Primos gêmeos, primos de Sophie Germain e o Teorema de Brun

Carlos Gustavo Moreira (IMPA)
Fabio Enrique Brochero Martínez (UFMG)

Os números primos podem ser considerados os tijolos fundamentais da aritmética, e a estrutura do conjunto dos números primos tem inquietado gerações de matemáticos de todos os tempos. Depois de tantos anos de trabalho intenso de muitos matemáticos, a quantidade de problemas abertos e conjecturas sobre números primos é muito grande.

Uma de tais conjecturas versa sobre os chamados *primos gêmeos*; dois números primos p e q são chamados *primos gêmeos* se $|p-q| = 2$. Conjectura-se, mas não se sabe demonstrar até agora, que existem infinitos pares de primos gêmeos. Se esse for o caso, teremos $\liminf_{n\to\infty}(p_{n+1} - p_n) = 2$, em que p_n denota o n-ésimo primo. Por outro lado, são conhecidos pares de primos gêmeos bastante grandes, como $65516468355 \cdot 2^{333333} \pm 1$, que têm 100355 dígitos cada.

Em geral, sabe-se muito pouco sobre o comportamento da função $d_n = p_{n+1} - p_n$, como veremos a seguir. O Teorema dos Números Primos, provado independentemente por Jacques Hadamard e Charles-Jean de la Vallée Poussin, em 1896, equivale a dizer que

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1\,.$$

Isso mostra que, "em média", d_n é da ordem de $\log n$. A conjectura de que existem infinitos primos gêmeos equivale a dizer que $\liminf d_n = 2$. Mas não se sabe provar nem que $\liminf d_n < +\infty$. Por outro lado, definindo-se

$$L = \liminf \frac{d_n}{\log p_n}\,,$$

Erdős provou que $L < 1$ e Maier que $L \leq 0{,}248$. Apenas em 2005, D. A. Goldston, J. Pintz e C. Y. Yıldırım provaram que $L = 0$ (ver [4]). De fato eles provaram bem mais (ver [5]): dentre outros resultados, eles mostraram que

$$\liminf \frac{d_n}{\sqrt{\log p_n}(\log\log p_n)^2} < \infty\,.$$

Por outro lado, o matemático norueguês Viggo Brun inventou a teoria do crivo combinatório e provou, em 1917 (ver [2]), que primos gêmeos são escassos no seguinte sentido: se

$$\pi_2(x) = \#\{p \leq x \mid \ p \text{ e } p+2 \text{ são primos}\}$$

é o número de pares de primos gêmeos até x então existe uma constante $A > 0$ tal que

$$\pi_2(x) \leq A\left(\frac{x(\log\log x)^2}{(\log x)^2}\right)\,.$$

Em particular, isto implica que

$$\sum_{p \text{ primo gêmeo}} \frac{1}{p} < +\infty\,,$$

enquanto sabemos que a soma sobre todos os primos $\sum_{p \text{ primo}} \frac{1}{p}$ diverge (Teorema 7). Apresentar uma prova deste resultado, da forma mais elementar e autocontida possível, é um dos principais objetivos deste artigo.

Brun provou posteriormente, em [3], que

$$\pi_2(x) < \frac{100x}{(\log x)^2}$$

para x suficientemente grande. Acredita-se, mas não se sabe demonstrar, que $\pi_2(x)$ seja assintótico a $Cx/(\log x)^2$ para alguma constante positiva C. Deixamos como exercício provar a seguinte caracterização de

primos gêmeos devida a Clement: *Seja $n \geq 2$. Os inteiros n e $n+2$ são ambos primos se, e somente se,*

$$4((n-1)!+1)+n \equiv 0 \pmod{n(n+2)};$$

bem como a seguinte generalização para primos com diferença d: *se n e d são inteiros maiores que 1 com $\mathrm{mdc}(n,d!)=1$, tem-se que n e $n+d$ são primos se, e somente se,*

$$d!d((n-1)!+1)+n(d!-1) \equiv 0 \pmod{n(n+d)}.$$

Este último problema foi proposto pelo professor André Contiero, da Universidade Federal de Alagoas, para a II Competição Iberoamericana Interuniversitária de Matemática, realizada em 2010 no Rio de Janeiro.

Outra família interessante de números primos é formada pelos primos p para os quais $2p+1$ também é primo – os chamados *primos de Sophie Germain*. Este nome é usado porque a matemática francesa Sophie Germain provou o chamado primeiro caso do Último Teorema de Fermat para primos p desta forma. Devemos destacar que Andrew Wiles, em colaboração com seu então aluno Richard Taylor, mostrou, em 1994, um resultado sobre curvas elípticas que, como consequência, implica o Último Teorema de Fermat.

Proposição 1 (Sophie Germain)**.** *Se p e $2p+1$ são primos com $p > 2$, então não existem inteiros x,y,z com $\mathrm{mdc}(x,y,z)=1$ e $p \nmid xyz$ tais que $x^p+y^p+z^p=0$.*

Demonstração. Observe inicialmente que $2p+1 \mid xyz$: caso contrário, pelo Pequeno Teorema de Fermat, $x^{2p} \equiv 1 \pmod{2p+1}$, o que equivale a $(x^p-1)(x^p+1) \equiv 0 \pmod{2p+1}$. Assim, temos que $x^p \equiv \pm 1 \pmod{2p+1}$ e, analogamente, $y^p \equiv \pm 1 \pmod{2p+1}$ e $z^p \equiv \pm 1 \pmod{2p+1}$. Mas $x^p+y^p+z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{2p+1}$, um absurdo.

Por outro lado, temos

$$(-x)^p = (y+z)(y^{p-1}-y^{p-2}z+\cdots-yz^{p-2}+z^{p-1}).$$

Vamos mostrar que os dois fatores da direita são primos entre si. Se q é um primo que divide ambos os termos, então $y \equiv -z \pmod{q}$ e, portanto,

$$0 \equiv y^{p-1}-y^{p-2}z+\cdots+z^{p-1} \equiv py^{p-1} \pmod{q};$$

temos $q \neq p$ pois $q \mid x$, assim $q \mid py^{p-1} \implies q \mid y$, mas então $z \equiv -y \equiv 0 \pmod{q}$ e q dividiria simultaneamente x,y,z, contrariando a hipótese $\mathrm{mdc}(x,y,z)=1$. Assim, pela fatoração única em primos existem inteiros a,d tais que

$$a^p = y+z$$

e

$$d^p = y^{p-1}-y^{p-2}z+\cdots-yz^{p-2}+z^{p-1}.$$

Analogamente, existem b,c,e,f inteiros tais que

$$b^p = x+z\ ,\ e^p = x^{p-1}-x^{p-2}z+\cdots-xz^{p-2}+z^{p-1}$$
$$c^p = x+y\ ,\ f^p = x^{p-1}-x^{p-2}y+\cdots-xy^{p-2}+y^{p-1}$$

Como $2p+1 \mid xyz$, podemos supor sem perda de generalidade que $2p+1 \mid x$. Assim, de $2x = b^p+c^p-a^p$, temos que $2p+1 \mid b^p+c^p-a^p$ e o mesmo argumento no início da demonstração mostra que $2p+1 \mid abc$ também. Mas se $2p+1 \mid b = x+z$ ou $2p+1 \mid c = x+y$, como $2p+1 \mid x$ e $x^p+y^p+z^p = 0$ teríamos que $2p+1 \mid \mathrm{mdc}(x,y,z)=1$, um absurdo. Por outro lado, temos $f^p \equiv y^{p-1} \pmod{2p+1}$ e, se $2p+1 \mid a$, então $2p+1 \nmid d$ e $y \equiv -z \pmod{2p+1} \implies d^p \equiv py^{p-1} \pmod{2p+1}$. Assim, $2p+1 \mid f$, pois caso contrário teríamos $\pm p \equiv pf^p \equiv py^{p-1} \equiv d^p \equiv \pm 1 \pmod{2p+1}$, um absurdo. Mas neste caso, $2p+1 \mid z$ também, o que é impossível já que $\mathrm{mdc}(x,y,z)=1$, completando a prova. □

Podemos mencionar também o seguinte resultado, que relaciona primos de Sophie Germain com números de Mersenne, que são números da forma $M_p = 2^p-1$. Os 9 maiores primos conhecidos no momento são números de Mersenne, sendo o maior deles $M_{43112609} = 2^{43112609}-1$. Não é difícil mostrar que, se M_p é primo então p também é primo. A recíproca, no entanto, não vale, e o resultado abaixo permite exibir exemplos de primos p bastante grandes para os quais M_p é composto.

Proposição 2. *Seja p primo, $p \equiv 3 \pmod{4}$. Então $2p+1$ é primo (i.e. p é primo de Sophie Germain) se, e somente se, $2p+1$ divide M_p.*

Deixamos a prova como exercício para o leitor.

Alguns primos de Sophie Germain bastante grandes são conhecidos, como $183027 \cdot 2^{265440} - 1$, que tem 79911 dígitos. Sabe-se também que se $\pi_{\mathrm{SG}}(x)$ denota o número de primos de Sophie Germain menores do que x então existe C tal que

$$\pi_{\mathrm{SG}}(x) < C\frac{x}{(\log x)^2}$$

para todo x. Acredita-se que $\pi_{\mathrm{SG}}(x)$ seja assintótico a $cx/(\log x)^2$ para algum $c > 0$, mas não se sabe demonstrar sequer que existem infinitos primos de Sophie Germain.

Na atualidade os primos de Sophie Germain têm utilidade prática nos métodos de criptografia pública RSA e ElGamal. Neste último método a chave pública consiste de três elementos (q, g, h), em que q é um primo muito grande, g é um número tal que $1 < g < q-1$ e é raiz primitiva módulo q (i.e., a ordem de g módulo q é $q-1$), e $h \equiv g^x \pmod{q}$, em que x é a chave privada. Para codificar uma mensagem M, o emissor escolhe um número $y \gg 0$ e transmite (a, b), em que $a \equiv g^y \pmod{q}$ e $b \equiv h^y M \pmod{q}$. Observemos que, para decodificar, basta calcular

$$a^{-x}b \equiv (g^y)^{-x}h^y M \equiv g^{-xy}(g^x)^y M \equiv M \pmod{q}.$$

Assim, é possível quebrar a codificação calculando x, isto é, calculando o chamado logaritmo discreto de h com respeito a g módulo q. No momento são conhecidos métodos para calcular o logaritmo discreto "facilmente" quando os fatores primos de $q-1$ são pequenos.

De fato, se $q - 1 = r_1^{\alpha_1} \cdots r_l^{\alpha_l}$ é sua fatoração prima, definimos $g_i = g^{(q-1)/r_i^{\alpha_i}}$ e $h_i = h^{(q-1)/r_i^{\alpha_i}}$, e temos que a ordem de g_i módulo q é $r_i^{\alpha_i}$ e $g_i^x = h_i \pmod{q}$. Assim, se encontramos x_i tais que $g_i^{x_i} \equiv h_i \pmod{q}$ temos que $x \equiv x_i \pmod{r_i^{\alpha_i}}$, e portanto x pode ser calculado usando-se o Teorema Chinês dos Restos. Agora observemos que para solucionar a congruência $g^x \equiv h \pmod{q}$ quando a ordem de g é r^k, do algoritmo da divisão temos que encontrar $0 \le b < r$ e $0 \le a < r^{k-1}$ tais que $x = ar + b$. Mas como

$$h^{r^{k-1}} \equiv (g^{r^{k-1}})^x \equiv g^{ar^k + br^{k-1}} \equiv (g^{r^{k-1}})^b \pmod{q},$$

temos que b é a solução do problema $u_1 \equiv v_1^b \pmod{q}$, em que $u_1 = h^{r^{k-1}}$ e $v_1 = g^{r^{k-1}}$ tem ordem r e a é a solução do problema $hg^{-b} \equiv (g^r)^a \pmod{q}$, em que g^r tem ordem r^{k-1}. Podemos então calcular a indutivamente e, portanto, a complexidade para calcular o logaritmo discreto depende do tamanho do maior primo que divide $q-1$ e linearmente da potência ao qual tal primo está elevado.

No caso em que q é tal que $\frac{q-1}{2} = p$ é primo, isto é, quando p é um primo de Sophie Germain, dizemos que q é um primo seguro. De fato, nesse caso a tarefa de tentar encontrar x dados q, g e h fica bastante dificultada.

Em geral, dados a, b, c números inteiros positivos, primos relativos dois a dois e com exatamente um de tais números par, denotamos por $\pi_{a,b,c}(x)$ a quantidade de pares de números primos (p, q) que satisfazem a condição $aq - bp = c$ com $p \le x$. G. H. Hardy e J. E. Littlewood conjecturaram, em [6], a seguinte estimativa assintótica para $\pi_{a,b,c}(x)$.

Conjectura 3 (Hardy, Littlewood)**.**

$$\pi_{a,b,c}(x) \sim \frac{2C}{a}\frac{x}{(\log x)^2} \prod_{\substack{p \mid abc \\ p \text{ primo} > 2}} \left(\frac{p-1}{p-2}\right),$$

em que $C = \prod_{\substack{p \text{ primo} \\ p>2}} \left(1 - \frac{1}{(p-1)^2}\right)$.

Em particular, se $a = 1$, $b = 1$ e $c = 2$ temos que $\pi_{1,1,2} = \pi_2$, e se $a = 1$, $b = 2$ e $c = 1$ temos que $\pi_{1,2,1}(x)$ é o número de primos de Sophie Germain menores do que ou iguais a x.

Alguns fatos e estimativas sobre primos

Um fato importante sobre números primos é que a série de seus inversos diverge, isto é,

$$\sum_{p \text{ primo}} \frac{1}{p} = +\infty.$$

Um interessante argumento devido a Erdös dá uma prova deste fato: supondo que $\sum_{p \text{ primo}} \frac{1}{p} < +\infty$, existe $N \in \mathbb{N}$ tal que

$$\sum_{\substack{p \text{ primo} \\ p \ge N}} \frac{1}{p} < \frac{1}{2}.$$

Vamos considerar a decomposição $\mathbb{N} = A \cup B$ em que

$$A = \{n \in \mathbb{N} \mid \text{todos os fatores primos de } n \text{ são menores que } N\}$$

e $B = \mathbb{N} \setminus A$. Sejam $p_1, p_2, \ldots, p_k$ todos os primos menores que N. Fixemos $M \in \mathbb{N}$. Se $n \in A$ e $n \leq M$, então n se fatora como $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, em que $\alpha_j \leq \frac{\log M}{\log 2}$, $\forall j \leq k$. Assim, $|A \cap [1, M]| \leq (1 + \frac{\log M}{\log 2})^k$. Por outro lado, todo elemento de B tem um fator primo maior ou igual a N e, portanto,

$$|B \cap [1, M]| \leq \sum_{\substack{p \text{ primo} \\ p \geq N}} \left\lfloor \frac{M}{p} \right\rfloor \leq M \sum_{\substack{p \text{ primo} \\ p \geq N}} \frac{1}{p} < \frac{M}{2}\,.$$

Como $M = |\mathbb{N} \cap [1, M]| = |A \cap [1, M]| + |B \cap [1, M]| < \left(1 + \frac{\log M}{\log 2}\right)^k + \frac{M}{2}$, temos $\frac{M}{2} < \left(1 + \frac{\log M}{\log 2}\right)^k$ para todo $M \in \mathbb{N}$, o que é absurdo, pois

$$\lim_{M \to +\infty} \frac{1}{M} \left(1 + \frac{\log M}{\log 2}\right)^k = 0\,.$$

Agora, mostremos algumas estimativas sobre números primos.

Proposição 4 (Chebyshev)**.** *Seja $\pi(x)$ a quantidade de primos menores do que ou iguais a x. Existe uma constante positiva C tal que*

$$\pi(x) < C \frac{x}{\log x}$$

para todo $x \geq 2$.

Demonstração. Observemos inicialmente que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é múltiplo de todos os primos p que satisfazem $n < p \leq 2n$. Como

$$\binom{2n}{n} < \sum_{0 \leq k \leq 2n} \binom{2n}{k} = 2^{2n}\,,$$

segue que o produto dos primos entre n e $2n$ é menor do que 2^{2n}. Como há $\pi(2n) - \pi(n)$ primos como esses, segue que $n^{\pi(2n) - \pi(n)} < 2^{2n}$ (pois todos esses primos são maiores que n), donde $(\pi(2n) - \pi(n)) \log n < 2n \log 2$ e

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

Isso implica facilmente, por indução, que

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

(começando com $k = 5$; até $k = 5$ segue de $\pi(n) \leq n/2$ para $n \geq 4$). Daí segue que se $2^k < x \leq 2^{k+1}$ então

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

pois $f(x) = \frac{x}{\log x}$ é uma função crescente para $x \geq 3$. □

Proposição 5 (Fatores do Fatorial)**.** *Seja p um primo. Então a maior potência de p que divide $n!$ é p^α, em que*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Observe que a soma acima é finita, pois os termos $\lfloor \frac{n}{p^i} \rfloor$ são nulos para i grande.

Demonstração. No produto $n! = 1 \cdot 2 \cdot \ldots \cdot n$, apenas os múltiplos de p contribuem com um fator p. Há $\lfloor \frac{n}{p} \rfloor$ tais múltiplos entre 1 e n. Destes, os que são múltiplos de p^2 contribuem com um fator p extra e há $\lfloor \frac{n}{p^2} \rfloor$ tais fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p e assim por diante, resultando na fórmula acima. □

Proposição 6.

$$\sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{\log p}{p} = \log n + O(1)\,.$$

Demonstração. Pela Proposição 5, temos

$$n! = \prod_{\substack{p \text{ primo} \\ p \leq n}} p^{v_p}\,, \quad \text{em que} \quad v_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor\,.$$

Tomando logaritmos, temos

$$\sum_{k=1}^{n} \log k = \sum_{\substack{p \text{ primo} \\ p \leq n}} v_p \log p$$

e, como

$$\frac{n}{p} - 1 < \left\lfloor \frac{n}{p} \right\rfloor \leq v_p < \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1}\,,$$

segue que

$$\sum_{\substack{p \text{ primo} \\ p \leq n}} \left(\frac{n}{p} - 1\right) \log p \leq \sum_{k=1}^{n} \log k \leq \sum_{\substack{p \text{ primo} \\ p \leq n}} \frac{n}{p-1} \log p\,.$$

Ou seja,

$$\frac{1}{n}\sum_{k=1}^{n}\log k - \sum_{\substack{p \text{ primo}\\ p\le n}}\frac{\log p}{p}$$

está entre

$$-\frac{1}{n}\sum_{\substack{p \text{ primo}\\ p\le n}}\log p$$

e

$$\sum_{\substack{p \text{ primo}\\ p\le n}}\frac{\log p}{p(p-1)}\,.$$

Como

$$\frac{1}{n}\sum_{\substack{p \text{ primo}\\ p\le n}}\log p \le \frac{1}{n}\pi(n)\log n\,,$$

então esse termo, pela Proposição 4, é $O(1)$. Por outro lado,

$$\sum_{\substack{p \text{ primo}\\ p\le n}}\frac{\log p}{p(p-1)} \le \sum_{k\ge 1}\frac{1}{k^{\frac{3}{2}}} = O(1)\,.$$

O resultado segue, pois $\frac{1}{n}\sum_{k=1}^{n}\log k = \log n + O(1)$. □

A proposição anterior nos permite estimar a ordem de crescimento da soma dos inversos dos primos.

Teorema 7.

$$\sum_{\substack{p \text{ primo}\\ p\le n}}\frac{1}{p} = \log\log n + O(1)\,.$$

Demonstração. Defina

$$a_k = \begin{cases} \frac{\log k}{k} & \text{se } k \text{ é primo}\\ 0 & \text{caso contrário}\end{cases}$$

e $S_n = \sum_{k=1}^{n} a_k$. Pela proposição anterior, temos que

$$S_k = \sum_{\substack{p \text{ primo}\\ p\le k}}\frac{\log p}{p} = \log k + O(1)\,.$$

Assim, por "integração por partes" discreta, temos

$$\begin{aligned}\sum_{\substack{p \text{ primo}\\ p\le n}}\frac{1}{p} &= \sum_{k=2}^{n}\frac{a_k}{\log k} = \sum_{k=2}^{n}\frac{S_k - S_{k-1}}{\log k}\\ &= \sum_{k=2}^{n} S_k\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + \frac{S_n}{\log(n+1)}\\ &= \sum_{k=2}^{n}\log k\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + O(1)\\ &= \sum_{k=2}^{n}\frac{\log(k+1)-\log k}{\log(k+1)} + O(1)\\ &= \sum_{k=2}^{n}\frac{1}{(k+1)\log(k+1)} + O(1)\,,\end{aligned}$$

em que a última igualdade segue do fato de que

$$\frac{1}{k+1} \le \int_k^{k+1}\frac{dx}{x} \le \frac{1}{k}$$

implica

$$\frac{1}{(k+1)\log(k+1)} \le \frac{\log(k+1)-\log k}{\log(k+1)} \le \frac{1}{k\log(k+1)}$$

e

$$\begin{aligned}\Big|\sum_{k=2}^{n}\frac{1}{k\log(k+1)} - \sum_{k=2}^{n}\frac{1}{(k+1)\log(k+1)}\Big|&\\ \le \sum_{k=2}^{n}\left(\frac{1}{k} - \frac{1}{k+1}\right) = O(1)\,.&\end{aligned}$$

O resultado é consequência do lema anterior, já que $\sum_{k=2}^{n}\frac{1}{k\log k} = \log\log n + O(1)$. □

Veremos a seguir algumas ferramentas que serão úteis para a prova do Teorema de Brun.

Funções multiplicativas e a função de Möbius

Uma função f definida sobre $\mathbb{N}_{>0}$ é dita *multiplicativa* se dados dois números naturais a e b tais que $\text{mdc}(a,b) = 1$ então $f(ab) = f(a)f(b)$. Algumas funções multiplicativas importantes são

$$d(n) \stackrel{\text{def}}{=} \text{número de divisores de } n$$

e

$$\sigma(n) \stackrel{\text{def}}{=} \text{soma dos divisores de } n\,.$$

Deixamos para o leitor mostrar o fato mais geral de que para todo número real k a função

$$\sigma_k(n) \stackrel{\text{def}}{=} \sum_{d|n} d^k$$

é multiplicativa. Assim, em particular, $d(n) = \sigma_0(n)$ e $\sigma(n) = \sigma_1(n)$ são multiplicativas.

O seguinte teorema nos mostra uma forma de construir funções multiplicativas.

Teorema 8. *Se f é uma função multiplicativa então a função*

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

é também multiplicativa.

Demonstração. Sejam a e b inteiros tais que $\mathrm{mdc}(a,b) = 1$. Então

$$\begin{aligned} F(ab) &= \sum_{d|ab} f(d) = \sum_{d_1|a, d_2|b} f(d_1 d_2) \\ &= \sum_{d_1|a, d_2|b} f(d_1) f(d_2) = \sum_{d_1|a} \sum_{d_2|b} f(d_1) f(d_2) \\ &= \sum_{d_1|a} f(d_1) \sum_{d_2|b} f(d_2) = F(a)F(b)\,. \end{aligned}$$

Segue que F também é multiplicativa. □

Definimos a *função de Möbius* $\mu\colon \mathbb{N}_{>0} \to \mathbb{Z}$ por

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

Facilmente se comprova que a função de Möbius é multiplicativa. Além disso, vale o seguinte lema.

Lema 9. *Para todo inteiro positivo n temos*

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

Demonstração. No caso $n = 1$ não temos nada para provar. Como a função $\sum_{d|n} \mu(d)$ é multiplicativa, pelo Teorema 8, basta mostra o lema para $n = p^k$, em que p é um número primo. De fato,

$$\sum_{d|p^k} \mu(d) = \sum_{j=0}^{k} \mu(p^j) = 1 - 1 = 0\,,$$

como queríamos demonstrar. □

Teorema 10 (Fórmula de inversão de Möbius)**.** *Seja $f(n)$ uma função multiplicativa e $F(n) = \sum_{d|n} f(d)$. Então, para todo inteiro positivo n,*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)\,.$$

Demonstração.

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d_1|\frac{n}{d}} f(d_1) \\ &= \sum_{d|n} \sum_{d_1|\frac{n}{d}} \mu(d) f(d_1) = \sum_{d_1|n} \sum_{d|\frac{n}{d_1}} \mu(d) f(d_1) \\ &= \sum_{d_1|n} f(d_1) \sum_{d|\frac{n}{d_1}} \mu(d) = f(n)\mu(1) = f(n)\,. \end{aligned}$$

□

Primos gêmeos e primos de Sophie Germain

Nesta seção, provaremos o teorema de Brun, segundo o qual a série dos inversos dos primos gêmeos converge. Pelo mesmo argumento se prova que a soma dos inversos dos primos de Sophie Germain converge, o que mostra que os primos gêmeos, assim como os primos de Sophie Germain, são bem mais raros que os primos.

Antes de enunciar a proposição fundamental desta seção, precisamos dos seguintes lemas.

Lema 11. *Sejam m e l números naturais com $l \geq 1$. Então*

$$\sum_{\substack{d|m \\ \omega(d) \leq 2l-1}} \mu(d) \leq \sum_{d|m} \mu(d) \leq \sum_{\substack{d|m \\ \omega(d) \leq 2l}} \mu(d)\,,$$

em que $\omega(d)$ denota o número de fatores primos distintos de d.

Demonstração. Se $m = 1$, os três termos são iguais a 1. Se $m > 1$, o termo do meio é igual a 0, pelo Lema 9. Agora seja $k = \omega(m)$. Como $\mu(d) \neq 0$ implica que d é produto de primos distintos, então para todo s temos que

$$\sum_{\substack{d|m \\ \omega(d) \leq s}} \mu(d) = \sum_{j=0}^{s} \sum_{\substack{d|m \\ \omega(d) = j}} \mu(d) = \sum_{j=0}^{s} \binom{k}{j} (-1)^j\,,$$

pois se d é produto de j primos distintos então $\mu(d) = (-1)^j$ e existem $\binom{k}{j}$ produtos de j primos distintos que dividem m. Por outro lado,

$$\begin{aligned} \sum_{j=0}^{s} \binom{k}{j} (-1)^j &= 1 + \sum_{j=1}^{s} \left[\binom{k-1}{j} + \binom{k-1}{j-1} \right] (-1)^j \\ &= (-1)^s \binom{k-1}{s}\,. \end{aligned}$$

Em particular, se s é par então $\sum_{j=0}^{s} \binom{k}{j} (-1)^j \geq 0$ e se s é ímpar então $\sum_{j=0}^{s} \binom{k}{j} (-1)^j \leq 0$, como queríamos demonstrar. □

Lema 12. *Sejam m um produto de primos distintos e b, c inteiros primos entre si. O número de soluções de $x(bx + c) \equiv 0 \pmod{m}$ contadas módulo m é*

$$f_{bc}(m) \stackrel{\text{def}}{=} \frac{d(m)}{d(\mathrm{mdc}(m, bc))} = 2^{\omega(m) - \omega(\mathrm{mdc}(m,bc))}\,,$$

em que $d(n)$ e $\omega(n)$ denotam o número de divisores de n e o número de fatores primos distintos de n, respectivamente.

Demonstração. Note que toda solução de $x(bx+c) \equiv 0 \pmod{m}$ é solução do sistema de congruências

$$\begin{aligned} x &\equiv \quad 0 \pmod{r} \\ bx &\equiv -c \pmod{\tfrac{m}{r}} \end{aligned}$$

para algum $r \mid m$. Por outro lado, para cada $r \mid m$, temos que $\operatorname{mdc}(r, \frac{m}{r}) = 1$ pois m é um produto de primos distintos. Assim, pelo Teorema Chinês dos Restos, o sistema acima possui uma única solução x_r módulo m, se $\operatorname{mdc}(b, \frac{m}{r}) = 1 \iff \operatorname{mdc}(m,b) \mid r$, ou nenhuma, caso contrário, uma vez que $\operatorname{mdc}(b,c) = 1$. Assim, devemos contar o número de soluções x_r distintas módulo m quando r percorre os divisores de m tais que $\operatorname{mdc}(m,b) \mid r$.

Sejam r e s dois divisores de m que são múltiplos de $\operatorname{mdc}(m,b)$ e suponha $x_s \equiv x_r \pmod{m}$. Temos que $t = \frac{\operatorname{mmc}(r,s)}{\operatorname{mdc}(r,s)}$ (a "diferença simétrica" dos primos que dividem r e s) divide simultaneamente x_s e $bx_s + c$, logo $t \mid c$ e, como $r, s \mid m$, temos que $t \mid \operatorname{mdc}(c,m)$. Reciprocamente, dado r como antes e um divisor t de $\operatorname{mdc}(m,c)$, podemos definir $s = \frac{\operatorname{mmc}(r,t)}{\operatorname{mdc}(r,t)}$, de modo que $\operatorname{mdc}(m,b) \mid s \mid m$; a solução correspondente x_s é tal que $x_s \equiv x_r \pmod{p}$ para todo primo $p \mid m$, ou seja, temos $x_s \equiv x_r \pmod{m}$. Assim, utilizando a multiplicatividade de $d(n)$, temos que o número de soluções é

$$\begin{aligned} \frac{d(m/\operatorname{mdc}(m,b))}{d(\operatorname{mdc}(m,c))} &= \frac{d(m)}{d(\operatorname{mdc}(m,bc))} \\ &= \frac{2^{\omega(m)}}{2^{\omega(\operatorname{mdc}(m,bc))}} = 2^{\omega(m)-\omega(\operatorname{mdc}(m,bc))}\,. \end{aligned}$$

□

A seguinte proposição é baseada na exposição de Y. Motohashi ([7]) sobre o chamado *método do crivo*. Ela implica que $\pi_2(x) = O\big(x(\frac{\log\log x}{\log x})^2\big)$. Como dissemos na introdução, Brun provou um resultado mais forte para primos gêmeos, isto é, $\pi_2(x) = O\big(\frac{x}{(\log x)^2}\big)$. No entanto, esta proposição tem uma prova mais simples e já é suficiente para garantir que a série dos inversos dos primos gêmeos converge, como veremos no final desta seção.

Proposição 13. *Sejam a, b, c inteiros positivos, primos relativos dois a dois e com exatamente um deles par. Então*

$$\pi_{a,b,c}(x) = O\Big(x\Big(\frac{\log\log x}{\log x}\Big)^2\Big)\,.$$

Demonstração. Seja $z \le \sqrt{x/b}$, defina $P_a(z)$ como o produto dos primos menores do que ou iguais a z que não dividem a e, ainda,

$$A \stackrel{\text{def}}{=} \{k(bk+c) \mid 1 \le k \le x\}\,.$$

Observemos que se $y = k(bk+c) \in A$ com k e $\frac{bk+c}{a}$ primos e $k > \frac{a}{b}z$, então $\frac{bk+c}{a} > \frac{b}{a}k > z$ e, portanto, $\operatorname{mdc}(y, P_a(z)) = 1$. Assim, temos que

$$\begin{aligned} \pi_{a,b,c}(x) &\le \#\{y \in A \mid \operatorname{mdc}(y, P_a(z)) = 1\} + \pi_{a,b,c}(\frac{a}{b}z) \\ &< \#\{y \in A \mid \operatorname{mdc}(y, P_a(z)) = 1\} + \frac{a}{b}z\,. \end{aligned}$$

De fato, esta última parcela $z \le \frac{a}{b}\sqrt{\frac{x}{b}}$ não afeta nossa estimativa, logo basta limitar o tamanho da primeira parcela. Para isso, observemos que, pelos Lemas 9 e 11, temos, para todo $l \ge 1$,

$$\begin{aligned} \#\{y \in A \mid \operatorname{mdc}(y, P_a(z)) = 1\} &= \sum_{y \in A} \sum_{m \mid \operatorname{mdc}(y, P_a(z))} \mu(m) \\ &\le \sum_{y \in A} \sum_{\substack{m \mid \operatorname{mdc}(y, P_a(z)) \\ \omega(m) \le 2l}} \mu(m) \\ &= \sum_{\substack{m \mid P_a(z) \\ \omega(m) \le 2l}} \mu(m) |A_m|\,, \end{aligned}$$

em que $A_m \stackrel{\text{def}}{=} \{y \in A \mid m \text{ divide } y\}$. Mas, do Lema 12, segue que

$$\Big|A_m - \frac{x}{m} f_{bc}(m)\Big| < f_{bc}(m)\,,$$

pois de cada conjunto de m inteiros consecutivos k, exatamente $f_{bc}(m)$ deles são tais que $m \mid k(bk+c)$. Assim

$$\begin{aligned} &\#\{y \in A \mid \operatorname{mdc}(y, P_a(z)) = 1\} \\ &\quad \le x \sum_{\substack{m \mid P_a(z) \\ \omega(m) \le 2l}} \frac{\mu(m) f_{bc}(m)}{m} + O\Big(\sum_{\substack{m \mid P_a(z) \\ \omega(m) \le 2l}} f_{bc}(m)\Big)\,. \end{aligned}$$

Como $m \mid P_a(z)$ e $\omega(m) \le 2l$ implica que m é produto de no máximo $2l$ primos distintos menores ou iguais a z, segue que $m \le z^{2l}$ e o último somando pode ser limitado como

$$\begin{aligned} \sum_{\substack{m \mid P_a(z) \\ \omega(m) \le 2l}} f_{bc}(m) &\le \sum_{1 \le r \le z^{2l}} d(r) = \sum_{1 \le r \le z^{2l}} \sum_{d \mid r} 1 \\ &= \sum_{d=1}^{z^{2l}} \Big\lfloor \frac{z^{2l}}{d} \Big\rfloor \le z^{2l} \sum_{d=1}^{z^{2l}} \frac{1}{d} \\ &= O(z^{2l} \log(z^{2l}))\,. \end{aligned}$$

Portanto, o propósito é escolher z e l adequados, de tal forma que o termo limitado por $z^{2l}\log(z^{2l})$ seja pequeno comparado com o outro. Tal escolha será feita mais para frente e dependerá também da limitação do somando principal

$$\sum_{\substack{m|P_a(z)\\ \omega(m)\le 2l}} \frac{\mu(m)f_{bc}(m)}{m} = \sum_{m|P_a(z)} \frac{\mu(m)f_{bc}(m)}{m} - \sum_{\substack{m|P_a(z)\\ \omega(m)\ge 2l+1}} \frac{\mu(m)f_{bc}(m)}{m}.$$

Assim, temos que dar valores a z e l de tal forma que cada um destes termos seja dominado por $O\big((\frac{\log\log x}{\log x})^2\big)$.

Para isto, observemos que a função $\frac{\mu(n)f_{bc}(n)}{n}$ é multiplicativa e, assim, $\sum_{m|n} \frac{\mu(m)f_{bc}(m)}{m}$ também é multiplicativa (Teorema 8). Logo podemos utilizar o Teorema 7, de onde temos que

$$\begin{aligned}
\sum_{m|P_a(z)} \frac{\mu(m)f_{bc}(m)}{m} &= \prod_{\substack{q \text{ primo}\\ q|P_a(z)}} \left(1+\frac{\mu(q)f_{bc}(q)}{q}\right)\\
&= A\prod_{\substack{q \text{ primo}\\ 3\le q\le z}} \left(1-\frac{2}{q}\right)\\
&= A\exp\left(\sum_{\substack{q \text{ primo}\\ 3\le q\le z}} \log\left(1-\frac{2}{q}\right)\right)\\
&= \exp\left(O(1)-2\sum_{\substack{q \text{ primo}\\ q\le z}} \frac{1}{q}\right)\\
&= \exp\left(O(1)-2\log\log z\right)\\
&= O\big((\log z)^{-2}\big),
\end{aligned}$$

em que

$$A = \begin{cases} \frac{1}{2}\displaystyle\prod_{\substack{q \text{ primo}\\ 3\le q\le z, q|bc}} \left(1-\frac{1}{q}\right)\left(1-\frac{2}{q}\right)^{-1} & \text{se } A \text{ é ímpar}\\ \displaystyle\prod_{\substack{q \text{ primo}\\ 3\le q\le z, q|bc}} \left(1-\frac{1}{q}\right)\left(1-\frac{2}{q}\right)^{-1} & \text{se } A \text{ é par.}\end{cases}$$

Para estimar o termo restante, observe que $\omega(m)\ge 2l+1$ implica $f_{bc}(m)\ge \frac{2^{2l+1}}{bc}$, donde $f_{bc}(m)\le \frac{bc}{2}2^{-2l}f_{bc}(m)^2$. Assim,

$$\left|\sum_{\substack{m|P_a(z)\\ \omega(m)\ge 2l+1}} \frac{\mu(m)f_{bc}(m)}{m}\right| \le \frac{bc}{2}2^{-2l}\sum_{m|P_a(z)} \frac{(f_{bc}(m))^2}{m}.$$

Como $\frac{(f_{bc}(n))^2}{n}$ é multiplicativa, segue que $\sum_{m|n} \frac{(f_{bc}(n))^2}{n}$ é multiplicativa e, portanto,

$$\begin{aligned}
\sum_{m|P_a(z)} \frac{(f_{bc}(m))^2}{m} &= \prod_{\substack{q \text{ primo}\\ q|P_a(z)}} \left(1+\frac{(f_{bc}(q))^2}{q}\right)\\
&= B\prod_{\substack{q \text{ primo}\\ 3\le q\le z}} \left(1+\frac{4}{q}\right)\\
&= B\exp\left(\sum_{\substack{q \text{ primo}\\ 3\le q\le z}} \log\left(1+\frac{4}{q}\right)\right)\\
&= \exp\left(O(1)+4\sum_{\substack{q \text{ primo}\\ q\le z}} \frac{1}{q}\right)\\
&= \exp\left(O(1)+4\log\log z\right)\\
&= O(\log^4 z),
\end{aligned}$$

em que

$$B = \begin{cases} \frac{3}{2}\displaystyle\prod_{\substack{q \text{ primo}\\ 3\le q\le z, q|bc}} \left(1+\frac{1}{q}\right)\left(1+\frac{4}{q}\right)^{-1} & \text{se } a \text{ é ímpar}\\ \displaystyle\prod_{\substack{q \text{ primo}\\ 3\le q\le z, q|bc}} \left(1+\frac{1}{q}\right)\left(1+\frac{4}{q}\right)^{-1} & \text{se } a \text{ é par.}\end{cases}$$

Desta forma obtemos

$$\#\{y\in A \mid \mathrm{mdc}(y,P_a(z))=1\} = O(x(\log z)^{-2}) + O(x2^{-2l}\log^4 z) + O(z^{2l}\log(z^{2l})).$$

Precisamos escolher z e l de tal forma que a ordem de grandeza dos somandos à direita sejam simultaneamente "pequenos". De fato, fazendo

$$z=\exp\Big(\frac{\log x}{20\log\log x}\Big) \text{ e } l=\left\lfloor\frac{\log x}{4\log z}\right\rfloor = \lfloor 5\log\log x\rfloor,$$

temos que

$$z^{2l}\log(z^{2l}) = O(\sqrt{x}\log x),$$
$$x(\log z)^{-2} = O\left(x\left(\frac{\log\log x}{\log x}\right)^2\right)$$

e

$$\begin{aligned}
O(x2^{-2l}\log^4 z) &= O(x\exp(-10\log 2\log\log x)\cdot\log^4 z)\\
&= O\left(x\log^{-6}x\cdot\left(\frac{\log x}{\log\log x}\right)^4\right)\\
&= O\left(\frac{x}{(\log\log x)^4\log^2 x}\right),
\end{aligned}$$

pois $10\log 2 > 6$. Isto completa a prova, pois as funções $\sqrt{x}\log x$ e $\frac{x}{(\log\log x)^4\log^2 x}$ são dominadas pela função $x\left(\frac{\log\log x}{\log x}\right)^2$. □

Corolário 14. *A soma* $\sum_{p,p+2 \text{ primos}} \frac{1}{p} = \frac{1}{3}+\frac{1}{5}+\frac{1}{11}+\frac{1}{17}+\frac{1}{29}+\cdots$ *é convergente.*

Demonstração. Do fato que no intervalo $[2^{n-1},2^n]$ o menor primo é maior que 2^{n-1} e o número de primos gêmeos nesse intervalo é menor que $\pi_2(2^n)$, segue que

$$\begin{aligned}\sum_{p,p+2 \text{ primos}} \frac{1}{p} &= \sum_{n=1}^{\infty} \sum_{\substack{p,p+2 \text{ primos} \\ 2^{n-1}\le p<2^n}} \frac{1}{p} \\ &\le \sum_{n=1}^{\infty} \frac{\pi_2(2^n)}{2^{n-1}} \\ &= O\left(\sum_{n=1}^{\infty} \frac{2^n(\frac{\log n}{n})^2}{2^{n+1}}\right) \\ &= O\left(\sum_{n=1}^{\infty}\left(\frac{\log n}{n}\right)^2\right),\end{aligned}$$

que claramente é finito, já que esta última soma é dominada por $\sum_{n=1}^{\infty}\frac{1}{n^\alpha}$ para todo α com $1<\alpha<2$. □

Convidamos o leitor a modificar a prova do teorema para provar o seguinte resultado.

Teorema 15. *Seja* $\Phi(x,y) = \#\{n \le x \mid$ *todo divisor primo de* n *é maior do que* $y\}$. *Se* $y \le \exp(\log x/10\log\log x)$ *então*

$$\Phi(x,y) = O\left(\frac{x}{\log y}\right).$$

Referências

[1] Brochero Martínez, F. E.; Moreira, C. G.; Saldanha, N. C.; Tengan, E. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro.* Rio de Janeiro: IMPA, 2010. (Projeto Euclides)

[2] Brun, V. La série $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\ldots$ où les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie. *Bulletin des Sciences Mathématiques (2)*, v. 43, p. 100–104, 124–128, 1919.

[3] Brun, V. *Le crible d'Eratosthène et le théorème de Goldbach*. Kristiania: En Comisión chez J. Dybwad, 1920. 36 p. (Videnskapsselskapets Skrifter 1, Mathematisk-Naturvidenskabelig Klasse, n. 3)

[4] Goldston, D. A.; Pintz, J.; Yildirim, C. Y. Primes in tuples I. *Annals of Mathematics (2)*, v. 170, n. 2, p. 819–862, 2009. Disponível também em arxiv.org/abs/math/0508185.

[5] Goldston, D. A.; Pintz, J.; Yildirim, C. Y. Primes in tuples II. *Acta Mathematica*, v. 204, n. 1, p. 1–47, 2010. Disponível também em arxiv.org/abs/0710.2728.

[6] Hardy, G. H.; Littlewood, J. E. Some problems of 'partitio numerorum'; III: on the expression of a number as a sum of primes. *Acta Mathematica*, v. 44, n. 1, p. 1–70, 1923.

[7] Motohashi, Y. An overview of the sieve method and its history. *Sugaku Expositions*, v. 21, p. 1–32, 2008. Disponível também em arxiv.org/abs/math/0505521.

Carlos Gustavo Moreira
gugu@impa.br

Fabio Enrique Brochero Martínez
fbrocher@mat.ufmg.br