Dois problemas em Teoria dos Números: a irracionalidade de π e o postulado de Bertrand

Bruno Fernandes Cerqueira Leite

Semana Olímpica — Janeiro 2002

1 O número π é irracional

Veremos uma prova de Ivan Niven[3] para este famoso resultado. Começamos com o seguinte

Lema. *Sejam n um inteiro positivo e $g(x)$ um polinômio de coeficientes inteiros. Então, $x^n g(x)$ e todas as suas derivadas, quando calculados em $x = 0$, são inteiros múltiplos de $n!$.*

Prova. Basta estudar o caso em que $g(x)$ é um monômio, $g(x) = a_k x^k$, pois a derivada da soma é a soma das derivadas. Definindo $h(x) = g(x)x^n$, temos que provar que $h(0), h'(0), h^{(2)}(0), \ldots$ são múltiplos de $n!$. Mas é fácil ver que estes números são todos nulos, com exceção de $h^{(n+k)}(0) = a_k(n+k)!$, que é, evidentemente, um múltiplo de $n!$. $\square$

Agora, suponha que $\pi = a/b$, com $a, b \in \mathbb{N}$. Fixamos $n \in \mathbb{N}$ e definimos

$$f(x) = \frac{x^n(a-bx)^n}{n!} = \frac{b^n x^n (\pi - x)^n}{n!}.$$

Pelo lema, $f(x)$ e todas as suas derivadas são números inteiros em $x = 0$.

Vemos que $f(\pi - x) = f(x)$, e, se derivarmos várias vezes, teremos que $(-1)^j f^{(j)}(\pi - x) = f^{(j)}(x)$. Fazendo $x = 0$, concluímos que $f^{(j)}(\pi)$ é um inteiro para todo $j \in \mathbb{N}$.

Mostraremos a seguir que $\int_0^\pi f(x) \operatorname{sen} x \, \mathrm{dx}$ é um inteiro, e obteremos uma contradição mostrando que é também um número estritamente entre 0 e 1. Para nos ajudar no cálculo da integral, definiremos uma função auxiliar F pela equação $F(x) = \sum_{k=0}^{n} (-1)^k f^{(2k)}(x)$. Vemos que $F(x) + F^{(2)}(x) = f(x)$, logo

$$\frac{\mathrm{d}}{\mathrm{dx}} \left(F'(x) \operatorname{sen} x - F(x) \cos x\right) = (F(x) + F^{(2)}(x)) \operatorname{sen} x = f(x) \operatorname{sen} x.$$

Com isto, podemos calcular a integral de $f(x) \operatorname{sen} x$:

$$\int_0^\pi f(x) \operatorname{sen} x \, \mathrm{dx} = [F'(x) \operatorname{sen} x - F(x) \cos x]_0^\pi = F(\pi) + F(0).$$

Observamos que $F(0)$ e $F(\pi)$ são inteiros, pois são uma soma de inteiros, pela definição de F. Logo, $\int_0^\pi f(x)\,\mathrm{sen}\,x\,\mathrm{dx}$ é um número inteiro, como havíamos dito.

Lembramos que $f(x) = x^n(a-bx)^n/n!$. Então, no intervalo $(0,\pi)$, temos $0 < f(x) < \pi^n a^n/n!$, logo $0 < f(x)\,\mathrm{sen}\,x < \pi^n a^n/n!$. Como o tamanho do intervalo de integração é π, $0 < \int_0^\pi f(x)\,\mathrm{sen}\,x < \pi(\pi^n a^n/n!)$. Observe que isto vale para todo $n \in \mathbb{N}$.

Como $\lim_{n\to\infty} \pi(\pi^n a^n/n!) = 0$, existe um $n_0 \in \mathbb{N}$ tal que, para $n > n_0$, $0 < \int_0^\pi f(x)\,\mathrm{sen}\,x < 1$, o que é um absurdo, pois vimos que a integral é um número inteiro. Logo, π é irracional.

2 O postulado de Bertrand

Joseph Bertrand conjecturou que

$$\text{Para cada } n \geq 1, \text{ existe ao menos um primo } p \text{ tal que } n < p \leq 2n. \tag{1}$$

Bertrand não conseguiu provar a sua conjectura, mas verificou sua validade para todo $n < 3.000.000$. Em 1850, Chebyshev deu a primeira demonstração completa de (1). Em 1932, Paul Erdős deu uma prova elementar para o Postulado de Bertrand, que reproduziremos a seguir, baseados no segundo capítulo da referência [1].

Lema 1. *Para $n < 4000$, (1) é verdadeira.*

Prova. Basta considerar a sequência de primos $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$. Note que cada primo desta sequência é menor que o dobro do anterior. $\square$

Lema 2. *Para todo $x \geq 2$ real,*

$$\prod_{p \leq x} p \leq 4^{x-1}. \tag{2}$$

Prova. A afirmação está correta para $x = 2$. Para $x > 2$, veja que, se provarmos (2) para os casos em que x é um primo ímpar, então teremos provado (2) para todo $x \geq 2$. Então, seja $x = 2m+1$ um primo ímpar. Faremos indução sobre m. Temos

$$\prod_{p \leq 2m+1} p = \left(\prod_{p \leq m+1} p\right)\left(\prod_{m+1 < p \leq 2m+1} p\right). \tag{3}$$

Por hipótese de indução, temos $\prod_{p \leq m+1} p \leq 4^m$. Por outro lado,

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

A primeira desigualdade em (4) segue da seguinte observação: se p é primo e $m+1 < p \leq 2m+1$, p aparece no numerador de $\binom{2m+1}{m} = (2m+1)!/(m!(m+1)!)$, mas não no denominador. Logo p divide $\binom{2m+1}{m}$, e $(\prod_{m+1<p\leq 2m+1} p)$ divide $\binom{2m+1}{m}$.

Para a segunda desigualdade em (4), basta observar que

$$4^m = \frac{1}{2}\sum_{k=0}^{2m+1}\binom{2m+1}{k} \geq \frac{1}{2}\left(\binom{2m+1}{m}+\binom{2m+1}{m+1}\right) = \binom{2m+1}{m}.$$

Isto completa a indução, pois, por (3),

$$\prod_{p\leq 2m+1} p = \left(\prod_{p\leq m+1} p\right)\left(\prod_{m+1<p\leq 2m+1} p\right) \leq 4^m 4^m = 4^{2m}.$$

$\square$

Lema 3 (Teorema de Legendre). *Seja p^m a maior potência de p que divide $n!$. Então $m = \sum_{k\geq 1}\left\lfloor \frac{n}{p^k}\right\rfloor$.*

Prova. Existem exatamente $\left\lfloor \frac{n}{p}\right\rfloor$ inteiros de 1 a n que são múltiplos de p, $\left\lfloor \frac{n}{p^2}\right\rfloor$ que são múltiplos de p^2, e, em geral, existem $\left\lfloor \frac{n}{p^k}\right\rfloor$ inteiros de 1 a n que são múltiplos de p^k. Fica como exercício completar a demonstração. (é bem fácil) $\square$

Lema 4. *A maior potência de p que divide $\binom{2n}{n}$ é no máximo $2n$. (ou seja, se $p^m \mid \binom{2n}{n}$, então $p^m \leq 2n$). Além disso, se p é primo e $\frac{2}{3}n < p \leq n$, p não divide $\binom{2n}{n}$.*

Prova. Aplicando o lema anterior, se p^m é a maior potência de p que divide $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, então

$$m = \sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right). \tag{5}$$

Como cada parcela da soma acima é um inteiro e

$$\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k}-1\right) = 2,$$

temos que cada parcela em (5) é no máximo 1.

Por outro lado, todas as parcelas em (5) são nulas se $p^k > 2n$. Logo,

$$m = \sum_{\substack{k\geq 1\\ p^k\leq 2n}}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right) \leq \sum_{\substack{k\geq 1\\ p^k\leq 2n}} 1 = \max\{k : p^k \leq 2n\}.$$

Isto prova que, se $p^m \mid \binom{2n}{n}$, então $p^m \leq 2n$.

Por último, temos que mostrar que, se p é primo e $\frac{2}{3}n < p \leq n$, então p não divide $\binom{2n}{n}$. Como $3p > 2n$, teremos que os "p" do numerador de $\frac{(2n)!}{(n!)^2}$ virão dos fatores p e $2p$. Por outro lado, o denominador também tem dois fatores "p", logo $\binom{2n}{n}$ não é múltiplo de p. $\square$

Corolário. *Primos $p > \sqrt{2n}$ aparecem no máximo uma vez em $\binom{2n}{n}$.*

Lema 5. *Para $n \geq 3$, temos*

$$\binom{2n}{n} \geq \frac{4^n}{2n}.$$

Prova. Fixe um inteiro $n \geq 3$. Considere os $2n$ números

$$2, \binom{2n}{1}, \binom{2n}{2}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1}.$$

Veja que $\binom{2n}{n}$ é o maior elemento desta sequência, logo, é maior ou igual à média aritmética destes números, $4^n/2n$. $\square$

Agora, vamos terminar a demonstração. Com o lema 5, conseguimos um limitante inferior para $\binom{2n}{n}$, e com o lema 4 e seu corolário, obteremos um limitante superior. Considere a fatoração prima de $\binom{2n}{n}$: $\binom{2n}{n} = \prod_i p_i^{e_i}$. Pelo lema 4, $p_i^{e_i} \leq 2n$ para todo i. Além disto, pelo corolário do lema 4, se $p_i > \sqrt{2n}$, então $e_i \leq 1$. Com isso, temos

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \left(\prod_{p \leq \sqrt{2n}} 2n\right) \left(\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p\right) \left(\prod_{n < p \leq 2n} p\right). \tag{6}$$

É claro que $\prod_{p \leq \sqrt{2n}} 2n \leq (2n)^{\sqrt{2n}}$, e, pelo lema 2,

$$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq 4^{\frac{2}{3}n}.$$

Se o postulado de Bertrand for falso para algum n, teremos $\prod_{n < p \leq 2n} p = 1$, e (6) implica que $\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n}$, ou seja, que $4^{n/3} \leq (2n)^{1+\sqrt{2n}}$. Isto equivale a $2^{2n} \leq (2n)^{3(1+\sqrt{2n})}$. Veremos que isto implica que $n < 4000$. De fato,

$$2n = (\sqrt[6]{2n})^6 < (\lfloor \sqrt[6]{2n} \rfloor + 1)^6 \leq 2^{6 \lfloor \sqrt[6]{2n} \rfloor} \leq 2^{6 \sqrt[6]{2n}}.$$

Se $n > 50$ (e portanto $18 < 2\sqrt{2n}$),

$$2^{2n} \leq (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20 \sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}},$$

logo $2n < 20(2n)^{2/3}$, $(2n)^{1/3} < 20$ e $n < 4000$, encerrando a demonstração, pelo lema 1.

3 Comentários

Há resultados mais fortes do que a irracionalidade de π. Na referência [1], demonstra-se, de modo bem parecido com o que fizemos, que π^2 é irracional. Na verdade, sabe-se que π é um número *transcendente*, isto é, *não é raiz de nenhum polinômio de coeficientes racionais*. Observe que isto implica que π é irracional, e, mais do que isto, que π^r é irracional, para todo r racional.

O postulado de Bertrand também pode ser melhorado. Seja $\pi(n)$ o número de primos menores ou iguais a n. O Teorema dos Números Primos (TNP) diz que

$$\lim_{n\to\infty} \frac{\pi(n)\log n}{n} = 1.$$

Usando o TNP, não é difícil mostrar (veja o problema 5, abaixo) que para todo $\epsilon > 0$, existe um $n_0 > 0$ tal que, se $n > n_0$, então existe um primo entre n e $(1+\epsilon)n$.

É difícil demonstrar o TNP. As primeiras demonstrações completas apareceram no fim do século XIX e usavam variáveis complexas. Uma demonstração analítica detalhada pode ser achada em [2]. O próprio Paul Erdős, em 1949, foi o primeiro a demonstrar o TNP de modo elementar (sem usar variáveis complexas), mas a demonstração é bastante complicada.

4 Problemas

1. Prove que $e = \sum_{k\geq 0} 1/k!$ é irracional.

2. Definimos y_n como o decimal que se obtém escrevendo

$$0,(\text{dígitos de } 1^n)(\text{dígitos de } 2^n)(\text{dígitos de } 3^n)\ldots$$

Por exemplo, $y_1 = 0,1234\ldots$, $y_2 = 0,1491625\ldots$, $y_3 = 0,182764\ldots$. Mostre que todos os y_n são irracionais.

3. Mostre que para todo $n \geq 1$, pode-se separar os inteiros de 1 a $2n$ em n pares, de modo que a soma dos números de cada par é um primo.

4. O postulado de Bertrand mostra que $\pi(2n) - \pi(n) \geq 1$. Usando a prova de Erdős, melhore isto provando que existe uma constante $k > 0$ tal que

$$\pi(2n) - \pi(n) \geq k\frac{n}{\log n},$$

para todo n suficientemente grande. Aqui, **não vale** usar o TNP!

5. Usando o TNP, prove que para todo $\epsilon > 0$, existe um $n_0 > 0$ tal que, se $n > n_0$, então existe um primo entre n e $(1+\epsilon)n$.

6. Determine todos os inteiros positivos n com a seguinte propriedade: se $1 < k < n$ e $\text{mdc}(k, n) = 1$ então k é primo.

Para terminar, um problema em que a resposta envolve a função $\pi(x)$. (não tem muito a ver com o resto do artigo, mas o problema é interessante)

7. Suponha que $a_1, \ldots, a_k$ são inteiros do intervalo $[1, n]$. Suponha também que os produtos da forma $a_i a_j$ são todos distintos, para todos i, j com $i < j$. Seja $E(n) = \max k$, onde o máximo é tomado sobre todas essas sequências. Mostre que

$$\lim_{n \to \infty} \frac{E(n)}{\pi(n)} = 1.$$

Mais ainda, tente dar boas estimativas para $E(n) - \pi(n)$. (Agradeço ao professor Yoshiharu Kohayakawa por sugerir este problema)

Referências

[1] M. Aigner and G. Ziegler, *Proofs from the book*, Springer-Verlag, Berlin and New York, 1998.

[2] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976, Undergraduate Texts in Mathematics.

[3] I. Niven and H.S. Zuckerman, *An introduction to the theory of numbers*, John Wiley and Sons, New York, 1972.