A Teoria dos Números tem como objecto de estudo o conjunto $\mathbb{Z}$ dos números inteiros (a letra Z vem da palavra alemã *Zahl* que significa número).

1. DIVISIBILIDADE

A divisibilidade é o conceito principal da teoria dos números. Dela dependem, por exemplo, os conceitos de número par e número primo. Dizemos que a *divide* b (e escrevemos $a|b$) se existir um número inteiro m tal que $b = am$.

Nota histórica: Para sermos rigorosos deveríamos escrever $b = a \times m$ (notação de William Oughtred (1575-1660)), ou $b = a \cdot m$ (notação de Thomas Harriot (1560-1621)). No entanto, tornou-se usual escrever o produto omitindo o operador. Na Grécia Antiga esta omissão significava adição e ainda hoje escreve-se por vezes $1\frac{1}{2}$ para denotar "um e meio".

A divisibilidade tem a propriedade básica da transitividade, como vamos ver agora. Suponhamos que $a|b$ e $b|c$. Queremos mostrar que $a|c$. Como $a|b$, existe um número inteiro m tal que $b = am$. Do mesmo modo, existe um número inteiro n tal que $c = bn$. Então temos $c = (am)n = a(mn)$, e, uma vez que mn é um número inteiro, concluimos que $a|c$.

Em seguida, são indicadas outras propriedades da divisibilidade, cuja prova sugerimos como exercício.

Exercício. Prove que, para quaisquer inteiros a, b e c:

1. $1|a$;
2. $a|a$;
3. $a|(-a)$;
4. $a|b \wedge a|c \Rightarrow a|(b+c)$;
5. $a|b \Rightarrow a|bc$.

Se o número a não divide b, podemos ainda efectuar a divisão de b por a, mas obtemos agora um resto. O teorema seguinte garante-nos que essa divisão é sempre possível e que o quociente e o resto obtidos são únicos.

Teorema. *(Algoritmo da divisão inteira) Sejam a e b dois inteiros positivos. Então existem dois únicos inteiros q e r (chamados o* quociente *e o* resto*) tais que $0 \leq r < a$ e $b = aq + r$.*

Prova. Esta é uma prova de existência e unicidade, que aparece com bastante frequência nos mais diversos ramos da matemática.

Existência: Claramente existem vários pares de inteiros (q, r) que verificam a igualdade $b = aq + r$. A dificuldade está em encontrar um destes pares em que o resto r está entre 0 e $a - 1$. Uma vez que queremos que seja $r = b - aq$, consideremos todos os inteiros não negativos da forma

$$b - ak, \qquad k \in \mathbb{Z}.$$

Nesta colecção (infinita) de números não negativos, existe um que é mais pequeno que todos os outros (esta propriedade dos subconjuntos dos inteiros não negativos é chamada o *Princípio da Boa Ordenação*).

Esse número é o resto $r = b - aq$ que procurávamos. Para o ver, basta mostrar que $r < a$. De facto, se fosse $b - aq > a$, então teríamos $b - aq > b - a(q + 1) = (b - aq) - a \geq 0$ e portanto $b - aq$ não seria o menor inteiro positivo da forma $b - ak$.

Unicidade: Suponhamos que existem dois pares de inteiros (q, r) e (q', r') que verificam as condições exigidas. Podemos admitir que $0 \leq r \leq r' < a$.

Então $b = aq + r = aq' + r'$, pelo que $a(q - q') = r' - r$. Como $0 \leq r' - r < a$ e $r' - r$ é múltiplo de a, temos $r - r' = 0$, ou seja, $r = r'$. Facilmente se conclui agora que também $q = q'$. □

A prova pode ser adaptada para o caso em que a ou b são negativos. Neste caso o resto r pertence ao conjunto $\{0, 1, \ldots, |a| - 1\}$.

Exercício. Prove que, para qualquer inteiros n:

1. $2|n^2 - n$;
2. $6|n^3 - n$;
3. $30|n^5 - n$;
4. Se n é ímpar, então $8|n^2 - 1$;
5. Se n é ímpar e não é múltiplo de 3, então $6|n^2 - 1$.

2. MÁXIMO DIVISOR COMUM

Dados dois números positivos a e b, o *máximo divisor comum* é, como o nome indica, o maior número inteiro que divide simultaneamente a e b. Este número representa-se por $\mathrm{mdc}(a,b)$, ou mais simplesmente, por (a,b). Todos os pares de números inteiros têm pelo menos um divisor comum positivo, que é o número 1. Pode acontecer que este seja, de facto, o único divisor comum positivo de a e b; neste caso, dizemos que a e b são *primos entre si*.

Euclides (300 a.C.) desenvolveu um algoritmo para encontrar o máximo divisor comum de dois números naturais a e b. Segue-se uma descrição deste algoritmo.

Passo 1: Suponhamos que $b > a$ e efectuemos a divisão inteira de b por a. Obtemos um quociente q_1 e um resto r_1 tal que $0 \leq r_1 < a$: $\quad b = aq_1 + r_1$

Passo 2: Efectua-se a divisão inteira de a por r_1, obtendo-se um quociente q_2 e um resto r_2 tal que $0 \leq r_2 < r_1$: $\quad a = r_1q_2 + r_2$

Passo 3: Efectua-se a divisão inteira de r_1 por r_2, obtendo-se um quociente q_3 e um resto r_3 tal que $0 \leq r_3 < r_2$: $\quad r_1 = r_2q_3 + r_3$

$\vdots$

Passo n: Efectua-se a divisão inteira de r_{n-2} por r_{n-1}, obtendo-se um quociente q_n e um resto r_n tal que $0 \leq r_n < r_{n-1}$: $\quad r_{n-2} = r_{n-1}q_n + r_n$

Passo $n+1$: Efectua-se a divisão inteira de r_{n-1} por r_n, obtendo-se um quociente q_{n+1} e um resto $r_{n+1} = 0$: $r_{n-1} = r_nq_{n+1}$

O máximo divisor comum de a e b é r_n.

Exemplificando para $a = 14$, $b = 24$, temos

- $24 = 14 \times 1 + 10$
- $14 = 10 \times 1 + 4$
- $10 = 4 \times 2 + 2$
- $4 = 2 \times 2$

O último resto não nulo é 2, logo $\mathrm{mdc}(14,24) = 2$.

Porque razão funciona este método?

Notemos $d = \mathrm{mdc}(a,b)$. No primeiro passo, obtemos um resto $r_1 = b - aq_1$ que é múltiplo de d, uma vez que a e b são múltiplos de d. No segundo passo, obtemos um resto $r_2 = a - r_1q_2$ que é múltiplo

de d, uma vez que a e r_1 são múltiplos de d. Continuando este processo, concluimos que os restos que aparecem em cada um dos passos são múltiplos de d. Em particular tem-se $d|r_n$.

Por outro lado, como $r_{n+1} = 0$ conclui-se do passo $n+1$ que $r_n|r_{n-1}$. Em seguida, vemos através do passo n que $r_n|r_{n-2}$, e assim sucessivamente, até chegar à conclusão que $r_n|a$ e finalmente que $r_n|b$. Assim, r_n é um divisor comum de a e b, pelo que $r_n \leq d$.

Por fim, concluimos dos dois parágrafos anteriores que $r_n = d$.

Exercício. Justifique que o algoritmo de Euclides termina num número finito de passos, isto é, que ao fim de um certo número de passos, chegamos a um resto nulo.

Exercício. Usando o algoritmo de Euclides, determine:

1. $\mathrm{mdc}(120, 80)$
2. $\mathrm{mdc}(13377, 10569)$
3. $\mathrm{mdc}(n, n+1)$
4. $\mathrm{mdc}(n, n+2)$

Exercício.

1. Usando o algoritmo de Euclides, determine $\mathrm{mdc}(144, 89)$.
2. Os números 144 e 89 são dois números de Fibonacci consecutivos. Prove por indução que dois números de Fibonacci consecutivos são sempre primos entre si.

O algoritmo de Euclides permite-nos mostrar algumas propriedades importantes do máximo divisor comum, cuja prova é deixada como exercício.

Exercício. Prove que, para quaisquer inteiros positivos a, b e c:

1. $\mathrm{mdc}(ca, cb) = c\,\mathrm{mdc}(a, b)$;
2. $c|a \wedge c|b \Rightarrow \mathrm{mdc}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\mathrm{mdc}(a,b)}{c}$; (portanto o máximo divisor comum de a e b é múltiplo de todos os divisores comuns de a e b)
3. Se $d = \mathrm{mdc}(a, b)$, então existem inteiros x e y tais que $d = ax + by$;
4. Se $c = ax + by$, então $\mathrm{mdc}(a, b)|c$;
5. Se $1 = ax + by$, então $\mathrm{mdc}(a, b) = 1$.

Exercício. Determine, caso existam, todos os inteiros positivos tais que:

i. $x + y = 100$ e $\mathrm{mdc}(x, y) = 3$; ii. $x + y = 100$ e $\mathrm{mdc}(x, y) = 5$.

3. NÚMEROS PRIMOS

Um número diz-se *primo* se tiver exactamente dois divisores positivos. O matemático grego Eratóstenes (276-194 a.C.) desenvolveu um método simples para encontrar todos os números primos entre os primeiros n inteiros positivos. Este método, descrito a seguir, para o caso $n = 50$, é conhecido por *Crivo de Eratóstenes*.

- Escrevem-se todos os números inteiros de 2 até 50;

	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

- Eliminam-se (riscam-se) todos os múltiplos de 2, maiores que 2.

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49

- Eliminam-se todos os múltiplos de 3, maiores que 3.

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49

- O número que se segue ao 3 na lista é o 5. Eliminam-se todos os múltiplos de 5, maiores que 5.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49

- Finalmente eliminam-se os múltiplos de 7, maiores que 7.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	

- O processo terminou porque o número seguinte ao quadrado, 11^2, é maior do que 50. Os números que restam são todos os números primos inferiores ou iguais a 50.

A lista dos números primos positivos começa da seguinte forma:

[1,50]	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
[51,100]	53	59	61	67	71	73	79	83	89	97					
[101,150]	101	103	107	109	113	127	131	137	139	149					
[151,200]	151	157	163	167	173	179	181	191	193	197	199				
[201,250]	211	223	227	229	233	239	241								
[251,300]	251	257	263	269	271	277	281	283	293						
[301,350]	307	311	313	317	331	337	347	349							
[351,400]	353	359	367	373	379	383	389	397							
[401,450]	401	409	419	421	431	433	439	443	449						
[451,500]	457	461	463	467	479	487	491	499							
[501,550]	503	509	521	523	541	547									
[551,600]	557	563	569	571	577	587	593	599							
[601,650]	601	607	613	617	619	631	641	643	647						
[651,700]	653	659	661	673	677	683	691								
[701,750]	701	709	719	727	733	739	743								
[751,800]	751	757	761	769	773	787	797								
[801,850]	809	811	821	823	827	829	839								
[851,900]	853	857	859	863	877	881	883	887							
[901,950]	907	911	919	929	937	941	947								
[951,1000]	953	967	971	977	983	991	997								
		⋮													
[9951,10000]	9949	9967	9973												

Algo que se pode observar desde já é que os números primos parecem ir rareando à medida que se avança no conjunto dos números naturais. É por isso razoável a seguinte questão:

Será que a partir de uma dada altura os números primos se extinguem?

Veremos em breve que a resposta a esta questão é negativa.

Exercício. Prove que, se p é um número primo, então, para quaisquer inteiros a e b, $p|ab \Rightarrow p|a \vee p|b$.

4. FACTORIZAÇÃO EM NÚMEROS PRIMOS

Teorema. *(Teorema Fundamental da Aritmética) Qualquer número inteiro superior a 1 pode ser factorizado em números primos positivos. Além disso, esta factorização é única, a menos de permutação dos factores.*

Prova. Estamos novamente na presença de uma demonstração de existência e unicidade (neste caso da factorização em números primos positivos).

Existência: Vamos usar o método de indução. O número 2 é primo, logo a sua factorização em números primos é trivial ($2 = 2$). Suponhamos que todos os números desde 2 até $n-1$ possuem uma factorização em números primos positivos e consideremos o número n. Se n é primo, a sua factorização é trivial. Se não o for, então possui um divisor positivo a diferente de 1 e de n. Assim, existe um inteiro b tal que $n = ab$. Mas a e b são inteiros entre 2 e $n - 1$, logo, por hipótese de indução, possuem factorizações em números primos positivos:

$$a = p_1 \dots p_k \qquad\qquad b = q_1 \dots q_l$$

Conclui-se por isso que n possui a factorização $m = p_1 \dots p_k q_1 \dots q_l$.

Unicidade: Utilizemos novamente o método de indução. É claro que o número 2 só pode ser factorizado de uma única forma, uma vez que é um número primo. Admitamos que todos os números desde 2 até $n - 1$ possuem uma única factorização em números primos positivos.

Suponhamos que o número n possui duas factorizações em números primos positivos, isto é,

$$n = p_1 \dots p_k = q_1 \dots q_l.$$

Então $p_1|q_1 \dots q_l$ e portanto $p_1|q_1 \vee p_1|q_2 \vee \dots \vee p_1|q_l$. Suponhamos, sem perda de generalidade, que $p_1|q_1$. Como $p_1 > 1$ então, por definição de número primo, tem-se $p_1 = q_1$. Assim, o número inteiro

$\frac{n}{p_1}$ tem duas factorizações em números primos positivos, e por hipótese de indução, esta é única. Logo, após permutação dos números primos de uma das factorizações, concluimos que $k = l$ e que $p_2 = q_2$, $p_3 = q_3, \ldots, p_k = q_k$. □

A factorização de um número em primos fornece-nos outro método para calcular o máximo divisor comum de a e b. Para tal, basta observar que os factores primos de qualquer divisor de a formam um subconjunto dos factores primos de a, passando-se o mesmo em relação a b. Assim, o máximo divisor comum de a e b é o produto dos factores primos comuns a a e b.

Voltando ao exemplo atrás apresentado, temos $24 = 2\times2\times2\times3$ e $14 = 2\times7$, pelo que $\mathrm{mdc}(14, 24) = 2$.

Teorema. *Existe uma infinidade de números primos.*

Prova. Suponhamos que existe apenas um número finito de números primos e designemo-los por $p_1 < p_2 < \ldots < p_k$. Notemos

$$N = p_1 \ldots p_k + 1.$$

Então $p_1, \ldots, p_k$ não dividem N e portanto na factorização de N em números primos têm de aparecer factores superiores a p_k, o que contradiz a hipótese que $p_1, \ldots, p_k$ era a lista de todos os primos. □

Observação. Nesta prova não se mostrou que somando 1 aos primeiros k primos se obtém um novo número primo. De facto, $2 + 1$, $2 \times 3 + 1$, $2 \times 3 \times 5 + 1$, $2 \times 3 \times 5 \times 7 + 1$, $2 \times 3 \times 5 \times 7 \times 11 + 1$ são todos primos, mas $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 509 \times 59$ não o é.

Ao observar a lista dos primeiros números primos encontramos vários pares de números primos que diferem por apenas duas unidades. Por exemplo, temos os pares $(5, 7)$, $(311, 313)$ e $(599, 601)$. É conjecturado que existe uma infinidade de pares deste tipo, mas não é conhecida nenhuma prova.

Exercício. Na mesma lista encontramos um triplo de números primos $(3, 5, 7)$ da forma $(n, n+2, n+4)$. Mostra que este é o único triplo de primos desta forma.