Autor: Krzysztof Zdon

Prowadzący: Krzysztof Zdon

Aproksymacje i Thue – Finaliści

Potrzebny wstęp - Aproksymacje

Twierdzenie 1 (Twierdzenie Dirichleta o aproksymacji)**.** Dana jest liczba rzeczywista α i liczba naturalna N. Wówczas istnieje taka liczba całkowita k, że $1 \leqslant k \leqslant N$ oraz

$$\left|\alpha - \frac{h}{k}\right| \leqslant \frac{1}{k(N+1)},$$

dla pewnej liczby całkowitej h.

Dowód. Rozważamy ciąg $(0, \{\alpha\}, \{2\alpha\}, \ldots, \{N\alpha\}, 1)$, gdzie nawiasami klamrowymi oznaczamy część ułamkową liczby. Teraz dzielimy przedział $[0, 1]$ na następujące przedziały:

$$\left[0,\ \frac{1}{N+1}\right], \left[\frac{1}{N+1},\ \frac{2}{N+1}\right], \ldots, \left[\frac{N}{N+1},\ 1\right].$$

Nasz ciąg ma $N+2$ elementów, więc do jednego przedziału wpadną dwie wartości. Mamy trzy możliwości, tj. $\mid 1 - \{s\alpha\} \mid \leqslant \frac{1}{N+1}$, $\mid \{t\alpha\} - 0 \mid \leqslant \frac{1}{N+1}$ lub $\mid \{s\alpha\} - \{t\alpha\} \mid \leqslant \frac{1}{N+1}$. W pierwszym przypadku $k = s$ i h to podłoga z $s\alpha + 1$. W drugim $k = t$ i h to podłoga z $t\alpha$, natomiast w trzecim $k = s - t$ a h to podłoga z $s\alpha$ minus podłoga z $t\alpha$. ■

Przykład 1 (Szybki skok w bok, czyli branie przedziałów)**.** Niech $x_1, x_2, \ldots, x_n$ będą liczbami nieujemnymi, których suma wynosi 1. Udowodnić, że istnieją liczby $a_1, a_2, \ldots, a_n \in \{0, 1, 2, 3, 4\}$ takie, że $(a_1, a_2, \ldots, a_n) \neq (2, 2, \ldots, 2)$ oraz

$$2 \leqslant a_1x_1 + a_2x_2 + \cdots + a_nx_n \leqslant 2 + \frac{2}{3^{n-1}}.$$

Rozwiązanie przykładu (1)**.** Rozważmy wszystkie możliwe ciągi $t = (t_1, t_2, \ldots, t_n)$, takie że $t_1, t_2, \ldots, t_n \in \{0, 1, 2\}$. Liczba takich ciągów wynosi 3^n. Dla każdego ciągu t, niech S_t oznacza sumę

$$S_t = t_1x_1 + t_2x_2 + \cdots + t_nx_n.$$

Ponieważ liczby $x_1, x_2, \ldots, x_n$ są nieujemne i ich suma wynosi 1, to zachodzą nierówności:

$$0 = 0 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_n \leqslant S_t \leqslant 2 \cdot x_1 + 2 \cdot x_2 + \cdots + 2 \cdot x_n = 2.$$

Z zasady szufladkowej Dirichleta wynika, że istnieją dwa różne ciągi $b = (b_1, b_2, \ldots, b_n)$ oraz $c = (c_1, c_2, \ldots, c_n)$, o wyrazach należących do zbioru $\{0, 1, 2\}$, takie że odpowiadające im sumy S_b oraz S_c należą do tego samego spośród 3^{n-1} przedziałów:

$$\left[0, \frac{2}{3^{n-1}}\right], \quad \left[\frac{2}{3^{n-1}}, \frac{4}{3^{n-1}}\right], \quad \ldots, \quad \left[\frac{2(3^{n-1}-1)}{3^{n-1}}, 2\right].$$

Bez utraty ogólności możemy założyć, że $S_b \leqslant S_c$. Wówczas:

$$0 \leqslant S_c - S_b \leqslant \frac{2}{3^{n-1}}. \tag{1}$$

Pokażemy, że warunki zadania spełnia ciąg $a = (a_1, a_2, \ldots, a_n)$, określony wzorem:

$$a_i = 2 + c_i - b_i \quad \text{dla } i = 1, 2, \ldots, n.$$

Każdy wyraz a_i należy do zbioru $\{0, 1, 2, 3, 4\}$. Ponadto $a \neq (2, 2, \ldots, 2)$, ponieważ ciągi b i c są różne. Obliczmy teraz sumę S_a:

$$S_a = \sum_{i=1}^{n}(2 + c_i - b_i)x_i = \sum_{i=1}^{n} 2x_i + \sum_{i=1}^{n} c_i x_i - \sum_{i=1}^{n} b_i x_i.$$

Zauważmy, że:

$$\sum_{i=1}^{n} 2x_i = 2, \quad \sum_{i=1}^{n} c_i x_i = S_c, \quad \text{oraz} \quad \sum_{i=1}^{n} b_i x_i = S_b.$$

Zatem:

$$S_a = 2 + S_c - S_b.$$

Wobec nierówności (1), mamy:

$$2 \leqslant S_a \leqslant 2 + \frac{2}{3^{n-1}},$$

co kończy dowód.

Lemat Thue'go, czyli małe rozwiązania kongruencji

Lemat 1 (Lemat Thue'go)**.** Jeżeli $m \geqslant 2$ jest liczbą naturalną i liczba całkowita a jest względnie pierwsza z m, to istnieją różne od 0 liczby całkowite x, y takie, że:

$$x \equiv ay \pmod{\text{m}} \quad \text{oraz} \quad |x|,\ |y| \leqslant \sqrt{m}$$

Dowód. Niech $A = \lfloor \sqrt{m} \rfloor$. Rozważmy wszystkie liczby postaci $x + ay$, gdzie x, y przebiegają $\{0, 1, \ldots, A\}$. Dostaniemy wówczas $A^2 + 1$ liczb, więc któreś dwie muszą dawać tą samą resztę. Załóżmy więc, że są to $x_1 + ay_1$ oraz $x_2 + ay_2$. Wówczas,

$$(x_1 - x_2) + a(y_1 - y_2) \equiv 0 \pmod{\text{m}}.$$

Z wyboru naszych liczb x_1, x_2, y_1, y_2 natychmiast wynikają nierówności $|x_1 - x_2| \leqslant \sqrt{m}$ oraz $|y_1 - y_2| \leqslant \sqrt{m}$. Musimy teraz tylko pokazać, że są one różne od zera. Istotnie tak jest, gdyż dzięki szacowaniom równość $y = 0$ implikowałaby podzielność $m \mid x_1 - x_2$, z czego wprost wynika, że $x_1 = x_2$. Analogicznie z równości $x = 0$ wynika równość $y = 0$. Dowód jest więc zakończony. ■

Twierdzenie Fermata-Eulera w dwóch smakach

Udowodnimy teraz poniższe tw. Fermata-Eulera na dwa sposoby, jeden wykorzystujący nasze twierdzenie aproksymacyjne, a drugi korzystający z lematu Thue'go:

Twierdzenie 2 (Twierdzenie Fermata-Eulera)**.** Nieparzysta liczba pierwsza p daje się przedstawić jako suma dwóch kwadratów wtw, gdy $p \equiv 1 \pmod{4}$.

Na początku udowodnimy, że prawdziwy jest następujący lemat:

Lemat 2. Jeżeli $n, a, b \in \mathbb{N}$, $NWD(a, b) = 1$ oraz $n \mid a^2 + b^2$ to istnieją takie liczby całkowite, że $n = x^2 + y^2$.

Dowód. Udowodnijmy go na początku dla $b = 1$. Oznaczmy $\frac{a}{n}$ jako α i $N = \lfloor \sqrt{n} \rfloor$. Wówczas z tw. Dirichleta istnieją takie h, k, że $\left|\frac{a}{n} - \frac{h}{k}\right| \leqslant \frac{1}{k(N+1)}$. Okazuje się, że $x = ak - nh$ oraz $y = k$ są dobre. Pokażemy teraz, że $x^2 + y^2$ jest wielokrotnością n, która jest mniejsza od $2n$, co zakończy dowód. Policzmy więc:

$$x^2 + y^2 = (ak - nh)^2 + k^2 = (a^2 + 1)k^2 + n(-2akh + nh^2)$$

A skoro $n \mid a^2 + b^2 = a^2 + 1$, to mamy naszą podzielność. Z drugiej strony, z naszych Dirichletowych szacowań mamy:

$$x^2 = (ak - nh)^2 = |ak - nh|^2 \leqslant \left(\frac{n}{N+1}\right)^2 < n.$$

Z twierdzenia Dirichleta wiemy również, że $k \leqslant N$, więc $y^2 = k^2 \leqslant N^2 \leqslant n$. A więc $0 < x^2 + y^2 < 2n$, co kończy dowód.
Jeśli $b \neq 1$, to wybieramy takie u, v całkowite, że $au + bv = 1$. Wówczas

$$(a^2 + b^2)(u^2 + v^2) = (av - bu)^2 + (au + bv)^2 = A^2 + 1,$$

więc $n \mid A^2 + 1$, to n można przedstawić jako sumę kwadratów. ■

Dowód 1. Twierdzenia Fermata-Eulera. Ten lemat natychmiast kończy dowód twierdzenia, gdyż jeśli $p \equiv 1 \pmod 4$, to istnieje a takie, że $a^2 \equiv -1 \pmod p$. ■

Dowód 2. Twierdzenia Fermata-Eulera. Skorzystamy z tw. Thue'go. Wybierzmy tak jak w wcześniejszym dowodzie $a \in \mathbb{Z}$ takie, że $a^2 \equiv -1 \pmod p$. Wybierzmy nasze x, y z Thue'go. Wówczas

$$x^2 + y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) \equiv 0 \pmod p.$$

Z drugiej jednak strony $x^2 < (\sqrt{p})^2 = p$ oraz $y^2 < (\sqrt{p})^2 = p$, więc $0 < x^2 + y^2 < 2p$, więc $x^2 + y^2 = p$, co kończy dowód. ■

Zadania

Zadanie 1. Niech f będzie funkcją zdefiniowaną z $\mathbb{Q}$ w $\mathbb{R}$. Zakładamy, że dla dowolnych liczb wymiernych $r, s \in \mathbb{Q}$ zachodzi:

$$f(r + s) - f(r) - f(s) \in \mathbb{Z}.$$

Udowodnić, że istnieje dodatnia liczba całkowita q oraz liczba całkowita p spełniające warunek:

$$\left| f\left(\frac{1}{q}\right) - p \right| \leqslant \frac{1}{2025}.$$

Zadanie 2. Udowodnij, że nieparzysta liczba pierwsza p daje się przedstawić w postaci x^2+2y^2 wtedy i tylko wtedy, gdy $p \equiv 1, 3 \pmod 8$

Wskazówka -2 jest resztą kwadratową (mod p) wtw, gdy $p \equiv 1, 3 \pmod 8$.

Zadanie 3. Dana jest niezerowa funkcja $f : \mathbb{R} \to \mathbb{R}$ oraz liczba dodatnia b, przy czym spełniona jest równość:

$$f(x+b) = -f(x) \quad \text{dla każdego } x \in \mathbb{R}.$$

Rozstrzygnąć, czy funkcja f musi mieć okres podstawowy (czyli najmniejszy z dodatnich okresów).

Zadanie 4. Niech p będzie pierwsze. Wówczas istnieją takie a, b całkowite, że $p = a^2 + ab + b^2$ wtedy i tylko wtedy, gdy $p = 3$ lub $p \equiv 1 \pmod 3$. *Wskazówka:* warto skorzystać z prawa wzajemności reszt kwadratowych.

Zadanie 5. Niech S będzie zbiorem wszystkich dodatnich liczb całkowitych, które można przedstawić w postaci

$$a^2 + 5b^2$$

dla pewnych względnie pierwszych liczb całkowitych a i b. Niech ponadto p będzie liczbą pierwszą dającą resztę 3 z dzielenia przez 4. Wykazać, że jeżeli pewna dodatnia wielokrotność liczby p należy do zbioru S, to również liczba $2p$ należy do zbioru S.

Rozwiązania

Rozwiązanie (1)**.** Niech N będzie wspólną wielokrotnością liczb $1, 2, \ldots, 2024$ (na przykład $N = 2024!$). Na mocy twierdzenia Dirichleta (dla $x = f\left(\frac{1}{N}\right)$ i $n = 2024$), istnieje liczba całkowita $a \leqslant 2024$ oraz liczba całkowita b, takie że:

$$\left| af\left(\frac{1}{N}\right) - b \right| \leqslant \frac{1}{2025}.$$

Z założenia zadania wiadomo, że $f\left(\frac{a}{N}\right)$ oraz $af\left(\frac{1}{N}\right)$ różnią się o liczbę całkowitą. Oznaczmy tę liczbę całkowitą przez p. Wówczas:

$$\left| f\left(\frac{a}{N}\right) - p \right| \leqslant \frac{1}{2025}.$$

Ponieważ N jest wielokrotnością a, możemy zdefiniować liczbę całkowitą $q = \frac{N}{a}$. Wówczas:

$$\left| f\left(\frac{1}{q}\right) - p \right| \leqslant \frac{1}{2025}.$$

Rozwiązanie (2)**.** Na początku rozważyć przypadki 5, 7 (mod 8), a potem ze wskazówki i lematu Thue'go.

Rozwiązanie (3)**.**

$$f(x) = \begin{cases} (-1)^{m+n}, & \text{gdy } x = b(m + n\sqrt{2}) \text{ dla pewnych liczb całkowitych } m, n, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Teraz dowolne takie dodatnie wyrażenie $b(2k + 2\ell\sqrt{2})$ jest okresem.

Rozwiązanie (4)**.** Najpierw udowodnimy, że jeśli $p \equiv 2 \pmod 3$, to nie możemy znaleźć takich a, b, że $p = a^2+ab+b^2$. (Jest to łatwiejsza, niekonstruktywna część problemu). Załóżmy przeciwnie, że $p = a^2 + ab + b^2$. Możemy przepisać tę równość w lepszej formie:

$$4p = 4(a^2 + ab + b^2) = (2a + b)^2 + 3b^2.$$

Stąd:

$$(2a + b)^2 \equiv -3b^2 \pmod p.$$

Zatem -3 jest resztą kwadratową modulo p, chyba że $p \mid b$. Jednakże, korzystając z prawa wzajemności kwadratów, mamy:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right).$$

Jeśli $p \equiv 2 \pmod 3$, to $\left(\frac{p}{3}\right) = -1$. Wówczas:

$$\left(\frac{-3}{p}\right) = (-1)(-1) = 1,$$

co prowadzi do sprzeczności. Zatem $p \mid b$, co oznacza również, że $p \mid a$. W konsekwencji $p^2 \mid a^2 + ab + b^2 = p$, co jest niemożliwe.

Teraz przechodzimy do ciekawszej części. Pomijamy przypadek $p = 3$, ponieważ wtedy para $(1, 1)$ spełnia równanie. Zauważmy, że powyższa metoda może zostać zmodyfikowana, aby znaleźć x, dla którego $p \mid x^2 + x + 1$, gdy $p \equiv 1 \pmod 3$ (spróbuj to zrobić!). Następnie, korzystając z Lematu Thue, znajdźmy a, b takie, że $ax \equiv b \pmod p$, przy czym $0 < |a|, |b| < \sqrt{p}$. Wówczas:

$$a^2 + ab + b^2 \equiv a^2 + a(ax) + (ax)^2 \equiv a^2(x^2 + x + 1) \equiv 0 \pmod p.$$

Otrzymujemy $p \mid a^2 + ab + b^2$, a jednocześnie $0 < a^2 + ab + b^2 < 3p$. Stąd:

$$a^2 + ab + b^2 \in \{p, 2p\}.$$

Rozważmy przypadek $a^2+ab+b^2 = 2p$. Wtedy zarówno a, jak i b muszą być liczbami parzystymi (sprawdź to). Jednakże, wówczas:

$$4 \mid a^2 + ab + b^2 = 2p,$$

co jest niemożliwe, ponieważ p jest liczbą pierwszą. Zatem ten przypadek jest wykluczony.

W konsekwencji:

$$a^2 + ab + b^2 = p,$$

co kończy dowód.

Rozwiązanie (5)**.** Wybierzmy dowolną liczbę pierwszą p z S. Wówczas istnieją $s, t \in \mathbb{Z}$ takie, że $p \mid s^2 + 5t^2$. Skoro s i t są względnie pierwsze, to $p \nmid t$, ergo, t jest odwracalne (mod p). Niech u będzie odwrotnością t (mod p). Wtedy dla $a = su$ mamy

$$a^2 \equiv -5 \text{ (mod p)}.$$

Teraz korzystamy z Thue'go - znajdujemy x, y takie, że $x \equiv ay$ (mod p) i wtedy:

$$x^2 + 5y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) \equiv 0 \text{ (mod p)}$$

Teraz jedynie trzeba pokazać, że to jest równie $2p$ i to się pałkuje.