 < p_2 < \cdots < p_k, \quad 1 < q_1 < q_2 < \cdots < q_l \quad \text{e} \quad x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l} \ .$$

Fixemos $i \in \{1, \ldots, k\}$. Temos que $p_i|q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$ e, dado que é primo, $p_i|q_j^{\beta_j}$, para algum $j \in \{1, \ldots, l\}$. Pelo corolário 7, $p_i|q_j$. Como são ambos primos e naturais, $p_i = q_j$. Dado que $1 < q_1 < q_2 < \cdots < q_l$, temos que $p_i = q_{f(i)}$, onde $f(i) \in \{1, \ldots, l\}$. Estabelecemos $f \colon \{1, \ldots, k\} \longrightarrow \{1, \ldots, l\}$ que é injetora pois $1 < p_1 < p_2 < \cdots < p_k$. Sendo assim, $k \leq l$. Analogamente, estabelecemos $g \colon \{1, \ldots, l\} \longrightarrow \{1, \ldots, k\}$ tal que $q_j = p_{g(j)}$, para todo $j \in \{1, \ldots, l\}$. Também g é injetora. Logo $l \leq k$. Portanto, $k = l$. Temos que $p_1 = q_{f(1)} \geq q_1$ e $q_1 = p_{g(1)} \geq p_1$. Logo $p_1 = q_1$ e $f(1) = 1 = g(1)$. Seja $T = \{i \in \{1, \ldots, k\} : f(i) \neq i \vee g(i) \neq i\}$ e suponhamos que $T \neq \emptyset$. Temos que $t = \min T > 1$ já que $1 \notin T$. Caso $u = f(t) < t$, então $f(u) = u = f(t)$, um absurdo pois $u < t$ e f é injetora. Sendo assim, $f(t) \geq t$ e $p_t = q_{f(t)} \geq q_t$. Analogamente $g(t) \geq t$ e $q_t = p_{g(t)} \geq p_t$. Logo $p_t = q_t$ e

$f(t) = t = g(t)$, um absurdo. Sendo assim, $T = \emptyset$, ou seja, $f(i) = i = g(i)$, para todo $i \in \{1, \ldots, k\}$. Logo $p_i = q_i$, para para todo $i \in \{1, \ldots, k\}$. Portanto $x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Para $i, j \in \{1, \ldots, k\}$, distintos, temos que $\text{mdc}(p_i^{\alpha_i}, p_j^{\beta_j}) = 1$. Fixemos $i \in \{1, \ldots, k\}$ e teremos $p_i^{\alpha_i} | p_i^{\beta_i}$ e $p_i^{\beta_j} | p_i^{\alpha_i}$. Consequentemente, $p_i^{\alpha_i} = p_i^{\beta_i}$ e $\alpha_i = \beta_i$. □

Definição 10. *A sequências de primos juntamente com a sequência de expoentes determinada para o natural x, no teorema anterior, é a* ***fatoração em primos de*** *x.*

Exercício 52. *Determine, se existem, naturais x, y e z tais que $2^x \cdot 3^4 \cdot 26^y = 39^z$.*

Exercício 53. *Decomponha em fatores primos os números:*

(1) 180	*(3)* 320	*(5)* 605	*(7)* 1008	*(9)* 2058	*(11)* 4225
(2) 220	*(4)* 308	*(6)* 616	*(8)* 1210	*(10)* 3125	*(12)* 5040

Exercício 54. *Qual é o menor natural n que torna $n!$ divisível por 1000?*

Exercício 55. *Ache os possíveis valores de $m, n \in \mathbb{N}$ de modo que o número de $9^m \cdot 10^n$ tenha:*
(1) 27 divisores naturais *(2) 243 divisores naturais*

Mas como determinar a fatoração em primos de um número dado x? Temos que os divisores primos de x são menores ou iguais a x. Se x já é primo, não há outros fatores primos. Como determinar que x é primo? Como determinar todos os primos abaixo de x? Vejamos agora alguns resultados que buscaram responder algumas dessas perguntas.

Proposição 47. *Seja $x \in \mathbb{N}$ tal que $x \geq 2$. São equivalentes:*
(1) x é composto e
(2) x admite divisor natural e primo p tal que $p^2 \leq x$.

Demonstração. Suponhamos que x é composto e seja $S = \{i \in D^+(x) \colon i \text{ é primo}\}$. Temos que $S \neq \emptyset$ e seja $p = \min S$. Como x não é primo, $p < x$. Ainda $1 < p$. Fixemos $q \in \mathbb{N}$ tal que $pq = x$. Como x não é primo e não é nulo, temos que $q \notin \{0, 1\}$. Pela proposição anterior, q admite divisor $r \in \mathbb{N}$, primo. Como $q|x$, temos que $r|x$ e $r \in S$. Daí $p \leq r$. Temos que $pr|x$ e $pr \leq x$. Como $p \leq r$, $p^2 \leq pr \leq x$.

Agora suponhamos que $p \in \mathbb{N}$ é primo, divide x e $p^2 \leq x$. Como $1 < p$, temos que $p < p^2 \leq x$. Logo $p|x$, $1 < p < x$ e consequentemente x não é primo. □

Observação 1 (Crivo de Eratóstenes)**.** *Vamos aqui descrever o chamado* ***Crivo de Eratóstenes****, que é um algoritmo que determina todos primos naturais até um número determinado.*

Sejam $x \in \mathbb{N}$, tal que $x \geq 4$, e $X = \{i \in \mathbb{N} \colon 2 \leq i \leq x\}$. Sejam $p_1, \ldots, p_k$ todos os primos que são elementos do conjunto X de tal forma que $2 = p_1 < p_2 < \cdots < p_k$ e $p_k^2 \leq x$. Seja

$$Y = \Big(X \setminus \big(p_1\mathbb{Z} \cup \cdots \cup p_k\mathbb{Z}\big)\Big) \cup \{p_1, \ldots, p_k\}$$

e vejamos que Y é o conjunto de todos os primos que são elementos de X. De fato, seja $y \in X$, primo. Se $y \in p_1\mathbb{Z} \cup \cdots \cup p_k\mathbb{Z}$, podemos fixar $i \in \{1, \ldots, k\}$, tal que $p_i|y$. Como ambos são primos e naturais, $y = p_i$ e $y \in \{p_1, \ldots, p_k\}$. Logo os primos em X são elementos de Y. Agora tomemos $z \in Y$ e suponhamos que z é composto. Nesse caso, pela proposição anterior, existe $q \in \mathbb{N}$, primo, tal que $q|z$ e $q^2 \leq z$. Como $z \leq x$, temos que $q = p_j$ para algum $j \in \{1, \ldots, k\}$. Daí $z \in p_j\mathbb{Z}$ e $z \notin Y$. Portanto, todos os elementos de Y são primos.

Observamos que $p_1 = 2 = \min X$. *Fixemos* $i \in \{1, \ldots, k\}$ *e suponhamos* $i > 1$. *Facilmente, temos que* $p_i \in X \setminus \big(p_1\mathbb{Z} \cup \cdots \cup p_{i-1}\mathbb{Z}\big)$. *Agora tomemos* $z \in X \setminus \big(p_1\mathbb{Z} \cup \cdots \cup p_{i-1}\mathbb{Z}\big)$. *Caso* z *seja primo e* $z^2 > x$, *então* $z > p_k \geq p_i$. *Caso* $z^2 \leq x$, *temos que* $z = p_j$, *para algum* $j \in \{1, \ldots, k\}$. *Como* $z \notin \big(p_1\mathbb{Z} \cup \cdots \cup p_{i-1}\mathbb{Z}\big)$, *então* $j \geq i$. *Daí* $p_i \leq p_j = z$. *Se* z *for composto, existe* $u \in \mathbb{N}$ *tal que* u *é primo,* $u|z$ *e* $u^2 \leq z$. *Dado que* $z \leq x$, $u \in \{p_1, \ldots, p_k\}$. *Como* $z \in u\mathbb{Z}$, *mas* $z \notin \big(p_1\mathbb{Z} \cup \cdots \cup p_{i-1}\mathbb{Z}\big)$, *temos que* $u \in \{p_i, \ldots, p_k\}$. *Daí* $z \geq u \geq p_i$. *Concluímos que* $p_i = \min\Big(X \setminus \big(p_1\mathbb{Z} \cup \cdots \cup p_{i-1}\mathbb{Z}\big)\Big)$.

O observado no parágrafo anterior mostra que podemos "descobrir" p_2 *a partir de* X *e* p_1; *que podemos determinar* p_3 *a partir de* X, p_1 *e* p_2; *e assim por diante, podemos determinar* p_i *a partir de* X, p_1, $\ldots$, *e* p_{i-1}, *enquanto* $p_i^2 \leq x$.

Para exemplificar o uso do Crivo, determinemos os primos entre 2 *e* 101. *Representamos abaixo* $X = \{i \in \mathbb{N} \colon 2 \leq i \leq 101\}$:

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	101

Temos que $p_1 = 2$ *e* $X \setminus 2\mathbb{Z}$:

3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41
43	45	47	49	51	53	55	57	59	61	63	65	67	69	71	73	75	77	79	81
83	85	87	89	91	93	95	97	99	101										

Temos que $p_2 = 3 = \min\big(X \setminus 2\mathbb{Z}\big)$ *e agora devemos fazer* $X \setminus \big(2\mathbb{Z} \cup 3\mathbb{Z}\big) = \big(X \setminus 2\mathbb{Z}\big) \setminus 3\mathbb{Z}$:

5	7	11	13	17	19	23	25	29	31	35	37	41	43	47	49	53	55	59	61
65	67	71	73	77	79	83	85	89	91	95	97	101							

Temos que $p_3 = 5 = \min\Big(X \setminus \big(2\mathbb{Z} \cup 3\mathbb{Z}\big)\Big)$ *e agora devemos fazer* $\Big(\big(X \setminus 2\mathbb{Z}\big) \setminus 3\mathbb{Z}\Big) \setminus 5\mathbb{Z}$:

7	11	13	17	19	23	29	31	37	41	43	47	49	53	59	61	67	71	73	77
79	83	89	91	97	101														

Temos que $p_4 = 7 = \min\Big(X \setminus \big(2\mathbb{Z} \cup 3\mathbb{Z} \cup 5\mathbb{Z}\big)\Big)$ *e* $\Big(\Big(\big(X \setminus 2\mathbb{Z}\big) \setminus 3\mathbb{Z}\Big) \setminus 5\mathbb{Z}\Big) \setminus 7\mathbb{Z}$:

11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	101

Uma vez que $11^2 = 121 > 101$, *não precisamos continuar com as eliminações. Logo os números primos entre* 2 *e* 101 *são* 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 *e* 101.

Exercício 56. *Apresente todos os números naturais primos menores ou iguais a* 200. *Quanto são?*

Exercício 57. *Determine se os seguintes números são primos e, nos casos contrários, apresente sua decomposição em fatores primos.*

(1) 181 *(2)* 227 *(3)* 327 *(4)* 311 *(5)* 659 *(6)* 176 *(7)* 1888 *(8)* 1211 *(9)* 2057 *(10)* 3129 *(11)* 4229 *(12)* 5041

Exercício 58. *O número* 2771 *é primo? Se for o caso, justifique sua resposta; caso contrário, encontre a fatoração de* 2771 *em primos.*

Proposição 48. *Sejam $p, \alpha, \beta \in \mathbb{N}$ onde p é primo. Então*

$$\mathrm{mdc}(p^\alpha, p^\beta) = p^\gamma \qquad e \qquad \mathrm{mmc}(p^\alpha, p^\beta) = p^\delta,$$

onde $\gamma = \min\{\alpha, \beta\}$ e $\delta = \max\{\alpha, \beta\}$.

Demonstração. Sem perda de generalidade, suponhamos que $\alpha \leq \beta$. Sendo assim, $p^\alpha | p^\beta$. □

Corolário 49. *Sejam $p_1, \ldots, p_n, \alpha_1 \ldots, \alpha_n, \beta_1 \ldots, \beta_n, \in \mathbb{N}$ onde p_1,...,p_n são primos e $2 \leq p_1 < \cdots < p_n$. Então*

$$\mathrm{mdc}(p_1^{\alpha_1} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n}) = p_1^{\gamma_1} \cdots p_n^{\gamma_n} \qquad e \qquad \mathrm{mmc}(p_1^{\alpha_1} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n}) = p_1^{\delta_1} \cdots p_n^{\delta_n},$$

onde $\gamma_i = \min\{\alpha_1, \ldots, \alpha_n\}$ e $\delta_i = \max\{\alpha_1, \ldots, \alpha_n\}$, para cada $i \in \{1, \ldots, n\}$.

Demonstração. Basta usar a proposição anterior e o exercício 25. Para o resultado sobre mínimo múltiplo comum, basta usar o teorema 30 ou o exercício 33. □

Exercício 59. *Qual é o expoente do* 2 *no número* 100! *(*100 *fatorial)? Qual é o expoente do* 5 *no número* 100! *? Com quantos zeros termina o número* 100! *?*

Exercício 60. *Sejam $a, b, p \in \mathbb{N} \setminus \{0, 1\}$ e suponha p é primo. Mostre que $p|\mathrm{mmc}(a, b)$ se, e somente se, p é divide a **ou** p divide b. Generalize o resultado para p^n, onde $n \in \mathbb{N}^*$.*

Exercício 61. *Sejam $a, b, p \in \mathbb{N} \setminus \{0, 1\}$ e suponha p é primo. Mostre que $p|\mathrm{mdc}(a, b)$ se, e somente se, p é divide a **e** p divide b. Generalize o resultado para p^n, onde $n \in \mathbb{N}^*$.*

8. Congruências

Definição 11. *Sejam $m, a, b \in \mathbb{Z}$. Dizemos que a **e** b **são congruentes módulo** m – situação denotada por $a \equiv b \pmod m$ – se, e somente se, $m|a - b$.*

Observamos que

$$a \equiv b \pmod m \quad \Leftrightarrow \quad a - b \in m\mathbb{Z} \quad \Leftrightarrow \quad a - b \in |m|\mathbb{Z} \quad \Leftrightarrow \quad a \equiv b \pmod{|m|}\ .$$

Portanto podemos somente falar em congruência módulo m, para $m \in \mathbb{N}$. Se $m = 0$, temos que

$$a \equiv b \pmod 0 \qquad \Leftrightarrow \qquad 0|a - b \qquad \Leftrightarrow \qquad 0 = a - b \qquad \Leftrightarrow \qquad a = b\ .$$

Logo congruência módulo 0 corresponde exatamente à igualdade. Tomando $m = 1$, temos que

$$a \equiv b \pmod 1 \qquad \Leftrightarrow \qquad 1|a - b\ ,$$

fato que sempre acontece. Sendo assim, congruências verdadeiramente interessantes serão sempre módulo $m \in \mathbb{N}$ e $m \geq 2$.

Proposição 50. *A relação $\equiv$ é relação de **equivalência**.*

Demonstração. Seja $a \in \mathbb{Z}$. Então $m|a - a$ e $a \equiv a \pmod m$. Logo $\equiv$ é reflexiva.

Sejam $a, b \in \mathbb{Z}$ tais que $a \equiv b \pmod m$. Daí $m|a - b$. Logo $m|b - a$ e $b \equiv a \pmod m$. Portanto $\equiv$ é simétrica.

Sejam $a, b, c \in \mathbb{Z}$ tais que $a \equiv b \pmod m$ e $b \equiv c \pmod m$. Daí $m|a - b$ e $m|b - c$. Sendo assim, $m|(a - b) + (b - c)$ e $m|a - c$, ou seja, $a \equiv c \pmod m$. Concluímos que $\equiv$ é relação transitiva. □

Na congruência módulo m, é frequente usar a notação $\overline{x}$ para a classe de equivalência do inteiro x. Sendo assim, para $x, y \in \mathbb{Z}$,

$$\overline{x} = \overline{y} \quad \Leftrightarrow \quad y \in \overline{x} \quad \Leftrightarrow \quad y \equiv x \,(\mathrm{mod}\, m) \quad \Leftrightarrow \quad \text{existe } k \in \mathbb{Z}, \text{ tal que } y = x + mk,$$

e também se costuma usar notação $x + m\mathbb{Z} = \{x + mk \colon k \in \mathbb{Z}\}$ para declarar a classe de equivalência de x. Denotamos o conjunto das classes de equivalência de congruência módulo m por Z_m ou, por vezes, $\mathbb{Z}/m\mathbb{Z}$.

Outra maneira de avaliarmos se dois números são congruentes (ou côngruos) módulo m é verificar seus restos na divisão euclidiana por m:

Proposição 51. *Seja $m \in \mathbb{Z}^*$. Se $a, b \in \mathbb{Z}$, então*

$$a \equiv b \,(\mathrm{mod}\, m) \quad \Leftrightarrow \quad \textit{a e b tem mesmo resto na divisão euclidiana por m.}$$

Demonstração. Suponhamos primeiro que $p, q, r, s \in \mathbb{Z}$ sejam tais que

$$a = pm + r, \quad b = qm + s, \quad \text{e} \quad r, s \in \{0, \ldots, m-1\} \ .$$

Se $r = s$, temos que $a - b = m(p - q)$ e $a \equiv b \,(\mathrm{mod}\, m)$. Agora suponhamos $a \equiv b \,(\mathrm{mod}\, m)$. Daí existe $u \in \mathbb{Z}$ tal que $a = b + mu$, ou seja

$$a = qm + s + um = (q + u)m + s \ .$$

Mas é resultado da divisão euclidiana que quociente e resto são únicos, logo $p = q + u$ e $r = s$. □

Corolário 52. *Seja $m \in \mathbb{Z}^*$. Se $a \in \mathbb{Z}$ e r é o resto da divisão euclidiana de a por m, então $a \equiv r \,(\mathrm{mod}\, m)$.* □

Corolário 53. *Seja $m \in \mathbb{Z}^*$. Se $x, y \in \{0, \ldots, |m| - 1\}$ e $x \equiv y \,(\mathrm{mod}\, m)$, então $x = y$.* □

Corolário 54. *Para $m \in \mathbb{Z}^*$, Z_m tem exatamente $|m|$ elementos.*

Demonstração. Temos que a função $f \colon \{0, \ldots, |m| - 1\} \longrightarrow \mathbb{Z}_m$ definida por

$$f(x) = \overline{x}$$

será injetora e im(f) $= \mathbb{Z}_m$. □

Temos a inteção de dar uma estrutura algébrica ao $\mathbb{Z}_m$, ou seja, definir soma e produto e verificar quais propriedades estas operações satisfarão. Para tanto precisamos de alguns resultados antes.

Proposição 55. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \equiv b \,(\mathrm{mod}\, m)$, então $a + c \equiv b + c \,(\mathrm{mod}\, m)$ e $ac \equiv bc \,(\mathrm{mod}\, m)$.*

Demonstração. Se $a \equiv b \,(\mathrm{mod}\, m)$, então existe $q \in \mathbb{Z}$, tal que $a - b = qm$. Daí $(a + c) - (b + c) = qm$ e $ac - bc = (a - b)c = qcm$, ou seja, $a + c \equiv b + c \,(\mathrm{mod}\, m)$ e $ac \equiv bc \,(\mathrm{mod}\, m)$. □

Corolário 56. *Se $a \equiv b \,(\mathrm{mod}\, m)$ e $c \equiv d \,(\mathrm{mod}\, m)$, então $a + c \equiv b + d \,(\mathrm{mod}\, m)$ e $ac \equiv bd \,(\mathrm{mod}\, m)$.*

Demonstração. Suponhamos $a \equiv b \,(\mathrm{mod}\, m)$ e $c \equiv d \,(\mathrm{mod}\, m)$. Pela proposição anterior temos que

$$a + c \equiv b + c \,(\mathrm{mod}\, m) \qquad \text{e} \qquad b + c \equiv b + d \,(\mathrm{mod}\, m) \ .$$

Logo $a + c \equiv b + d \,(\mathrm{mod}\, m)$.

Ainda $ac \equiv bc \,(\mathrm{mod}\, m)$ e $bc \equiv bd \,(\mathrm{mod}\, m)$, logo $ac \equiv bd \,(\mathrm{mod}\, m)$. □

Exercício 62. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$ tal que $m > 1$. Suponha que $a \equiv b \pmod m$. Mostre que, para todo $n \in \mathbb{N}$, $a^n \equiv b^n \pmod m$.*

Exercício 63. *Determine o resto da divisão:*
(1) de 12^{12} por 5 *(2) de 7^{21} por 127* *(3) de 2^{100} por 11*

Exercício 64. *(1) Determine os restos da divisão de 10^2, 10^3 e 10^5 por 13.*
(2) Mostre que, para $x, r, s \in \mathbb{Z}$,

$$10x + r \equiv s \pmod{13} \quad \text{se, e só se,} \quad x + 4r \equiv 4s \pmod{13} \ .$$

(3) Determine, usando o "critério" estabelecido no item anterior, o resto da divisão de 2168 por 13.

Exercício 65. *Mostre que se $a \in \mathbb{Z}$ **não** é divisível por 3, então a^2 deixa resto 1 na divisão por 3.*

Exercício 66. *Mostre que se $a \in \mathbb{Z}$ **não** é divisível por 5, então a^4 deixa resto 1 na divisão por 5.*

Exercício 67. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}^*$. Mostre que, se $a \equiv b \pmod m$, então $\text{mdc}(a, m) = \text{mdc}(b, m)$.*

Agora queremos resolver equações da forma $ax \equiv b \pmod n$.

Proposição 57. *Seja $n \in \mathbb{N}^*$ e $a, b \in \mathbb{Z}$. A equação $ax \equiv b \pmod n$ tem solução se, e somente se, $\text{mdc}(a, n)|b$. Em particular, se $\text{mdc}(a, n) = 1$ e x_0 é solução da equação, então $ax \equiv b \pmod n$ se, e somente se, $x \equiv x_0 \pmod n$.*

Demonstração. Suponhamos que exista $x \in \mathbb{Z}$ tal que $ax \equiv b \pmod n$. Sendo assim, $n|ax - b$ e existe $y \in \mathbb{Z}$ tal que $ny = ax - b$, ou equivalentemente, $ax - ny = b$. Por resultado anterior, temos que $\text{mdc}(a, -n) = \text{mdc}(a, n)|b$.

Suponha que $\text{mdc}(a, n)|b$. Sendo assim, existem $u, v \in \mathbb{Z}$ tais que $au - nv = b$. Logo $n|au - b$ e $au \equiv b \pmod n$. Portanto u resolve a equação $ax \equiv b \pmod n$.

Agora suponhamos $\text{mdc}(a, n) = 1$ e seja $x_0 \in \mathbb{Z}$ tal que $ax_0 \equiv b \pmod n$. Observamos que, para $x \in \mathbb{Z}$,

$$ax \equiv b \pmod n \Leftrightarrow ax \equiv ax_0 \pmod n \Leftrightarrow n|a(x - x_0) \ .$$

Dado que $\text{mdc}(a, n) = 1$, temos que

$$n|a(x - x_0) \Leftrightarrow n|x - x_0 \Leftrightarrow x \equiv x_0 \pmod n \ .$$

Concluímos que x é solução de $ax \equiv b \pmod n$ se, e somente se, $x \equiv x_0 \pmod n$. □

Exemplo 11. *Resolvamos a equação $2x \equiv 3 \pmod 5$. Dado que $\text{mdc}(2, 5) = 1$, temos que esta equação admite solução. Logo estamos procurando $x, y \in \mathbb{Z}$ tais que $2x = 1 + 5y$. Observamos que*

$$2x - 5y = 3 = 5 - 2 \Leftrightarrow 2(x + 1) = 5(1 + y) \Leftrightarrow \begin{cases} x + 1 = 5k \\ 1 + y = 2k \end{cases} \Leftrightarrow \begin{cases} x = 5k - 1 \\ y = 2k - 1 \end{cases} \text{, para algum } k \in \mathbb{Z}.$$

Portanto, as soluções são os números da forma $x = 5k - 1$, para $k \in \mathbb{Z}$.

Exercício 68. *Resolva as equações em $x \in \mathbb{Z}$:*
(1) $2x \equiv 4 \pmod 5$ *(2) $3x \equiv 7 \pmod 9$* *(3) $3x \equiv 7 \pmod 8$* *(4) $4x \equiv 8 \pmod{12}$*

Exercício 69. *Sejam $a, b, m_1, m_2 \in \mathbb{Z}$. Mostre que*

$$\begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{cases} \quad \Leftrightarrow \quad a \equiv b \pmod{\text{mmc}(m_1, m_2)} \ .$$

9. Teorema do Resto Chinês

Queremos resolver sistemas de congruência do tipo

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \end{cases}, \quad \text{para } x \in \mathbb{Z}.$$

Teorema 58 (Teorema do Resto Chinês)**.** *Sejam $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ e $n_1, n_2 \in \mathbb{N}^*$ tais que $\text{mdc}(a_1, n_1) = 1 = \text{mdc}(a_2, n_2) = \text{mdc}(n_1, n_2)$. Então o sistema*

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \end{cases}, \quad \textit{para } x \in \mathbb{Z},$$

tem solução. Ainda, se x' é solução do sistema, então x é solução do sistema se, e somente se, $x \equiv x' \pmod{n_1n_2}$.

Demonstração. Como $\text{mdc}(a_1, n_1) = 1 = \text{mdc}(a_2, n_2)$, temos que as equações, separadamente, admitem soluções. Sejam $x_1, x_2 \in \mathbb{Z}$ tais que

$$a_1x_1 \equiv b_1 \pmod{n_1} \qquad \text{e} \qquad a_2x_2 \equiv b_2 \pmod{n_2}\ .$$

Tomemos a equação diofantina $n_1y - n_2z = x_2 - x_1$. Dado que $\text{mdc}(n_1, n_2) = 1$, temos que existem $y_0, z_0 \in \mathbb{Z}$ tais que $n_1y_0 - n_2z_0 = x_2 - x_1$. Seja $x_0 = x_1 + n_1y_0 = x_2 + n_2z_0$. Logo

$$a_1x_0 - b_1 = a_1x - b_1 + a_1n_1y_0 \in n_1\mathbb{Z}, \quad \text{pois } a_1x - b_1 \in n_1\mathbb{Z}.$$

Ou seja, $a_1x_0 \equiv b_1 \pmod{n_1}$. Analogamente temos que $a_2x_0 \equiv b_2 \pmod{n_2}$. Portanto, x_0 é solução para o sistema.

Fixemos x', solução do sistema. Observamos que

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \end{cases} \Leftrightarrow \begin{cases} a_1x \equiv a_1x' \pmod{n_1} \\ a_2x \equiv a_2x' \pmod{n_2} \end{cases} \Leftrightarrow \begin{cases} n_1 | a_1(x - x') \\ n_2 | a_2(x - x') \end{cases}.$$

Como $\text{mdc}(a_1, n_1) = 1 = \text{mdc}(a_2, n_2)$, temos que

$$\begin{cases} n_1 | a_1(x - x') \\ n_2 | a_2(x - x') \end{cases} \Leftrightarrow \begin{cases} n_1 | (x - x') \\ n_2 | (x - x') \end{cases} \Leftrightarrow x - x' \in n_1\mathbb{Z} \cap n_2\mathbb{Z}\ .$$

Dado $\text{mdc}(n_1, n_2) = 1$, temos que $\text{mmc}(n_1, n_2) = n_1n_2$. Portanto $n_1\mathbb{Z} \cap n_2\mathbb{Z} = (n_1n_2)\mathbb{Z}$. Logo x é solução do sistema se, e somente, $x \equiv x' \pmod{n_1n_2}$. □

Exemplo 12. *Resolvamos o sistema*

$$\begin{cases} 3x \equiv 2 \pmod{4} \\ 5x \equiv 1 \pmod{7} \end{cases}.$$

Observamos que $3x \equiv 2 \pmod{4}$ se, e somente se, $3x - 2 = 4y$, para algum $y \in \mathbb{Z}$. Temos que

$$3x - 4y = 2 = 8 - 6 \Leftrightarrow 3(x + 2) = 4(y + 2) \Rightarrow x = -2 + 4k, \quad \textit{para algum } k \in \mathbb{Z}.$$

Substituindo na segunda equação, temos que, $5x \equiv -10 + 20k \equiv 1 \pmod{7}$, ou seja, $20k \equiv 11 \equiv 4 \pmod{7}$. Portanto, $7|20k - 4 = 4(5k - 1)$ e, para algum $q \in \mathbb{Z}$, temos $7q = 5k - 1$. Observamos que

$$7q - 5k = -1 = 14 - 15 \Leftrightarrow 7(q - 2) = 5(k - 3)\ .$$

Logo $k - 3 = 7p$, para algum $p \in \mathbb{Z}$. Sendo assim,

$$x = -2 + 4k = -2 + 4(3 + 7p) = 10 + 28p\ .$$

Exercício 70. *Determine quais $x \in \mathbb{Z}$ satisfazem $x \equiv 1 \pmod 7$ e $x \equiv 2 \pmod 3$.*

Exercício 71. *Ache o menor múltiplo positivo de 5 que deixa resto 2 quando dividido por 3 e por 4.*

Exercício 72. *Subindo uma escada de dois em dois degraus, sobra um degrau. Subindo a mesma escada de três em três degraus, sobram dois degraus. Determine quantos degraus possi a escada, sabendo que o seu número de degraus é múltiplo de 7 e está compreendido entre 40 e 100.*

Corolário 59. *Sejam $a_1, \ldots, a_n, b_1, \cdots, b_n \in \mathbb{Z}$ e $m_1, \ldots, m_n \in \mathbb{N}^*$ tais que $\mathrm{mdc}(a_i, m_i) = 1 = \mathrm{mdc}(m_i, m_j)$, para todo $i, j \in \{1, \ldots, n\}$, com $i \neq j$. O sistema*

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases}$$

tem solução única a menos de congruência módulo $m_1 m_2 \cdots m_n$.

Demonstração. Demonstremos esse teorema por indução em n, o número de equações do sistema. Nitidamente o sistema tem solução única a menos de congruência m_1, para $n = 1$, pela proposição 57. Suponhamos que o teorema seja verdadeiro para todo sistema de n equações nas condições propostas. Fixemos $a_1, \ldots, a_{n+1}, b_1, \ldots, b_{n+1} \in \mathbb{Z}$ e $m_1, \ldots, m_{n+1} \in \mathbb{N}^*$ tais que $\mathrm{mdc}(a_i, m_i) = 1 = \mathrm{mdc}(m_i, m_j)$, para todo $i, j \in \{1, \ldots, n+1\}$, com $i \neq j$. Fixemos u_1 uma solução das n primeiras equações e seja $m = m_1 \cdots m_n$. Pelo Teorema do Resto Chinês,

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases} \Leftrightarrow x \equiv u_1 \pmod m .$$

Portanto

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_n x \equiv b_n \pmod{m_n} \\ a_{n+1} x \equiv b_{n+1} \pmod{m_{n+1}} \end{cases} \Leftrightarrow \begin{cases} x \equiv u_1 \pmod m \\ a_{n+1} x \equiv b_{n+1} \pmod{m_{n+1}} \end{cases} .$$

Uma vez que $\mathrm{mdc}(a_i, m_i) = 1 = \mathrm{mdc}(m_i, m_j)$, para todo $i, j \in \{1, \ldots, n+1\}$, com $i \neq j$, temos que $\mathrm{mdc}(m, m_{n+1}) = 1$ e consequentemente $M = \mathrm{mmc}(m, m_{n+1}) = m \cdot m_{n+1}$. Pelo Teorema do Resto Chinês, este último sistema tem solução e se x_0 é solução dele, então

$$\begin{cases} x \equiv u_1 \pmod m \\ a_{n+1} x \equiv b_{n+1} \pmod{m_{n+1}} \end{cases} \Leftrightarrow x \equiv x_0 \pmod M .$$

Vale lembrar que $M = m_1 \cdots m_n \cdot m_{n+1}$. □

Exercício 73. *Um general chinês possuía 1200 tropas antes da guerra. Após a guerra, ele alinhou as tropas de 5 em 5 de forma que sobraram 3 tropas. Quando alinhou de 6 em 6, também sobraram 3 tropas. Quando alinhou de 7 em 7, sobrou 1 tropa. Quantas tropas restaram ao general sabendo que ele ainda tinha mais de 1000 tropas?*

Exercício 74. *Ache o menor natural que deixa restos* 5, 4, 3 *e* 2 *quando dividido, respectivamente, por* 6, 5, 4 *e* 3.

10. Funções definidas em $\mathbb{Z}_m$

Quando fixamos $m \in \mathbb{N}$, fica naturalmente definida uma função de $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_m$ dada por

$$\pi(x) = \overline{x} \quad , \qquad \text{para } x \in \mathbb{Z},$$

que é chamada de **projeção canônica de $\mathbb{Z}$ em $\mathbb{Z}_m$**. Observamos que $\mathrm{im}(\pi) = \mathbb{Z}_m$. Se $f\colon \mathbb{Z}_m \longrightarrow A$ é uma função, naturalmente teremos que a composta $f \circ \pi$ que será função de $\mathbb{Z}$ em A satisfazendo:

$$(\forall x, y \in \mathbb{Z})\Big(\; x \equiv y \,(\mathrm{mod}\, m) \quad \Rightarrow \quad f(\pi(x)) = f(\pi(y)) \; \Big) \; ,$$

ou seja, $(f \circ \pi)(x) = (f \circ \pi)(y)$, sempre que x e y são inteiros congruentes módulo m. Essa condição é também suficiente para existência de função com domínio $\mathbb{Z}_m$

Teorema 60. *Sejam $F\colon \mathbb{Z} \longrightarrow A$ uma função e $m \in \mathbb{N}$. Se F satisfaz*

$$(\forall x, y \in \mathbb{Z})\Big(\; x \equiv y \,(\mathrm{mod}\, m) \quad \Rightarrow \quad F(x) = F(y) \; \Big) \; ,$$

então existe única $f\colon \mathbb{Z}_m \longrightarrow A$ tal que $f \circ \pi = F$. Ainda $\mathrm{im(f)} = \mathrm{im(F)}$.

Demonstração. Seja $f = \Big\{(a, b) \in \mathbb{Z}_m \times A\colon (\exists x \in \mathbb{Z})\Big(\; a = \overline{x} \; \wedge \; b = F(x) \; \Big)\Big\}$. Temos que:

(1) f é relação de domínio $\mathbb{Z}_m$ e com contradomínio A. De fato, $\mathrm{dom(f)} \subseteq \mathbb{Z}_m$. Ainda, se $a \in \mathbb{Z}_m$, temos que $a = \overline{x}$ para algum $x \in \mathbb{Z}$. Logo $(a, F(x)) \in f$. Nitidamente $\mathrm{im(f)} \subseteq A$.
(2) f é função. Suponha que $(a, b), (a, c) \in f$. Sendo assim, existem $x, y \in \mathbb{Z}$ tais que

$$a = \overline{x}, \quad b = F(x), \quad a = \overline{y} \quad \text{e} \quad c = F(y) \; .$$

Mas, nesse caso, $x \equiv y \,(\mathrm{mod}\, m)$, o que nos leva a $b = F(x) = F(y) = c$.

Fixemos $x \in \mathbb{Z}$ e seja $b = F(x)$. Daí o par $(\overline{x}, b) = (\pi(x), b) \in f$ e

$$(f \circ \pi)(x) = f(\pi(x)) = b = F(x) \; .$$

Acabamos de mostrar que, para todo $x \in \mathbb{Z}$, $(f \circ \pi)(x) = F(x)$, ou seja, $f \circ \pi = F$.

Agora suponhamos que exista $g\colon \mathbb{Z}_m \longrightarrow A$ tal que $g \circ \pi = F$. Fixemos $a \in \mathbb{Z}_m$. Daí, $a = \overline{x}$, para algum $x \in \mathbb{Z}$. Logo

$$g(a) = g(\overline{x}) = g(\pi(x)) = (g \circ \pi)(x) = F(x) = (f \circ \pi)(x) = f(\pi(x)) = f(\overline{x}) = f(a) \; .$$

Logo $g(a) = f(a)$, para todo $a \in \mathbb{Z}_m$, ou equivalentemente, $g = f$.

Seja $b \in \mathrm{im(F)}$. Daí, $b = F(x)$ para algum $x \in \mathbb{Z}$. Logo $b = F(x) = f(\pi(x))$ e $b \in \mathrm{im(f)}$. Por outro lado, se $c \in \mathrm{im(f)}$, temos que $c = f(a)$, para algum $a \in \mathbb{Z}_m$. Fixemos $y \in \mathbb{Z}$ tal que $a = \overline{y}$. Daí $c = f(a) = f(\pi(y)) = F(y) \in \mathrm{im(F)}$. Concluímos que $\mathrm{im(f)} = \mathrm{im(F)}$. □

Corolário 61. *Nas condições do teorema anterior, temos que f é injetora se, e só se,*

$$(\forall x, y \in \mathbb{Z})\Big(\; x \equiv y \,(\mathrm{mod}\, m) \Leftrightarrow F(x) = F(y) \; \Big).$$

Demonstração. Suponhamos que $(\forall x, y \in \mathbb{Z})\Big(\ x \equiv y \,(\mathrm{mod}\, m) \Leftrightarrow F(x) = F(y)\ \Big)$ e sejam $p, q \in \mathbb{Z}_m$ tais que $f(p) = f(q)$. Sejam $r, s \in \mathbb{Z}$ tais que $\overline{r} = p$ e $\overline{s} = q$. Logo

$$F(r) = f(\overline{r}) = f(p) = f(q) = f(\overline{s}) = F(s)\ .$$

Da suposição temos que $r \equiv s \,(\mathrm{mod}\, m)$, ou seja, $p = \overline{r} = \overline{s} = q$. Temos que f é injetora.

Agora suponhamos que f seja função injetora. Pela discussão prévia ao teorema, temos que $(\forall x, y \in \mathbb{Z})(\ x \equiv y \,(\mathrm{mod}\, m) \Rightarrow F(x) = F(y)\ )$. Fixemos $x, y \in \mathbb{Z}$ tais que $F(x) = F(y)$. Sendo assim, $f(\pi(x)) = F(x) = F(y) = f(\pi(y))$. Uma vez que f foi suposta injetora, temos $\overline{x} = \overline{y}$, ou seja, $x \equiv y \,(\mathrm{mod}\, m)$. □

11. Aritmética em $\mathbb{Z}_m$

Em $\mathbb{Z}_m$, podemos definir a soma e produto:

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{x + y} \\ \overline{x} \cdot \overline{y} &= \overline{x \cdot y}\ , \end{aligned}$$

onde $x, y \in \mathbb{Z}$. Observamos que temos total liberdade de escolha nos representantes, uma vez que, se $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$, teremos $x \equiv a \,(\mathrm{mod}\, m)$ e $y \equiv b \,(\mathrm{mod}\, m)$, donde se conclui, $x + y \equiv a + b \,(\mathrm{mod}\, m)$ e $xy \equiv ab \,(\mathrm{mod}\, m)$ e, consequentemente, $\overline{x + y} = \overline{a + b}$ e $\overline{xy} = \overline{ab}$.

Teorema 62. *Para $a, b, c \in \mathbb{Z}_m$, temos:*

(1) $x + y = y + x$;
(2) $x + (y + z) = (x + y) + z$;
(3) $x + \overline{0} = x$;
(4) existe $u \in \mathbb{Z}_m$ tal que $x + u = \overline{0}$.
(5) $xy = yx$;
(6) $x(yz) = (xy)z$;
(7) $\overline{1} \cdot x = x$; *e*
(8) $(x + y)z = xy + yz$. □

Todos os oito itens do teorema anterior provam que $\mathbb{Z}_m$ é um **anel abeliano (ou comutativo) com unidade**. Uma vez que valem essas propriedades, pode-se demonstrar vários resultados análogos aos demonstrados para $\mathbb{Z}$, a saber: unicidade dos elementos neutros ($\overline{0}$ e $\overline{1}$), lei do cancelamento para a soma e construção da subtração.

Tomemos $m \in \mathbb{Z}^*$ e vejamos quando $\mathbb{Z}_m$ é **domínio de integridade**, ou seja, quando que vale a **lei do cancelamento para o produto**. Analisemos a equação $ax = \overline{0}$, para $a, x \in \mathbb{Z}_m$. Se $a = \overline{u}$ e $x = \overline{v}$, para $u, v \in \mathbb{Z}$, teremos que

$$ax = \overline{uv} = \overline{0} \qquad \Leftrightarrow \qquad uv \equiv 0 \,(\mathrm{mod}\, m) \qquad \Leftrightarrow \qquad m | uv\ .$$

Se $|m| = 1$, temos que $\mathbb{Z}_m$ é unitário e não há o que ser discutido. Caso $m = 0$, $\mathbb{Z}_m$ é uma "cópia" de $\mathbb{Z}$ e se comporta algebricamente da mema maneira. Quando $|m|$ é **composto**, ou seja, quando $|m| = pq$, para $p, q \in \mathbb{N}$ tais $1 << p \leq q < m$, teremos $\overline{pq} = \overline{|m|} = \overline{0}$. Sendo assim, se m é composto, é possível encontrar elementos ambos não nulos cujo produto é nulo.

Teorema 63. *Sejam $m \in \mathbb{Z}^*$. Para $a \in \mathbb{Z}_m$, a tem inverso (ou oposto multiplicativo) se, e somente se, $a = \overline{x}$, para $x \in \mathbb{Z}$ primo relativo a m (ou seja,* $\mathrm{mdc}(x, m) = 1$*).*

Demonstração. Suponha que a tem oposto multiplicativo. Então existem $x, y \in \mathbb{Z}$, tais que $a = \overline{x}$ e $\overline{xy} = \overline{1}$, ou seja, $xy \equiv 1 \,(\mathrm{mod}\, m)$. Pela proposição 57, $\mathrm{mdc}(x, m) | 1$, ou seja, x e m são primos entre si.

Reciprocamente, se $a = \overline{x}$, tal que $\mathrm{mdc}(x, m) = 1$, temos que existem $y \in \mathbb{Z}$ tais que $xy \equiv 1 \,(\mathrm{mod}\, m)$, pela mesma proposição 57. Portanto $\overline{1} = \overline{xy} = \overline{x} \cdot \overline{y}$ e a admite inverso multiplicativo. □

Corolário 64. *Seja $p \in \mathbb{N}$, primo. Mostre que, para todo $a \in \mathbb{Z}_p \setminus \{\overline{0}\}$, a admite um inverso multiplicativo, ou seja, exsite $y \in \mathbb{Z}_p$, tal que $ay = \overline{1}$. Portanto $\mathbb{Z}_p$ é **corpo**.*

Demonstração. Fixemos $a \in \mathbb{Z}_p$, tal que $a \neq \overline{0}$. Temos que $a = \overline{x}$, para $x \in \mathbb{Z}$. Como p não divide x, temos que $\text{mdc}(p, x) = 1$. Pelo teorema anterior, a tem inverso. □

12. A função fi de Euler

A **função fi de Euler** (ou **função totiente**) é definida a seguir e conta quanto elementos inversíveis há em $\mathbb{Z}_n$. A princípio pode parecer que sua definição é mera curiosidade mas ela tem outra aplicações e algums dessas colocaremos aqui.

Definição 12. *Para $n \in \mathbb{N}^*$, $\varphi(n) = |\{i \in \mathbb{N} \colon i < m \ \wedge \ \text{mdc}(i, n) = 1\}|$.*

Para facilitar referências futuras, para $n \in \mathbb{N}^*$, definiremos $U_n = \{i \in \mathbb{N} \colon i < n \ \wedge \ \text{mdc}(i, n) = 1\}$. Uma vez que o teorema 63 relacionou elementos primos relativos a m com os elementos inversíveis de $\mathbb{Z}_n$, aproveitamos para definir o conjunto das unidades de A, onde A é um anel:

Definição 13. *Se A é um anel com identidade $\mathbf{1}$. Definimos o conjunto das unidades de A – denotado por $U(A)$ – como sendo o conjunto*

$$U(A) = \{x \in A \colon (\exists y \in A)(\ xy = yx = \mathbf{1}\ )\} \ .$$

Portanto o teorema 63 mostrou que, para $n \in \mathbb{N}^*$, com $n > 1$,

$$\varphi(n) = |(U(\mathbb{Z}_n))| \ .$$

Facilmente, vemos que $\varphi(1) = 1$ e que $1 \leq \varphi(n) \leq n - 1$, para todo $n \in \mathbb{N}$, $n \geq 2$. Pelo corolário 64, temos que, se $p \in \mathbb{N}$ é primo, então $\varphi(p) = p - 1$. Gostaríamos de calcular $\varphi(n)$ para qualquer natural composto.

Teorema 65. *Sejam $n, p \in \mathbb{N}^*$ tais que p é primo. Então $\varphi(p^n) = p^n - p^{n-1}$.*

Demonstração. Sejam

$$A = \{i \in \mathbb{N} \colon i < p^n \wedge \text{mdc}(i, p^n) \neq 1\}, \quad X = \{i \in \mathbb{N} \colon i < p^n\} \quad \text{e} \quad Y = \left\{i \in \mathbb{N} \colon i < p^{n-1}\right\}.$$

Temos que a $f \colon Y \longrightarrow X$, dada por $f(y) = py$, para $y \in Y$, é injetora e ainda $\text{im(f)} = A$. Portanto

$$\varphi(p^n) = |X \setminus A| = |X| - |A| = p^n - |Y| = p^n - p^{n-1}.$$

□

Agora vamos nos concentrar em calcular φ em outros números compostos.

Teorema 66. *Sejam $m, n \in \mathbb{N}^*$ primos entre si. Então $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demonstração. Caso $m = 1$ ou $n = 1$, temos facilmente o resultado. Portanto vamos supor que $m > 1$ e $n > 1$.

A intenção é estabelecer uma bijeção entre U_{mn} e $U_m \times U_n$, o que provaria que $\varphi(mn) = \varphi(m)\varphi(n)$. Essa bijeção será construída com o auxílio de F definida a seguir.

Seja $F \colon U_{mn} \longrightarrow \mathbb{N} \times \mathbb{N}$ dada por $f(i) = (x, y)$, onde x é o resto da divisão de i por m e y é o resto da divisão de i por n, para $i \in U_{mn}$.

Tomemos $i, j \in U_{mn}$ tais que $f(i) = f(j)$. Pela definição de f, temos que $i \equiv j \pmod m$ e $i \equiv j \pmod n$. Sendo assim, $i - j \in m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$, dado que $\text{mdc}(m, n) = 1$ e $\text{mmc}(m, n) = mn$. Logo $i \equiv j \pmod{mn}$ e $i = j$, pois $i, j \in \{0, \ldots, mn - 1\}$. Portanto provamos que f é injetora.

Tomemos $i \in U_{mn}$ e seja $x, y \in \mathbb{N}$ tais que $f(i) = (x, y)$. Como $\text{mdc}(i, mn) = 1$, temos que $\text{mdc}(i, m) = 1$. Dado que x é o resto da divisão de i por m, temos que $\text{mdc}(x, m) = 1$. Logo $x \in U_m$. Analogamente, $y \in U_n$. Logo estabelecemos que $\text{im(f)} \subseteq U_m \times U_n$. Agora tomemos $(a, b) \in U_m \times U_n$. Pelo Teorema do Resto Chinês, existe $y \in \mathbb{Z}$ tal que $y \equiv a \pmod m$ e $y \equiv b \pmod n$, pois $\text{mdc}(m, n) = 1$. Sendo assim, $\text{mdc}(y, m) = \text{mdc}(a, m) = 1 = \text{mdc}(y, n) = \text{mdc}(b, n)$. Logo $\text{mdc}(y, mn) = 1$. Seja k o resto da divisão de y por mn. Temos que $k \equiv y \pmod{mn}$ e $\text{mdc}(k, mn) = 1$. Logo $k \in U_{mn}$. Ainda $k \equiv y \pmod m$ e $k \equiv y \pmod n$. Sendo assim, $k \equiv a \pmod m$ e $k \equiv b \pmod n$. Portanto, $(a, b) = f(k) \in \text{im(f)}$. Concluímos que $\text{im(f)} = U_m \times U_n$.

Portanto f é uma bijeção entre U_{mn} e $U_m \times U_n$. Logo

$$\varphi(mn) = |U_{mn}| = |U_m| \cdot |U_n| = \varphi(m)\varphi(n).$$

□

Exercício 75. *Calcule a função de fi de Euler para os valores:* $3, 4, 5, 6, 9, 10, 34, 55, 67, 89, 98, 100,$ $1000, 180, 220, 320, 308, 605, 616, 1008, 1210, 2058, 3125, 4225, 5040$ *e* 1239.

Exercício 76. *(1) Sejam $n, p \in \mathbb{N}^*$ e suponha que p é primo e $p|n$. Mostre que $(p-1)|\varphi(n)$.*
(2) Resolva a equação $\varphi(n) = 1$, para $n \in \mathbb{N}^*$.
(3) Resolva a equação $\varphi(n) = 2$, para $n \in \mathbb{N}^*$ e n sendo ímpar.
(4) Resolva a equação $\varphi(n) = 2$, para $n \in \mathbb{N}^*$.

Vejamos algumas aplicações de φ.

Lema 67. *Sejam $n \in \mathbb{N}^*$ e $a \in \mathbb{Z}$ tais que $\text{mdc}(a, n) = 1$. Seja $f\colon U_n \longrightarrow \mathbb{N}$ onde $f(x)$ é o resto da divisão de ax por n, para $x \in U_n$. Então f é injetora e $\text{im(f)} = U_n$.*

Demonstração. Fixemos $x \in U_n$. Como $\text{mdc}(a, n) = 1 = \text{mdc}(x, n)$, temos que $\text{mdc}(ax, n) = 1$. Pela definição de f, $\text{mdc}(f(x), n) = 1$. Logo $f(x) \in U_n$. Portanto $\text{im(f)} \subseteq U_n$. Tomemos $b \in U_n$. Como $\text{mdc}(a, n) = 1$, temos que existe $y \in \mathbb{Z}$ tal que $ay \equiv b \pmod n$. Como $\text{mdc}(b, n) = 1$, temos que $\text{mdc}(ay, n) = 1$ e $\text{mdc}(y, n) = 1$. Seja r o resto da divisão de y por n. Então $\text{mdc}(r, n) = 1$ e $r \in U_n$. Ainda $r \equiv y \pmod n$. Logo $ar \equiv ay \pmod n$ e $ar \equiv b \pmod n$. Dado que $b \in \{0, \ldots, n - 1\}$, $b = f(r) \in \text{im(f)}$. Concluímos que $\text{im(f)} = U_n$.

Sejam $i, j \in U_n$ tais que $f(i) = f(j)$. Logo $i \equiv j \pmod n$. Dado que $i, j \in \{0, \ldots, n - 1\}$, temos que $i = j$. Sendo assim, f é injetora. □

Teorema 68 (Euler)**.** *Sejam $n \in \mathbb{N}^*$ e $a \in \mathbb{Z}$ tais que $\text{mdc}(a, n) = 1$. Então $a^{\varphi(n)} \equiv 1 \pmod n$.*

Demonstração. Sejam $k = \varphi(n)$ e $x_1, \ldots, x_k$ os k diferentes elementos de U_n. Seja f a função descrita no lema anterior. Temos que:

$$\begin{cases} ax_1 & \equiv & f(x_1) \pmod n \\ \vdots & & \vdots \\ ax_k & \equiv & f(x_k) \pmod n \end{cases}$$

Sendo assim, $a^k(x_1 \cdots x_k) = \Big((ax_1) \cdots (ax_k)\Big) \equiv \Big(f(x_1) \cdots f(x_k)\Big) \pmod{n}$. Dado que a função é bijeção entre U_n e U_n, temos que $b = (x_1 \cdots x_k) = \Big(f(x_1) \cdots f(x_k)\Big)$. Ainda, $\text{mdc}(b, n) = 1$. Logo

$$n | b\big(a^k - 1\big).$$

Já que $\text{mdc}(b, n) = 1$, temos que $n | \big(a^k - 1\big)$, ou seja, $a^k \equiv 1 \pmod{n}$. □

Corolário 69 (Pequeno Teorema de Fermat)**.** *Seja $p \in \mathbb{N}$ primo.*

(1) Para $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.
(2) Para $a \in \mathbb{Z}$, $a^{p-1} \equiv 1 \pmod{p}$ se, e somente se, $\text{mdc}(a, p) = 1$.

Demonstração. Como p é primo, $\varphi(p) = p - 1$. Tomemos $a \in \mathbb{Z}$. Se $\text{mdc}(a, p) = 1$, pelo teorema anterior, $a^{p-1} \equiv 1 \pmod{p}$. Ainda, $a^p \equiv a \pmod{p}$. Caso $\text{mdc}(a, p) \neq 1$, temos que $p | a$. Logo $p | a(a^{p-1} - 1) = a^p - a$ e $a^p \equiv a \pmod{p}$. Ainda, $a \equiv 0 \pmod{p}$ e $a^{p-1} \equiv 0 \pmod{p}$. □

Exemplo 13. *Achemos o resto da divisão de 3^{100} por 34. Temos que $\varphi(34) = \varphi(2 \cdot 17) = \varphi(2)\varphi(17) = 1 \cdot 16 = 16$. Pelo Teorema de Euler, $3^{16} \equiv 1 \pmod{34}$. Uma vez que $100 = 16 \cdot 6 + 4$, então $3^{100} = 3^{16 \cdot 6 + 3} = 3^{16 \cdot 6} \cdot 3^4 \equiv 3^4 \pmod{34}$. Dado que $3^4 \equiv 13 \pmod{34}$, temos que na divisão de 3^{100} por 34 obtemos resto 13.*

Exercício 77. *Ache o resto da divisão de*

(1) 5^{60} por 26 *(2) 3^{100} por 10*

Exercício 78. *Mostre que, para $n \in \mathbb{N}$, $n \geq 3$, temos que $\varphi(n)$ é par.*

Exercício 79. *Resolva em $m \in \mathbb{N}^*$ as equações:*

(1) $\varphi(m) = 12$ *(2) $\varphi(m) = 8$* *(3) $\varphi(m) = 16$* *(4) $\varphi(m) = 24$*

Exercício 80. *Mostre que, se n é natural não nulo qua satisfaz $\varphi(n) = n - 1$, então n é primo.*

Exercício 81. *Escrevendop $n = 2^k r$, onde r é natural ímpar, mostre que, se $2\varphi(n) = n$, então n é potência de 2.*

Exercício 82. *Mostre que, se $m | n$, então $\varphi(mn) = m\varphi(n)$.*

Exercício 83. *Sejam $m, n \in \mathbb{N}^*$ e $d = \text{mdc}(m, n)$. Mostre que $\varphi(d)\varphi(mn) = d\varphi(m)\varphi(n)$.*

Exercício 84. *Mostre que, se $d | n$, então $\varphi(d) | \varphi(n)$.*

Proposição 70. *Sejam $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$ e $I = \big\{i \in \mathbb{N} \colon a^i \equiv 1 \pmod{n}\big\}$. Então $I \neq \{0\}$ se, e somente se,* $\text{mdc}(a, n) = 1$.

Demonstração. Suponhamos que $I \neq \{0\}$ e fixemos $i \in \mathbb{N}^*$ tal que $a^i \equiv 1 \pmod{n}$. Sendo assim, $a \cdot a^{i-1} \equiv 1 \pmod{n}$. Pela proposição 57, $\text{mdc}(a, n) = 1$. Reciprocamente, se $\text{mdc}(a, n) = 1$, temos que $\varphi(n) \in I$. □

Corolário 71. *Nas mesmas condição da proposição anterior. Existe único $m \in \mathbb{N}$ tal que $I = m\mathbb{N} = \{mk \colon k \in \mathbb{N}\}$.*

Demonstração. Caso $I = \{0\}$, temos que $I = 0\mathbb{N}$. Caso $I \neq \{0\}$, seja $m = \min\{i \in I : i > 0\}$. Para $k \in \mathbb{N}$, temos que $a^{mk} \equiv 1 \pmod{n}$, já que $a^m \equiv 1 \pmod{n}$. Tomemos $i \in I$. Como $m \neq 0$, pela Divisão Euclidiana, existem $q, r \in \mathbb{N}$, tais que $i = qm + r$. Sendo assim,

$$a^i = a^{qm+r} = a^{mq} \cdot a^r \equiv a^r \equiv 1 \pmod{n}.$$

Daí $r \in I$ mas $r < m$. Logo $r = 0$ e $i \in m\mathbb{N}$.

Suponhamos que $n, n' \in \mathbb{N}$ são tais que $n\mathbb{N} = n'\mathbb{N}$. Daí $n|n'$ e $n'|n$. Como ambos são naturais, $n = n'$. □

Definição 14. *Para $a \in \mathbb{Z}$ e $n \in \mathbb{N}^*$, definimos $ord_n(a)$ como sendo o natural determinado no corolário anterior.*

Temos que $ord_1(a) = 1$, para todo $a \in \mathbb{Z}$. Para $n \geq 2$, natural, e $a \in \mathbb{Z}$, tal que $\text{mdc}(a, n) \neq 1$, $ord_n(a) = 0$.

Corolário 72. *Para $a \in \mathbb{Z}$ e $n \in \mathbb{N}^*$, se $\text{mdc}(a, n) = 1$, então $ord_n(a)|\varphi(n)$.* □

Exercício 85. *Seja $n \in \mathbb{N}^*$. Mostre que, se $a, b \in \mathbb{Z}$ são tais que $a \equiv b \pmod{n}$, então $ord_n(a) = ord_n(b)$.*

Exercício 86. *(1) Determine $ord_{17}(a)$, para $a \in \mathbb{N}$ tal que $a < 30$.*
(2) Determine $ord_{16}(a)$, para $a \in \mathbb{N}$ tal que $a < 15$.