# Equações Diofantinas Lineares

Equações, com uma ou mais incógnitas, de que se procuram soluções inteiras designam-se habitualmente por *Equações diofantinas*. Vamos apenas considerar as equações diofantinas lineares, isto é, equações do tipo $aX + bY = c$, com $a, b, c \in \mathbb{Z}$.

## Lema

*Sejam $a$ e $b$ inteiros não ambos nulos tais que $\mathrm{mdc}(a, b) = 1$. Se $aX + bY = 0$, para certos $X, Y \in \mathbb{Z}$, então existe $n \in \mathbb{Z}$ tal que $X = -nb$ e $Y = na$.*

**Demonstração.** Suponhamos que $aX + bY = 0$, para certos $X, Y \in \mathbb{Z}$. Se $a = 0$, como $\mathrm{mdc}(a, b) = 1$, então $b = \pm 1$ e a equação fica $0X + (\pm 1)Y = 0$. Logo, $Y = 0 = n \cdot 0$ e $X = -n \cdot (\pm 1)$, para qualquer $n \in \mathbb{Z}$.
Se $a \neq 0$, de $aX = -bY$ segue que $a \mid bY$. Como $\mathrm{mdc}(a, b) = 1$ então $a \mid Y$. Isto significa que existe um inteiro $n$ tal que $an = Y$. Substituindo $Y$ na equação inicial obtemos $X = -nb$. □

## Teorema

*Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos e $d = \mathrm{mdc}(a, b)$. As soluções inteiras da equação $aX + bY = 0$ são pares da forma*

$$X = \frac{-nb}{d} \quad e \quad Y = \frac{na}{d}$$

*com $n \in \mathbb{Z}$.*

**Demonstração.** Suponhamos que existem $X, Y \in \mathbb{Z}$ tais que $aX + bY = 0$. Dividindo esta igualdade por $d$, obtemos $\frac{a}{d}X + \frac{b}{d}Y = 0$. Como $\mathrm{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$, então, existe $n \in \mathbb{Z}$ tal que $X = -n\frac{b}{d}$ e $Y = n\frac{a}{d}$.
Como para qualquer $n \in \mathbb{Z}$, $a\frac{-nb}{d} + b\frac{na}{d} = \frac{-nab+nab}{d} = 0$, concluimos que as soluções inteiras da equação $aX + bY = 0$ são pares da forma

$$X = \frac{-nb}{d} \quad e \quad Y = \frac{na}{d}$$

com $n \in \mathbb{Z}$. □

Podemos agora provar o caso geral.

## Teorema

*Sejam $a, b, c \in \mathbb{Z}$, com $a$ e $b$ não simultaneamente nulos, e seja $d = \mathrm{mdc}(a, b)$. A equação $aX + bY = c$ tem solução inteira se e só se $d \mid c$. Neste caso, existem infinitas soluções inteiras dadas por pares da forma*

$$X = \frac{xc + nb}{d} \quad e \quad Y = \frac{yc - na}{d}$$

*com $n \in \mathbb{Z}$ e $x, y \in \mathbb{Z} : d = xa + yb$.*

**Demonstração.** A equação $aX + bY = c$ tem solução inteira se e só se $d \mid c$.
($\Rightarrow$) Suponhamos que $aX + bY = c$ tem solução, isto é, que existem $X, Y \in \mathbb{Z}$ tais que $aX + bY = c$. Como $d \mid a$ e $d \mid b$, então $d \mid aX + bY$, ou seja, $d \mid c$.
($\Leftarrow$) Suponhamos que $d \mid c$. Existem inteiros $x$ e $y$ tais que $d = ax + by$. Multiplicando ambos os membros pelo inteiro $\frac{c}{d}$, obtemos $c = a\frac{xc}{d} + b\frac{yc}{d}$. Fazendo $X_0 = \frac{xc}{d}$ e $Y_0 = \frac{yc}{d}$ temos uma solução inteira da equação.

Resta provar a segunda parte do teorema.
Suponhamos que o par ordenado de inteiros $(X, Y)$ é uma solução de $aX + bY = c$. Subtraindo, membro a membro, as igualdades $aX_0 + bY_0 = c$ e $aX + bY = c$ vem que $a(X_0 - X) + b(Y_0 - Y) = 0$. E, o par ordenado $(X_0 - X, Y_0 - Y)$ é uma solução inteira da equação $aX' + bY' = 0$. Sabemos que as soluções de $aX' + bY' = 0$ são da forma $X' = \frac{-nb}{d}$ e $Y' = \frac{na}{d}$, com $n \in \mathbb{Z}$. Portanto, $X_0 - X = \frac{-nb}{d}$ e $Y_0 - Y = \frac{na}{d}$, ou seja, $X = \frac{xc+nb}{d}$ e $Y = \frac{yc-na}{d}$, com $n \in \mathbb{Z}$. □

O Teorema anterior pode escrever-se na forma de um algoritmo.

## Algoritmo (Soluções de uma equação diofantina linear)

INPUT: termos $a, b, c \in \mathbb{Z}$, $a, b$ não ambos nulos, da equação $aX + bY = c$

- Determinar $\mathrm{mdc}(a, b)$ e $x, y \in \mathbb{Z}$ tais que $\mathrm{mdc}(a, b) = ax + by$ (utilizando o Algoritmo de Euclides - versão alargada)
- $d \leftarrow \mathrm{mdc}(a, b)$
- if $d \nmid c$ then
  - OUTPUT: Não existem soluções inteiras

  else
  - $X \leftarrow \frac{x*c+n*b}{d}$, $Y \leftarrow \frac{y*c-n*a}{d}$, com $n \in \mathbb{Z}$
- end

OUTPUT: $X$ e $Y$, forma geral das soluções inteiras da equação $aX + bY = c$

## Exemplo

Com a ajuda do GAP vamos determinar soluções da equação diofantina linear $1492X + 1066Y = -4$.

```
gap> a:=1492;; b:=1066;; c:=-4;;
gap> L:=Gcdex(a,b);
rec(gcd:=2,coeff1:=-5,coeff2:=7,coeff3:=533,coeff4:=-746)
gap> d:=L.gcd;; x:=L.coeff1;; y:=L.coeff2;;
gap> IsInt(c/d);
true                        # logo a equacao dada tem solucao #
gap> d = x*a + y*b;
true
gap> SolEqDiofantinaLinear:=n->[(x*c+n*b)/d,(y*c-n*a)/d];
function( n ) ... end
gap> SolEqDiofantinaLinear(0);
[ 10, -14 ]
gap> SolEqDiofantinaLinear(1);
[ 543, -760 ]
gap> SolEqDiofantinaLinear(9376);
[ 4997418, -6994510 ]
```

## Definição (Mínimo Múltiplo Comum)

*O mínimo múltiplo comum de dois inteiros a e b não nulos é o menor inteiro positivo que é simultaneamente múltiplo de ambos. Vamos denotar este inteiro por* $\mathrm{mmc}(a, b)$.

## Exemplo

Vamos determinar o mínimo múltiplo comum de 10 e 12. Começamos por considerar os conjuntos dos múltiplos positivos dos dois números: $M_{10} = \{10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, \ldots\}$ e $D_{12} = \{12, 24, 36, 48, 60, 72, 84, 96, 108, 120, 132 \ldots\}$. Ora $D_{10} \cap D_{12} = \{60, 120, \ldots\}$. Logo

$$\mathrm{mmc}(10, 12) = \min D_{10} \cap D_{12} = 60.$$

## Exercício

Construa uma função GAP para determinar o mínimo múltiplo comum de dois números inteiros não nulos.

A função GAP `LcmInt` permite determinar o mínimo múltiplo comum de dois inteiros diferentes de 0.

```
gap> LcmInt(23,12);
276
gap>
```

## Teorema

*Sejam $a$ e $b$ inteiros positivos. Qualquer múltiplo comum de $a$ e $b$ é múltiplo de $\mathrm{mmc}(a, b)$.*

**Demonstração.** Seja $s$ um inteiro múltiplo comum de $a$ e $b$. Dividamos $s$ por $m = \mathrm{mmc}(a, b)$. Existem números inteiros $q$ e $r$ tais que $s = mq + r$, com $0 \leq r < m$. Donde, $r = s - mq$ e portanto $r$ é um múltiplo comum de $a$ e $b$ (por $s$ e $m$ o serem). Como $r$ é menor do que $m$, não pode ser positivo, pois $m$, por definição, é o menor múltiplo comum positivo de $a$ e $b$. Portanto $r = 0$ e $s \mid m$. □

## Proposição

*Sejam $a$ e $b$ inteiros positivos.*

(i) *Sendo $n \in \mathbb{N}$, tem-se* $\operatorname{mmc}(na, nb) = n \cdot \operatorname{mmc}(a, b)$.

(ii) *Se $d$ for um divisor comum positivo de $a$ e $b$, então* $\operatorname{mmc}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \operatorname{mmc}(a, b)$.

**Demonstração.** (i) Sejam $n \in \mathbb{N}$ e $h = \operatorname{mmc}(a, b)$. Pretendemos provar que $\operatorname{mmc}(na, nb) = nh$. Ora $h$ é um múltiplo comum de $a$ e $b$, donde $nh$ é um múltiplo comum de $na$ e $nb$. Portanto, $\operatorname{mmc}(na, nb) \leq nh$. Por outro lado, temos que $\operatorname{mmc}(na, nb) = ina = jnb$, para alguns $i, j$ inteiros positivos. Como $ina = jnb$ é múltiplo comum de $a$ e $b$, então é múltiplo de $h$ (pelo mesmo resultado anterior) e, portanto, é múltiplo de $nh$. Assim, $\operatorname{mmc}(na, nb)$ é multiplo de $nh$, pelo que $\operatorname{mmc}(na, nb) \geq nh$. Logo, $\operatorname{mmc}(na, nb) = nh$, ou seja, $\operatorname{mmc}(na, nb) = n \cdot \operatorname{mmc}(a, b)$.
(ii) Seja $d$ um divisor positivo comum a $a$ e a $b$. Por (i) temos que $\operatorname{mmc}(a, b) = \operatorname{mmc}\left(d\frac{a}{d}, d\frac{b}{d}\right) = d \cdot \operatorname{mmc}\left(\frac{a}{d}, \frac{b}{d}\right)$. □

## Teorema (Relação entre o MDC e o MMC)

*Sejam $a$ e $b$ inteiros positivos. Então* $\mathrm{mmc}(a,b)\cdot\mathrm{mdc}(a,b)=a\cdot b$.

**Demonstração.** Se $\mathrm{mdc}(a,b)=1$, basta provar que $\mathrm{mmc}(a,b)=a\cdot b$. Como $a\mid\mathrm{mmc}(a,b)$, existe $q\in\mathbb{N}$ tal que $\mathrm{mmc}(a,b)=qa$. Como também $b\mid\mathrm{mmc}(a,b)$, tem-se que $b\mid qa$. Dado que $a$ e $b$ são primos entre si, então $b\mid q$, ou seja, $q=tb$, para algum $t\in\mathbb{N}$. Constatamos assim que $\mathrm{mmc}(a,b)=tab$ e, portanto, que $\mathrm{mmc}(a,b)\geq ab$. Mas, como $\mathrm{mmc}(a,b)$ é, por definição, o menor dos múltiplos comuns positivos de $a$ e $b$ e $ab$ é um múltiplo comum positivo de $a$ e $b$, só pode ser $\mathrm{mmc}(a,b)=ab$.

Suponhamos agora que $\mathrm{mdc}(a,b)=d>1$. Então $\mathrm{mdc}\left(\frac{a}{d},\frac{b}{d}\right)=1$. Estamos, agora, nas condições da primeira parte desta prova, assim $\mathrm{mmc}\left(\frac{a}{d},\frac{b}{d}\right)\mathrm{mdc}\left(\frac{a}{d},\frac{b}{d}\right)=\frac{a}{d}\cdot\frac{b}{d}$. Multiplicando ambos os membros por $d^2$ obtemos que $\mathrm{mmc}(a,b)\cdot\mathrm{mdc}(a,b)=a\cdot b$, como pretendíamos. □

# Números Primos e Teorema Fundamental da Aritmética

## Teorema

*Qualquer natural maior ou igual a 2 tem pelo menos um divisor primo.*

**Demonstração.** Seja $n \geq 2$ um número inteiro positivo. Consideremos o conjunto $D = \{d \in \mathbb{N} \mid d > 1 \text{ e } d \mid n\}$. Este conjunto é não-vazio, pois $n \in D$. Pelo Princípio de Boa Ordenação, $D$ tem um elemento mínimo, digamos $p$. Suponhamos que $p$ não é primo. Então, $\exists k \in \mathbb{N} : k \mid p, 1 < k < p$, ou seja, $p = zk$ para algum $z \in \mathbb{N}$. Por outro lado, como $p \in D$, então $p \mid n$, ou seja, $n = tp$, para algum $t \in \mathbb{N}$. Assim, $n = tp = tzk$, donde resulta que $k \mid n$ e portanto, que $k \in D$. Mas, isto contraria o facto de que $p$ é o mínimo de $D$. A contradição resultou de supor que $p$ não é primo. Logo, $p$ é primo. □

A existência dum número infinito de primos foi provada por Euclides. Actualmente, existem diversas demonstrações deste facto.

## Corolário (Euclides)

*Há uma infinidade de números primos.*

**Demonstração.** Suponhamos que há um número finito de primos distintos, digamos $p_1, p_2, \ldots, p_k$, para certo $k \in \mathbb{N}$. Seja $n = p_1 p_2 \ldots p_k + 1$. Pelo teorema anterior existe um número primo que divide $n$, ou seja, $\exists i \in \{1, 2, \ldots, k\}$ tal que $p_i \mid n$. Além disso, como $p_i \mid p_1 p_2 \ldots p_k$, temos que $p_i \mid n - p_1 p_2 \ldots p_k$, ou seja, $p_i \mid 1$, o que não pode ser, pela definição de primo. A contradição resultou de supor que existe um número finito de primos. Logo, existem infinitos números primos. □

## Corolário

*Seja $n \geq 2$ um inteiro. Se nenhum número primo $p \leq \sqrt{n}$ divide $n$, então $n$ é um número primo.*

**Demonstração.** Seja $n \geq 2$ tal que nenhum número primo menor ou igual a $\sqrt{n}$ divide $n$. Suponhamos que $n$ não é primo. Então, $n = ab$, para alguns inteiros $1 < a, b < n$. Sabemos que existem primos $p$ e $q$ tais que $p \mid a$ e $q \mid b$. Como $p$ e $q$ também dividem $n$ então, por hipótese, $p, q > \sqrt{n}$. Temos então $n = ab \geq pq > \sqrt{n}\sqrt{n} = n$, o que é absurdo. O absurdo resultou de supor que $n$ não é primo. Logo, $n$ é um número primo. □

## Exemplo

Vejamos que 193 é um número primo. Tem-se $\sqrt{193} < \sqrt{196} = 14$. Os números primos menores do que 14 são $2, 3, 5, 7, 11, 13$ e nenhum deles divide 193. Logo, 193 é um número primo.

O Crivo de Eratóstenes permite obter listas de números primos.

## Algoritmo (Crivo de Eratóstenes)

INPUT: um número inteiro $n \geq 2$

Definir a lista $L = [2, ..., n]$ e a lista vazia $M$

repeat

Escolher o menor número $m$ da lista $L$
Colocar $m$ na lista $M$
Remover todos os múltiplos de $m$ da lista $L$

until $L$ ficar vazia

OUTPUT: $M$, lista de primos menores ou iguais a $n$

## Exercício

Implemente no GAP o Crivo de Eratóstenes e faça uma lista com os números primos entre 1 e 1000. Confirme o resultado comparando com a lista predefinida `Primes` presente no GAP.

O exemplo seguinte dá conta de algumas funções existentes no GAP para lidar com números primos.

## Exemplo

```
gap> IsPrimeInt(10453);
true
gap> IsPrimeInt(1043);
false
gap> IsPrime(2*3*5*7*11+1);
true
gap> PrevPrimeInt(45);
43
gap> NextPrimeInt(45);
47
gap> NextPrimeInt(47);
53
```

## Lema (Lema de Euclides)

*Sejam $p$ um primo e $a, b$ inteiros. Se $p$ divide $ab$, então $p$ divide $a$ ou $p$ divide $b$.*

**Demonstração.** Suponhamos que $p$ divide $ab$, mas não divide $a$. Pretendemos provar que $p$ divide $b$. Como $p$ não divide $a$, temos $\mathrm{mdc}(p, a) = 1$. Então, por um resultado anterior, vem que $p$ divide $b$. □

O Lema de Euclides pode ser generalizado para um qualquer produto finito de inteiros.

## Corolário

*Sejam $p$ um primo e $a_1, a_2, \ldots, a_k$ inteiros. Se $p \mid a_1 a_2 \ldots a_k$ então existe um índice $i \in \{1, 2, \ldots, k\}$ tal que $p \mid a_i$.*

## Exercício

Use o Princípio de Indução para provar o resultado anterior..

## Teorema (Teorema Fundamental da Aritmética)

*Qualquer inteiro maior que* 1 *é primo ou um produto de primos. Este produto é único a menos da ordem dos factores.*

**Demonstração.** Vamos utilizar a segunda forma do Princípio de Indução para provar a existência de uma factorização de $a$ em primos. Seja $S$ o conjunto de inteiros que são primos ou produtos de primos. Sem dúvida, $2 \in S$. Suponhamos, agora, que para algum inteiro $n$, $S$ contém todos os inteiros $k$, com $2 \leq k < n$. Queremos provar que $n \in S$. Se $n$ é primo, então $n \in S$, por definição de $S$. Se $n$ não é primo, então $n = ab$, para alguns inteiros $1 < a, b < n$. Como, por hipótese de indução, $a$ e $b$ pertencem a $S$, temos que cada um destes inteiros é um primo ou um produto de primos. Portanto, $n$ é também um produto de primos. Logo, por indução, concluímos que $S = \{a \in \mathbb{Z} \mid a > 1\}$, ou seja, qualquer inteiro $a > 1$ pode ser escrito como um produto de números primos.

Resta provar a unicidade.

Suponhamos que $a$ tem duas factorizações em números primos: $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$, onde $p_1, p_2, \dots, p_s$ e $q_1, q_2, \dots, q_t$ são números primos. Da primeira factorização temos que $p_1 \mid a$, logo $p_1 \mid q_i$, para algum $i \in \{1, 2, \dots, t\}$. Trocando e renumerando os primos da segunda factorização (se necessário) podemos assumir que $i = 1$ e que $p_1 \mid q_1$. Como $q_1$ é primo, segue-se que $p_1 = q_1$. Cancelando este primo das duas factorizações temos: $p_2 \dots p_s = q_2 \dots q_t$. Continuando este processo repetidamente, esgotam-se todos os primos de uma das factorizações. Se uma das factorizações se esgotar antes da outra, as factorizações reduzidas expressam 1 como um produto de primos $p_i$ ou $q_j$, o que não pode ser pois, $p_i, q_j > 1$. Portanto, as duas factorizações esgotam os seus primos por cancelamento em simultâneo. Logo, $s = t$ e $p_i = q_i$ (depois de uma troca conveniente dos factores primos). □

A factorização de $a > 1$ em números primos pode conter factores repetidos. É comum escrevê-la na forma

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} = \prod_{i=1}^{n} p_i^{\alpha_i}, \quad (\alpha_i \geq 1)$$

que se diz a factorização de $a$ em *potências primas*.

O exemplo seguinte dá conta de algumas funções existentes no GAP para lidar com factorizações.

## Exemplo

```
gap> FactorsInt(32);
[ 2, 2, 2, 2, 2 ]
gap> FactorsInt(6820);
[ 2, 2, 5, 11, 31 ]
gap> PrimePowersInt(32);
[ 2, 5 ]
gap> PrimePowersInt(6820);
[ 2, 2, 5, 1, 11, 1, 31, 1 ]
gap> PrintFactorsInt(32);Print("\n");
2^5
gap> PrintFactorsInt(6820);Print("\n");
2^2*5*11*31
gap>
```