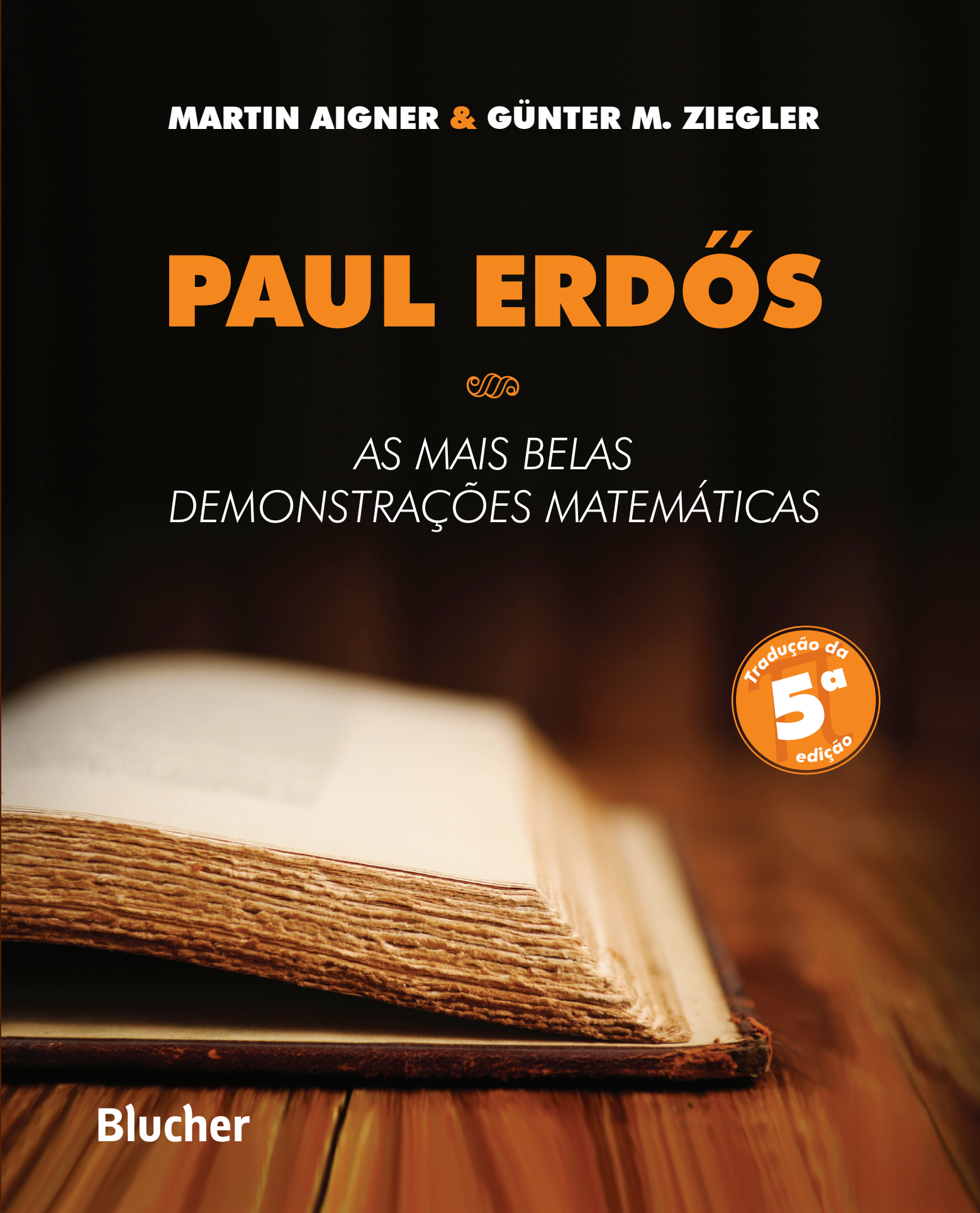
MARTIN AIGNER & GÜNTER M. ZIEGLER

PAUL ERDŐS

AS MAIS BELAS DEMONSTRAÇÕES MATEMÁTICAS

Tradução da 5ª edição



Blucher

Martin Aigner
Universidade Livre de Berlim

Günter M. Ziegler
Universidade Livre de Berlim

Paul Erdős:
as mais belas demonstrações matemáticas

Tradução da 5ª edição

Tradução
Marcos Botelho
Departamento de Matemática do
Instituto Tecnológico de Aeronáutica

Tradução e revisão
Helena Castro
Instituto de Matemática e Estatística da
Universidade de São Paulo

Paul Erdős: as mais belas demonstrações matemáticas, tradução da 5.ª edição
Tradução da edição em língua inglesa:
Proofs from THE BOOK
de Martin Aigner e Günter M. Ziegler

Blucher

Rua Pedroso Alvarenga, 1245, 4º andar
04531-934 - São Paulo - SP - Brasil
Tel.: 55 11 3078-5366
contato@blucher.com.br
www.blucher.com.br

Segundo o Novo Acordo Ortográfico, conforme 5. ed. do *Vocabulário Ortográfico da Língua Portuguesa*, Academia Brasileira de Letras, março de 2009.

Dados Internacionais de Catalogação na Publicação (CIP)
Angélica Ilacqua CRB-8/7057

Aigner, Martin
Paul Erdős: as mais belas demonstrações matemáticas / Martin Aigner, Günter M. Ziegler; tradução de Marcos Botelho; tradução e revisão de Helena Castro. – São Paulo: Blucher, 2017.
368 p.; il. color.

ISBN 978-85-212-1005-4

Título original em inglês: *Proofs from the book*

1. Matemática I. Título II. Ziegler, Günter M. III. Botelho, Marcos IV. Castro, Helena

16-0114 CDD 510

Índices para catálogo sistemático:
1. Matemática

Conteúdo

CAPÍTULO 1

SEIS DEMONSTRAÇÕES DA INFINIDADE DOS NÚMEROS PRIMOS

Nada mais natural do que começarmos estas notas com provavelmente a mais antiga demonstração d'O Livro, usualmente atribuída a Euclides (*Os Elementos*, IX, 20). Ela mostra que a sequência de números primos nunca termina.

Demonstração de Euclides. Para qualquer conjunto finito $\{p_1,\ldots, p_r\}$ de números primos, considere o número $n = p_1p_2 \cdots p_r + 1$. Esse n tem um divisor primo p. Mas p não é um dos p_i: caso contrário, p seria um divisor de n e do produto $p_1p_2 \cdots p_r$, e assim também da diferença $n - p_1p_2 \cdots p_r = 1$, o que é impossível. Portanto, um conjunto finito $\{p_1,\ldots, p_r\}$ não pode ser a coleção de todos os números primos. □

Antes de continuar, vamos fixar algumas notações. $\mathbb{N} = \{1, 2, 3,\ldots\}$ é o conjunto dos números naturais, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2,\ldots\}$, o conjunto dos inteiros e $\mathbb{P} = \{2, 3, 5, 7,\ldots\}$ o conjunto dos números primos.

No que segue, estaremos exibindo várias outras demonstrações (tiradas de uma lista muito maior) as quais esperamos que o leitor aprecie tanto quanto nós. Embora usem enfoques diferentes, a seguinte ideia básica é comum a todas elas: os números naturais crescem além de qualquer limite, e todo número natural $n \geq 2$ tem um divisor primo. Esses dois fatos, juntos, fazem com que $\mathbb{P}$ seja infinito. A próxima demonstração é devida a Christian Glodbach (de uma carta de 1730 a Leonhard Euler), a terceira demonstração aparentemente faz parte do folclore, a quarta é do próprio Euler, a quinta demonstração foi proposta por Harry Fürstenberg, enquanto a última é devida a Paul Erdős.

$$
\begin{aligned}
F_0 &= 3\\
F_1 &= 5\\
F_2 &= 17\\
F_3 &= 257\\
F_4 &= 65537\\
F_5 &= 641 \cdot 6700417\\
&\vdots
\end{aligned}
$$

Os primeiros números de Fermat

Segunda demonstração. Primeiramente, vamos olhar para os *números de Fermat* $F_n = 2^{2^n} + 1$, para $n = 0, 1, 2,\ldots$. Mostraremos que quaisquer dois

Teorema de Lagrange

Se G é um grupo (multiplicativo) finito e U é um subgrupo, então $|U|$ *divide* $|G|$.

Demonstração. Considere a relação binária

$$a \sim b : \Leftrightarrow ba^{-1} \in U.$$

Segue, dos axiomas de grupo, que ~ é uma relação de equivalência. A classe de equivalência contendo um elemento *a* é precisamente a classe lateral

$$Ua = \{xa : x \in U\}.$$

Uma vez que claramente $|Ua| = |U|$, temos que *G* se decompõe em classes de equivalência, todas de tamanho $|U|$ e, consequentemente, $|U|$ divide $|G|$.

No caso especial em que *U* é um subgrupo cíclico $\{a, a^2, \ldots, a^m\}$, temos que *m* (o menor inteiro positivo tal que $a^m = 1$, chamado de *ordem* de *a*) divide a ordem $|G|$ do grupo.

Em particular, temos que $a^{|G|} = 1$.

números de Fermat são relativamente primos; consequentemente, deverão existir infinitos números primos. Para esse fim, vamos verificar a recursão

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geq 1),$$

da qual nossa afirmação segue imediatamente. De fato, se *m* é um divisor de, digamos, F_k e F_n $(k < n)$, então *m* divide 2 e, daí, $m = 1$ ou 2. Mas $m = 2$ é impossível, uma vez que todos os números de Fermat são ímpares.

Para demonstrar a recursão, usamos indução em *n*. Para $n = 1$, temos $F_0 = 3$ e $F_1 - 2 = 3$. Pela indução, concluímos que

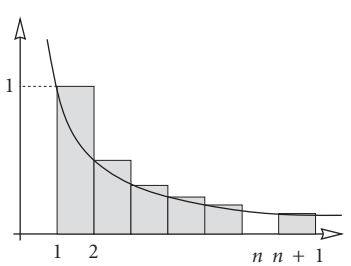
$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n = \left(F_n - 2\right) F_n =$$
$$= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2^{n+1}} - 1 = F_{n+1} - 2. \qquad \square$$

Terceira demonstração. Suponha que $\mathbb{P}$ seja finito e *p* seja o maior número primo. Consideremos o número $2^p - 1$, conhecido como *número de Mersenne*, e mostremos que qualquer fator primo *q* de $2^p - 1$ é maior do que *p*, o que resultará na conclusão desejada. Seja *q* um primo que divide $2^p - 1$, de forma que temos $2^p \equiv 1 \pmod{q}$.

Já que *p* é primo, isso significa que o elemento 2 tem ordem *p* no grupo multiplicativo $\mathbb{Z}_q \setminus \{0\}$ do corpo $\mathbb{Z}_q$. Esse grupo tem $q - 1$ elementos. Pelo teorema de Lagrange (ver quadro), sabemos que a ordem de cada elemento divide a ordem do grupo, ou seja, temos que $p | q - 1$, e daí $p < q$. $\square$

Agora vamos ver uma demonstração que usa cálculo elementar.

Quarta demonstração. Seja $\pi(x) := \#\{p \leq x : p \in \mathbb{P}\}$ o número de primos que são menores que ou iguais ao número real *x*. Enumeremos os primos $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ em ordem crescente. Considere o logaritmo natural $\log x$, definido como $\log x = \int_1^x \frac{1}{t} dt$.



Degraus acima da função $f(t) = \frac{1}{t}$

Agora, vamos comparar a área sob o gráfico de $f(t) = \frac{1}{t}$ com uma função degrau superior. (Para esse método, ver também o apêndice na página 15.) Assim, para $n \leq x \leq n + 1$, temos

$$\log x \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n} \leq \sum \frac{1}{m},$$

onde a soma se estende sobre todos os $m \in \mathbb{N}$ que têm somente divisores $p \leq x$.

Uma vez que cada um desses m pode ser escrito de um modo único como um produto da forma $\prod_{p\leq x} p^{k_p}$, vemos que a última soma é igual a

$$\prod_{p\in\mathbb{P},p\leq x}\left(\sum_{k\geq 0}\frac{1}{p^k}\right).$$

A soma interior é uma série geométrica com razão $\frac{1}{p}$, de onde

$$\log x \leq \prod_{p\in\mathbb{P},p\leq x}\frac{1}{1-\frac{1}{p}} = \prod_{p\in\mathbb{P},p\leq x}\frac{p}{p-1} = \prod_{k=1}^{\pi(x)}\frac{p_k}{p_k-1}.$$

Agora, claramente, $p_k \geq k+1$ e, assim,

$$\frac{p_k}{p_k-1} = 1+\frac{1}{p_k-1} \leq 1+\frac{1}{k} = \frac{k+1}{k}.$$

Consequentemente,

$$\log x \leq \prod_{k=1}^{\pi(x)}\frac{k+1}{k} = \pi(x)+1.$$

É de conhecimento comum que $\log x$ não é limitado, donde concluímos que $\pi(x)$ também não é limitado e, portanto, existe um número infinito de primos. □

Quinta demonstração. Depois de análise, agora é topologia! Considere a curiosa topologia no conjunto $\mathbb{Z}$ dos números inteiros a seguir. Para $a, b \in \mathbb{Z}$, $b > 0$, façamos

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Cada conjunto $N_{a,b}$ é uma progressão aritmética infinita nos dois sentidos. Agora, dizemos que um conjunto $O \subseteq \mathbb{Z}$ é *aberto* se O é vazio ou se, para cada $a \in O$, existe algum $b > 0$ com $N_{a,b} \subseteq O$. É claro que a união de conjuntos abertos é também um conjunto aberto. Se O_1, O_2 são abertos, e $a \in O_1 \cap O_2$, com $N_{a,b_1} \subseteq O_1$ e $N_{a,b_2} \subseteq O_2$, então $a \in N_{a,b_1b_2} \subseteq O_1 \cap O_2$. Então, concluímos que qualquer interseção finita de conjuntos abertos também é um conjunto aberto. Assim, essa família de conjuntos abertos induz uma topologia em $\mathbb{Z}$.

"Jogando pedras chatas, infinitamente"

Convém observar dois fatos:

(A) Qualquer conjunto aberto não vazio é infinito.

(B) Qualquer conjunto $N_{a,b}$ também é fechado.

O primeiro fato decorre da definição. Quanto ao segundo, observamos que

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b},$$

o que demonstra que $N_{a,b}$ é o complementar de um conjunto aberto e, portanto, fechado.

Até agora, os números primos ainda não entraram em cena – mas ei-los aqui. Uma vez que qualquer número $n \neq 1, -1$ tem um divisor primo p e, consequentemente, está contido em $N_{0,p}$, concluímos que

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Agora, se $\mathbb{P}$ fosse finito, então $\cup_{p \in \mathbb{P}} N_{0,p}$ seria uma união finita de conjuntos fechados devido a (B), e portanto fechado. Consequentemente, $\{1, -1\}$ seria um conjunto aberto, o que contradiz (A). □

Sexta demonstração. Nossa demonstração final dá um considerável passo adiante e mostra não somente que há infinitos números primos, mas também que a série $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverge. A primeira demonstração desse resultado importante foi dada por Euler (e é interessante em si mesma), mas nossa demonstração, concebida por Erdős, é de uma beleza irresistível.

Seja $p_1, p_2, p_3, \ldots$ a sequência dos números primos em ordem crescente, e suponha que $\sum_{p \in \mathbb{P}} \frac{1}{p}$ converge. Então deve existir um número natural k tal que $\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Vamos chamar $p_1, \ldots, p_k$ de *primos pequenos*, e $p_{k+1}, p_{k+2}, \ldots$ de *primos grandes*. Para um número natural arbitrário N, por conseguinte, temos

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{1}$$

Seja N_b o número de inteiros positivos $n \leq N$ que são divisíveis por pelo menos um número primo grande, e N_s o número de inteiros positivos $n \leq N$ que têm somente divisores primos pequenos. Vamos mostrar que, para um N conveniente,

$$N_b + N_s < N,$$

o que será nossa contradição desejada, uma vez que, por definição, $N_b + N_s$ teria que ser igual a N.

Para estimar N_b observe que $\left[\frac{N}{p_i}\right]$ é o número de inteiros positivos $n \leq N$ que são múltiplos de p_i.

Portanto, de (1), obtemos

$$N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}. \tag{2}$$

Vamos agora olhar para N_s. Escrevemos todo $n \leq N$ que tem apenas divisores primos pequenos na forma $n = a_n b_n^2$, onde a_n é a parte sem nenhum quadrado. Todo a_n é, portanto, um produto de primos pequenos *diferentes*, e concluímos que existem precisamente 2^k partes sem nenhum quadrado diferentes. Além disso, como $b_n \leq \sqrt{n} \leq \sqrt{N}$, vemos que existem no máximo $\sqrt{N}$ partes quadradas diferentes e, daí,

$$N_s \leq 2^k \sqrt{N}.$$

Uma vez que (2) vale para *qualquer* N, resta achar um número N com $2^k \sqrt{N} \leq \frac{N}{2}$ ou $2^{k+1} \leq \sqrt{N}$ e, para isso, $N = 2^{2k+2}$ serve. □

Apêndice: outras infinitas demonstrações

Nossa coleção de demonstrações para a infinidade dos primos contém diversos outros tesouros, antigos e novos, mas existe um especial, muito recente, que é bem diferente e merece uma menção especial. Vamos tentar identificar sequências de inteiros S tais que o conjunto $\mathbb{P}_S$ dos primos que dividem algum membro de S seja infinito. Toda sequência dessa forneceria então sua própria demonstração para a infinidade dos primos. Os números de Fermat F_n estudados na segunda demonstração formam uma destas sequências, enquanto que as potências de dois não formam. Muitos outros exemplos são fornecidos por um teorema de Issai Schur, que mostrou em 1912 que, para todo polinômio não constante $p(x)$ com coeficientes inteiros, o conjunto de todos os valores não nulos $\{p(n) \neq 0 : n \in \mathbb{N}\}$ é uma dessas sequências. Para o polinômio $p(x) = x$, o resultado de Schur nos dá o teorema de Euclides. Como outro exemplo, para $p(x) = x^2 + 1$ obtemos que o "quadrado mais um" contém um número infinito de fatores primos.

Issai Schur

O resultado a seguir, devido a Christian Elsholtz, é realmente notável: ele generaliza o teorema de Schur, a demonstração é simplesmente uma contagem inteligente e é, em certo sentido, a melhor possível.

Seja $S = (s_1, s_2, s_3, \ldots)$ uma sequência de inteiros. Dizemos que:

- S é *quase injetiva* se todo valor ocorre no máximo c vezes, para alguma constante c.
- S é *de crescimento subexponencial* se $|s_n| \leq 2^{2^{f(n)}}$ para todo n, em que $f : \mathbb{N} \to \mathbb{R}_+$ é uma função com $\frac{f(n)}{\log_2 n} \to 0$.

No lugar de 2, poderíamos usar qualquer outra base maior que 1; por exemplo, $|s_n| \leq e^{e^{f(n)}}$ leva à mesma classe de sequências.

Teorema. *Se a sequência* $S = (s_1, s_2, s_3, \ldots)$ *for quase injetiva e de crescimento subexponencial, então o conjunto* $\mathbb{P}_S$ *dos primos que dividem algum membro de S é infinito.*

Demonstração. Podemos supor que $f(n)$ é monotonamente crescente. Caso contrário, substitua $f(n)$ por $\max_{i \le n} f(i)$; você pode verificar facilmente que com esta $F(n)$ a sequência S também satisfaz a condição de crescimento subexponencial.

Vamos supor, por absurdo, que $\mathbb{P}_S = \{p_1, \ldots, p_k\}$ seja finito. Para $n \in \mathbb{N}$, faça

$$s_n = \varepsilon_n p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \text{ com } \varepsilon_n \in \{1, 0, -1\}, a \ge 0,$$

em que $\alpha_i = \alpha_i(n)$ depende de n. (Para $s_n = 0$ podemos tomar $\alpha_i = 0$ para todo i.) Então,

$$2^{\alpha_1 + \cdots + \alpha_k} \le |s_n| \le 2^{2^{f(n)}} \qquad \text{para } s_n \ne 0,$$

e, portanto, tomando o logaritmo binário,

$$0 \le \alpha_i \le \alpha_1 + \cdots + \alpha_k \le 2^{f(n)} \text{ para } 1 \le i \le k.$$

Logo, não existem mais do que $2^{f(n)} + 1$ valores diferentes possíveis para cada $\alpha_i = \alpha_i(n)$. Já que f é monótona, isto nos dá uma primeira estimativa.

$$\#\{\text{distintos } |s_n| \ne 0 \text{ para } n \le N\} \le (2^{f(N)} + 1)^k \le 2^{(f(N)+1)k}.$$

Por outro lado, uma vez que S é quase injetiva, somente c termos na sequência podem ser iguais a 0, e cada valor absoluto não nulo pode ocorrer no máximo $2c$ vezes. Assim, obtemos a estimativa inferior

$$\#\left\{\text{distintos } |s_n| \ne 0 \text{ para } n \le N\right\} \ge \frac{N - c}{2c}.$$

Juntando tudo, obtemos

$$\frac{N - c}{2c} \le 2^{k(f(N)+1)}.$$

Tomando novamente o logaritmo na base 2 em ambos os lados, obtemos

$$\log_2(N - c) - \log_2(2c) \le k(f(N) + 1) \qquad \text{para todo } N.$$

Isso, entretanto, é claramente falso para valores grandes de N, já que k e c são constantes, e $\frac{\log_2(N-c)}{\log_2 N}$ tende a 1 para $N \to \infty$, enquanto que $\frac{f(N)}{\log_2 N}$ tende a 0. □

Seria possível relaxar as condições? Pelo menos, nenhuma das duas é supérflua.

Que precisamos da condição "quase injetiva" pode ser visto a partir de sequências como (2, 2, 2, …) ou (1, 2, 2, 4, 4, 4, 4, 8, …), que satisfazem a condição de crescimento, enquanto que $\mathbb{P}_S = \{2\}$ é finito.

Quanto à condição de crescimento subexponencial, salientamos que ela não pode ser enfraquecida a uma exigência da forma $\frac{f(n)}{\log_2 n} \leq \varepsilon$ para um $\varepsilon > 0$ fixo. Para ver isso, basta analisar a sequência de todos os números da forma $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, arrumados na ordem crescente, em que $p_1, \ldots, p_k$ são primos fixos e k é grande. Esta sequência S cresce aproximadamente como $2^{2^{f(n)}}$, com $\frac{f(n)}{\log_2 n} \approx \frac{1}{k}$, enquanto $\mathbb{P}_S$ é finito por construção.

Referências

[1] B. Artmann: *Euclid – The Creation of Mathematics,* Springer-Verlag, New York, 1999.

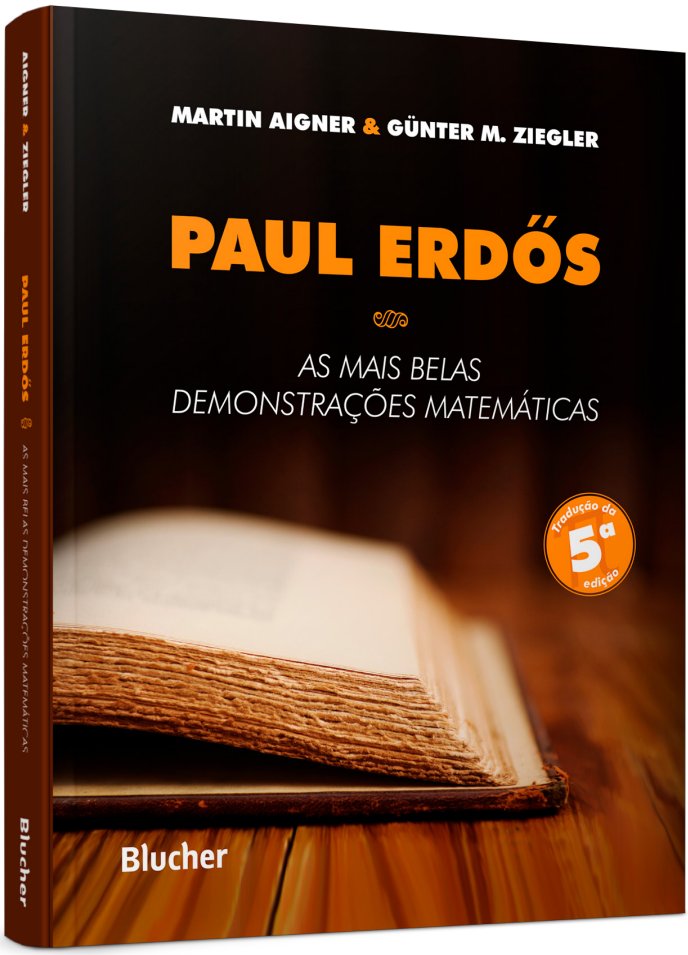
[2] C. Elsholtz: *Prime divisors of thin sequences*, Amer. Math. Monthly 119 (2012), 331-333.

[3] P. Erdős: *Über die Reihe* $\sum \frac{1}{p}$, Mathematica, Zutphen B 7 (1938), 1-2.

[4] L. Euler: *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8.

[5] H. Fürstenberg: *On the infinitude of primes,* Amer. Math. Monthly 62 (1955), 353.

[6] I. Schur: *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmeetischen Progressionen,* Sitzungsberichte der Berliner Math. Gesellschaft 11 (1912), 40-50.



Clique aqui e:

Veja na loja

Paul Erdős
As mais belas demonstrações matemáticas

Martin Aigner e Gunter M. Ziegler

ISBN: 9788521210054
Páginas: 368
Formato: 20,5x25,5 cm
Ano de Publicação: 2017
Peso: 0.779 kg