

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 49 (2003)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ADDITIVE NUMBER THEORY SHEDS EXTRA LIGHT ON THE HOPF-STIEFEL \circ FUNCTION
Autor: Plagne, Alain
Kapitel: 2. Proof of Theorem 4
DOI: <https://doi.org/10.5169/seals-66682>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 02.04.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

With these results, we know the behaviour of μ_G at the two endpoints of the spectrum (cyclic groups and groups of prime exponent). What now remains to be done is to fill the gap between the upper bound and the lower bound for general finite Abelian groups.

2. PROOF OF THEOREM 4

Let G be any given finite Abelian group and let $1 \leq r, s \leq |G|$.

2.1 THE LOWER BOUND

If $\mu_G(r, s) \geq r + s - 1$, the result is immediate (take $d = 1$). We may thus assume that

$$(2.1) \quad \mu_G(r, s) \leq r + s - 1.$$

Then, choosing two sets \mathcal{A} and \mathcal{B} in G with respective cardinalities r and s , such that $|\mathcal{A} + \mathcal{B}|$ attains $\mu_G(r, s)$, we get

$$|\mathcal{A} + \mathcal{B}| = \mu_G(r, s) \leq |\mathcal{A}| + |\mathcal{B}| - 1.$$

We are in a position to apply Kneser's theorem [9] on the structure of sets with a small sumset. It follows that there exists a subgroup H of G (namely the stabilizer of $\mathcal{A} + \mathcal{B}$) such that

$$|\mathcal{A} + \mathcal{B}| = |\mathcal{A} + H| + |\mathcal{B} + H| - |H|.$$

Denoting by $(\mathcal{A} + H)/H$ (resp. $(\mathcal{B} + H)/H$) the H -cosets that \mathcal{A} (resp. \mathcal{B}) intersects, we obtain

$$\begin{aligned} |\mathcal{A} + \mathcal{B}| &= \left(\left| \frac{\mathcal{A} + H}{H} \right| + \left| \frac{\mathcal{B} + H}{H} \right| - 1 \right) |H| \\ &\geq (\lceil r/f \rceil + \lceil s/f \rceil - 1)f \end{aligned}$$

where f denotes the cardinality of H . Since Lagrange's theorem shows that f divides $|G|$, we get

$$|\mathcal{A} + \mathcal{B}| \geq \min_{d| |G|} (\lceil r/d \rceil + \lceil s/d \rceil - 1)d.$$

From this it follows that, in any case,

$$\mu_G(r, s) \geq \min_{d| |G|} (\lceil r/d \rceil + \lceil s/d \rceil - 1)d,$$

which is the desired lower bound.

2.2 THE UPPER BOUND

Let H be any subgroup of G . Choose \mathcal{A}_0 and \mathcal{B}_0 in G/H with respective cardinalities $\lceil r/|H| \rceil$ and $\lceil s/|H| \rceil$ and such that

$$|\mathcal{A}_0 + \mathcal{B}_0| = \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil).$$

Now choose \mathcal{A} of cardinality r and \mathcal{B} of cardinality s in G such that the image of \mathcal{A} (resp. \mathcal{B}) by the canonical projection on G/H is included in \mathcal{A}_0 (resp. \mathcal{B}_0). One has

$$|\mathcal{A} + \mathcal{B}| \leq \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H|.$$

This proves the first lemma we need.

LEMMA 1. *For any finite Abelian group G*

$$\mu_G(r, s) \leq \min_{H \leq G} \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H|.$$

The second useful point is synthesized in the next folkloric lemma.

LEMMA 2. *Let G be a finite Abelian group. For any positive integer m , the following two propositions are equivalent*

- (i) m divides $\exp G$,
- (ii) there exists a subgroup H of G such that G/H is isomorphic to $\mathbf{Z}/m\mathbf{Z}$.

In the case of a cyclic group K , trivial considerations (take two sets with consecutive elements), show that, for any $u, v \leq |K|$,

$$(2.2) \quad \mu_K(r, s) \leq r + s - 1.$$

Using consecutively Lemma 1, inequality (2.2) and Lemma 2 yields the following chain of inequalities:

$$\begin{aligned} \mu_G(r, s) &\leq \min_{H \leq G} \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H| \\ &\leq \min_{H \leq G, G/H \text{ cyclic}} \mu_{G/H}(\lceil r/|H| \rceil, \lceil s/|H| \rceil)|H| \\ &\leq \min_{H \leq G, G/H \text{ cyclic}} (\lceil r/|H| \rceil + \lceil s/|H| \rceil - 1) |H| \\ &= \min_{|G/H| \text{ divides } \exp G} (\lceil r/|H| \rceil + \lceil s/|H| \rceil - 1) |H| \\ &= \min_{f | \exp G} (\lceil rf/|G| \rceil + \lceil sf/|G| \rceil - 1) \frac{|G|}{f}. \end{aligned}$$

The change of variable $d = |G|/f$ yields a parameter d subject to the two restrictions $\frac{|G|}{\exp G} \mid d$ and $d \mid |G|$; this proves the upper bound in Theorem 4.