Twierdzenie Waringa

Przedstawianie liczby jako sumy kwadratów – twierdzenia

1. Jeżeli n, $N \in \mathbb{N}$ i zachodzi $n \mid N^2 + 1$, to istnieją liczby s, $t \in \mathbb{Z}$, że $n = s^2 + t^2$ (warunek dostateczny).
2. Jeżeli n jest liczbą pierwszą postaci $n = p = 4k + 1$, to istnieją liczby s, $t \in \mathbb{Z}$, że $n = s^2 + t^2$ (warunek dostateczny).
3. Liczbę $n \in \mathbb{N}$ możemy przedstawić w postaci sumy dwóch kwadratów liczb całkowitych wtedy i tylko wtedy jeżeli w jej rozkładzie kanonicznym wszystkie podstawy pierwsze postaci $4k + 3$ występują w potęgach parzystych (są kwadratami). Jest to warunek konieczny i dostateczny –
por. dyskusję przy **tw. Wilsona**.
4. (Lagrange, ca. 1770)
Każda liczba naturalna n jest sumą czterech kwadratów liczb całkowitych.

Hipoteza Waringa . . .

. . . pojawia się po raz pierwszy – bez dowodu – w *Meditationes Algebraicae* Edwarda Waringa (1770), profesora (*Lucasian Professor*) matematyki w Cambridge (poznaliśmy go przy okazji twierdzenia Wilsona, który był jego uczniem).

Dla każdej liczby naturalnej $k > 2$ istnieje taka liczba naturalna $r(k)$, r, $k \in \mathbb{N}$, że każdą liczbę naturalną n można przedstawić w postaci

$$n = {n_1}^k + {n_2}^k + \ldots + {n_{r(k)}}^k,$$

a więc każdą liczbę n możemy przedstawić w postaci sumy k-tych potęg, gdzie liczba składników sumy $r = r(k)$.

Pełny dowód hipotezy podał Hilbert (1909).
W momencie potwierdzenia tej hipotezy pojawił się problem znalezienia *najmniejszej* liczby $r(k)$ – zgodnie z ogólnie przyjętą konwencją takie najmniejsze r oznaczamy $g = g(k)$.

Hipoteza Waringa . . .

- z twierdzenia Lagrange'a wynika, że $g(2) \leqslant 4$. Jednak możemy łatwo sprawdzić, że liczba 7 nie może być przedstawiona jako suma dwóch, albo trzech kwadratów – stąd $g(2) = 4$.
- Mamy też $g(3) = 9, \;\; g(4) = 19, \;\; g(5) = 37, \;\; g(6) = 73.$ jeszcze do tego wrócimy . . .

Około 50 lat temu (ca. 1957) Mahler udowodnił, że dla dostatecznie dużych k prawdziwe jest

$$g(k) \geqslant \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2.$$

Dowód: Rozważmy

$$n = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1.$$

Oczywiście $n < 3^k$. Z definicji $g(k)$ wynika, że istnieją całkowite liczby nieujemne x_i, $i = 1, \ldots, g(k)$, takie że

$$n = {x_1}^k + {x_2}^k + \ldots {x_{g(k)}}^k, \text{ przy czym każde } x_i < 3$$

Jeżeli tak, to mamy tylko trzy możliwości: $x_i = 0, 1$ i 2.
Niech pomiędzy x_i będzie s dwójek ($x_i = 2$), t jedynek ($x_i = 1$) i u zer ($x_i = 0$). Zachodzi więc $g(k) = s + t + u \geqslant s + t$;
Nasza liczba $n = 2^k \cdot s + t$.
Z ostatniej równości wynika $n \geqslant 2^k \cdot s$. Mieliśmy – z definicji –

$$n + 1 = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor \qquad \rightarrow \qquad s < \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor,$$

skąd wynika

$$s \leqslant \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1. \tag{1}$$

W takim razie $t = n - 2^k s$; $\quad s + t = s + n - 2^k s = n - (2^k - 1)s$.
Liczba $k \in \mathbb{N}$ a więc i $2^k - 1$ też $\in \mathbb{N}$. Mnożymy (1) przez $2^k - 1$

$$(2^k - 1)s \leqslant (2^k - 1)\left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1\right). \quad \text{Ostatecznie}$$

$$g(k) \geqslant s + t \geqslant n - (2^k - 1)\left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1\right) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2. \quad \square$$

Hipoteza Waringa . . .

- dla $k = 2$ mamy $g(2) \geqslant 2^2 + \lfloor \frac{9}{4} \rfloor - 2 = 4 + 2 - 2$, a więc $g(2) \geqslant 4$. (Możemy łatwo sprawdzić, że liczba 7 nie może być przedstawiona jako suma dwóch, albo trzech kwadratów.) Jednocześnie, z twierdzenia Lagrange'a wynika, że $g(2) \leqslant 4$ – stąd $g(2) = 4$.
- dla $k = 3$ mamy $g(2) \geqslant 2^3 + \lfloor \frac{27}{8} \rfloor - 2 = 9$, a więc $g(3) \geqslant 9$.
  I znowu możemy sprawdzić, że liczba 23 nie może być przedstawiona jako suma ośmiu kwadratów.
  Udowodniono, że $g(3) = 9$.
- dla $k = 4$ mamy $g(4) \geqslant 2^4 + \lfloor \frac{81}{16} \rfloor - 2 = 19$, a więc $g(4) \geqslant 19$.
  Udowodniono, że $g(4) = 19$.
- dla $k = 5$ nasze ograniczenie daje $g(5) \geqslant 37$. I tutaj, zamiast słabej nierówności zachodzi równość, jak i *dla wszystkich* $k \geqslant 6$.
- Ciekawostka: każda liczba naturalna może zostać wyrażona jako suma 50-ciu *bikwadratów* (składników typu ${x_i}^4$).