Jedno zdanie

Nieparzysta liczba pierwsza p może być przedstawiona jako suma dwóch kwadratów liczb naturalnych

$$p = x^2 + y^2 \tag{1}$$

wtedy i tylko wtedy jeśli $p \equiv 1 \pmod 4$. Taką hipotezę postawił w 1625 roku Albert Girard, a w 1640 roku również Pierre de Fermat i to z jego powodu ten fakt nazywany jest teraz twierdzeniem Fermata o sumie dwóch kwadratów.

Jednak żaden z powyższych matematyków nie udowodnił postawionej hipotezy. Zrobił to dopiero w 1747 roku Leonard Euler, jego dowód był jednak dosyć skomplikowany. Potem pojawiały się kolejne, coraz prostsze dowody, udział wzięli m.in. Lagrange w 1775 roku i Dedekind w 1877 roku. Aż w końcu parę lat temu, w roku 1990, Don Zagier, amerykański matematyk, przedstawił dowód, który miał dokładnie *jedno* zdanie. Aby je zobaczyć polecam spojrzeć tu:

`people.mpim-bonn.mpg.de/zagier/files/doi/10.2307/2323918/fulltext.pdf`.

Przedstawimy tutaj ten dowód w nieco większej, ale wciąż małej liczbie zdań. Po pierwsze, zauważmy, że jeśli $p \not\equiv 1 \pmod 4$ i p jest nieparzysta, to $p \equiv 3 \pmod 4$. Zatem w oczywisty sposób p nie jest sumą dwóch kwadratów, bo każdy kwadrat przystaje do 0 lub 1 modulo 4.

Ustalmy taką liczbę p, że $p \equiv 1 \pmod 4$. Do dowodu twierdzenia wystarczy wykazać, że równanie $p = x^2 + y^2$ ma przynajmniej jedno rozwiązanie. Przyjrzyjmy się dokładniej innemu równaniu

$$p = x^2 + 4yz. \tag{2}$$

Wykażemy, że ma ono nieparzyście wiele rozwiązań. Nim to jednak zrobimy zobaczmy, jak z tego wynika, że $p = x^2 + y^2$ ma rozwiązanie. Zauważmy, że jeśli (x, y, z) jest rozwiązaniem (2), to (x, z, y) również. A więc rozwiązania równania (2) łączą się w pary, oprócz takich rozwiązań, że $(x, y, z) = (x, z, y)$, czyli gdy $y = z$. Ponieważ, jak wykażemy wkrótce, rozwiązań (2) jest nieparzyście wiele, to nie wszystkie mogą połączyć się w pary i istnieje pewne rozwiązanie takie, że $y = z$. A to oznacza, że mamy $p = x^2 + 4y^2 = x^2 + (2y)^2$, czyli również (1) ma rozwiązanie.

Żeby wykazać, że (2) ma nieparzyście wiele rozwiązań, stosujemy podobną metodę co poprzednio. Rozważmy przekształcenie

$$f(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) & \text{jeśli } x \leqslant y - z \\ (2y - x, y, x - y + z) & \text{jeśli } y - z < x \leqslant 2y \\ (x - 2y, x - y + z, y) & \text{jeśli } x > 2y. \end{cases} \tag{3}$$

Okazuje się, że jeśli (x, y, z) rozwiązuje równanie (2), to $f(x, y, z)$ również, ponadto po dwukrotnym zastosowaniu funkcji f do trójki (x, y, z) otrzymujemy ponownie (x, y, z), co Czytelnik Cierpliwy może sprawdzić samodzielnie. A więc funkcja f może nam posłużyć do sparowania rozwiązań równania (2): (x, y, z) jest w parze z $f(x, y, z)$. Jedyne rozwiązania, które nie stoją w parach, to te, dla których $(x, y, z) = f(x, y, z)$. Okazuje się, że takie rozwiązania można jedynie otrzymać za pomocą środkowej linii definicji (3), czyli dla

$$(x, y, z) = (2y - x, y, x - y + z). \tag{4}$$

Łatwo sprawdzić, że linia pierwsza i trzecia dawałaby $(x, y, z) = (0, 0, 0)$, co oczywiście nie spełnia równania (2). Dla (4) otrzymujemy $x = y$, czyli $p = x^2 + 4xz = x(x + 4z)$. Musi to oznaczać $x = 1$, więc $y = 1$ oraz $z = \frac{p-1}{4}$, czyli jest tylko jedno rozwiązanie (2), które nie stoi w parze: $(1, 1, \frac{p-1}{4})$. A zatem rozwiązań (2) jest nieparzyście wiele, co kończy dowód.

Wojciech CZERWIŃSKI