Funções Aritméticas

Por Gabriel Bastos e João Lemos

O que são Funções Aritméticas

Uma função aritmética é uma função definida sobre o conjunto dos números naturais e que assumem valores reais ou complexos. As funções φ de Euler, quantidade de divisores de um número, soma dos divisores de um número são exemplos das funções aritméticas mais importantes. O objetivo deste artigo é apresentar ao leitor propriedades importantes sobre algumas dessas funções e sobre o comportamento assintótico delas. Além disso, aproveitamos para deixar claro que um divisor de um natural é um divisor positivo, e que $\mathbb{N}$ representa o conjunto dos inteiros positivos.
Dada uma função $g\colon \mathbb{N} \to \mathbb{R}$, dizemos que $g = O(f)$, com $f\colon \mathbb{N} \to \mathbb{R}^+$ se $\frac{|g(n)|}{f(n)} \leq c$ para alguma constante $c > 0$ e todo n suficientemente grande, e dizemos que $g = o(f)$ se $\lim_{n\to\infty} \frac{|g(n)|}{f(n)} = 0$. Ainda mais, denotamos log como o logaritmo natural.

1 Funções Multiplicativas

Uma função f definida sobre $\mathbb{N}$ é *multiplicativa* se, para todos m e n naturais com $\text{mdc}(m,n) = 1$, temos que $f(mn) = f(m)f(n)$. Caso a igualdade $f(mn) = f(m)f(n)$ ocorra para todos os naturais m e n, dizemos que f é *totalmente multiplicativa.* Alguns exemplos de funções multiplicativas são

$$\varphi(n) = n \prod_{\substack{p\mid n \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right); \quad d(n) = \sum_{d\mid n} 1 \quad \text{e} \quad \sigma(n) = \sum_{d\mid n} d$$

Começamos com o seguinte

Exemplo 1.1. *Mostre que, para todo $n \geq 1$, existe um inteiro m para o qual $\varphi(m) = n!$.*

SOLUÇÃO. Primeiro, veja que a função φ satisfaz as seguintes propriedades:
1. Se $p \nmid n$ é primo, então $\varphi(pn) = \varphi(p)\varphi(n) = (p-1)\varphi(n)$ pela multiplicatividade de φ;
2. Se $p|n$, então $\varphi(p^a n) = p^a\varphi(n)$, uma vez que os divisores primos de pn são os mesmos que os divisores primos de n.
Essa análise nos diz o que acontece quando "adicionamos" um primo no número n. Como queremos construir um m tal que $\varphi(m) = n!$, a melhor forma de fazer isso é "adicionar" primos no m. Façamos alguns casos iniciais: $\varphi(2) = 1 = 1!$; $\varphi(2\cdot 3) = 2 = 2!$; $\varphi(2\cdot 3^2) = 3\varphi(2\cdot 3) = 3!$; $\varphi(2\cdot 3^2\cdot 5) = 4\varphi(2\cdot 3^2) = 4!$.
Vamos supor que, para algum n, exista um inteiro m com $\varphi(m) = n!$. Como construiríamos um m' com $\varphi(m') = (n+1)! = (n+1)\varphi(m)$? Se $n+1 = p-1$, com p primo, seria bom que $p \nmid m$, que daí poderíamos tomar $m' = pm$. Se $p_1, p_2, \ldots, p_k$ são os divisores primos de $n+1$, seria bom que $p_1p_2\ldots p_k | m$, pois poderíamos adicionar potências de $p_1, p_2, \ldots, p_k$ em m para construir m', já que teríamos $\varphi(p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}m) = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}\varphi(m)$.
Assim, podemos construir m com $\varphi(m) = n!$ indutivamente, mas adicionaremos uma hipótese sobre m: os divisores primos de m são $p_1, p_2, \ldots, p_i$, onde $2 = p_1 < p_2 < \cdots$ é a sequência dos números primos.
Essa condição é satisfeita para os casos pequenos de n que fizemos, e vamos mostrar que podemos mantê-la. De fato, se $\varphi(m) = n!$ satisfaz a condição imposta, suponha primeiro que $p_i \leq n+1 \leq p_{i+1} - 2$. Então basta tomar $m' = (n+1)m$, pois primos que dividem $n+1$ também dividem m. Se $n+1 = p_{i+1} - 1$, basta tomar $m' = p_{i+1}m$, pois $p_{i+1} \nmid m$, de modo que $\varphi(p_{i+1}m) = (p_{i+1}-1)\varphi(m) = (n+1)!$. Agora, m' tem como divisores primos $p_1, p_2, \ldots, p_{i+1}$, de modo que a hipótese sobre m se mantém, e acabamos o problema. □

Teorema 1.2. *Se f é uma função multiplicativa, então*

$$F(n) = \sum_{d\mid n} f(d)$$

também é multiplicativa.

DEMONSTRAÇÃO. Sejam m e n inteiros positivos com $\text{mdc}(m,n)=1$, então qualquer divisor de mn pode ser escrito da forma $d\cdot e$, com $d|m$ e $e|n$, ou seja, $\text{mdc}(d,e)=1$. Assim,

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) = \sum_{d|m,e|n} f(d)f(e) \\ &= \sum_{d|m}\sum_{e|n} f(d)f(e) = \sum_{d|m} f(d)\sum_{e|n} f(e) \\ &= F(m)F(n). \end{aligned}$$

Portanto, F também é multiplicativa. □

Com o teorema 1.2 provado, podemos concluir o seguinte e importante

Lema 1.3. *Para todo n vale que*

$$\sum_{d|n} \varphi(n) = n.$$

DEMONSTRAÇÃO. Como φ é multiplicativa, a função $f(n)=\sum_{d|n}\varphi(n)$ também é. Assim, basta mostrar que $f(p^k)=p^k$, com p primo e $k\geq 0$ inteiro:

$$f(p^k) = \sum_{i=0}^{k} \varphi(p^i) = 1+(p-1)\sum_{i=1}^{k} p^{i-1} = 1+(p-1)\left(\frac{p^k-1}{p-1}\right) = p^k.$$

□

O teorema 1.2 também pode ser usado para provar que a função $\sigma_\alpha(n)=\sum_{d|n} d^\alpha$, com $\alpha\in\mathbb{R}$, é multiplicativa, já que $f(n)=n^\alpha$ é multiplicativa; em particular, $d(n)$ e $\sigma(n)$ são funções multiplicativas.

Exemplo 1.4. *Mostre que $\varphi(n)d(n)\geq n$.*

SOLUÇÃO. Note que $\varphi(n)\geq\varphi(d)$ se $d|n$, já que $\varphi(p^k)\geq\varphi(p^l)$ se $k\geq l$ e φ é multiplicativa. Logo, utilizando o lema 1.3,

$$\varphi(n)d(n) \geq \sum_{d|n}\varphi(d) = n.$$

□

O próximo resultado caracteriza as funções totalmente multiplicativas e monótonas.

Proposição 1.5. *Uma função $f\colon\mathbb{N}\to\mathbb{R}^+$ que é totalmente multiplicativa e monótona pode ser escrita da forma $f(n)=n^\alpha$, com $\alpha\in\mathbb{R}$.*

DEMONSTRAÇÃO. Podemos supor, sem perdas, que f é crescente; de fato, se f satisfaz as condições do enunciado, $1/f$ também satisfaz. Além disso, veja que uma função totalmente multiplicativa satisfaz $f(a^b)=f(a)^b$ para todos a,b naturais. Note que existe $\alpha\in\mathbb{R}$ para o qual $f(2)=2^\alpha$ e, portanto, $f(2^k)=2^{\alpha}k$ para todo k natural. Para cada n, sabemos que

$$\begin{aligned} & 2^{\lfloor k\log_2 n\rfloor} \leq n^k \leq 2^{\lfloor k\log_2 n\rfloor+1} \\ \Longrightarrow & 2^{\alpha\lfloor k\log_2 n\rfloor} \leq f(n)^k \leq 2^{\alpha(\lfloor k\log_2 n\rfloor+1)} \quad \text{(apenas usamos que } f \text{ é crescente)} \\ \Longrightarrow & 2^{\alpha\frac{\lfloor k\log_2 n\rfloor}{k}} \leq f(n) \leq 2^{\alpha\frac{(\lfloor k\log_2 n\rfloor+1)}{k}} \end{aligned}$$

Mas sabemos que

$$\lim_{k\to\infty}\frac{(\lfloor k\log_2 n\rfloor+1)}{m} = \lim_{k\to\infty}\alpha\frac{\lfloor k\log_2 n\rfloor}{k} = \alpha\log_2 n.$$

Assim, pelo Teorema do Confronto, temos que $f(n)=2^{\alpha\log_2 n}=n^\alpha$, como queríamos. □

Exemplo 1.6 (Números Perfeitos)**.** *Um número perfeito é um número n tal que $\sigma(n)=2n$. Mostre que todo número perfeito par pode ser escrito da forma $2^{p-1}(2^p-1)$, onde 2^p-1 é um número primo.*

SOLUÇÃO. Seja n um número perfeito. Escreva $n = 2^k m$, com m ímpar e $k > 0$. Sabemos que

$$2n = \sigma(n) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m)$$
$$\Longrightarrow \frac{2^{k+1}}{2^{k+1} - 1} = \frac{\sigma(m)}{m}.$$

Como $2^{k+1}/(2^{k+1}-1)$ é uma fração irredutível, sabemos que existe um inteiro t tal que $\sigma(m) = 2^{k+1}t$ e $m = (2^{k+1} - 1)t$. Se $t > 1$, então $\sigma(m) \geq m + t + 1 = 2^{k+1}t + 1$, um absurdo. Logo, $t = 1$, e $\sigma(m) = 2^{k+1} = m + 1$, o que nos diz que m tem que ser primo. Veja ainda que $k + 1$ deve ser primo para que $2^{k+1} - 1$ seja primo. Portanto, $n = 2^{p-1}(2^p - 1)$. Além disso, é fácil mostrar que todo n dessa forma é perfeito. □

Exemplo 1.7. *Dado um natural $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ e sua fatoração em primos, definimos a sua* falsa derivada *como*

$$f(n) = \prod_{i=1}^{k} a_i p_i^{a_i - 1}.$$

Mostre que a igualdade $f(n) = f(n-1) + 1$ ocorre para infinitos n.

SOLUÇÃO. Primeiro, é fácil ver que f é multiplicativa. Além disso, se n é um inteiro livre de quadrados, isto é, não existe p primo tal que $p^2|n$, então $f(n) = 1$. Assim, se $\text{mdc}(m, n) = 1$ e n é livre de quadrados, então $f(mn) = f(m)$.
Portanto, basta encontrarmos inteiros a e b com $f(a) = f(b) + 1$ e mostrarmos que existem infinitos inteiros livres de quadrados m e n com $ma - nb = 1$. Um exemplo de tais a e b são os números 5^3 e 37^2.
Assim, suponha que a e b são inteiros positivos com $\text{mdc}(a, b) = 1$. Pelo Teorema de Bèzout, existem k e ℓ inteiros positivos para os quais $ak - b\ell = 1$. Claramente todos os pares $(bt + k, at + \ell)$ são soluções de $ax - by = 1$. Além disso, $\text{mdc}(a, b) = \text{mdc}(a, \ell) = \text{mdc}(b, k) = 1$. Logo, basta mostrarmos que existem infinitos t tais que $at + \ell$, $bt + k$ são livres de quadrados.
Suponha que os primos que dividem ab são $p_1 < p_2 < \ldots < p_s$ e seja $P = \prod_{u \leq p_s} u$. Considere os pares $(a_t, b_t) = (btP + k, atP + \ell)$. Tome α como um número real positivo. Dado um primo p, a quantidade de números a_t ou b_t que são divisíveis por p^2, com $t \leq \alpha$, é no máximo $2\left\lceil \frac{\alpha}{p^2} \right\rceil$, uma vez que $p \nmid a_t b_t$ para todo $p \leq p_s$, e se $p > p_s$, então $atP + \ell \equiv at'P + \ell \pmod{p^2} \iff t \equiv t' \pmod{p^2}$. Logo, sendo $N(\alpha)$ a quantidade de números do conjunto $\{a_t, b_t | t \leq \alpha\}$ que são divisíveis por um quadrado, sabemos que

$$N(\alpha) \leq \sum_{\sqrt{\alpha} \geq p > p_s} 2\left\lceil \frac{\alpha}{p^2} \right\rceil$$
$$\leq \sum_{\sqrt{\alpha} \geq p > p_s} \frac{2\alpha}{p^2} + 2\sqrt{\alpha}.$$

Como

$$\sum_{n > p_s} \frac{1}{n^2} \leq \sum_{n > p_s} \frac{1}{n(n-1)}$$
$$= \sum_{n > p_s} \frac{1}{n-1} - \frac{1}{n}$$
$$= \frac{1}{p_s},$$

Para $p_s > 4$ (e podemos supor isso, já que, tomando $a = 5^3$, $b = 37^2$, temos $p_s = 37$), temos então que $N(\alpha) \leq \sqrt{\alpha} + \frac{\alpha}{2} < \frac{2(\alpha-1)}{3}$ para α suficientemente grande. Como há $\lfloor \alpha \rfloor$ pares (a_t, b_t) com $t \leq \alpha$ e no conjunto $\{a_t, b_t | t \leq \alpha\}$ no máximo $\frac{2\lfloor \alpha \rfloor}{3}$ são divisíveis por algum quadrado, então pelo menos $\frac{\lfloor \alpha \rfloor}{3}$ dos pares (a_t, b_t), $t \leq \alpha$, são formados por números livres de quadrados, e isso garante a existência de infinitos pares (a_t, b_t) livres de quadrados. □

Adaptando a solução do exemplo anterior, podemos concluir a seguinte

Proposição 1.8. *Dados inteiros a, b com $mdc(a, b)$ livre de quadrados, o número $an + b$ é livre de quadrados para infinitos inteiros positivos n.*

As próximas subseções são destinadas à resolução de problemas envolvendo as funções aritméticas mais conhecidas: $d(n), \sigma(n), \varphi(n)$ e também $\nu_p(n)$. No início de cada seção, colocamos algumas propriedades de cada uma delas.

1.1 A função número de divisores $d(n)$

Propriedades da função $d(n)$:

1. $d(n) \stackrel{\text{def}}{=} \sum_{d|n} 1$;

2. d é multiplicativa, isto é, $\text{mdc}(a,b) = 1 \Rightarrow d(ab) = d(a)d(b)$;

3. Se $n = \prod_{i=1}^{r} p_i^{a_i}$, onde $p_1, p_2, \ldots, p_r$ são primos, então $d(n) = \prod_{i=1}^{r}(a_i+1)$. Portanto, os valores de $d(n)$ não dependem dos primos que dividem n, e sim dos expoentes em sua fatoração canônica.

Problemas que envolvem $d(n)$

Exemplo 1.9. *Encontre todos os naturais n tais que $n^{d(n)+1}(n+21)^{d(n)}$ é um quadrado perfeito.*

SOLUÇÃO. Note que, se $ab^2 = c^2$, com $a, b, c \in \mathbb{N}$, então a deve ser quadrado perfeito. Usaremos isso implicitamente durante a solução.
Se $d(n)$ for par, então $n^{d(n)}(n+21)^{d(n)}$ é quadrado perfeito, e portanto n é quadrado perfeito. Mas se n é quadrado perfeito, temos que $d(n)$ é ímpar, um absurdo.
Logo, $d(n)$ é ímpar e n é um quadrado perfeito. Então $(n+21)^{d(n)}$ é um quadrado perfeito, ou seja, $n+21$ é quadrado perfeito. Desse modo, concluímos que $n = t^2$ e $n+21 = s^2 \Rightarrow 21 = (s+t)(s-t)$. Como $s+t > s-t$, devemos ter $s+t = 21$ e $s-t = 1$ ou $s+t = 7$ e $s-t = 3$, o que nos dá $n = 100$ ou $n = 4$. □

Exemplo 1.10. *Encontre todos os inteiros positivos n tais que*

$$\prod_{i=1}^{n} d(ni) = (n!)^2.$$

SOLUÇÃO. Note que $n = 1$ nos dá uma solução. A partir de agora, vamos supor que $n \geq 2$.
Seja p o maior primo do intervalo $[1, n]$. Então $p|d(nk)$ para algum $k \leq n$. Ou seja, $q^{pm-1}|nk$ para algum primo q e inteiro m. Isso nos diz que $2^{p-1} \leq n^2$. Porém, pelo Postulado de Bertrand (ver teorema 3.13), $n/2 \leq p \leq n$, de modo que $2^{n/2-1} \leq n^2$. Isso não ocorre para $n \geq 20$. Ou seja, $2 \leq n \leq 19$, e deixamos para o leitor realizar a análise desses casos. □

Exemplo 1.11. *Encontre todos os naturais n que possuem exatamente divisores positivos, que chamamos de $1 = d_1 < d_2 < \cdots < d_{16} = n$, $d_6 = 18$ e $d_9 - d_8 = 17$.*

SOLUÇÃO. Note que $18 = 2 \cdot 3^2$ possui 6 divisores, isto é, temos que $d_1 = 1$, $d_2 = 2$, $d_3 = 3$, $d_4 = 6$, $d_5 = 9$ (disso, segue que $4 \nmid n$). Se $n = 3^a b$, com $3 \nmid b$, então a é uma potência de dois menos um, já que $a+1|d(n) = 16$. Como $a \geq 2$, então $a = 3$ ou $a = 7$ (se $a > 7$, $2 \cdot 3^a | n \Rightarrow d(n) \geq 2(a+1) > 16$). Se $a = 7$, $2 \cdot 3^7 | n \Rightarrow d(n) \geq 2 \cdot 8 = 16$, ou seja, $n = 2 \cdot 3^7$. Mas teríamos $d_9 - d_8 > 17$, um absurdo. Então $n = 2 \cdot 3^3 p$, onde p é um primo maior que 18. Se $p < 27$, teríamos $d_7 = p$, $d_8 = 27$ e $d_9 = d_8 + 17 = 44$, ou seja, $11|n$, absurdo ($p > 18$). Se $27 < p < 54$, então $d_7 = 27$, $d_8 = p$ e $d_9 = 54 = 17 + p$, ou seja, $p = 37$. Se $p > 54$, então $d_8 = 54$ e $d_9 = 54 + 17 = 71$, ou seja, $p = 71$. Então obtemos duas soluções: $n = 2 \cdot 3^3 \cdot 37$ e $n = 2 \cdot 3^3 \cdot 71$. □

Exemplo 1.12. *Mostre que a sequência $\{d(n^2+1)\}_{n \geq 0}$ não é eventualmente crescente.*

SOLUÇÃO. Para $n \geq 1$, $d(n^2+1)$ é par, já que n^2+1 não é quadrado perfeito. Assim, se $d((n+1)^2+1) > d(n^2+1)$ para $n > N$, teríamos $d((n+1)^2+1) \geq d(n^2+1) + 2 \Rightarrow d(n^2+1) \geq d((N+1)^2+1) + 2(n-N-1)$. Por outro lado, para n par, $d(n^2+1) \leq n$ (ver exercício 1.1), e as desigualdades $2(n-N-1) + d((N+1)^2+1) \leq d(n^2+1) \leq n$ se contradizem para n par grande. □

Exemplo 1.13. *Encontre todos os inteiros k para o qual a igualdade $d(n^2) = kd(n)$ ocorre para algum inteiro positivo n.*

SOLUÇÃO. Como $d(n^2)$ é ímpar, então $d(n)$ deve ser ímpar, ou seja, n é quadrado perfeito. Em outras palavras, queremos encontrar os possíveis valores inteiros de

$$\prod_{i=1}^{m} \frac{4x_i + 1}{2x_i + 1},$$

onde $x_i \in \mathbb{N}$ e m é um natural qualquer. Como essa fração deve ser ímpar caso seja inteira, todos os inteiros que buscamos devem ser ímpares. De fato, mostramos que todos os ímpares podem ser escritos dessa forma.

A prova será por indução em k. Os casos $k = 1$ (trivial, $n = 1$) e $k = 3(\frac{4\cdot1+1}{2\cdot1+1}\frac{4\cdot2+1}{2\cdot2+1} = 3)$ estão feitos. Suponha que todos os inteiros menores que k podem ser escritos dessa forma. Então, escreva $k = 2^t r - 1$, com $r < k$ ímpar. Note que, se tomarmos $x_i = 2^{i-2}(2^t r - r - 1)$, com $1 \le i \le t$, teremos então

$$\prod_{i=1}^{t} \frac{4 \cdot 2^{i-2}(2^t r - r - 1) + 1}{2 \cdot 2^{i-2}(2^t r - r - 1) + 1} = \prod_{i=1}^{t} \frac{2^i(2^t r - r - 1) + 1}{2^{i-1}(2^t r - r - 1) + 1} = \frac{2^t(2^t r - r - 1) + 1}{2^t r - r} = \frac{2^t r - 1}{r}.$$

Por hipótese de indução, r pode ser escrito na forma desejada, e portanto k também pode. □

Exemplo 1.14. *Dizemos que um natural n é* bom *se $d(n) > d(m)$ para todos $m < n$. Dois naturais bons m e n são chamados de* amigos *se não existe nenhum natural bom entre eles. Mostre que existem apenas finitos pares (m, n) de inteiros bons e amigos tais que $m|n$, mas que para todo primo p existem infinitos naturais r tais que r e pr são bons.*

SOLUÇÃO. Seja $p_1 < p_2 < \cdots$ a sequência de todos os números primos. É imediato que todo número bom é da forma $\prod_{i=1}^{k} p_i^{\alpha_i}$, onde $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_k > 0$. Além disso fixado $a \ge 2$, note que, se $p_k^{a-1} \nmid n$, onde $n = \prod_{i=1}^{\ell} p_i^{\alpha_i - 1}$ $(\alpha_i \ge 1)$ é um número bom, então $\alpha_k = a - c$, com $0 < c < a$. Como n é um número bom, sendo $b_i = \lceil \log_{p_k} p_i \rceil$, temos que $m = (p_k/p_i^{b_i})^c n < n$, de modo que

$$d(m) < d(n) \iff (\alpha_i - cb_i)a < \alpha_i(a - c) \iff \alpha_i < ab_i$$

(isso só vale se $m \in \mathbb{N}$. Entretanto, se $m \notin \mathbb{N}$, isso significa que $\alpha_i < cb_i < ab_i$, de modo que $\alpha_i < ab_i$ é sempre válido.)
Assim, α_i é limitado para todo i se $p^{a-1} \nmid n$. Portanto, se não existe n bom divisível por p_k^{a-1}, então algum inteiro bom n teria um divisor primo p suficientemente grande, de modo que $p_k^{2a} < p$, e é fácil de ver que $(p_k^{2a}/p)n < n$ e possui mais divisores, um absurdo. Portanto, conclui-se que, a partir de algum momento, dado $a > 1$ e um primo p, todo número bom n é divisível por p^{a-1} (caso isso não ocorresse, teríamos uma sequência de números bons com expoentes limitados, e já vimos que nos dá um absurdo).
Agora estamos prontos para terminar o problema. Seja (m, n) um par de números amigos suficientemente grandes, com $m \le n$. Então sabemos que $12|m$. Mas é fácil ver que ou $d(4m/3) > d(m)$ ou $d(3m/2) > d(m)$, de modo que $n \le 3m/2 < 2m$, e portanto $m \nmid n$ para todo par de números amigos suficientemente grandes.
Seja p um primo. Suponha que t é o menor número bom tal que $p^k|t$ para algum natural k. Vamos mostrar que t/p é bom, o que termina o problema. Caso t/p não seja bom, existe um número bom $u < t/p$ com $d(u) \ge d(t/p)$, mas $d(u \cdot p) < d(t)$, e com $p^k \nmid u$. Sendo $u = p^{k-c-1}x$ e $t = p^{k+d}y$, com $p \nmid xy$, temos que $(k - c)d(x) \ge (k + d)d(y)$, e $(k + d + 1)d(y) > (k - c + 1)d(x)$, ou seja,

$$\frac{k+d}{k-c} \le \frac{d(x)}{d(y)} < \frac{k+d+1}{k-c+1},$$

o que é um absurdo já que $k + d \ge k - c$. Logo, t/p deve ser um número bom, o que acaba o problema. □

1.2 A função soma dos divisores $\sigma(n)$

Propriedades da função $\sigma(n)$:

1. $\sigma(n) \stackrel{\text{def}}{=} \sum_{d|n} d$;

2. σ é multiplicativa, isto é, $\text{mdc}(a, b) = 1 \Rightarrow \sigma(ab) = \sigma(a)\sigma(b)$;

3. Se $n = \prod_{i=1}^{r} p_i^{a_i}$, onde $p_1, p_2, \ldots, p_r$ são primos, então $\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}$.

Problemas que envolvem $\sigma(n)$

Exemplo 1.15. *Para todo $n \ge 2$ vale que*

$$\frac{\sigma(n)}{d(n)} \ge \sqrt{n}.$$

SOLUÇÃO. Sejam $d_1, d_2, \ldots, d_t$ os divisores de n menores ou iguais a $\sqrt{n}$. Como os outros divisores (maiores ou iguais a $\sqrt{n}$) são $n/d_1, n/d_2, \ldots, n/d_t$, temos que $d_i + n/d_i \ge 2\sqrt{n}$, então $\sum_{d|n} d = \sum_{i=1}^{t} d_i + n/d_i \ge 2t\sqrt{n}$ se $\sqrt{n} \notin \mathbb{Z}$, e, caso contrário, suponha sem perdas $d_t = \sqrt{n}$, $\sum_{d|n} d = \sqrt{n} \sum_{i=1}^{t-1} d_i + n/d_i \ge (2t - 1)\sqrt{n}$. É imediato que $2t = d(n)$ no primeiro caso e que $2t - 1 = d(n)$ no segundo caso, de modo que o problema acabou. □

Exemplo 1.16. *Mostre que, se os naturais n, k, m satisfazem $mdc(k, m) = 1$ e $\sigma(n)^k = n^m$, então $n = 1$.*

SOLUÇÃO. A equação $\sigma(n)^k = n^m$ é equivalente à existência de um $t \in \mathbb{N}$ tal que $\sigma(n) = t^m$ e $n = t^k$ (como $\text{mdc}(m, k) = 1$, então $k|\nu_p(n)$ para todo p e $m|\nu_p(\sigma(n))$ para todo p). Suponha que $1 < t = \prod_{i=1}^{r} p_i^{\alpha_i}$. Temos que

$$\prod_{i=1}^{r} \frac{p_i^{k\alpha_i+1} - 1}{p_i - 1} = \sigma(n) = \prod_{i=1}^{r} p_i^{m\alpha_i}.$$

Como $\sigma(n) > n$ $(n > 1)$, sabemos também que $m > k$. Mas então é fácil ver que

$$\frac{p_i^{k\alpha_i+1} - 1}{p_i - 1} < p_i^{m\alpha_i},$$

um absurdo. Logo, $t = 1$ e $n = 1$. □

Exemplo 1.17. *Para qualquer inteiro $n \geq 2$ vale que*

$$\sigma(n) < n\sqrt{2d(n)}.$$

SOLUÇÃO. Vamos mostrar que

$$\begin{aligned} &\sigma(p^\alpha) \leq p^\alpha \sqrt{d(p^\alpha)} \qquad (\chi) \\ \iff &\left(\frac{p^{\alpha+1} - 1}{p - 1}\right) \leq p^\alpha \sqrt{\alpha + 1} \end{aligned}$$

Para quase todo par (p, α), onde p é primo e α é um natural. De fato, essa última desigualdade é equivalente a

$$\begin{aligned} &p^\alpha \sqrt{\alpha+1} - 1 \leq p^{\alpha+1}(\sqrt{\alpha+1} - 1) \\ \iff &\sqrt{\alpha+1} \leq p(\sqrt{\alpha+1} - 1) + \frac{1}{p^\alpha}. \qquad (1) \end{aligned}$$

É suficiente ver quando

$$\begin{aligned} &\sqrt{\alpha+1} \leq 2(\sqrt{\alpha+1} - 1) \\ \iff &\alpha \geq 3. \end{aligned}$$

Ou seja, ainda falta analisar os casos $\alpha = 1, 2$. Se $\alpha = 1$, (1) transforma-se em

$$\sqrt{2} \leq p(\sqrt{2} - 1) + \frac{1}{p},$$

o que só não ocorre para $p = 2$. Se $\alpha = 2$, então (1) transforma-se em

$$\sqrt{3} \leq p(\sqrt{3} - 1) + \frac{1}{p^2},$$

o que também não ocorre apenas para $p = 2$. Ou seja, apenas os pares $(2, 1)$ e $(2, 2)$ não satisfazem (χ). É trivial verificar que 2 e 4 satisfazem a desigualdade do enunciado.
Desse modo, sendo $m = \prod p^\alpha$ um inteiro ímpar, temos que

$$\begin{aligned} &\sigma(m) < m\sqrt{d(m)} \\ \iff &\prod \sigma(p^\alpha) < \prod p^\alpha \sqrt{d(p^\alpha)}, \end{aligned}$$

o que é verdade por (χ). Como $\sigma(2^a) < 2^a\sqrt{2d(2^a)}$, o resultado segue. □

Exemplo 1.18. *Mostre que o n-ésimo número relativamente coprimo com n é maior ou igual a $\sigma(n)$, e encontre todos os casos de igualdade.*

Apresentamos duas soluções para esse problema. A primeira solução mostra que "força bruta" pode ser bastante útil caso você não tenha uma ideia mais esperta, como ocorre na segunda solução.

SOLUÇÃO 1. Fica a cargo do leitor mostrar que todas as potências de primo são casos de igualdade. A partir de agora, vamos supor que n não é potência de primo.
Dado um inteiro m, estamos interessados em saber quantos inteiros no conjunto $I_m = \{1, 2, \ldots, m\}$ são coprimos com n. Utilizando o Princípio da Inclusão-Exclusão, segue que tal número é

$$f_n(m) = \sum_{C \subseteq I_k} (-1)^{|C|} \left\lfloor \frac{m}{\prod_{i \in C} p_i} \right\rfloor,$$

Onde $p_1, p_2, \ldots, p_k$ são todos os divisores primos de n. Como $\lfloor a/b \rfloor = a/b - \{a/b\}$, temos que

$$\begin{aligned} f_n(m) &= m \prod_{i=1}^{k} (1 - 1/p_i) + \sum_{C \subseteq I_k} (-1)^{|C|} \left\{ \frac{m}{\prod_{i \in C} p_i} \right\} \\ &< m\varphi(n)/n + 2^{k-1}, \end{aligned}$$

onde a desigualdade ocorre pois $m \prod_{i=1}^{k} (1 - 1/p_i) = m\varphi(n)/n$ e, se $|C|$ for par, $(-1)^{|C|} \left\{ \frac{m}{\prod_{i \in C} p_i} \right\} < 1$ e, se $|C|$ for ímpar, $(-1)^{|C|} \left\{ \frac{m}{\prod_{i \in C} p_i} \right\} < 0$, e existem 2^{k-1} subconjuntos de tamanho par de I_k.
Como queremos $f_n(\sigma(n)) \leq n$, é suficiente que $\sigma(n)\varphi(n)/n + 2^{k-1} \leq n \iff \sigma(n)\varphi(n)/n \leq n - 2^{g(n)-1}$, onde $g(n)$ é a quantidade de divisores primos de n.
Sejam a e b naturais coprimos que satisfaçam $\sigma(x)\varphi(x)/x \leq x - 2^{g(x)-1}$. Então,

$$\sigma(ab)\varphi(ab)/ab \leq (a - 2^{g(a)-1})(b - 2^{g(b)-1}).$$

Como

$$\begin{aligned} & ab - a2^{g(b)-1} - b2^{g(a)-1} + 2^{g(a)+g(b)-2} < ab - 2^{g(ab)-1} = ab - 2^{g(a)+g(b)-1} \\ \iff & a2^{g(b)-1} + b2^{g(a)-1} > 2^{g(a)+g(b)-1} + 2^{g(a)+g(b)-2}, \end{aligned}$$

e $m \geq 2^{g(m)}$ para todo m, então

$$a2^{g(b)-1} + b2^{g(a)-1} \geq 2^{g(a)+g(b)} > 2^{g(a)+g(b)-1} + 2^{g(a)+g(b)-2}.$$

Assim, basta analisar os casos $g(n) = 2$ e $g(n) = 3$ (estamos supondo $g(n) > 1$).
Para $g(n) = 2$, temos $n = p^a q^b$, $a, b \geq 1$, e

$$\begin{aligned} & \sigma(n)\varphi(n)/n = \frac{p^{a+1} - 1}{p} \frac{q^{b+1} - 1}{q} \\ \implies & \frac{p^{a+1} - 1}{p} \frac{q^{b+1} - 1}{q} \leq n - 2 \\ \iff & 2pq \leq p^{a+1} q^{b+1} - 1, \end{aligned}$$

o que é verdade, pois $a + 1, b + 1 \geq 2$ e $p \neq q$. Se $g(n) = 3$, escreva $n = p^a q^b r^c$, e a desigualdade tranforma-se em

$$\begin{aligned} & \frac{p^{a+1} - 1}{p} \frac{q^{b+1} - 1}{q} \frac{r^{c+1} - 1}{r} < p^a q^b r^c - 4 \\ \iff & \frac{p^{a+1}q^{b+1} + q^{b+1}r^{c+1} + r^{c+1}p^{a+1} - p^{a+1} - q^{b+1} - r^{c+1} + 1}{pqr} \geq 4. \end{aligned}$$

Sendo $x = p^{a+1}$, $y = q^{b+1}$, $z = r^{c+1}$, temos $x, y, z > 2$, e portanto

$$xy + yz + zx - x - y - z > \frac{xy + yz + zx}{2},$$

e então basta

$$\begin{aligned} & \frac{p^a q^b}{2r} + \frac{q^b r^c}{2p} + \frac{r^c p^a}{2q} \geq 4 \\ \impliedby & \frac{pq}{2r} + \frac{qr}{2p} + \frac{rp}{2q} \geq 4. \end{aligned}$$

Se $r > q > p$, então $r \geq 5$ e $r/2(\frac{p}{q} + \frac{q}{p}) > r$, o que finaliza o problema, já que todo inteiro n com $g(n) \geq 4$ é produto de dois inteiros a, b com $g(a), g(b) \geq 2$. □

SOLUÇÃO 2. Sejam $d_1, d_2, \ldots, d_k$ os divisores de n. Particione o intervalo $[1, \sigma(n)]$ nos intervalos $[1, d_1]$, $[d_1+1, d_1+d_2], \ldots, [d_1+d_2+\ldots+d_{k-2}+1, d_1+d_2+\ldots+d_{k-2}+d_{k-1}]$ e $[d_1+d_2+\ldots+d_{k-2}+d_{k-1}+1, d_1+d_2+\ldots+d_{k-1}+d_k] = [d_1+d_2+\ldots+d_{k-2}+d_{k-1}+1, \sigma(n)]$. Como entre d inteiros consecutivos existem exatamente $\varphi(d)$ números coprimos com d (tente provar isso, não é táo difícil!), então existem no máximo $\sum_{d|n}\varphi(d) = n$ (ver lema 1.3) números menores ou iguais a $\sigma(n)$, já que, se um número é coprimo com n, então é coprimo com qualquer divisor de n (ou seja, em cada um dos intervalos que formamos, existem no máximo $\varphi(d_i)$ inteiros coprimos com n), apesar da volta não ser válida.
Para encontrar os casos de desigualdade estrita, basta ver que se $pq|n$, com $p > q$ primos, podemos escolher $d_1 = p$, de modo que $q \in [1, d_1]$, mas q não é coprimo com n, de modo que a igualdade não ocorre. Assim como na solução anterior, fica a cargo do leitor mostrar que para toda potência de primo a igualdade ocorre. □

Exemplo 1.19. *Encontre todos os naturais n tais que $n^n + 1$ é um número perfeito.*

SOLUÇÃO. Começamos com o caso n par. Note que todo divisor primo de $N = n^n + 1$ é da forma $4k+1$, de modo que

$$\sigma(N) = \sum_{d|N} d \equiv \sum_{d|N} 1 \equiv d(N) \pmod 4.$$

Além disso, N é ímpar e, por hipótese, $\sigma(N) = 2N \equiv 2 \pmod 4$. Assim, $d(N) \equiv 2 \pmod 4$, e disso segue que $N = p^{4\alpha+1}m^2$ $(p \nmid m)$.
Por outro lado, como $3 \nmid N$ (isso ocorre pois $3 \nmid x^2+1$), então

$$3 \nmid 2N = \sigma(N) = \sigma(m^2)(p^{4\alpha+2}-1)/(p-1)$$

e, como $p \neq 3$, temos que $p \equiv 1 \pmod 3$, já que $p^{4\alpha+2} - 1 \equiv 0 \pmod 3$ e portanto 3 deve dividir $p-1$. Isso nos diz que ($m^2 \equiv 1 \pmod 3$) $N \equiv 1 \pmod 3$, de forma que $n^n \equiv 0 \pmod 3$, e portanto $3|n$.
Agora, podemos escrever $n = 3t$, e teremos $(3t)^{3t} + 1 = (n^t+1)((n^t)^2 - (n^t) + 1)$. Se $q|n^t+1$, então $n^{2t} - n^t + 1 \equiv 3 \pmod q$. Como $3 \nmid n^t + 1$, segue que $\text{mdc}(n^t+1, n^{2t}-n^t+1) = 1$. Mas $p^{4\alpha+1}m^2 = (n^t+1)(n^{2t}-n^t+1)$, de modo que algum dos números n^t+1, $n^{2t}-n^t+1$ é quadrado perfeito. Como t é par ($t = 2s$), segue que $n^{2t} - n^t + 1$ é quadrado, ou seja $(n^{2s}-1)^2 + (n^s)^2 = T^2$. Logo, devemos ter $n^s = 2ab$, enquanto $n^{2s} - 1 = a^2 - b^2$, já que esse números são coprimos e são catetos de um triângulo retângulo de lados inteiros. Mas isso nos diria que $4a^2b^2 + b^2 - a^2 - 1 = 0$, o que é um absurdo, já que $4a^2b^2 > a^2$ e $b^2 \geq 1$.
Assim, resta o caso n ímpar. Sabemos que $n^n + 1 = 2^{p-1}(2^p - 1)$ (ver exemplo 1.6), onde p e $2^p - 1$ são primos. Mas

$$n^n + 1 = (n+1)(n^{n-1} - n^{n-2} + \cdots - n + 1) = 2^{p-1}(2^p - 1),$$

e $\frac{n^n+1}{n+1} > 1$ é ímpar, de modo que $n + 1 = 2^{p-1}$. Portanto,

$$(2^{p-1}-1)^{2^{p-1}-1} + 1 = 2^{p-1}(2^p-1) = 2^{2p-1} - 2^{p-1}.$$

Como $p = 2$ não funciona, temos $p \geq 3$, e então

$$2^{2^{p-2}(p-2)} < 2^{p-1}(2^p-1) = 2^{2p-1} - 2^{p-1} < 2^{2p-1}.$$

Assim, $2^{p-2}(p-2) < 2p-1 \Rightarrow 2^{p-2} < \frac{2p-1}{p-2} < 8$. Logo $p - 2 \leq 2 \Rightarrow p \leq 4$. Concluímos que $p = 3$, que nos dá a única solução $n = 3$. □

1.3 A função $\varphi(n)$

Propriedades da função $\varphi(n)$:

1. $\varphi(n) \stackrel{\text{def}}{=} \sum_{\substack{\text{mdc}(n,k)=1 \\ k \leq n}} 1$;

2. φ é multiplicativa, isto é, $\text{mdc}(a,b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$;

3. Se $n = \prod_{i=1}^{r} p_i^{a_i}$, onde $p_1, p_2, \ldots, p_r$ são primos, então $\varphi(n) = \prod_{i=1}^{r} p_i^{a_i-1}(p_i-1) = n\prod_{i=1}^{r}(1-1/p_i)$.

4. Se p é primo e $p|n$, então $\varphi(pn) = p\varphi(n)$. Além disso, se $p \nmid n$, então $\varphi(pn) = \varphi(p)\varphi(n) = (p-1)\varphi(n)$.

Problemas que envolvem $\varphi(n)$

Exemplo 1.20. *Mostre que*

$$\sum_{\substack{k\le n\\ mdc(k,n)=1}} k = \frac{n\varphi(n)}{2}.$$

SOLUÇÃO. Basta ver que $\text{mdc}(k,n)=1 \iff \text{mdc}(n-k,n)=1$. Assim,

$$2\sum_{\substack{k\le n\\ \text{mdc}(k,n)=1}} k = \sum_{\substack{k\le n\\ \text{mdc}(k,n)=1}} k + \sum_{\substack{k\le n\\ \text{mdc}(k,n)=1}} n-k = \sum_{\substack{k\le n\\ \text{mdc}(k,n)=1}} n = n\varphi(n),$$

donde o resultado segue. □

Exemplo 1.21. *Mostre que, se n é composto, $\varphi(n) \le n - \sqrt{n}$.*

SOLUÇÃO. Como n é composto, existe um primo $p \le \sqrt{n}$ que divide n. Como

$$\varphi(n) = n\prod_{q|n}\Big(1-1/q\Big) \le n\Big(1-1/p\Big) \le n-\sqrt{n}.$$

□

Exemplo 1.22. *Seja $n>6$ um inteiro e $a_1, a_2, \ldots, a_k$ todos os naturais menores que n que são relativamente coprimos com n. Mostre que se*

$$a_2 - a_1 = a_3 - a_2 = \cdots = a_k - a_{k-1} > 0,$$

então n é uma potência de 2 ou n é primo.

SOLUÇÃO 1. Suponha que $2 \nmid n$. Então $a_1 = 1$ e $a_2 = 2$ então, $a_{i+1} - a_i = a_2 - a_1 = 1$, e concluímos que n é primo. Assim, suponha que $2|n$, e seja $p \ge 3$ o menor primo que não divide n. Então $a_1 = 1$, $a_2 = p$, e segue que $a_i = (i-1)(p-1)+1$. Se $p = 3$, teríamos $a_i = 2i-1$, e então todos os ímpares menores que n seriam coprimos com n, de modo que n seria uma potência de 2. Se $p > 3$, então note que $3|n$ e que

$$\begin{aligned} &n-1 = a_k = (k-1)(p-1)+1\\ \implies &n-2 = (k-1)(p-1). \end{aligned}$$

Como $3 \nmid n-2$, então $p \equiv 2 \pmod 3$. Mas teríamos $a_3 = 2(p-1)+1 \equiv 0 \pmod 3$, um absurdo se $2(p-1)+1 < n$. Se $2(p-1)+1 \ge n$, $k = \varphi(n) \le 2$ e $6|n$, ou seja $2 = \varphi(6) \le \varphi(n) \le 2$, de modo que $n = 6$, mas estávamos supondo $n > 6$. □

SOLUÇÃO 2. Apresentamos outra solução para o caso $p > 3$. Pelo Postulado de Bertrand (ver 3.13), existe um primo q tal que $2 < q < p < 2q$ e $q|n$ por hipótese. Em particular, $q \nmid p-1$. Mas como $\text{mdc}(n, i(p-1)+1) = 1$ para $0 \le i \le k-1 = \varphi(n)-1$. Se $q > 3$, então $\varphi(n) \ge (q-1)2 > q$ e então algum dos números $i(p-1)+1$, $0 \le k \le \varphi(n)-1$, deve ser divisível por q, absurdo, pois $q|n$. Assim, $q = 3$, $3 < p < 2\cdot 3 \Rightarrow p = 5$ e $\varphi(n) < 3$, já que, caso contrário, algum dos números $k(p-1)+1 = 4i+1$, $0 \le i \le \varphi(n)-1$ seria divisível por 3. Disso segue que $n = 6$. □

Exemplo 1.23. *Encontre todas as funções $f\colon \mathbb{N} \to \mathbb{N}$ tais que, para todos $m \ge n > 0$,*

$$f(m\varphi(n^3)) = f(m)\cdot\varphi(n^3).$$

SOLUÇÃO. Na verdade, a ideia aqui é nos livrarmos do $\varphi(n^3)$! Para isso, Veja que $\varphi(p^6) = p^3\varphi(p^3)$, p primo (isso vale se p não é primo?). Assim, para $m \ge p^2$,

$$f(mp^3)\varphi(p^3) = f(mp^3\varphi(p^3)) = f(m\varphi(p^6)) = f(m)p^3\varphi(p^3),$$

De modo que $f(mp^3) = f(m)p^3$ para $m \ge p^2$. Em particular, $f(8m) = 8f(m)$ para todo $m \ge 4$. Por outro lado, para $m \ge 2$, $f(m\varphi(8)) = f(m)\varphi(8) \Rightarrow f(4m) = 4f(m)$, $m \ge 2$. Assim, para $m \ge 4$,

$$\begin{aligned} &8f(m) = f(8m) = 4f(2m)\\ \implies &f(2m) = 2f(m). \end{aligned}$$

Mas $4f(m) = f(4m) = 2f(2m)$ para $m \geq 2$ pois $2m \geq 4$, de modo que $f(2m) = 2f(m)$ para todo $m \geq 2$.
Podemos tentar realizar um processo análogo para o 3. Sabemos que $f(27m) = 27f(m)$ para $m \geq 9$ e que $f(m\varphi(27)) = f(m)\varphi(27) \Rightarrow f(2 \cdot 9m) = 2 \cdot 9f(m)$ para $m \geq 3$. Como $f(2 \cdot 9m) = 2f(9m)$, então $f(9m) = 9f(m)$ para $m \geq 3$. Logo, para $m \geq 9$,

$$\begin{aligned} & 27f(m) = f(27m) = 9f(3m) \\ \implies & f(3m) = 3f(m). \end{aligned}$$

Mas $9f(m) = f(9m) = 3f(3m)$ para $m \geq 3$. Assim, temos na verdade que $f(3m) = 3f(m)$ para todo $m \geq 3$. Ainda mais, $6f(2) = 3f(4) = f(3 \cdot 4) = 2f(6)$, de modo que $f(6) = 3f(2)$. Estabelecemos a seguinte conjectura:

$$f(pm) = pf(m) \quad \text{para todo } m \geq 2 \text{ e } p \text{ primo.}$$

Suponha que isso valha para todos os primos menores que um primo p (já fizemos para $p = 2, 3$). Então, para $m \geq p$

$$\begin{aligned} & f(m\varphi(p^3)) = f(m)\varphi(p^3) \\ \implies & f(mp^2(p-1)) = f(m)p^2(p-1) \\ \implies & (p-1)f(mp^2) = (p-1)p^2 f(m) \\ \implies & f(mp^2) = p^2 f(m), \end{aligned}$$

já que $p-1$ possui apenas fatores primos menores que p. Além disso, $f(mp^3) = p^3 f(m)$ para $m \geq p^2$. Logo, $p^3 f(m) = f(p^3 m) = p^2 f(pm)$ para $m \geq p^2$, ou seja, $f(mp) = pf(m)$ para $m \geq p^2$. Mas, para $m \geq p$,

$$\begin{aligned} & pf(mp) = f(mp^2) = p^2 f(m) \\ \implies & f(mp) = pf(m). \end{aligned}$$

Agora, tome um primo $q < p$ e um inteiro t tal que $q^t > p$. Então, $pq^t f(m) = pf(mq^t) = f(mq^t p) = q^t f(mp)$ para $m \geq 2$, pois, por hipótese, $f(qn) = qf(n)$ para $n \geq 2$. Logo, $f(mp) = pf(m)$ para $m \geq 2$ e todo primo p.
Com isso, note que $pf(q) = f(pq) = qf(p)$ para todos p, q primos. Logo, $f(p)/p = C$ para todo p primo e uma constante inteira C. Daí, se $2 \leq n = p_1 p_2 \dots p_k$, onde $p_i's$ não são necessariamente distintos (e são primos), temos que $f(n)/n = f(p_1 p_2 \dots p_k)/p_1 p_2 \dots p_k = p_1 p_2 \dots p_{k-1} f(p_k)/p_1 p_2 \dots p_k = f(p_k)/p_k = C$, ou seja, $f(n) = nC$ para algum C natural, e $n \geq 2$. Note que $f(1)$ pode ser qualquer número. □

1.4 A função $\nu_p(n)$

Propriedades da função $\nu_p(n)$:
1. $\nu_p(n) \stackrel{\text{def}}{=} \max(a \geq 0; p^a | n)$;
2. Para todos a, b naturais vale que $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;
3. Para todos a, b naturais vale que $\min(\nu_p(a), \nu_p(b)) \leq \nu_p(a+b) \leq \max(\nu_p(a), \nu_p(b))$ e $\nu_p(a+b) = \min(\nu_p(a), \nu_p(b))$ se $\nu_p(a) \neq \nu_p(b)$ (a volta não vale);
4. $a|b \iff \nu_p(a) \leq \nu_p(b)$ para todo p primo.
Problemas que envolvem $\nu_p(n)$

Exemplo 1.24. *Mostre que 2^n não divide $n!$ para todo n natural.*

SOLUÇÃO. Sabemos que

$$\nu_2(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{2^k} \right\rfloor.$$

Assim,

$$\nu_2(n!) < \sum_{k \geq 1} \frac{n}{2^k} = n,$$

como queríamos. □

Exemplo 1.25. *Mostre que existe uma constante positiva c tal que, para todos a, b, n satisfazendo $a!b!|n!$, então $a + b < n + c \log n$.*

SOLUÇÃO. Aqui, usamos outra fórmula para $\nu_p(n!)$:

$$\nu_p(n!) = \frac{n - S_p(n)}{p-1},$$

onde $S_p(n)$ é soma dos dígitos de n na base p. Assim, se $a!b!|n!$, temos que $\nu_p(a!) + \nu_p(b!) \leq \nu_p(n!)$, e portanto

$$a + b - S_p(a) - S_p(b) \leq n - S_p(n) < n \Longrightarrow a + b < n + S_p(a) + S_p(b).$$

Para terminar, basta ver que $S_p(m) \leq (p-1)\lceil \log_p m \rceil$, de modo que

$$\begin{aligned} a + b &< n + (p-1)(\lceil \log_p a \rceil + \lceil \log_p b \rceil) \\ &< n + (p-1)(\log_p ab + 2) \\ &< n + 2(p-1) + 2(p-1)\log_p n, \end{aligned}$$

onde a última passagem vem do fato de que $a, b \leq n$, e com isso o problema acaba. □

Exemplo 1.26. *Encontre todas as funções $f\colon \mathbb{N} \to \mathbb{N}$ totalmente multiplicativas e que, para todos $a, b \in \mathbb{N}$, vale que pelo menos dois dos números $f(a), f(b), f(a+b)$ são iguais.*

SOLUÇÃO. Sabemos que, como a função é totalmente multiplicativa, todos os seus valores dependem apenas das imagens dos número primos.
Se $f(n) = 1$ para todo n, obtemos uma solução. Caso $f(n) > 1$ para algum n, seja p o menor primo tal que $c = f(p) > 1$. Vamos mostrar que $f(n) > 1 \Longleftrightarrow p|n$.
Se $p \nmid n$ e $f(n) > 1$, então existe um primo $q > p$ tal que $f(q) > 1$, e tome q como o menor tal primo. Como entre $f(p), f(q-p), f(q)$ existem dois números iguais, mas $f(q-p) = 1$, pois $q - p$ possui divisores primos menores que q e diferentes de p, então $f(p) = f(q)$. Seja $a \geq 2$ o inteiro tal que $p^a > q > p^{a-1}$. $p^a = qx + y$, então $x < p$ ($f(x) = 1$) e portanto $y < q$ e $p \nmid y$. Assim, $f(y) = 1$. Mas então teríamos que entre $f(qx), f(y), f(p^a)$ existem dois números iguais, mas $f(p^a) = f(p)^a = f(q)^a > f(q) = f(qx) > f(y) = 1$, um absurdo. Logo, tal primo q não existe.
Assim, fica claro que $f(n) = c^{\nu_p(n)}$ para todo n, e todas as funções assumem essa forma (a função $f(n) = 1$ é expressa dessa forma quando $c = 1$). □

Exemplo 1.27. *Mostre que*

$$10^{-n} = \sum_{i=1}^{k} \frac{1}{n_i!}$$

não possui soluções inteiras com $1 \leq n_1 < n_2 < \cdots < n_k$.

SOLUÇÃO. Suponha que $(n, n_1, n_2, \ldots, n_k)$ seja uma solução. Note que, multiplicando a equação por $10^n n_k!$,

$$n_k! = 10^n \left(1 + \sum_{i=1}^{k-1} \prod_{j=1}^{n_k - n_i} (n_i + j)\right) = 10^n T.$$

Como $T \equiv 1 \pmod{n_k}$, então $n_k | 10^n$, e portanto $n_k = 2^a 5^b$. Se $10|n_k$, então $T \equiv 1 \pmod 1 0$, e portanto $\nu_2(n_k!) = \nu_5(n_k!) = n$, e isso nos diz que $\lfloor n_k/2^j \rfloor = \lfloor n_k/5^j \rfloor$ para todo j, mas isso diz que $n_k \leq 3$, e deixamos para o leitor testar os possíveis casos.
Suponha que $5 \nmid n_k$. Mas então $2 \nmid T$ e concluímos que $n = \nu_2(n_k!) \leq \nu_5(n_k!)$, e isso nos diz novamente que $n_k \leq 3$.
Por último, suponha que $2 \nmid n_k$. Se $n_k - n_{k-1} \geq 2$, ainda temos $2 \nmid T$ e $5 \nmid T$, e portanto $n = \nu_2(n_k!) = \nu_5(n_k!)$. Logo, devemos ter $5^b = n_k = n_{k-1} + 1$. Esses fatos nos dizem que $2|T$, mas $4 \nmid T$ (verifique!), e também $5 \nmid T$, ou seja, $\nu_2(n_k!) = n+1 = \nu_5(n_k!)+1$. Logo, $\lfloor n_k/2^j \rfloor \leq \lfloor n_k/5^j \rfloor + 1$, e disso segue que $n_k \leq 6$ e portanto $n_k = 5$ e $n_{k-1} = 4$. Deixamos para o leitor testar os casos. □

Finalizamos esta seção com um problema que envolve as três funções $\varphi(n), \sigma(n)$ e $d(n)$:

Exemplo 1.28. *Dado um inteiro m no quadro, podemos apagá-lo e trocá-lo por $\varphi(m)$, $d(m)$ ou por $\sigma(m)$. Se o número $a > 1$ está escrito no quadro inicialmente, mostre que, com um número finito de operações, é possível obter qualquer inteiro $b > 1$.*

SOLUÇÃO. Note que, como $d(2^k) = k+1$, se provarmos que toda potência de 2 pode ser alcançada, então acabamos. Ainda mais, como $\varphi(2^k) = 2^{k-1}$, basta encontrarmos potências de 2 suficientemente grandes.
Agora, fazemos uma observação crucial: sendo $n = 2^a b$, com $b > 1$ ímpar, então $\nu_2(\varphi(n)) \geq \nu_2(n)$, e isso segue diretamente do fato de $\varphi(p^k) = p^{k-1}(p-1)$, que é par se p é primo ímpar. Entretanto, $1 < \varphi(n) < n$ para $n \geq 3$. Assim, como o ν_2 é não descrescente enquanto $b > 1$, mas sabemos que $\varphi^k(n) = 1$ para algum valor k, então em algum momento o ν_2 diminuiu, ou seja, existe um t tal que $\varphi^t(n) = 2^a$. Isso nos diz que precisamos garantir apenas que alcançamos números com ν_2 suficientemente grande.
Apliquemos a operação σ diversas vezes. Caso o ν_2 seja limitado, os números escritos no quadro ou possuem muitos fatores primos distintos ou possuem primos com ν_p arbitrariamente grandes. Caso $n = 2^\alpha \prod_{i=1}^{M} p_i \alpha_i$, com M arbitrariamente grande, aplicando a função φ, obtemos um número com ν_2 arbitrariamente grande, já que $\prod_{i=1}^{M} p_i - 1 | \varphi(n)$. Caso os expoentes se tornem arbitrariamente grandes, escolha n e i com $\alpha_i > 2^k$, para algum k fixado. Como $\nu_{p_i}(\varphi(n)) \geq \nu_{p_i}(n) - 1$ (essa análise é semelhante àquela feita para o ν_2) e, como o ν_p deve eventualmente diminuir, encontramos t tal que $\nu_{p_i}(\varphi^t(n)) = 2^k - 1$. Assim, podemos aplicar a função d e obter um número divisível por 2^k, como queríamos. □

Problemas Propostos

1.1. *Mostre que $d(n) < 2\sqrt{n}$ para todo n. Se $n > 3$ for ímpar, mostre que $d(n) < \sqrt{n}$.*

1.2. *Se n é um natural composto, mostre que $n + \sqrt{n} + 1 \leq \sigma(n)$.*

1.3. *Mostre que o conjunto $\left\{ \frac{\varphi(n)}{n} \mid n \in \mathbb{N} \right\}$ é denso em $[0,1]$. Você consegue mostrar que $\left\{ \frac{\varphi(n+1)}{\varphi(n)} \mid n \in \mathbb{N} \right\}$ é denso em $\mathbb{R}^+$?*

1.4. *Dado um inteiro $n \geq 2$, definimos a* lonjura *de n como o menor inteiro k para o qual $d^k(n) = 2$, onde d^k representa a $k-$ésima iterada de d.*

(a) Quantos inteiros entre 3 e 1000 possuem lonjura 2?

(b) Qual a maior lonjura que encontramos dentre os números de 3 a 1000?

1.5. *Encontre todos inteiros n para os quais $n = d(n)^2$.*

1.6. *Encontre todas as funções $f\colon \mathbb{N} \to \mathbb{N}$ tais que f é totalmente multiplicativa e $m+n | f(m)+f(n)$ para todos m, n naturais.*

1.7. *Mostre que a equação $\sigma(x) = m$ não possui solução para infinitos inteiros m.*

1.8. *Seja $d_3(n)$ a quantidade de divisores de n que deixam resto 1 na divisão por 3. Encontre todos os possíveis valores inteiros de $\frac{d(10n)}{d_3(10n)}$.*

1.9. *Mostre que, para toda função multiplicativa e crescente, existe $k \in \mathbb{R}$ tal que $f(n) = n^k$ para todo $n \in \mathbb{N}$.*

1.10. *Mostre que existe um inteiro positivo m para o qual a equação $\varphi(x) = m$ possui mais de 2023 soluções.*

1.11. *Seja $f(n)$ o maior divisor próprio de n, isto é, se $d|n$, então $d = n$ ou $d \leq f(n)$. Determine se existe um inteiro k tal que a equação $n - f(n) = k$ possui exatamente $10^{10^{10}}$ soluções.*

1.12. *Mostre que, para todo natural n,*

$$d((n+1)!) < 2d(n!).$$

1.13. *Determine todas as funções $f\colon \mathbb{N} \to \mathbb{N} \cup \{0\}$ tais que $f(n) \neq 0$ para algum n, $f(mn) = f(m) + f(n)$ para todos $m, n \in \mathbb{N}$ e existem infinitos n tais que $f(k) = f(n-k)$ para todo $k < n$.*

1.14. *Encontre todos os naturais n tais que $n^3 + 1$ é um número perfeito.*

2 A Função μ de Möbius

A função $\mu\colon \mathbb{N} \to \mathbb{Z}$ é definida por

$$\mu(n) = \begin{cases} 0 & \text{se } p^2|n \text{ para algum } p \text{ primo} \\ (-1)^k & \text{se } n > 1 \text{ e } n \text{ é o produto de } k \text{ primos distintos} \\ 1 & \text{se } n = 1. \end{cases}$$

É fácil ver que a função μ é multiplicativa. Além disso, temos o seguinte

Lema 2.1. *Temos que*

$$\sum_{d|n} \mu(d) = \begin{cases} 0 & \text{se } n > 1 \\ 1 & \text{se } n = 1. \end{cases}$$

Como consequência disso,

$$\sum_{d^2|n} \mu(d) = |\mu(n)| = \begin{cases} 0 & \text{se } p^2|n \text{ para algum } p \text{ primo} \\ 1 & \text{se } n \text{ é livre de quadrados.} \end{cases}$$

DEMONSTRAÇÃO. Como μ é multiplicativa, segue do teorema 1.2 que $\sum_{d|n} \mu(d)$ é multiplicativa, de modo que é necessário provar o lema apenas para n potência de primo. Como $\mu(1) = 1$, $\mu(p) = -1$ e $\mu(p^j) = 0$, $j \geq 2$, segue que:

$$\sum_{d|p^a} \mu(d) = \sum_{0 \leq j \leq a} \mu(p^j) = \mu(1) + \mu(p) = 0.$$

O segundo resultado é consequência imediata do primeiro. □

Teorema 2.2 (Primeira Fórmula de Inversão de Möbius)**.** *Dadas duas funções $f, F\colon \mathbb{N} \to \mathbb{C}$, vale que $F(n) = \sum_{d|n} f(d)$ para todo inteiro positivo n se, e somente se, $f(n) = \sum_{d|n} \mu(d)F(n/d)$ para todo n inteiro positivo.*

DEMONSTRAÇÃO. Primeiro, vejamos que $F(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{d|n} \mu(d)F(n/d)$:

$$\begin{aligned} \sum_{d|n} \mu(d)F(n/d) &= \sum_{d|n} \mu(d) \left(\sum_{dd'|n} f(d') \right) \\ &= \sum_{d'|n} f(d') \left(\sum_{dd'|n} \mu(d) \right) \\ &= f(n). \end{aligned}$$

Agora, mostramos que $f(n) = \sum_{d|n} \mu(d)F(n/d) \Rightarrow F(n) = \sum_{d|n} f(d)$:

$$\begin{aligned} \sum_{d|n} f(d) = \sum_{d|n} f(n/d) &= \sum_{d|n} \sum_{dd'|n} \mu\Big(\frac{n}{dd'}\Big) F(d') \\ &= \sum_{d'|n} F(d') \left(\sum_{dd'|n} \mu\Big(\frac{n}{dd'}\Big) \right) \qquad \text{(I)} \\ &= F(n). \end{aligned}$$

□

Teorema 2.3 (Segunda Fórmula de Inversão de Möbius)**.** *Sejam $f, g\colon \mathbb{R}^+ \to \mathbb{R}^+$ duas funções para as quais $f(x) = g(x) = 0$ para todo $0 < x < 1$. Então,*

$$g(x) = \sum_{k=1}^{\infty} f\Big(\frac{x}{k}\Big)$$

para todo $x > 0$ se, e somente se,

$$f(x) = \sum_{k=1}^{\infty} \mu(k) g\Big(\frac{x}{k}\Big)$$

para todo $x > 0$.

DEMONSTRAÇÃO. Suponha primeiro que $g(x) = \sum_{k=1}^{\infty} f(x/k)$ para todo $x > 0$. Então

$$\begin{aligned}\sum_{k=1}^{\infty} \mu(k) g\Big(\frac{x}{k}\Big) &= \sum_{k=1}^{\infty} \mu(k) \left(\sum_{k_1=1}^{\infty} f\Big(\frac{x}{kk_1}\Big)\right) \\ &= \sum_{n=1}^{\infty} f\Big(\frac{x}{n}\Big) \left(\sum_{d|n} \mu(d)\right) \qquad \text{(II)} \\ &= f(x).\end{aligned}$$

Uma conta similar mostra que, se $f(x) = \sum_{k=1}^{\infty} \mu(k) g(x/k)$ para todo $x > 0$, então

$$\begin{aligned}\sum_{k=1}^{\infty} f\Big(\frac{x}{k}\Big) &= \sum_{k=1}^{\infty} \sum_{k_1=1}^{\infty} \mu(k_1) g\Big(\frac{x}{kk_1}\Big) \\ &= \sum_{n=1}^{\infty} g\Big(\frac{x}{n}\Big) \left(\sum_{d|n} \mu(d)\right) \qquad \text{(III)} \\ &= g(x).\end{aligned}$$

□

Segue uma detalhação das transformações feitas nas passagens I,II e III:

- Em I, uma "contagem dupla" foi realizada. Tudo estava sendo contado em função de d, mas contar em função de d' era mais promissor pois junta os termos $\mu(m)$, sendo m um divisor de um certo inteiro t (no caso, $t = n/d'$). Esse tipo de soma é bom, pois conseguimos controlá-la facilmente, de acordo com o lema 2.1.
- Em II e III, o truque foi fixar o produto $kk_1 = n$, de modo que os termos $\mu(d)$, com $d|n$, se juntassem (basta ver que todos os pares $(k, k_1) = (d, n/d)$ aparecem no somatório inicial). Daí, uma aplicação do lema 2.1 nos dá o resultado desejado.

Em suma, forçar as somas $\sum_{d|n} \mu(d))$ aparecerem quando lidando com somatórios pode facilitar na contagem, e é uma ideia que trabalharemos melhor no decorrer do artigo.

Exemplo 2.4. *Para todo inteiro positivo n, defina $d_0(n)$ e $d_1(n)$ como sendo a quantidade de divisores pares e ímpares de n, respectivamente. Mostre que*

$$\left| \sum_{k \le n} d_0(k) - d_1(k) \right| \le n$$

Para todo inteiro positivo n.

SOLUÇÃO. Note que $d_0(n) + d_1(n) = d(n)$ para todo inteiro positivo n. Assim, $d_0(k) - d_1(k) = d(k) - 2d_1(k)$. Seja $a\colon \mathbb{N} \to \{0, 1\}$ uma função tal que $n - a(n)$ é par para todo $n \in \mathbb{N}$. Logo, $d_1(k) = \sum_{d|k} a(d)$ e $d(k) = \sum_{d|k} 1$. Com essa notação, fica fácil vizualizar que

$$\begin{aligned}\sum_{k \le n} d(k) &= \sum_{k \le n} \sum_{d|k} 1 \qquad (1) \\ &= \sum_{d} \Big\lfloor \frac{n}{d} \Big\rfloor\end{aligned}$$

e que

$$\begin{aligned}\sum_{k \le n} d_1(k) &= \sum_{k \le n} \sum_{d|k} a(d) \qquad (2) \\ &= \sum_{d} a(d) \Big\lfloor \frac{n}{d} \Big\rfloor.\end{aligned}$$

Ambas as transformações são contagens duplas; deixamos de contar em k para contar em d. Logo, $\sum_{k \le n} d(k) - 2d_1(k) = \sum_d \lfloor n/d \rfloor - 2a(d) \lfloor n/d \rfloor = \sum_m (-1)^m \lfloor n/m \rfloor = \sum_m \lfloor \frac{n}{2m} \rfloor - \lfloor \frac{n}{2m-1} \rfloor$. Como essa soma certamente é negativa, queremos mostrar que $\sum_m \lfloor \frac{n}{2m-1} \rfloor - \lfloor \frac{n}{2m} \rfloor \le n \iff n - \sum_m \lfloor \frac{n}{2m} \rfloor - \lfloor \frac{n}{2m+1} \rfloor \le n$, o que é verdade pois $\lfloor \frac{n}{2m} \rfloor - \lfloor \frac{n}{2m+1} \rfloor \ge 0$ para todo m. □

O exemplo anterior mostra como escrever funções complexas, como $\sum_{k\le n} d(k)$, em termos de funções simples ou conhecidas ajuda a enxergar contagens duplas. Para isso, foi necessário escrever d e d_1 como somatórios de funções fáceis de se trabalhar. Portanto, pode ser muito conveniente forçar aparecer a maior quantidade de somatórios e funções simples nesse tipo de problema.

Exemplo 2.5. *Para cada real positivo $x \ge 1$, Ramon calcula quantos inteiros a livre de quadrados satisfazem que o número $\left\lfloor \frac{x}{\sqrt{a}} \right\rfloor$ é ímpar e chama esse número de $f(x)$. Calcule $f(x)$ para cada real positivo $x \ge 1$.*

SOLUÇÃO. Seja $\mathbb{A}$ o conjunto dos naturias livres de quadrados e $g\colon \mathbb{R}_{\ge 1} \to \{0,1\}$ uma função tal que $n - g(n)$ é par para todo $n \in \mathbb{N}$ e $g(x) = g(\lfloor x \rfloor)$ para todo $x \ge 1$. Sabemos que

$$f(x) = \sum_{a\in\mathbb{A}} g\left(\left\lfloor \frac{x}{\sqrt{a}} \right\rfloor\right).$$

Pelo lema 2.1, podemos nos livrar da condição $a \in \mathbb{A}$:

$$f(x) = \sum_{a} g\left(\left\lfloor \frac{x}{\sqrt{a}} \right\rfloor\right) \sum_{d^2\mid a} \mu(d).$$

Como $g(x) = \sum_{i\le x} (-1)^{i+1}$, segue que

$$\begin{aligned} f(x) &= \sum_a \left(\sum_{i\le \frac{x}{\sqrt{a}}} (-1)^{i+1} \sum_{d^2\mid a} \mu(d) \right) \\ \implies f(x) &= \sum_a \left(\left[\sum_{i\le \frac{x}{\sqrt{a}}} 1 + 2 \sum_{i\le \frac{x}{2\sqrt{a}}} -1 \right] \sum_{d^2\mid a} \mu(d) \right) \\ \implies f(x) &= \sum_a \left(\sum_{i\le \frac{x}{\sqrt{a}}} 1 \sum_{d^2\mid a} \mu(d) \right) - 2 \sum_a \left(\sum_{i\le \frac{x}{2\sqrt{a}}} 1 \sum_{d^2\mid a} \mu(d) \right) \end{aligned}$$

Fazendo $h(x) = \sum_a \sum_{i\le \frac{x}{\sqrt{a}}} 1 \sum_{d^2\mid a} \mu(d)$, temos que: $f(x) = h(x) - 2h(x/2)$. Logo, basta calcular $h(x)$ para $x \ge 1$:

$$\begin{aligned} h(x) &= \sum_a \left(\sum_{i\le \frac{x}{\sqrt{a}}} 1 \sum_{d^2\mid a} \mu(d) \right) = \sum_a \sum_{i\le \frac{x}{\sqrt{a}}} \sum_{d^2\mid a} \mu(d) \\ &= \sum_{\substack{a \\ i^2 a \le x^2}} \sum_{i} \sum_{d^2\mid a} \mu(d) \end{aligned}$$

Escrevendo $a = d^2 e$, com e livre de quadrados, obtemos que

$$\begin{aligned} h(x) &= \sum_{\substack{a \\ i^2 a \le x^2}} \sum_{i} \sum_{d^2\mid a} \mu(d) = \sum_{\substack{e \\ i^2 d^2 e \le x^2}} \sum_{i} \sum_{d} \mu(d) \\ &= \sum_{e\le x^2} \left(\sum_{\substack{i \\ di \le \frac{x}{\sqrt{e}}}} \sum_{d} \mu(d) \right). \end{aligned} \tag{$\star$}$$

Analisemos melhor uma expressão do tipo $\sum_{\substack{i \\ id\le T}} \sum_d \mu(d) = \sum_d \sum_{i\le T/d} \mu(d) = \sum_d \mu(d) \left\lfloor T/d \right\rfloor$ com $T \ge 1$ real. Como $\left\lfloor T/d \right\rfloor = \left\lfloor \lfloor T \rfloor / d \right\rfloor$ (verifique!), basta analisarmos $\sum_d \mu(d) \left\lfloor T/d \right\rfloor$ para T natural. Note que esse somatório é parecido com os somatórios 1 e 2 encontrados. O que fizemos naqueles casos? Tomamos uma função f e sua função $F(n) = \sum_{d\mid n} f(d)$ (por exemplo, tomamos a função a

e $d_1(n) = \sum_{d|n} a(d)$ em 2), e calculamos $\sum_{k\leq n} F(k)$:

$$\begin{aligned}\sum_{k\leq n} F(k) &= \sum_{k\leq n}\sum_{d|k} f(d)\\ &= \sum_{d} f(d)\sum_{dk\leq n} 1\\ &= \sum_{d} f(d)\left\lfloor \frac{n}{d}\right\rfloor.\end{aligned}$$

Fazendo $f = \mu$, sabemos que $\sum_{k\leq n} F(k) = 1$, pois $F(n) = 0$ para $n \geq 2$ e $F(1) = 1$ pelo lema 2.1. Logo,

$$\sum_{m} \mu(m)\left\lfloor \frac{n}{m}\right\rfloor = 1$$

para todo n natural. Logo, $\star$ vira

$$h(x) = \sum_{e\leq x^2} 1 = \lfloor x^2\rfloor.$$

Portanto, $f(x) = \lfloor x^2\rfloor - 2\lfloor x^2/4\rfloor$. □

A relação $\sum_{k\leq n} F(k) = \sum_m f(m)\left\lfloor \frac{n}{m}\right\rfloor$ pode ser útil em diversos problemas de funções aritméticas, uma vez que F é fácil de se calcular para diversas funções; μ, φ, e até a função $n \mapsto 1$ são exemplos disso.

Exemplo 2.6. *Seja p um primo e t um divisor de $p-1$. Então, existem exatamente $\varphi(t)$ restos módulo p que satisfazem a equação $\mathrm{ord}_p x = t$.*

SOLUÇÃO. Sabemos que $x^t \equiv 1 \pmod p$ possui exatamente t soluções quando $t|p-1$ (consideramos apenas os números do conjunto $\{0, 1, 2, \ldots, p-1\}$). Seja $f(t)$ a quantidade de inteiros módulo p que satisfazem $\mathrm{ord}_p x = t$. Então, $F(t) = \sum_{d|t} f(d) = t$, já que esse somatório conta a quantidade de raízes de $x^t - 1 \pmod p$. Como isso vale para todo $t|p-1$, podemos realizar contas análogas às feitas no teorema 2.2 para mostrar que $f(t) = \sum_{d|t} \mu(d)F(t/d) = \sum_{d|t} \mu(d)\frac{t}{d}$. Aplicando a primeira fórmula de inversão de Möbius para $f = \varphi$, concluímos que $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$, de modo que $f(t) = \varphi(t)$ para $t|p-1$. □

Note que, na solução anterior, não é possível aplicar diretamente a fórmula de inversão, uma vez que a função f não está definida para todos os naturais. No entanto, é fácil ver que as contas feitas no teorema 2.2 podem ser refeitas no problema, já que $\sum_{d|t} f(d) = t$ vale para todos os $t|p-1$, de modo que todo divisor d de t também satisfaz essa relação, e na prova da fórmula usamos apenas que o resultado é válido para divisores do número n.

Problemas Propostos

2.1. *Mostre que, para todo inteiro $n \geq 1$,*

$$\sum_{k|n} d(k)^3 = \left(\sum_{k|n} d(k)\right)^2.$$

Isso nos diz que existem diversas soluções $(a_1, a_2, \ldots, a_n)$ de

$$\sum_{i\leq n} a_i^3 = \left(\sum_{i\leq n} a_i\right)^2.$$

2.2. *Mostre que, para todo $n > 1$,*

$$\left|\sum_{k\leq n} \frac{\mu(k)}{k}\right| < 1.$$

2.3. *Mostre que existem infinitos M para os quais $\frac{\sigma(m)}{m} < \frac{\sigma(M)}{M}$ para todo $m < M$.*

2.4. *Mostre que $\varphi(n) \leq n - \sqrt{n}$ para n composto.*

2.5. *Encontre todas as funções crescentes $f\colon \mathbb{N} \to \mathbb{N}$ tais que $f(2) = 7$ e, para todos $m, n \in \mathbb{N}$,*

$$f(mn) = f(m)f(n) + f(m) + f(n).$$

2.6. *Para cada inteiro $n > 0$, seja $f(n)$ o menor inteiro positivo que possui exatamente n divisores positivos. Mostre que $f(2^k)$ divide $f(2^{k+1})$ para todo $k \geq 0$.*

2.7. *Sejam n e k inteiros positivos tais que*

$$1 = \underbrace{\varphi(\varphi(\ldots\varphi(}_{k \text{ vezes}} n)\ldots)).$$

Mostre que $n \leq 3^k$.

2.8. *Dado um inteiro não negativo n, seja $rad(n) = 1$ se $n = 0$ ou $n = 1$ e $rad(n) = p_1 p_2 \cdots p_k$, onde $p_1, p_2, \ldots, p_k$ são os fatores primos de n para $n \geq 2$. Encontre todos os polinômios P de coeficientes inteiros não negativos para os quais $rad(P(n))$ divide $rad(P(n^{rad(n)}))$ para todo n não negativo.*

2.9. *Seja D_n o conjunto de todos os divisores positivos de n. Encontre todos os inteiros positivos ímpares n tais que se $a, b \in D_n$ e $mdc(a, b) = 1$, então $a + b - 1 \in D_n$.*

2.10. *Mostre que*

$$\sum_{\substack{k \leq n \\ mdc(n,k)=1}} k^2 = \frac{\varphi(n)}{6}\left(2n^2 + (-1)^k \prod_{p|n} p\right).$$

($\prod_{p|n} p$ percorre somente os primos que dividem n e k é a quantidade de divisores primos de n)

3 Estimativas

Nesta seção o nosso objeto de estudo são propriedades de crescimento de funções aritméticas. Começamos com a seguinte

Proposição 3.1. *A série*

$$\sum_{\substack{p \\ p \text{ primo}}} \frac{1}{p}$$

diverge.

DEMONSTRAÇÃO. Sabemos que $\sum_{n \geq 1} 1/n$ diverge. Entretanto,

$$\sum_{n \geq 1} \frac{1}{n} = \prod_{\substack{p \\ p \text{ primo}}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \prod_{\substack{p \\ p \text{ primo}}} \left(1 + \frac{1}{p-1}\right).$$

Tomando logaritmos,

$$\begin{aligned} \log\left(\sum_{n \geq 1} \frac{1}{n}\right) &= \sum_{\substack{p \\ p \text{ primo}}} \log\left(1 + \frac{1}{p-1}\right) \\ &\leq \sum_{\substack{p \\ p \text{ primo}}} \frac{1}{p-1} \end{aligned}$$

Usamos a desigualdade $\log(x+1) \leq x$ para todo $x \geq 0$. Disso, segue que $\sum_p 1/(p-1)$ diverge. Logo $\sum_{p>2} 1/(p-1)$ diverge, e como $1/(p_n - 1) \leq 1/p_{n-1}$ para $n \geq 2$ (onde p_n é o $n-$ésimo primo), concluímos que $\sum_p 1/p$ diverge. □

Exemplo 3.2. *Mostre que, dados $\alpha > 1$ real e m natural, existe n para o qual $\frac{p_{m+n}}{p_n} \leq \alpha$, onde p_n denota o $n-$ésimo primo.*

SOLUÇÃO. Queremos que em algum intervalo da forma $T(N) = [\alpha^N, \alpha^{N+1})$ exista uma quantidade suficientemente grande de primos. Suponha, por absurdo, que em cada intervalo dessa forma existam no máximo C primos. Então,

$$\sum_{\substack{p \in T(N) \\ p \text{ primo}}} \frac{1}{p} \leq \frac{C}{\alpha^N}.$$

Logo,

$$\sum_{\substack{p \leq \alpha^{N+1} \\ p \text{ primo}}} \frac{1}{p} \leq \sum_{0 \leq n \leq N} \frac{C}{\alpha^N},$$

uma contradição à proposição 3.1, já que o lado direito direito da desigualdade diverge. □

No exemplo anterior, poderíamos substituir $\alpha, \alpha^2, \ldots$ por qualquer sequência crescente $a_1, a_2, \ldots$ para a qual $\sum_n 1/a_n$ converge, e concluímos que em algum intervalo da forma $[a_{N-1}, a_N)$ existe uma quantidade suficientemente grande de primos e, portanto, $p_{m+n}/p_n \leq a_N/a_{N-1}$ para alguns n, N.

Proposição 3.3. *Seja $H_n = \sum_{k \leq n} 1/k$. Então,*

$$H_n = \log n + O(1).$$

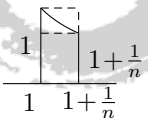
Precisaremos de alguns lemas.

Lema 3.4. $\lim_{n\to\infty} \log\left(\left(1+\frac{1}{n}\right)^n\right) = \lim_{n\to\infty} \log\left(\left(1+\frac{1}{n}\right)^{n+1}\right) = 1.$

DEMONSTRAÇÃO. Note que

$$\frac{1}{n+1} < \log\left(1+\frac{1}{n}\right) < \frac{1}{n}.$$

Isso segue pela definição do logartimo como a integral $\log(x) = \int_1^x \frac{1}{x} dx$ (estimamos a área por retângulos):



Assim,

$$\frac{n}{n+1} < \log\left(\left(1+\frac{1}{n}\right)^n\right) < 1 \qquad \text{e} \qquad 1 < \log\left(\left(1+\frac{1}{n}\right)^{n+1}\right) < \frac{n+1}{n}.$$

Pelo Teorema do Confronto, o resultado segue. □

Lema 3.5. *As sequências $\left\{\left(1+\frac{1}{n}\right)^n\right\}_{n\geq 1}$ e $\left\{\left(1+\frac{1}{n}\right)^{n+1}\right\}_{n\geq 1}$ são crescente e decrescente, respectivamente.*

DEMONSTRAÇÃO. Utilizaremos a Desigualdade de Bernoulli: $(1+x)^n \geq 1+nx$ para todo n inteiro e $x > -1$ real:

$$\begin{aligned}
\frac{\left(1+\frac{1}{n+1}\right)^{n+1}}{\left(1+\frac{1}{n}\right)^n} &= \frac{n+1}{n}\left(\frac{n(n+2)}{(n+1)^2}\right)^{n+1} \\
&\geq \frac{n+1}{n}\left(1-\frac{1}{n+1}\right) \\
&= 1.
\end{aligned}$$

Apenas escrevemos $\frac{n(n+2)}{(n+1)^2} = 1 - \frac{1}{(n+1)^2}$ e, então, utilizamos Bernoulli. Analogamente prova-se a monotonicidade de $\left\{\left(1+\frac{1}{n}\right)^{n+1}\right\}_{n\geq 1}$. □

Lema 3.6. *Temos que*

$$\log 2 - \frac{1}{2n+1} \leq \sum_{k \leq 2n} \frac{(-1)^{k+1}}{k} \leq \log 2.$$

DEMONSTRAÇÃO. Primeiro, mostramos que $\sum_k \frac{(-1)^{k+1}}{k}$ converge. Sendo $S_n = \sum_{k \leq n} \frac{(-1)^{k+1}}{k}$, temos que $S_{2n+1} - S_{2n} = \frac{1}{2n+1} > 0$, $S_{2n+1} - S_{2n-1} = \frac{1}{2n+1} - \frac{1}{2n} < 0$ e que $S_{2n+2} - S_{2n} = \frac{1}{2n+1} - \frac{1}{2n+2} > 0$. Ou seja, $S_{2n+1} > S_{2n}$, $S_{2n+1} < S_{2n-1}$ e $S_{2n+2} > S_{2n}$. Logo, $S_2 \leq S_{2n} < S_{2n+1} \leq S_1$. Isso diz que as sequências S_{2n+1} e S_{2n} convergem para limites L_1 e L_2, respectivamente. Basta mostrar que $L_1 = L_2$:

$$L_1 - L_2 = \lim_{n\to\infty} S_{2n+1} - S_{2n} = \lim_{n\to\infty} \frac{1}{2n+1} = 0.$$

Assim, segue que $\lim_{n\to\infty} S_n = L$, e que $S_{2n} < L < S_{2n+1}$ para todo n. Portanto, veja que

$$\begin{aligned} 0 < L - S_{2n} < S_{2n+1} - S_{2n} &= \frac{1}{2n+1} \\ \implies L - \frac{1}{2n+1} < S_{2n} &< L. \end{aligned}$$

Agora, basta mostrar que $L = \log 2$.
Pelos lemas 3.4 e 3.5, temos que

$$\left(1 + \frac{1}{n}\right)^n \leq \left(1 + \frac{1}{n+t}\right)^{n+t} < e$$

e que

$$\left(1 + \frac{1}{n}\right)^{n+1} \geq \left(1 + \frac{1}{n+t}\right)^{n+t+1} > e.$$

Isso nos diz que

$$\left(1 + \frac{1}{n+t}\right)^{\frac{n}{n+1}} \leq \left(1 + \frac{1}{n}\right)^{\frac{n}{n+t}} \leq \left(1 + \frac{1}{n+t}\right). \tag{i}$$

Assim, como $\sum_{n<k\leq 2n} \frac{1}{k} = \sum_{k\leq n} \frac{1}{2k} + \frac{1}{2k-1} - \frac{1}{k} = \sum_{k\leq 2n} \frac{(-1)^{k+1}}{k}$, então $L = \lim_{n\to\infty} \sum_{n<k\leq 2n} \frac{1}{k}$. Portanto,

$$\begin{aligned} e &= \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n \\ \implies e^L &= \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^{\sum_{n<k\leq 2n} \frac{n}{k}} \end{aligned}$$

Mas i nos diz que

$$\left(\frac{2n+1}{n+1}\right)^{\frac{n}{n+1}} \leq \left(1 + \frac{1}{n}\right)^{\sum_{n<k\leq 2n} \frac{n}{k}} \leq \frac{2n+1}{n+1}.$$

Logo, pelo Teorema do Confronto,

$$\lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^{\sum_{n<k\leq 2n} \frac{n}{k}} = 2$$

Portanto, $e^L = 2 \Rightarrow L = \log 2$. □

DEMONSTRAÇÃO (DA PROPOSIÇÃO 3.3). Note que

$$\begin{aligned} H_{2n} - H_n &= \sum_{k\leq n} \frac{1}{2k} + \frac{1}{2k-1} - \frac{1}{k} \\ &= \sum_{k\leq 2n} \frac{(-1)^{k+1}}{k}. \end{aligned}$$

Pelo lema 3.6, segue que $\log 2 - \frac{1}{2n+1} \leq H_{2n} - H_n \leq \log 2$. Disso, concluímos que $H_{2^n} = n \log 2 + O(1)$, já que $\sum_{k \leq n} H_{2^k} - H_{2^k - 1} = H_{2^n} - H_1$. Logo, sendo $m = \lfloor \log_2 n \rfloor$,

$$\frac{H_{2^m}}{(m+1)\log 2} \leq \frac{H_n}{\log n} \leq \frac{H_{2^{m+1}}}{m \log 2},$$

donde segue que $H_n = \log n + O(1)$. □

Observação 3.7. *Grande parte da demonstração do lema 3.6 é baseada no critério de Leibniz para a convergência de séries alternadas, e afirma que, dada uma sequência a_n de reais positivos satisfazendo $\lim_{n\to\infty} a_n = 0$ e $a_{n+1} \leq a_n$ para todo n, então a série $\sum_n (-1)^n a_n$ converge.*

Segue diretamente da proposição 3.3 a seguinte

Proposição 3.8. $\frac{1}{n} \sum_{k \leq n} d(n) = \log n + O(1)$.

Exemplo 3.9. *Determine se existe algum inteiro positivo t para o qual a equação*

$$\sum_k \left\lfloor \frac{n}{k} \right\rfloor = m^2 + t \tag{1}$$

possui mais de $10^{10^{10}}$ soluções $(n, m) \in \mathbb{N} \times \mathbb{N}$.

SOLUÇÃO. Intuitivamente, fixado t, se (1) possui muitas soluções (n, m), t fica proporcionalmente pequeno em relação a m quando m fica grande. Assim, sendo $D(n) = \sum_k \left\lfloor \frac{n}{k} \right\rfloor$, parece que olhar para a equação $D(n) = \lfloor \sqrt{D(n)} \rfloor^2 + t$ é promissor, pois t fica pequeno em relação a $D(n)$.
Como $D(n) - \lfloor \sqrt{D(n)} \rfloor^2 \leq 2\lfloor \sqrt{D(n)} \rfloor$, para garantir que $D(n) - \lfloor \sqrt{D(n)} \rfloor^2$ assuma diversas vezes o mesmo valor, basta que $\frac{n}{\lfloor \sqrt{D(n)} \rfloor}$ seja grande o suficiente. De fato, como $D(n)$ é crescente, e sendo $f(n, t)$ o número de soluções de $D(x) = \lfloor \sqrt{D(x)} \rfloor^2 + t$ com $x \leq n$, sabemos que $f(n, t) \geq \frac{n}{2\lfloor \sqrt{D(n)} \rfloor}$ para algum t, pois $t > 2\lfloor \sqrt{D(n)} \rfloor \Rightarrow f(n, t) = 0$. Logo, basta que $\frac{n}{\lfloor \sqrt{D(n)} \rfloor}$ assuma valores suficientemente grandes, isto é, queremos que $\frac{n^2}{D(n)} \to \infty$ quando $n \to \infty$. Mas isto é verdade, já que, pela proposição 3.3, $D(n) = n \log n + O(n)$. Portanto, tal t existe. □

A próxima proposição indica a densidade dos números livres de quadrados no conjunto dos naturais.

Proposição 3.10. $\lim_{n\to\infty} \frac{\left|\{x \leq n \,|\, x \text{ livre de quadrados}\}\right|}{n} = \frac{6}{\pi^2}$.

DEMONSTRAÇÃO. Note que

$$\begin{aligned}
\left|\{x \leq n \,|\, x \text{ livre de quadrados}\}\right| &= \sum_{k \leq n} |\mu(k)| \\
&= \sum_{k \leq n} \sum_{d^2 | k} \mu(d) \\
&= \sum_d \mu(d) \left(\sum_{e \leq \frac{n}{d^2}} 1 \right) \\
&= \sum_d \mu(d) \left\lfloor \frac{n}{d^2} \right\rfloor \\
&= n \sum_{d \leq \sqrt{n}} \frac{\mu(d)}{d^2} + O(\sqrt{n}).
\end{aligned}$$

Logo, a densidade procurada equivale a encontrar o limite

$$\lim_{n\to\infty} \frac{n \sum_{d \leq \sqrt{n}} \frac{\mu(d)}{d^2} + O(\sqrt{n})}{n} = \lim_{n\to\infty} \sum_{d \leq \sqrt{n}} \frac{\mu(d)}{d^2} = \sum_d \frac{\mu(d)}{d^2}.$$

Por outro lado,

$$\sum_k \frac{1}{k^2} \sum_d \frac{\mu(d)}{d^2} = \sum_k \sum_d \frac{\mu(d)}{k^2 d^2}$$
$$= \sum_n \frac{\sum_{d|n} \mu(d)}{n^2} = 1.$$

Logo,

$$\sum_d \frac{\mu(d)}{d^2} = \left(\sum_k \frac{1}{k^2} \right)^{-1} = \frac{6}{\pi^2}.$$

(Assumimos, sem provas, que $\sum_n \frac{1}{n^2} = \frac{\pi^2}{6}$) □

Agora, apresentamos algumas estimativas envolvendo números primos.

Lema 3.11. *Para todo $n > 1$ vale que*

$$\prod_{\substack{p \leq n \\ p \text{ primo}}} p \leq 4^{n-1}.$$

DEMONSTRAÇÃO. Note que precisamos provar o resultado apenas para números ímpares, já que, se vale para $n = 2k+1$, então também vale para $n = 2k+2$. Como o resultado é verdadeiro para valores pequenos de n (verifique!), podemos proceder por indução em $n = 2k+1$. Para isso, note que todo primo $k+1 < p < 2k+2$ divide $\binom{2k+1}{k+1}$. Logo,

$$\prod_{k+1<p<2k+2} p \leq \binom{2k+1}{k+1} \leq 4^k.$$

A segunda desigualdade ocorre pois $2^{2m+1} = \sum_t \binom{2k+1}{t} \geq \binom{2k+1}{k+1} + \binom{2k+1}{k} = 2\binom{2k+1}{k+1}$. Portanto,

$$\prod_{p \leq 2k+1} p = \prod_{p \leq k+1} p \prod_{k+1<p<2k+2} p \leq 4^{2k},$$

como desejado ($\prod_{p \leq k+1} p \leq 4^k$ por hipótese de indução). □

Lema 3.12. *Sejam n um natural e p um número primo. Então a maior potência de p que divide $\binom{2n}{n}$ é menor ou igual a $2n$. Além disso, para todo $\frac{2}{3}n < p < n$, p não divide $\binom{2n}{n}$.*

DEMONSTRAÇÃO. O expoente da maior potência de p que divide $\binom{2n}{n}$ é

$$\sum_k \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor.$$

Como $\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \leq 1$ (verifique!), segue que

$$\sum_k \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{p^k \leq 2n} 1 = \lfloor \log_p 2n \rfloor.$$

Portanto, se p^a divide $\binom{2n}{n}$, segue que $p^a \leq p^{\lfloor \log_p 2n \rfloor} \leq 2n$. Ainda mais, se $\frac{2}{3}n < p < n$, então a maior potência de p que divide $(2n)!$ é 2, e a maior potência de p que divide n é 1. Assim, $p \nmid \binom{2n}{n}$. □

Com esses lemas, estamos prontos para o

Teorema 3.13 (Postulado de Bertrand)**.** *Para qualquer inteiro positivo n, existe um primo p tal que $n \leq p \leq 2n$.*

DEMONSTRAÇÃO. Suponha, por absurdo, que isso não ocorre para algum n suficientemente grande. Dado um primo p_i, seja α_i o maior inteiro tal que $p_i^{\alpha_i} | \binom{2n}{n}$. Como estamos supondo que não existem primos entre n e $2n$, e, pelo lema 3.12, concluímos que $\binom{2n}{n}$ é o produto de primos menores ou iguais a $\frac{2}{3}n$ com $p_i^{\alpha_i} \leq 2n$. Além disso, segue também do lema 3.12 que $\alpha_k \leq 1$ para $p_k \geq \sqrt{2n}$, de modo que

$$\binom{2n}{n} \leq \prod_{p_i \leq 2n} p_i^{\alpha_i} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq \prod_{p \leq \sqrt{2n}} 2n \prod_{p \leq \frac{2}{3}n} p.$$

Como estamos supondo que n é suficientemente grande, vamos supor que a quantidade de primos entre 1 e $\sqrt{2n}$ é menor que $\sqrt{n/2} - 1$ (isso é verdade para $\sqrt{2n} \geq 15 \Rightarrow n \geq 115$, já que metade dos inteiros são pares e os ímpares 9 e 15 não são primos). Portanto,

$$\binom{2n}{n} \leq (2n)^{\sqrt{n/2}-1} 4^{\frac{2}{3}n}.$$

Entretanto, como $4^n = \sum_k \binom{2n}{k} \leq 2n\binom{2n}{n}$, segue que

$$\frac{2^{2n-1}}{n} \leq (2n)^{\sqrt{n/2}-1} 4^{\frac{2}{3}n} \iff 2^{\frac{2}{3}n} \leq (2n)^{\sqrt{n/2}}.$$

Logo, como essa última igualdade não ocorre para $n \geq 115$, se o teorema é falso para algum n, então $n < 115$. Como podemos tomar $p = 2, 5, 11, 23, 47, 79, 127$ para $n \in [1, 2]$, $[3, 5]$, $[6, 11]$, $[12, 23]$, $[24, 47]$, $[48, 79]$, $[80, 115]$, respectivamente, o teorema é verdadeiro para todos os valores de n. □

A seguir, provaremos uma versão fraca do Teorema dos Números Primos, que diz que $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$, onde $\pi(x)$ é a quantidade de primos menores ou iguais a x.

Teorema 3.14. *Sendo $\pi(x)$ a quantidade de primos menores ou iguais a x, então*

$$(\log 2 - o(1))\frac{x}{\log x} < \pi(x) < (2\log 2 + o(1))\frac{x}{\log x}.$$

Ainda mais, tem-se que

$$\frac{x}{3\log x} < \pi(x) < \frac{5x\log 2}{\log x}$$

para todo $x \geq 2$.

DEMONSTRAÇÃO. Note que todo primo entre $n+1$ e $2n$ divide $\binom{2n}{n}$. Assim, como

$$\binom{2n}{n} < 4^n,$$

o produto dos primos entre $n+1$ e $2n$ é menor que 4^n, ou seja, $n^{\pi(2n)-\pi(n)} < 4^n \Rightarrow (\pi(2n) - \pi(n))\log n < 2n\log 2$, isto é,

$$\pi(2n) - \pi(n) < \frac{2n\log 2}{\log n}. \qquad (*)$$

Assim,

$$\sum_{k\geq 0} \pi(x/2^k) - \pi(x/2^{k+1}) = \pi(x) < \sum_{k\geq 0} \frac{\frac{x}{2^{k-1}}\log 2}{\log \frac{x}{2^k}} = (2\log 2 + o(1))\frac{x}{\log x}.$$

Note que, por indução, $(*)$ nos diz que

$$\pi(2^{k+1}) \leq \frac{5\cdot 2^k}{k}.$$

Logo, para $2^k < x \leq 2^{k+1}$, segue que

$$\pi(x) \leq \frac{5\cdot 2^{k+1}}{k} \leq \frac{5x\log 2}{\log x},$$

uma vez que $x/\log x$ é crescente para $x \geq 3$ (para valores pequenos de x testa-se facilmente que essa desigualdade ocorre).

Agora, estamos interessados na outra desigualdade. Dado um primo p, seja α o maior inteiro para o qual $p^\alpha | \binom{2n}{n}$. Pelo lema 3.12, sabemos que $p^\alpha \leq 2n$, de modo que, como $p | \binom{2n}{n} \Rightarrow p \leq 2n$,

temos $\binom{2n}{n} \leq 2n^{\pi(2n)} \Rightarrow \log\binom{2n}{n} \leq \pi(2n)\log 2n$. Assim, $\pi(2n) \geq \frac{\log\binom{2n}{n}}{\log 2n}$. Mas $4^n = \sum_k \binom{2n}{k} \leq (2n+1)\binom{2n}{n}$, e concluímos que

$$\pi(2n) \geq \frac{n\log 4 - \log(2n+1)}{\log 2n} = \frac{(\log 2 - o(1))2n}{\log 2n},$$

donde sai que, para todo x,

$$\pi(x) > (\log 2 - o(1))\frac{x}{\log x}.$$

Para obter uma constante, note que

$$\binom{2n}{n} > 2^{\frac{2n}{3}}$$

para $n \geq 15$, e disso segue que

$$\pi(2n) \geq \frac{\log\binom{2n}{n}}{\log 2n} \geq \frac{2n}{3\log 2n}$$

para $n \geq 15$, e, portanto,

$$\pi(x) \geq \frac{x}{3\log x}$$

para todo $x \geq 30$. Verfica-se facilmente que essa desigualdade também é válida para $2 \leq x \leq 30$. □

Os próximos exemplos mostram como as ideias por trás dos teoremas 3.13 e 3.14 são importantes.

Exemplo 3.15. *Dado um inteiro n, escreva $n! = a_n b_n^2$, onde a_n é um inteiro livre de quadrados. Então mostre que, dado $\epsilon > 0$, existe u, n_ϵ tal que, para todo $n > n_\epsilon$,*

$$2^{(1-\epsilon)n} < a_n < 2^{(1+\epsilon)n}.$$

SOLUÇÃO. Primeiro, defina como $s(n)$ a parte livre de quadrados de n. O problema nos pede para mostrar que $s(n!)$ é da ordem de 2^n (a condição do problema é equivalente a $\log a_n = n\log 2 + o(n)$). Veja que, se $d^2|n$ então $d^2|n/s(n)$, de modo que $s(n) = s(n/d^2)$. Nos resultados anteriores, vimos diversas estimativas nos divisores primos de $\binom{2n}{n}$. Como $(n!)^2|(2n)!$, concluímos que $s((2n)!) = s\left(\binom{2n}{n}\right)$.
Pelo lema 3.12, sabemos que, se $p^2|\binom{2n}{n}$, então $p^2 \leq 2n \Rightarrow p \leq \sqrt{2n}$. Assim, sendo $\nu_p(n)$ o maior inteiro para o qual $p^{\nu_p(n)}|\binom{2n}{n}$, temos que

$$\frac{\binom{2n}{n}}{\prod\limits_{p\leq\sqrt{2n}} p^{\nu_p(n)}} \leq s((2n)!).$$

Mas

$$\prod_{p\leq\sqrt{2n}} p^{\nu_p(n)} \leq \prod_{p\leq\sqrt{2n}} p^{\log_p 2n} \leq (2n)^{\sqrt{2n}} = 2^{\sqrt{2n}\log_2 2n}.$$

Como $\binom{2n}{n} > \frac{2^{2n-1}}{n}$ (ver 3.13), segue que

$$s((2n)!) \geq \frac{\binom{2n}{n}}{\prod\limits_{p\leq\sqrt{2n}} p^{\nu_p(n)}} \geq \frac{\frac{2^{2n-1}}{n}}{2^{\sqrt{2n}\log_2 2n}} = 2^{2n-o(2n)} = 2^{2n\left(1-o(1)\right)},$$

Demonstrando a primeira desigualdade. Para a segunda, basta ver que

$$s((2n)!) = s\left(\binom{2n}{n}\right) \leq \binom{2n}{n} < 2^{2n}.$$

Deste modo, para n par,

$$2^{n\left(1-o(1)\right)} < s(n!) < 2^n.$$

Logo, $\log s((2n)!) = 2n\log 2 + o(2n)$.
Para n ímpar, note que

$$s\big((2n+1)!\big) = \frac{s\big((2n)!\big)\cdot s(2n+1)}{\mathrm{mdc}\big(s((2n)!), s(2n+1)\big)^2}.$$

De fato, como $s(2n+1)b_{2n+1}^2 = (2n+1)! = (2n+1)s\big((2n)!\big)b_{2n}^2$, então $s(2n+1)b_{2n+1}^2 = s(2n+1)s\big((2n)!\big)b^2$, onde $b = b_{2n}\cdot\frac{2n+1}{s(2n+1)}$. Se um inteiro divide $s(2n+1)$ e $s\big((2n)!\big)$, ele "vai" para a parte quadrada, e disso segue a igualdade desejada.
Como $\frac{s(2n+1)}{\mathrm{mdc}\left(s((2n)!),s(2n+1)\right)^2} = O(n)$, então

$$\begin{aligned} & s((2n+1)!) = s((2n)!)O(n) \\ \implies & \log s((2n+1)!) = \log s((2n)!) + O(\log n) \\ \implies & \log s((2n+1)!) = (2n+1)\log 2 + o(2n+1), \end{aligned}$$

como desejado. □

Exemplo 3.16. *Mostre que, dado $c\in\mathbb{N}$, o número $(n!)^{n+c}$ divide $(n^2)!$ para infinitos naturais n.*

SOLUÇÃO. Queremos mostrar que, para infinitos $n\in\mathbb{N}$, a seguinte desigualdade valha para todo p primo:

$$\begin{aligned} & v_p\big((n!)^{n+c}\big) \le v_p\big((n^2)!\big) \\ \iff & (n+c)v_p(n!) \le v_p\big((n^2)!\big) \\ \iff & (n+c)\cdot\frac{n-s_p(n)}{p-1} \le \frac{n^2-s_p(n^2)}{p-1}. \end{aligned}$$

Dizemos que $s_p(n)$ é soma dos dígitos de n quando escrito na base p. Como $s_p(ab)\le s_p(a)s_p(b)$ (verifique!), então $\frac{n^2-s_p(n^2)}{p-1}\ge\frac{n^2-s_p(n)^2}{p-1}$. Logo, simplificando a última desigualdade trocando $s_p(n^2)$ por $s_p(n)^2$, basta mostrar que existem infinitos n para os quais

$$c\le s_p(n)$$

para todo p primo. Para $n\ge c$ e $p>n$ essa desigualdade ocorre, já que n vira um dígito na base p. Portanto, precisamos nos preocupar apenas com os primos $p\le n$.
Seja $\alpha_p = \lfloor\log_p n\rfloor$ (consideramos apenas n suficientemente grande). Vamos contar quantos inteiros k entre 1 e n satisfazem $s_p(k)<c$. Essa quantidade é certamente menor que o número de vetores $(m_0,m_1,\ldots,m_{\alpha_p})$ de entradas inteiras não negativas com $m_0+m_1+\cdots+m_{\alpha_p}<c$ (a entrada m_i indica o coeficiente de p^i na representação de k na base p), que é, por sua vez, menor que α_p^C para algum C suficientemente grande que independe de n e p (de fato, o número de soluções de $m_0+m_1+\ldots+m_{\alpha_p+1}=c$ é $\binom{\alpha_p+c+1}{c}$, que é um polinômio de grau c em α_p e portanto, para x e C suficientemente grandes, vale que $x^C>\binom{x+c+1}{c}$). Assim, se mostrarmos que

$$\sum_{p\text{ primo}\le n}(\log_p n)^C < \frac{n}{t} \qquad (\triangle)$$

para n suficientemente grande e um $t>1$ fixo, então pelo menos $n-\frac{n}{t}$ inteiros entre 1 e n vão satisfazer $c\le s_p(k)$ para todo p primo, de modo que provaremos a existência de infinitos inteiros que satisfazem as condições desejadas. Como $\log_p n\le 2$ para $p>\sqrt{n}$ (ou seja, é um número pequeno), e $\log_p n\le\log_2 n$, temos que

$$\sum_{p\le n}(\log_p n)^C \le \sum_{p\le\sqrt{n}}(\log_2 n)^C + \sum_{\sqrt{n}<p\le n}2^C = \pi(\sqrt{n})(\log_2 n)^C + (\pi(n)-\pi(\sqrt{n}))2^C.$$

Fazendo $n=2^{2m}$, segue que

$$\sum_{p\le n}(\log_p n)^C \le \pi(2^m)(2m)^C + (\pi(2^{2m})-\pi(2^m))2^C$$

Agora, pelo teorema 3.14, temos que $\pi(2^m) < \frac{5\cdot 2^m\log 2}{m\log 2} = \frac{5\cdot 2^m}{m}$, e, por $(*)$, $\pi(2^{2m})-\pi(2^m) < \frac{2^{2m+1}\log 2}{2m\log 2} = \frac{2^{2m}}{m}$ (pois $m\le 2m-1$). Portanto,

$$\begin{aligned} \sum_{p\le n}(\log_p n)^C &\le (2m)^C\cdot\frac{5\cdot 2^m}{m} + 2^C\cdot\frac{2^{2m}}{m} \\ &= 2^{2m}\left(\frac{2^C}{m}+\frac{5\cdot(2m)^C}{2^m\cdot m}\right). \end{aligned}$$

Mas $\frac{2^C}{m}\to 0$ e $\frac{5\cdot(2m)^C}{2^m\cdot m}\to 0$ quando $m\to\infty$; em particular, para qualquer $t>1$, $(\triangle)$ é verdadeira para n suficientemente grande. □

Exemplo 3.17. *Seja $a_1 < a_2 < \cdots$ a sequência dos naturais livres de quadrados. Mostre que, dado $c \in \mathbb{N}$, existem infinitos n para os quais $a_{n+1} - a_n = c$.*

SOLUÇÃO. Como não existem inteiros livres de quadrados entre a_n e a_{n+1} por definição, precisamos garantir que $a_n + 1, a_n + 2, \ldots, a_n + (c-1)$ sejam inteiros com algum divisor quadrado perfeito. Para isso, tome $c-1$ primos distintos $p_1, p_2, \ldots, p_{c-1}$, inicialmente sem restrições. Então, pelo Teorema Chinês dos Restos, o sistema de congruências $a_n + i \equiv 0 \pmod{p_i^2}$ possui solução única módulo $\prod_{i \leq c-1} p_i^2 = P$. Seja m tal solução. Então, todos os inteiros que satisfazem tal congruência são da forma $Pn + m$, com $n \in \mathbb{Z}$. Nosso objetivo agora é mostrar que existem infinitos n para os quais $Pn + m$ e $Pn + (m + c)$ são livres de quadrados. Para que não haja risco de $\text{mdc}(P, m) > 1$ ou $\text{mdc}(P, m + c) > 1$ (e esse mdc poder ser um inteiro dívisivel por p_i^2 para algum i), vamos supor que $p_i > c$ para todo i, de modo que $p_i | Pn + (m + i)$, mas $p_i \nmid Pn + m, Pn + (m + c)$.
Agora, mostremos que, dado q um primo diferente de $p_1, p_2, \ldots, p_{c-1}$,

$$\lim_{n\to\infty} \frac{|\{i \leq n \mid q^2 \text{ divide } Pi + t\}|}{n} = \frac{1}{q^2},$$

onde $t \in \{m, m + c\}$.
Como $q \nmid P$, então se $Pi + t \equiv Pj + t \pmod{q^2} \implies i \equiv j \pmod{q^2}$. Assim, como $\{P \cdot 0 + t, P \cdot 1 + t, \ldots, P \cdots (q^2 - 1) + t\}$ é um sistema completo de restos módulo q^2, tome $0 \leq r \leq q^2 - 1$ para o qual $q^2 | Pr + t$. Então, todos os inteiros i para os quais $q^2 | Pi + t$ são da forma $q^2 k + r$, $k \in \mathbb{Z}$. Logo, basta contarmos quantos são inteiros positivos da forma $q^2 k + r$ menores ou iguais a n, ou seja, $q^2 k + r \leq n \iff k \leq \frac{n-r}{q^2}$. Portanto, a quantidade de tais inteiros é $\lfloor \frac{n-r}{q^2} \rfloor + 1$. Assim,

$$\frac{|\{i \leq n \mid q^2 \text{ divide } Pi + t\}|}{n} = \frac{\left\lfloor \frac{n-r}{q^2} \right\rfloor + 1}{n} = f(n).$$

Como $\lim_{n\to\infty} f(n)$ existe (aconselhamos o leitor a verificar tal existência. É importante ter em mente que só podemos calcular um limite se provarmos a existência dele), é facilmente calculável que esse limite é $1/q^2$, como queríamos.
Assim, mostramos que a densidade dos inteiros do conjunto $\{Pn + t, n \in \mathbb{N}\}$, com $t \in \{m, m + c\}$ que são divisíveis por q^2 é $1/q^2$. Logo, a densidade dos inteiros do conjunto $\{Pn + m, Pn + (m + c) \mid n \in \mathbb{N}\}$ que são divisíveis por q^2 é $2/q^2$. Portanto, a densidade dos inteiros i para os quais q^2 divide algum número do par $(Pi + m, Pi + (m + c))$ para algum q primo é, no máximo (possivelmente contaremos algum i mais de uma vez; se q^2 e r^2 dividem $Pi + m$, então contamos i duas vezes),

$$\sum_{q \text{ primo}} \frac{2}{q^2}.$$

Mas, como

$$\begin{aligned}
\sum_{q \text{ primo}} \frac{1}{q^2} &\leq \sum_k \frac{1}{(2k-1)^2} + \frac{1}{2^2} - \frac{1}{1^2} \\
&= \sum_k \frac{1}{k^2} - \sum_k \frac{1}{(2k)^2} - \frac{3}{4} \\
&= \frac{3}{4}\left(\frac{\pi^2}{6}\right) - \frac{3}{4} < \frac{1}{2},
\end{aligned}$$

a densidade desejada é menor que 1, donde segue que existem infinitos i para os quais $(Pi + m, Pi + (m + c))$ são livres de quadrados. □

Exemplo 3.18. *Determine se existe uma constante C tal que, para todo n natural,*

$$F(n) = \frac{\varphi(d(n))}{d(\varphi(n))} \leq C.$$

SOLUÇÃO. Tomando a fatoração canônica de $n = \prod_i p_i^{\alpha_i}$, temos

$$F(n) = \frac{\varphi\left(\prod_i (\alpha_i + 1)\right)}{d\left(\prod_i (p_i - 1) p_i^{\alpha_i - 1}\right)}.$$

A fim de facilitar as contas, escreveremos $\alpha_i = q_i - 1$ e $c_i = v_{p_i}\Big(\prod_i (p_i - 1)\Big)$. Com uma conta simples concluímos que

$$F(n) \leq \frac{\varphi\Big(\prod_i q_i\Big)}{\prod_i q_i + c_i - 1} \leq \frac{\prod_i q_i}{\prod_i q_i + c_i - 1}.$$

Assim, caso $F(n)$ assuma valores aribitrariamente grandes (note que podemos controlar os $q_i's$ sem alterar os $c_i's$), devemos maximizar cada razão da forma $\frac{q}{q+c-1}$. Assim, quando $c = 0$, fazemos $q = 2$ e, para $c > 0$, fazemos q arbitrariamente grande. Assim, novamente para facilitar as contas, tomemos $p_1 < p_2 < \cdots$ a sequência de todos os números primos. Vamos tomar n de modo que os divisores primos de n são $p_1, p_2, \ldots, p_m$ para algum m, ou seja, $n = \prod_{i \leq m} p_i^{\alpha_i}$. Mantendo a notação anterior, concluímos que

$$F(n) = \frac{\varphi\Big(\prod_{i \leq m} q_i\Big)}{\prod_{i \leq m} q_i + c_i - 1}.$$

Note que, para $p > 3$ primo, todos os divisores de $p - 1$ são menores que $p/2$, dividiremos os primos $p_1, p_2, \ldots, p_m$ em duas partes: escreva $m = r + t$, com $p_r < N < p_{r+1}$ e $p_{r+t} \leq 2N$ para algum N. Então, é claro que $c_i = 0$ para todo $i > r$. Assim, tomemos $n = \prod_{i \leq r} p_i^{q-1} \prod_{r < i \leq r+t} p_i$ para algum q suficientemente grande (vamos supor que q é primo). Então,

$$\begin{aligned} F(n) &= \frac{\varphi(q^r \cdot 2^t)}{\prod_{i \leq r} \frac{q}{q + c_i - 1}} \\ &= 2^t \frac{q-1}{q} \prod_{i \leq r} \frac{q}{q + c_i - 1}. \end{aligned}$$

Como q é suficientemente grande (podemos fazer $q \to \infty$ sem alterar os c_i's), então, para cada m escolhido, podemos fazer $F(n)/2^t \to 1$. Logo, basta mostrar que t atinge valores suficientemente grandes. Mas isso já foi provado no exemplo 3.2. Portanto, $F(n)$ atinge valores suficientemente grandes e tal C não existe. □

Problemas Propostos

3.1. *Mostre que existem infinitos inteiros n tais que $n^2 + 1$ é livre de quadrados.*

3.2. *Mostre que*

$$\sum_{k \leq n} \varphi(k) = \frac{3n^2}{\pi^2} + O(n \log n).$$

3.3. *Mostre que a quantidade de primos entre n e $2n$ é menor do que $\frac{2n}{\log_2 n}$. Ainda mais, mostre que existe um $c > 0$ para o qual a quantidade de primos entre n e $2n$ é maior que $c\frac{n}{\log n}$.*

3.4. *Sejam $a_1, a_2, \ldots, a_t$ dígitos dados. Mostre que esses dígitos aparecem como uma sequência consecutiva de dígitos de infinitos primos.*

3.5. *Seja $f\colon \mathbb{N} \to \mathbb{R}^+$ uma função descrescente. Então,*

$$\sum_{p \text{ primo}} f(p)$$

diverge se, e somente se,

$$\sum_{n \geq 2} \frac{f(n)}{\log n}$$

diverge. Com isso, dê outra prova para a divergência de $\sum 1/p$.

3.6. *Encontre todos os inteiros positivos n tais que, se $mdc(n,k) = 1$, com $1 < k < n$, então k é primo.*

3.7. *Utilizando o Teorema dos Números Primos (ver 3.14), mostre que, dado $\epsilon > 0$, existe N tal que, para todo $n > N$, existe um primo entre n e $(1+\epsilon)n$.*

3.8. *Encontre todos os inteiros $n \geq 2$ tais que $\frac{\sigma(n)}{p(n)-1} = n$, onde $p(n)$ denota o maior divisor primo de n.*

3.9. *Seja n um inteiro positivo. Seja D_n o conjunto dos divisores de n e $f(n)$ o menor inteiro m tal que todos os elementos de D_n são distintos módulo m. Mostre que, para algum n, $f(n) \leq n^{\frac{1}{100}}$.*

3.10. *Seja S_n a soma dos n primeiros primos. Mostre que o intervalo $[S_n, S_{n+1}]$ contém algum quadrado perfeito.*

3.11. *Seja n um natural. Definimos $f(n)$ como*

$$f(n) = \frac{1}{n}\left(\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \ldots + \left\lfloor \frac{n}{n} \right\rfloor\right).$$

Mostre que $f(n+1) > f(n)$ para infinitos n e que $f(n+1) < f(n)$ para infinitos n.

Referências

1. Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro (você pode acessar uma versão virtual do livro aqui).

2. Dois problemas em Teoria dos Números: a irracionalidade de π e o Postulado de Bertrand (você pode acessar esse material aqui)

3. Modern Number Theory, de Aditya Khurmi