Capítulo 1

Divisibilidade e Congruências

Neste primeiro capítulo veremos os tópicos básicos de Teoria dos Números, como divisibilidade, congruências e aritmética módulo n.

1.1 Divisibilidade

Dados dois inteiros d e a, dizemos que d *divide* a ou que d é um *divisor* de a ou ainda que a é um *múltiplo* de d e escrevemos

$$d \mid a$$

se existir $q \in \mathbb{Z}$ com $a = qd$. Caso contrário, escrevemos $d \nmid a$. Por exemplo, temos que $-5 \mid 10$ mas $10 \nmid -5$.

Eis algumas propriedades importantes da divisibilidade:

Lema 1.1. *Sejam $a, b, c, d \in \mathbb{Z}$. Temos*

(i) ("d divide") Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.

(ii) (Limitação) Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.

(iii) (Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração: Se $d \mid a$ e $d \mid b$, então podemos escrever $a = dq_1$ e $b = dq_2$ com $q_1, q_2 \in \mathbb{Z}$, logo $ax+by = d(q_1x+q_2y)$. Como $q_1x+q_2y \in \mathbb{Z}$,

Cópia eletrônica

temos $d \mid ax + by$. Para mostrar *(ii)*, suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \geq 1$ e $|a| = |d||q| \geq |d|$. Finalmente, se $a \mid b$ e $b \mid c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto $a \mid c$. □

Vejamos como utilizar estas propriedades para resolver alguns problemas de divisibilidade.

Exemplo 1.2. *Encontre todos os inteiros positivos n tais que $2n^2 + 1 \mid n^3 + 9n - 17$.*

Solução: Utilizando o "$2n^2 + 1$ divide" para reduzir o grau de $n^3 + 9n - 17$, temos que

$$\begin{aligned} &\begin{cases} 2n^2 + 1 \mid n^3 + 9n - 17 \\ 2n^2 + 1 \mid 2n^2 + 1 \end{cases} \\ \Longrightarrow\ & 2n^2 + 1 \mid (n^3 + 9n - 17) \cdot 2 + (2n^2 + 1) \cdot (-n) \\ \Longleftrightarrow\ & 2n^2 + 1 \mid 17n - 34. \end{aligned}$$

Como o grau de $17n - 34$ é menor do que o de $2n^2 + 1$, podemos utilizar a "limitação" para obter uma lista finita de candidatos a n. Temos $17n - 34 = 0 \iff n = 2$ ou $|2n^2 + 1| \leq |17n - 34| \iff n = 1, 4$ ou 5. Destes candidatos, apenas $n = 2$ e $n = 5$ são soluções. □

Exemplo 1.3 (IMO1994)**.** *Determine todos os pares (m, n) de inteiros positivos para os quais $\frac{n^3+1}{mn-1}$ é inteiro.*

Solução: Vamos tentar reduzir o grau em n utilizando o "d divide". Temos

$$\begin{aligned} mn - 1 \mid n^3 + 1 &\Longrightarrow mn - 1 \mid (n^3 + 1) \cdot m - (mn - 1) \cdot n^2 \\ &\Longleftrightarrow mn - 1 \mid n^2 + m. \end{aligned}$$

Da mesma forma,

$$\begin{aligned} mn - 1 \mid n^2 + m &\Longrightarrow mn - 1 \mid (n^2 + m) \cdot m - (mn - 1) \cdot n \\ &\Longleftrightarrow mn - 1 \mid m^2 + n \end{aligned}$$

e, finalmente,

$$\begin{aligned} mn-1 \mid m^2+n &\implies mn-1 \mid (m^2+n)\cdot m-(mn-1) \\ &\iff mn-1 \mid m^3+1 \end{aligned}$$

que é a mesma expressão com que começamos, trocando n por m. Assim, temos que a condição é simétrica em m e n e as divisibilidades acima são todas equivalentes entre si. Portanto podemos supor sem perda de generalidade que $m \geq n$. Utilizando a "limitação" temos

$$mn-1 \mid n^2+m \implies mn-1 \leq n^2+m \iff m(n-1) \leq n^2+1.$$

Se $n \neq 1$ temos $m \leq \frac{n^2+1}{n-1} = n+1+\frac{2}{n-1}$. Como estamos assumindo $m \geq n$, se $n \geq 4$ temos apenas duas possibilidades: $m = n$ ou $m = n+1$. Agora temos alguns casos a analisar.

- Se $m \geq n = 1$ devemos ter $m-1 \mid 1^2+m \implies m-1 \mid m+1-(m-1) \iff m-1 \mid 2$ e portanto $m = 2$ ou $m = 3$, ambos os casos fornecendo soluções.

- Se $m \geq n = 2$ devemos ter $2m-1 \mid 2^2+m \implies 2m-1 \mid 2(m+4)-(2m-1) \iff 2m-1 \mid 9 \iff m = 2$ ou $m = 5$, ambos os casos fornecendo soluções.

- Se $m \geq n = 3$ devemos ter $3m-1 \mid 3^2+m \implies 3m-1 \mid 3(m+9)-(3m-1) \iff 3m-1 \mid 28 \iff m = 5$, que fornece uma solução.

- Se $m = n \geq 4$ devemos ter

  $$\begin{aligned} n^2-1 \mid n^2+n &\iff n-1 \mid n \\ &\implies n-1 \mid n-(n-1) \iff n-1 \mid 1 \end{aligned}$$

  o que não é possível pois $n \geq 4$.

- Se $m = n+1 \geq 5$ devemos ter

  $$\begin{aligned} &(n+1)n-1 \mid n^2+(n+1) \\ \iff &n^2+n-1 \mid (n^2+n+1)-(n^2+n-1) \\ \iff &n^2+n-1 \mid 2 \end{aligned}$$

  o que novamente não é possível pois $n \geq 4$.

Logo as soluções (m,n) são $(1,2)$, $(2,1)$, $(1,3)$, $(3,1)$, $(2,2)$, $(2,5)$, $(5,2)$, $(3,5)$ e $(5,3)$. □

Cópia eletrônica

1.2 mdc, mmc e Algoritmo de Euclides

Dados dois números inteiros a e b com $a \neq 0$ ou $b \neq 0$, a cada um deles pode-se associar seu conjunto de divisores positivos, D_a e D_b respectivamente, e a intersecção de tais conjuntos $D_a \cap D_b$ é finita (pela "limitação") e não vazia (já que 1 pertence à intersecção). Por ser finito, $D_a \cap D_b$ possui elemento máximo, que é chamado de *máximo divisor comum* (mdc) dos números a e b. Denotamos este número por $\mathrm{mdc}(a, b)$ (alguns autores usam a notação (a, b)). Para $a = b = 0$ convencionamos $\mathrm{mdc}(0, 0) = 0$. Quando $\mathrm{mdc}(a, b) = 1$ dizemos que a e b são *primos entre si*.

Por outro lado, se denotamos por M_n o conjunto dos múltiplos positivos de n, dados dois números inteiros a e b com $a \neq 0$ e $b \neq 0$, então a intersecção $M_a \cap M_b$ é não vazia (já que $|ab|$ está na intersecção). Como os naturais são bem ordenados, $M_a \cap M_b$ possui elemento mínimo. Tal número é chamado *mínimo múltiplo comum* (mmc) de a e b e o denotaremos por $\mathrm{mmc}(a, b)$ (alguns autores escrevem $[a, b]$).

Para calcularmos o mdc e o mmc de maneira eficiente, vamos descrever o chamado *algoritmo de Euclides* ou *algoritmo das divisões sucessivas*. Primeiramente, vamos relembrar o conceito de *divisão euclidiana*, ou *divisão com resto*, que é uma das quatro operações que toda criança aprende na escola. Sua formulação precisa é: dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ com

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

Tais q e r estão unicamente determinados pelas duas condições acima (veja o argumento a seguir) e são chamados o *quociente* e *resto* da divisão de a por b. O resto r é também denotado por $a \bmod b$.

Para $x \in \mathbb{R}$, definimos o *piso* ou *parte inteira* $\lfloor x \rfloor$ de x como sendo o único $k \in \mathbb{Z}$ tal que $k \leq x < k + 1$; definimos o *teto* $\lceil x \rceil$ de x como o único $k \in \mathbb{Z}$ tal que $k - 1 < x \leq k$. Por exemplo, temos $\lfloor \sqrt{2} \rfloor = 1$, $\lceil \sqrt{2} \rceil = 2$, $\lfloor 10 \rfloor = \lceil 10 \rceil = 10$, $\lfloor -\pi \rfloor = -4$ e $\lceil -\pi \rceil = -3$. Podemos agora mostrar a existência de q e r satisfazendo as duas condições acima: basta tomar

$$q = \begin{cases} \lfloor a/b \rfloor & \text{se } b > 0 \\ \lceil a/b \rceil & \text{se } b < 0 \end{cases} \qquad \text{e} \qquad r = a - bq \quad \text{em ambos os casos}$$

e é fácil verificar que $0 \leq r < |b|$ a partir das definições das funções piso e teto. Por outro lado, se $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \leq r_1, r_2 < |b|$,

então temos que $r_2 - r_1 = b(q_1 - q_2)$ é um múltiplo de b com $|r_2 - r_1| < |b|$, portanto $r_2 - r_1 = 0$ e assim $q_1 = q_2$ também, o que prova a unicidade.

Podemos agora descrever o *algoritmo de Euclides* para calcular o mdc, que se baseia na seguinte simples observação:

Lema 1.4 (Euclides)**.** *Se $a = bq + r$, então* $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, r)$.

Demonstração: Basta mostrar que $D_a \cap D_b = D_b \cap D_r$, já que se estes conjuntos forem iguais em particular os seus máximos também serão iguais. Se $d \in D_a \cap D_b$ temos $d \mid a$ e $d \mid b$, logo $d \mid a - bq \iff d \mid r$ e portanto $d \in D_b \cap D_r$. Da mesma forma, se $d \in D_b \cap D_r$ temos $d \mid b$ e $d \mid r$, logo $d \mid bq + r \iff d \mid a$ e assim $d \in D_a \cap D_b$. □

O algoritmo de Euclides consiste na aplicação reiterada do lema acima onde q e r são o quociente e o resto na divisão de a por b (note que o lema vale mesmo sem a condição $0 \leq r < |b|$). Como os restos formam uma sequência estritamente decrescente, o algoritmo eventualmente para quando atingimos o resto 0.

Exemplo 1.5. *Calcule* $\mathrm{mdc}(1001, 109)$.

Solução: Realizando as divisões sucessivas, temos

$$\begin{aligned} 1001 &= 109 \cdot 9 + 20 \\ 109 &= 20 \cdot 5 + 9 \\ 20 &= 9 \cdot 2 + 2 \\ 9 &= 2 \cdot 4 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Assim, temos $\mathrm{mdc}(1001, 109) = \mathrm{mdc}(109, 20) = \mathrm{mdc}(20, 9) = \mathrm{mdc}(9, 2) = \mathrm{mdc}(2, 1) = \mathrm{mdc}(1, 0) = 1$. □

Exemplo 1.6. *Sejam $m \neq n$ dois números naturais. Demonstrar que*

$$\mathrm{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{se } a \text{ é par,} \\ 2 & \text{se } a \text{ é ímpar.} \end{cases}$$

SOLUÇÃO: Suponha sem perda de generalidade que $m > n$ e observe a fatoração

$$a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-2}} + 1)(a^{2^{m-3}} + 1) \dots (a^{2^n} + 1)(a^{2^n} - 1).$$

Logo $a^{2^m} + 1 = (a^{2^n} + 1) \cdot q + 2$ com $q \in \mathbb{Z}$ e assim

$$\mathrm{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \mathrm{mdc}(a^{2^n} + 1, 2)$$

que é igual a 2 se $a^{2^n} + 1$ for par, isto é, se a for ímpar, e é igual a 1 caso contrário. □

Além de servir de ferramenta computacional para o cálculo do mdc, a divisão euclidiana tem consequências teóricas importantes. O próximo teorema mostra que é sempre possível escrever o mdc de dois números como combinação linear destes (com coeficientes inteiros).

Teorema 1.7 (Bachet-Bézout)**.** *Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com*

$$ax + by = \mathrm{mdc}(a, b).$$

Portanto se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid \mathrm{mdc}(a, b)$.

DEMONSTRAÇÃO: O caso $a = b = 0$ é trivial (temos $x = y = 0$). Nos outros casos, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b:

$$I(a, b) \stackrel{\text{def}}{=} \{ax + by : x, y \in \mathbb{Z}\}.$$

Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$ (há pelo menos um elemento positivo, verifique!). Afirmamos que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \leq r < d$. Temos

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

Mas como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e portanto $d \mid m$.

Em particular, como $a, b \in I(a, b)$ temos que $d \mid a$ e $d \mid b$, logo $d \leq \mathrm{mdc}(a, b)$. Note ainda que se $c \mid a$ e $c \mid b$, então $c \mid ax_0 + by_0 \iff c \mid d$. Tomando $c = \mathrm{mdc}(a, b)$ temos que $\mathrm{mdc}(a, b) \mid d$ o que, juntamente com a desigualdade $d \leq \mathrm{mdc}(a, b)$, mostra que $d = \mathrm{mdc}(a, b)$. □

Corolário 1.8. *Sejam $a, b, c \in \mathbb{Z}$. A equação*

$$ax + by = c$$

admite solução inteira em x e y se, e somente se, $\mathrm{mdc}(a, b) \mid c$.

Demonstração: Se a equação admite solução inteira, então $\mathrm{mdc}(a, b)$ divide o lado esquerdo, logo deve dividir o direito também. Reciprocamente, se $\mathrm{mdc}(a, b) \mid c$, digamos $c = k \cdot \mathrm{mdc}(a, b)$ com $k \in \mathbb{Z}$, pelo teorema acima existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = \mathrm{mdc}(a, b)$ e multiplicando tudo por k obtemos que $x = kx_0$ e $y = ky_0$ são soluções da equação dada. □

Dados um inteiro $n > 2$ e inteiros $a_1, a_2, \ldots, a_n$, não todos nulos, definimos recursivamente

$$\mathrm{mdc}(a_1, a_2, \ldots, a_n) = \mathrm{mdc}(\mathrm{mdc}(a_1, a_2, \ldots, a_{n-1}), a_n).$$

É fácil mostrar por indução em n que este número é um divisor positivo comum de $a_1, a_2, \ldots, a_n$. Também podemos provar por indução em n que existem inteiros $x_1, x_2, \ldots, x_n$ tais que $a_1x_1 + a_2x_2 + \cdots + a_nx_n = \mathrm{mdc}(a_1, a_2, \ldots, a_n)$. De fato, pelo teorema anterior, existem u e v inteiros tais que $\mathrm{mdc}(\mathrm{mdc}(a_1, a_2, \ldots, a_{n-1}), a_n) = \mathrm{mdc}(a_1, a_2, \ldots, a_{n-1})u + a_nv$, e, se existem inteiros $y_1, y_2, \ldots, y_{n-1}$ com $a_1y_1 + a_2y_2 + \cdots + a_{n-1}y_{n-1} = \mathrm{mdc}(a_1, a_2, \ldots, a_{n-1})$, temos

$$\mathrm{mdc}(a_1, a_2, \ldots, a_n) = \mathrm{mdc}(\mathrm{mdc}(a_1, a_2, \ldots, a_{n-1}), a_n) =$$

$$= \mathrm{mdc}(a_1, a_2, \ldots, a_{n-1})u + a_nv = a_1x_1 + a_2x_2 + \cdots + a_nx_n,$$

onde $x_j = y_ju$ para $1 \leq j \leq n-1$ e $x_n = v$. Em particular, se d é um divisor comum de $a_1, a_2, \ldots, a_n$ então $d \mid \mathrm{mdc}(a_1, a_2, \ldots, a_n)$.

O corolário anterior se generaliza então da seguinte forma: dado $c \in \mathbb{Z}$, a equação

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

admite solução inteira em $x_1, x_2, \ldots, x_n$ se, e somente se, $\mathrm{mdc}(a_1, a_2, \ldots, a_n) \mid c$.

Temos uma outra importante consequência do teorema anterior:

Cópia eletrônica

Proposição 1.9. *Se* $\mathrm{mdc}(a,b) = 1$ *e* $a \mid bc$*, então* $a \mid c$*.*

Demonstração: Como $\mathrm{mdc}(a,b) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1 \implies a \cdot cx + (bc) \cdot y = c$. Do fato de a dividir cada termo do lado esquerdo, temos que $a \mid c$. □

Lembramos que um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de p são 1 e p e um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e n. Observemos que 1 não é nem primo nem composto.

Claramente, se p é primo e $p \nmid a$ temos $\mathrm{mdc}(p,a) = 1$. Usando a proposição anterior e indução temos o seguinte resultado:

Corolário 1.10. *Seja* p *um número primo e sejam* $a_1, \ldots a_m \in \mathbb{Z}$*. Se* $p \mid a_1 \cdots a_m$*, então* $p \mid a_i$ *para algum* i*,* $1 \leq i \leq m$*.*

O próximo lema resume algumas propriedades úteis do mdc:

Lema 1.11. *Temos*

1. *Se* p *é primo, então* $\mathrm{mdc}(a,p)$ *é* 1 *ou* p*.*
2. *Se* k *é um inteiro, então* $\mathrm{mdc}(a,b) = \mathrm{mdc}(a - kb, b)$*.*
3. *Se* $a \mid c$*, então* $\mathrm{mdc}(a,b) \mid \mathrm{mdc}(c,b)$*.*
4. *Se* $\mathrm{mdc}(a,b) = 1$*, então* $\mathrm{mdc}(ac,b) = \mathrm{mdc}(c,b)$*.*

Demonstração: O primeiro item é claro e o segundo é apenas uma reformulação do lema 1.4. Para provar o terceiro item, observe que $\mathrm{mdc}(a,b) \mid a$ e $a \mid c$ implicam que $\mathrm{mdc}(a,b) \mid c$. Como também temos $\mathrm{mdc}(a,b) \mid b$, concluímos que $\mathrm{mdc}(a,b) \mid \mathrm{mdc}(b,c)$ por Bachet-Bézout. Finalmente, para mostrar o último item, note primeiro que $\mathrm{mdc}(c,b) \mid \mathrm{mdc}(ac,b)$ pois $\mathrm{mdc}(c,b)$ divide simultaneamente ac e b. Reciprocamente, para mostrar que $\mathrm{mdc}(ac,b) \mid \mathrm{mdc}(c,b)$, podemos escrever $ax + by = 1$ com $x, y \in \mathbb{Z}$ por Bachet-Bézout. Assim, $\mathrm{mdc}(ac,b)$ divide $ac \cdot x + b \cdot cy = c$ e também divide b, logo divide $\mathrm{mdc}(c,b)$. □

Vejamos como podemos usar as propriedades acima para solucionar o seguinte

Exemplo 1.12. *Sejam* $a_n = 100 + n^2$ *e* $d_n = \text{mdc}(a_n, a_{n+1})$. *Calcular* d_n *para todo* n.

Solução: Aplicando a propriedade 2 temos que

$$d_n = \text{mdc}(100 + n^2, 100 + (n+1)^2) = \text{mdc}(100 + n^2, 2n + 1).$$

Como $2n + 1$ é ímpar, $\text{mdc}(4, 2n + 1) = 1$ e pelas propriedades 4 e 2 temos que

$$\begin{aligned} d_n &= \text{mdc}(400 + 4n^2, 2n + 1) \\ &= \text{mdc}(400 + 4n^2 - (2n + 1)(2n - 1), 2n + 1) \\ &= \text{mdc}(401, 2n + 1). \end{aligned}$$

Como 401 é primo, então $\text{mdc}(401, 2n+1) = 401$ se $2n+1 = 401k$ (com $k = 2r+1$ inteiro ímpar) e $\text{mdc}(401, 2n+1) = 1$ caso contrário, ou seja,

$$d_n = \begin{cases} 401 & \text{se } n = 401r + 200 \text{ com } r \in \mathbb{Z} \\ 1 & \text{caso contrário.} \end{cases}$$

□

A próxima proposição conecta o mdc e o mmc de dois inteiros e pode ser utilizada, juntamente com o algoritmo de Euclides, para o cálculo eficiente do mmc.

Proposição 1.13. *Sejam* a *e* b *dois números naturais, então*

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = a \cdot b.$$

Demonstração: Escreva $d = \text{mdc}(a, b)$ e $a = a_1 d$ e $b = b_1 d$ onde $a_1, b_1 \in \mathbb{Z}$ são tais que $\text{mdc}(a_1, b_1) = 1$. Temos $\text{mmc}(a, b) = al$ para algum $l \in \mathbb{Z}$; além disso, $b \mid \text{mmc}(a, b) \iff b_1 d \mid a_1 dl \iff b_1 \mid a_1 l$. Como $\text{mdc}(a_1, b_1) = 1$, isto implica que $b_1 \mid l$ pela proposição 1.9. Pela definição de mínimo múltiplo comum, temos que l deve ser o mínimo número divisível por b_1, assim concluímos que $l = b_1$ e portanto $\text{mmc}(a, b) = b_1 a$. Logo $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = d \cdot b_1 a = a \cdot b$. □

Cópia eletrônica

Dados um inteiro $n > 2$ e inteiros $a_1, a_2, \ldots, a_n$, não todos nulos, definimos recursivamente

$$\text{mmc}(a_1, a_2, \ldots, a_n) = \text{mmc}(\text{mmc}(a_1, a_2, \ldots, a_{n-1}), a_n).$$

É fácil mostrar por indução em n que este número é um múltiplo positivo comum de $a_1, a_2, \ldots, a_n$, e que, se m é um múltiplo comum de $a_1, a_2, \ldots, a_n$, então $\text{mmc}(a_1, a_2, \ldots, a_n) \mid m$.

A demonstração que demos do teorema de Bachet-Bézout não mostra como efetivamente encontrar uma solução de $ax + by = \text{mdc}(a, b)$. Porém, isto pode ser feito utilizando-se o algoritmo de Euclides, como mostra o exemplo a seguir. De fato, este exemplo pode servir como ponto de partida para uma segunda demonstração do teorema de Bachet-Bézout (veja os exercícios).

Exemplo 1.14. *Encontre todos os $x, y \in \mathbb{Z}$ tais que*

$$1001x + 109y = \text{mdc}(1001, 109).$$

Solução: Fazemos as divisões sucessivas para o cálculo de mdc(1001, 109) = 1 utilizando o algoritmo de Euclides (veja o exemplo 1.5). Em seguida, isolamos os restos:

$$\begin{aligned}
\boxed{20} &= \boxed{1001} - \boxed{109} \cdot 9 \\
\boxed{9} &= \boxed{109} - \boxed{20} \cdot 5 \\
\boxed{2} &= \boxed{20} - \boxed{9} \cdot 2 \\
\boxed{1} &= \boxed{9} - \boxed{2} \cdot 4
\end{aligned}$$

Note que a última divisão permite expressar o mdc 1 como combinação linear de 9 e 2:

$$\boxed{9} \cdot 1 - \boxed{2} \cdot 4 = 1.$$

Mas da penúltima divisão, temos que $\boxed{2} = \boxed{20} - \boxed{9} \cdot 2$, logo substituindo esta expressão na combinação linear acima, temos

$$\boxed{9} - (\boxed{20} - \boxed{9} \cdot 2) \cdot 4 = 1 \iff \boxed{9} \cdot 9 - \boxed{20} \cdot 4 = 1$$

e agora expressamos 1 como combinação linear de 20 e 9. Repetindo este procedimento, eventualmente expressaremos 1 como combinação linear

de 1001 e 109. Tomamos o cuidado de $\boxed{\text{lembrar}}$ quais são os "coeficientes" a e b nas equações $ax + by = \text{mdc}(a, b)$ durante as simplificações. Continuando, obtemos

$$1 = (\boxed{109} - \boxed{20} \cdot 5) \cdot 9 - \boxed{20} \cdot 4 = \boxed{109} \cdot 9 - \boxed{20} \cdot 49$$
$$1 = \boxed{109} \cdot 9 - (\boxed{1001} - \boxed{109} \cdot 9) \cdot 49 = \boxed{1001} \cdot (-49) + \boxed{109} \cdot 450.$$

Logo uma solução da equação $1001x + 109y = 1$ é $(x_0, y_0) = (-49, 450)$. Para encontrar as demais, escrevemos o lado direito desta equação utilizando a solução particular que acabamos de encontrar:

$$1001x + 109y = 1001x_0 + 109y_0 \iff 1001(x - x_0) = -109(y - y_0).$$

Como $\text{mdc}(1001, 109) = 1$ temos pela proposição 1.9 que 1001 divide $y - y_0$, ou seja, $y - y_0 = 1001t$ para algum $t \in \mathbb{Z}$ e, portanto, $x - x_0 = -109t$. Assim, as soluções da equação dada são todos os pontos da reta $1001x + 109y = 1$ da forma

$$(x, y) = (x_0 - 109t, y_0 + 1001t) = (-49, 450) + (-109, 1001) \cdot t$$

com $t \in \mathbb{Z}$. □

Em geral, o raciocínio do exemplo acima mostra que se $\text{mdc}(a, b) = 1$ e (x_0, y_0) é uma solução da equação $ax + by = c$, então todas as soluções inteiras são dadas por $x = x_0 - bk$ e $y = y_0 + ak$ com $k \in \mathbb{Z}$.

Exemplo 1.15. *Sejam a, b inteiros positivos com $\text{mdc}(a, b) = 1$. Mostre que para todo $c \in \mathbb{Z}$ com $c > ab - a - b$, a equação $ax + by = c$ admite soluções inteiras com $x, y \geq 0$.*

Solução: Seja (x_0, y_0) uma solução inteira (que existe pelo teorema de Bachet-Bézout). Devemos mostrar a existência de um inteiro k tal que

$$x = x_0 - bk > -1 \qquad \text{e} \qquad y = y_0 + ak > -1,$$

ou seja,

$$-\frac{y_0 + 1}{a} < k < \frac{x_0 + 1}{b}.$$

Mas isto segue do fato de o intervalo $(-\frac{y_0+1}{a}, \frac{x_0+1}{b})$ ter tamanho maior do que 1:

$$\frac{x_0 + 1}{b} - \left(-\frac{y_0 + 1}{a}\right) = \frac{ax_0 + by_0 + a + b}{ab} = \frac{c + a + b}{ab} > 1.$$

□

1.3 O Teorema Fundamental da Aritmética

Estamos agora prontos para enunciar o teorema que caracteriza todo número natural em termos de seus "constituintes" primos.

Teorema 1.16 (Teorema Fundamental da Aritmética)**.** *Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \ldots \leq p_m$ são primos.

Demonstração: Mostramos a existência da fatoração de n em primos por indução. Se n é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n.

Vamos agora mostrar a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \ldots \leq p_m$, $q_1 \leq \ldots \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 \mid q_1 \cdots q_{m'}$ temos $p_1 \mid q_i$ para algum valor de i pelo corolário 1.10. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, pela minimalidade de n, donde $m = m'$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações. □

Outra forma de escrever a fatoração acima é

$$n = p_1^{e_1} \ldots p_m^{e_m},$$

com $p_1 < \cdots < p_m$ e $e_i > 0$. Ainda outra formulação é escrever

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \ldots p^{e_p} \ldots$$

onde o produto é tomado sobre *todos* os primos mas apenas um número finito de expoentes é maior do que zero. Vamos nos referir a qualquer destas expressões como a *fatoração canônica* de n em primos.

A fatoração única em primos se aplica em contextos mais gerais, como veremos mais tarde. Aqui, como aplicação imediata do Teorema Fundamental da Aritmética, vamos mostrar a prova atribuída a Euclides para a existência de infinitos primos (uma prova com mais de 2000 anos e que ainda funciona!).

Teorema 1.17 (Euclides)**.** *Existem infinitos primos.*

Demonstração: Suponha por absurdo que $p_1, p_2, \ldots, p_m$ fossem *todos* os primos. O número $N = p_1 p_2 \ldots p_m + 1 > 1$ não seria divisível por nenhum primo p_i, o que contradiz o Teorema Fundamental da Aritmética.

□

Observe que *não* provamos que $p_1 p_2 \ldots p_m + 1$ é primo para algum conjunto finito de primos (por exemplo, os m primeiros primos). Aliás, $2{\cdot}3{\cdot}5{\cdot}7{\cdot}11{\cdot}13{+}1 = 30031 = 59{\cdot}509$ não é primo. Não se conhece nenhuma fórmula simples que gere sempre números primos (veja a seção 7.2 para uma discussão sobre este assunto).

Embora a quantidade de primos seja infinita, uma questão natural é saber o quão "raros" ou "frequentes" eles são. Na segunda parte do livro, discutiremos mais a fundo esta questão sobre a distribuição dos primos. Por outro lado, é interessante notar que existem cadeias arbitrariamente longas de números compostos consecutivos: na sequência

$$(k+1)! + 2, (k+1)! + 3, (k+1)! + 4, \ldots, (k+1)! + (k+1),$$

nenhum termo é primo, pois eles admitem fatores próprios $2, 3, 4, \ldots, k+1$, respectivamente.

Uma interessante prova alternativa, devida a Erdős, de que existem infinitos primos é a seguinte:

Suponha, por contradição, que existe um número finito de primos, digamos $p_1, p_2, \ldots, p_k$. Seja n um número natural. Então podemos escrever qualquer número $m \leq n$ na forma $m = m_1^2 m_2$, onde $m_1^2 \leq n$ e

$$m_2 = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \qquad \text{onde } a_k = 0 \text{ ou } 1 \text{ para cada } k.$$

Assim, considerando todas as possíveis maneiras de escrever os naturais $m \leq n$, temos: 2^k escolhas para m_2 e no máximo $\lfloor \sqrt{n} \rfloor$ escolhas para m_1. Ou seja, para todo n natural, vale que

$$n \leq 2^k \sqrt{n}$$

absurdo, pois esta desigualdade não vale para n suficientemente grande. □

Exemplo 1.18 (OIbM1987)**.** *A sequência p_n é definida da seguinte forma:*

(i) $p_1 = 2$.

(ii) Para todo $n \geq 2$, p_n é o maior divisor primo da expressão

$$p_1 p_2 p_3 \cdots p_{n-1} + 1.$$

Demonstrar que p_n é diferente de 5.

Solução: Dado que $p_1 = 2$, $p_2 = 3$, $p_3 = 7$, segue-se que para qualquer $n \geq 3$, $p_1 p_2 \cdots p_{n-1}$ é múltiplo de 2 e de 3, portanto $p_1 p_2 \cdots p_{n-1} + 1$ não é múltiplo nem de 2 nem de 3. Além disso, como $p_1 = 2$, então p_n é ímpar para todo $n \geq 2$, assim $p_1 p_2 \cdots p_{n-1}$ não é múltiplo de 4.

Suponhamos que exista n tal que $p_n = 5$, isto é, o maior divisor primo de $p_1 p_2 \cdots p_{n-1} + 1$ é 5. Como 2 e 3 não dividem $p_1 p_2 \cdots p_{n-1} + 1$, temos que

$$p_1 p_2 \cdots p_{n-1} + 1 = 5^k.$$

Portanto

$$p_1 p_2 \cdots p_{n-1} = 5^k - 1 = (5-1)(5^{k-1} + 5^{k-2} + \cdots + 5 + 1),$$

donde $4 \mid p_1 p_2 \cdots p_{n-1}$, uma contradição. □

Exemplo 1.19. *Determine todas as ternas (a, b, c) de inteiros positivos tais que $a^2 = 2^b + c^4$.*

Solução: Como $a^2 = 2^b + c^4 \iff (a - c^2)(a + c^2) = 2^b$, pelo Teorema Fundamental da Aritmética existem dois naturais $m > n$ tais que $m +$

$n = b$, $a - c^2 = 2^n$ e $a + c^2 = 2^m$. Subtraindo as duas últimas equações, obtemos que $2c^2 = 2^m - 2^n$, assim $c^2 = 2^{n-1}(2^{m-n} - 1)$. Como 2^{n-1} e $2^{m-n} - 1$ são primos entre si e o seu produto é um quadrado perfeito (i.e. os expoentes das potências de primos distintos são pares), novamente pelo Teorema Fundamental da Aritmética 2^{n-1} e $2^{m-n} - 1$ devem ser ambos quadrados perfeitos, logo $n - 1$ é par e $2^{m-n} - 1 = (2k-1)^2$ para algum inteiro positivo k. Como $2^{m-n} = (2k-1)^2 + 1 = 4k(k-1) + 2$ é divisível por 2 mas não por 4, temos $m - n = 1$. Assim, fazendo $n - 1 = 2t$, temos que todas as soluções são da forma $(a, b, c) = (3 \cdot 2^{2t}, 4t + 3, 2^t)$ com $t \in \mathbb{N}$ e é fácil verificar que todos os números desta forma são soluções. □

Segue do Teorema Fundamental da Aritmética que todo divisor de $n = p_1^{e_1} \dots p_m^{e_m}$ é da forma

$$p_1^{d_1} \dots p_m^{d_m}$$

com $0 \leq d_i \leq e_i$. Assim, obtemos o outro algoritmo usual para calcular o mdc de dois números: fatoramos os dois números em primos e tomamos os fatores comuns com os menores expoentes. Este algoritmo é bem menos eficiente do que o de Euclides para inteiros grandes (que em geral não sabemos fatorar de forma eficiente computacionalmente) mas é instrutivo saber que os dois algoritmos dão o mesmo resultado. Além disso, este algoritmo tem consequências teóricas importantes, como por exemplo o

Corolário 1.20. *Se* $\mathrm{mdc}(a, n) = \mathrm{mdc}(b, n) = 1$, *então* $\mathrm{mdc}(ab, n) = 1$.

Demonstração: Evidente a partir do algoritmo descrito acima. □

Para encerrar esta seção, vejamos ainda algumas outras aplicações do Teorema Fundamental da Aritmética.

Proposição 1.21. *Seja* $n = p_1^{e_1} \dots p_m^{e_m}$ *a fatoração de* n *em potências de primos distintos* p_i *e seja* $\sigma_k(n) \stackrel{\text{def}}{=} \sum_{d|n,\, d>0} d^k$ *a soma das* k*-ésimas potências dos divisores positivos de* n. *Então*

$$\sigma_k(n) = \frac{p_1^{(e_1+1)k} - 1}{p_1^k - 1} \cdot \dots \cdot \frac{p_m^{(e_m+1)k} - 1}{p_m^k - 1}.$$

Para $k = 0$, a fórmula acima deve ser interpretada tomando-se o limite $k \to 0$, de modo que a quantidade de divisores positivos de n é $\sigma_0(n) = (e_1 + 1) \cdots (e_m + 1)$.

DEMONSTRAÇÃO: Como a soma na definição de $\sigma_k(n)$ percorre todos os números da forma $d^k = p_1^{d_1 k} \dots p_m^{d_m k}$ com $0 \leq d_i \leq e_i$, temos a seguinte fatoração:

$$\sigma_k(n) = (1 + p_1^k + p_1^{2k} + \cdots + p_1^{e_1 k}) \cdot \ldots \cdot (1 + p_m^k + p_m^{2k} + \cdots + p_m^{e_m k}).$$

Somando as progressões geométricas $1 + p_i^k + p_i^{2k} + \cdots + p_i^{e_i k} = \frac{p_i^{(e_i+1)k} - 1}{p_i^k - 1}$, o resultado segue. □

Proposição 1.22 (Fatores do Fatorial)**.** *Seja p um primo. Então a maior potência de p que divide $n!$ é p^α onde*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Observe que a soma acima é finita pois os termos $\left\lfloor \frac{n}{p^i} \right\rfloor$ são eventualmente zero.

DEMONSTRAÇÃO: No produto $n! = 1 \cdot 2 \cdot \ldots \cdot n$, apenas os múltiplos de p contribuem com um fator p. Há $\left\lfloor \frac{n}{p} \right\rfloor$ tais múltiplos entre 1 e n. Destes, os que são múltiplos de p^2 contribuem com um fator p extra e há $\left\lfloor \frac{n}{p^2} \right\rfloor$ tais fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p e assim por diante, resultando na fórmula acima. □

Exemplo 1.23. *Determine com quantos zeros termina* 1000!.

SOLUÇÃO: O problema é equivalente a determinar qual a maior potência de 10 que divide 1000! e como há muito mais fatores 2 do que 5 em 1000!, o expoente desta potência coincide com o da maior potência de 5 que divide 1000!, ou seja,

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 249.$$

Assim, 1000! termina com 249 zeros. □