JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Sergei V. KONYAGIN et Vsevolod F. LEV

Character sums in complex half-planes

Tome 16, n° 3 (2004), p. 587-606.

<http://jtnb.cedram.org/item?id=JTNB_2004__16_3_587_0>

Journal de Théorie des Nombres
de Bordeaux **16** (2004), 587–606

Character sums in complex half-planes

par Sergei V. KONYAGIN et Vsevolod F. LEV

Résumé. Soit A un sous-ensemble fini d'un groupe abélien G et P un demi-plan fermé du plan complexe contenant zéro. Nous montrons qu'il existe un coefficient de Fourier non-trivial de la fonction indicatrice de A qui appartient à P (si A ne possède pas une structure spéciale explicite). Autrement dit, il existe un caractère non-trivial $\chi \in \widehat{G}$ tel que $\sum_{a\in A} \chi(a) \in P$.

Abstract. Let A be a finite subset of an abelian group G and let P be a closed half-plane of the complex plane, containing zero. We show that (unless A possesses a special, explicitly indicated structure) there exists a non-trivial Fourier coefficient of the indicator function of A which belongs to P. In other words, there exists a non-trivial character $\chi \in \widehat{G}$ such that $\sum_{a\in A} \chi(a) \in P$.

1. Summary of results

Let G be an abelian group and let $\widehat{G}$ denote the dual group. For a finite subset $A \subseteq G$ and a character $\chi \in \widehat{G}$ we write

$$S_A(\chi) := \sum_{a\in A} \chi(a);$$

that is, $S_A(\chi)$ are Fourier coefficients of the indicator function of A.

Fix A and let χ run over all characters of G. How are the numbers $S_A(\chi)$ distributed on the complex plane? What can be said about A if $S_A(\chi)$ exhibit an "irregular" behavior? For instance, when are all $S_A(\chi)$ situated in the same half-plane? The following theorem is our main result.

Theorem 1.1. *Let P be a closed complex half-plane with zero on its boundary, and let A be a finite subset of an abelian group G. Then either there exists a non-trivial character $\chi \in \widehat{G}$ such that $S_A(\chi) \in P$, or at least one of the following holds:*

i) *$A = \{0, g\}$, where $g \in G$ is a non-zero element of odd order;*
ii) *G is finite and $A = G \setminus \{0, g\}$, where $g \in G$ is a non-zero element of odd order;*
iii) *$A \cap (-A) = \{0\}$, and $A \cup (-A)$ is a finite subgroup of G;*

Manuscrit reçu le 9 mai 2003.

iv) *G is finite, $A \cup (-A) = G \setminus \{0\}$, and $A \cap (-A)$ is the complement of a subgroup of G.*

For cyclic groups of prime order and torsion-free abelian groups we were able to drop the assumption that P is closed. This yields additional exceptional cases; however, specific features of the groups allow us to put conditions i)–iv) of Theorem 1.1 in a more explicit form.

Theorem 1.2. *Let P be an open complex half-plane with zero on its boundary and such that $P \cap \mathbb{R} \neq \varnothing$. Suppose that G is a cyclic group of odd prime order, and let A be a non-empty proper subset of G. Then either there exists a non-trivial character $\chi \in \widehat{G}$ such that $S_A(\chi) \in P$, or at least one of the following holds:*

i) $0 \in A$ *and* $|A| \leq 2$;
ii) $0 \notin A$ *and* $|A| \geq |G| - 2$;
iii) $A \cap (-A) = \{0\}$, *and* $A \cup (-A) = G$;
iv) $A \cup (-A) = G \setminus \{0\}$, *and* $A \cap (-A) = \varnothing$.

Theorem 1.3. *Let P be an open complex half-plane with zero on its boundary and such that $P \cap \mathbb{R} \neq \varnothing$. Suppose that G is a torsion-free abelian group, and let A be a finite non-empty subset of G. Then either there exists a non-trivial character $\chi \in \widehat{G}$ such that $S_A(\chi) \in P$, or $0 \in A$ and $|A| \leq 2$.*

Remark. Conditions given in Theorems 1.1–1.3 are easily seen to be not only necessary, but also sufficient for a half-plane P to exist so that $S_A(\chi) \notin P$ for any non-trivial character $\chi \in \widehat{G}$. For instance, if A satisfies either of conditions i) and iii) of Theorem 1.1 and if $P = \{z \in \mathbb{C} \colon \Re(z) \leq 0\}$ (the left closed half-plane), then $S_A(\chi) \notin P$ for any $\chi \in \widehat{G}$. Indeed, this is obvious for condition i). As to condition iii), suppose that L is a finite subgroup of G and that $A \subseteq L$ satisfies $A \cap (-A) = \{0\}$ and $A \cup (-A) = L$. Then

$$2\Re(S_A(\chi)) = S_A(\chi) + S_{-A}(\chi) = 1 + S_L(\chi) \geq 1,$$

whence $S_A(\chi) \notin P$. Similarly, it is not difficult to verify that if A satisfies either of conditions ii) and iv) of Theorem 1.1 and if $P = \{z \in \mathbb{C} \colon \Re(z) \geq 0\}$ (the right closed half-plane), then $S_A(\chi) \notin P$ for any non-trivial character $\chi \in \widehat{G}$. We notice also that the sets $\{0\}$ and $G \setminus \{0\}$ satisfy conditions iii) and iv) of Theorem 1.1.

Remark. The assumption $P \cap \mathbb{R} = \varnothing$ of Theorems 1.2 and 1.3 excludes the situation when P is either the upper or the lower complex half-plane, and $A = -A$, implying that $S_A(\chi)$ is real for any $\chi \in \widehat{G}$. In fact, it is easy to see that the condition $A = -A$ is necessary and sufficient for all character sums $S_A(\chi)$ ($\chi \in \widehat{G}$) to be real.

We derive Theorems 1.1–1.3 from a particular case of the first of these theorems — the case that refers to the left closed half-plane and finite abelian groups. We state it separately.

Proposition 1.4. *Let A be a subset of a finite abelian group G. Then we have $\Re(S_A(\chi)) > 0$ for all $\chi \in \widehat{G}$ if and only if one of the following holds:*

i) *$A = \{0, g\}$, where $g \in G \setminus \{0\}$ is of odd order;*
ii) *$A \cap (-A) = \{0\}$, and $A \cup (-A)$ is a subgroup of G.*

We prove Proposition 1.4 in Section 3 (this presents the major difficulty), and then derive Theorems 1.1–1.3 in Section 4. The proofs are mostly of combinatorial nature. Two auxiliary geometry of numbers results are established in the Appendix.

Before we turn to the proofs, we discuss some consequences of Theorems 1.1–1.3.

2. Applications

For certain groups G the property in question has a transparent "geometric" interpretation. Say, if A is a subset of the elementary 2-group $\mathbb{Z}_2^r$ (where r is a positive integer), then letting $H = \ker\chi$ we get $S_A(\chi) = |A \cap H| - |A \setminus H| = 2(|A \cap H| - |A|/2)$. As χ runs over all non-trivial characters of $\mathbb{Z}_2^r$, the kernel $\ker\chi$ runs over all index two subgroups of $\mathbb{Z}_2^r$. Thus, $|A \cap H| > |A|/2$ for any index two subgroup H if and only if there is no character χ such that $S_A(\chi)$ lies in the left closed half-plane, and $|A \cap H| < |A|/2$ for any index two subgroup if and only if there is no non-trivial character χ such that $S_A(\chi)$ lies in the right closed half-plane. Applying Theorem 1.1 we obtain the following corollary.

Corollary 2.1. *Let $r \geq 1$ be an integer, and let $A \subseteq \mathbb{Z}_2^r$.*

i) *If $A \neq \{0\}$ then there exists an index two subgroup $H \leq \mathbb{Z}_2^r$ such that $|A \cap H| \leq |A|/2$;*
ii) *if $A \neq \mathbb{Z}_2^r \setminus \{0\}$ then there exists an index two subgroup $H \leq \mathbb{Z}_2^r$ such that $|A \cap H| \geq |A|/2$.*

(In fact, it can be shown that there exists an index two subgroup $H \leq \mathbb{Z}_2^r$ such that $|A \cap H| < |A|/2$, unless A is a subgroup itself, and there exists an index two subgroup $H \leq \mathbb{Z}_2^r$ such that $|A \cap H| > |A|/2$, unless A is the complement of a subgroup.)

Consider now the elementary 3-group $\mathbb{Z}_3^r$. We have $\Re(S_A(\chi)) = |A \cap H| - |A \setminus H|/2 = \frac{3}{2}(|A \cap H| - |A|/3)$, where $H = \ker\chi$. As χ runs over all non-trivial characters of $\mathbb{Z}_3^r$, the kernel $\ker\chi$ runs over all index three subgroups of $\mathbb{Z}_3^r$. Applying Theorem 1.1 we get

Corollary 2.2. *Let $r \geq 1$ be an integer, and let $A \subseteq \mathbb{Z}_3^r$.*

i) *If* $|A \cap H| > |A|/3$ *for all index three subgroups* $H \le \mathbb{Z}_3^r$, *then there exists a subgroup* $L \le \mathbb{Z}_3^r$ *such that* $A \cap (-A) = \{0\}$ *and* $A \cup (-A) = L$;
ii) *if* $|A \cap H| < |A|/3$ *for all index three subgroups* $H \le \mathbb{Z}_3^r$, *then there exists a subgroup* $L \le \mathbb{Z}_3^r$ *such that* $A \cup (-A) = \mathbb{Z}_3^r \setminus \{0\}$ *and* $A \cap (-A) = \mathbb{Z}_3^r \setminus L$.

Characters of the additive group of integers are of the form $\chi\colon a \mapsto e^{2\pi i a z}$, where $z \in [0,1)$. Consequently, applied to this group and the left open half-plane, Theorem 1.3 yields

Corollary 2.3. *Let* $T(z) = \cos(2\pi a_1 z) + \cdots + \cos(2\pi a_n z)$, *where* $n \ge 2$ *and* $a_1, \dots, a_n$ *are pairwise distinct integers. Then* $\min_{z \in [0,1)} T(z) < 0$, *unless* $n = 2$ *and* $a_1 a_2 = 0$.

It should be pointed out that Corollaries 2.1–2.3 can be established directly, without appealing to Theorems 1.1 and 1.3. However, application of these theorems to other groups (like finite cyclic groups) leads to results which we cannot prove in another way.

The problem of estimating the minimum value of the polynomial $T(z)$ of Corollary 2.3 in terms of n is well-known and is far from being solved; see [2]. If the absolute values of $a_1, \dots, a_n$ are pairwise distinct, the best known result for large n is

$$\min_{z \in [0,1]} T(z) \le -e^{(\ln n)^{\delta}}$$

(where δ is an absolute positive constant), obtained by Bourgain [1]. For arbitrary integers $a_1, \dots, a_n$ it is known that

$$\min_{z \in [0,1]} T(z) \le -\delta \ln n,$$

see [3, 5, 6]. To our knowledge, for abelian groups other than the additive group of integers this problem has never been considered.

Some problems concerning the distribution of character sums for cyclic groups of prime order were studied in [4].

3. Proof of Proposition 1.4

Throughout this section we assume that G is a finite non-trivial abelian group. (Notice, that Proposition 1.4 is immediate for the trivial group $G = \{0\}$.) By A we denote a non-empty subset of G. We say that A is *positive* if $\Re(S_A(\chi)) > 0$ for any $\chi \in \widehat{G}$. We want to establish the structure of positive subsets $A \subseteq G$.

Lemma 3.1. *If* $A \subseteq G$ *is positive, then* $0 \in A$.

Proof. If χ_0 denotes the principal character of G, then

$$|A| = S_A(\chi_0) \le \sum_\chi \Re(S_A(\chi)) = \Re\left(\sum_a \sum_\chi \chi(a)\right) = \begin{cases} 0 & \text{if } 0 \notin A, \\ |G| & \text{if } 0 \in A. \end{cases}$$

□

Notice that the above computation gives

$$\min_\chi \Re(S_A(\chi)) \le (|G| - |A|)/(|G| - 1) \le 1,$$

while our goal is to prove that

$$\min_\chi \Re(S_A(\chi)) \le 0$$

(unless A possesses some special structure).

Observing that for any element $g \in G$ of either infinite or even order there exists a character $\chi \in \widehat{G}$ such that $\chi(g) = -1$, we obtain

Corollary 3.2. *Suppose that $A \subseteq G$ is positive.*

i) *If $|A| = 1$, then $A = \{0\}$;*
ii) *if $|A| = 2$, then $A = \{0, g\}$, where $g \in G \setminus \{0\}$ is of odd order.*

We say that $A \subseteq G$ is *antisymmetric* if $A \cap (-A) \subseteq \{0\}$. If A is antisymmetric and $A \cup (-A)$ is a finite subgroup of G then we say that A is *maximal antisymmetric*.

Proposition 1.4 essentially states that any positive set A of cardinality $|A| > 2$ is maximal antisymmetric. Though maximality is subtle, the fact that positive sets are antisymmetric is easy to establish.

In the proof of the following lemma and henceforth, we denote by δ_A the indicator function of A.

Lemma 3.3. *If $A \subseteq G$ is positive, then it is antisymmetric.*

Proof. Fix $b \in G \setminus \{0\}$. We have

$$\begin{aligned} 0 &< \frac{1}{|G|} \sum_\chi \Re(S_A(\chi)) \, |1 - \chi(b)|^2 \\ &= \frac{1}{|G|} \Re\Big(\sum_\chi S_A(\chi) \, (2 - \chi(b) - \chi(-b)) \Big) \\ &= 2 - \delta_A(b) - \delta_A(-b), \end{aligned}$$

hence either $b \notin A$, or $b \notin -A$. □

Corollary 3.4. *If $A \subseteq G$ is positive, then $A \cap (-A) = \{0\}$. In particular, A does not contain elements of order two.*

Lemma 3.5. *Suppose that $B \subseteq G$ is symmetric, contains zero (that is, $0 \in B = -B$) and satisfies $kS_B(\chi) + 1 \ge 0$ for some fixed integer $k \ge 2$ and all characters $\chi \in \widehat{G}$. Then B is a subgroup of G.*

Proof. We assume that $k = 2$, which yields the weakest restriction on B.

If $|B| = 2$ then $B = \{0, b\}$ where b is of order two and the assertion is trivial.

If $|B| = 3$ then $B = \{0, -b, b\}$ where b is of order $m \ge 3$. Indeed, the case $m = 3$ is trivial, while otherwise there exists an mth root of unity, say ζ, such that $\Re(\zeta) \le \cos 4\pi/5 < -3/4$. Accordingly, there exists a character $\chi \in \widehat{G}$ such that $\chi(b) = \zeta$ and then $2S_B(\chi) + 1 = 4\Re(\zeta) + 3 < 0$, a contradiction.

Suppose now that $|B| \ge 4$. Let $b, c \in B \setminus \{0\}$, $b \ne \pm c$. Then

$$
\begin{aligned}
(*) \qquad 0 &\le \frac{1}{|G|} \sum_{\chi} (2S_B(\chi) + 1) \left|1 - \chi(b)\right|^2 \left|1 - \chi(c)\right|^2 \\
&= \frac{1}{|G|} \sum_{\chi} (2S_B(\chi) + 1) \big(2 - \chi(b) - \chi(-b)\big)\big(2 - \chi(c) - \chi(-c)\big) \\
&= 12 - 8\delta_B(b) - 8\delta_B(c) + 4\delta_B(b + c) + 4\delta_B(b - c) \\
&= 4\delta_B(b + c) + 4\delta_B(b - c) - 4.
\end{aligned}
$$

This shows that $b \pm c \in B$, unless each summand in the right-hand side of $(*)$ equals zero. But in this case we would have

$$
\begin{aligned}
0 &= \frac{1}{|G|} \sum_{\chi} (2S_B(\chi) + 1)\,(1 - \chi(b))(1 - \chi(c)) \\
&= \frac{1}{|G|} \sum_{\chi} (2S_B(\chi) + 1)\,(1 - \chi(b) - \chi(c) + \chi(b + c)) \\
&= 3 - 2\delta_B(b) - 2\delta_B(c) + 2\delta_B(b + c) \\
&= 2\delta_B(b + c) - 1
\end{aligned}
$$

which is impossible.

We see that $b + c \in B$ for any $b, c \in B$, provided that $c \ne b$. To conclude the proof it suffices to show that $2b \in B$ for any $b \in B$. For this, fix arbitrarily $c \in B \setminus \{0, \pm b\}$; such c exists as $|B| \ge 4$. By the above, $b - c, b + c \in B$. If $2c \ne 0$ then $b + c \ne b - c$ whence $2b = (b + c) + (b - c) \in B$. Now suppose that $2c = 0$. Since $b + c \in B$ and thus also $2b + c = (b + c) + b \in B$, we have $2b = (2b + c) + c \in B$ unless $2b + c = c$. But in this case $2b = 0 \in B$. □

We now introduce some more notation. Given a set $A \subseteq G$, we put $A^* := A \cup (-A)$ and denote by $S^*(\chi)$ the Fourier coefficients, and by δ^* the indicator function of A^*; this allows us to avoid bulky expressions

like S_{A^*} and δ_{A^*}. Clearly, if A is antisymmetric and contains zero then $|A^*| = 2|A| - 1$ and moreover, $2\Re(S_A(\chi)) = S_A(\chi) + S_{-A}(\chi) = S^*(\chi) + 1$. It follows that if $A \cap (-A) = \{0\}$, then for A to be positive it is necessary and sufficient that $S^*(\chi) + 1 > 0$ for any $\chi \in \widehat{G}$.

Lemma 3.6. *Suppose that $A \subseteq G$ is positive. Then for any $b, c \in A^*$ at least one of the two elements $b + c$ and $b - c$ belongs to A^*.*

Proof. We can assume that $b, c, b \pm c \neq 0$. Then

$$\sum_{\chi}(1 - \chi(b))(1 - \chi(c)) = |G| > 0,$$

hence there is a character χ such that both $\chi(b)$ and $\chi(c)$ are distinct from one. Thus

$$\begin{aligned}
0 &< \frac{1}{|G|}\sum_{\chi}(S^*(\chi) + 1)\left|1 - \chi(b)\right|^2\left|1 - \chi(c)\right|^2 \\
&= \frac{1}{|G|}\sum_{\chi}(S^*(\chi) + 1)\big(2 - \chi(b) - \chi(-b)\big)\big(2 - \chi(c) - \chi(-c)\big) \\
&= 8 - 4\delta^*(b) - 4\delta^*(c) + 2\delta^*(b + c) + 2\delta^*(b - c) \\
&= 2\delta^*(b + c) + 2\delta^*(b - c)
\end{aligned}$$

implying the result. □

Lemma 3.7. *Suppose that $A \subseteq G$ is positive, and let $b - c, b, b + c \in A^*$. Then $c \in A^*$.*

Proof. We can assume that $b, c, b \pm c \neq 0$. Then, as in the proof of the previous lemma,

$$\begin{aligned}
0 &< \frac{1}{|G|}\sum_{\chi}(S^*(\chi) + 1)\left|1 - \chi(b)\right|^2\left|1 + \chi(c)\right|^2 \\
&= \frac{1}{|G|}\sum_{\chi}(S^*(\chi) + 1)\big(2 - \chi(b) - \chi(-b)\big)\big(2 + \chi(c) + \chi(-c)\big) \\
&= 8 - 4\delta^*(b) + 4\delta^*(c) - 2\delta^*(b + c) - 2\delta^*(b - c) \\
&= 4\delta^*(c)
\end{aligned}$$

and the result follows. □

Lemma 3.8. *Suppose that $A \subseteq G$ is positive. If there exists a non-zero element $h \in G$ such that $A^* + h = A^*$ (that is, if A^* is periodic), then A is maximal antisymmetric.*

Proof. Let H be the set of *all* $h \in G$ satisfying $A^* + h = A^*$. Clearly, H is a non-zero subgroup of G, and we denote by A^*/H the image of A^* under the canonical homomorphism $G \to G/H$. If $\widetilde{\chi}$ is a character of G/H and χ is the induced character of G, then

$$|H|\, S_{A^*/H}(\widetilde{\chi}) + 1 = S^*(\chi) + 1 > 0.$$

Plainly, $0 \in A^*/H$ and A^*/H is symmetric. By Lemma 3.5, the set A^*/H is a subgroup of G/H, whence A^* is a subgroup of G, as wanted. $\square$

Lemma 3.9. *Suppose that $A \subseteq G$ is positive. If A^* contains a non-zero subgroup $H \subseteq G$, then A is maximal antisymmetric.*

Proof. We fix arbitrarily $b \in A^*$ and $h \in H \setminus \{0\}$ and show that $b + h \in A^*$; the result will follows then from Lemma 3.8. Assume the opposite: $b + h \notin A^*$. Denote by T the set of all those non-negative integers t satisfying $b - th \in A^*$. Clearly, $0 \in T$. Furthermore, if $t \in T$ then applying Lemma 3.6 to $b-th, (t+1)h \in A^*$ we conclude that $2t+1 \in T$. Moreover, if $t-1, t+1 \in T$ then applying Lemma 3.7 to $b-(t-1)h, h, -b+(t+1)h \in A^*$ we obtain $t \in T$. This shows that in fact T contains all non-negative integers: for if $t \ge 1$ is the smallest integer which does not belong to T, then t is even and $t-1, t+1 \in T$, which is impossible. It remains to observe that h is of finite order, so that there exists t such that $b - ht = b + h$. $\square$

Lemma 3.10. *Suppose that $A \subseteq G$ is positive. If there exists $a \in A^* \setminus \{0\}$ such that $2a \in A^*$, then A^* is maximal antisymmetric.*

Proof. By Lemma 3.9, it suffices to show that A^* contains the cyclic subgroup generated by a. Assuming that this is false, let $k \ge 3$ denote the smallest positive integer such that $ka \notin A^*$.

Suppose first that $k \ge 4$. Applying Lemma 3.7 with $b = a$, $c = ka$ we see that $(k+1)a \notin A^*$. Applying Lemma 3.7 with $b = (k-j)a$, $c = ka$ for $j \in \{1, 2, 3\}$ we see that $(2k-j)a \notin A^*$. Applying Lemma 3.7 with $b = (k-1)a$, $c = (2k-2)a$ we see that $(3k-3)a \notin A^*$. Since

$$\sum_{\chi} (1 - \chi((k-2)a))(1 - \chi((k-1)a))(1 + \chi(ka)) = |G| > 0,$$

it follows that

$$\begin{aligned}
0 &< \frac{1}{|G|}\sum_{\chi}(S^*(\chi)+1)\,\big|1-\chi((k-2)a)\big|^2\big|1-\chi((k-1)a)\big|^2\big|1+\chi(ka)\big|^2\\
&= \frac{1}{|G|}\sum_{\chi}(S^*(\chi)+1)\,\big(2-\chi((k-2)a)-\chi(-(k-2)a)\big)\\
&\qquad\qquad\cdot\big(2-\chi((k-1)a)-\chi(-(k-1)a)\big)\big(2+\chi(ka)+\chi(-ka)\big)\\
&= 16-4\delta^*(2a)+2\delta^*((k-3)a)-8\delta^*((k-2)a)-6\delta^*((k-1)a)\\
&\qquad\qquad+8\delta^*(ka)+2\delta^*((k+1)a)+4\delta^*((2k-3)a)\\
&\qquad\qquad\qquad-4\delta^*((2k-2)a)-4\delta^*((2k-1)a)+2\delta^*((3k-3)a)\\
&= 16-4+2-8-6,
\end{aligned}$$

a contradiction.

Now suppose that $k=3$. Let l be the smallest positive integer such that $l\geq 4$ and $la\in A^*$. Applying Lemma 3.7 with $b=a$, $c=3a$ we see that $4a\notin A^*$. Applying Lemma 3.7 with $b=2a$, $c=3a$ we see that $5a\notin A^*$. Applying Lemma 3.7 with $b=2a$, $c=4a$ we see that $6a\notin A^*$. Therefore, $l\geq 7$. Applying Lemma 3.6 with $b=la$, $c=a$ we see that $(l+1)a\in A^*$. Applying Lemma 3.6 with $b=la$, $c=2a$ we see that $(l+2)a\in A^*$. Applying Lemma 3.6 with $b=(l+1)a$, $c=2a$ we see that $(l+3)a\in A^*$. In view of $-3a\notin A^*$ (recall that $k=3$) this implies that the order of a is either $l+2$, or at least $l+7$. This gives

$$\sum_{\chi}(1-\chi(a))(1-\chi(2a))(1-\chi(la))\geq |G|>0$$

and it follows that

$$\begin{aligned}
0 &< \frac{1}{|G|}\sum_{\chi}(S^*(\chi)+1)\,\big|1-\chi(a)\big|^2\big|1-\chi(2a)\big|^2\big|1-\chi(la)\big|^2\\
&= \frac{1}{|G|}\sum_{\chi}(S^*(\chi)+1)\,\big(2-\chi(a)-\chi(-a)\big)\\
&\qquad\qquad\cdot\big(2-\chi(2a)-\chi(-2a)\big)\big(2-\chi(la)-\chi(-la)\big)\\
&= 16-4\delta^*(a)-8\delta^*(2a)+4\delta^*(3a)-2\delta^*((l-3)a)\\
&\qquad\qquad+4\delta^*((l-2)a)+2\delta^*((l-1)a)-8\delta^*(la)+2\delta^*((l+1)a)\\
&\qquad\qquad\qquad+4\delta^*((l+2)a)-2\delta^*((l+3)a)\\
&= 16-4-8-8+2+4-2,
\end{aligned}$$

a contradiction. □

Corollary 3.11. *Any positive set $A\subseteq G$ of cardinality $|A|=3$ is maximal antisymmetric.*

Proof. Let $A = \{0, b, c\}$. By Lemma 3.3 we have $b + c \neq 0$, thus by Lemma 3.6 at least one of

$$b + c = -b,\ b + c = -c,\ b - c = -b,\ \text{or } b - c = c$$

holds. In any case we have either $2b = \pm c \in A^*$, or $2c = \pm b \in A^*$, hence A is maximal antisymmetric by Lemma 3.10. □

We are now in a position to sharpen Lemmas 3.6 and 3.7 considerably.

Lemma 3.12. *Suppose that $A \subseteq G$ is positive. Then either A is maximal antisymmetric, or for any $b, c \in A^* \setminus \{0\}$* exactly one *of the two elements $b + c$ and $b - c$ belongs to A^*.*

Proof. Assume that both $b+c$ and $b-c$ belong to A^*. Then by Lemma 3.6 either $2b = (b+c)+(b-c) \in A^*$, or $2c = (b+c)-(b-c) \in A^*$. However, if A is not maximal antisymmetric then any of the two conclusions contradicts Lemma 3.10. □

Lemma 3.13. *Suppose that $A \subseteq G$ is positive and let $b - c, b, b + c \in A^*$. Then either A is maximal antisymmetric, or $b = 0$, or $c = 0$. That is, either A is maximal antisymmetric, or A^* contains no three-term arithmetic progressions, except those centered at zero.*

Proof. By Lemma 3.7 we have $c \in A^*$, and by Lemma 3.12 from $b+c, b-c \in A^*$ it follows that either A is maximal antisymmetric, or $b = 0$, or $c = 0$. □

Lemma 3.14. *Any positive set $A \subseteq G$ of cardinality $|A| \geq 5$ is maximal antisymmetric.*

Proof. Suppose that A is not maximal antisymmetric. Fix arbitrarily $a \in A^* \setminus \{0\}$ and $b \in A^* \setminus \{0, \pm a\}$ and observe that by Lemma 3.12, either $b + a \in A^*$, or $b - a \in A^*$. Replacing b by $-b$, if necessary, we can assume that $b + a \in A^*$. Notice that $b + a \notin \{0, \pm a, \pm b\}$: for if $b + a = -a$ then $2a = -b \in A^*$ and if $b + a = -b$ then $2b = -a \in A^*$, contradicting Lemma 3.10. Since $|A| \geq 5$, there exists an element $c \in A^* \setminus \{0, \pm a, \pm b, \pm(b + a)\}$. Similarly to the above, we can assume that $c+a \in A^*$ and verify that $c+a \notin \{0, \pm a, \pm b, \pm(b+a), \pm c\}$. (Say, if $c+a = b$ then $c, c+a, c+2a = b+a \in A^*$, contradicting Lemma 3.13; if $c + a = -b$ then $c = -(b + a)$, contradicting the choice of c; if $c + a = -(b + a)$, then $c, c + a, c + 2a = -b \in A^*$, again, contradicting Lemma 3.13.) Thus, $\{0, \pm a, \pm b, \pm(b+a), \pm c, \pm(c+a)\} \subseteq A^*$.

We claim that $a+b+c \in A^*$. Indeed, otherwise we would have $(a+c)+b \notin A^*$, hence $a + c - b \in A^*$ by Lemma 3.12, and similarly $a + b - c \in A^*$. However, $a + c - b, a$, and $a + b - c$ are in a progression, which contradicts Lemma 3.13.

The only property of c we used in the above argument is that $\{\pm c, \pm(c+a)\} \subseteq A^* \setminus \{0, \pm a, \pm b, \pm(b+a)\}$. Since $c' := -c-a$ also has this

property, we conclude that $b-c=a+b+c'\in A^*$ and therefore $b+c\notin A^*$ by Lemma 3.12.

As $b-c=(b+a)-(c+a)\in A^*$, by Lemma 3.12 we have $2a+b+c=(b+a)+(c+a)\notin A^*$.

We have obtained that $a+b+c\in A^*$, whereas $(a+b+c)+a=2a+b+c\notin A^*$ and $(a+b+c)-a=b+c\notin A^*$; this, however, is impossible by Lemma 3.12. □

The assertion of Proposition 1.4 follows at once from Corollaries 3.2 and 3.11, Lemma 3.14, and our next lemma.

Lemma 3.15. *Any positive set $A\subseteq G$ of cardinality $|A|=4$ is maximal antisymmetric.*

Proof. The proof is based on two more claims.

Claim 3.16. *Let $d\geq 2$ be an integer. Suppose that $m,n\in\mathbb{Z}$ satisfy*

$$m,n,m+n\not\equiv 0 \pmod d \quad \text{and} \quad \gcd(m,n,d)=1.$$

Then there exists an integer z such that

$$\cos\pi\frac{mz}{d}\,\cos\pi\frac{nz}{d}\,\cos\pi\frac{(m+n)z}{d}\leq 0,$$

except if $d=7$ and $0,\pm m,\pm n,\pm(m+n)$ represent all residue classes modulo d.

Claim 3.17. *Let $d_0,d\geq 2$ be integers such that $d_0\mid d$. Suppose that $m_0,n_0,m,n\in\mathbb{Z}$ satisfy*

$$\gcd(m,n,d)=\gcd(m_0n-mn_0,\,d_0)=1.$$

Then there exist integers z_0 and z such that

$$\cos\pi\Big(\frac{m_0z_0}{d_0}+\frac{mz}{d}\Big)\,\cos\pi\Big(\frac{n_0z_0}{d_0}+\frac{nz}{d}\Big)\,\cos\pi\Big(\frac{(m_0+n_0)z_0}{d_0}+\frac{(m+n)z}{d}\Big)\leq 0.$$

Remark. Though this is not obvious, these two claims are actually geometry of numbers statements. For instance, the former of them asserts that the cyclic two-dimensional lattice $(m,n)\mathbb{Z}+d\mathbb{Z}^2$ has a point in the "butterfly area" formed by the two triangles $x,y\leq d/2$, $x+y\geq d/2$ and $x,y\geq d/2$, $x+y\leq(3/2)d$. This is the idea underpinning the proof of Claim 3.16.

Postponing the proofs of Claims 3.16 and 3.17 until the Appendix, we return to the proof of Lemma 3.15. Assume that $A\subseteq G$ is a positive set of cardinality $|A|=4$ which is not maximal antisymmetric. Fix $a\in A^*\setminus\{0\}$ and $b\in A^*\setminus\{0,\pm a\}$. By Lemma 3.12 we have either $b+a\in A^*$ or $b-a\in A^*$. Replacing b by $-b$, if necessary, we can assume that $b+a\in A^*$, whence $A^*=\{0,\pm a,\pm b,\pm(b+a)\}$. (Observe, that $b+a\notin\{0,\pm a,\pm b\}$ by

Lemma 3.10.) Denote by G_0 the subgroup of G, generated by a and b. Clearly, A remains positive when considered as a subset of G_0.

Suppose first that G_0 is cyclic. Denote by g its generator and let $d = |G_0|$ be the order of g. Choose $m, n \in \mathbb{Z}$ such that $a = mg$, $b = ng$. Since $a, b, a+b \neq 0$ we have $m, n, m+n \not\equiv 0 \pmod d$. Furthermore, if α and β are integers such that $g = \alpha a + \beta b$, then $g = (m\alpha + n\beta)g$ whence $m\alpha + n\beta \equiv 1 \pmod d$ and consequently, $\gcd(m, n, d) = 1$. This shows that the assumptions of Claim 3.16 are satisfied.

Given an integer z, consider the character $\chi \in \widehat{G}_0$ that maps g into $e^{2\pi i z/d}$. We have

$$\begin{aligned} S^*(\chi) + 1 &= 2 + 2\cos 2\pi\frac{mz}{d} + 2\cos 2\pi\frac{nz}{d} + 2\cos 2\pi\frac{(m+n)z}{d} \\ &= 4\cos\pi\frac{(m-n)z}{d}\,\cos\pi\frac{(m+n)z}{d} + 4\cos^2\pi\frac{(m+n)z}{d} \\ &= 8\cos\pi\frac{mz}{d}\,\cos\pi\frac{nz}{d}\,\cos\pi\frac{(m+n)z}{d}, \end{aligned}$$

and by Claim 3.16 either there exists $\chi \in \widehat{G}_0$ such that $S^*(\chi)+1 \le 0$, or we have $d = 7$ and $\{0, \pm m, \pm n, \pm(m+n)\} \pmod d = \mathbb{Z}_d$. However, the former is impossible in view of the assumption that A is positive, and the latter is impossible for otherwise we would have $A^* = \{0, \pm a, \pm b, \pm(b+a)\} = G_0$, contradicting the assumption that A is not maximal antisymmetric.

Now suppose that G_0 is not cyclic, and therefore of rank two. (Recall that G_0 is generated by two elements, a and b.) Fix $g_0, g \in G_0$ such that $G = \langle g_0\rangle \oplus \langle g\rangle$ and that the orders d_0 and d of g_0 and g satisfy $d_0 \mid d$; here $\langle g_0\rangle$ and $\langle g\rangle$ denote the cyclic subgroups, generated by g_0 and g, respectively. Choose $m_0, n_0, m, n \in \mathbb{Z}$ satisfying

$$a = m_0 g_0 + mg,\ \ b = n_0 g_0 + ng.$$

If $\alpha_0, \beta_0, \alpha$, and β are integers such that

$$g_0 = \alpha_0 a + \beta_0 b,\ \ g = \alpha a + \beta b,$$

then

$$(*) \qquad g_0 = (\alpha_0 m_0 + \beta_0 n_0)g_0 + (\alpha_0 m + \beta_0 n)g,$$

$$(**) \qquad g = (\alpha m_0 + \beta n_0)g_0 + (\alpha m + \beta n)g$$

implying $\alpha m + \beta n \equiv 1 \pmod d$ and consequently, $\gcd(m, n, d) = 1$. We observe also that $(*)$ and $(**)$ can be interpreted as

$$\begin{pmatrix} g_0 \\ g \end{pmatrix} = \begin{pmatrix} \alpha_0 & \beta_0 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} m_0 & m \\ n_0 & n \end{pmatrix} \begin{pmatrix} g_0 \\ g \end{pmatrix}$$

whence

$$\begin{pmatrix} \alpha_0 & \beta_0 \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} m_0 & m \\ n_0 & n \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{d_0}$$

and therefore

$$\begin{vmatrix}\alpha_0 & \beta_0\\ \alpha & \beta\end{vmatrix}\begin{vmatrix}m_0 & m\\ n_0 & n\end{vmatrix} \equiv 1 \pmod{d_0},$$
$$\gcd(m_0 n - m n_0,\, d_0) = 1.$$

Thus the assumptions of Claim 3.17 are satisfied.

Given integers z_0 and z, consider the character $\chi \in \widehat{G}_0$ defined by $\chi(g_0) = e^{2\pi i z_0/d_0}$ and $\chi(g) = e^{2\pi i z/d}$. We have

$$\begin{aligned} S^*(\chi) + 1 &= 2 + 2\cos 2\pi\Big(\frac{m_0 z_0}{d_0} + \frac{mz}{d}\Big) + 2\cos 2\pi\Big(\frac{n_0 z_0}{d_0} + \frac{nz}{d}\Big)\\ &\qquad + 2\cos 2\pi\Big(\frac{(m_0+n_0) z_0}{d_0} + \frac{(m+n)z}{d}\Big)\\ &= 8\cos\pi\Big(\frac{m_0 z_0}{d_0} + \frac{mz}{d}\Big)\cos\pi\Big(\frac{n_0 z_0}{d_0} + \frac{nz}{d}\Big)\\ &\qquad \cos\pi\Big(\frac{(m_0+n_0) z_0}{d_0} + \frac{(m+n)z}{d}\Big), \end{aligned}$$

which, according to Claim 3.17, contradicts the fact that A is positive. □

4. Proof of Theorems 1.1–1.3

In this section we derive Theorems 1.1–1.3 from Proposition 1.4.

A special role in our argument is played by the half-planes

$$P^- := \{z \in \mathbb{C}\colon \Re(z) < 0\}, \quad P^+ := \{z \in \mathbb{C}\colon \Re(z) > 0\}$$

and their closures

$$P_0^- := \{z \in \mathbb{C}\colon \Re(z) \le 0\}, \quad P_0^+ := \{z \in \mathbb{C}\colon \Re(z) \ge 0\}.$$

Indeed, it suffices to prove Theorem 1.1 only for the half-planes P_0^+ and P_0^-, and Theorems 1.2 and 1.3 only for the half-planes P^+ and P^-. For let P be an *arbitrary* closed half-plane with zero on its boundary, and let A be a finite subset of an abelian group G. Consider the "conjugate" half-plane $\overline{P} := \{z \in \mathbb{C}\colon \bar{z} \in P\}$. If $S_A(\chi) \notin P$ for any non-trivial character χ, then considering conjugate characters we conclude that also $S_A(\chi) \notin \overline{P}$ for any non-trivial character χ. Therefore $S_A(\chi) \notin (P \cup \overline{P})$. However, the union $P \cup \overline{P}$ contains one of the half-planes P_0^+ and P_0^-. The situation when P is open and G is torsion-free or cyclic of prime order is considered similarly.

Theorem 1.1 is a consequence of the two lemmas that follow. The former of them is identical to Proposition 1.4, except that the group G is not assumed to be finite.

Lemma 4.1. *Let A be a finite subset of an abelian group G. Then we have $\Re(S_A(\chi)) > 0$ for any $\chi \in \widehat{G}$ if and only if one of the following holds:*

i) *$A = \{0, g\}$, where $g \in G \setminus \{0\}$ is of odd order;*

ii) $A \cap (-A) = \{0\}$, *and* $A \cup (-A)$ *is a subgroup of* G.

Proof. Suppose that $\Re(S_A(\chi)) > 0$ for any $\chi \in \widehat{G}$. Since every character of a subgroup can be extended to a character of the whole group, A is a positive subset of $\langle A \rangle$, the subgroup that it generates. We can write $\langle A \rangle = G_0 \oplus G_1$, where G_0 is finite and G_1 is freely generated. Let $k \ge 0$ be the rank, and $\{g_1, \dots, g_k\}$ a free system of generators of G_1. Fix an integer N and a prime number $p > N^k$ and consider the homomorphism $\varphi\colon \langle A \rangle \to G_0 \oplus \mathbb{Z}_p$ defined by

$$(g_0, m_1 g_1 + \dots + m_k g_k) \stackrel{\varphi}{\longmapsto} (g_0, m_1 + N m_2 + \dots + N^{k-1} m_k \pmod p)$$

(for any $g_0 \in G_0$ and $m_1, \dots, m_k \in \mathbb{Z}$). Provided that N is large enough, the restriction of φ onto A is one-to-one and moreover, if $a \notin G_0$ then also $\varphi(a) \notin G_0$ for any $a \in A$. Letting $\widetilde{A} = \varphi(A)$, for any character χ of the group $G_0 \oplus \mathbb{Z}_p$ we have $S_A(\chi \circ \varphi) = S_{\widetilde{A}}(\chi)$. Thus $\widetilde{A}$ is a positive subset of the finite group $G_0 \oplus \mathbb{Z}_p$. By Proposition 1.4, either $|\widetilde{A}| \le 2$ holds, or $\widetilde{A} \cup (-\widetilde{A})$ is a subgroup of $G_0 \oplus \mathbb{Z}_p$. In the former case we have $|A| = |\widetilde{A}| \le 2$ and the result follows easily. In the latter case, observing that any subgroup of $G_0 \oplus \mathbb{Z}_p$ is actually a subgroup of G_0, or otherwise has cardinality at least p, we conclude that $\widetilde{A} \subseteq G_0$, and consequently $A \subseteq G_0$. This, again, reduces the situation to the finite case. □

Next, we consider "negative" sets.

Lemma 4.2. *Let A be a finite subset of an abelian group G. Then $\Re(S_A(\chi)) < 0$ for any non-trivial character $\chi \in \widehat{G}$ if and only if G is finite and moreover, one of the following holds:*

i) $A = G \setminus \{0, g\}$, *where $g \in G \setminus \{0\}$ is of odd order;*
ii) $A \cup (-A) = G \setminus \{0\}$, *and $A \cap (-A)$ is the complement of a subgroup of G.*

Proof. Suppose that $\Re(S_A(\chi)) < 0$ for any non-trivial character $\chi \in \widehat{G}$. Denote by $\langle A \rangle$ the subgroup of G, generated by A. If $\langle A \rangle \ne G$, we choose arbitrarily a non-trivial character $\widetilde{\chi}$ of the factor group $G/\langle A \rangle$ and lift it to a non-trivial character $\chi \in \widehat{G}$. As χ contains A in its kernel, we have $S_A(\chi) = |A| > 0$, contradicting the assumption. This shows that $\langle A \rangle = G$ and in particular, G is finitely generated. To simplify the notation we assume that $G = G_0 \oplus \mathbb{Z}^k$ where G_0 is finite and $k \ge 0$. If $k \ge 1$, we fix a real number $\alpha > 0$ and consider the character $\chi \in \widehat{G}$ defined by

$$\chi\colon (g_0, m_1, \dots, m_k) \mapsto e^{2\pi i m_1 \alpha} \qquad (g_0 \in G_0,\ m_1, \dots, m_k \in \mathbb{Z}).$$

If α is small enough then evidently $\Re(\chi(a)) > 0$ for any $a \in A$, whence $\Re(S_A(\chi)) > 0$, again, contradicting the assumptions. Thus $k = 0$ and G is finite. Since $S_{G \setminus A}(\chi) = -S_A(\chi)$ for any non-trivial character χ,

the complement $G \setminus A$ is a positive subset of G, and it remains to apply Proposition 1.4. □

Theorem 1.1 is an immediate corollary of Lemmas 4.1 and 4.2 and the observation at the beginning of this section. Theorem 1.2 follows from this observation, Theorem 1.1, and our next lemma.

Lemma 4.3. *Let G be a cyclic group of odd prime order, and let A be a non-empty proper subset of G. Then $\Re(S_A(\chi)) \neq 0$ for any character $\chi \in \widehat{G}$.*

Proof. Let $p = |G|$ be the order of G. Identifying the elements of G with residue classes modulo p, we can write any non-trivial character of G in the form

$$\chi\colon z \mapsto \zeta^z \ (z \in G),$$

where $\zeta = \zeta(\chi)$ a primitive root of unity of degree p. Consequently,

$$2\Re(S_A(\chi)) = \sum_{a\in A} \zeta^a + \sum_{a\in A} \zeta^{p-a}.$$

If $\Re(S_A(\chi)) = 0$ then $\sum_{a\in A} t^a + \sum_{a\in A} t^{p-a}$ is a multiple of $P_\zeta(t) = t^{p-1} + \cdots + t + 1$, the minimal polynomial of ζ over the field of rational numbers. (Here we identify the elements of A with their integer representatives in $[0, p-1]$.) It is immediately seen, however, that this cannot be the case. □

Finally, we turn to torsion-free abelian groups. Theorem 1.3 follows from the observation at the beginning of this section and Lemmas 4.4 and 4.5 below.

Lemma 4.4. *Let A be a finite non-empty subset of a torsion-free abelian group G. Then $\Re(S_A(\chi)) \geq 0$ for any $\chi \in \widehat{G}$ if and only if $0 \in A$ and $|A| \leq 2$.*

Proof. We can assume that $G = \mathbb{Z}^k$. Fix an integer N and a prime number $p > N^k$, and define a homomorphism $\varphi\colon G \to \mathbb{Z}_p$ by

$$(m_1, \ldots, m_k) \overset{\varphi}{\longmapsto} m_1 + Nm_2 + \cdots + N^{k-1}m_k \pmod p$$

(for any $m_1, \ldots, m_k \in \mathbb{Z}$). We assume that N is so large that the restriction of φ on A is one-to-one and moreover, no non-zero element of A maps to zero. Write $\widetilde{A} := \varphi(A) \subseteq \mathbb{Z}_p$. Since for any character $\widetilde{\chi} \in \widehat{\mathbb{Z}}_p$ we have $S_{\widetilde{A}}(\widetilde{\chi}) = S_A(\widetilde{\chi} \circ \varphi)$, if $\Re(S_A(\chi)) \geq 0$ for any $\chi \in \widehat{G}$ then also $\Re(S_{\widetilde{A}}(\widetilde{\chi})) \geq 0$ for any $\widetilde{\chi} \in \widehat{\mathbb{Z}}_p$. By Lemma 4.3, the set $\widetilde{A}$ is strictly positive and by Proposition 1.4 we have either $\widetilde{A} = \{0\}$, or $\widetilde{A} = \{0, \tilde{g}\}$ for some $\tilde{g} \in \mathbb{Z}_p$. Accordingly, either $A = \{0\}$, or $A = \{0, g\}$ for some $g \in G \setminus \{0\}$. □

Lemma 4.5. *For any finite non-empty subset A of a torsion-free abelian group G there exists a non-trivial character $\chi \in \widehat{G}$ such that $\Re(S_A(\chi)) > 0$.*

Proof. As in the proof o Lemma 4.4, we assume that $G = \mathbb{Z}^k$. For $\alpha > 0$ consider the character $\chi \in \widehat{G}$ defined by

$$\chi\colon (m_1, \dots, m_k) \mapsto e^{2\pi i \alpha m_1} \qquad (m_1, \dots, m_k \in \mathbb{Z}).$$

We can choose α so small that $\Re(\chi(a)) > 0$ for any $a \in A$, and then $\Re(S_A(\chi)) > 0$. □

Appendix. Proof of Claims 3.16 and 3.17

Proof of Claim 3.16. If d is even the assertion follows by taking $z = d/2$ and observing that at least one of m and n is odd. Below we assume that d is odd.

Denote the product under consideration by $P_{m,n}(z)$. Since

$$P_{m,n}(z) = P_{n,m}(z) = P_{-m,-n}(z) = P_{m+n,-m}(z),$$

we can assume that

$$\gcd(m, d) \le \min\{\gcd(n, d),\ \gcd(m + n, d)\}.$$

We let $\delta := \gcd(m, d)$ and observe that if $\delta > 1$, then the inequality above is strict in view of $\gcd(m, n, d) = 1$.

Notice that $P_{m,n}(z)$ actually depends only on the residue classes of m, n, and z modulo d. Hence, if u is an integer such that $mu \equiv \delta \pmod d$, then $P_{m,n}(zu) = P_{mu,nu}(z) = P_{\delta,nu}(z)$. It is not difficult to see that u can be chosen to be co-prime with d, and this shows that $m = \delta$ can be assumed without loss of generality.

Next, we can assume that $1 \le n \le d - 1$. In fact we have then $\delta \le n \le d - \delta$, for otherwise

$$\gcd(n, d) = \gcd(d - n, d) \le \min\{n, d - n\} < \delta.$$

Since $P_{\delta,n}(z) = P_{\delta+n,-\delta}(z) = P_{\delta,d-\delta-n}(z)$, we can actually assume that

$$\delta \le n \le \frac{d - \delta}{2}.$$

Moreover, if $n = \delta$ then $\delta = 1$ and it is easy to verify that $\min_z P_{1,1}(z) \le 0$. Similarly, if $n = (d-\delta)/2$ then $\delta \,|\, (n, d)$ whence $\delta = 1$, and $\min_z P_{1,(d-1)/2}(z) \le P_{1,(d-1)/2}(1) \le 0$ in view of

$$\begin{aligned} P_{1,(d-1)/2}(1) &= \cos\frac{\pi}{d}\,\cos\pi\frac{(d-1)/2}{d}\,\cos\pi\frac{(d+1)/2}{d} \\ &= -\cos\frac{\pi}{d}\,\cos^2\pi\frac{(d-1)/2}{d}. \end{aligned}$$

With the above said in mind, for the rest of the proof we assume that

$$\delta + 1 \le n \le \frac{d - \delta}{2} - 1$$

and we notice that this implies $\delta \le d/5$.

If n is odd we set $z := (d-1)/2$ and observe that

i) $\delta z = \frac{\delta-1}{2}\, d + \frac{d-\delta}{2}$, whence $\operatorname{sign}\cos\pi\frac{\delta z}{d} = (-1)^{\frac{\delta-1}{2}}$;
ii) $nz = \frac{n-1}{2}\, d + \frac{d-n}{2}$, whence $\operatorname{sign}\cos\pi\frac{nz}{d} = (-1)^{\frac{n-1}{2}}$;
iii) $(\delta+n)z = \frac{\delta+n}{2}\, d - \frac{\delta+n}{2} > \frac{\delta+n}{2}\, d - \frac{d}{2}$, whence $\operatorname{sign}\cos\pi\frac{(\delta+n)z}{d} = (-1)^{\frac{\delta+n}{2}}$.

It follows that

$$\operatorname{sign} P_{\delta,n}(z) = (-1)^{\frac{\delta-1}{2}+\frac{n-1}{2}+\frac{\delta+n}{2}} = -1.$$

If n is even we fix positive integers k and t such that $(2k+1)\delta = n+1+2nt$ (this is possible as $\gcd(2\delta, 2n) = 2$ divides $n+1-\delta$) and set

$$z := \left\lceil \frac{2k+1}{2n}\, d \right\rceil.$$

We have then

i) $\delta z > \frac{(2k+1)\delta}{2n}\, d = td + \frac{d}{2} + \frac{d}{2n} > (t+1)d - \frac{d}{2}$,
$\delta z < td + \frac{d}{2} + \frac{d}{2n} + \delta \le td + \frac{d}{2} + \frac{d}{4} + \frac{d}{5} < (t+1)d$,
whence $\operatorname{sign}\cos\pi\frac{\delta z}{d} = (-1)^{t+1}$;
ii) $nz > (k+1)d - \frac{d}{2}$ and $nz < (k+1)d - \frac{d}{2} + n < (k+1)d$, whence $\operatorname{sign}\cos\pi\frac{nz}{d} = (-1)^{k+1}$;
iii) $(\delta+n)z = \delta z + nz > \big((t+1)d - \frac{d}{2}\big) + \big((k+1)d - \frac{d}{2}\big) = (k+t+1)d$.

To complete the proof it suffices to show that

$$(*) \qquad (\delta+n)z < (k+t+3/2)d,$$

as then we obtain $\operatorname{sign}\cos\pi\frac{(\delta+n)z}{d} = (-1)^{k+t+1}$ and

$$\operatorname{sign} P_{\delta,n}(z) = (-1)^{(t+1)+(k+1)+(k+t+1)} = -1.$$

We multiply $(*)$ by $2n$ (for technical reasons) and then consider the difference between its left-hand and right-hand sides. Denoting this difference by Δ, we get

$$\begin{aligned}
\Delta &:= 2n(\delta+n)z - 2n(k+t+3/2)d \\
&\le (\delta+n)\left((2k+1)d + 2n - \gcd(n,d)\right) - (2k+2t+3)nd \\
&\le (\delta+n)(2k+1)d + (\delta+n)(2n-\delta) - (2k+1)nd - 2(t+1)nd \\
&= (2k+1)\delta d - 2(t+1)nd + (2n^2 + n\delta - \delta^2) \\
&= (1-n)d + (2n^2 + n\delta - \delta^2) \\
&\le (1-n)(2n+\delta+2) + (2n^2 + n\delta - \delta^2) \\
&= -\delta^2 + \delta + 2.
\end{aligned}$$

Thus, if $\delta > 1$ then $\Delta \le 0$, proving $(*)$. (Observe, that $\Delta \ne 0$ as the left-hand side of $(*)$ is an integer, while the right-hand side is not.) Moreover, if $\delta = 1$ and $n \le (d-\delta)/2-2$, then $d \ge 2n+\delta+4$ and the latter computation can be strengthened to give

$$\begin{aligned}\Delta &\le (1-n)(2n+\delta+4) + (2n^2+n\delta-\delta^2)\\ &= -\delta^2+\delta+4-2n\\ &= -2n+4\\ &\le 0.\end{aligned}$$

We can assume, therefore, that $\delta = 1$ (which yields $2k = n + 2nt$) and $n = (d-\delta)/2 - 1 = (d-3)/2$.

If $(2k+1)d \not\equiv 1 \pmod{2n}$, then $z \le ((2k+1)d+2n-2)/2n$ and we have

$$\begin{aligned}\Delta &\le (1+n)\left((2k+1)d+2n-2\right) - (2k+2t+3)nd\\ &= -3(n-1) \qquad\qquad \text{(verification left to the reader)}\\ &< 0.\end{aligned}$$

Finally, suppose that $\delta = 1$, $n = (d-3)/2$, and $(2k+1)d \equiv 1 \pmod{2n}$. Then

$$1 \equiv (2k+1)d \equiv (n+1)\cdot 3 \equiv n+3 \pmod{2n},$$

hence $2n \mid n+2$ implying $n = 2$ and $d = 7$. This is the exceptional case. □

Proof of Claim 3.17. If d is even then the result follows easily as in the proof of Claim 3.16. Suppose that d is odd and consequently, $d_0 > 2$.

If $d = 7$ then $d_0 = 7$, and the assumptions imply that there exist integers z_0 and z such that

$$m_0 z_0 + mz \equiv n_0 z_0 + nz \equiv 2 \pmod 7.$$

Plainly, with this choice of z_0 and z the product we are interested in is negative.

Suppose now that d is odd and $d \ne 7$. If $m, n, m+n \not\equiv 0 \pmod d$, then we can disregard z_0 (taking it to be zero) and the result follows from Claim 3.16. Otherwise, we can assume that $m + n \equiv 0 \pmod d$: for if, say, $m \equiv 0 \pmod d$, then one verifies readily that

$$m_0' := m_0 + n_0,\ n_0' := -n_0,\ m' := m+n,\ n' := -n$$

satisfy the assumptions, and $m' + n' \equiv 0 \pmod d$. Next, since our product remains unchanged when n increases by a multiple of d, we can assume that $n = -m$. Similarly, the product is invariant under changes of n_0 by multiples of d_0, and therefore we can assume that m_0 and n_0 are of the same parity.

In view of $\gcd(m,d) = \gcd(m,-m,d) = \gcd(m,n,d) = 1$, for any integer z_0 we can find z so that

$$mz \equiv \frac{n_0 - m_0}{2}\,\frac{d}{d_0}\,z_0 \pmod{d}.$$

With this choice of z (and under the assumption that $n = -m$) we have

$$\frac{m_0 z_0}{d_0} + \frac{mz}{d} = \frac{((m_0+n_0)/2)\,z_0}{d_0} + u$$

and

$$\frac{n_0 z_0}{d_0} + \frac{nz}{d} = \frac{((m_0+n_0)/2)\,z_0}{d_0} - u$$

for some $u \in \mathbb{Z}$. Thus our product equals

$$\cos^2 \pi \frac{((m_0+n_0)/2)\,z_0}{d_0}\,\cos \pi \frac{(m_0+n_0)z_0}{d_0}$$

and since $m_0+n_0 \not\equiv 0 \pmod{d_0}$ (along with $m+n=0$ this would contradict the assumptions of the claim), there exists $z_0 \in \mathbb{Z}$ which makes this last expression negative. □

Acknowledgment

Much of this paper was completed when the authors attended the "Research in Pairs" program of the Oberwolfach Mathematics Institute. We are greatly indebted to the institute administration and stuff for their hospitality and support.

References

[1] J. Bourgain, *Sur le minimum d'une somme de cosinus, [On the minimum of a sum of cosines]*. Acta Arithmetica **45 (4)** (1986), 381–389.

[2] A.S. Belov, S.V. Konyagin, *On the conjecture of Littlewood and minima of even trigonometric polynomials*. Harmonic analysis from the Pichorides viewpoint (Anogia, 1995), 1–11, Publ. Math. Orsay, 96-01, Univ. Paris XI, Orsay, 1996.

[3] S.V. Konyagin, *On the Littlewood problem* Izv. Akad. Nauk SSSR Ser. Mat. **45 (2)** (1981), 243–265. (English translation: Mathematics of the USSR - Izvestiya **45 (2)** (1982), 205–225.)

[4] S.V. Konyagin, V. Lev, *On the distribution of exponential sums*. Integers **0** (2000), #A1 (electronic).

[5] O.C. McGehee, L. Pigno, B. Smith, *Hardy's inequality and the Littlewood conjecture*. Bull. Amer. Math. Soc. (N.S.) **5 (1)** (1981), 71–72.

[6] O.C. McGehee, L. Pigno, B. Smith, *Hardy's inequality and the L^1 norm of exponential sums*. Annals of Mathematics (2) **113 (3)** (1981), 613–618.

Sergei V. Konyagin
Department of Mechanics and Mathematics
Moscow State University
Moscow, Russia
E-mail : konyagin@ok.ru

Vsevolod F. Lev
Department of Mathematics
Haifa University at Oranim
Tivon 36006, Israel
E-mail : seva@math.haifa.ac.il