Przerwy w liczbach pierwszych

Wojciech CZERWIŃSKI

Wielu Czytelników słyszało zapewne o twierdzeniu Czebyszewa, mówiącym, że dla każdej liczby naturalnej n w przedziale $(n, 2n]$ istnieje jakaś liczba pierwsza. Jednak już jego dowód nie jest tak znany. A szkoda, bo jest niebywale elegancki i daje się prześledzić bez wiedzy spoza zakresu liceum. Poniższy tekst jest oparty na rozdziale książki *Dowody z księgi* autorstwa Martina Aignera i Güntera M. Zieglera.

Najpierw trochę historii. W 1845 roku Joseph Bertrand sformułował hipotezę twierdzącą, że „odległość od najbliższej liczby pierwszej nie może być większa niż liczba, od której zaczynamy poszukiwania". Dlatego też niekiedy omawiane twierdzenie nazywane jest hipotezą Bertranda. Sam Bertrand udowodnił swoją hipotezę dla liczb $n < 3000000$. W 1850 roku Pafnutij Czebyszew znalazł pierwszy pełny dowód dla wszystkich liczb naturalnych. My przedstawimy dowód autorstwa słynnego Paula Erdösa, który publikując go w 1932 roku, miał zaledwie 19 lat.

Najpierw wykażemy prawdziwość twierdzenia dla liczb $n < 4000$. Zauważmy, że nie musimy sprawdzać wszystkich przypadków, a wystarczy jedynie wskazać ciąg liczb pierwszych, z których każda jest mniejsza niż dwukrotność poprzedniej. Przykładowy taki ciąg to

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001.$$

Zajmijmy się więc dowodem dla $n \geqslant 4000$. W tym celu będziemy przyglądać się liczbie $\binom{2n}{n}$. Oszacujemy ją z dołu i z góry. Następnie okaże się, że przy założeniu, że nie ma żadnych liczb pierwszych w przedziale $(n, 2n]$, dojdziemy do sprzeczności.

Wykażmy na początek dosyć proste oszacowanie dolne. Dla dowolnego $n \geqslant 1$ zachodzi

$$\frac{4^n}{2n} \leqslant \binom{2n}{n}. \tag{1}$$

Jest tak, gdyż $4^n = \sum_{k=0}^{2n} \binom{2n}{k}$, a wartość $\binom{2n}{n}$ jest największą spośród $2n$ liczb: $\binom{2n}{0} + \binom{2n}{2n}, \binom{2n}{1}, \binom{2n}{2}, \ldots, \binom{2n}{2n-1}$.

Przejdziemy teraz do oszacowania górnego, które otrzymamy w kilku krokach. Pierwsze oszacowanie, które będzie nam pomocne za moment, jest samo w sobie bardzo interesujące. Pokażemy, że

$$\prod_{p \in \mathrm{P}(1,n]} p \leqslant 4^{n-1}, \tag{2}$$

dla wszystkich $n \in \mathbb{N}, n \geqslant 2$, gdzie $\mathrm{P}(i, j]$ to zbiór zawierający wszystkie liczby pierwsze w przedziale $(i, j]$. Zauważmy najpierw, że wystarczy udowodnić ten fakt tylko dla liczb pierwszych. Wówczas niech q będzie największą liczbą pierwszą nie większą niż n. Dostajemy

$$\prod_{p \in \mathrm{P}(1,n]} p = \prod_{p \in \mathrm{P}(1,q]} p \leqslant 4^{q-1} \leqslant 4^{n-1}.$$

Udowodnimy więc (2) przez indukcję. Dla $n = 2$ mamy $2 \leqslant 4$, więc jest to prawda. Aby wykonać krok indukcyjny, załóżmy, że nierówność (2) jest prawdziwa dla wszystkich liczb pierwszych mniejszych od liczby pierwszej $q = 2m + 1$. Mamy

$$\prod_{p \in \mathrm{P}(1,2m+1]} p = \prod_{p \in \mathrm{P}(1,m+1]} p \cdot \prod_{p \in \mathrm{P}(m+1,2m+1]} p \leqslant 4^m \cdot \binom{2m+1}{m} \leqslant 4^m 2^{2m} = 4^{2m}.$$

Nierówność

$$\prod_{p \in P[1,m+1]} p \leqslant 4^m$$

wynika z założenia indukcyjnego. Nierówność

$$\prod_{p\in P(m+2,2m+1]} p \leqslant \binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$

natomiast wynika z tego, że wszystkie liczby pierwsze w $\mathrm{P}(m+1,2m+1]$ dzielą licznik $(2m+1)!$, ale nie dzielą mianownika $n!(n+1)!$. Ostatnia nierówność $\binom{2m+1}{m} \leqslant 2^{2m}$ wynika zaś z tego, że $\sum_{k=0}^{2m+1}\binom{2m+1}{k} = 2^{2m+1}$ oraz dwa z tych wyrazów to $\binom{2m+1}{m}$ i $\binom{2m+1}{m+1} = \binom{2m+1}{m}$.

Przypomnijmy teraz twierdzenie Legendre'a, mówiące, że w rozkładzie liczby $n!$ na czynniki pierwsze liczba pierwsza p pojawia się dokładnie $\sum_{k\geqslant 1}\left\lfloor \frac{n}{p^k}\right\rfloor$ razy. Łatwo je udowodnić, zauważając, że w iloczynie $1\cdot 2\cdot \ldots \cdot n$ dokładnie $\frac{n}{p}$ liczb jest podzielnych przez p, dokładnie $\frac{n}{p^2}$ jest podzielnych przez p^2, itd.

Przypomnijmy też, że $\binom{2n}{n} = \frac{(2n)!}{n!\cdot n!}$. Z twierdzenia Legendre'a łatwo wywnioskować, że dowolna liczba pierwsza dzieli $\frac{(2n)!}{n!\cdot n!}$ w potędze dokładnie

$$\sum_{k\geqslant 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right).$$

Dla dowolnych liczb $a,b\in\mathbb{N}$ liczba $\left\lfloor \frac{2a}{b}\right\rfloor - 2\left\lfloor \frac{a}{b}\right\rfloor$ jest równa albo 0, albo 1. Dodatkowo dla $p^k > 2n$ wartości $\left\lfloor \frac{2n}{p^k}\right\rfloor$ oraz $\left\lfloor \frac{n}{p^k}\right\rfloor$ są równe zeru. Zatem otrzymujemy, że liczba pierwsza p dzieli $\binom{2n}{n}$ w potędze dokładnie

$$\sum_{k\geqslant 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right) \leqslant \sum_{k\geqslant 1, p^k\leqslant 2n} 1 = \max\{r \mid p^r \leqslant 2n\}. \tag{3}$$

Możemy więc przejść do właściwego oszacowania. Będziemy się zastanawiać, ile razy różne liczby pierwsze występują w rozkładzie $\binom{2n}{n}$ na czynniki pierwsze. Zauważmy najpierw, że z (3) wynika, iż dla dowolnego $p\in\mathrm{P}(1,n]$ potęga r jest taka, że $p^r\leqslant 2n$. A więc w szczególności liczby pierwsze $p > \sqrt{2n}$ występują tam co najwyżej jeden raz. Istotne jest spostrzeżenie, że liczby pierwsze p spełniające $\frac{2}{3}n < p \leqslant n$ wcale nie dzielą $n!$. Jest tak, gdyż dzielą zarówno licznik $(2n)!$, jak i mianownik $n!\cdot n!$ w potędze równej dwa. Otrzymujemy więc

$$\binom{2n}{n} \leqslant \prod_{p\in\mathrm{P}(1,\sqrt{2n}]} 2n \cdot \prod_{p\in\mathrm{P}(\sqrt{2n},\frac{2}{3}n]} p \cdot \prod_{p\in\mathrm{P}(n,2n]} p.$$

W połączeniu z (1) mamy

$$\frac{4^n}{2n} \leqslant \prod_{p\in\mathrm{P}(1,\sqrt{2n}]} 2n \cdot \prod_{p\in\mathrm{P}(\sqrt{2n},\frac{2}{3}n]} p \cdot \prod_{p\in\mathrm{P}(n,2n]} p. \tag{4}$$

Przypuśćmy teraz, że dla pewnego $n\in\mathbb{N}$ zbiór $\mathrm{P}(n,2n]$ jest pusty. Wówczas z (4) wynika, że

$$\frac{4^n}{2n} \leqslant \prod_{p\in\mathrm{P}(1,\sqrt{2n}]} 2n \cdot \prod_{p\in\mathrm{P}(\sqrt{2n},\frac{2}{3}n]} p \leqslant (2n)^{\sqrt{2n}}\cdot 4^{\frac{2}{3}n},$$

gdzie druga nierówność wynika z (2). Przekształcając, otrzymujemy

$$4^n \leqslant (2n)^{\sqrt{2n}+1}\cdot 4^{\frac{2}{3}n}$$

oraz

$$4^{\frac{1}{3}n} \leqslant (2n)^{\sqrt{2n}+1}, \tag{5}$$

co, jak zaraz wykażemy, nie jest prawdą dla $n\geqslant 4000$.

Korzystając z nierówności $k+1\leqslant 2^k$ prawdziwej dla $k\geqslant 2$, mamy

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

Dla liczb $n\geqslant 50$ dostajemy

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

gdzie pierwsza nierówność wynika z (5), następna z (6), a ostatnia z faktu, że $18 < 2\sqrt{2n}$ dla $n\geqslant 50$. Mamy więc $2^{2n} < 2^{20(2n)^{\frac{2}{3}}}$, czyli $2n < 20(2n)^{\frac{2}{3}}$, czyli $(2n)^{\frac{1}{3}} < 20$, czyli $n < 4000$. A zatem zbiór $P(n,2n]$ nie może być pusty dla liczb $n\geqslant 4000$, co kończy dowód twierdzenia Czebyszewa.