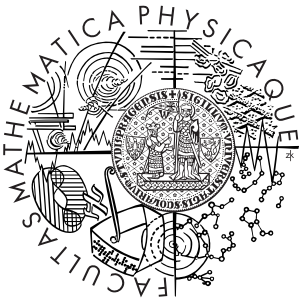
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Jaroslav Hančl

Freimanova věta v aditivní kombinatorice

Katedra aplikované matematiky

Vedoucí bakalářské práce: doc. RNDr. Martin Klazar, Dr.
Studijní program: Matematika, obecná matematika

2009

Děkuji vedoucímu mojí bakalářské práce panu docentu Martinu Klazarovi za jeho vedení, poskytnutí doporučené literatury a cenné rady, které mi v průběhu řešení práce poskytl.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 28.5.2009 Jaroslav Hančl

Obsah

Název práce: Freimanova věta v aditivní kombinatorice
Autor: Jaroslav Hančl
Katedra: Katedra Aplikované Matematiky
Vedoucí bakalářské práce: doc. RNDr. Martin Klazar, Dr.
e-mail vedoucího: klazar@kam.mff.cuni.cz

Abstrakt: V předložené shrnující práci studujeme takzvaný inverzní problém aditivní teorie čísel. Snažíme se tedy charakterizovat množiny A přirozených čísel, víme-li nějaké informace o jejich násobcích $2A = A + A$. Zpočátku se budeme věnovat konečným množinám s vlastností $|2A| = 2|A| - 1$, dále si ukážeme zobecnění pro takové abelovské grupy G, v nichž má každý prvek řád omezený konstantou r, a jejich podmnožiny A splňující $|2A| \leq c|A|$. Nakonec se dostaneme až k slavné Freimanově větě, která popisuje množiny přirozených čísel A, jež jsou malé ve smyslu $|2A| \leq c|A|$. Tuto větu dokážeme a uvedeme některé její důsledky a aplikace.

Klíčová slova: Aditivní teorie čísel, Součet množin, Multidimenzionální aritmetická posloupnost, Freimanova věta

Title: Freiman's theorem in additive combinatorics
Author: Jaroslav Hančl
Department: Department of Applied Mathematics
Supervisor: doc. RNDr. Martin Klazar, Dr.
Supervisor's e-mail address: klazar@kam.mff.cuni.cz

Abstract: In the presented summary work we study the inverse problem in additive number theory. More specifically, we try to characterize sets A of positive integers if we know some information about their sumsets $2A = A + A$. At the beginning we devote some time to finite sets with the property $|2A| = 2|A| - 1$, then we solve a generalized problem for such abelian groups G in whose order of all elements is bounded by a constant $r$and their subsets A satisfying $|2A| \leq c|A|$. At the end we present the famous Freiman theorem, which describes sets of positive integers A small in the sense $|2A| \leq c|A|$. We prove this theorem and give some corollaries and applications.

Keywords: Additive number theory, Sumset, Multidimensional arithmetic progression, Freiman's theorem

Prolog

V předložené práci se zabýváme inverzním problémem aditivní teorie čísel. To znamená, že se snažíme co nejlépe popsat množiny přirozených čísel A, známe-li nějakou charakteristickou vlastnost jejich násobků hA. Zaobírejme se pouze případem $h = 2$. Většina důkazů uvedených v této práci není původních, jsou převzaté z knihy [1] od M. B. Nathansona.

V první kapitole si nejprve ukážeme nejlepší možné odhady velikosti množiny $A + B$ a poté si dokonale charakterizujeme množiny A s vlastností $|2A| = 2|A| - 1$. Ke konci kapitoly se budeme věnovat Freimanově větě pro ty abelovské grupy G, ve kterých je řád každého prvku omezený konstantou r. Dokážeme si tedy pro libovolnou konstantu c, že takovýchto grupách G je každá konečná množina A splňující $|A + B| \leq c|A|$ již nutně podmnožinou grupy I, jejíž velikost je $|I| \leq c^2 r^{c^4} |B|$.

Následující kapitola slouží k zavedení pojmů potřebných k důkazu Freimanovy věty. V sekci 2.1 zadefinujeme multidimenzionální aritmetické posloupnosti (MAP) a ukážeme si mimo jiné, že součet a rozdíl MAP je MAP. Druhá sekce 2.2 je věnovaná Freimanově izomorfismu a jeho vlastnostem. Například se zde dozvíme, že Freimanův izomorfismus zachovává vlastní MAP. Ve třetí sekci 2.3 si ukážeme jednoduché vlastnosti komplexních čísel na jednotkové kružnici.

Poslední a nejdůležitější kapitola začíná zněním Freimanovy věty, kterou první v roce 1964 dokázal G. A. Freiman, zde však uvedeme důkaz I. Z. Ruszy. Freimanova věta, že pro libovolnou konstantu c existují l a n takové, že každá konečná množina přirozených čísel A s vlastností $|2A| \leq c|A|$ je obsažena v nějaké n-dimenzionální aritmetické posloupnosti délky nejvýše $l|A|$. V následujících sekcích 3.2 a 3.3 je proveden důkaz. Ten začíná Bogoljubovou větou a její aplikací, jež garantuje existenci dostatečně velké MAP v množině $2A-2A$, pokračuje Ruszovou metodu až je dokázáno mírně obecnější tvrzení, jehož důsledkem je Freimanova věta. Toto tvrzení je ještě zobecněno do beztorzních grup. Poslední sekce 3.4 uvádí dvě aplikace pro existenci aritmetických posloupností v jistých množinách přirozených čísel.

Kapitola 1

Úvod

1.1 Něco málo o součtech množin

Aditivní teorie čísel je obor matematiky zkoumající součty množin celých nebo přirozených čísel. Pod pojmem množina přirozených čísel budeme rozumět množinu

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Buď $h \geq 2$ a $A_1, A_2, \dots, A_h$ množiny přirozených čísel. *Součtem množin*

$$A_1 + A_2 + \cdots + A_h$$

budeme rozumět množinu všech čísel tvaru $a_1 + a_2 + \cdots + a_h$, kde $a_i \in A_i$ pro $i = 1, 2, \dots, h$. Jestliže bude $A_i = A$ pro $i = 1, 2, \dots, h$, poté budeme značit součet množin $A_1 + A_2 + \cdots + A_h$ jednodušeji symbolem hA. Obecněji, součty množin mohou být definovány v libovolných abelovských grupách, a to úplně stejně jako pro množiny přirozených čísel. Abelovskou grupou G s operací $\circ$ rozumíme grupu $(G, \circ)$ ve které je operace $\circ$ komutativní (tj. $a \circ b = b \circ a$ pro libovolné $a, b \in G$).

Nechť A a B jsou množiny přirozených čísel. Symbolem $|A|$ budeme značit velikost (kardinalitu) množiny A. Dále definujme *rozdílovou množinu* $A - B$ následovně:

$$A - B = \{a - b \mid a \in A, b \in B\}.$$

Pro přirozená čísla c a d budeme dále značit

$$c \pm A = \{c\} \pm A$$

a

$$d * A = \{da \mid a \in A\}.$$

Dva základní problémy, se kterými se v aditivní teorii čísel nemůžete minout jsou přímý a inverzní problém:

Přímý problém zkoumá vlastnosti množiny hA, je-li známá množina A. Například, bude-li M množina všech druhých mocnin přirozených čísel s nulou, poté Lagrangeova věta o čtyřech čtvercích tvrdí, že množina $4M$ jsou již všechna přirozená čísla.

Naproti tomu *inverzní problém* se snaží popsat množinu A, umí-li charakterizovat množinu hA. Hezký příklad nám mohou poskytnout množiny pro něž platí vztah $|2A| = 2|A| - 1$, jelikož každá množina A splňující tuto vlastnost již nutně musí být aritmetická posloupnost. Důkaz tohoto tvrzení si ukážeme v následující kapitole.

1.2 Případ $|2A| = 2|A| - 1$

V této sekci zjistíme, jak vypadají množiny A, pro které platí vztah $|2A| = 2|A| - 1$. Dokážeme si také odhady pro velikost množiny $|A + B|$, známe-li velikosti množin A a B.

Buď k a d přirozená čísla a a číslo celé. *Aritmetickou posloupností* délky k s diferencí d a počátečním členem a budeme rozumět množinu

$$\{a, a + d, a + 2d, \ldots, a + (k - 1)d\} = a + d * [0, k - 1],$$

kde $[0, k - 1]$ značí interval celých čísel od 0 do $(k - 1)$.

Věta 1.2.1 *Nechť A a B jsou konečné množiny přirozených čísel, pak*

$$|A| + |B| - 1 \leq |A + B| \leq |A||B|.$$

Důkaz. Označme si $A = \{a_0, a_1, \ldots, a_{k-1}\}$ a $B = \{b_0, b_1, \ldots, b_{l-1}\}$, kde $a_0 < a_1 < \cdots < a_{k-1}$ a $b_0 < b_1 < \cdots < b_{l-1}$. Součet $A + B$ zajisté obsahuje různé prvky

$$\begin{aligned} a_0 + b_0 < a_0 + b_1 < a_0 + b_2 < \cdots < a_0 + b_{l-1} \\ < a_1 + b_{l-1} < a_2 + b_{l-1} < \cdots < a_{k-1} + b_{l-1}, \end{aligned}$$

a proto

$$|A + B| \geq (l - 1) + k = k + l - 1 = |A| + |B| - 1.$$

Horní odhad dostaneme z faktu, že počet výrazů formy $a + b$, kde $a \in A$ a $b \in B$ je právě $|A||B|$. □

Poznámka 1.2.2. Oba tyto odhady jsou nejlepší možné. Je jednoduché ověřit, že pro $A = [0, k-1]$ a $B = [0, l-1]$ platí $|A+B| = [0, k+l-2]$, což dává rovnost $|A+B| = |A| + |B| - 1$.

Pro horní odhad to bude malinko složitější. Je-li $A = k$ a $B = l$, definujme $a_i = li$ pro $i = 0, 1, \ldots, k-1$ a $B = [0, l-1]$. Pak $|A+B| = [0, kl-1]$ a tedy platí $|A+B| = |A||B|$.

Věta 1.2.3 *Jestliže pro konečnou množinu přirozených čísel A platí $|2A| = 2|A| - 1$, pak A je aritmetická posloupnost.*

Důkaz. Označme

$$A = \{a_0, a_1, \ldots, a_{k-1}\},$$

kde

$$a_0 < a_1 < \cdots < a_{k-1}.$$

Díky našemu uspořádání množina $2A$ má $2|A| - 1$ různých prvků

$$\begin{aligned} a_0 + a_0 < a_0 + a_1 < a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < \cdots \\ < a_{k-2} + a_{k-2} < a_{k-2} + a_{k-1} < a_{k-1} + a_{k-1}, \end{aligned}$$

jenže také $2|A| - 1$ různých prvků

$$\begin{aligned} a_0 + a_0 < a_0 + a_1 < a_0 + a_2 < a_1 + a_2 < a_1 + a_3 < a_2 + a_3 < \cdots \\ < a_{k-3} + a_{k-1} < a_{k-2} + a_{k-1} < a_{k-1} + a_{k-1}. \end{aligned}$$

Pokud má množina $2A$ mít právě $2|A| - 1$ prvků, musí se rovnat příslušné prvky v obou uspořádáních rovnat, tedy

$$2a_i = a_{i-1} + a_{i+1}$$

pro $i = 1, 2, \ldots, k-2$. A tudíž máme

$$a_i - a_{i-1} = a_{i+1} - a_i$$

pro $i = 1, 2, \ldots, k-2$. Proto sousední prvky A jsou od sebe vždy stejně vzdálené, což znamená, že A je aritmetická posloupnost. □

Poznámka 1.2.4. Obě předchozí věty se dají zobecnit pro soubor m množin $A_1, A_2, \ldots, A_m$. Důkazy by se provedly obdobně.

Jednoduše se dá také popsat velikost množiny mA, pokud v A tvoří aritmetickou posloupnost všechny členy až na ten největší. Dobře je také známý popis množin, jejichž dvojnásobek (tj. množina $2A$) má vlastnost $|2A| \leq 3|A| - 4$. Všechny tyto výsledky naleznete v knize [1] postupně na stranách 18 a 21.

1.3 Analogie Freimanovy věty

Než přejdeme k Freimanově větě, dokážeme si její obdobu pro třídu komutativních grup, v nichž řád každého prvku je omezený číslem r. Přestože se tímto dodatečným předpokladem důkaz velice zjednoduší, budeme už potřebovat složitější aparát v podobě následujícího lemmatu.

Lemma 1.3.1 *Buď G abelovská grupa a α reálné číslo. Mějme $A, B \subset G$ takové, že $|B| = n$ a $|A + B| \leq \alpha n$. Pak pro libovolné přirozené čísla k a l platí vztah*

$$|kA - lA| \leq \alpha^{k+l} n.$$

Důkaz tohoto lemmatu není jednoduchý. Je založen na teorii grafů a Plünneckeho nerovnosti, proto ho zde nebudeme uvádět. Lze ho najít v knihách [1] na straně 219 a [3] na straně 269.

Věta 1.3.2 *Buď $r \geq 2$ přirozené číslo, α reálné číslo a G abelovská grupa, jejíž každý prvek má řád nejvýše r. Buďte $A, B \subset G$ dvě konečné množiny takové, že $|A| = |B| = n$ a $|A + B| \leq \alpha n$. Pak A je obsaženo v podgrupě I grupy G takové, že*

$$|I| \leq f(r, \alpha) n,$$

kde

$$f(r, \alpha) = \alpha^2 r^{\alpha^4}.$$

Navíc, tato grupa I je grupa generovaná množinou A.

Důkaz. Nalezněme maximální soubor $B = \{b_1, b_2, \ldots, b_k\} \subset G$ takový, že $b_i \in 2A - A$ a $b_i - A$ jsou po dvou disjunktní pro $i = 1, 2, \ldots, k$. Jelikož platí $b_i - A \subseteq 2A - 2A$, proto

$$kn = k|A| = \left| \bigcup_{i=1}^{k} (b_i - A) \right| \leq |2A - 2A|.$$

Podle předešlého Lemmatu 1.3.1 máme

$$|2A - 2A| \leq \alpha^4 n,$$

čímž dostáváme odhad

$$k \leq \alpha^4. \tag{1.1}$$

Vezměme libovolné $x \in 2A-A$. Protože soubor B byl maximální, existuje index i takový, že

$$(x - A) \cap (b_i - A) \neq \emptyset.$$

To znamená, že pro nějaké $a_1, a_2 \in A$ platí $x - a_1 = b_i - a_2$, neboli

$$x = b_i + a_1 - a_2 \in b_i + A - A.$$

Dostáváme tedy

$$2A - A \subseteq \bigcup_{i=1}^{k} (b_i + A - A) = B + A - A. \tag{1.2}$$

Nyní dokážeme indukcí vztah

$$jA - A \subseteq (j-1)B + A - A. \tag{1.3}$$

Pro $j = 2$ je to již dokázaná rovnost (1.2), soustřeďme se tedy na indukční krok. Platí

$$\begin{aligned}(j+1)A - A &= (2A - A) + (j-1)A \\ &\overset{(1.2)}{\subseteq} B + A - A + (j-1)A \\ &= B + jA - A \\ &\overset{\text{indukce}}{\subseteq} B + (j-1)B + A - A \\ &= jB + A - A,\end{aligned}$$

což jsme chtěli dokázat.

Označme postupně I a J podgrupy G, které jsou generovány množinami A a B. Z tvrzení (1.3) máme

$$jA - A \subseteq (j-1)B + A - A \subseteq J + A - A. \tag{1.4}$$

Protože každý prvek v G má konečný řád, platí také

$$\bigcup_{j=1}^{\infty} (jA - A) = I. \tag{1.5}$$

Z předchozích dvou vztahů (1.4) a (1.5) plyne

$$I \subseteq J + A - A. \tag{1.6}$$

Jelikož J je generováno k prvky s řádem nejvýše r a k je odhadnuté podle (1.1), platí

$$|J| \leq r^k \leq r^{\alpha^4}, \tag{1.7}$$

Dále víme dle Lemmatu 1.3.1, že $|A - A| \leq \alpha^2 n$, což společně s (1.6) a (1.7) dává kýžený výsledek

$$|I| \leq |J||A - A| \leq \alpha^2 r^{\alpha^4} n.$$

□

Domněnka 1.3.3 (Marton)**.** Odhad $f(r, \alpha) = \alpha^2 r^{\alpha^4}$ zdaleka není nejlepším možným. Již v malých případech roste nesrovnatelně rychleji než velikost největší podgrupy z předchozí věty. Katalin Marton vyslovila domněnku, že $|I| \leq r^{C\alpha} n$ s vhodnou konstantou C. Problém se však zdá býti komplikovaným, neboť tato domněnka doposud nebyla dokázána ani vyvrácena.

Kapitola 2

Příprava na důkaz Freimanovy věty

2.1 Multidimenzionální aritmetické posloupnosti

V této sekci si pojem aritmetická posloupnost rozšíříme na obecnější pojem multidimenzionální aritmetická posloupnost. V těchto obecnějších posloupnostech se již nebude vyskytovat pouze jedna diference, ale hned několik diferencí. V druhé části si ukážeme základní vlastnosti těchto posloupností.

Pro $n \in \mathbb{N}$ buďte a, $d_1, d_2, \ldots, d_n$ ne nutně různé prvky abelovské grupy G a $l_1, l_2, \ldots, l_n$ přirozená čísla. Množinu

$$Q = \{a + t_1 d_1 + t_2 d_2 + \cdots + t_n d_n : 0 \leq t_i < l_i \text{ pro } i = 1, 2, \ldots, n\}$$

nazvěme *n-dimenzionální aritmetickou posloupností* v abelovské grupě G a jednoduše značme

$$Q = Q(a; d_1, d_2, \ldots, d_n; l_1, l_2, \ldots, l_n).$$

Čísla d_i pro $i = 1, 2, \ldots, n$ budeme nazývat diferencemi Q. Bude-li Q multidimenzionální aritmetická posloupnost, pak její délkou $l(Q)$ budeme rozumět číslo

$$l(Q) = l_1 l_2 \cdots l_n.$$

Multidimenzionální aritmetickou posloupnost Q nazveme *vlastní*, jestliže $|Q| = l(Q)$, v opačném případě budeme hovořit o *nevlastní* multidimen-

zionální aritmetické posloupnosti. To jinak řečeno znamená, že některý prvek Q lze napsat jako součet diferencí (s možnou násobností omezenou hodnotami l_i) více různými způsoby. Proto reprezentace množiny aritmetickou posloupností není jednoznačná. Reprezentací může být více, mohou se lišit dimenzí, nebo délkou.

Následující sada tvrzení nám shrnují některé jednoduché vlastnosti multidimenzionálních aritmetických posloupností.

Tvrzení 2.1.1 *Buď G abelovská grupa a v ní dvě multidimenzionální aritmetické posloupnosti Q a Q' o dimenzích n a n' a délkách l a l'. Pak $Q+Q'$ je multidimenzionální aritmetická posloupnost dimenze $n+n'$ a délky $l(Q+Q') = ll'$.*

Důkaz. Označme si posloupnosti Q a Q' následovně:

$$Q = Q(a; d_1, d_2, \ldots, d_n; l_1, l_2, \ldots, l_n),$$
$$Q' = Q'(a'; d'_1, d'_2, \ldots, d'_n; l'_1, l'_2, \ldots, l'_{n'}).$$

Potom posloupnost $Q + Q'$ můžeme zapsat jako

$$Q + Q' = \{a + t_1d_1 + t_2d_2 + \cdots + t_nd_n + a' + t'_1d'_1 + t'_2d'_2 + \cdots + t'_{n'}d'_{n'} : \\ 0 \leq t_i < l_i \text{ a } 0 \leq t'_j < l'_j \text{ pro } i = 1, 2, \ldots, n \text{ a } j = 1, 2, \ldots, n'\},$$

což se dá chápat také jako

$$Q(a + a'; d_1, d_2, \ldots, d_n, d'_1, d'_2, \ldots, d'_{n'}; l_1, l_2, \ldots, l_n, l'_1, l'_2, \ldots, l'_{n'}).$$

A proto $Q + Q'$ je aritmetická posloupnost dimenze $n + n'$ a délky

$$l(Q + Q') = l_1l_2 \cdots l_nl'_1l'_2 \cdots l'_{n'} = l(Q)l(Q') = ll'.$$

□

Tvrzení 2.1.2 *Buď G abelovská grupa a v ní buď Q multidimenzionální aritmetická posloupnost dimenze n a délky l. Pak $Q - Q$ je multidimenzionální aritmetická posloupnost dimenze n, která má délku $l(Q - Q) < 2^n l$.*

Důkaz. Označíme-li si $Q = Q(a; d_1, d_2, \ldots, d_n; l_1, l_2, \ldots, l_n)$, můžeme podobně jako v předešlém důkazu psát

$$Q - Q = \{s_1d_1 + s_2d_2 + \cdots + s_nd_n, \text{ kde } -l_i < s_i < l_i \text{ pro } i = 1, 2, \ldots, n\}.$$

Abychom $Q - Q$ mohli reprezentovat jako multidimenzionální aritmetickou posloupnost, definujme

$$b = -\sum_{i=1}^{n}(l_i - 1)d_i$$

a

$$k_i = 2l_i - 1,$$

protože pak

$$Q-Q = \{b + s_1d_1 + s_2d_2 + \cdots + s_nd_n, \text{ kde } 0 \leq s_i < k_i \text{ pro } i = 1, 2, \ldots, n\}.$$

To neznamená nic jiného než že $Q - Q$ je aritmetická posloupnost dimenze n, jejíž délka je ze shora odhadnutá

$$l(Q - Q) = k_1k_2 \cdots k_n < 2^n l_1l_2 \cdots l_n = 2^n l(Q),$$

což jsme chtěli dokázat. □

Tvrzení 2.1.3 *Buď G abelovská grupa, $h \geq 2$ přirozené číslo a Q vlastní multidimenzionální aritmetická posloupnost dimenze n a délky l v G. Potom $l(hQ) < h^n|Q|$.*

Důkaz. Při označení $Q = Q(a; d_1, d_2, \ldots, d_n; l_1, l_2, \ldots, l_n)$ máme

$$hQ = Q(ha; d_1, d_2, \ldots, d_n; h(l_1 - 1) + 1, h(l_2 - 1) + 1, \ldots, h(l_n - 1) + 1).$$

Proto můžeme jednoduše odhadnout délku hQ shora

$$l(hQ) = \prod_{i=1}^{n}(h(l_i - 1) + 1) < \prod_{i=1}^{n} hl_i = h^n \prod_{i=1}^{n} l_i = h^n l(Q) = h^n|Q|,$$

což jsme chtěli dokázat. □

Tvrzení 2.1.4 *Je-li F konečná podmnožina abelovské grupy G, pak F je podmnožinou nějaké multidimenzionální aritmetické posloupnosti dimenze $|F|$ a délky $2^{|F|}$.*

Důkaz. Buď $|F| = n$ a $F = \{f_1, f_2, \ldots, f_n\}$. Pak množina

$$Q = Q(0; f_1, f_2, \ldots, f_n; 2, 2, \ldots, 2)$$

je zajisté aritmetická posloupnost dimenze n, která má délku $l(Q) = 2^n$ a obsahuje F jako podmnožinu. □

2.2 Freimanův izomorfismus

Podstatnou roli v důkazu Freimanovy věty hraje také Freimanem zavedený Freimanův izomorfismus. Jedná se o izomorfismus, který zachovává součty prvků a tedy i součty množin. V druhé části si ukážeme jednoduché vlastnosti Freimanova izomorfismu, které nám v dalších kapitolách poslouží jako nástroj v důkazu Freimanovy věty.

Buďte G a H dvě abelovské grupy a $A \subseteq G$ a $B \subseteq H$ jejich podmnožiny. Zobrazení $\psi : A \to B$ nazveme *Freimanovým homomorfismem řádu* h, jestliže z podmínky

$$a_1 + a_2 + \cdots + a_h = a'_1 + a'_2 + \cdots + a'_h,$$

platné pro libovolné $a_1, a_2, \ldots, a_h, a'_1, a'_2, \ldots, a'_h \in A$, plyne vztah

$$\psi(a_1) + \psi(a_2) + \cdots + \psi(a_h) = \psi(a'_1) + \psi(a'_2) + \cdots + \psi(a'_h).$$

Poté můžeme korektně definovat indukované zobrazení $\psi^{(h)} : hA \to hB$ vztahem

$$\psi^{(h)}(a_1 + a_2 + \cdots + a_h) = \psi(a_1) + \psi(a_2) + \cdots + \psi(a_h).$$

Jestliže navíc $\psi : A \to B$ je bijekce, tedy jestli

$$a_1 + a_2 + \cdots + a_h = a'_1 + a'_2 + \cdots + a'_h,$$

kde $a_1, a_2, \ldots, a_h, a'_1, a'_2, \ldots, a'_h \in A$, platí právě tehdy, když

$$\psi(a_1) + \psi(a_2) + \cdots + \psi(a_h) = \psi(a'_1) + \psi(a'_2) + \cdots + \psi(a'_h),$$

pak ψ nazveme *Freimanovým izomorfismem řádu* h. Budeme tedy psát, že množiny A a B jsou *Freimanovsky izomorfní řádu* h. Nebudeme-li zmiňovat řád Freimanova izomorfismu, myslíme tím automaticky řád $h = 2$. Taktéž můžeme korektně definovat indukované zobrazení $\psi^{(h)} : hA \to hB$ vztahem jako výše, které pak bude bijekcí.

Příklad 2.2.1. Pro lepší představivost uveďme dva příklady:

Nechť pro b, d, k, p přirozená čísla jsou definovány množiny A a B vztahy $A = [0, p-1]$ a $B = \{b + kd : 0 \leq k \leq (p-1)\}$. Pak zobrazení $\psi : A \to B$ definované vztahem $\psi(g) = b + gd$ pro $0 \leq g \leq p-1$ je Freimanovým izomorfismem řádu h pro libovolné $h \geq 2$.

Nechť $A = \{0, 1, 3\}$ a $B = \{(0, 0), (0, 1), (1, 1)\}$. Pak zobrazení $\psi : A \to B$ definované bodově vztahy $\psi(0) = (0, 0)$, $\psi(1) = (0, 1)$ a $\psi(3) = (1, 1)$ je Freimanův izomorfismus řádu $h = 2$, ale již ne řádu $h \geq 3$, neboť $3+0+0 = 1+1+1$, ale $\psi(3) + \psi(0) + \psi(0) \neq \psi(1) + \psi(1) + \psi(1)$.

Pozorování 2.2.2. Následuje několik poznatků o Freimanově homomorfismech a izomorfismech, které okamžitě plynou z definice:

(i) Jsou-li A a B grupy a je-li $\psi : A \to B$ grupový homomorfismus (resp. izomorfismus), pak ψ je také Freimanův homomorfismus (resp. izomorfismus) řádu h pro libovolné $h \geq 2$.

(ii) Jsou-li $\psi : A \to B$ a $\varphi : B \to C$ Freimanovy izomorfizmy řádu h, pak také $\varphi \circ \psi : A \to C$ je Freimanův izomorfismus řádu h.

(iii) Je-li $\psi : A \to B$ Freimanův izomorfismus řádu h a $h' \leq h$, pak ψ je Freimanův izomorfismus řádu h'.

(iv) Je-li $\psi : A \to B$ Freimanův izomorfismus řádu h, $A' \subset A$ a $B' = \psi(A')$, pak $\psi : A' \to B'$ je Freimanův izomorfismus řádu h.

Věta 2.2.3 *Buď G a H dvě abelovské grupy a Q buď n-dimenzionální aritmetická posloupnost v G. Buď $h \geq 2$. Jestliže $\psi : Q \to H$ je Freimanův homomorfismus řádu h, pak i $\psi(Q)$ je n-dimenzionální aritmetická posloupnost v H. Jestliže $\psi : Q \to \psi(Q)$ je Freimanův izomorfismus, pak Q je vlastní n-dimenzionální aritmetická podposloupnost v G tehdy a jen tehdy, když $\psi(Q)$ je vlastní n-dimenzionální aritmetická posloupnost v $\psi(G) \subseteq H$.*

Důkaz. Označme si $Q = Q(a; d_1, d_2, \ldots, d_n; l_1, l_2, \ldots, l_n)$. Je-li ψ Freimanův homomorfismus řádu h, pak definujeme pro $i = 1, 2, \ldots, n$ v H prvky

$$a' = \psi(a),$$

$$d'_i = \psi(a + d_i) - \psi(a).$$

Vzniklá množina $Q' = Q(a'; d'_1, d'_2, \ldots, d'_n; l_1, l_2, \ldots, l_n)$ je n-dimenzionální aritmetická posloupnost v H. Dokažme nyní, že $\psi(Q) = Q'$. K tomu nám stačí dokázat, že

$$\psi(a + x_1 d_1 + x_2 d_2 + \cdots + x_n d_n) = a' + x_1 d'_1 + x_2 d'_2 + \cdots + x_n d'_n \qquad (2.1)$$

platí pro libovolnou volbu $0 \leq x_i < l_i$, $i = 1, 2, \ldots, n$.

Tento důkaz provedeme indukcí podle hodnoty $m = \sum_{i=1}^{n} x_i$. Výsledek dostáváme ihned pro hodnoty $m = 0$ a $m = 1$ z definic čísel $a', d'_1, d'_2, \ldots, d'_n$.

Dokažme kýženou rovnost (2.1) pro $m+1$, víme-li, že platí pro m. Volme libovolné $x_k > 0$ a označme $r = a + x_1 d_1 + \cdots + x_n d_n$ a $r' = r - d_k$. Pak podle indukčního předpokladu platí rovnost

$$\psi(r') = a' + x_1 d'_1 + \cdots + (x_k - 1)d'_k + \cdots + x_n d'_n.$$

Použijme rovnost $r = r' + d_k$, která se mírnou úpravou změní na $r + a = r' + d_k + a$. Neboť ψ je Freimanův homomorfismus řádu alespoň 2, dostáváme vztah $\psi(r) + \psi(a) = \psi(r') + \psi(a + d_k)$. Nyní si stačí jen správně napsat $\psi(r)$ a máme vztah (2.1):

$$\psi(r) = \psi(r') + \psi(a + d_k) - \psi(a) = \psi(r') + d'_k = a' + x_1 d'_1 + \cdots + x_n d'_n.$$

Je-li ψ Freimanův izomorfismus řádu h, pak $|Q| = |\psi(Q)| = |Q'|$ a proto Q je vlastní právě když Q' je vlastní multidimenzionální aritmetická posloupnost. □

Věta 2.2.4 *Buď G a H dvě abelovské grupy a $A \subseteq G$ a $B \subseteq H$ jejich neprázdné konečné podmnožiny. Dále buďte h, k a l přirozená čísla a h' definované vztahem $h' = h(k + l)$. Jsou-li A a B Freimanovsky izomorfní řádu h', pak množiny $kA - lA$ a $kB - lB$ jsou Freimanovsky izomorfní řádu h.*

Důkaz. Buď $\psi : A \to B$ Freimanův izomorfismus řádu h'. Pak zobrazení $\psi^{(l)} : lA \to lB$, $\psi^{(k)} : kA \to kB$ a $\psi^{(k+l)} : kA + lA \to kB + lB$ indukované zobrazením ψ jsou dle definice bijekce, pro něž platí

$$\psi^{(k+l)}(a_1 + \cdots + a_{k+l}) = \psi^{(k)}(a_1 + \cdots + a_k) + \psi^{(l)}(a_{k+1} + \cdots + a_{k+l})$$

pro libovolné $a_1, a_2, \ldots, a_{k+l} \in A$. Vezměme $d \in kA - lA$, pro které existují $u, u' \in kA$ a $v, v' \in lA$ takové, že $d = u - v = u' - v'$. Díky tomu, že ψ je Freimanův izomorfismus řádu $h \geq (k + l)$ máme vztah

$$\psi^{(k)}(u) + \psi^{(l)}(v) = \psi^{(k+l)}(u + v') = \psi^{(k+l)}(u' + v) = \psi^{(k)}(u') + \psi^{(l)}(v),$$

který lze zapsat také jako

$$\psi^{(k)}(u) - \psi^{(l)}(v) = \psi^{(k)}(u') - \psi^{(l)}(v').$$

To však znamená, že zobrazení $\varphi : kA - lA \to kB - lB$ definované vztahem

$$\varphi(d) = \varphi(u - v) = \psi^{(k)}(u) - \psi^{(l)}(v)$$

je korektně definováno. Jelikož ψ je surjektivní, je i φ surjekce. Navíc φ je prosté, neboť pokud pro $d, d' \in kA - lA$ zapsané rovnostmi $d = u - v$ a $d' = u' - v'$, kde $u, u' \in kA$ a $v, v' \in lA$ platí $\varphi(d) = \varphi(d')$, pak

$$\psi^{(k+l)}(u + v') = \psi^{(k)}(u) + \psi^{(l)}(v') = \psi^{(k)}(u') + \psi^{(l)}(v) = \psi^{(k+l)}(u' + v),$$

což znamená, že $u + v' = u' + v$, neboli $d = d'$. Tedy φ je bijekce.

Nyní dokážeme, že φ je Freimanův izomorfismus řádu h. Vezměme si $d_i, d_i' \in kA - lA$ a definujme $u_i, u_i' \in kA$ a $v_i, v_i' \in lA$ vztahy $d_i = u_i - v_i$ a $d_i' = u_i' - v_i'$ pro $i = 1, 2, \ldots, h$. Pak z rovnosti

$$d_1 + \cdots + d_h = d_1' + \cdots + d_h'$$

plyne vztah

$$u_1 + \cdots + u_h + v_1' + \cdots + v_h' = u_1' + \cdots + u_h' + v_1 + \cdots + v_h.$$

Díky faktu, že ψ je Freimanův izomorfismus řádu $h' = h(k + l)$, dostáváme

$$\begin{aligned}
&\psi^{(k)}(u_1) + \cdots + \psi^{(k)}(u_h) + \psi^{(l)}(v_1') + \cdots + \psi^{(l)}(v_h') \\
&= \psi^{(h(k+l))}(u_1 + \cdots + u_h + v_1' + \cdots + v_h') \\
&= \psi^{(h(k+l))}(u_1' + \cdots + u_h' + v_1 + \cdots + v_h) \\
&= \psi^{(k)}(u_1') + \cdots + \psi^{(k)}(u_h') + \psi^{(l)}(v_1) + \cdots + \psi^{(l)}(v_h).
\end{aligned}$$

Nyní stačí všechny čárkované členy převést na jednu stranu, nečárkované na druhou a z definice φ máme

$$\varphi(d_1) + \cdots + \varphi(d_h) = \varphi(d_1') + \cdots + \varphi(d_h'),$$

tedy φ je Freimanův homomorfismus řádu h. Celý tento postup lze obrátit, platí tedy ekvivalence a zobrazení φ je Freimanův izomorfismus řádu h. □

2.3 Exponenciální součty

Tato sekce je jen příprava pro důkaz Bogoljubovovy věty. Odvodíme si zde několik pomocných lemmat, které se týkají exponenciálních součtů. Symbolem $\mathbb{Z}/m\mathbb{Z}$ budeme značit množinu všech zbytkových tříd modulo m.

Buďte $m \geq 2$ a x celá čísla, dále buď $a = r + m\mathbb{Z}$ prvek grupy $\mathbb{Z}/m\mathbb{Z}$. Definujme

$$e^{2\pi i a x/m} = e^{2\pi i r x/m},$$

což je korektní, neboť jsou-li $r \equiv r' \pmod{m}$, pak platí

$$e^{2\pi irx/m} = e^{2\pi ir'x/m}$$

pro libovolné $x \in \mathbb{Z}$.

Pro posloupnost $A = \{a_0, a_1, \ldots, a_{k-1}\}$ ne nutně různých zbytkových tříd v grupě $\mathbb{Z}/m\mathbb{Z}$ definujme exponenciální součet

$$S_A(x) = \sum_{j=0}^{k-1} e^{2\pi i a_j x/m}. \tag{2.2}$$

Pro $x \in \mathbb{C}$ označme $\overline{x}$ číslo komplexně sdružené k x. Obdobně budeme psát

$$\overline{S_A}(x) = \overline{\sum_{j=0}^{k-1} e^{2\pi i a_j x/m}} = \sum_{j=0}^{k-1} e^{-2\pi i a_j x/m} = S_{-A}(x) \tag{2.3}$$

Lemma 2.3.1 *Buď $m \geq 2$ přirozené číslo a $a \in \mathbb{Z}/m\mathbb{Z}$, pak*

$$\sum_{x=0}^{m-1} e^{2\pi iax/m} = \begin{cases} m & \text{pro } a = 0 \\ 0 & \text{pro } a \neq 0 \end{cases}$$

Důkaz. Uvažme $a = r + m\mathbb{Z}$. Je-li $r = 0$, pak všechny členy v součtu jsou jedničky, proto

$$\sum_{x=0}^{m-1} e^{2\pi irx/m} = \sum_{x=0}^{m-1} e^0 = m.$$

Nyní uvažme $r \in \{1, 2, \ldots, m-1\}$. Jelikož sčítáme x pro všechny přirozené hodnoty $1, 2, \ldots (m-1)$, můžeme si představit sumu jako konečný součet geometrické řady. Pro něj ale už máme vzorec. Jelikož $|e^{2\pi ir/m}| = 1$ a $e^{2\pi ir/m} \neq 1$, máme

$$\sum_{x=0}^{m-1} e^{2\pi irx/m} = \sum_{x=0}^{m-1} \left(e^{2\pi ir/m}\right)^x = \frac{1 - e^{2\pi im/m}}{1 - e^{2\pi ir/m}} = \frac{1-1}{1 - e^{2\pi ir/m}} = 0,$$

čímž jsme dokázali požadované tvrzení. □

Lemma 2.3.2 *Buďte pro přirozená čísla n a n' množiny $A_1, A_2, \ldots A_n$, $B_1, B_2, \ldots B_{n'}$ podmnožinami $\mathbb{Z}/m\mathbb{Z}$. Nechť K značí počet řešení rovnice*

$$a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_{n'} \pmod{m},$$

kde $a_i \in A_i$ *a* $b_j \in B_j$ *pro* $i = 1, 2, \ldots, n$ *a pro* $j = 1, 2, \ldots, n'$. *Pak*

$$Km = \sum_{x=0}^{m-1} S_{A_1}(x) S_{A_2}(x) \cdots S_{A_n}(x) \overline{S_{B_1}}(x) \overline{S_{B_2}}(x) \cdots \overline{S_{B_{n'}}}(x).$$

Důkaz. Podle definice (2.2) a (2.3) máme

$$\begin{aligned}
&\sum_{x=0}^{m-1} S_{A_1}(x) S_{A_2}(x) \cdots S_{A_n}(x) \overline{S_{B_1}}(x) \overline{S_{B_2}}(x) \cdots \overline{S_{B_{n'}}}(x) \\
&= \sum_{x=0}^{m-1} \left(\sum_{a_1 \in A_1} \cdots \sum_{a_n \in A_n} \sum_{b_1 \in B_1} \cdots \sum_{b_{n'} \in B_{n'}} e^{2\pi i (a_1 + \cdots + a_n - b_1 - \cdots - b_{n'}) x/m} \right) \\
&= \sum_{a_1 \in A_1} \cdots \sum_{a_n \in A_n} \sum_{b_1 \in B_1} \cdots \sum_{b_{n'} \in B_{n'}} \left(\sum_{x=0}^{m-1} e^{2\pi i (a_1 + \cdots + a_n - b_1 - \cdots - b_{n'}) x/m} \right).
\end{aligned}$$

Výraz

$$\sum_{x=0}^{m-1} e^{2\pi i (a_1 + \cdots + a_n - b_1 - \cdots - b_{n'}) x/m}$$

je podle předešlého Lemmatu 2.3.1 roven m pro každé řešení rovnice

$$a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_{n'}$$

a je jinak nulový, proto se hledaný součet rovná

$$\sum_{\substack{a_i \in A_i,\ i=1,\ldots n \\ b_j \in B_j,\ j=1,\ldots n' \\ a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_{n'}}} m = Km,$$

což jsme chtěli dokázat. □

Důsledek 2.3.3 *Buď* A *neprázdná podmnožina* $\mathbb{Z}/m\mathbb{Z}$ *s velikostí* $|A| = k$. *Pak*

$$\sum_{j=0}^{m-1} |S_A(x)|^2 = km.$$

Důkaz. Jelikož počet řešení rovnice $a = a'$ pro $a, a' \in A$ je $|A| = k$, použijeme Lemma 2.3.2 a dostáváme

$$\sum_{j=0}^{m-1} |S_A(x)|^2 = \sum_{j=0}^{m-1} S_A(x) \overline{S_A}(x) = km.$$

□

Kapitola 3

Freimanova věta

3.1 Znění Freimanovy věty

Podle Věty 1.2.3 víme, že každá konečná množina přirozených čísel splňující $|2A| = 2|A| - 1$ je již aritmetickou posloupností. Mírným zobecněním tohoto tvrzení je Poznámka 1.2.4, ve které se zkoumají konečné množiny přirozených čísel s vlastností $|2A| \leq 3|A| - 4$, ještě silnější tvrzení je Věta 1.3.2.

Freiman však objevil a dokázal obecnější verzi, která tvrdí, že libovolná množina A přirozených čísel malá ve smyslu $|2A| \leq c|A|$, pak A je obsažena v multidimenzionální aritmetické posloupnosti, jejíž dimenze a délka jsou závislé pouze na konstantě c. Formálněji formulujme Freimanovu větu následovně:

Věta 3.1.1 (Freiman) *Buď c kladná reálná konstanta. Je-li A je množina přirozených čísel taková, že $|A| = k$ a*

$$|2A| \leq c|A|,$$

pak A je podmnožinou n-dimenzionální aritmetické posloupnosti délky maximálně $lk = l|A|$, kde n a l závisejí pouze na c.

Důkaz. Plyne okamžitě z Věty 3.3.2 volbou $A = B$, $c_1 = c_2 = 1$ a $c_3 = c$. Tato věta je dokázána na konci kapitoly. □

Poznámka 3.1.2. Dají se formulovat a dokázat i silnější verze Freimanovy věty. Například, množina A může být podmnožinou abelovské grupy G místo množiny $\mathbb{N}$ (viz 3.3.4), nebo také velikost množin A a B může být omezena

konstantami c_1 a c_2 (viz 3.3.2). V obou případech zobecnění platí, jak si ukážeme na konci kapitoly.

Ačkoli Freimanova věta byla dokázána již v roce 1964, nepodařilo se doposud prokázat ani vyvrátit platnost obdobného tvrzení pro množiny splňující $|hA| \leq c|A|$. Řada problémů kolem této věty proto stále zůstává nezodpovězených.

3.2 Bogoljubovova věta a její aplikace

Účelem této sekce bude dokázat větu, která tvrdí, že je-li A podmnožina $\mathbb{Z}/p\mathbb{Z}$, kde p je prvočíslo a $|A| > \alpha p$, pak množina $2A - 2A$ obsahuje n-dimenzionální aritmetickou posloupnost, která má v jistém smyslu velkou délku. Zde už je vidět určitá spojitost s Freimanovou větou. Důkaz provedeme Bogoljubovovou metodou.

Pro přirozená čísla $a_1, a_2, \ldots, a_n$ budeme symbolem $(a_1, a_2, \ldots, a_n)$ značit největší společný dělitel.

Zavedeme normu $\|x\| : \mathbb{R} \to [0, \frac{1}{2}]$, která udává vzdálenost reálného čísla x od nejbližšího celého čísla. Proto je obor hodnot interval $[0, \frac{1}{2}]$. Buď $m \geq 2$ přirozené číslo. Jelikož pro libovolné $a, b \in \mathbb{Z}$ takové, že $a \equiv b \pmod m$ platí $\|\frac{a}{m}\| = \|\frac{b}{m}\|$, je tato norma korektně definovaná na zbytkových třídách modulo m. Proto můžeme pro $c \in \mathbb{Z}/m\mathbb{Z}$, $c = x + m\mathbb{Z}$ korektně definovat $\left\|\frac{c}{m}\right\| = \left\|\frac{x}{m}\right\|$.

Jsou-li $c_1, c_2, \ldots, c_n \in \mathbb{Z}/m\mathbb{Z}$ a $\varepsilon > 0$, potom definujeme *Bohrovo ε-okolí prvku* $(c_1, c_2, \ldots, c_n)$ vztahem

$$B(c_1, c_2, \ldots, c_n; \varepsilon) = \left\{ a \in \mathbb{Z}/m\mathbb{Z} : \left\| \frac{ac_i}{m} \right\| \leq \varepsilon \text{ pro } i = 1, 2, \ldots, n \right\}.$$

Ihned vidíme, že $B(0, \varepsilon) = \mathbb{Z}/m\mathbb{Z}$ pro libovolné $\varepsilon > 0$.

Věta 3.2.1 (Bogoljubov) *Buď $m \geq 2$ a A neprázdná podmnožina $\mathbb{Z}/m\mathbb{Z}$. Buď α definováno vztahem $|A| = \alpha m$. Pak existuje $n \leq \alpha^{-2}$ a existují po dvou různé zbytkové třídy $c_1, c_2, \ldots, c_n \in \mathbb{Z}/m\mathbb{Z}$ takové, že $c_1 = 0$ a*

$$B(c_1, c_2, \ldots, c_n; \frac{1}{4}) \subseteq 2A - 2A.$$

Důkaz. Označme $Z = \mathbb{Z}/m\mathbb{Z}$. Pro $z \in Z$ definujme charakteristickou funkci $\chi_z : Z \to \mathbb{C}$ vztahem

$$\chi_z(a) = e^{2\pi i z a/m},$$

a již dříve používanou funkci

$$S_A(z) = \sum_{a\in A} \chi_z(a) = \sum_{a\in A} e^{2\pi iza/m}.$$

Triviálně vidíme, že $\chi_0(a) = 1$ pro všechna $a \in A$ a proto $S_A(0) = |A|$. Z Důsledku 2.3.3 dostáváme pro $z \in Z$ rovnost

$$\sum_{z\in Z} |S_A(z)|^2 = m|A| \tag{3.1}$$

a podle Lemmatu 2.3.2, počítáme-li obdobně jako v důkazu Důsledku 2.3.3 dostaneme pro $a \in A$ vztah

$$\sum_{z\in G} |S_A(z)|^4 \chi_z(a) = \sum_{z\in G} \sum_{a_1,a_2,b_1,b_2\in A} e^{2\pi iz(b_1+b_2-a_1-a_2+a)/m}. \tag{3.2}$$

Tento součet je nenulový právě když a lze vyjádřit ve tvaru $a = a_1 + a_2 - b_1 - b_2$, kde $a_1, a_2, b_1, b_2 \in A$, což jinak napsáno znamená, že $a \in 2A - 2A$. Rozdělme si nyní množinu Z na dvě disjunktní množiny Z_1 a Z_2 následovně:

$$Z_1 = \left\{ z \in Z : |S_A(z)| \geq \sqrt{\alpha}|A| \right\}, \tag{3.3}$$

$$Z_2 = \left\{ z \in Z : |S_A(z)| < \sqrt{\alpha}|A| \right\}. \tag{3.4}$$

Počítejme

$$\begin{aligned}\left| \sum_{z\in Z_2} |S_A(z)|^4 \chi_z(a) \right| &\leq \sum_{z\in Z_2} |S_A(z)|^4 \overset{(3.4)}{\leq} \alpha|A|^2 \sum_{z\in Z_2} |S_A(z)|^2 \\ &\overset{0\in Z_1}{<} \alpha|A|^2 \sum_{z\in Z} |S_A(z)|^2 \overset{(3.1)}{=} \alpha|A|^2 m|A| \\ &= \alpha|A|^2\alpha^{-1}|A|^2 = |A|^4. \end{aligned} \tag{3.5}$$

Označme prvky množiny $Z_1 = \{c_1, c_2, \ldots, c_n\}$. Protože $|A| \geq \sqrt{\alpha}|A|$, je $0 \in Z_1$ a proto BÚNO $c_1 = 0$. Vezměme libovolné $a \in B(c_1, c_2, \ldots, c_n; \frac{1}{4})$. Pak

$$\left\| \frac{c_i a}{m} \right\| \leq \frac{1}{4}$$

pro $i = 1, 2, \ldots, n$, z čehož plyne

$$\Re(\chi_{c_i}(a)) = \Re(e^{2\pi ic_i a/m}) = \cos(2\pi c_i a/m) \geq 0, \tag{3.6}$$

neboť pro libovolné $x \in \mathbb{R}$ platí

$$\|x\| \leq \frac{1}{4} \;\Leftrightarrow\; \cos(2\pi x) \geq 0.$$

Proto máme

$$\begin{aligned}
&\Re\left(\sum_{z\in Z}|S_A(z)|^4\chi_z(a)\right)\\
&=\Re\left(\sum_{z\in Z_1}|S_A(z)|^4\chi_z(a)\right)+\Re\left(\sum_{z\in Z_2}|S_A(z)|^4\chi_z(a)\right)\\
&=|A|^4+\sum_{z\in Z_1\setminus\{0\}}|S_A(z)|^4\Re(\chi_z(a))+\Re\left(\sum_{z\in Z_2}|S_A(z)|^4\chi_z(a)\right)\\
&\overset{(3.6)}{\geq}|A|^4+\Re\left(\sum_{z\in Z_2}|S_A(z)|^4\chi_z(a)\right)\\
&\geq|A|^4-\left|\sum_{z\in Z_2}|S_A(z)|^4\chi_z(a)\right|\overset{(3.5)}{>}0.
\end{aligned}$$

Tedy

$$\Re\left(\sum_{z\in Z}|S_A(z)|^4\chi_z(a)\right)\neq 0$$

pro libovolné $a \in B(c_1, c_2, \ldots, c_n; \frac{1}{4})$ a podle (3.2) máme

$$B(c_1, c_2, \ldots, c_n; \frac{1}{4}) \subseteq 2A - 2A.$$

Nakonec odhadneme $n = |Z_1|$. Protože $|S_A(z)| \geq \sqrt{\alpha}|A|$ pro libovolné $a \in Z_1$, dostáváme

$$n\alpha|A|^2 \overset{(3.3)}{\leq} \sum_{z\in Z_1}|S_A(z)|^2 \leq \sum_{z\in Z}|S_A(z)|^2 \overset{(3.1)}{=} m|A| = \alpha^{-1}|A|^2,$$

a proto $n \leq \alpha^{-2}$, což jsme chtěli dokázat. □

Pro důkaz jedné z podstatných vět této sekce budeme potřebovat několik pojmů z geometrie čísel.

Pro množinu $M \subset \mathbb{R}^n$ označme $\mathrm{vol}(M)$ n-rozměrnou Lebesgueovu míru množiny M. Buď dále $\{a_1, a_2, \ldots, a_n\}$ báze Euklidovského prostoru $\mathbb{R}^n$. Abelovská grupa generovaná těmito n nezávislými vektory je množina všech vektorů tvaru

$$u_1 a_1 + u_2 a_2 + \cdots + u_n a_n,$$

kde $u_1, \ldots, u_n \in \mathbb{Z}$. Řekneme, že Λ je *mřížka v* $\mathbb{R}^n$, jestliže Λ je abelovská grupa generovaná množinou nezávislých vektorů.

Buď $\{e_1, e_2, \ldots, e_n\}$ standartní báze Euklidovského prostoru. Jsou-li vektory a_j zadané pro $j = 1, 2, \ldots n$ vztahem

$$a_j = \sum_{i=1}^{n} a_{ij} e_i,$$

pak $n \times n$ matici $A = \{a_{ij}\}_{i,j=1}^{n}$ nazveme *matici vektorů* $a_1, a_2, \ldots, a_n$. Dále definujeme *determinant mřížky* Λ vztahem $\det(\Lambda) = |\det(A)|$. Nakonec ještě zmiňme, že *elementární rovnoběžnostěn* mřížky Λ vzhledem k bázi $\{a_1, a_2, \ldots, a_n\}$ je množina

$$F(\Lambda) = \{\sum_{i=1}^{n} x_i a_i : 0 \leq x_i \leq 1 \text{ pro } i = 1, \ldots, n\} \subseteq \mathbb{R}^n.$$

Mezi determinantem a elementárním rovnoběžnostěnem lze dokázat vztah $\det(\Lambda) = F(\Lambda)$.

Věta 3.2.2 (Minkowski - obecná verze) *Buď K symetrická (kolem počátku) konvexní množina v $\mathbb{R}^n$ a buď Λ mřížka v $\mathbb{R}^n$. Pak existují reálná čísla $\lambda_1, \lambda_2, \ldots, \lambda_n$ a k nim příslušné lineárně nezávislé vektory $b_1, b_2, \ldots, b_n \in \Lambda$ takové, že $b_i \in \overline{\lambda_i K} \cap \Lambda$ pro libovolné $i = 1, \ldots, n$ a*

$$\lambda_1 \lambda_2 \cdots \lambda_n \,\mathrm{vol}(K) \leq 2^n \det(\Lambda).$$

Poznámka 3.2.3. Lze ukázat, že rovnost v předchozí nerovnosti může nastat, proto je Minkowského věta v tomto smyslu nejlepší možná.

V geometrii čísel se čísla $\lambda_1, \lambda_2, \ldots, \lambda_n$ definují (v závislosti na K a Λ) jako samostatný pojem *postupná minima* a definují se vztahy

$$\lambda_k = \inf\{\lambda > 0 : \lambda * K \text{obsahuje } k \text{ lineárně nezávislých prvků } \Lambda\}.$$

Minkowského větu si stejně jako následující Lemma nebudeme dokazovat. Ne proto, že by to byla příliš obtížná tvrzení, ale jejich důkazy vyžadují zavedení dalších pojmů z geometrie čísel. Náruživý čtenář si je může přečíst v knize [1] na stranách 181 a 194.

Lemma 3.2.4 *Buď $m \geq 2$ a $c = (c_1, c_2, \ldots, c_n)$ vektor v $\mathbb{Z}^n$ takový, že $(c_1, c_2, \ldots, c_n, m) = 1$. Definujme množinu*

$$M = \{v = (v_1, \ldots, v_n) \in \mathbb{Z}^n : v_i \equiv 0 \pmod{m} \text{ pro } i = 1, 2, \ldots, n\}.$$

Pak množina vektorů

$$\Lambda = \bigcup_{q=0}^{m-1} (qc + M)$$

je mřížka a $\det(\Lambda) = m^{n-1}$.

Věta 3.2.5 *Buď $m, n \in \mathbb{N}$ takové, že $m \geq 2$ a buď $C = \{c_1, c_2, \ldots, c_n\}$ množina zbytkových tříd modulo m, pro kterou platí $(c_1, c_2, \ldots, c_n, m) = 1$. Pak existuje vlastní n-dimenzionální aritmetická posloupnost Q v $\mathbb{Z}/m\mathbb{Z}$ s vlastnostmi*

$$Q \subseteq B(c_1, c_2, \ldots, c_n; \frac{1}{4}) \quad a \quad |Q| = l(Q) \geq \frac{m}{(4n)^n}.$$

Důkaz. V důkazu použijeme předchozí poznatky z geometrie čísel. Buďte $u = (u_1, u_2, \ldots, u_n)$ a $v = (v_1, v_2, \ldots, v_n)$ dva vektory v $\mathbb{Z}^n$. Platí-li $u_i \equiv v_i \pmod{m}$ pro všechna $i = 1, \ldots, n$, budeme psát $u \equiv v \pmod{m}$. Definujme množinu M vztahem

$$M = \{v \in \mathbb{Z}^n : v \equiv 0 \pmod{m}\}.$$

Pak $M = (m\mathbb{Z})^n$ a determinant M je roven $\det(M) = m^n$.

Buďte dle předpokladů $c_1, c_2, \ldots, c_n$ zbytkové třídy modulo m pro něž platí $(c_1, c_2, \ldots, c_n, m) = 1$. Definujme $c = (c_1, c_2, \ldots, c_n)$. Buď Λ množina vektorů $u \in \mathbb{Z}^n$ tvaru $u \equiv qc \pmod{m}$ pro nějaké $q = 0, 1, \ldots, (m-1)$, neboli

$$\Lambda = \bigcup_{q=0}^{m-1} (qc + M).$$

Pak dle Lemmatu 3.2.4 je Λ mřížka, jejíž determinant je roven m^{n-1}.

Označme K n-dimenzionální krychli obsahující všechny vektory tvaru $x = (x_1, x_2, \ldots, x_n)$ splňující $|x_i| < \frac{1}{4}$ pro $i = 1, \ldots, n$. Pak K je konvexní symetrická množina a $\mathrm{vol}(K) = 1/2^n$. Tudíž dle Minkowského Věty 3.2.2 existují reálná čísla $\lambda_1, \lambda_2, \ldots, \lambda_n$ a k nim příslušné lineárně nezávislé vektory

$b_1, b_2, \ldots, b_n \in \Lambda$ takové, že $b_i = (b_{i1}, b_{i2}, \ldots, b_{in}) \in \overline{\lambda_i K} \cap \Lambda$ pro libovolné $i = 1, \ldots, n$ a

$$\lambda_1 \lambda_2 \cdots \lambda_n \leq \frac{2^n \det(\Lambda)}{\mathrm{vol}(K)} = 4^n m^{n-1}. \tag{3.7}$$

Jelikož pro libovolné $i = 1, \ldots, n$ máme

$$b_i \in \overline{\lambda_i K} = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n : |x_i| \leq \frac{\lambda_i}{4} \text{ pro } i = 1, \ldots, n\},$$

pak musí též pro $i, j = 1, \ldots, n$ platit

$$|b_{ij}| \leq \frac{\lambda_i}{4}. \tag{3.8}$$

Vektory b_i jsou ale dle Minkowského věty v mřížce Λ, proto $b_i \equiv q_i c \pmod m$ pro nějaké $q_i \in [0, m-1]$, z čehož dostaneme

$$b_{ij} \equiv q_i c_j \pmod m \tag{3.9}$$

pro libovolné $i, j = 1, \ldots, n$. Pro

$$l_i' = \left\lfloor \frac{m}{n\lambda_i} \right\rfloor \tag{3.10}$$

definujme hledanou n-dimenzionální aritmetickou posloupnost Q vztahem

$$Q = \{x_1 q_1, \ldots, x_n q_n : -l_i' \leq x_i \leq l_i' \text{ pro } i = 1, \ldots, n\}.$$

Stačí nám tedy dokázat, že $Q \subseteq B(c_1, c_2, \ldots, c_n; \frac{1}{4})$, Q je vlastní a $|Q| \geq \frac{m}{(4n)^n}$. Ukažme postupně všechny tyto vlastnosti.

Pro důkaz $Q \subseteq B(c_1, c_2, \ldots, c_n; \frac{1}{4})$ vezměme $x = x_1 q_1 + \cdots + x_n q_n \in Q$, pro nějaké hodnoty $|x_i| < l_i'$ a libovolný index $i = 1, \ldots, n$. Víme, že

$$x c_j = \sum_{i=1}^{n} x_i q_i c_j \overset{(3.9)}{\equiv} \sum_{i=1}^{n} x_i b_{ij} \pmod m, \tag{3.11}$$

což nám dává

$$\left\| \frac{x c_j}{m} \right\| \overset{(3.11)}{=} \left\| \sum_{i=1}^{n} \frac{x_i b_{ij}}{m} \right\| \leq \left| \sum_{i=1}^{n} \frac{x_i b_{ij}}{m} \right| \leq \sum_{i=1}^{n} \frac{|x_i||b_{ij}|}{m}$$
$$< \sum_{i=1}^{n} \frac{l_i' |b_{ij}|}{m} \overset{(3.8)}{\leq} \sum_{i=1}^{n} \frac{l_i' \lambda_i}{4m} \overset{(3.10)}{\leq} \sum_{i=1}^{n} \frac{1}{4n} = \frac{1}{4},$$

tedy $x \in B(c_1, c_2, \ldots, c_n; \frac{1}{4})$ a proto máme

$$Q \subseteq B(c_1, c_2, \ldots, c_n; \frac{1}{4}).$$

Dále ukážeme, že Q je vlastní n-dimenzionální aritmetická posloupnost. Sporem, připusťme rovnost dvou prvků

$$x_1q_1 + \cdots + x_nq_n \equiv y_1q_1 + \cdots + y_nq_n \pmod{m},$$

kde $-l'_i \leq x_i, y_i \leq l'_i$ pro $i = 1, \ldots, n$. Definujme rozdíl $z_i = x_i - y_i$. Pak máme

$$|z_i| \leq 2l'_i \tag{3.12}$$

a

$$\sum_{i=1}^{n} q_i z_i \equiv 0 \pmod{m}.$$

Proto jako předešle pro $j = 1, \ldots, n$ dostáváme

$$c_j \sum_{i=1}^{n} q_i z_i \overset{(3.9)}{=} \sum_{i=1}^{n} b_{ij} z_i \equiv 0 \pmod{m}. \tag{3.13}$$

Počítejme

$$\left| \sum_{i=1}^{n} b_{ij} z_i \right| \leq \sum_{i=1}^{n} |b_{ij}||z_i| \overset{(3.8)}{\leq} \sum_{i=1}^{n} \frac{\lambda_i |z_i|}{4} \overset{(3.12)}{\leq} \sum_{i=1}^{n} \frac{\lambda_i l'_i}{2} \overset{(3.10)}{\leq} \sum_{i=1}^{n} \frac{m}{2n} = \frac{m}{2} < m.$$

Z čehož společně s (3.13) plyne $\sum_{i=1}^{n} b_{ij} z_i = 0$ pro libovolné $j = 1, \ldots, n$ a tudíž

$$\sum_{i=1}^{n} b_i z_i = 0.$$

Vektory b_i jsou však lineárně nezávislé, proto $z_i = 0$ pro libovolné $i = 1, \ldots, n$. Tedy Q je vlastní n-dimenzionální aritmetická posloupnost.

Nyní odhadněme zdola délku Q. Nejprve si Q zapišme trochu jednodušeji. Definujeme-li $a = -\sum_{i=1}^{n} l'_i q_i$ a $l_i = 2l'_i + 1$ pro $i = 1, \ldots, n$, pak

$$\begin{aligned} Q &= \{x_1q_1, \ldots, x_nq_n : -l'_i \leq x_i \leq l'_i \text{ pro } i = 1, \ldots, n\} \\ &= \{a + x_1q_1, \ldots, x_nq_n : 0 \leq x_i < l_i \text{ pro } i = 1, \ldots, n\} \\ &= Q(a; q_1, \ldots, q_n; l_1, \ldots, l_n). \end{aligned}$$

Nyní již snadno upravujme délku Q:

$$|Q| = \prod_{i=1}^{n} l_i = \prod_{i=1}^{n}(2l_i' + 1) \geq \prod_{i=1}^{n}(l_i' + 1) \overset{(3.10)}{>} \prod_{i=1}^{n} \frac{m}{n\lambda_i}$$
$$= \left(\frac{m}{n}\right)^n \prod_{i=1}^{n} \frac{1}{\lambda_i} \overset{(3.7)}{\geq} \left(\frac{m}{n}\right)^n \frac{1}{4^n m^{n-1}} = \frac{m}{(4n)^n},$$

což jsme chtěli dokázat. □

Věta 3.2.6 *Buď $p \in \mathbb{N}$ prvočíslo a A podmnožina $\mathbb{Z}/p\mathbb{Z}$. Definujme $\alpha \in \mathbb{R}$ vztahem $|A| = \alpha p$. Potom existuje $n \leq \alpha^{-2}$ a na něm závislá vlastní n-dimenzionální aritmetická posloupnost Q v $\mathbb{Z}/p\mathbb{Z}$ pro kterou platí*

$$Q \subseteq 2A - 2A$$

a

$$|Q| = l(Q) > \delta p, \quad \text{kde } \delta = \frac{1}{(4n)^n} > \left(\frac{\alpha^2}{4}\right)^{\alpha^{-2}}.$$

Důkaz. Nejprve vyřešme případ $2A-2A = \mathbb{Z}/p\mathbb{Z}$. Uvažujme 1-dimenzionální aritmetickou posloupnost $Q = Q(0; 1; p) = \mathbb{Z}/p\mathbb{Z}$, pro kterou jistě platí

$$|Q| = p > \delta p,$$

neboť $\delta < 1$.

Uvažujme $2A - 2A \neq \mathbb{Z}/p\mathbb{Z}$. Podle Bogoljubovovy Věty 3.2.1 existuje $n \leq \alpha^{-2}$ zbytkových tříd $c_1, c_2, \ldots, c_n$ modulo p takových, že $c_1 = 0$ a

$$B(c_1, c_2, \ldots, c_n; \frac{1}{4}) \subseteq 2A - 2A.$$

Kdyby $n = 1$, pak $c_1 = 0$ a máme

$$\mathbb{Z}/p\mathbb{Z} \supsetneq 2A - 2A \supseteq B(0; \frac{1}{4}) = \mathbb{Z}/p\mathbb{Z},$$

což evidentně neplatí. Proto musí být $n \geq 2$. Pak ale máme $(c_1, p) = 1$, neboť $c_1 < p$ a p je prvočíslo. Proto $(c_1, c_2, \ldots, c_n, m) = 1$. Můžeme tudíž použít předchozí Větu 3.2.5 podle které v $\mathbb{Z}/p\mathbb{Z}$ existuje n-dimenzionální aritmetická posloupnost Q s vlastnostmi

$$Q \subseteq 2A - 2A$$

a

$$|Q| \geq \frac{p}{(4n)^n} = \delta p,$$

což jsme chtěli dokázat. □

3.3 Ruzsův důkaz Freimanovy věty

V této sekci si předvedeme stěžejní a poslední část důkazu Freimanovy věty. Takto dokázanou ji publikoval I. Z. Rusza roku 1992 ve svém článku [2].

Věta 3.3.1 *Buď W konečná neprázdná množina přirozených čísel a $h \geq 2$. Je-li*

$$m > 4h|hW - hW|,$$

pak existuje podmnožina W' množiny W taková, že

$$|W'| \geq \frac{|W|}{h}$$

a W' je Freimanovsky izomorfní řádu h nějaké množině zbytkových tříd modulo m.

Důkaz. Značme $D = hW - hW$. Buď p prvočíslo splňující

$$p > \max\{m, 2h \max_{w \in W} |w|\}. \tag{3.14}$$

Ve zbývající části důkazu zkonstruujeme postupně pro každé $1 \leq q \leq p-1$ zobrazení $\phi_q : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ a následně dokážeme, že existují q a $W' \subset W \subset \mathbb{Z}$ takové, že $|W'| \geq |W|/h$ a ϕ_q restringované na W' je Freimanův izomorfismus řádu h.

Definujme tedy zobrazení $\phi_q : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ jako složení čtyř zobrazení $\phi_q = \delta \circ \gamma \circ \beta_q \circ \alpha$ vztahem

$$\mathbb{Z} \xrightarrow{\alpha} \mathbb{Z}/p\mathbb{Z} \xrightarrow{\beta_q} \mathbb{Z}/p\mathbb{Z} \xrightarrow{\gamma} \mathbb{Z} \xrightarrow{\delta} \mathbb{Z}/m\mathbb{Z},$$

přičemž zobrazení $\alpha, \beta_q, \gamma, \delta$ budeme definovat postupně v průběhu důkazu.

Buď $\alpha : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ zobrazení, které libovolnému $w \in \mathbb{Z}$ přiřadí jeho zbytkovou třídu $w + p\mathbb{Z}$. Takto definované zobrazení je grupový homomorfismus, a proto podle Pozorování 2.2.2(i) i Freimanův homomorfismus řádu h pro libovolné $h \geq 2$. Není to však Freimanův izomorfizmus řádu h, neboť $(p-1+p\mathbb{Z})+(4+p\mathbb{Z}) = 3+p\mathbb{Z}$, ale $(p-1)+4 \neq 3$. Proto omezme zobrazení α jen na množinu W, kde pak díky naší volbě p ukážeme, že α je Freimanův izomorfismus řádu h. Buďte tedy $w_1, w_2, \ldots, w_h, w_1', w_2', \ldots, w_h' \in W$ splňující

$$\alpha(w_1) + \alpha(w_2) + \cdots + \alpha(w_h) = \alpha(w_1') + \alpha(w_2') + \cdots + \alpha(w_h'),$$

neboli

$$\alpha(w_1 + w_2 + \cdots + w_h - w_1' - w_2' - \cdots - w_h') = 0,$$

což podle definice α znamená

$$w_1 + w_2 + \cdots + w_h - w_1' - w_2' - \cdots - w_h' \equiv 0 \pmod{p}.$$

Jelikož ale podle volby p je

$$|w_1 + w_2 + \cdots + w_h - w_1' - w_2' - \cdots - w_h'| \leq 2h \max_{w \in W} |w| < p,$$

dostáváme

$$w_1 + w_2 + \cdots + w_h = w_1' + w_2' + \cdots + w_h',$$

což jsme chtěli. A proto zobrazení $\alpha : W \to \alpha(W)$ je Freimanův izomorfismus řádu h.

Uvažujme $1 \leq q \leq p-1$. Druhé zobrazení $\beta_q : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ nechť zbytkové třídě $w + p\mathbb{Z}$ přiřadí zbytkovou třídu $qw + p\mathbb{Z}$. Takto definované zobrazení je grupový izomorfismus a proto podle Pozorování 2.2.2(i) je β_q také Freimanův izomorfismus řádu h, tedy i zobrazení $\beta_q : \alpha(W) \to \beta_q(\alpha(W))$ je Freimanův izomorfismus řádu h.

Nechť třetí zobrazení $\gamma : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}$ přiřadí zbytkové třídě $w + p\mathbb{Z}$ jejího nejmenšího nezáporného zástupce, tj. přirozené číslo z intervalu $[0, p-1]$, které leží v této zbytkové třídě. Toto zobrazení bohužel není Freimanův homomorfismus řádu h, stačí zase vzít $(p-1+p\mathbb{Z}) + (4+p\mathbb{Z}) = 3+p\mathbb{Z}$, ale $(p-1)+4 \neq 3$. Naštěstí ale umíme zapsat $\mathbb{Z}/p\mathbb{Z}$ jako sjednocení h množin, na nichž už γ bude Freimanův izomorfizmus řádu h. Definujme pro $j = 1, 2, \ldots, h$

$$U_j = \gamma^{-1}\left(\left[\frac{(j-1)(p-1)}{h}, \frac{j(p-1)}{h}\right]\right) \subseteq \mathbb{Z}/p\mathbb{Z}. \tag{3.15}$$

Snadno vidíme, že

$$\mathbb{Z}/p\mathbb{Z} = \bigcup_{j=1}^{h} U_j,$$

neboť platí

$$[0, p-1] = \bigcup_{j=1}^{h} \left[\frac{(j-1)(p-1)}{h}, \frac{j(p-1)}{h}\right].$$

Dokážeme nyní, že γ restringováno na U_j jsou Freimanovy izomorfismy řádu h. Buďte $w_i + p\mathbb{Z}, w_i' + p\mathbb{Z} \in U_j$ pro $i = 1, 2, \ldots, h$ takové, že

$$w_1 + w_2 + \cdots + w_h + p\mathbb{Z} = w_1' + w_2' + \cdots + w_h' + p\mathbb{Z}.$$

Pak

$$\sum_{i=1}^{h} \gamma(w_i + p\mathbb{Z}) \equiv \sum_{i=1}^{h} \gamma(w_i' + p\mathbb{Z}) \pmod{p}. \tag{3.16}$$

Neboť se jedná o prvky z U_j, musí pro obě sumy dle (3.15) platit

$$\sum_{i=1}^{h} \gamma(w_i + p\mathbb{Z}) \in [(j-1)(p-1), j(p-1)],$$

$$\sum_{i=1}^{h} \gamma(w_i' + p\mathbb{Z}) \in [(j-1)(p-1), j(p-1)],$$

což znamená, že

$$\left| \sum_{i=1}^{h} \gamma(w_i + p\mathbb{Z}) - \sum_{i=1}^{h} \gamma(w_i' + p\mathbb{Z}) \right| \leq p - 1,$$

a proto dle (3.16) γ restringováno na U_j je Freimanův homomorfismus řádu h. To, že se jedná o Freimanův izomorfismus řádu h plyne jednoduše z definice zobrazení γ, protože $\sum_{i=1}^{h} \gamma(w_i + p\mathbb{Z}) = \sum_{i=1}^{h} \gamma(w_i' + p\mathbb{Z})$ podle 2.2.2(i) okamžitě implikuje $w_1 + w_2 + \cdots + w_h + p\mathbb{Z} = w_1' + w_2' + \cdots + w_h' + p\mathbb{Z}$, neboť γ^{-1} je grupový homomorfismus.

Definujme

$$W_{j,q} = W \cap \alpha^{-1}(\beta_q^{-1}(U_j)).$$

Jelikož $\cup_{j=1}^{h} W_{j,q} = W$ vidíme, že musí existovat $k \leq h$ takové, že

$$|W_{k,q}| \geq \frac{|W|}{h}. \tag{3.17}$$

Označme tedy $W_q' = W_{k,q}$. Zavedeme-li zobrazení $\theta_q : W \to \mathbb{Z}$ vztahem $\theta_q = \gamma \circ \beta_q \circ \alpha$ a definujeme-li $V_q = \theta_q(W) \subseteq [0, p-1]$ a $V_q' = \theta_q(W_q') \subseteq [0, p-1]$, pak

$$\theta_q : W_q' \to V_q'$$

je Freimanův izomorfismus řádu h dle Pozorování 2.2.2(i) a (iv), protože zobrazení α, β_q a γ jsou na příslušných množinách Freimanovy izomorfismy řádu h.

Poslední zobrazení $\delta : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ nechť přirozeně zobrazuje w na $w + m\mathbb{Z}$. Jelikož se jedná o grupový homomorfismus, je tedy δ i Freimanův homomorfismus dle Pozorování 2.2.2(i). V další části ukážeme, že existuje $1 \leq q \leq p-1$ takové, že $\delta : V_q \to \mathbb{Z}/m\mathbb{Z}$ je Freimanův izomorfismus řádu h.

Toto tvrzení dokážeme sporem. Vyberme si libovolné $1 \leq q \leq p-1$. Jelikož zobrazení $\delta : V_q \to \mathbb{Z}/m\mathbb{Z}$ není Freimanův izomorfismus řádu h, existují $v_i, v_i' \in V_q$ pro $i = 1, 2, \ldots, h$, které splňují

$$v_1 + v_2 + \cdots + v_h \neq v_1' + v_2' + \cdots + v_h', \tag{3.18}$$

$$\delta(v_1) + \delta(v_2) + \cdots + \delta(v_h) = \delta(v_1') + \delta(v_2') + \cdots + \delta(v_h'). \tag{3.19}$$

Definujeme-li v^* vztahem $v^* = v_1 + v_2 + \cdots + v_h - v_1' - v_2' - \cdots - v_h'$, pak z (3.19) plyne

$$\delta(v^*) = \delta(v_1 + v_2 + \cdots + v_h - v_1' - v_2' - \cdots - v_h') = 0 + m\mathbb{Z}$$

a proto dle předchozího a (3.18)

$$v^* \equiv 0 \pmod{m} \quad \text{a} \quad v^* \neq 0. \tag{3.20}$$

Dále z definice v^* máme

$$|v^*| \leq h(p-1) < hp < mp. \tag{3.21}$$

Definujme $w_i, w_i' \in W$ pro $i = 1, 2, \ldots, h$ jako vzory v_i, v_i' v zobrazení θ_q, tedy

$$\theta_q(w_i) = v_i \quad \text{a} \quad \theta_q(w_i') = v_i'$$

a w^* vztahem

$$w^* = w_1 + w_2 + \cdots + w_h - w_1' - w_2' - \cdots - w_h'.$$

Pak $w^* \in D$ a pro $i = 1, 2, \ldots, h$ platí

$$qw_i \equiv v_i \pmod{p} \quad \text{a} \quad qw_i' \equiv v_i' \pmod{p},$$

z čehož plyne

$$qw^* \equiv v^* \pmod{p}.$$

To ale znamená, že

$$v^* = \gamma(qw^* + p\mathbb{Z}) + xp \tag{3.22}$$

pro vhodné $x \in \mathbb{Z}$.

Kdyby $w^* \equiv 0 \pmod{p}$, pak z (3.22) plyne $v^* \equiv 0 \pmod{p}$, což společně s faktem $(m, p) = 1$ a (3.20) dává, že $v^* \equiv 0 \pmod{mp}$ a $v^* \neq 0$. Tedy musí být $|v^*| \geq mp$ a dostáváme spor s (3.21). Proto budeme uvažovat jen $w^* \not\equiv 0 \pmod{p}$.

Dáme-li dohromady (3.22) a (3.20), dostaneme

$$v^* = \gamma(qw^* + p\mathbb{Z}) + xp \equiv 0 \pmod{m}, \tag{3.23}$$

což nám společně s (3.21) dává odhad na x v podobě

$$-h \leq x \leq h - 1.$$

Dokázali jsme tedy, že pokud zobrazení $\delta : V_q \to \mathbb{Z}/m\mathbb{Z}$ není Freimanův izomorfismus řádu h, pak podle vztahu (3.23) existují $w^* \in D$, $w^* \not\equiv 0 \pmod{p}$ a $x \in [-h, h-1]$ splňující

$$\gamma(qw^* + p\mathbb{Z}) + xp \equiv 0 \pmod{m}. \tag{3.24}$$

Spočtěme, kolik nejvýše takovýchto trojic (w^*, x, q) může existovat. Zvolme $w^* \in D$, $w^* \not\equiv 0 \pmod{p}$, to můžeme právě $|D| - 1$ způsoby, protože $w^* \neq 0$ a dle (3.14) každý prvek $t \in D$ splňuje $|t| < p$. Jelikož p je prvočíslo, operace násobení prvkem w^* zobrazuje interval $[1, p-1]$ na interval $[1, p-1]$ jednoznačně modulo p (formálněji $\gamma(w^* * ([1, p-1] + p\mathbb{Z})) = [1, p-1]$). Proto stačí pro každé $w^* \in D$, $w^* \not\equiv 0 \pmod{p}$ spočítat počet řešení diofantické rovnice

$$y + xp \equiv 0 \pmod{m}$$

pro $y \in [1, p-1]$ a $x \in [-h, h-1]$. Zde však pro každé $x \in [-h, h-1]$, celkem $2h$ možností, máme nejvýše

$$\frac{p-1}{m} + 1 < \frac{2(p-1)}{m}$$

možností pro $y \in [1, p-1]$. Proto celkový počet trojic (w^*, x, q) splňujících (3.24) bude nejvýše

$$\underbrace{(|D| - 1)}_{\text{počet } w^*} \underbrace{(2h)}_{\text{počet } x} \underbrace{\frac{2(p-1)}{m}}_{\text{počet } q} < \frac{4h|D|(p-1)}{m} \leq p - 1. \tag{3.25}$$

Jelikož pro každé $q \in [1, p-1]$, pro které $\delta : V_q \to \mathbb{Z}/m\mathbb{Z}$ není Freimanův izomorfismus musí existovat trojice (w^*, x, q) splňující (3.24) a těchto trojic je dle (3.25) méně než $p-1$, pak bude existovat q_0, které se nevyskytuje ani v jedné ze zmiňovaných trojic. A pro toto q_0 je $\delta : V_{q_0} \to \mathbb{Z}/m\mathbb{Z}$ Freimanův izomorfismus řádu h, tudíž i zobrazení

$$\delta : V'_{q_0} \to \mathbb{Z}/m\mathbb{Z}$$

je Freimanův izomorfismus řádu h.

Víme ale už, že zobrazení

$$\theta_{q_0} : W'_{q_0} \to V'_{q_0}$$

je Freimanův izomorfismus řádu h. Tudíž stačí volit množinu $W' = W'_{q_0}$ a zobrazení $\psi = \delta \circ \gamma \circ \beta_{q_0} \circ \alpha$. Pak dle (3.17) platí $|W'| \geq |W|/h$, a zobrazení

$$\psi : W' \to \mathbb{Z}/m\mathbb{Z}$$

je Freimanův izomorfismus řádu h, což jsme chtěli dokázat. □

Věta 3.3.2 *Buďte c_1, c_2 a c_3 kladné reálné konstanty. Dále buď $k \geq 1$ a množiny A, B podmnožinami $\mathbb{N}$ s vlastnostmi*

$$c_1 k \leq |A| \leq c_2 k, \qquad c_1 k \leq |B| \leq c_2 k,$$

$$|A + B| \leq c_3 k.$$

Pak A je podmnožinou n-dimenzionální aritmetické posloupnosti délky maximálně lk, kde n a l závisejí pouze na konstantách c_1, c_2 a c_3.

Důkaz. Definujeme-li $c = c_3/c_1$ a $c' = c_2/c_1$, ze zadání máme

$$|B| \leq c_2 k \leq \frac{c_2}{c_1}|A| = c'|A|, \tag{3.26}$$

a

$$|A + B| \leq c_3 k \leq \frac{c_3}{c_1}|B| = c|B|,$$

tudíž podle Lemmatu 1.3.1 platí

$$|8A - 8A| \leq c^{16}|B| \overset{(3.26)}{\leq} c^{16}c'|A|. \tag{3.27}$$

Bertrandův postulát tvrdí, že mezi každými dvěma čísly m a $2m$ pro $m \geq 2$ existuje prvočíslo p. Najděme tedy pro $m = |8A - 8A|$ prvočíslo p splňující

$$|A| \leq |8A - 8A| < p < 2|8A - 8A| \overset{(3.27)}{\leq} 2c^{16}c'|A|. \tag{3.28}$$

Nyní využijeme předchozí Větu 3.3.1 pro $h = 8$ na množinu A. Existuje tedy množina $A' \subseteq A$, která je Freimanovsky izomorfní řádu 8 nějaké podmnožině R zbytkových tříd modulo p a splňuje vztah $|A'| \geq |A|/8$. Definujme $\alpha \in [0, 1]$ vztahem $|R| = \alpha p$. Platí

$$\alpha p = |R| = |A'| \geq \frac{|A|}{8} \overset{(3.28)}{>} \frac{p}{8 \cdot 2c^{16}c'},$$

neboli

$$\alpha > \frac{1}{2^4 c^{16} c'}. \tag{3.29}$$

Pak dle Věty 3.2.6 množina $2R - 2R$ obsahuje vlastní n_1-dimenzionální aritmetickou posloupnost Q_1 délky

$$l(Q_1) = |Q_1| > \delta p > \delta |A|, \quad \text{kde } \delta = \frac{1}{(4n_1)^{n_1}} \tag{3.30}$$

s dimenzí

$$n_1 < \alpha^{-2} \overset{(3.29)}{<} (2^4 c^{16} c')^2 = \frac{2^8 c_3^{32} c_2^2}{c_1^{34}}. \tag{3.31}$$

Jelikož A' a R jsou Freimanovsky izomorfní řádu $8 = 2(2 + 2)$, pak podle Tvrzení 2.2.4 množiny $2A' - 2A'$ a $2R - 2R$ jsou Freimanovsky izomorfní řádu 2. Označme Q_2 obraz Q_1 v tomto izomorfismu. Podle Tvrzení 2.2.3 je Q_2 také vlastní n_1-dimenzionální aritmetická posloupnost splňující

$$Q_2 \subseteq 2A' - 2A' \subseteq 2A - 2A \subseteq \mathbb{N}$$

a

$$\delta|A| < |Q_1| = |Q_2| \leq |2A - 2A| \overset{1.3.1}{\leq} c^4|B| \overset{(3.26)}{\leq} c^4 c'|A|. \tag{3.32}$$

Nechť $A^* = \{a_1, a_2, \ldots, a_{n_2}\}$ je maximální podmnožina A taková, že množiny $a_i + Q_2$ jsou po dvou disjunktní. Neboť

$$\bigcup_{i=1}^{n_2} (a_i + Q_2) = A^* + Q_2 \subseteq A + Q_2 \subseteq 3A - 2A,$$

máme z Lemmatu 1.3.1 vztah

$$n_2|Q_1| = \sum_{i=1}^{n_2} |a_i + Q_2| = \left|\bigcup_{i=1}^{n_2}(a_i + Q_2)\right| = |A^* + Q_2|$$
$$\leq |3A - 2A| \overset{1.3.1}{\leq} c^5|B| \overset{(3.26)}{\leq} c^5c'|A|.$$

A proto

$$n_2 \leq \frac{c^5c'|A|}{|Q_2|} < \frac{c^5c'|A|}{\delta|A|} = \frac{c^5c'}{\delta} \overset{(3.30)}{=} c^5c'(4n_1)^{n_1}. \tag{3.33}$$

Dle Tvrzení 2.1.4 je A^* podmnožinou aritmetické posloupnosti

$$Q_3 = \{x_1a_1 + x_2a_2 + \cdots + x_{n_2}a_{n_2} : 0 \leq x_i < 2, \text{ pro } i = 1, 2, \ldots, n_2\},$$

která má dimenzi n_2 a délku $l(Q_3) = 2^{n_2}$. Vezmeme-li libovolné $a \in A$, pak dle maximality A^* existuje $a_i \in A^*$ takové, že

$$(a + Q_2) \cap (a_i + Q_2) \neq \emptyset$$

a proto existují přirozená čísla $q, q' \in Q_2$ taková, že $a + q = a_i + q'$. Máme

$$a = a_i + q' - q \subseteq A^* + Q_2 - Q_2 \subseteq Q_3 + Q_2 - Q_2.$$

Označme $Q = Q_3 + Q_2 - Q_2$. Pak $A \subseteq Q$. Podle Tvrzení 2.1.2 je $Q_2 - Q_2$ n_1-dimenzionální aritmetická posloupnost s délkou

$$l(Q_2 - Q_2) < 2^{n_1}l(Q_2) \overset{(3.32)}{\leq} 2^{n_1}c^4c'|A| \leq 2^{n_1}\frac{c_3^4c_2}{c_1^5}|A| \leq 2^{n_1}\frac{c_3^4c_2^2}{c_1^5}k.$$

A proto $Q = Q_3 + Q_2 - Q_2$ je dle Tvrzení 2.1.1 n-dimenzionální aritmetická posloupnost dimenze

$$n = n_1 + n_2$$

a délky

$$l(Q) \overset{2.1.1}{\leq} l(Q_3)l(Q_2 - Q_2) < 2^{n_2}2^{n_1}\frac{c_3^4c_2^2}{c_1^5}k = 2^{n_1+n_2}\frac{c_3^4c_2^2}{c_1^5}k = lk. \tag{3.34}$$

To ale znamená, že jsme našli n-dimenzionální posloupnost s délkou lk a dimenzí n, kde hodnoty l a n závisejí dle (3.31), (3.33) a (3.34) pouze na konstantách c_1, c_2 a c_3, obsahující A, což jsme chtěli dokázat. □

Poznámka 3.3.3. Důkaz Freimanovy věty však s sebou přinesl také řadu otázek. Není třeba dosud známo, jak velká je závislost délky a dimenze nalezené multidimenzionální aritmetické posloupnosti Q na konstantách c_1, c_2 a c_3. Předchozí důkaz tvrzení 3.3.2 nám dal pouze exponenciální odhad. Zdali to jde polynomiálně, se zatím neumí dokázat ani vyvrátit.

Buď $h \geq 3$. Lze potom popsat množiny A splňující $|hA| \leq c|A|$, nebo dokonce $|hA| \leq c|A|^{h-1}$? Tyto domněnky zůstávají stále otevřené a můžeme kolem nich vyslovit řadu otevřených problému. Například, existuje $\delta > 1$ takové, že množina A splňující $|3A| \leq c|A|^{1+\delta}$ lze nějakým způsobem charakterizovat?

Ukažme si ale také zobecnění Freimanovy věty, které platí. Řekneme, že grupa G je *beztorzní grupa*, jestliže každý její prvek s vyjímkou identity má nekonečný řád. Vezmeme-li nyní místo množiny $A \subset \mathbb{N}$ množinu $A \subset G$, kde G je beztorzní grupa, pak obdoba Věty 3.3.2 platí. Zformulujme a dokažme si proto následující důsledek.

Důsledek 3.3.4 *Buďte c_1, c_2 a c_3 kladné reálné konstanty, $k \geq 1$ přirozené číslo. Buď G beztorzní grupa a buďte množiny A a B podmnožinami G s vlastnostmi*

$$c_1 k \leq |A| \leq c_2 k, \qquad c_1 k \leq |B| \leq c_2 k,$$
$$|A + B| \leq c_3 k.$$

Pak A je podmnožinou n-dimenzionální aritmetické posloupnosti délky maximálně lk, kde n a l závisejí pouze na konstantách c_1, c_2 a c_3.

Důkaz. Zvolme libovolné $h \geq 2$. Snažme se dokázat, že množina A je Freimanovsky izomorfní řádu h nějaké množině přirozených čísel. Pak budeme moci převést Důsledek 3.3.4 na Větu 3.3.2, a tedy důkaz bude hotov.

Známá věta z algebry tvrdí, že každá beztorzní konečně generovaná grupa je izomorfní $\mathbb{Z}^n$ pro nějaké n. Označíme-li H grupu generovanou A, pak dle tohoto tvrzení je konečně generovaná beztorzní grupa H izomorfní $\mathbb{Z}^n$, tedy množina A je Freimanovsky izomorfní řádu h nějaké konečné množině C mřížových bodů v $\mathbb{Z}^n$. Pokud ukážeme, že každá konečná množina $C \subset \mathbb{Z}^n$ je Freimanovsky izomorfní řádu h nějaké množině přirozených čísel, jsme hotovi. Pojďme na to.

Najděme přirozené číslo m takové, že $C \subseteq [0, m-1]^n \cap \mathbb{Z}^n$. Existence m plyne z konečnosti C. Definujme si pro $j = 1, \ldots, n$ čísla

$$d_j = \sum_{k=1}^{j-1} hmd_k$$

a označme $Q = Q(0, d_1, \ldots, d_n, m, \ldots, m)$ n-dimenzionální aritmetickou posloupnost. Dokažme, že Q a $[0, m-1]^n \cap \mathbb{Z}^n$ jsou Freimanovsky izomorfní řádu h. Definujme $\psi : [0, m-1]^n \cap \mathbb{Z}^n \to Q$ vztahem

$$\psi(x_1, \ldots, x_n) = x_1 d_1 + \cdots + x_n d_n.$$

Jsou-li pro $i = 1, \ldots, h$ prvky $x_i = (x_{i1}, \ldots, x_{in})$ a $y_i = (y_{i1}, \ldots, y_{in}) \in [0, m-1]^n \cap \mathbb{Z}^n$ takové, že platí

$$\psi(x_1) + \cdots + \psi(x_h) = \psi(y_1) + \cdots + \psi(y_h),$$

pak musí platit

$$\sum_{j=1}^{n} \sum_{i=1}^{h} x_{ij} d_j = \sum_{j=1}^{n} \sum_{i=1}^{h} y_{ij} d_j.$$

Pokud označíme $z_j = \sum_{i=1}^{h} x_{ij} - \sum_{i=1}^{h} y_{ij} = \sum_{i=1}^{h} (x_{ij} - y_{ij})$, máme

$$|z_j| \leq h(m-1) \quad \text{a} \quad \sum_{i=1}^{h} z_j d_j = 0.$$

Jsou-li všechna $z_j = 0$, pak $x_1 + \cdots + x_n = y_1 + \cdots + y_n$ a jsme hotovi. V opačném případě najděme nejmenší index k takový, že $z_k \neq 0$. Pak máme

$$d_k \leq |z_k d_k| = \left| \sum_{j=1}^{k-1} z_j d_j \right| \leq \sum_{j=1}^{k-1} h(m-1) d_j < d_k,$$

což neplatí, proto $z_j = 0$ pro libovolné $j = 1, \ldots, n$. Tedy ψ je Freimanův izomorfismus řádu h, čímž je důsledek dokázán. □

3.4 Aplikace Freimanovy věty

Od roku 1964, kdy byla Freimanova věta dokázána se našlo spousta jejich aplikací. Nejvíce se jich týká kombinatorické teorie čísel, zejména pak výskytu (jednodimenzionálních) aritmetických posloupností v množinách s určitou vlastností. Uvedeme si dva příklady.

První tvrzení říká, že pro libovolné dostatečně velké konstanty c a t existuje konstanta $k = k(c, t)$ taková, že každá množina přirozených čísel A s vlastnostmi $|A| \geq k$ a $|2A| \leq c|A|$ už obsahuje aritmetickou posloupnost délky t. Druhé tvrzení požaduje pro výskyt aritmetické posloupnosti délky t existenci dostatečně mnoha aritmetických posloupností délky 3. Zformulujme si obě věty.

Věta 3.4.1 *Buďte $c \geq 2$ a $t \geq 3$. Pak existuje konstanta $k = k(c,t)$ taková, že jestliže množina A přirozených čísel splňuje $|A| \geq k$ a $|2A| \leq c|A|$ pak A musí obsahovat aritmetickou posloupnost délky t.*

Poznámka 3.4.2. Důkaz této věty vyžaduje znalost tvrzení, jež roku 1974 dokázal Szemerédi. Toto tvrzení říká, že pro libovolné $\varepsilon > 0$ a $t \geq 3$ existuje konstanta l taková, že je-li B podmnožinou $\{0, 1, \ldots, l-1\}$ a $|B| \geq \varepsilon l$, pak B obsahuje aritmetickou posloupnost délky t. Jelikož množiny $\{0, 1, \ldots, l-1\}$ a $\{a + x_i d_i : 0 \leq l-1\}$ jsou Freimanovsky izomorfní řádu $h \geq 2$, dá se ekvivalentně tvrzení vyslovit pro B podmnožinu (jednodimenzionální) aritmetické posloupnosti délky l.

Při použití tohoto Szemerédiho výsledku již důkaz předchozí věty není složitý. Myšlenka spočívá v tom, že nejprve podle Freimanovy Věty 3.1.1 existuje n-dimenzionální aritmetická posloupnost Q délky $l(Q) \leq l|A|$. Z Q si vybereme vhodnou jednodimenziální aritmetickou posloupnost, jejíž diference je shodná s jednou s diferencí Q, řekněme d_p. Takovýchto posloupností je celkem alespoň $l(Q)/l_p$. Následuje řada mírně složitějších úvah dokazující, že jedna z těchto aritmetických posloupností v průniku s A obsahuje aritmetickou posloupnost délky t.

Věta 3.4.3 *Buďte $\varepsilon \geq 0$ a $t \geq 3$. Pak existuje přirozené číslo $k = k(\varepsilon, t)$ takové, že každá množina přirozených čísel A taková, že $|A| \geq k$ a A obsahuje alespoň εk^2 různých aritmetických posloupností délky 3, musí obsahovat aritmetickou posloupnost délky t.*

Poznámka 3.4.4. Toto tvrzení je již složitější. Kromě Freimanovy věty se zde využije také Szemerédiho lemma o regularitě a Balog-Szemerédiho věta. Celý důkaz je proveden v knize [1] na stranách 257 až 278, přičemž Věta 3.4.3 je dokázána na straně 277.

Domněnka 3.4.5. Na závěr ještě zformulujme jeden otevřený problém. Freimanova Věta 3.1.1 nám tvrdí, že každá množina s malým dvojnásobkem $2A$ je obsažena v nějaké multidimenzionální aritmetické posloupnosti Q. Umíme však najít Q vlastní? Ve Freimanově větě se tato vlastnost býti vlastní ztratila při volbě $Q = Q_3 + Q_2 - Q_2$. Zatím se většina matematiků domnívá, že taková vlastní multidimenzionální aritmetické posloupnost Q by měla existovat, nikdo z nich však neumí říci proč. Umíte to vy?

Literatura

[1] Nathanson Melvyn B.: *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[2] Rusza I. Z.: *Arithmetic progressions and the number of sums*, Periodica Math. Hungar. 25, 105-111, 1992.

[3] Tao Terence, Vu Van H.: *Additive Combinatorics*, Cambridge University Press, 2006.