O TEOREMA FUNDAMENTAL DA ARITMÉTICA

FERNANDO FERREIRA

Denotamos por $\mathbb{N}$ o conjunto dos números naturais $\{1, 2, 3, \ldots\}$ e por $\mathbb{Z}$ o conjunto dos números inteiros. Dados dois números inteiros a e b, diz-se que a *divide* b, e escreve-se $a \mid b$, se existir um inteiro c tal que $b = ac$. Mostra-se imediatamente que se $a \mid b$ e $a \mid c$ então $a \mid (bn + ck)$, para $n, k \in \mathbb{Z}$.

Definição 1. *Um número natural $n > 1$ diz-se* primo *se os seus únicos divisores positivos são 1 e n.*

Um número natural $n > 1$ que não é primo diz-se um número *composto*. O número 1 nem é primo nem composto.

Teorema fundamental da aritmética. *Todo o número natural pode ser escrito como produto de números primos. Esse produto é único a menos da ordem dos fatores.*

A parte mais importante deste teorema é a asserção de unicidade. A presente secção é maioritariamente dedicada a esta demonstração. A asserção de existência demonstra-se facilmente por indução completa. Na formulação do teorema, o leitor pode estar preocupado com o caso do número 1 ou, mesmo, com os números primos. O número 1 é um produto de zero primos pois, convencionalmente, um produto sem fatores tem como resultado 1. Este caso é excecional na medida em que em todos os outros casos a fatorização é não vazia (há, pelo menos, um fator) e, portanto, todo o número natural diferente de 1 é divisível por pelo menos um primo. No caso do número ser primo, esse número é um produto de primos com um único fator (o próprio primo).

Definição 2. *Sejam $a, b \in \mathbb{N}$. Define-se o* máximo divisor comum *de a e b como sendo o número natural* $\max\{d \in \mathbb{N} : d \mid a \text{ e } d \mid b\}$. *Este número denota-se por* $\mathrm{mdc}(a, b)$.

Note-se que, nesta definição, estamos a considerar o máximo dum conjunto finito e não vazio de números naturais (dado que 1 está no conjunto e que um divisor positivo dum número natural não excede esse número). Tem-se, obviamente, que se $b \mid a$ então $\mathrm{mdc}(a, b) = b$. Também se tem que $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, a + bs)$, onde $s \in \mathbb{Z}$ (desde que $a + bs$ seja um inteiro positivo). Esta igualdade é consequência da igualdade dos conjuntos $\{d \in \mathbb{N} : d \mid a \text{ e } d \mid b\}$ e $\{d \in \mathbb{N} : d \mid b \text{ e } d \mid (a + bs)\}$.

Dizemos que dois números naturais a e b são *coprimos* ou *primos entre si* se $\mathrm{mdc}(a, b) = 1$. Neste caso, escrevemos $a \perp b$.

Divisão inteira. *Sejam $a, b \in \mathbb{N}$. Então existem números inteiros não negativos q e r com $a = bq + r$ e $0 \leq r < b$. Estes números são únicos e denominam-se, respetivamente, por* cociente *e* resto *da divisão inteira de a por b.*

Demonstração. Tome-se q máximo tal que $bq \leq a$. Note-se que há pelo menos um número nestas circunstâncias (o número 0) e que q não excede a. A parte de existência do resultado segue-se obviamente do facto de que $a - bq < b$. Este facto é muito fácil de argumentar por absurdo. Com efeito, se $a - bq \geq b$, viria $b(q + 1) \leq a$ o que contradiz a maximalidade de q.

A parte da unicidade é deixada ao cuidado do leitor. □

Estamos em condições de descrever o algoritmo de Euclides para calcular o máximo divisor comum de dois números naturais a e b, com $a \geq b$. Para calcular o $\mathrm{mdc}(a, b)$, obtenha-se o resto

r de a por b. Se o resto é 0 (a chamada cáusula de escape do algoritmo) então $b \mid a$ e, portanto, $\mathrm{mdc}(a,b) = b$. Caso contrário, calcule-se $\mathrm{mdc}(b,r)$. Note-se que este valor é o $\mathrm{mdc}(a,b)$, pois r é a subtraído dum múltiplo de b. Repita-se este procedimento até chegar à cláusula de escape. Note-se que se tem que chegar à cláusula de escape porque a segunda entrada do máximo divisor comum vai decrescendo e, portanto, o resto tem que atingir 0. Eis um exemplo: $\mathrm{mdc}(30,21) = \mathrm{mdc}(21,9) = \mathrm{mdc}(9,3) = 3$.

Este algoritmo é muito eficiente. O cálculo dos sucessivos restos pode ser feito eficientemente através do algoritmo da divisão que aprendemos na infância (os algoritmos da soma, subtração e multiplicação então também aprendidos são, igualmente, eficientes). Não é difícil de mostrar que o número de iterações do algoritmo de Euclides é pequeno: é, de facto, majorado pelo dobro do comprimento do número a quando escrito em notação posicional binária.

Desde os anos setenta do século passado que a teoria dos números (de facto, a parte mais acessível desta teoria) tem tido aplicações importantes e fundamentais em criptografia. Estas aplicações asseguram a segurança do trânsito digital e já fazem parte do modo de viver atual. Falaremos neste curso de algumas destas aplicações criptográficas (troca de chaves Diffie-Helman, protocolo El Gamal, criptosistema RSA, criptografia de curvas elípticas, etc). É fundamental para estas aplicações que certos algoritmos sejam muito eficientes. É por isso que, ao longo do curso, falaremos de quando em quando na eficiência (ou não) de alguns algoritmos.

Lema 1. *Sejam $a, b, n \in \mathbb{N}$. Tem-se* $\mathrm{mdc}(an, bn) = n\,\mathrm{mdc}(a,b)$.

Demonstração. Fixe-se $n \in \mathbb{N}$. Sem perda de generalidade, $b \leq a$. Argumenta-se por indução completa em $a+b$. Sejam q e r o cociente e resto (respetivamente) da divisão de a por b. Se $r = 0$, vem $b \mid a$ (e, consequentemente, $bn \mid an$). Logo $\mathrm{mdc}(a,b) = b$ e $\mathrm{mdc}(an,bn) = bn$. Este caso está verificado.

Consideremos agora o caso em que $a = bq + r$, com $0 < r < b$. Dado que $b + r < a + b$, por hipótese de indução completa, tem-se $\mathrm{mdc}(bn, rn) = n\,\mathrm{mdc}(b,r)$. Vem

$$\mathrm{mdc}(an, bn) = \mathrm{mdc}(bn, rn) = n\,\mathrm{mdc}(b,r) = n\,\mathrm{mdc}(a,b)$$

A primeira igualdade justifica-se porque $rn = an - (bn)q$. □

Com este lema, podemos demonstrar o seguinte resultado importante: o máximo divisor comum de dois números naturais não é somente o maior dos divisores comuns, como é múltiplo de todos os divisores comuns.

Proposição 1. *Sejam $a, b, d \in \mathbb{N}$. Se $d \mid a$ e $d \mid b$, então $d \mid \mathrm{mdc}(a,b)$.*

Demonstração. Suponhamos que $d \mid a$ e $d \mid b$. Então existem $k, s \in \mathbb{N}$ tais que $a = dk$ e $b = ds$. Vem $\mathrm{mdc}(a,b) = \mathrm{mdc}(dk, ds) = d\,\mathrm{mdc}(k,s)$. Logo, $d \mid \mathrm{mdc}(a,b)$. □

Teorema 1 (Euclides)**.** *Seja p um número primo e $a, b \in \mathbb{N}$. Suponhamos que $p \mid ab$. Então $p \mid a$ ou $p \mid b$*

Demonstração. Se $p \mid a$, já temos o pretendido. Suponhamos que $p \nmid a$. Então $\mathrm{mdc}(p,a) = 1$. Logo, $\mathrm{mdc}(pb, ab) = b\,\mathrm{mdc}(p,a) = b$. Dado que $p \mid pb$ e, por hipótese, $p \mid ab$, conclui-se pela proposição anterior que $p \mid b$. □

Este é o facto charneira da demonstração da parte da unicidade do teorema fundamental da aritmética. Seja, então, n um número natural e suponhamos que $n = q_1 \cdot q_2 \cdot \ldots \cdot q_k$ e $n = r_1 \cdot r_2 \cdot \ldots \cdot r_l$, onde tanto q_1, q_2, …, q_k como r_1, r_2, …, r_l são números primos (não necessariamente distintos). Queremos demonstrar que os primos que ocorrem na primeira fatorização são exatamente os mesmos (contando as repetições) primos que aparecem na segunda fatorização. A demonstração é por indução completa em n. No caso em que $n = 1$, não ocorrem primos nem na primeira nem na segunda fatorização ($k = l = 0$) e, portanto, tem-se o resultado. Suponhamos que $n > 1$. Neste

caso, tome-se um número primo p com $p \mid n$. Logo, $p \mid (q_1 \cdot q_2 \cdot \ldots \cdot q_k)$. Pela proposição anterior, sai então facilmente que $p \mid q_i$, para algum $1 \leq i \leq k$. Como ambos p e q_i são primos, sai que $p = q_i$. Sem perda de generalidade, podemos supor que $p = q_1$ (simplesmente reordenam-se os primos da primeira fatorização). De modo análogo, e também sem perda de generalidade, $p = r_1$. Tem-se então que $q_2 \cdot \ldots \cdot q_k = r_2 \cdot \ldots \cdot r_l$. Este número m é menor do que n, já que $n = pm$. Logo, por hipótese de indução completa, os primos que ocorrem em q_2, ..., q_k são exatamente os mesmos primos que ocorrem em r_2, ..., r_l. O resultado segue-se.

Terminamos esta secção com um facto bem conhecido.

Teorema 2 (Euclides)**.** *Há um número infinito de primos.*

Demonstração. Suponhamos, com vista a um absurdo, que apenas existe um número finito de primos. Sejam eles $p_1, p_2, \ldots, p_k$. Considere-se o número natural $n = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1$. Este número tem um fator primo, digamos p. Dado que p é um dos primos $p_1, p_2, \ldots, p_k$, vem $p \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_k)$. Como p também divide n sai imediatamente que p divide a diferença, ou seja, $p \mid 1$. Isto é uma contradição. □

Numa próxima secção iremos dar outra demonstração da infinitude dos números primos. Mostraremos um resultado de Euler que afirma que $\sum_{p\ primo} \frac{1}{p} = +\infty$.