Introdução à Teoria dos Números
Ficha Complementar: números perfeitos

Definição 0.1 $\sigma : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ *designa a função que a cada natural positivo faz corresponder a soma dos seus divisores positivos:*

$$\sigma(n) = \sum_{0<d|n} d.$$

Por exemplo, $\sigma(10) = 1 + 2 + 5 + 10 = 18$.

Notação 0.2 *No que se segue, usaremos a notação $s(n)$ para representar a soma dos divisores positivos próprios de n, ou seja, $s(n) = \sigma(n) - n$.*

1. Mostrar que σ é uma **função multiplicativa**: se $mdc(m, n) = 1$ então $\sigma(mn) = \sigma(m)\sigma(n)$ e que se $n = \prod_i p_i^{k_i}$ então

$$\sigma(n) = \prod_i \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

Os matemáticos da escola de Pitágoras designavam por **números perfeitos** aqueles que satisfaziam $\sigma(n) = 2n$, ou de modo equivalente, $s(n) = n$, ou seja, aqueles números em que "o todo é a soma das partes". Vamos introduzir termos para designar as possíveis relações entre um número e a soma dos seus divisores próprios:

Definição 0.3 *Um natural $n > 0$ diz-se*

1. ***perfeito*** *se $s(n) = n$,*
2. ***abundante*** *se $s(n) > n$ e*
3. ***escasso*** *se $s(n) < n$.*

2. Demonstrar o seguinte teorema de Euclides:

Teorema 0.4 *Se $2^t - 1$ é primo então $2^{t-1}(2^t - 1)$ é perfeito.*

Nota 0.5 *A condição $2^t - 1$ é primo implica que t é primo (porquê?). Os números da forma $2^n - 1$ com n primo designam-se por números de Mersenne, em homenagem ao matemático e teólogo francês Marin Mersenne (1588-1648), e os primos dessa forma são os primos de Mersenne. A investigação sobre estes números continua activa e em Dezembro de 2018 foi descoberto o maior primo de Mersenne conhecido até agora:*

$$2^{82589933} - 1$$

um número primo cuja representação decimal tem 24862048 *algarismos...*

Cerca de vinte séculos depois de Euclides, Euler demonstrou a seguinte recíproca parcial:

Teorema 0.6 *Se N é um número perfeito* par *então existe um primo n tal que $N = 2^{n-1}(2^n - 1)$ e $2^n - 1$ é primo.*

3. Demonstrar este teorema de Euler:

a) Escrever $N = 2^{n-1}t$, com t ímpar e $n > 1$; usar a hipótese de que N é perfeito e as propriedades da função σ para obter uma expressão para $\sigma(t)$, dependente de t e n;

b) deduzir de a) que $\frac{t}{2^n-1}$ é inteiro e portanto um dos divisores de t;

c) concluir que $t = 2^n - 1$ é primo.

Continua em aberto, entre muitos outros relacionados com este, o problema de saber se existem números perfeitos ímpares. Pode-se começar a perceber a dificuldade do problema estudando condições para que um número ímpar seja abundante (ou escasso).

4. Mostrar que se m é abundante, então mn também o é, para qualquer $n > 0$.

5. Mostrar que se p é um primo ímpar, $p2^k$ é abundante se $p < 2^{k+1} - 1$ e escasso se $p > 2^{k+1} - 1$.
Como se generaliza este resultado para números da forma $p^2 2^k$?

6. Usando a expressão obtida acima para $\sigma(m)$, mostrar que se $m = \prod_{i=1}^{l} p_i^{k_i}$, com $k_i > 0$ para todo o i, é a factorização de m em factores primos, então

$$\prod_{i=1}^{l}\left(1 + \frac{1}{p_i}\right) \leq \frac{\sigma(m)}{m} < \prod_{i=1}^{l} \frac{p_i}{p_i - 1},$$

e que a primeira desigualdade é estrita se e só se para algum $1 \leq i \leq l$ se tem $k_i > 1$.

7. Deduzir a partir das desigualdades do enunciado anterior (e da sua demonstração):

a) Não existe nenhum m abundante ou perfeito ímpar só com dois factores primos;

b) Só existe m abundante ou perfeito ímpar com exactamente três factores primos para as triplas de primos $\{3, 5, 7\}$, $\{3, 5, 11\}$, $\{3, 5, 13\}$, e para cada um destes casos existem infinitos m abundantes nessas condições;

c) Se m é abundante ou perfeito e ímpar e $3 \nmid m$ então m tem pelo menos 7 factores primos distintos; se, além disso, $5 \nmid m$, m tem pelo menos 15 factores primos distintos;

d) Se $m = 3^i 5^j \times n$, onde n é um produto de factores primos maiores que 5, e $i > 1$ e $j > 1$, então m é abundante (e portanto não perfeito).

Um outro problema relacionado com este tema é o da determinação de ciclos para a função $s(n)$: existem vários pares m, n tais que $s(m) = n$ e $s(n) = m$ (os pares de inteiros "amigáveis"), embora não exista uma caracterização completa destes pares. Existem, isso sim, algumas fórmulas para obter pares amigáveis, como por exemplo a seguinte, descoberta pelo matemático árabe do século IX, Al-Ṣābiʾ Thābit ibn Qurra al-Ḥarrānī :

8. Mostrar que, dado $k > 1$, se os inteiros

$$p = 3 \times 2^{k-1} - 1, \qquad q = 3 \times 2^k - 1 \text{ e } r = 9 \times 2^{2k-1} - 1$$

são primos, então

$$m = 2^k pq \text{ e } n = 2^k r$$

são amigáveis.

Não se conhece nenhum par m, n de inteiros amigáveis com paridade diferente.

Existem ciclos de comprimento maior para $s(n)$, ou seja, inteiros positivos $m_1, m_2, \cdots, m_k$, com $k > 2$, tais que

$$s(m_i) = m_{i+1} \; \forall i < k, \text{ e } s(m_k) = m_1.$$

Mas o estudo computacional destes ciclos, e mais geralmente das órbitas de $s(n)$, depende da nossa capacidade de calcular $s(n)$, ou seja, de factorizar um inteiro n.