Capítulo 5

Rudimentos Matemáticos

Definição 3 (divisibilidade) *Sejam* $a, b \in \mathbb{Z}$ *com* $a \neq 0$*, diz-se que* $a \mid b$ *(*a *divide* b*) se*

$$(\exists z \in \mathbb{Z})(b = az)$$

5.0.1 Propriedades da divisibilidade:

1. $a \mid 1 \Rightarrow a = \pm 1$
2. $((a \mid b) \wedge (b \mid a)) \Rightarrow a = \pm b$
3. $(\forall b)(b \mid 0)$
4. $(b \mid g) \wedge (b \mid h) \Rightarrow ((\forall m, n \in \mathbb{Z})(b \mid (mg + nh)))$
5. $((a \mid (b + c)) \wedge (a \mid b)) \Rightarrow a \mid c$

   Dem.:

$$\begin{aligned} a \mid b &\Rightarrow b = ak \\ a \mid (b + c) &\Rightarrow (b + c) = ak' = (ak + c) \\ ak' = ak + c &\Rightarrow a(k' - k) = c \\ &\Rightarrow a \mid c \end{aligned}$$

■

Definição 4 (número primo) *O numero* $p > 1$ *diz-se um número primo se admitir somente* 1 *e* p *como divisores positivos.*

Definição 5 (máximo divisor comum) *Diz-se que* g *é o máximo divisor comum de dois inteiros* a *e* b *(*$g = (a, b)$*) se*

$$g \mid a \wedge g \mid b \wedge ((\forall d)(d \mid a \wedge d \mid b) \Rightarrow d \mid g).$$

Teorema 6 $g = (a, b)$ *é a menor combinação linear positiva de* a *e* b.

Dem.: Seja $S = \{ax + by \ : x, y \in \mathbb{Z} \ \wedge \ ax + by > 0\}$. $S \neq \emptyset$ (pois $a^2 + b^2 \in S$). Seja então d o primeiro elemento de S

- Seja d' tal que $d' \mid a \ \wedge \ d' \mid b$, então

$$d \ = \ ax + by \ = \ d'q_1x + d'q_2y \ = \ d'(q_1x + q_2y)$$

logo

$$d' \mid d.$$

- $a = dq + r$, $0 \leq r < d$, então

$$r \ = \ a - dq \ = \ a - (ax + by)q \ = \ a(1 - xq) + b(-yq)$$

ou seja r é combinação linear de a e b.

Se $r > 0$ então teríamos $r \in S$, mas como $r < d$ isso seria um absurdo pois estamos a tomar d como o primeiro elemento de S. Pelo que

$$0 \leq r \ \Rightarrow r = 0.$$

Logo

$$d \mid a.$$

Exactamente da mesma forma se prova que $d \mid b$.

Portanto $d = (a, b)$.

■

Teorema 7 *O inteiro* p *é primo se e só se*

$$(\forall a, b \in \mathbb{Z} \setminus \{0\})(p \mid ab \ \Rightarrow p \mid a \vee p \mid b). \tag{5.1}$$

Dem.: ($\Rightarrow$) Seja p primo e suponhamos que $p \mid ab$. Se $p \mid a$ nada há a demonstrar, se $p \nmid a$ então, como p não admite divisores, tem-se que

$$(p, a) = 1$$

Logo

$$(\exists x, y) \ 1 = ax + py \ \Rightarrow \ b = bax + bpy \ \Rightarrow \ p \mid b$$

($\Leftarrow$) Seja p tal que $(\forall a, b \in \mathbb{Z} \setminus \{0\})(p \mid ab \Rightarrow p \mid a \vee p \mid b)$ e S o conjunto dos divisores positivos de p, diferentes da unidade. $S \neq \emptyset$ pois $p \in S$. Seja m o primeiro elemento de S,

$$m \mid p \ \wedge \ (\exists k)\ mk = p$$

como p tem a propriedade (5.1), $p \mid m$ ou $p \mid k$. Mas

$$p \mid k \ \Rightarrow \ k \geq p \ \Rightarrow \ p = k \ \Rightarrow m = 1$$

o que é **absurdo!** Logo

$$p \mid m \ \Rightarrow \ p = m.$$

E portanto p é primo.

■

Proposição 8 *Para quaisquer inteiros positivos* a, b *e* m*,*

$$(ma, mb) = m(a, b).$$

Dem.: Pelo Teorema 6 (ma, mb) é a menor combinação linear positiva de ma e mb ou seja o menor positivo da forma $max + mby$ com x e y inteiros. Mas então é o menor valor positivo de $m(ax + by)$ e portanto $(ma, mb) = m(a, b)$.

■

Corolário 9 *Se* $d|a$, $d|b$ *e* $d > 0$*, então*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

Se $(a, b) = g$*, então*

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1.$$

Teorema 10 *Qualquer inteiro* n $(n > 1)$ *se escreve de forma única (a menos da ordem) como produto de primos.*

Dem.: Primeiro provemos que tal representação existe sempre. Seja S o conjunto dos inteiros compostos que não se podem representar como produto de primos. Se $S \neq \emptyset$ então existe um primeiro elemento de S, a que chamamos s. Como s não é primo então existem m' e m'' tais que $s = m'm''$ com $1 < m' < s$ e $1 < m'' < s$. Mas como tanto m' como m'' são menores que s, têm factorizações em factores primos, pelo que s também admite uma factorização em factores primos, logo $S = \emptyset$.

Para provar que tal factorização é única procedamos por indução. É trivial que a representação de 2 é única, e suponhamos que todos os inteiros menores que n $(2 \ldots n-1)$ admitem uma única factorização. Suponhamos que para n temos

$$n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k} = q_1^{t_1} q_2^{t_2} \ldots q_r^{t_r}$$

com p_i e q_j primos e $s_i > 0$ e $t_j > 0$. Suponhamos também que $1 < s_1 < \ldots < s_k$ e $1 < q_1 < \ldots < q_r$.

Como $p_1 \mid n$ temos que $p_1 \mid q_1^{t_1} q_2^{t_2} \ldots q_r^{t_r}$, mas pela definição de número primo, então para algum j $(1 \leq j \leq r)$ $p_1 \mid q_j$, o que implica, como q_j é primo, que $p_1 = q_j$. Tem que se ter $j = 1$, pois senão, como $q_1 \mid p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$ logo existe $1 < e \leq k$ tal que $q_1 = p_e$, e então $p_1 < p_e = q_1 < q_j = p_1$ que seria absurdo. Então, como $p_1 = q_1$, podemos tomar

$$n_1 = \frac{n}{p_1} = p_1^{s_1 - 1} p_2^{s_2} \ldots p_k^{s_k} = q_1^{t_1 - 1} q_2^{t_2} \ldots q_r^{t_r}.$$

Como $n_1 < n$, por hipótese de indução, a factorização de n_1 em factores primos é única, pelo que $k = r$, $s_i = t_i$ e $p_i = q_i$ $(i \leq k)$. Ou seja a factorização de n é única.

■

Teorema 11 (Euclides) *O conjunto dos inteiros primos não é finito.*

Dem.: Suponhamos, por absurdo que o conjunto dos inteiros primos $\mathbb{P}$ era finito. Então

$$\mathbb{P} = \{p_1, p_2, ..., p_k\}$$

para algum k. Seja então $p = (p_1 \times p_2 \times ... \times p_k) + 1$, $p \notin \mathbb{P}$. Temos que:

$$\begin{aligned} p_1 &\nmid p \\ p_2 &\nmid p \\ &\vdots \\ p_k &\nmid p \end{aligned}$$

Portanto como a decomposição em primos de p não pode involver nenum dos p_i, p seria primo o que é absurdo pois $p > p_i$ para todos os $p_i \in \mathbb{P}$ O absurdo resultou de se ter suposto $\mathbb{P}$ finito, pelo que $\mathbb{P}$ não é finito.

■

São muitas e muito variadas as demonstrações conhecidas deste teorema (a que é apresentada aqui é a do próprio Euclides), por isso é costume gracejar dizendo que a "qualidade"

de um matemático pode ser medida pelo número de demonstrações que conhece (deste teorema). Algumas das das mais elegantes (e surpreendentes!) podem ser encontradas em [AZ98]. De qualquer forma não foi possível resistir à tentação de apresentar aqui a demonstração de um teorema (por Paul Erdös) do qual o anterior resulta como consequência trivial.

Necessitamos primeiro de uma definição adicional:

Definição 12 (*floor*)

$$\lfloor x \rfloor = \max\{z \in \mathbb{Z} : z \leq x\}$$

Teorema 13 (Erdös) *A série*

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

é divergente.

Dem.: Suponhamos, por absurdo, que a série é convergente e consideremos $\mathbb{P} = \{p_i | i > 0\}$ de forma que os p_i estejam ordenados por forma crescente. Então

$$(\exists k \in \mathbb{N}) \ \sum_{i>k} \frac{1}{p_i} < \frac{1}{2}.$$

Chamemos aos $(p_i)_{i \leq k}$ *"primos pequenos"* e aos $(p_i)_{i>k}$ *"primos grandes"*. Para qualquer $m \in \mathbb{N}$ podemos escrever $m = m_p + m_g$ em que m_g é o número dos inteiros $0 < n \leq m$ que são divisíveis por algum *primo grande*, e m_p o número dos inteiros $0 < n \leq m$ que não ocorrem "primos grandes" na sua factorização em primos. Comecemos por estimar m_g. Para cada *primo grande* p

$$\left\lfloor \frac{m}{p} \right\rfloor$$

é o número de inteiros n (não superiores a m) que são divisíveis por p. Portanto temos

$$m_g \leq \sum_{i>k} \left\lfloor \frac{m}{p_i} \right\rfloor \leq \sum_{i>k} \frac{m}{p_i} < \frac{m}{2}.$$

Quanto a m_p comecemos por escrever cada um dos inteiros n_i não superiores a m que não são divisíveis por nenhum *primo grande* na forma $n_i = a_i b_i^2$, por forma que a_i não contenha nenhum quadrado. Ou seja, na decomposição de n_i em factores primos, tomamos a_i como o produto de todos os primos cujos expoentes são ímpares, e portanto $\frac{n_i}{a_i}$ passará a ter somente factores de expoente par. Agora estamos então em condições de estimar quantos são então estes inteiros n_i: como a_i contém, no máximo, um de cada um dos *primos pequenos*, sabemos que podemos contar com não mais

de 2^k diferentes componentes livres de quadrados; por outro lado $b_i^2 \leq n_i \leq m$ pelo que não poderão existir mais de $\sqrt{m}$ componentes "quadradas". Assim sabemos que

$$m_p \leq 2^k \sqrt{m}.$$

Se tomarmos $m = 2^{2k+2}$ temos

$$\begin{aligned} m = m_g + m_p &< \frac{m}{2} + 2^k\sqrt{m} \\ &= \frac{2^{2k+2}}{2} + 2^k\sqrt{2^{2k+2}} \\ &= 2^{2k+1} + 2^{2k+1} = 2^{2k+2} \\ &= m \end{aligned}$$

o que é absurdo! O absurdo resultou da suposição que a série convergia pelo que a série tem que divergir.

■

A existência de uma infinidade de primos fica por isto demostrada, pois se o conjunto $\mathbb{P}$ fosse finito a série referida seria obrigatoriamente convergente pois seria constituída somente por um número finito de parcelas.

Definição 14 (números primos entre si) a *e* b *dizem-se primos entre si (ou primos relativos) se*

$$(a, b) = 1.$$

Tomando a e $n \neq 0$ inteiros quaisquer, é sempre possível encontrar $q, r \in \mathbb{Z}$ por forma que $a = qn + r$ com $0 \leq r < n$. A saber: $q = \lfloor a/n \rfloor$ e $r = a - qn$.

Definição 15 *Sejam* $a, n \in \mathbb{Z}$ *e* $n > 0$ *definimos* $a \mod n$ *como o resto da divisão de* a *por* n.

Definição 16 (congruência) *Dois inteiros* a, b *dizem-se congruentes módulo* n *(*$a \equiv b \pmod n$*) se* $a \mod n = b \mod n$.

Definição 17 *Definimos o conjunto* $\mathbb{Z}_n = \{0, 1, ..., (n-1)\}$.

Observemos que:

1. $(w + x) \mod n = (x + w) \mod n$
2. $(w \times x) \mod n = (x \times w) \mod n$

3. $((w+x)+y) \mod n = (w+(x+y)) \mod n$
4. $((w \times x) \times y) \mod n = (w \times (x \times y)) \mod n$
5. $(w \times (x+y)) \mod n = ((w \times x)+(w \times y)) \mod n$
6. $(0+w) \mod n = w \mod n$
7. $(1 \times w) \mod n = w \mod n$
8. $(\forall w \in \mathbb{Z}_n)(\exists z \in \mathbb{Z}_n)(w+z = 0 \mod n)$

Notemos que a "lei de corte" se verifica para a adição:

$$(a+b) \equiv (a+c) \pmod{n} \Rightarrow b \equiv c \pmod{n}$$

o que é consistente com a existência de inverso aditivo para todos os elementos de $\mathbb{Z}_n$, pelo que:

$$((-a)+a+b) \equiv ((-a)+a+c) \pmod{n}$$
$$b \equiv c \pmod{n}.$$

No entanto, a seguinte afirmação só é válida para as condições indicadas:

$$((a \times b) \equiv (a \times c) \pmod{n} \Rightarrow b \equiv c \pmod{n}) \text{ se } (a,n) = 1$$

isto porque se $(a,n) \neq 1$ a função

$$\begin{array}{rccl} f: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & z & \longmapsto & a \times z \pmod{n} \end{array}$$

não é sobrejectiva.

Dem.: Seja $m = (a,n)$ então $m \mid a \wedge m \mid n$, logo $((\exists x)(\exists y)\ a = xm \wedge n = ym)$. Então $f(0) = a \times 0 = 0$ e $f(y) = ay = xym = xn \equiv 0 \pmod{n}$. Portanto f não é injectiva, e como tal (porque se trata de um endomorfismo definido num conjunto finito) não é sobrejectiva.

■

Proposição 18 *Quaisquer que sejam* $b, n \in \mathbb{Z}$ *com* $n > 0$, $b^n - 1$ *é divisível por* $b-1$ *com quociente* $b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$.

Dem.: Como 1 é raiz de $x^n - 1$, $x^n - 1$ deve ser divisível por $x-1$. Da divisão polinomial resulta o quociente $x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1$, pelo que a proposição resulta trivial.

■

Proposição 19 *Sejam* a *e* m *tal que* $(a, m) = 1$ *e* $b, c > 0$. *Se* $a^b \equiv 1 \mod m$ *e* $a^c \equiv 1 \mod m$, *então seja* $d = (b, c)$, *temos* $a^d \equiv 1 \mod m$.

Dem.: Como $d = (b, c)$ podemos encontrar $u, v \in \mathbb{Z}$ tais que $d = ub + vc$. Então como $(a^b)^u \equiv 1 \mod m$ e $(a^c)^v \equiv 1 \mod m$ temos

$$a^d = a^{ub+vc} \equiv 1 \pmod{m}.$$

■

5.1 Algoritmo de Euclides

O Algoritmo de Euclides para determinar o máximo divisor comum entre dois inteiros assenta no seguinte teorema

Teorema 20 *Sejam* $0 \leq a$ *e* $0 < b$

$$(a, b) = (b, a \mod b)$$

Dem.: Seja $d = (a, b)$, então $d \mid a$ e $d \mid b$. Temos

$$\begin{aligned} a = kb + r &\equiv r \mod b \\ a \mod b &= r \end{aligned}$$

Portanto $(a \mod b) = a - kb$ para algum inteiro k. Como $d \mid b$, $d \mid kb$. Como $d \mid a$ temos que $d \mid (a \mod b)$. Portanto temos que $d \mid b \wedge d \mid (a \mod b)$.

Suponhamos que d é um factor comum de b e $(a \mod b)$, então $d \mid kb$ logo

$$d \mid (kb + (a \mod b))$$

ou seja

$$d \mid a.$$

Assim o conjunto de divisores comuns a a e b é o mesmo que o conjunto de divisores comuns a b e $(a \mod b)$, e portanto o seu elemento máximo deve ser o mesmo.

■

Podemos então usar este resultado repetidamente para determinar o máximo divisor comum entre dois inteiros.

Para verificar que este processo é algorítmico, isto é que termina sempre, basta observar que em cada passo se reduz o problema de calcular (x, y) ao problema de calcular (y, z) com $z < y$ e $x, y, z \in \mathbb{N}$, pelo que ao cabo de um número finito de etapas se tem $z = 0$.

O seguinte programa em **python** implementa este algoritmo supondo $d > f > 0$:

	$(1970, 1066) =$
$1970 = 1 \times 1066 + 904$	$= (1066, 904) =$
$1066 = 1 \times 904 + 162$	$= (904, 162) =$
$904 = 5 \times 162 + 94$	$= (162, 94) =$
$162 = 1 \times 94 + 68$	$= (94, 68) =$
$94 = 1 \times 68 + 26$	$= (68, 26) =$
$68 = 2 \times 26 + 16$	$= (26, 16) =$
$26 = 1 \times 16 + 10$	$= (16, 10) =$
$16 = 1 \times 10 + 6$	$= (10, 6) =$
$10 = 1 \times 6 + 4$	$= (6, 4) =$
$6 = 1 \times 4 + 2$	$= (4, 2) =$
$4 = 2 \times 2 + 0$	$= (2, 0) =$
	$= 2$

Tabela 5.1: Cálculo de $(1970, 1066)$.

```
def Euclid(d,f):
  x,y = f,d
  while True:
    if y == 0: return x
    x, y = y, x % y
```

Claro que uma versão recursiva é muito mais elegante:

```
def Euclid(a,b):
  r = a % b
  if not r: return b
  else: return Euclid(b,r)
```

Pelo que vimos anteriormente, se $(d, f) = 1$ então d tem um inverso multiplicativo módulo f.

O algoritmo anterior pode ser extendido por forma que se $(d, f) = 1$ o algoritmo retorne d^{-1}:

```
def xEuclid(d,f):
  x1, x2, x3 = 1, 0, f
  y1, y2, y3 = 0, 1, d
  while True:
    if y3 == 0: return (x3,'no inverse')
    if y3 == 1: return (y3, y2)
```

```
q = x3/y3
x1,x2,x3, y1,y2,y3 = y1,y2,y3, x1-q*y1,x2-q*y2,x3-q*y3
```

q	x1	x2	x3	y1	y2	y3
—	1	0	**1643**	0	1	**1067**
1	0	1	1067	1	-1	576
1	1	-1	576	-1	2	491
1	-1	2	491	2	-3	85
5	2	-3	85	-11	17	66
1	-11	17	66	13	-20	19
3	13	-20	19	-50	77	9
2	-50	77	9	113	**-174**	**1**

Tabela 5.2: Valores das variáveis de `xEuclid` executado para 1643 e 1067.

Que o processo termina sempre, é trivial pois observe-se que os valores de `x3` e `y3` são os da execução de `Euclid`, que já vimos estar correcto. Temos somente que provar que, caso $(d, f) = 1$ o último valor de `y2` corresponde a $d^{-1} \mod f$. Para tal observe-se que se tem sempre

$$\begin{aligned} f \times x1 + d \times x2 &= x3 \\ f \times y1 + d \times y2 &= y3 \end{aligned}$$

ao longo da execução de `xEuclid`. Representemos por x_1^0, x_2^0 e x_3^0 os valores iniciais das variáveis `x1`, `x2` e `x3` e por x_1^i, x_2^i e x_3^i os seus valores no fim da i-ésima execução do ciclo `while`, o mesmo para as variáveis `y1`, `y2` e `y3`. Provemos então as igualdades anteriores por indução. Trivialmente tem-se

$$\begin{aligned} f x_1^0 + d x_2^0 &= x_3^0 \\ f y_1^0 + d y_2^0 &= y_3^0. \end{aligned}$$

Suponhamos então que as igualdades $f x_1^i + d x_2^i = x_3^i$ e $f y_1^i + d y_2^i = y_3^i$ se verificam. Então

$$f x_1^{i+1} + d x_2^{i+1} = x_3^{i+1}$$

pois $x_1^{i+1} = y_1^i$, $x_2^{i+1} = y_2^i$ e $x_3^{i+1} = y_3^i$. Por outro lado como

$$y_1^{i+1} = x_1^i - q y_1^i \quad y_2^{i+1} = x_2^i - q y_2^i \quad y_3^{i+1} = x_3^i - q y_3^i$$

temos

$$\begin{aligned} f y_1^{i+1} + d y_2^{i+1} &= \\ f(x_1^i - q y_1^i) + d(x_2^i - q y_2^i) &= \\ f x_1^i - f q y_1^i + d x_2^i - d q y_2^i &= \\ (f x_1^i + d x_2^i) - q(f y_1^i + d y_2^i) &= x_3^i - q y_3^i \\ &= y_3^{i+1}, \end{aligned}$$

pelo que a relação se verifica durante toda a execução do programa. Mas se $(d, f) = 1$, então no passo final temos $y_3 = 1$ e então

$$\begin{aligned} f y_1 + d y_2 &= 1 \\ d y_2 &= 1 + (-y_1) \times f \\ d y_2 &\equiv 1 \pmod{f} \end{aligned}$$

portanto e então y_2 é o inverso multiplicativo de d módulo f.