Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 2

On a theorem of Hildebrand

Carsten Dietzel

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 2, 2019
dx.doi.org/10.2140/moscow.2019.8.189

On a theorem of Hildebrand

Carsten Dietzel

We give a short proof that for each multiplicative subgroup H of finite index in $\mathbb{Q}^+$, the set of integers a with $a, a+1 \in H$ is an IP-set. This generalizes a theorem of Hildebrand concerning completely multiplicative functions taking values in the k-th roots of unity.

A theorem of Hildebrand [1991, Theorem 2], which was essential in answering a question of Lehmer, Lehmer and Mills [Lehmer et al. 1963] on consecutive power residues can be formulated as follows:

Theorem 1 (Hildebrand). *Fix some $k \in \mathbb{Z}^+$. If $f : \mathbb{Z}^+ \to \mathbb{C}$ is a completely multiplicative function (i.e., $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{Z}^+$) taking its values in the k-th roots of unity then the set of $a \in \mathbb{Z}^+$ fulfilling $f(a) = f(a+1) = 1$ is nonempty.*

Remark 2. Hildebrand actually proved more; i.e., there is a constant $c(k)$, independent of the specific multiplicative function f, and an $a \in \mathbb{Z}^+$ such that $a \le c(k)$ and $f(a) = f(a+1) = 1$. By a standard compactness argument, these versions can be seen to be equivalent. It should, however, be noted that from Hildebrand's proof one can get an effective value for $c(k)$ (as was pointed out by the anonymous referee).

It makes sense to restate Hildebrand's result as follows:

Theorem 3 (Hildebrand). *Let $H \le \mathbb{Q}^+$ be a (multiplicative) subgroup such that $\mathbb{Q}^+/H$ is cyclic of finite order. Let $H^* := H \cap \mathbb{Z}^+$. Then $H^* \cap (H^* - 1)$ is nonempty.*

The original proof made use of analytic methods and was rather long. We will give a short elementary proof of a more general theorem.

However, before we can state (and prove) our generalization we need some notation and the set-theoretical version of Hindman's theorem:

We denote by $\mathcal{P}^{\mathrm{fin}}(\mathbb{Z}^+)$ the set of finite, nonempty subsets of $\mathbb{Z}^+$.

For $A, B \in \mathcal{P}^{\mathrm{fin}}(\mathbb{Z}^+)$ write $A \prec B$ if $\max A < \min B$.

Furthermore, for a sequence $A_1 \prec A_2 \prec \cdots$ in $\mathcal{P}^{\mathrm{fin}}(\mathbb{Z}^+)$, we define

$$\mathrm{FU}((A_i)_{i \in \mathbb{Z}^+}) = \left\{ \bigcup_{i \in I} A_i : I \subseteq \mathbb{Z}^+,\ 0 < |I| < \infty \right\}.$$

Similarly, for a sequence $a_1, a_2, \ldots$ in $\mathbb{Z}^+$, we define

$$\mathrm{FS}((a_i)_{i \in \mathbb{Z}^+}) = \left\{ \sum_{i \in I} a_i : I \subseteq \mathbb{Z}^+,\ 0 < |I| < \infty \right\}.$$

MSC2010: 11B75.
Keywords: IP-set, multiplicative subgroup.

We call a set $M \subseteq \mathbb{Z}^+$ an *IP-set* [Hindman and Strauss 2012, Definition 16.3] if there is a sequence $a_1, a_2, \ldots$ in $\mathbb{Z}^+$ such that $\mathrm{FS}((a_i)_{i\in\mathbb{Z}^+}) \subseteq M$.

If a set A is the disjoint union of subsets $B_1, \ldots, B_n \subseteq A$, that is, $B_1 \cup \cdots \cup B_n = A$ and $B_i \cap B_j = \varnothing$ for $1 \le i < j \le n$, we denote this relation by $A = B_1 \sqcup \cdots \sqcup B_n$.

Now Hindman's theorem on partitions of $\mathcal{P}^{\mathrm{fin}}(\mathbb{Z}^+)$ [Hindman and Strauss 2012, Corollary 5.17] can be stated as follows:

Theorem 4 (Hindman). *For any finite partition $\mathcal{P}^{\mathrm{fin}}(\mathbb{Z}^+) = M_1 \sqcup M_2 \sqcup \cdots \sqcup M_n$ there are sets $A_1 \prec A_2 \prec \cdots$ and $1 \le j \le k$ such that*

$$\mathrm{FU}((A_i)_{i\in\mathbb{Z}^+}) \subseteq M_j.$$

We can now state our generalization of Hildebrand's theorem:

Theorem 5. *Let $H \le \mathbb{Q}^+$ be a (multiplicative) subgroup of finite index.*[1]*Let $H^* := H \cap \mathbb{Z}^+$. Then $H^* \cap (H^* - 1)$ is an IP-set.*

Hildebrand's proof of Theorem 3 is an application of Ramsey's theorem on *special* sets, i.e., finite sets $\{n_1 < n_2 < \cdots < n_r\}$ such that $n_j - n_i = \gcd(n_i, n_j)$ holds for $1 \le i < j \le r$.

We will use a similar concept:

Definition 6. For a sequence s_n and a finite subset $A \subset \mathbb{Z}^+$, set

$$s_A := \sum_{n\in A} s_n.$$

A *block-divisible sequence* is a strictly decreasing sequence s_n in $\mathbb{Z}^+$ such that for $A, B \in \mathcal{P}^{\mathrm{fin}}(\mathbb{Z}^+)$, s_A divides s_B whenever $A \prec B$.

For our proof, *any* block-divisible sequence will work. Thus, we only need to confirm the existence of block-divisible sequences:

Lemma 7. *There is a block-divisible sequence in $\mathbb{Z}^+$.*

Proof. We construct a sequence as follows:

$$s_0 := 1, \quad s_{n+1} := \prod_{\substack{A\subseteq\{0,\ldots,n\}\\ A\neq\varnothing}} s_A.$$

Ignoring the s_0 at the beginning, we end up with a strictly increasing sequence fulfilling the desired divisibility condition. □

Now we can show our main result:

Proof of Theorem 5. Let N_i' $(1 \le i \le k)$ be the (multiplicative) cosets of H in $\mathbb{Q}^+$.

These give a finite partition $\mathbb{Z}^+ = N_1 \sqcup N_2 \sqcup \cdots \sqcup N_k$, where $N_i = N_i' \cap \mathbb{Z}^+$.

We now fix a block-divisible sequence s_n (whose existence is guaranteed by Lemma 7) and define a partition $\mathcal{P}^{\mathrm{fin}}(\mathbb{Z}^+) = M_1 \sqcup M_2 \sqcup \cdots \sqcup M_k$ by declaring $A \in M_i$ if and only if $s_A \in N_i$.

By Theorem 4 there is a sequence $A_1 \prec A_2 \prec \cdots$ such that $\mathrm{FU}(A_1, A_2, \ldots)$ is contained in one M_i for some $1 \le i \le k$.

[1]Note that we do not require $\mathbb{Q}^+/H$ to be cyclic.

By the definition of block-divisibility, s_{A_1} divides s_A for all $A \in \mathrm{FU}(A_2, A_3, \dots)$ and, consequently, for all $A \in \mathrm{FU}(A_1, A_2, \dots)$, too.

Thus, defining $b_i := s_{A_i}$, the members of $\mathrm{FS}(b_1, b_2, \dots)$ all lie in the same coset of H and are divisible by b_1. Therefore, setting $a_i := b_i/b_1$, one has

$$\mathrm{FS}(a_1, a_2, \dots) = \mathrm{FS}(1, a_2, a_3, \dots) \subseteq H^*.$$

Furthermore, $\mathrm{FS}(1, a_2, a_3, \dots) = \mathrm{FS}(a_2, a_3, \dots) \cup (\mathrm{FS}(a_2, a_3, \dots) + 1) \subseteq H^*$.

We conclude that $\mathrm{FS}(a_2, a_3, \dots) \subseteq H^* \cap (H^* - 1)$. □

Remark 8. We use the terminology of Theorem 5 to summarize the state of possible generalizations:

There are (multiplicative) subgroups H of arbitrary even index in $\mathbb{Q}^+$ such that $H^* \cap (H^* - 1) \cap (H^* - 2)$ is empty, as has been shown by Lehmer and Lehmer [1962, p. 103].

Graham [1964] proved that there are subgroups of arbitrary (finite) index in $\mathbb{Q}^+$ such that $H^* \cap \dots \cap (H^* - 3)$ is empty.

However, if $\mathbb{Q}^+/H$ is of odd order k, it is still an open question if $H^* \cap (H^* - 1) \cap (H^* - 2)$ is necessarily nonempty. Only in the case $k = 3$ is this set known to be always nonempty, as has been shown computationally by Lehmer, Lehmer, Mills and Selfridge [Lehmer et al. 1962]. Maybe the combinatorial methods presented in this article may help in resolving this problem!

Remark 9. Some ideas shown in this article are based on notes of the author, [Dietzel 2013], which have not been submitted to any journal.

References

[Dietzel 2013] C. Dietzel, "A generalization of Schur's theorem and its application to consecutive power residues", preprint, 2013. arXiv

[Graham 1964] R. L. Graham, "On quadruples of consecutive kth power residues", *Proc. Amer. Math. Soc.* **15** (1964), 196–197. MR Zbl

[Hildebrand 1991] A. Hildebrand, "On consecutive kth power residues, II", *Michigan Math. J.* **38**:2 (1991), 241–253. MR Zbl

[Hindman and Strauss 2012] N. Hindman and D. Strauss, *Algebra in the Stone–Čech compactification: theory and applications*, 2nd ed., Walter de Gruyter & Co., Berlin, 2012. MR Zbl

[Lehmer and Lehmer 1962] D. H. Lehmer and E. Lehmer, "On runs of residues", *Proc. Amer. Math. Soc.* **13** (1962), 102–106. MR Zbl

[Lehmer et al. 1962] D. H. Lehmer, E. Lehmer, W. H. Mills, and J. L. Selfridge, "Machine proof of a theorem on cubic residues", *Math. Comp.* **16** (1962), 407–415. MR Zbl

[Lehmer et al. 1963] D. H. Lehmer, E. Lehmer, and W. H. Mills, "Pairs of consecutive power residues", *Canad. J. Math.* **15** (1963), 172–177. MR Zbl

Received 29 Jan 2019. Revised 7 Feb 2019.

CARSTEN DIETZEL:
carstendietzel@gmx.de
Institute of algebra and number theory, University of Stuttgart, Stuttgart, Germany

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 2 2019