Przykłady „paczek”

Dwie „paczki” kwadratowe liczb naturalnych a^2 i b^2 dają „paczkę” kwadratową c^2 (czyli $a^2 + b^2 = c^2$) wtedy i tylko wtedy, gdy istnieją takie liczby naturalne p, q, r, że a i b to $r(p^2 - q^2)$ i $2rpq$ oraz c to $r(p^2 + q^2)$.

Przykłady takich trójek liczb a, b, c były znane już Sumerom, a ich kojarzenie z geometrią, czyli długościami boków trójkątów prostokątnych (gdzie nie jest wymagane, by były to liczby całkowite), jest o blisko 2 tysiące lat późniejsze, już greckie. I wtedy powstaje nazwa „trójki pitagorejskie” (nazwa zaś „trójkąt egipski” dla trójkąta o bokach 3, 4, 5, to XIX-wieczny wymysł dydaktyków).

Dowód, że tak wyglądają wszystkie trójki pitagorejskie, przypisujemy Diofantosowi (I wiek).

W jego pracach znajdujemy też spostrzeżenie, że iloczyn dwóch sum dwóch „paczek” kwadratowych jest sumą dwóch (innych) „paczek” kwadratowych, (czyli dla całkowitych a, b, c, d istnieją takie całkowite p, q, że

$$(a^2 + b^2)(c^2 + d^2) = p^2 + q^2).$$

Mianowicie jest tak dla $p = (ac - bd)$ i $q = (ad + bc)$

oraz dla $p = (ac + bd)$ i $q = (ad - bc)$.

Np. dla 2, 5, 4 i 3 mamy 7 i 26 lub 23 i 14, bo $(4 + 25)(16 + 9) = (8 - 15)^2 + (6 + 20)^2 = (8 + 15)^2 + (6 - 20)^2$, czyli $29 \cdot 25 = 49 + 676 = 529 + 196$.

Wytłumaczyć to spostrzeżenie, gdy zna się liczby zespolone, jest łatwo: to fakt, że moduł iloczynu jest równy iloczynowi modułów – Diofantos, rzecz jasna, liczb zespolonych nie znał.

„Paczki” kwadratowe występują w twierdzeniu Lagrange’a (XVIII wiek), że każda liczba całkowita nieujemna jest równa sumie czterech kwadratów liczb naturalnych. Niedługo potem Euler wykazał, że każda taka liczba jest sumą dziewięciu sześcianów liczb naturalnych.

Dało to asumpt Edmundowi Waringowi do postawienia hipotezy, iż coś podobnego dotyczy również wszelkich „paczek” potęgowych (dalej nie będę już używał słowa *paczki*). Mianowicie dla każdego naturalnego n istnieje taka liczba naturalna m, że dowolna liczba naturalna k da się przedstawić jako suma długości m złożona z n-tych potęg liczb całkowitych nieujemnych.
formalnie wygląda to obrzydliwie: $\forall n \exists m \forall k \exists a_1, \ldots, a_m (k = a_1^n + \ldots + a_m^n)$.
Ta hipoteza Waringa została udowodniona w 1910 roku przez Dawida Hilberta.

$\lfloor n \rfloor$ oznacza część całkowitą liczby n.

Waring wysunął jeszcze drugą hipotezę, mianowicie, że $m = 2^n + \lfloor (\frac{3}{2})^n \rfloor - 2$. Łatwo zauważyć, że $m \geq 2^n + \lfloor (\frac{3}{2})^n \rfloor - 2$, bowiem w minimalnym rozkładzie liczby $k = \lfloor (\frac{3}{2})^n \rfloor \cdot 2^n - 1$ (mniejszej od 3^n) występuje $\lfloor (\frac{3}{2})^n \rfloor - 1$ składników 2^n i (reszta) $2^n - 1$ składników 1^n. Natomiast problem równości pozostaje do dziś otwarty, choć odpowiedź brzmi zapewne „tak” – w 1957 Mahler wykazał, że *dla odpowiednio dużych n* zachodzi równość natomiast komputery sprawdziły równość dla n do 471 600 000.

Problematyka równości różnych sum różnych potęg jest obszernym działem teorii liczb (i nie tylko). Powszechnie znanym celebrytą (czyli uznanym za wielkiej wagi, choć dla matematyki bez znaczenia) było przez trzy stulecia Wielkie Twierdzenie Fermata, orzekające, że równanie $x^n + y^n = z^n$ dla $n > 2$ nie ma rozwiązania wśród liczb całkowitych dodatnich. Wykazał, że tak jest (na gruncie krzywych eliptycznych) Andrew Wiles 1993–1995.