



Pochwała nieskończoności?

Mariusz SKAŁBA*

A w ósmy dzień Bóg stworzył liczby pierwsze. I stworzył ich nieskończenie wiele. I widział, że to było dobre. (apokryf z XXI wieku)

1. Niech $\pi(x)$ oznacza liczbę liczb pierwszych nie większych od x . Tak więc $\pi(x) \geq 1$ dla $x \geq 2$ oraz

$$\lim_{x \rightarrow \infty} \pi(x) = \infty,$$

co udowodnił już Euklides. Natomiast Czebyszew w połowie XIX wieku wykazał między innymi, że

$$\pi(2x) - \pi(x) \geq 1 \quad \text{dla } x \geq 1.$$

Jeszcze wcześniej Legendre udowodnił, że

$$(1) \quad \lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0.$$

I tu zaczyna się nasza historia. Z (1) wynika mianowicie, że dla każdego $x \geq 2$ istnieje $y > x$, takie że

$$\frac{\pi(y)}{y} < \frac{\pi(x)}{x}.$$

Czy dla dostatecznie dużych x można przyjąć $y = 2x$? Głównym celem tej notki jest uzasadnienie odpowiedzi twierdzącej na to pytanie – okaże się, że wymaga to użycia dość subtelnych metod. Mamy więc udowodnić, że istnieje $x_0 > 0$, takie że dla $x \geq x_0$ zachodzi nierówność

$$\frac{\pi(2x)}{2x} < \frac{\pi(x)}{x},$$

lub, co na jedno wychodzi, nierówność jej równoważna

$$(2) \quad \pi(2x) < 2\pi(x).$$

Nierówność (2) można wysłowić w ten sposób:

dla $x \geq x_0$ w przedziale $(0, x]$ jest więcej liczb pierwszych niż w przedziale $(x, 2x]$.

Pokażemy najpierw, że (2) nie wynika z następującej popularnej wersji twierdzenia o liczbach pierwszych

$$(3) \quad \lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Na mocy (3) możemy bowiem napisać

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) \quad \text{oraz} \quad \pi(2x) = \frac{2x}{\log 2x} + o\left(\frac{2x}{\log 2x}\right),$$

skąd otrzymujemy

$$2\pi(x) - \pi(2x) = \frac{(2 \log 2)x}{\log x(\log x + \log 2)} + o\left(\frac{x}{\log x}\right).$$

Widać, że wyraz główny może być zdominowany przez człon resztowy $o(\dots)$, a więc nie można wnioskować, że lewa strona jest dodatnia dla dostatecznie dużych x . Z powyższego oszacowania wynika „tylko”, że

$$\lim_{x \rightarrow \infty} \frac{\pi(2x)}{2\pi(x)} = 1.$$

Aby wykazać (2), trzeba skorzystać z następującej mocniejszej wersji twierdzenia o liczbach pierwszych

$$(4) \quad \pi(x) = \frac{x}{\log x} + \frac{x}{(\log x)^2} + o\left(\frac{x}{(\log x)^2}\right).$$

Po prostych rachunkach otrzymujemy stąd

$$2\pi(x) - \pi(2x) = \frac{(2 \log 2)x}{\log x(\log x + \log 2)} + o\left(\frac{x}{(\log x)^2}\right),$$

co daje

$$\lim_{x \rightarrow \infty} \frac{2\pi(x) - \pi(2x)}{x/(\log x)^2} = 2 \log 2 > 0,$$



Rozwiązanie zadania F 836.

Masa m przelewającej się wody zależy od wysokości h , na jakiej znajduje się jej powierzchnia nad poziomą krawędzią tamy, od przyspieszenia ziemskiego g , gęstości wody d i jest proporcjonalna do długości tamy L . Mamy:

$$\frac{dm}{dt} \propto h^\alpha g^\beta d^\delta L.$$

Porównanie wymiarów lewej i prawej strony równania prowadzi do wniosku, że $\alpha = 3/2$, $\beta = 1/2$, $\delta = 1$. Ostatecznie ilość wody (jej masa) przelewająca się w jednostce czasu wzrośnie $k^{3/2}$ razy.

*Instytut Matematyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski



a z tego (2) wynika natychmiast. Obie powyższe wersje twierdzenia o liczbach pierwszych (oszacowania (3) oraz (4)) są wnioskami z twierdzenia o liczbach pierwszych Hadamarda–de la Vallée-Poussina, udowodnionego przez tych matematyków niezależnie w 1896 roku w postaci

$$(5) \quad \pi(x) = \int_2^x \frac{dt}{\log t} + O(xe^{-c\sqrt{\log x}}),$$

gdzie $c > 0$ jest stałą absolutną. Rzeczywiście, dwukrotne całkowanie przez części prowadzi do

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right),$$

co na mocy (5) i prostej obserwacji

$$O(xe^{-c\sqrt{\log x}}) = O\left(\frac{x}{(\log x)^3}\right)$$

proceedzi do (4). Na zakończenie części 1. zauważmy, że hipotetyczne ulepszenie (5)

$$(6) \quad \pi(x) = \int_2^x \frac{dt}{\log t} + O(x^{1-\delta})$$

nie zostało, póki co, udowodnione dla żadnego $\delta > 0$. Natomiast to, że (6) zachodzi dla każdego $\delta \in (0, \frac{1}{2})$, jest równoważne hipotezie Riemanna, co udowodnił von Koch w 1901 roku.

2. To, że wielu interesujących pytań dotyczących liczb pierwszych nie można by w ogóle postawić, gdyby było ich tylko skończenie wiele, wykazano powyżej. Krótko mówiąc: analityczna teoria liczb nie miałyby racji bytu. W punkcie **2.** pokażemy pokrótce, że algebraiczna teoria liczb byłaby też dużo mniej pasjonująca. Z ogólnej teorii pierścieni Dedekinda wynika bowiem, że jeśli w takim pierścieniu jest tylko skończenie wiele ideałów pierwszych, to obowiązuje w nim twierdzenie o jednoznaczności rozkładu. To wygodne twierdzenie zachodziłoby więc w szczególności w pierścieniach cyklotomicznych $\mathbb{Z}[\omega_p]$, które są zbiorami liczb postaci

$$\mathbb{Z}[\omega_p] = \{a_0 + a_1\omega_p + \dots + a_{p-2}\omega_p^{p-2} \mid a_0, a_1, \dots, a_{p-2} \in \mathbb{Z}\},$$

gdzie p jest ustaloną liczbą pierwszą, a $\omega_p = \cos(2\pi/p) + i \sin(2\pi/p)$ jest pierwiastkiem pierwotnym p -tego stopnia z 1. Już Kummer udowodnił w połowie XIX wieku wspaniałe, ogólne twierdzenie o równaniu Fermata

$$(7) \quad x^p + y^p + z^p = 0,$$

z którego wynika, między innymi, że w przypadku jednoznaczności rozkładu w pierścieniu $\mathbb{Z}[\omega_p]$, równanie (7) możliwe jest tylko dla $xyz = 0$. Tak więc historia Wielkiego Twierdzenia Fermata *zakończyłaby się* ponad 150 lat temu i to niezależnie od tego, jak wielka *byłaby rzekomo skończona* moc zbioru wszystkich liczb pierwszych! Ale na szczęście (?) jest inaczej: liczb pierwszych jest nieskończenie wiele, a największą liczbą pierwszą p , taką, że w $\mathbb{Z}[\omega_p]$ zachodzi twierdzenie o jednoznaczności rozkładu, jest $p = 19$. Kummer, co prawda, we wspomnianym wyżej wspaniałym twierdzeniu zadowala się założeniem znacznie słabszym niż założenie o jednoznaczności rozkładu: aby udowodnić, że równanie (7) nie ma nietrywialnych rozwiązań, wystarczy mu założenie, iż tzw. *liczba klas ideałów* pierścienia $\mathbb{Z}[\omega_p]$ nie jest podzielna przez p . Warto wspomnieć, że metoda Kummera opiera się na następującym rozkładzie liczby $-z^p$ na czynniki:

$$-z^p = x^p + y^p = \prod_{k=0}^{p-1} (x + \omega_p^k y) \quad \text{dla } p > 2$$

oraz że na tej drodze nie udało się uzyskać pełnego dowodu Wielkiego Twierdzenia Fermata! Dowód Andrew Wilesa z 1995 r. opiera się na wnikliwym badaniu konsekwencji istnienia nietrywialnego rozwiązania równania (7) w nowoczesnej teorii krzywych eliptycznych – w ten sposób uzyskuje się upragnioną sprzeczność.



Można się z nią zapoznać, na przykład, z książek: J. Browkin, *Teoria ciał*, Warszawa 1978 oraz Z.I. Borewicz, I.R. Szafarewicz, *Teoria ciał*, Moskwa 1985.



A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. 141 (1995), 443–551.