Ile jest liczb pierwszych?

Już Euklides wiedział, że liczb pierwszych jest nieskończenie wiele, jednak pierwsze twierdzenie o rozmieszczeniu liczb pierwszych zostało udowodnione w 1850 roku przez rosyjskiego matematyka Czebyszewa. Podał on oszacowanie liczby liczb pierwszych wśród liczb $1, 2, \ldots, n$. Tę liczbę oznacza się przez $\pi(n)$. Czebyszew udowodnił, że

$$0{,}92\,\frac{n}{\ln n} < \pi(n) < 1{,}06\,\frac{n}{\ln n},$$

dla dostatecznie dużych n.
Obecnie znane są znacznie lepsze oszacowania, np.

$$\frac{n}{\ln n+2} < \pi(n) < \frac{n}{\ln n-4} \quad \text{dla } n \geqslant 55,$$

ale dowód Czebyszewa wart jest przytoczenia w *Delcie*.

Udowodnimy słabsze oszacowania

(*) $\pi(n) < 2\cdot\dfrac{n}{\ln n}$,

(**) $0{,}6\,\dfrac{n}{\ln n} < \pi(n)$ dla $n \geqslant 3$.

Dowód nierówności (*) jest indukcyjny. Najpierw bezpośrednio sprawdzamy dla $n \leqslant 200$.

Oto liczby pierwsze nie większe od 200:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.

Krok indukcyjny jest nieco nietypowy.
Zakładamy, że nierówność (*) jest prawdziwa dla $n = k$, gdzie $k \geqslant 100$ i dowodzimy, że jest prawdziwa dla $n = 2k$ i $n = 2k+1$. Mamy

$$\binom{2k}{k} = \frac{2k\cdot(2k-1)\cdot\ldots\cdot 1}{(k\cdot(k-1)\cdot\ldots\cdot 1)^2}.$$

Każda liczba pierwsza p, spełniająca nierówność $k < p < 2k$, jest dzielnikiem licznika tego ułamka, a nie dzieli mianownika. Tak więc dzieli ona $\binom{2k}{k}$. Iloczyn wszystkich takich liczb też dzieli $\binom{2k}{k}$. Ponieważ jest w nim $\pi(2k)-\pi(k)$ czynników, z których każdy jest większy niż k, więc otrzymujemy

$$k^{\pi(2k)-\pi(k)} < \binom{2k}{k} < \binom{2k}{0}+\binom{2k}{1}+\ldots+\binom{2k}{2k} = (1+1)^{2k} = 2^{2k}$$

i logarytmując

$$\pi(2k)-\pi(k) < \frac{2k\ln 2}{\ln k} < 1{,}4\,\frac{k}{\ln k}.$$

Z założenia indukcyjnego $\pi(k) < 2\,\dfrac{k}{\ln k}$. Dodając obie nierówności mamy

$$\pi(2k) < 3{,}4\,\frac{k}{\ln k}.$$

Zauważmy, że dla $k \geqslant 100$

$$\ln(2k) = \ln 2+\ln k = \ln k\left(1+\frac{\ln 2}{\ln k}\right) \leqslant \ln k\left(1+\frac{\ln 2}{\ln 100}\right) < 1{,}16\ln k.$$

Tak więc

$$\pi(2k) < \frac{3{,}4}{2}\,1{,}16\,\frac{2k}{\ln(2k)} = 2\,\frac{2k}{\ln(2k)} - 0{,}028\,\frac{2k}{\ln(2k)}.$$

Mamy zatem $\quad \pi(2k) \leqslant 2\,\dfrac{2k}{\ln(2k)}$

oraz

$$\pi(2k+1) \leqslant \pi(2k)+1 < 2\,\frac{2k}{\ln(2k)} + \left(1-0{,}028\,\frac{2k}{\ln(2k)}\right) \leqslant$$

$$\leqslant 2\,\frac{2k+1}{\ln(2k+1)} + \left(1-0{,}028\,\frac{200}{\ln 200}\right) < 2\,\frac{2k+1}{\ln(2k+1)}.$$

Korzystaliśmy tu z tego, że ciąg $\left(\dfrac{n}{\ln n}\right)_{n=3}^{\infty}$ jest rosnący.

Dla udowodnienia (**) zauważmy najpierw, że wykładnik największej potęgi p (p — liczba pierwsza) dzielącej $n!$ jest równy $\left[\dfrac{n}{p}\right] + \left[\dfrac{n}{p^2}\right] + \ldots$ (Suma jest skończona, gdyż dla $i > \dfrac{\ln n}{\ln p}$ mamy $\dfrac{n}{p^i} < 1$.) Wśród liczb $1, \ldots, n$ jest bowiem dokładnie $\left[\dfrac{n}{p}\right]$ liczb podzielnych przez p i $\left[\dfrac{n}{p^2}\right]$ podzielnych przez p^2, itd. Tak więc wykładnik największej potęgi p dzielącej $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ jest równy

$$\left(\left[\frac{n}{p}\right]-\left[\frac{k}{p}\right]-\left[\frac{n-k}{p}\right]\right)+\left(\left[\frac{n}{p^2}\right]-\left[\frac{k}{p^2}\right]-\left[\frac{n-k}{p^2}\right]\right)+\ldots$$

Każdy składnik tej sumy może być równy 0 lub 1 (bo $[a]+[b] \leqslant [a+b] \leqslant [a]+[b]+1$) i jest ich nie więcej niż $\dfrac{\ln n}{\ln p}$. A zatem jeśli p^r dzieli $\binom{n}{k}$, to $p^r \leqslant n$. Rozkładając liczbę $\binom{n}{k}$ na czynniki pierwsze otrzymujemy

$$\binom{n}{k} = 2^{r_1}\cdot 3^{r_2}\cdot\ldots\cdot p_j^{r_j} \leqslant n^j,$$

gdzie j jest liczbą liczb pierwszych nie większych niż n, a więc $i = \pi(n)$. Zatem

$$2^n = (1+1)^n = \binom{n}{0}+\ldots+\binom{n}{n} \leqslant (n+1)n^{\pi(n)}$$

i po zlogarytmowaniu

$$\pi(n) \geqslant \frac{n\ln 2}{\ln n} - \frac{\ln(n+1)}{\ln n} > 0{,}6\,\frac{n}{\ln n} \quad \text{dla } n \geqslant 40.$$

Dla $3 \leqslant n < 40$ sprawdzamy bezpośrednio prawdziwość nierówności (**).

Opracował *J. R.*