Twierdzenie Fermata o rozkładzie liczby pierwszej na sumę kwadratów

Klasyczne już dziś twierdzenie Fermata mówi, że każda liczba pierwsza p postaci $4n+1$ jest sumą dwóch kwadratów: $p = a^2 + b^2$. Znamy wiele dowodów tego twierdzenia. Chyba najkrótszy został niedawno opublikowany przez D. Zagiera w *American Mathematical Monthly*. Zapoznajmy się z tym dowodem.

Rozważmy skończony zbiór S zdefiniowany następująco:

$$S = \{(x,y,z) \in \mathbf{N}^3 : x^2 + 4yz = p\}$$

oraz funkcję $f : S \to S$ określoną wzorem:

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

Funkcja f jest inwolucją, tzn. dla dowolnej trójki liczb $(x,y,z) \in S$ zachodzi równość $f(f(x,y,z)) = (x,y,z)$.

Zauważamy następnie, że trójka $(1,1,n)$ jest punktem stałym funkcji f : $f(1,1,n) = (1,1,n)$. Jest to przy tym jedyny punkt stały tej funkcji. Inny punkt stały dawałby bowiem rozkład liczby p na iloczyn dwóch liczb całkowitych. Wynika stąd, że zbiór S ma nieparzystą liczbę elementów.

Weźmy teraz nową funkcję $g : S \to S$ daną wzorem

$$g(x,y,z) = (x,z,y).$$

Ta funkcja jest również inwolucją: $g(g(x,y,z)) = (x,y,z)$. Zbiór S ma nieparzystą liczbę elementów, a więc funkcja g musi mieć co najmniej jeden punkt stały: $g(x,y,z) = (x,y,z)$.

Ale wtedy $y = z$, czyli $p = x^2 + 4yz = x^2 + 4y^2 = x^2 + (2y)^2$, co kończy dowód twierdzenia. Pominięte szczegóły dowodu pozostawię Czytelnikowi jako bardzo łatwe ćwiczenie.

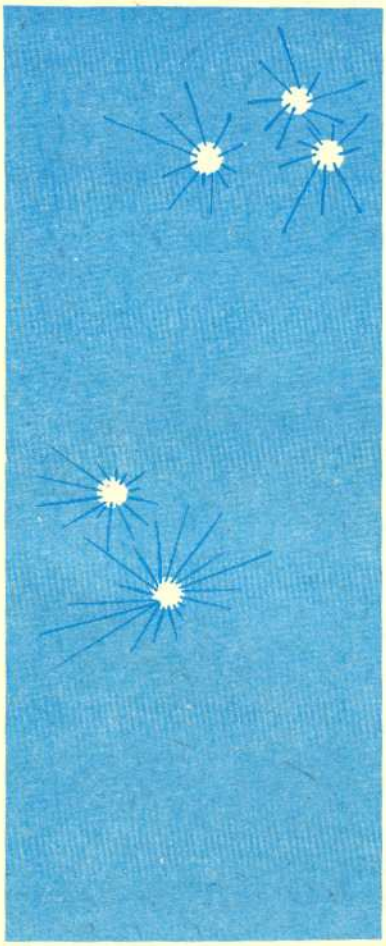
Przeprowadzony wyżej dowód twierdzenia Fermata jest bardzo prosty, ale ma jedną zasadniczą wadę. Nie pokazuje on, w jaki sposób można znaleźć takie liczby a i b, że $p = a^2 + b^2$. Jest on całkowicie niekonstruktywny. Znamy wiele dowodów tego twierdzenia dających różne metody otrzymywania liczb a i b. Uzyskiwane w ten sposób algorytmy mają różne własności, jedne działają szybciej, inne wolniej.

Bardzo ładne wzory podał Gauss. Jeśli $p = 4n+1$ oraz przez $\langle x \rangle$ oznaczymy taką „resztę" z dzielenia x przez p, że $|\langle x \rangle| < \frac{p}{2}$, (tzn. $x = q \cdot p + \langle x \rangle$ oraz $|\langle x \rangle| < \frac{p}{2}$), to:

$$a = \left\langle \frac{1}{2} \cdot \binom{2n}{n} \right\rangle, \qquad b = \langle (2n)! \cdot a \rangle .$$

Te wzory, niestety, też są zupełnie nieprzydatne w praktyce. Do obliczenia liczby $(2n)!$ trzeba wykonać $2n$ mnożeń. Jeśli liczba n ma kilkadziesiąt cyfr, to takie obliczenia trwałyby co najmniej miliardy lat. Przy wyznaczaniu liczb a i b, zgodnie z algorytmem danym przez wzory Gaussa, musimy wykonać liczbę działań proporcjonalną do liczby p. Dla dużych liczb p jest to niewykonalne. Jesteśmy więc zainteresowani znalezieniem algorytmu szybkiego i prostego. Są takie algorytmy. Jeden z nich przedstawiamy w tym numerze *Delty* (str. 10).

doc. dr Wojciech GUZICKI



Zadania

Redaguje mgr Michał WOJCIECHOWSKI

M 583. Czy szachownicę o wymiarach $4 \times n$ można obejść ruchem konika szachowego tak, by na każdym polu stać dokładnie raz i w ostatnim posunięciu wrócić na pole startu?
Rozwiązanie na str. 1.

M 584. Czy w prostokąt o stosunku długości boków 9 : 16 można wpisać prostokąt o stosunku długości boków 4 : 7, tak by na każdym boku pierwszego prostokąta leżał wierzchołek drugiego?
Rozwiązanie na str. 1.

M 585. Udowodnić, że nie istnieje wielomian dodatniego stopnia o współczynnikach całkowitych, którego wartości we wszystkich punktach całkowitych są liczbami pierwszymi.
Rozwiązanie na str. 1.

Redaguje dr Krzysztof CHARCHUŁA

F 296. Rakieta wyposażona w impulsowy silnik odrzutowy, pozwalający zmieniać prędkość w ciągu bardzo krótkiego czasu, krąży wokół Ziemi po orbicie kołowej. Jak użyć tego silnika, aby przemieścić rakietę na orbitę również kołową, ale o nieco większym promieniu?
Rozwiązanie na str. 16.

F 297. Do szklanki o średnicy d i wysokości h nalano wody. Przy jakim poziomie wody środek masy układu: szklanka + woda przyjmie najniższe położenie? Przyjąć, że ścianki i dno szklanki są jednorodne i mają gęstość powierzchniową μ, woda zaś gęstość objętościową ρ.
Rozwiązanie na str. 3.