Ciągi arytmetyczne liczb pierwszych

W 2004 roku rozwiązany został bardzo znany problem dotyczący liczb pierwszych, wydaje się więc, że jest to wystarczający powód, aby tytuł *Aktualności* wziąć serio i poświęcić je teorii liczb, nie zaś fizyce. Otóż, B. Green i T. Tao [1] udowodnili następujący wynik.

Twierdzenie. *Dla każdej liczby naturalnej $k \geqslant 3$ istnieje nieskończenie wiele k-wyrazowych ciągów arytmetycznych, złożonych z samych liczb pierwszych.*

Dla $k = 5$ przykładem jest m.in. ciąg 5, 11, 17, 23, 29, a dla $k = 22$ – znaleziony przez Morana, Pritcharda i Thyssena ciąg $11410337850553 + 4609098694200j$, gdzie $j = 0, 1, \ldots, 21$. Przypadek $k = 3$ w powyższym twierdzeniu udowodnił van der Corput już w 1933 roku.

Z dowodu wynika, że pewien ciąg arytmetyczny złożony z k liczb pierwszych ma wszystkie wyrazy mniejsze od

$$2^{2^{2^{2^{2^{2^{2^{100k}}}}}}}, \tag{1}$$

ale zapewne jest to oszacowanie wysoce nieoptymalne.

Wynik Greena i Tao jest szczególnym przypadkiem następującej klasycznej hipotezy.

Hipoteza (Erdős, Turán 1936). *Jeśli rosnący ciąg $A = (a_n)$ liczb naturalnych ma tę własność, że*

$$\sum_{n=1}^{\infty} \frac{1}{a_n} = +\infty\,,$$

to A zawiera dowolnie długie ciągi arytmetyczne.

Ciąg liczb pierwszych spełnia założenia tej hipotezy, gdyż szereg odwrotności wszystkich liczb pierwszych jest rozbieżny. (Więcej na ten temat – w artykule *Sumowanie odwrotności* w *Delcie* 9/1999.)

Hipotezę związaną z ciągami arytmetycznymi liczb pierwszych sformułowali w 1923 roku Hardy i Littlewood. Spróbujmy ją wysłowić choćby w przybliżeniu. Dla ustalonego k niech $L(k, n)$ oznacza liczbę wszystkich takich ciągów arytmetycznych, które mają długość k, są złożone z samych liczb pierwszych i są zawarte w zbiorze $\{1, 2, \ldots, n\}$. Otóż, Hardy i Littlewood wysunęli przypuszczenie, że

$$\lim_{n\to\infty} \frac{L(k,n)}{n^2/(\log n)^k} = C_k, \tag{2}$$

gdzie C_k jest konkretną stałą, daną wzorem na tyle strasznym, że nie będziemy go tu przytaczać, lecz na tyle wygodnym, że można C_k wyznaczyć z dowolną dokładnością. Wspomnimy tylko dla przykładu, że

$$C_3 = \frac{3}{2} \prod_{p\geqslant 5} \left(1 + \frac{1}{(p-1)^3}\right) = 1{,}53\ldots$$

Innymi słowy, jeśli k jest ustalone, to dla dużych n liczba ciągów arytmetycznych długości k, złożonych z samych liczb pierwszych nie większych od n, jest, z dokładnością do konkretnego stałego czynnika, równa z grubsza $n^2/(\log n)^k$. Powinno więc być takich ciągów dużo, bo $n^2/(\log n)^k \to \infty$ dla $n \to \infty$.

Green i Tao nie potrafią udowodnić pełnej hipotezy Hardy'ego i Littlewooda. Z ich dowodu wynika jednak, że liczba $L(n, k)$ rośnie przy ustalonym k nie wolniej, niż $c_k n^2/(\log n)^k$, gdzie c_k jest pewną stałą dodatnią – niestety – dużo mniejszą od C_k.

Dowód twierdzenia Greena i Tao wykorzystuje różne techniki analizy matematycznej, teorii układów dynamicznych i rachunku prawdopodobieństwa. Są w nim trzy zasadnicze składniki. Pierwszy z nich to słynny wynik Szemerédiego z 1975 roku.

Twierdzenie. *Niech A będzie takim rosnącym ciągiem liczb naturalnych, że dla pewnej liczby dodatniej ε jest*

$$\frac{\overline{\overline{A \cap [1, N]}}}{N} > \varepsilon \quad \textit{dla nieskończenie wielu } N.$$

Wtedy A zawiera dowolnie długie ciągi arytmetyczne.

To bardzo trudne twierdzenie; jego istotnie nowy dowód był jednym z powodów, dla których W.T. Gowers otrzymał w 1998 roku medal Fieldsa.

Drugi składnik, a zarazem zasadniczy pomysł Greena i Tao, to uogólnienie twierdzenia Szemerédiego ze zbioru liczb naturalnych na dowolne jego pseudolosowe podzbiory. Mniejsza tu o ścisłą definicję pseudolosowości; chodzi o to, że jeśli w nieskończonym pseudolosowym zbiorze liczb naturalnych Z mamy mniejszy, dowolny, byle „w miarę gęsty” podzbiór P – tzn. podzbiór P, zawierający w dobrze zdefiniowanym sensie ustalony dodatni procent elementów zbioru Z – to wówczas P zawiera dowolnie długie ciągi arytmetyczne.

Trzeci składnik to konstrukcja odpowiedniego zbioru pseudolosowego Z, zawierającego m.in. wszystkie liczby pierwsze. Zasadniczą część zbioru Z stanowią te liczby n, których wszystkie dzielniki pierwsze są większe od $\sqrt[m]{n}$, gdzie m jest stałą zależną od k. Z uwagi na techniczny wymóg pseudolosowości trzeba dorzucić jeszcze odrobinę innych liczb. W takim zbiorze Z zbiór wszystkich liczb pierwszych P jest „w miarę gęsty” (wśród N początkowych elementów zbioru Z jest co najmniej εN liczb pierwszych, gdzie $\varepsilon = \varepsilon(k) > 0$).

I to już, w telegraficznym skrócie, wszystko. Wystarczy do takiego zbioru Z i jego „w miarę gęstego” podzbioru P zastosować uogólnione twierdzenie Szemerédiego.

Paweł STRZELECKI

Literatura

[1] Green, T. Tao. *The primes contain arbitrarily long arithmetic progressions*. (Preprint, 50 str.)

[2] Tao. *Arithmetic progressions and the primes – El Escorial lectures*. (Preprint, 38 str.)

Oba preprinty można łatwo wyszukać w elektronicznym archiwum `http://www.arxiv.org/`