

TÉCNICA

Um Passeio com Primos e Outros Caras Bacanas

Rafael Filipe dos Santos

Introdução

A infinitude dos números primos é um fato conhecido desde a Antiguidade, cuja demonstração mais célebre remonta ao argumento clássico de Euclides.

Teorema 1. [Euclides] *Existem infinitos primos.*

Prova. Suponha por absurdo que haja um número finito de primos e sejam $p_1, p_2, \dots, p_k$ todos os primos. Considere o número $N = p_1 p_2 \dots p_k + 1$ e observe que, pelo teorema fundamental da aritmética, N possui algum fator primo p_j . Mas então p_j divide $N - p_1 \cdot p_2 \dots p_k = 1$, um absurdo. $\square$

E se quisermos provar que existem infinitos primos em uma certa progressão aritmética? Por exemplo, será que existem infinitos primos da forma $4k + 1$? A resposta é afirmativa e é possível adaptar a ideia de Euclides!

Teorema 2. *Existem infinitos números primos da forma $4k + 1$, com $k \in \mathbb{Z}$.*

Prova. Suponha por absurdo que haja um número finito de primos e sejam $p_1, p_2, \dots, p_k$ todos os primos congruentes a 1 módulo 4. Considere o número

$$N = (p_1 p_2 \dots p_k)^2 + 1.$$

Sabemos que todo número da forma $x^2 + 1$ com $x > 1$ possui um fator primo congruente a 1 módulo 4. Logo, N deve possuir algum fator primo p_j . Mas então p_j divide $N - (p_1 p_2 \dots p_k)^2 = 1$, um absurdo. $\square$

Um questionamento interessante é se é possível generalizar as ideias das soluções acima para mostrar

que existem infinitos primos em uma progressão aritmética mais geral, da forma $ak + b$ com a e b inteiros fixados tais que $\text{mdc}(a, b) = 1$? Note que a condição de a e b serem primos entre si é necessária, pois do contrário qualquer fator comum de a e b dividiria $ak + b$.

A resposta para essa pergunta é afirmativa e é o famoso *teorema de Dirichlet*, provado em 1837.

Teorema 3 (Dirichlet, 1837). *Sejam a e b inteiros positivos com $\text{mdc}(a, b) = 1$. Existem infinitos números primos da forma $ak + b$, com $k \in \mathbb{Z}$.*

As principais demonstrações desse teorema utilizam variáveis complexas e não vão na linha dos argumentos apresentados acima.

O objetivo deste material é, inicialmente, apresentar alguns contextos em que os argumentos utilizados nas demonstrações dos Teoremas 1 e 2 se mostram particularmente interessantes. Em seguida, mudamos ligeiramente o foco para discutir resultados sobre os fatores primos de sequências mais gerais de inteiros. Por fim, comentamos alguns aspectos relevantes relacionados à distribuição dos números primos.

Primos em Uma Progressão Aritmética

Nesta seção discutiremos de modo mais aprofundado alguns pontos por trás das demonstrações de Euclides e do caso $4k + 1$ apresentadas acima.

Para adaptar as ideias para o caso $ak + b$, podemos procurar um polinômio $f(x) \in \mathbb{Z}[x]$ para o qual $f(m)$ possua algum fator da forma $ak + b$ para todo

m suficientemente grande. No caso da prova de Euclides, como não temos restrições para o primo, usamos simplesmente $f(x) = x + 1$. Já no segundo caso, foi fundamental escolher $f(x) = x^2 + 1$.

Se existisse um número finito de primos da forma $ak + b$, digamos $p_1, p_2, \dots, p_t$ e se existisse tal f com a propriedade de que, para m suficientemente grande, $f(m)$ sempre possui algum fator da forma $ak + b$, poderíamos tomar

$$N = f((p_1 p_2 \dots p_t)^\ell),$$

com ℓ suficientemente grande de modo que $N > 1$. Pela propriedade de f , concluiríamos que N deve possuir algum fator primo p_j . Dessa forma, lembrando que $x - y \mid f(x) - f(y)$, concluímos que p_j também divide $f((p_1 p_2 \dots p_k)^\ell) - f(0) = N - f(0)$ e, portanto, p_j divide $f(0)$. Isso em princípio não necessariamente produz um absurdo, mas se encontrarmos f tal que $f(0) = 1$, resolvemos nosso problema chegando a uma contradição.

Uma outra opção seria encontrar f tal que, para m suficientemente grande, todos os fatores primos de $f(m)$ sejam congruentes a b módulo a , à exceção, possivelmente, de uma quantidade finita de primos, como ocorre em $f(x) = x^2 + 1$, para o caso $4k + 1$. De fato, tomando $m_\ell = (P p_1 p_2 \dots p_t)^\ell$, em que P é o produto dos primos que são possíveis exceções, observe que, para ℓ suficientemente grande, os expoentes da fatoração em primos de $f(m_\ell)$ estão limitados pelo expoente do termo independente $f(0)$ (podemos supor $f(0) \neq 0$, tomando f irredutível em $\mathbb{Z}[x]$). Isso significa que a sequência (a_ℓ) definida por $a_\ell = |f(m_\ell)|$ é limitada. Porém, para f não constante e ℓ arbitrariamente grande, ela deveria “explodir”.

A principal dificuldade dessas abordagens reside, em geral, na construção de polinômios com as propriedades desejadas. Ainda assim, essa ideia pode ser explorada em outros contextos. Encerramos a discussão apresentando um caso particularmente interessante em que tal abordagem é possível, a saber, a existência de infinitos primos da forma $nk + 1$, para um inteiro positivo fixo n . A demonstração utiliza a noção de *polinômios ciclotômicos*. Para saber mais a respeito, veja [4].

Teorema 4. *Seja n um inteiro positivo. Existem infinitos números primos da forma $nk + 1$, com $k \in \mathbb{Z}$.*

Prova. Suponha que haja um número finito de primos congruentes a 1 módulo n e sejam $p_1, p_2, \dots, p_k$ estes primos. Defina $a = (np_1 p_2 \dots p_k)^\ell$. Para definir o polinômio f , precisaremos recorrer aos polinômios ciclotômicos. Seja $\phi_n(x)$ o n -ésimo polinômio

ciclotômico. Vamos mostrar que $\phi_n(a)$ possui um fator primo congruente a 1 módulo n . Isso produz a contradição desejada, pois argumentando como anteriormente, se q é um fator de $\phi_n(a)$ congruente a 1 módulo n , teremos que $q \mid a$ e, como $a = a - 0 \mid \phi_n(a) - \phi_n(0)$, concluímos que $q \mid \phi_n(0)$, porém sabemos que $|\phi_n(0)| = 1$.

Na verdade, vamos mostrar algo mais forte: todo fator primo de $\phi_n(a)$ é congruente a 1 módulo n . Observe primeiramente que podemos tomar ℓ suficientemente grande de modo que $|\phi_n(a)| > 1$, para garantir que $\phi_n(a)$ tem pelo menos um fator primo. Seja então q um fator primo de $\phi_n(a)$. Sabemos das propriedades de polinômios ciclotômicos que

$$\prod_{d \mid n} \phi_d(x) = x^n - 1.$$

Em particular, para $x = a$, temos que $q \mid a^n - 1$ e então, para mostrar que q é congruente a 1 módulo n , é suficiente verificar que $\text{ord}_q(a) = n$, pois, como pelo teorema de Fermat temos $a^{q-1} \equiv 1 \pmod{q}$, segue que $q \equiv 1 \pmod{n}$.

Suponha que $\text{ord}_q(a) = h \neq n$. Como $q \mid a^n - 1$, temos que $h \mid n$. Logo, a equação anterior implica que $x^n - 1 = (x^h - 1)\phi_n(x)p(x)$ para algum polinômio $p(x)$. Analisando módulo q , podemos escrever $x^n - a^n \equiv (x^h - a^h)\phi_n(x)p(x) \pmod{q}$. Pela fatoração única em $\mathbb{Z}_q$, podemos cancelar um fator $(x - a)$ em ambos os lados, obtendo

$$\begin{aligned} & x^{n-1} + x^{n-2}a + \dots + xa^{n-2} + a^{n-1} \\ & \equiv (x^{h-1} + x^{h-2}a + \dots + xa^{h-2} + a^{h-1})\phi_n(x)p(x) \pmod{q}. \end{aligned}$$

Fazendo $x = a$ e lembrando que $q \mid \phi_n(a)$, concluímos que $na^{n-1} \equiv 0 \pmod{q}$, um absurdo, pois $q \mid a^n - 1$ e $n \mid a$, de modo que $\text{mdc}(na^{n-1}, q) = 1$. Isso conclui a demonstração. $\square$

Fatores Primos de uma Sequência

Uma forma alternativa e bastante útil de interpretar as ideias anteriores consiste em evitar o argumento por contradição, isto é, em vez de supor que há apenas um número finito de primos de uma dada forma, buscamos construir explicitamente uma sequência (a_n) com a seguinte propriedade: para cada termo a_n , existe um primo $p_n \equiv b \pmod{a}$ tal que $p_n \mid a_n$ e $p_n \notin \{p_1, \dots, p_{n-1}\}$. Dessa forma, garantimos a produção sucessiva de novos primos da forma desejada.

Uma maneira natural de construir tal sequência é por meio de uma recorrência adequada do tipo

$a_{n+1} = f(a_n)$. Por exemplo, na demonstração do caso $4k + 1$, pode-se considerar a recorrência

$$a_{n+1} = (a_1 \cdots a_n)^2 + 1.$$

Por indução, nota-se facilmente que $a_{n+1} = a_n^3 - a_n^2 + 1$, com $a_1 = 5$. Dessa forma, teríamos $f(x) = x^3 - x^2 + 1$.

Diversas questões podem ser formuladas a respeito dos fatores primos de sequências de inteiros. Em muitos casos, é possível caracterizá-los, especialmente para sequências definidas por recorrências do tipo $a_{n+1} = f(a_n)$, em que f é um polinômio bem compreendido.

Outra questão natural consiste em determinar se o conjunto dos divisores primos dos termos da sequência é infinito. Um resultado clássico relacionado a esse problema é o *teorema de Schur*.

Teorema 5. (Schur) *Seja $P(x) \in \mathbb{Z}[x]$ um polinômio não constante. Então o conjunto dos fatores primos da sequência (a_n) , definida por $a_n = P(n)$ é infinito.*

Prova. Suponha que exista apenas um número finito de primos que dividem algum termo da sequência e sejam $p_1, p_2, \dots, p_k$ tais primos. Se $P(0) = 0$, então $n \mid P(n)$ e o resultado é trivial. Suponha então $P(0) = m \neq 0$ e defina $n_\ell = (p_1 p_2 \cdots p_k)^\ell$, com $\ell > \max\{v_{p_1}(m), \dots, v_{p_k}(m)\}$. Observe que $v_{p_i}(a_{n_\ell}) = v_{p_i}(m)$, o que implica que $|a_{n_\ell}| \leq m$, já que os fatores primos de a_{n_ℓ} pertencem ao conjunto $\{p_1, p_2, \dots, p_k\}$. Mas tomando ℓ arbitrariamente grande, como P é não constante, $|P(n_\ell)| = |a_{n_\ell}|$ fica eventualmente maior que m , um absurdo. $\square$

Outro resultado relacionado é o *teorema de Kobayashi*.

Teorema 6. (Kobayashi) *Seja (x_n) uma sequência de inteiros positivos ilimitada cujo conjunto dos divisores primos é finito. Então, para todo inteiro $y \neq 0$, o conjunto dos fatores primos da sequência $(x_n + y)$ é infinito.*

Sua demonstração original recorre a ferramentas de geometria algébrica. Entretanto, existe uma abordagem alternativa baseada no *teorema de Thue*.

Teorema 7. (Thue) *Seja $d \geq 3$ e $k \in \mathbb{Z}$. Se f é um polinômio homogêneo irredutível de grau d , então existe uma quantidade finita de soluções inteiras para a equação $f(x, y) = k$.*

Embora o teorema de Thue ainda não seja elementar por utilizar teoria de aproximações diofantinas, ele permite uma prova relativamente simples do teorema de Kobayashi. Finalizamos a seção apresentando tal demonstração.

Prova do teorema de Kobayashi. Escreva $a_n = ax^3$ e $a_n + t = by^3$, com a, b livre de cubos. Se (a_n) e $(a_n + t)$ possuem uma quantidade finita de divisores primos, então há uma quantidade finita de possibilidades para a e b , de modo que há uma quantidade finita de equações da forma $by^3 - ax^3 = t$. Mas então, pelo teorema de Thue, temos uma quantidade finita de soluções para essas equações e, em particular, uma quantidade finita de possibilidades para x , o que contradiz o fato de (a_n) ser ilimitada. $\square$

Exercícios

Problema 1. (OBM 2016 - N2) Seja $a_0 = a > 1$ um inteiro e, para $n \geq 0$, defina $a_{n+1} = 2^{a_n} - 1$. Mostre que o conjunto dos divisores primos dos termos da sequência a_n é infinito.

Problema 2. (IMO SL 2009) Seja f uma função não-constante dos inteiros positivos nos inteiros positivos tal que $a - b$ divide $f(a) - f(b)$ para quaisquer inteiros positivos a, b distintos. Prove que existem infinitos números primos p tais que p divide $f(c)$ para algum inteiro positivo c .

Problema 3. (OIMU 2003) Prove que se $P(x)$ é um polinômio não constante com coeficientes inteiros, então existe n inteiro tal que $P(n)$ tem mais de 2003 fatores primos distintos.

Problema 4. (Ibero 2019) Sejam $a_1, a_2, \dots, a_{2019}$ inteiros positivos e P um polinômio com coeficientes inteiros tal que, para todo o inteiro positivo n , $P(n)$ divide $a_1^n + a_2^n + \cdots + a_{2019}^n$. Prove que P é um polinômio constante.

Problema 5. (Irã 2011) Seja $P(x)$ um polinômio não nulo com coeficientes inteiros. Prove que existem infinitos primos q tais que q divide $2^n + P(n)$ para algum n natural.

Problema 6. (TST Irã 2024) Seja $\{a_n\}$ uma sequência de números naturais tal que todo número primo maior que 1402 divide algum termo da sequência. Prove que o conjunto dos divisores primos dos termos da sequência $\{b_n\}$, definida por $b_n = a_1 a_2 \cdots a_n - 1$, é infinito.

Problema 7. (OBMU 2017) Fixados os inteiros positivos a e b , mostre que o conjunto dos divisores primos dos termos da sequência $a_n = a \cdot 2017^n + b \cdot 2016^n$ é infinito.

Sobre a Distribuição dos Primos

Nesta seção vamos apresentar demonstrações para o *postulado de Bertrand* e para provar o *teorema de Chebyshev*. A prova do postulado de Bertrand apresentada é devida a Erdős e os dois lemas utilizados também servem para provar o teorema de Chebyshev.

No que segue, todos os logaritmos são na base natural. Sabendo da existência de infinitos números primos, torna-se natural procurar entender a respeito da *distribuição* dos primos nos inteiros positivos. Mais precisamente, dado um inteiro positivo n , definindo

$\pi(n)$ como a quantidade de números primos no conjunto $[n] = \{1, 2, 3, \dots, n\}$, seria interessante entender o comportamento assintótico desta função. O teorema de Chebyshev responde essa pergunta, provando que $\pi(n) = \Theta\left(\frac{n}{\log n}\right)$.

Teorema 8. (Chebyshev) *Existem constantes positivas $c < C$ tais que para todo $x \geq 2$ vale*

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

Outra pergunta bastante natural é a respeito do comportamento da quantidade de números primos em um certo intervalo $[f(n), g(n)]$. Por exemplo, como consequência do teorema de Chebyshev, podemos facilmente concluir que a quantidade de primos no intervalo $[n, an]$, com $a > 1$ é pelo menos

$$\pi(an) - \pi(n) \geq c \frac{an}{\log(an)} - C \frac{n}{\log n} = (ca - C + o(1)) \frac{n}{\log n}.$$

Logo, quando $a > C/c$, conseguimos muitos primos em intervalos da forma $[n, an]$ para n suficientemente grande. Na demonstração apresentada, teremos $C = 5 \log 2$ e $c = \frac{\log 2}{2}$, o que implica $a > 10$. Mas para valores menores de a , em princípio sequer sabemos se podemos garantir a existência um primo no intervalo para n grande. O postulado de Bertrand responde essa pergunta quando $a = 2$.

Teorema 9. (Postulado de Bertrand) *Seja n um inteiro positivo. Existe um primo $p \in [n, 2n]$.*

Antes de provar os Teoremas 8 e 9, vamos enunciar dois lemas necessários para prová-los.

Lema 1. *Sejam $n \in \mathbb{Z}_{>0}$ e p um número primo. Seja θ_p o inteiro tal que $p^{\theta_p} \leq 2n < p^{\theta_p+1}$. Então¹*

$$v_p \left(\binom{2n}{n} \right) \leq \theta_p.$$

Em particular, se $p > \sqrt{2n}$, então o expoente de p em $\binom{2n}{n}$ é 1, e se $\frac{2n}{3} < p < n$, então p não divide $\binom{2n}{n}$.

Prova. Observe que

$$\begin{aligned} v_p \left(\binom{2n}{n} \right) &= v_p((2n)!) - 2v_p(n!) \\ &= \sum_{i=1}^{\theta_p} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) \leq \theta_p, \end{aligned}$$

pois cada parcela é sempre 0 ou 1. Se $p > \sqrt{2n}$, temos que $\theta_p = 1$ e o resultado segue. Além disso, se $\frac{2n}{3} < p < n$, é fácil ver que todas as parcelas são 0 e então p não divide $\binom{2n}{n}$. $\square$

¹ $v_p(n)$ é o maior número m tal que p^m divide n . (N. do E.)

Lema 2. *Para todo inteiro positivo n , temos*

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

Prova. A prova segue por indução em n . Para n pequeno o resultado é claro. Suponha válido para todo $k < n$. Se n é par, temos que

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

Suponha então n ímpar e seja $n = 2m + 1$. Observe que

$$\begin{aligned} \prod_{\substack{p \leq n \\ p \text{ primo}}} p &= \prod_{\substack{p \leq m+1 \\ p \text{ primo}}} p \cdot \prod_{\substack{m+2 \leq p \leq 2m+1 \\ p \text{ primo}}} p \\ &\leq 4^{m+1} \binom{2m+1}{m+1} \leq 4^{m+1} 2^{2m} = 4^n. \end{aligned}$$

A primeira desigualdade segue da hipótese de indução e do fato de todos os primos p entre $m+2$ e $2m+1$ dividirem $\binom{2m+1}{m+1}$. A cota no binomial segue de $\sum_{i=1}^{2m+1} \binom{2m+1}{i} = 2^{2m+1}$ e de $\binom{2m+1}{m+1} = \binom{2m+1}{m}$. $\square$

Com esses dois resultados em mãos, podemos provar os Teoremas 8 e 9. Ressaltamos que a prova do teorema de Bertrand apresentada é devida a Paul Erdős.

Prova do Teorema 9. Suponha que exista $n \geq 2$ para o qual não há primos no intervalo $[n, 2n]$. Pelas Afirmções 1 e 2, junto com o fato de que até $\sqrt{2n}$ temos no máximo $\sqrt{2n}/2 - 1$ primos e que $p^{\theta_p} \leq 2n$, temos que

$$\begin{aligned} \binom{2n}{n} &\leq \prod_{\substack{p \leq \sqrt{2n} \\ p \text{ primo}}} p^{\theta_p} \cdot \prod_{\substack{\sqrt{2n} < p \leq \frac{2n}{3} \\ p \text{ primo}}} p \\ &= \prod_{\substack{p \leq \sqrt{2n} \\ p \text{ primo}}} p^{\theta_p} \cdot \prod_{\substack{p \leq \frac{2n}{3} \\ p \text{ primo}}} p \leq (2n)^{\sqrt{2n}/2-1} \cdot 4^{2n/3}. \end{aligned}$$

Por outro lado, pela relação de Stifel, temos que

$$\begin{aligned} n \binom{2n}{n} &= n \binom{2n-1}{n} + n \binom{2n-1}{n-1} \\ &> (1+1)^{2n-1}, \end{aligned}$$

o que implica $\binom{2n}{n} > \frac{2^{2n-1}}{n}$. Concluimos então que

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

Tomando logaritmo na base 2, ficamos com a desigualdade $2\sqrt{2n} < 3\log_2(n) + 3$, que é falsa para todo $n \geq 50$. Portanto, para finalizar, basta verificar até $2 \cdot 50 = 100$ e não é difícil observar que os primos 2, 5, 11, 23, 47, 79, 101 cobrem todos os intervalos da forma $[n, 2n]$ com $1 \leq n \leq 50$. $\square$

Agora vejamos a demonstração do teorema de Chebyshev.

Prova do Teorema 8. Basta mostrar uma cota inferior do tipo

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

para $x = 2n$, pois $\pi(2n-1) = \pi(2n)$ e $\frac{x}{\log x}$ é crescente para $x \geq 3$. Vamos cotar a quantidade de números primos menores ou iguais a $2n$ pelos primos que dividem $\binom{2n}{n}$. Pela Afirmação 1, temos que

$$\begin{aligned} \binom{2n}{n} &\leq \prod_{\substack{p \leq 2n \\ p \text{ primo}}} p^{\theta_p} \leq (2n)^{\pi(2n)} \\ \Rightarrow \pi(2n) &\geq \frac{\log \binom{2n}{n}}{\log(2n)} \geq \frac{n \log 2}{\log(2n)}, \end{aligned}$$

em que a última desigualdade segue de

$$\begin{aligned} \binom{2n}{n} &= \binom{n}{0}^2 + \dots + \binom{n}{n}^2 \\ &\geq \binom{n}{0} + \dots + \binom{n}{n} = 2^n. \end{aligned}$$

Portanto, concluímos que

$$\pi(2n) \geq \frac{n \log 2}{\log(2n)} \Rightarrow \pi(x) \geq \frac{\log 2}{2} \frac{x}{\log x}.$$

Resta provarmos a cota superior. Veja que também temos

$$\binom{2n}{n} = \binom{n}{0}^2 + \dots + \binom{n}{n}^2 < \left(\binom{n}{0} + \dots + \binom{n}{n} \right)^2 = 2^{2n}.$$

Portanto, em particular, o produto dos primos entre n e $2n$ é menor que 2^{2n} e então

$$\begin{aligned} n^{\pi(2n) - \pi(n)} &< \prod_{\substack{n < p \leq 2n \\ p \text{ primo}}} p < 2^{2n} \\ \Leftrightarrow \pi(2n) - \pi(n) &< \frac{2n \log 2}{\log n}, \end{aligned}$$

o que implica, por indução, que

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

Finalmente, se $2^k < x \leq 2^{k+1}$, temos que

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

Para concluir esta seção, apresentamos o celebrado teorema dos números primos, provado independentemente por Jacques Hadamard e Charles Jean de la Vallée Poussin, em 1896. Sua demonstração usual também utiliza variáveis complexas e não será apresentada aqui.

Teorema 10. (*Teorema dos Números Primos*) Tem-se que

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x} = 1.$$

Em outras palavras, para todo $\varepsilon > 0$, existe $n_0 > 0$ tal que se $n \geq n_0$, então

$$(1 - \varepsilon) \frac{n}{\log n} < \pi(n) < (1 + \varepsilon) \frac{n}{\log n}.$$

Em particular, para todo $n \geq n_0$, temos $\Theta(\frac{n}{\log n})$ primos no intervalo $[n, (1 + \delta)n]$, com $\delta > 0$ fixado.

A Soma dos Inversos dos Primos

Nesta seção apresentaremos uma demonstração sobre o fato bastante útil de que a série da soma dos inversos dos primos

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots$$

é divergente.

Antes de apresentarmos o argumento, será útil discutir a demonstração de Erdős para a infinitude dos números primos. Essa prova baseia-se, essencialmente, na noção de densidade nos inteiros positivos, cuja ideia pode ser descrita da seguinte forma: dado um inteiro positivo M , estimamos, em função de M , quantos números no intervalo $[1, M]$ satisfazem determinada propriedade. Ao fazer $M \rightarrow \infty$, buscamos compreender se há infinitos inteiros que a satisfazem (ou, alternativamente, que não a satisfazem).

Segunda prova do Teorema 1. Suponha que a quantidade de primos seja finita e sejam $p_1, p_2, \dots, p_k$. Fixado um inteiro M , escreva cada inteiro $m \in [1, M]$ na forma $m = ax^2$, com a livre de quadrados. Observe que para a temos 2^k possibilidades, pois cada p_i pode aparecer ou não na fatoração dele. Por outro lado, para x temos no máximo $\sqrt{M}$ possibilidades. Dessa forma, concluímos que $2^k \sqrt{M} \geq M$, o que equivale a $2^{2k} \geq M$. Mas como M é qualquer, tomando $M > 2^{2k}$, temos um absurdo. $\square$

Com a ideia da prova anterior em mente, podemos agora apresentar a demonstração de Paul Erdős de que a soma dos inversos dos primos diverge.

Teorema 11. A série

$$\sum_{p \text{ primo}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots$$

diverge.

Prova. Suponha que a série converge. Então existe $N > 0$ tal que

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

Considere a partição dos naturais $\mathbb{N} = A \cup B$, em que $B = \mathbb{N} \setminus A$ e

$$A = \{n \in \mathbb{N} : p \mid n, p \text{ primo} \Rightarrow p < N\}.$$

Seja $M \in \mathbb{N}$ e $n \leq M$, note que o expoente de um fator primo na fatoração de n é no máximo $\frac{\log M}{\log 2}$. Portanto, a quantidade de inteiros positivos que utilizam apenas fatores menores que N é

$$|A \cap [1, n]| \leq \left(1 + \frac{\log M}{\log 2}\right)^{\pi(N)}.$$

Por outro lado, todo elemento de B possui um fator primo maior ou igual a N e então

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

Dessa forma, temos que

$$\begin{aligned} M &= |A \cap [1, M]| + |B \cap [1, M]| \\ &< \left(1 + \frac{\log M}{\log 2}\right)^{\pi(N)} + \frac{M}{2}, \end{aligned}$$

e então

$$\frac{M}{2} < \left(1 + \frac{\log M}{\log 2}\right)^{\pi(N)},$$

que é claramente absurdo para M suficientemente grande. $\square$

Exercícios

Problema 8. (IMC 2012) O conjunto dos inteiros positivos n tais que $n! + 1$ divide $(2012n)!$ é finito ou infinito?

Problema 9. (IMO SL 2007) Encontre todas as funções sobrejetivas $f: \mathbb{N} \rightarrow \mathbb{N}$ tais que, para quaisquer $m, n \in \mathbb{N}$ e para todo primo p , o número $f(m+n)$ é divisível por p se, e somente se, $f(m) + f(n)$ é divisível por p .

Problema 10. Sejam k e n inteiros positivos com $n > 2^k$. Prove que os k primeiros números que são maiores do que n e primos relativos com $n!$ são primos.

Problema 11. (Sylvester-Schur) Sejam $n, k \in \mathbb{Z}_{>0}$, $n \geq 2k$. Então $\binom{n}{k}$ tem um fator primo $p > k$.

Problema 12. (Erdős-Pálffy) Sejam a e b inteiros positivos tais que quando os dividimos por qualquer primo p , o resto de a é sempre menor ou igual ao resto de b . Prove que $a = b$.

Problema 13. Sejam (p_n) a sequência dos primos. Prove que

$$\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \left(1 - \frac{1}{p_3}\right) \cdot \dots = 0.$$

Problema 14. Seja $\lambda > 1$ um número real. Denote por p_n o n -ésimo número primo em ordem crescente. Prove que a sequência $(\lfloor \lambda p_n \rfloor)$ possui infinitos divisores primos.

Problema 15. (Rioplatense 1999) Sejam $p_1, p_2, \dots, p_k$ k números primos distintos. Consideramos todos os inteiros positivos que utilizam apenas esses primos (não necessariamente todos) em sua fatoração em primos e organizamos esses números em ordem crescente, formando uma sequência infinita $a_1 < a_2 < \dots < a_n < \dots$. Prove que, para todo número c , existe um n tal que $a_{n+1} - a_n > c$.

Problema 16. (CIIM 2024) Dado um inteiro positivo n , seja $\varphi(n)$ o número de inteiros positivos menores ou iguais a n que são relativamente primos com n . Determine todos os inteiros positivos k para os quais existem inteiros positivos $1 \leq a_1 < a_2 < \dots < a_k$ tais que

$$\left\lfloor \frac{\varphi(a_1)}{a_1} + \frac{\varphi(a_2)}{a_2} + \dots + \frac{\varphi(a_k)}{a_k} \right\rfloor = 2024.$$

Bibliografia

- [1] David Galvin. Erdos's proof of bertrand's postulate. 2013.
- [2] FB MARTINEZ, CG MOREIRA, N Saldanha, and Eduardo Tengan. Teoria dos números: um passeio com primos e outros números. IMPA, Rio de Janeiro, 5ª edição, 2018.
- [3] CJ Quines. Sledgehammers in number theory, June 2023. Manuscript.
- [4] Carlo Sanna. A survey on coefficients of cyclotomic polynomials. *Expositiones Mathematicae*, 40(3):469–494, 2022.



Rafael Filipe dos Santos é natural do Rio de Janeiro, formado em Engenharia da Computação pelo Instituto Militar de Engenharia (IME) e mestre em Matemática Pura pelo Instituto de Matemática Pura e Aplicada (IMPA), onde cursa doutorado em Combinatória. Participou de olimpíadas de matemática, com medalha de bronze na IMO e duas de ouro na IMC. Hoje atua na Comissão Nacional de Olimpíadas da OBM.