Introdução à Teoria dos Números
Ficha 2: Aritmética de $\mathbb{Z}$

Dados $a, b \in \mathbb{Z}$ denotamos por

$$a \mid b :$$

a divide b ou a é um **divisor** de b, a relação definida por

$$a \mid b \iff \exists q \in \mathbb{Z} : b = aq$$

Como consequência do Princípio da Boa Ordenação de $\mathbb{N}$ (ver Ficha 1) temos

Lema 0.1 *da Divisão (inteira):*

Dados $b \in \mathbb{N} \setminus 0$ e $a \in \mathbb{Z}$, existem $q, r \in \mathbb{Z}$ ***únicos****, tais que*

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

Este Lema implica, por sua vez, o

Teorema 0.2 *(Representação dos inteiros em bases):*

Seja b um inteiro ≥ 2. Então qualquer inteiro positivo a pode ser representado na base b*, isto é, a pode ser escrito de forma única como*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_2 b^2 + r_1 b + r_0$$

com $0 \leq r_i < b; i = 1, 2, \ldots, n$.

Notação 0.3 *Escreve-se então $a = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b$.*

Exercício 0.4 *Calcular a representação de* 29674 *na base* 3 *e na base* 11*.*

Definição 0.5 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, diz-se que d é o* ***máximo divisor comum*** *de a e b, $d = mdc(a, b)$, se*

(i) $d > 0$; (ii) $d \mid a$ e $d \mid b$; (iii) $c \mid a$ e $c \mid b \implies c \mid d$.

Nota 0.6 *Temos obviamente*

- $\forall a \in \mathbb{N} : mdc(a, 0) = a$;
- $\forall a \in \mathbb{N} : mdc(a, 1) = 1$.

Teorema 0.7 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, existe sempre o* ***máximo divisor comum*** *de a e b.*

Este facto pode ser estabelecido teoricamente e resolvido na prática pelo

Algoritmo de Euclides para calcular $mdc(a, b)$; $a, b \in \mathbb{N}$,:

1 Inicializar $u = a$ e $v = b$;

2 Enquanto $v > 0$,, calcular $u = qv + r$ com $0 \leq r < v$, substituir u por v e v por r;

3 Quando $v = 0$, $u = mdc(a, b)$.

Calculamos o Máximo Divisor Comum de $a = 5324$ e $b = 1023$; designamos os sucessivos restos obtidos por r_i, sendo $r_{-1} = a$ e $r_0 = b$.

Exemplo 0.8 *seja* $a = r_{-1} = 5324$ *e* $b = r_0 = 1023$*; obtemos sucessivamente*

$$\begin{aligned} r_{-1} = 5324 = \quad & 5 \times 1023 + 209 = \quad q_1 r_0 + r_1 \\ r_0 = 1023 = \quad & 4 \times 209 + 187 = \quad q_2 r_1 + r_2 \\ r_1 = 209 = \quad & 1 \times 187 + 22 = \quad q_3 r_2 + r_3 \\ r_2 = 187 = \quad & 8 \times 22 + 11 = \quad q_4 r_3 + r_4 \\ r_3 = 22 = \quad & 2 \times 11 + 0 = \quad q_5 r_4 + r_5 \end{aligned}$$

Conclui-se que $mdc(5324, 1023) = 11$.

Corolário 0.9 *Se* $d = mdc\,(a, b)$ *, existem* $x, y \in \mathbb{Z}$:

$$xa + yb = d.$$

Os coeficientes x e y podem ser obtidos a partir da tabela de cálculo do $mdc(a, b)$, trabalhando "de baixo para cima", mas é preferível melhorar o algoritmo do seguinte modo:
como, para todo o $n > 0$, se tem $r_n = r_{n-2} - q_n r_{n-1}$, se já tivermos

$$r_{n-2} = x_{n-2}a + y_{n-2}b, \text{ e do mesmo modo } r_{n-1} = x_{n-1}a + y_{n-1}b$$

então obtemos igualmente uma combinação

$$r_n = x_n a + y_n b = (x_{n-2} - q_n x_{n-1})a + (y_{n-2} - q_n y_{n-1})b.$$

Podemos portanto ir calculando os coeficientes x_k e y_k ao mesmo tempo que calculamos os sucessivos r_k e q_k e chegar ao fim da aplicação do algoritmo, obtendo como resultado final o $mdc(a, b)$ e os coeficientes x e y da equação. Esta versão do algoritmo é habitualmente chamada **Algoritmo de Euclides estendido**.

A tabela seguinte descreve a aplicação do algoritmo de Euclides estendido a $a = 2163$ e $b = 910$:

				r_i	q_i	x_i	y_i
				2163		1	0
				910		0	1
$2163 =$	2×910	$+$	343	343	2	1	-2
$910 =$	2×343	$+$	224	224	2	-2	5
$343 =$	1×224	$+$	119	119	1	3	-7
$224 =$	1×119	$+$	105	105	1	-5	12
$119 =$	1×105	$+$	14	14	1	8	-19
$105 =$	7×14	$+$	7	7	7	-61	145
$14 =$	2×7	$+$	0				

Exercícios I

1. Calcular $d = mdc(a, b)$ e determinar os $x, y \in \mathbb{Z}$ tais que $d = ax + by$ nos casos seguintes:

   a) $a = 721 \qquad b = 448$

   b) $a = 341 \qquad b = 209$

   c) $a = 2163 \qquad b = 922$

   d) $a = 3794 \qquad b = 1122$

2. O menor múltiplo comum de dois números inteiros a, b define-se como o inteiro positivo $mmc(a, b)$ que é múltiplo de ambos e tal que

   $$a|c \wedge b|c \implies mmc(a, b)|c$$

   Mostrar que para a, b positivos se tem

   $$mmc(a, b) = \frac{ab}{mdc(a, b)}$$

3. A definição de máximo divisor comum generaliza-se para qualquer conjuntos finito de inteiros: se $a_1, a_2, \cdots, a_n$ são inteiros (não nulos) d é o seu máximo divisor comum se

   $$\forall 1 \leq i \leq n \; d \mid a_i, \text{ e } (\forall 1 \leq i \leq n \; c \mid a_i) \implies c \mid d.$$

a) Provar, por indução em n, que existe o máximo divisor comum de quaisquer $n > 2$ inteiros $a_1, a_2, \cdots, a_n$, que se verifica a seguinte recorrência:

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

e que se $d = mdc(a_1, a_2, \cdots, a_n)$, então existem inteiros $x_1, x_2, \cdots, x_n$ tais que

$$d = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

b) A fórmula de recorrência através da qual se prova na alínea anterior a existência do mdc e a sua representação como combinação dos a_i com coeficientes inteiros, não é prática para o calcular, para n muito maior que 2 (se a usássemos para programar esse cálculo, teríamos um algoritmo recursivo).
Em alternativa, podemos chegar ao resultado assim: dados $n > 2$ inteiros $a_1, a_2, \cdots, a_n$, definimos por recorrência a sucessão

$$d_1 = a_1, \qquad d_{k+1} = mdc(d_k, a_{k+1}).$$

Provar, mais uma vez por indução em n, que d_n é o máximo divisor comum de $a_1, a_2, \cdots, a_n$. Deste modo podemos calcular d os coeficientes x_i com menos cálculos do que pela fórmula anterior.

4. Neste exercício usamos a notação abreviada $(a_1, a_2, \cdots, a_n)$ para designar o máximo divisor comum dos inteiros $a_1, a_2, \cdots, a_n$.
O menor múltiplo comum é designado por $[a_1, a_2, \cdots, a_n]$.
Provar que se verificam as seguintes identidades ou dar um contra-exemplo:

a) $(ma, mb) = m(a, b)$ e $[ma, mb] = m[a, b]$ para $m \in \mathbb{N}$;

b) $((a, b), (a, c)) = (a, b, c)$ e $[[a, b], [a, c]] = [a, b, c]$;

c) $(a, b)(c, d) = (ac, ad, bc, bd)$;

d) se $(a, b) = (c, d)$ então $[a, b] = [c, d]$;

e) se $(a, b) = (c, d)$ então $(a^2, b^2) = (c^2, d^2)$;

f) $(ab, ac, b, c)[a, b, c] = abc$;

5. Mostrar que, dado um natural $a > 1$, se verifica

$$mdc\,(a^m - 1, a^n - 1) = a^{mdc(m,n)} - 1$$

Sugestão: verificar que se $m = qn + r$, com $0 \leq r < n$, então

$$a^m - 1 = a^r(1 + a^n + \cdots + a^{(q-1)n})(a^n - 1) + a^r - 1$$

e aplicar o algoritmo de Euclides.

6. Sejam $a_0, a_1, \cdots, a_n$ inteiros e $x = \dfrac{r}{s}$ um número racional (com $mdc(r, s) = 1$) tal que

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Mostrar que $s \mid a_n$ e $r \mid a_0$.

7. Mostar que a sucessão r_k de restos obtida pelo algoritmo de Euclides aplicado a inteiros $a > b > 0$ satisfaz $r_{k+2} < \frac{r_k}{2}$ e que portanto o número de passos necessário para o algoritmo terminar é majorado por $2\log_2(b)$.

8. Se $mdc(a, b) = 5$, quais os possíveis valores de

   a) $mdc(a + b, a - b)$?

   b) $mdc(a + 2b, 4a - b)$?

9. Quais os possíveis valores de $mdc(n^2 + 2, n^4 + 4)$?

10. Na aplicação aos inteiros a e b do algoritmo de Euclides estendido, obtêm-se a sucessão de restos

$$r_{-1} = a, r_0 = b, r_1, \cdots, r_m = mdc(a, b),$$

e a sucessão de pares x_i, y_i satisfazendo

$$r_i = ax_i + by_i,\ -1 \leq i \leq m.$$

Provar que, para todo o $i < m$ se tem

$$x_{i+1}y_i - x_i y_{i+1} = (-1)^i.$$

Definição 0.10 *Dizemos que a e b são* ***primos entre si*** *se $mdc(a,b)=1$, ou seja, a e b são primos entre si se e só se existem inteiros x e y tais que*

$$xa+yb=1$$

.

Se $a,b,c\in\mathbb{Z}$, e a e c são primos entre si, então existem inteiros x,y tais que

$$abx+cby=b,$$

e portanto $c\mid b$.

Se $mdc(a,b)=1$

$$a|c \text{ e } b|c \implies (ab)|c.$$

De facto, sabemos que existem inteiros u,v,x,y tais que $au+bv=1$ e $c=ax=by$. Portanto,

$$c=acu+bcv=ab(uy+vx).$$

Mais geralmente,

Se $a_1,a_2,\cdots,a_k$ são primos dois a dois, ou seja

$$mdc(a_i,a_j)=1 \qquad \forall\, i\neq j$$

então

$$a_i|c \quad \forall\, 1\leq i\leq k \implies (\prod_{i=1}^{k} a_i)|c$$

Se $d=mdc\,(a,b)$, a equação

$$ax+by=c$$

tem soluções $x, y \in \mathbb{Z}$ se e só se $d \mid c$.
Além disso, se (x_0, y_0) é uma solução desta equação, o conjunto de todas as soluções é constituído pelos pares de inteiros (x, y) da forma

$$x = x_0 + k\frac{b}{d} \quad ; \quad y = y_0 - k\frac{a}{d} \quad ; \quad k \in \mathbb{Z}.$$

Exercício 0.11 *Deduzir (ou estudar nas Notas) a demonstração.*

Definição 0.12 *Um inteiro $p > 1$ diz-se **primo** se os seus únicos divisores positivos são 1 e o próprio p.*

Os números primos caracterizam-se pela propriedade de dados $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ e p primo,

$$p \mid a_1 a_2 \ldots a_n \implies \exists i : p \mid a_i.$$

O conjunto dos números primos é infinito: Se $p_1, p_2, \cdots, p_m$ um qualquer conjunto finito de primos, os factores primos do número

$$N = p_1 p_2 \cdots p_m + 1$$

são diferentes dos p_i.

Teorema 0.13 *Teorema Fundamental da Aritmética*

Para cada inteiro $n > 1$, existem primos $p_1, p_2, \ldots, p_r$, tais que

$$n = p_1 p_2 \ldots p_r$$

e essa factorização é única a menos de permutação dos factores.

Designando por p_k o k-ésimo primo na ordem dos naturais ($p_1 = 2, p_2 = 3$, etc.) o Teorema é equivalente à afirmação de que para qualquer inteiro positivo n existe uma única sequência α_k de inteiros maiores ou iguais a zero tal que

$$n = \prod_k p_k^{\alpha_k}.$$

Exercícios II

1. Determinar o máximo divisor comum d de 843 e 312 e inteiros x, y tais que
$$d = 843x + 312y$$
com $0 < x < 100$.

2. Determinar os pares de inteiros x, y que satisfazem as condições
$$303x + 231y = 9, \qquad -100 < y < 100.$$

3. Seja b um inteiro. Provar por indução que, para todo o $m \geq 1$, se $a_1, a_2, \cdots a_m$ são inteiros e $mdc(a_i, b) = 1$, para todo o $i \leq m$, então $mdc(\prod_{i=1}^{m} a_i, b) = 1$.

4. Seja c um inteiro. Provar por indução que, para todo o $m \geq 1$, se $a_1, a_2, \cdots a_m$ são inteiros co-primos dois a dois (ou seja, se $i \neq j$ então $mdc(a_i, a_j) = 1$), entã
$$(\forall i \leq m,\ a_i \mid c) \implies \prod_{i=1}^{m} a_i \mid c.$$

5. Dada a sucessão definida por
$$A_1 = 2 \ \wedge \ A_{n+1} = A_n^2 - A_n + 1, \forall n,$$
mostrar que $mdc(A_i, A_j) = 1$ para quaisquer $i \neq j$.
Sugestão: provar que $\forall n \ A_{n+1} = A_1 A_2 \cdots A_n + 1$.

6. Com quantos zeros termina a expansão decimal de 100!?
   Sugestão: dado um primo p, quantos inteiros $1 \leq n \leq 100$ são divisíveis por p? e, para cada $k > 0$, quantos são divisíveis por p^k? Deduzir uma fórmula para o maior inteiro m que satisfaz $p^m \mid n!$.

7. Mostrar que

   a) Se $2^k - 1$ é primo então k é primo;

   b) Se $2^k + 1$ é primo então $k = 2^m$, para algum m.

8. Sejam a e b dois inteiros positivos com factorizações

$$a = \prod_k p_k^{\alpha_k}, \qquad b = \prod_k p_k^{\beta_k}.$$

   a) Determinar as factorizações de

$$ab^2, \qquad , mdc(a,b), \qquad mmc(a,b);$$

   b) provar alguns dos problemas 2 e 4 de **Exercícios I** usando essas factorizações.