Liczby ważniejsze od innych

Jarosław GÓRNICKI

Geometria i teoria liczb to dwie najstarsze gałęzie matematyki. W *Elementach* Euklidesa (napisanych około 300 roku p.n.e.) księgi VII, VIII i IX poświęcone są arytmetyce. W księdze VII wyróżnione są liczby pierwsze.

Liczbę naturalną $p > 1$ nazywamy **liczbą pierwszą**, *jeśli ma ona tylko dwa naturalne dzielniki: samą siebie oraz liczbę* 1.

Wśród liczb naturalnych mniejszych od 50 liczbami pierwszymi są:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Elementy zawierają dwie fundamentalne obserwacje dotyczące liczb pierwszych. Przypomnimy je wraz z uzasadnieniami (uzasadnienia te są wzorami rozumowań matematycznych).

Pierwszą obserwację zawiera twierdzenie 31 z księgi VII:

liczba naturalna $n > 1$, która nie jest liczbą pierwszą, zawsze ma czynnik pierwszy.

Jeśli $n > 1$ nie jest liczbą pierwszą (taką liczbę nazywamy *złożoną*), to ma ona czynnik naturalny d_1, $1 < d_1 < n$. Jeśli d_1 jest liczbą pierwszą, to twierdzenie jest dowiedzione. Jeśli d_1 jest liczbą złożoną, to ma czynnik naturalny d_2, $1 < d_2 < d_1$. Jeśli d_2 jest liczbą pierwszą, to dowód jest zakończony, w przeciwnym przypadku rozumowanie powtarzamy. Postępowanie to nie może mieć więcej niż n kroków i kończy się na liczbie d, $1 < d < n$, będącej liczbą pierwszą. Zatem liczba n ma czynnik pierwszy.

Obserwacja ta leży u podstaw tzw. *zasadniczego twierdzenia arytmetyki*, które orzeka, że

każdą liczbę naturalną $n > 1$ można rozłożyć na iloczyn liczb pierwszych w jeden tylko sposób

(gdy ignorujemy kolejność występowania czynników).

Potrzebę dowodu jednoznaczności rozkładu liczb na czynniki pierwsze dostrzegał już Euklides (rozumowanie zawarte w *Elementach* ma lukę). Precyzyjne sformułowanie *zasadniczego twierdzenia arytmetyki* wraz z dowodem podał C.F. Gauss (1777–1855) w swoich *Disquisitiones arithmeticae* (*Rozważaniach arytmetycznych*) dopiero w 1801 roku. Wcześniej przez ponad 2000 lat twierdzenie to przyjmowano za oczywiste. Dopiero w połowie XIX wieku (głównie dzięki pracom E. Kummera (1810–1893)) okazało się, że w pierścieniach liczbowych jednoznaczność rozkładu (z dokładnością do czynników odwracalnych, czyli takich, jak 1 i -1 w pierścieniu $\mathbb{Z}$) występuje raczej wyjątkowo. Na przykład, w pierścieniu $\mathbb{Z}[\sqrt{-5}]$ liczb postaci $a + b\sqrt{-5}$, $a, b \in \mathbb{Z}$, każda z liczb

$$3,\ 7,\ 1 + 2\sqrt{-5},\ 1 - 2\sqrt{-5}$$

jest nierozkładalna i

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Drugą z zapowiedzianych obserwacji zawiera twierdzenie 20 z księgi IX:

Liczb pierwszych jest nieskończenie wiele.

Dowód Euklidesa był przytoczony np. w *Delcie* 5/2002.

Kilka innych (późniejszych) dowodów istnienia nieskończenie wielu liczb pierwszych można znaleźć w [3]. Gdy już wiemy, że liczb pierwszych jest nieskończenie wiele, oraz że są one „cegiełkami", z których zbudowane są wszystkie liczby naturalne $n > 1$, to istotne są dwa pytania:

- ♠ jak rozpoznać, czy dana liczba naturalna jest liczbą pierwszą?
- ♠ jak są rozmieszczone liczby pierwsze?

Pytania te są wciąż aktualne, gdyż na żadne z nich nie znamy zadowalającej odpowiedzi. W przypadku pierwszego pytania, oczywiście, znamy teoretyczne metody pozwalające zbadać, czy dana liczba jest liczbą pierwszą – na przykład *sito Eratostenesa*. Kłopot polega na tym, że metoda ta jest praktycznie bezużyteczna dla dużych liczb. Ponadto, niestety, nie znamy żadnego algorytmu działającego w czasie wielomianowym, który pozwalałby rozłożyć dużą liczbę naturalną na czynniki pierwsze [2] (choć wiemy, że dla sprawdzenia, czy dana liczba naturalna $n > 4$ jest liczbą pierwszą, wystarczy tylko zbadać, czy $\frac{(n-1)!}{n}$ jest liczbą całkowitą). Problem ten okazał się bardzo ważny, gdy w 1976 roku W. Diffie i M.E. Hellman wskazali prosty sposób szyfrowania wiadomości (z jawnym kluczem), który z „technicznych" powodów jest niezwykle trudny do złamania (zob. [1], [3, str. 127]). (Z tego względu odnajdywane współcześnie olbrzymie liczby pierwsze w znakomitej większości nie są podawane do publicznej wiadomości.)

Drugie pytanie również okazało się interesujące. W 1744 roku L. Euler (1707–1783) udowodnił, że liczb pierwszych jest tak dużo, iż szereg

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

jest rozbieżny, i tak mało, że stosunek $\frac{\pi(x)}{x}$ zbiega do zera (symbol $\pi(x)$ oznacza liczbę liczb pierwszych nie większych od x). Obserwując odkrywane kolejno liczby pierwsze, zauważono, że pojawiają się one bardzo nieregularnie: zdarzają się ich skupiska, np.

$$1871,\ 1873,\ 1877,\ 1879,$$

bądź można wskazać ciąg kolejnych liczb naturalnych o zadanej z góry długości, wśród których nie ma liczby pierwszej.

Dla wybranego n ciąg taki tworzymy następująco:

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1).$$

Na podstawie analizy „materiału empirycznego” C.F. Gauss (w 1792 r., miał wtedy 15 lat(!) [3, str. 159]) i A.M. Legendre (1752–1833) (w 1798 r.) wysunęli przypuszczenie, że liczbę $\pi(x)$ można przybliżać wielkością $\frac{x}{\ln x}$ (choć nie jest to przybliżenie najlepsze).

x	$\pi(x)$	$\left[\frac{x}{\ln x}\right]$	$\frac{\pi(x)}{\frac{x}{\ln x}}$
1000	168	144	1,159
1000000	78498	72382	1,084
1000000000	50847534	48254942	1,053

Problem ten, łączący zjawiska dyskretne z ciągłymi(!), został uznany za niezwykle interesujący. W 1896 roku, korzystając z rezultatów P. Czebyszewa (1821–1894) i B. Riemanna (1826–1866), J. Hadamard (1865–1963) w Paryżu i Ch. de la Vallée Poussin (1866–1962) w Louvain udowodnili

twierdzenie o liczbach pierwszych:

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Twierdzenie to ma wiele ciekawych konsekwencji. Oto dwie z nich [5, str. 164–165]:

♠ Dla dowolnie wybranego skończonego ciągu cyfr $c_1, c_2, \ldots, c_m$ istnieje liczba pierwsza, której m początkowych cyfr stanowią wybrane cyfry (W. Sierpiński).

♠ Dla każdej liczby rzeczywistej $x > 0$ istnieje nieskończony ciąg liczb pierwszych $q_1, q_2, \ldots,$ taki że

$$\lim_{x\to\infty} \frac{q_n}{n} = x$$

(H. Steinhaus).

Z twierdzenia o liczbach pierwszych wynika również, że n-ta liczba pierwsza jest w przybliżeniu równa $n \ln n$ ($p_n \sim n \ln n$), co jest równoważne istnieniu dodatnich liczb A, B, takich że dla $n > 1$,

$$(1) \qquad A \cdot \ln n \leqslant \tfrac{p_n}{n} \leqslant B \cdot \ln n.$$

Korzystając z tych nierówności, wykażemy interesującą zależność między wszystkimi liczbami pierwszymi a „najważniejszą” liczbą w analizie [4]:

$$\lim_{n\to\infty} \sqrt[p_n]{p_1 \cdot p_2 \cdot \ldots \cdot p_n} = e.$$

Niech $I_n = \sqrt[p_n]{p_1 \cdot p_2 \cdot \ldots \cdot p_n}$.

Wówczas

$$(2) \quad \ln I_n = \frac{1}{p_n}\sum_{k=1}^{n} \ln p_k = \frac{1}{p_n}\sum_{k=1}^{n} \ln k + \frac{1}{p_n}\sum_{k=1}^{n} \ln \frac{p_k}{k} =$$

$$= \frac{1}{p_n} \ln n! + \frac{1}{p_n}\sum_{k=1}^{n} \ln \frac{p_k}{k}.$$

Stosując wzór J. Stirlinga (1692 – 1770)

$$n! \sim \sqrt{2\pi} \cdot n^{n+\frac{1}{2}} \cdot e^{-n},$$

otrzymujemy

$$\frac{1}{p_n} \ln n! \sim \frac{\ln\sqrt{2\pi}}{p_n} + \frac{\ln n}{2p_n} - \frac{n}{p_n} + \frac{n \ln n}{p_n} \xrightarrow[n\to\infty]{} 1,$$

gdyż przy n zmierzającym do nieskończoności, pierwsze trzy składniki ostatniej sumy dążą do zera, natomiast ostatni składnik (wobec zależności $p_n \sim n \ln n$) dąży do 1. Drugi składnik w ostatniej sumie wzoru (2), przy n zmierzającym do nieskończoności, dąży do zera, gdyż dzięki oszacowaniu

$$\ln \frac{p_k}{k} \leqslant \ln(B \cdot \ln k),$$

które wynika z (1), mamy

$$\frac{1}{p_n}\sum_{k=1}^{n} \ln \frac{p_k}{k} \leqslant \frac{n}{p_n} \ln(B \cdot \ln n) \leqslant \frac{1}{A \cdot \ln n} \ln(B \cdot \ln n) =$$

$$= \frac{\ln B}{A \cdot \ln n} + \frac{\ln(\ln n)}{A \cdot \ln n} \xrightarrow[n\to\infty]{} 0.$$

Zatem

$$\lim_{n\to\infty} \ln I_n = 1,$$

a to daje tezę.

W teorii liczb (w tym w teorii liczb pierwszych) wiele jest pytań, na które nie znamy odpowiedzi, np.:

♠ Czy każda liczba naturalna $n > 5$ jest sumą trzech liczb pierwszych? Czy każda liczba naturalna parzysta $n \geqslant 4$ jest sumą dwóch liczb pierwszych? (Odpowiedź twierdząca znana jest jako *hipoteza Goldbacha.*)

♠ Ile jest par liczb pierwszych różniących się o 2 (np. 5 i 7, 11 i 13, 17 i 19, …, 10006427 i 10006429, …, $260497545 \cdot 2^{6625} \pm 1$, itd.)?

♠ Czy dla każdego naturalnego n istnieje liczba pierwsza między n^2 a $(n+1)^2$?

Przy każdej okazji należy je przypominać. Może akurat ktoś z Czytelników otworzy kolejne drzwi i weźmie udział w fascynującej przygodzie…

Literatura:

[1] W. Guzicki, *Szyfry z kluczem publicznym, Delta* 3/1997, 1-3.

[2] W. Guzicki, *Jak rozpoznajemy liczby pierwsze, Delta* 4/1997, 1–4.

[3] P. Ribenboim, *Mała księga wielkich liczb pierwszych,* WNT, Warszawa 1997.

[4] S.M. Ruiz, *A result on prime numbers,* Math. Gaz. 81 (1997), 269–270.

[5] W. Sierpiński, *Elementary theory of numbers* (A. Schinzel, red.), PWN, Warszawa 1987.