

Problem Waringa i funkcje gęstości w teorii liczb

Michał GOS*

*Student, Wydział Matematyki i Informatyki, Uniwersytet Jagielloński

Teoria liczb wyróżnia się wyjątkowo intensywnym stosowaniem narzędzi pozostałych działów matematyki. W tej dziedzinie nierzadko okazuje się, że badanie prostych do sformułowania problemów wymaga szeroko zakrojonej rozbudowy znanych metod, co historycznie przyczyniało się do prężnego rozwoju innych dziedzin. Poniżej zajmujemy się przykładem takiego problemu. Przypomnijmy najpierw następujące:

Twierdzenie 1 (Lagrange). *Każdą liczbę naturalną można wyrazić jako sumę czterech nieujemnych kwadratów.*

Dowód, choć niekrótki, można uzyskać skromnymi środkami elementarnej algebry i arytmetyki modularnej reszt kwadratowych. W 1770 roku Edward Waring zapostulował następujące uogólnienie twierdzenia Lagrange’a, które zostało udowodnione dopiero w 1909 roku przez Davida Hilberta:

Twierdzenie 2 (Waring–Hilbert). *Dla każdego $k \in \mathbb{N}$ istnieje $g \in \mathbb{N}$ takie, że każdą liczbę $n \in \mathbb{N}$ można zapisać jako $n = x_1^k + \dots + x_g^k$ dla pewnych nieujemnych liczb całkowitych $x_1, x_2, \dots, x_g$.*

Najmniejsze g spełniające warunek twierdzenia 2 oznaczmy jako $g(k)$. Tak więc $g(2) = 4$, zaś Waring przypuszczał, że $g(3) = 9$ oraz $g(4) = 19$ (co okazało się prawdą). Obok hipotezy Goldbacha, problem Waringa stał się jednym z ważniejszych obszarów badań *addytywnej teorii liczb*. W niniejszym artykule przedstawimy szkic dowodu tego klasycznego już twierdzenia.

Dla wstępnej oceny trudności zadania, możemy łatwo otrzymać oszacowanie dolne wartości $g(k)$ przez sprytny wybór $n = 2^k \cdot \lfloor (\frac{3}{2})^k \rfloor - 1$. Wtedy $n < 3^k$, więc $x_1, \dots, x_{g(k)} \in \{0, 1, 2\}$. Niech a z tych liczb przyjmuje wartość 1, b z nich wartość 2. Mamy $n = a + b \cdot 2^k$, skąd $b \leq \lfloor \frac{n}{2^k} \rfloor \leq \lfloor (\frac{3}{2})^k \rfloor - 1$, a zatem

$$g(k) \geq a + b = n - (2^k - 1)b \geq 2^k + \lfloor (\frac{3}{2})^k \rfloor - 2.$$

Patrząc na wykładniczy wzrost wartości $g(k)$, możemy porzucić nadzieję na dowód konstruktywny, jaki można przeprowadzić w przypadku twierdzenia 1. Zastosujemy inne podejście – zamiast konstruować odpowiednie przedstawienie danej liczby n jako sumy k -tych potęg, będziemy badać zbiór wszystkich liczb postaci $x_1^k + \dots + x_l^k$ dla określonego l . Oznaczmy przez $\mathcal{S}_k$ zbiór $\{m^k : m \in \mathbb{Z}_{\geq 0}\}$, gdzie $\mathbb{Z}_{\geq 0}$ to zbiór nieujemnych liczb całkowitych. Sumą Minkowskiego zbiorów $A, B \subset \mathbb{Z}_{\geq 0}$ będziemy nazywać zbiór $A + B := \{a + b : a \in A, b \in B\}$; będziemy też domyślnie pisać $lA = A + \dots + A$ (mamy l „składników” po prawej stronie). Twierdzenie 1 możemy więc zapisać w postaci $4\mathcal{S}_2 = \mathbb{Z}_{\geq 0}$. Chcielibyśmy opisać, jak dużą „część” zbioru $\mathbb{Z}_{\geq 0}$ stanowią zbiory $l\mathcal{S}_k$ dla kolejnych liczb $l \in \mathbb{N}$ oraz znaleźć kryteria określające, kiedy $l\mathcal{S}_k = \mathbb{Z}_{\geq 0}$.

Jeśli Czytelnik miał okazję poznać olimpijskie zastosowania analitycznej teorii liczb (nie jest to potrzebne do lektury tego artykułu), może on skojarzyć w tym miejscu pojęcie *gęstości naturalnej* $d(A)$ dla zbioru $A \subset \mathbb{Z}_{\geq 0}$. Definiujemy ją jako granicę przy $n \rightarrow \infty$ wyrażenia $\frac{A(n)}{n}$, gdzie $A(n) = |A \cap \{1, \dots, n\}|$. Intuicyjnie, mierzy ona dokładnie to, jaką „część” zbioru $\mathbb{N}$ stanowi podzbiór A ; do naszych celów jest ona jednak wybrakowana. Po pierwsze, ciąg liczb $\{\frac{A(n)}{n}\}_{n \in \mathbb{N}}$ nie musi posiadać dobrze określonej granicy – do opisu „gęstości” zbioru A za pomocą tego ciągu potrzebne byłyby wtedy bardziej techniczne pojęcia analityczne. Po drugie, nawet „najgęstszy” przypadek $d(A) = 1$ nie pozwala stwierdzić, że $A = \mathbb{N}$.

Badając zagadnienia addytywnej teorii liczb, matematyk rosyjski Lew Schnirelman wprowadził „ostrzejszą” funkcję gęstości, zwaną dziś *gęstością Schnirelmana*. Dla zbioru $A \subset \mathbb{Z}_{\geq 0}$, oznaczamy ją przez $\delta(A)$ i definiujemy jako

Hipoteza Goldbacha (1742) głosi, iż każda liczba parzysta większa od 2 jest sumą dwóch liczb pierwszych. Do dziś pozostaje nierozstrzygnięta, choć udowodniono wiele słabszych sformułowań i powiązanych twierdzeń.

Przedstawiamy tylko drobną część zjawisk i teorii powiązanych z problemem Waringa. Czytelnik Zainteresowany znajdzie pełniejszy przegląd w Rozdziale 8 *Teorii Liczb* W. Narkiewicza (WN PWN, Warszawa 2003).

Oszacowanie $g(k) \geq 2^k + \lfloor (\frac{3}{2})^k \rfloor - 2$ podał L. Euler około 1772 roku. Na tej podstawie wysunął on śmiałą hipotezę, że $g(k)$ jest równe podanej wartości ograniczenia dolnego. Obecnie wiemy, że jest to prawda dla $k \leq 471\,600\,000$ oraz że może istnieć co najwyżej skończona liczba wyjątków; w ich (hipotetycznym) przypadku, dokładne wartości $g(k)$ również są opisane.

Artykuł w Δ_{16}^3 autorstwa Tomasza Kobosa przedstawia obfitą selekcję standardowych metod. Czytelnik Zainteresowany znajdzie więcej zadań olimpijskich z zakresu analitycznej teorii liczb w odpowiednim skrypcie broszury MIKO 2023/24 pod adresem <https://mikomath.org/editions/>.

Czytelnik Zaciekawiony zechce zbadać w tym miejscu gęstość naturalną zbioru liczb, których zapis dziesiętny zaczyna się od 1.



Czytelnik Skrupulatny może zapytać, czy wynik ten da się poprawić. Okazuje się, że tak: H.B. Mann wykazał, że dla $A, B \subset \mathbb{Z}_{\geq 0}$ takich, że $0 \in A \cap B$ i $1 \in A \cup B$, zachodzi nawet $\delta(A+B) \geq \min\{1, \delta(A) + \delta(B)\}$.

Uwagę przykuwa kombinatoryczny charakter powyższych wyników, mimo analitycznej definicji gęstości Schnirelmana $\delta(A)$ – to za sprawą jej wygodnej interpretacji w ramach nierówności $A(n) \geq \delta(A)n$ dla $n \in \mathbb{N}$.

Do dowodu lematu 3 konieczne są zaawansowane narzędzia analityczne lub żmudne obliczenia. Czytelnik Zawzięty może znaleźć elementarne uzasadnienie oparte na tych drugich w książce *Three Pearls of Number Theory*, A.Y. Khinchin (Graylock Press, Rochester, NY, 1952), dostępnej online. Dowód analityczny zawarty jest w *Teorii Liczb* W. Narkiewicza (WN PWN, Warszawa 2003).

infimum (największe ograniczenie dolne) zbioru $\{\frac{A(n)}{n} : n \in \mathbb{N}\}$, to jest największą liczbę $\delta \in \mathbb{R}$ taką, że $\frac{A(n)}{n} \geq \delta$ dla każdego $n \in \mathbb{N}$. Zaznaczmy, że każdy podzbiór liczb rzeczywistych posiada dobrze określone infimum. Ponadto z definicji $\delta(A)$ natychmiast wynika, że $\delta(A) = 1$ wtedy i tylko wtedy, gdy $A \cap \mathbb{N} = \mathbb{N}$. Zatem $\delta(A)$ zapewnia „gęstościowe” kryterium na zajęcie $A = \mathbb{Z}_{\geq 0}$ dla zbioru A zawierającego 0. Okazuje się, że mówi o wiele więcej w sytuacji, gdy rozważamy sumy Minkowskiego lA dla $l \in \mathbb{N}$ zdefiniowane powyżej:

Twierdzenie 3 (Sznirelman). *Jeżeli zbiór $A \subset \mathbb{Z}_{\geq 0}$ zawiera 0 i spełnia $\delta(A) > 0$, to istnieje $g \in \mathbb{N}$ takie, że $gA = \mathbb{Z}_{\geq 0}$.*

Zbiór $A \subset \mathbb{Z}_{\geq 0}$ spełniający tezę twierdzenia 3 nazywamy *bazą* zbioru liczb naturalnych. Powyższy wynik otwiera drogę do dowodu twierdzenia 2 – wystarczy wykazać $\delta(lS_k) > 0$ dla pewnego $l \in \mathbb{N}$. Zaznaczmy, że warunek twierdzenia 3 dla zbioru $A \subset \mathbb{Z}_{\geq 0}$ na bycie bazą $\mathbb{N}$ nie jest warunkiem koniecznym – mamy wszak $\delta(S_2) = 0$, ale $4S_2 = \mathbb{Z}_{\geq 0}$. Dowód twierdzenia 3 opiera się na opisie przyrostu gęstości Schnirelmana dla sumy Minkowskiego $A + B$ w porównaniu do gęstości składników A, B i jest konsekwencją dwóch kolejnych lematów:

Lemat 1. *Dla dowolnych zbiorów $A, B \subset \mathbb{Z}_{\geq 0}$ zawierających 0 zachodzi $\delta(A+B) \geq \delta(A) + \delta(B) - \delta(A)\delta(B)$.*

Dowód. Do wykazania $\delta(A+B) \geq c$ wystarczy $(A+B)(n) \geq cn$ dla każdego $n \in \mathbb{N}$. Wypiszmy elementy $A \cap \{1, \dots, n\}$: $1 \leq a_1 < a_2 < \dots < a_r \leq n$, gdzie $r = A(n) \geq \delta(A)n$. Oznaczmy $B_i = B \cap \{1, \dots, a_{i+1} - a_i - 1\}$ dla $i \in \{0, \dots, r\}$ przy dodatkowym oznaczeniu $a_0 = 0$ i $a_{r+1} = n+1$ (niekoniecznie $a_{r+1} \in A$).

Zbiory $\{a_i\}_{i=1}^r$ oraz $\{a_i\} + B_i$ dla $i \in \{0, \dots, r\}$ stanowią rozłączne podzbiory $(A+B) \cap \{1, \dots, n\}$ – zatem $(A+B)(n) \geq A(n) + \sum_{i=0}^r B(a_{i+1} - a_i - 1)$. Z definicji gęstości Schnirelmana $B(a_{i+1} - a_i - 1) \geq \delta(B)(a_{i+1} - a_i - 1)$, więc otrzymujemy

$$(A+B)(n) \geq A(n) + \sum_{i=0}^r \delta(B)(a_{i+1} - a_i - 1) = A(n) + \delta(B)(n - r),$$

gdyż prawa suma „teleskopuje się”. Zapis prawej strony jako $(1 - \delta(B))A(n) + n\delta(B)$ i podstawienie $A(n) \geq \delta(A)n$ dają żadaną nierówność. $\square$

Lemat 2. *Dla dowolnych zbiorów $A, B \subset \mathbb{Z}_{\geq 0}$ zawierających 0 i spełniających $\delta(A) + \delta(B) \geq 1$ zachodzi $A+B = \mathbb{Z}_{\geq 0}$.*

Dowód. Rozważmy dowolne $n \in \mathbb{N}$ – pokażemy, że $n \in A+B$. Jeżeli $n \in A \cup B$, to sytuacja jest jasna. W przeciwnym razie zbiory $A \cap \{1, \dots, n\}$ oraz $B' = \{n - b : b \in B \cap \{1, \dots, n\}\}$ są zawarte w $\{1, \dots, n-1\}$. Jednocześnie $A(n) + B'(n) = A(n) + B(n) \geq (\delta(A) + \delta(B))n \geq n$. Te dwa zbiory muszą zatem mieć niepuste przecięcie – dlatego istnieją $a \in A, b \in B$ takie, że $a = n - b$, czyli $n = a + b \in A+B$. $\square$

Dowód twierdzenia 3. Tezę lematu 1 możemy zapisać alternatywnie jako $1 - \delta(A+B) \leq (1 - \delta(A))(1 - \delta(B))$. Z indukcji matematycznej wynika teraz, że $1 - \delta(A_1 + \dots + A_l) \leq \prod_{i=1}^l (1 - \delta(A_i))$, w szczególności $\delta(lA) \geq 1 - (1 - \delta(A))^l$ dla $A \subset \mathbb{Z}_{\geq 0}$ zawierającego 0. Jeśli więc $\delta(A) > 0$, to istnieje $l \in \mathbb{N}$ takie, że $\delta(lA) > \frac{1}{2}$, a wtedy $2lA = \mathbb{Z}_{\geq 0}$ na mocy lematu 2. $\square$

Przystępujemy do dowodu twierdzenia 2. Chcemy znaleźć $l \in \mathbb{N}$ takie, że $\delta(lS_k) > 0$ – wystarczy wykazać, że dla pewnego $c > 0$ zachodzi $(lS_k)(n) \geq cn$ dla każdego $n \in \mathbb{N}$. Dla $m \in \mathbb{Z}_{\geq 0}$ oznaczmy przez $r_{l,k}(m)$ liczbę uporządkowanych nieujemnych krotek $(x_1, \dots, x_l)$ spełniających równanie $x_1^k + \dots + x_l^k = m$, to jest:

$$r_{l,k}(m) = |\{(x_1, \dots, x_l) \in \mathbb{Z}_{\geq 0}^l : x_1^k + \dots + x_l^k = m\}|.$$

Nie obędzie się, niestety, bez lematu *deus ex machina*:

Lemat 3 (Linnik). *Dla każdego $k \in \mathbb{N}$ istnieją takie $l \in \mathbb{N}$ i stała $\alpha(k) > 0$ zależna tylko od k , że dla każdego $m \in \mathbb{N}$ zachodzi nierówność $r_{l,k}(m) \leq \alpha(k)m^{\frac{l}{k}-1}$.*

Powyższe oszacowanie może wydać się przypadkowe; uwydatnimy jego rolę, poprzedzając jego zastosowanie (nieudaną) próbą dowodu.

Dowód twierdzenia 2. Oszacujemy sumę $\sum_{m=0}^n r_{l,k}(m)$ od góry i od dołu dla $n \in \mathbb{N}$ – porównanie oszacowań zapewni nam oczekiwaną nierówność.

Zauważmy, że jeśli $x_i \in \mathbb{Z}_{\geq 0}$ spełniają $0 \leq x_i \leq \left(\frac{n}{l}\right)^{1/k}$ dla $i \in \{1, \dots, l\}$, to z całą pewnością zachodzi $x_1^k + \dots + x_l^k \leq n$ – zatem dolne oszacowanie dla $\sum_{m=0}^n r_{l,k}(m)$ zapewni liczba uporządkowanych krotek $(x_1, \dots, x_l) \in \mathbb{Z}_{\geq 0}^l$ spełniających powyższy warunek. Z reguły mnożenia, jest ich $(\lfloor \left(\frac{n}{l}\right)^{1/k} \rfloor + 1)^l \geq \left(\frac{n}{l}\right)^{l/k}$.

Szukając elementarnego ograniczenia górnego, moglibyśmy postąpić podobnie – jeśli $x_1^k + \dots + x_l^k = m$ ma być spełnione dla $m \in \mathbb{N}$, z pewnością dla $i \in \{1, \dots, l\}$ musi zachodzić $0 \leq x_i \leq m^{1/k}$. Z reguły mnożenia, odpowiednich krotek jest $(\lfloor m^{1/k} \rfloor + 1)^l \leq (m^{1/k} + 1)^l = m^{l/k} (1 + m^{-1/k})^l$, przy czym ostatnia równość jest prawdziwa dla $m > 0$. Czynnikiem $(1 + m^{-1/k})^l$ nietrudno ograniczyć od góry stałą $\beta(l) > 0$, np. $\beta(l) = 2^l$. Mamy zatem:

$$\sum_{m=0}^n r_{l,k}(m) \leq 1 + \sum_{\substack{m=1, \\ r_{l,k}(m) > 0}}^n \beta(l) m^{l/k} \leq 1 + \beta(l) n^{l/k} (l\mathcal{S}_k)(n),$$

korzystając z $(l\mathcal{S}_k)(n) = |\{m \in \{1, \dots, n\} : r_{l,k}(m) > 0\}|$. Porównując ograniczenia górne i dolne, mamy $1 + \beta(l) n^{l/k} (l\mathcal{S}_k)(n) \geq l^{-l/k} n^{l/k}$. Niestety nie jest to wystarczająco mocna nierówność: przekształcając ją, otrzymujemy jedynie $(l\mathcal{S}_k)(n) \geq \frac{l^{-l/k}}{\beta(l)} - \frac{1}{n^{l/k} \beta(l)}$; po prawej stronie nie otrzymaliśmy składnika cn dla żadnej stałej $c > 0$.

Teraz łatwo jest dostrzec rolę lematu 3 – wybierając $l \in \mathbb{N}$ przewidziane przez niego i wyznaczając ograniczenie górne analogicznie, otrzymamy nierówność

$$1 + \alpha(k) n^{\frac{1}{k}-1} (l\mathcal{S}_k)(n) \geq l^{-l/k} n^{l/k}.$$

Pozostaje podzielić obie strony przez $\alpha(k) n^{\frac{1}{k}-1}$ – składnik „+1” po lewej stronie okazuje się tu nieistotny i ostatecznie wnioskujemy istnienie stałej $c > 0$ takiej, że $(l\mathcal{S}_k)(n) \geq cn$ dla każdego $n \in \mathbb{N}$, co daje $\delta(l\mathcal{S}_k) > 0$. $\square$

Zastosowania gęstości Sznirelmana i twierdzenia 3 nie kończą się na problemie Waringa; pracując nad zagadnieniem hipotezy Goldbacha, Sznirelman wykazał:

Twierdzenie 4 (Sznirelman). Istnieje $l \in \mathbb{N}$ takie, że każdą liczbę naturalną większą od 1 można wyrazić jako sumę nie więcej niż l liczb pierwszych.

Dowód tego twierdzenia przebiegnie podobnym szlakiem co dowód twierdzenia 2; ponownie, jego sednem jest niełatwy do wykazania lemat, oparty na analitycznej teorii liczb ($\mathbb{P}$ oznacza zbiór liczb pierwszych):

Lemat 4. Zachodzi $d(2\mathbb{P}) > 0$, to jest zbiór $2\mathbb{P}$ ma dodatnią gęstość naturalną.

Dowód twierdzenia 4. Jeżeli zbiór $2\mathbb{P}$ ma dodatnią gęstość naturalną, z pewnością to samo tyczy się zbioru $2\mathbb{P}^*$, gdzie $\mathbb{P}^* = \mathbb{P} \cup \{0, 1\}$. Skoro $d(2\mathbb{P}^*) > 0$ oraz $1 \in 2\mathbb{P}^*$, to również $\delta(2\mathbb{P}^*) > 0$. Ponieważ $0 \in 2\mathbb{P}^*$, więc z twierdzenia 3 wnioskujemy, że istnieje $c \in \mathbb{N}$ takie, że $2c\mathbb{P}^* = \mathbb{Z}_{\geq 0}$. Zatem każdą liczbę $n \in \mathbb{N}$ można przedstawić w postaci sumy $p_1 + \dots + p_i + j$, gdzie $i, j \leq 2c$. Pozostaje rozważyć kilka przypadków wartości liczby j , by zapisać ją w postaci sumy liczb pierwszych 2 i 3 o ograniczonej przez c liczbie składników (w przypadku $j = 1$ należy zastąpić n przez $n - 2$). $\square$

Wariacje na temat problemu Waringa są liczne; wspomnijmy na koniec o jeszcze jednej z nich. Zamiast $g(k)$ z twierdzenia 2, rozważmy $G(k)$ – najmniejszą możliwą liczbę $l \in \mathbb{N}$ taką, że każdą dostatecznie dużą liczbę $n \in \mathbb{N}$ można zapisać jako $x_1^k + \dots + x_l^k$ dla pewnych $x_i \in \mathbb{Z}_{\geq 0}$. W kontraście do wartości $g(k)$, obecnie znane są jedynie wartości $G(2) = 4$ i $G(4) = 16$. Wiadomo również, że $G(k) < g(k)$ dla $k > 2$. Okazuje się, że $G(k)$ rośnie o wiele wolniej niż w tempie wykładniczym (jak $g(k)$); najostrzejsze znane obecnie ograniczenie górne ma postać $G(k) \leq k(\log k + \log \log k + C)$ dla pewnej stałej $C \in \mathbb{R}$.

Najmniejsza liczba l spełniająca warunki twierdzenia 4 nosi nazwę *stałej Sznirelmana* s_0 . Wskażmy dwa obecnie najlepsze jej oszacowania z góry: $s_0 \leq 6$ wynika z opublikowanej w 2014 pracy Terrence’a Tao, zaś $s_0 \leq 4$ wynika z tzw. *słabej hipotezy Goldbacha*, której dowód został ogłoszony w 2013 roku przez Haralda Helfgotta, jak dotąd nie został jednak opublikowany w recenzowanym czasopiśmie.

Czytelnik znajdzie dowód lematu 4 w Rozdziałach 4, 5, 8 ww. *Teorii Liczb* W. Narkiewicza (WN PWN, Warszawa 2003).

