Exercise sheet 2

1. Show that if $A_1 \subset G_1$ and $A_2 \subset G_2$ are Sidon sets with $|A_i| \geqslant 2$, then $A_1 \times A_2$ is not a Sidon set in $G_1 \times G_2$.

   Solution. Since $|A_i| \geqslant 2$, $i = 1, 2$, we can take $a_1 \neq b_1 \in A_1$ and $a_2 \neq b_2 \in A_2$. Observe that

   $$(a_1, a_2) + (b_1, b_2) = (a_1, b_2) + (b_1, a_2)$$

   but $(a_1, a_2) \neq (a_1, b_2), (b_1, a_2)$. Thus $A_1 \times A_2$ is not a Sidon set.

2. Let G be a finite abelian group. Let $\alpha \in G$ be a fixed element. A subset $A \subset G$ is called a *symmetric Sidon set* with center α if $A = \alpha - A$ (i.e., for any x in A, the element $\alpha - x$ is also in A) and if the equation

   $$a + b = c + d$$

   with $(a, b, c, d) \in A^4$ implies that $a \in \{c, d\}$ or $a + b = \alpha$.

   (a) Let E be a field with characteristic different from 3. Prove that the set

   $$A = \{(x, x^3) \mid x \in E\} \subset E \times E$$

   is a symmetric Sidon set with center 0.

   (b) Prove that if $A \subset G$ is a symmetric Sidon set, then it contains a subset $A' \subset A$ with $|A'| \geqslant (|A| - 1)/2$ such that A' is a Sidon set.

   (c) Let G be a finite abelian group and $A \subset \widehat{G}$ a finite set of characters of G. If A is a symmetric Sidon set with center α, prove that

   $$\sum_{x \in G} \Big| \sum_{\chi \in A} \lambda_\chi \chi(x) \Big|^4 \leqslant 3 \Big(\sum_{\chi \in A} |\lambda_\chi|^2 \Big)^2.$$

   Solution.

   (a) First we observe that if $(x, x^3) \in A$ then $(-x, -x^3) = (-x, (-x)^3) \in A$. To conclude that A is a summetric Sidon set, we let $a, b, c, d \in E$ be such that

   $$a + b = c + d$$
   $$a^3 + b^3 = c^3 + d^3.$$

Taking the cube of the first equation and subtracting the second one, we get

$$3ab(a+b) = 3cd(c+d)$$

and since E has characteristic different than 3, it holds that

$$ab(a+b) = cd(c+d).$$

If $a+b=0$, there is nothing to prove. If $a+b \neq 0$, then it holds that

$$\begin{aligned} a+b &= c+d \\ ab &= cd, \end{aligned}$$

and, as we saw in class, this implies that $a \in \{c,d\}$.

(b) Recall that if A is a symmetric Sidon set with center α, it holds that $x \in A \Leftrightarrow \alpha - x \in A$. First we observe that there is at most one element $x \in A$ such that $x = \alpha - x \Rightarrow 2x = \alpha$. If it exists, we remove it and consider the ordering $A \backslash \{x\} = \{x_1, \alpha - x_1, \ldots, x_n, \alpha - x_n\}$. Let $A' = \{x_1, \ldots x_n\}$.
First let's prove that A' is a Sidon set. Let $a,b,c,d \in A'$ satisfying

$$a+b = c+d.$$

First, observe that $a+b \neq \alpha$, otherwise we would have $a = \alpha - b$ which is not possible by construction. Thus, since $A' \subset A$ and A is a symmetric Sidon set, it holds that $a \in \{c,d\}$ and we conclude that A' is a Sidon set.
Since we removed a potential $x = \alpha - x$, and for all $x_i, \alpha - x_i \in A$ we added exactly one of them, it holds that

$$|A'| \geqslant (|A|-1)/2.$$

(c) Opening the sum on the (LSH) we get

$$\frac{1}{|G|}\sum_{x\in G}\sum_{\chi_1,\chi_2,\chi_3,\chi_4\in A}\lambda_{\chi_1}\lambda_{\chi_2}\overline{\lambda_{\chi_3}\lambda_{\chi_4}}\chi_1(x)\chi_2(x)\overline{\chi_3(x)\chi_4(x)} =$$
$$\frac{1}{|G|}\sum_{\chi_1,\chi_2,\chi_3,\chi_4\in A}\lambda_{\chi_1}\lambda_{\chi_2}\overline{\lambda_{\chi_3}\lambda_{\chi_4}}\sum_{x\in G}\chi_1(x)\chi_2(x)\overline{\chi_3(x)\chi_4(x)}$$

and observe that from the orthogonality relations in $\hat{G}$ imply the sum inner sum is non-zero if an only if $\chi_1\chi_2 = \chi_3\chi_4$ and, since A is a symmetric Sidon set, this can only happen if $\chi_1 \in \{\chi_3, \chi_4\}$ or $\chi_1\chi_2 = \chi_3\chi_4 = \alpha$. Thus, the some above becomes

$$2\sum_{\substack{\chi_1,\chi_2\in A\\ \chi_1\chi_2\neq\alpha\\ \chi_1\neq\chi_2}}|\lambda_{\chi_1}|^2|\lambda_{\chi_2}|^2 + \sum_{\chi\in A}|\lambda_\chi|^4 + \sum_{\chi_1,\chi_3\in A}\lambda_{\chi_1}\lambda_{\alpha\chi_1^{-1}}\overline{\lambda_{\chi_3}\lambda_{\alpha\chi_3^{-1}}}.$$

Observe that

$$2 \sum_{\substack{\chi_1,\chi_2 \in A \\ \chi_1\chi_2 \neq \alpha + \sum_{\chi\in A} |\lambda_\chi|^4 \\ \chi_1 \neq \chi_2}} |\lambda_{\chi_1}|^2 |\lambda_{\chi_2}|^2 \leqslant 2 \left(\sum_{\chi \in A} |\lambda_\chi|^2 \right)^2,$$

and

$$\left| \sum_{\chi_1,\chi_3 \in A} \lambda_{\chi_1} \lambda_{\alpha\chi_1} \overline{\lambda_{\chi_3} \lambda_{\alpha\chi_3}} \right| \leqslant \left(\sum_{\chi\in A} |\lambda_\chi| \cdot |\lambda_{\alpha\chi}| \right)^2 = \left(\frac{1}{2} \sum_{\chi\in A} 2|\lambda_\chi| \cdot |\lambda_{\alpha\chi}| \right)^2$$
$$\leqslant \left(\frac{1}{2} \sum_{\chi\in A} |\lambda_\chi|^2 + |\lambda_{\alpha\chi}|^2 \right)^2 = \left(\sum_{\chi\in A} |\lambda_\chi|^2 \right)^2,$$

concluding the result.

3. Let G be an abelian group, denoted additively. For a finite subset $A \subset G$, we denote by $E(A)$ the number of quadruples $(a,b,c,d) \in A^4$ such that $a+b = c+d$.

   (a) Show that A is a Sidon set in G if and only if $E(A) = 2|A|^2 - |A|$.

   The remainder of the exercise shows that a finite set A may satisfy $E(A) = 2|A|^2 + O(|A|)$, but not contain any Sidon subset of size $\sim |A|$. We take $G = \mathbf{Z}$.

   (b) Show that for all large integers N, there exists a Sidon set $A \subset \{1,\dots,N\} \cap 2\mathbf{Z}$ with $|A| \to +\infty$ as $N \to +\infty$.

   (c) Consider a Sidon set $A \subset \{1,\dots,N\} \cap 2\mathbf{Z}$. Define

   $$A' = A \cup \{a + N2^{a+1} \mid a \in A\} \cup \{a - N2^{a+1} \mid a \in A\} \subset \mathbf{Z}.$$

   (d) Show that if $A'' \subset A'$ is a Sidon set, we have $|A''| \leqslant \frac{2}{3}|A'|$.

   (e) Let

   $$x_1 + x_2 = x_3 + x_4,$$

   with

   $$x_i = a_i + \varepsilon_i N 2^{a_i+1}, \quad a_i \in A, \quad \varepsilon_i \in \{-1,0,1\},$$

   Show that $a_1 + a_2 = a_3 + a_4$.

   (f) Suppose that $a_1 = a_3$, hence $a_2 = a_4$. Show that

   $$(\varepsilon_1 - \varepsilon_3)2^{a_1} = (\varepsilon_4 - \varepsilon_2)2^{a_2}.$$

   (g) Deduce that $x_1 = x_3$ if $\varepsilon_1 = \varepsilon_3$ or $\varepsilon_2 = \varepsilon_4$.

(h) Suppose further that $\varepsilon_1 \neq \varepsilon_3$ and $\varepsilon_2 \neq \varepsilon_4$. Show that $a_1 = a_2 = a_3 = a_4$ and $\varepsilon_1 + \varepsilon_2 = \varepsilon_3 + \varepsilon_4$.

(i) Conclude that if $x_1 \notin \{x_3, x_4\}$, then (x_1, x_2, x_3, x_4) has one of the forms

$$(a + N2^{a+1}, a - N2^{a+1}, a, a), \qquad (a - N2^{a+1}, a + N2^{a+1}, a, a),$$
$$(a, a, a - N2^{a+1}, a + N2^{a+1}), \qquad (a, a, a + N2^{a+1}, a - N2^{a+1}),$$

for some $a \in A$. (Hint: consider the various possibilities for $(\varepsilon_1, \ldots, \varepsilon_4)$ for given $(\varepsilon_3, \varepsilon_4)$.

(j) Deduce that

$$E(A'') = 2|A''|^2 + O(|A''|).$$

Solution.

(a) For any $(a, b, c, d) \in A^4$, let's count the number of trivial solutions for $a+b = c+d$:
   - if $a \neq b$, there are $|A|(|A|-1) \cdot 2$ solutions
   - if $a = b$ there are $|A|$ solutions.

   Thus, if A is a Sidon set, $E(A) = |A|(|A|-1) \cdot 2 + |A| = 2|A|^2 - |A|$. On the other hand, if $E(A) = |A|(|A|-1) \cdot 2 + |A| = 2|A|^2 - |A|$., there are only trivial solutions for the equation $a + b = c + d$, so A is a Sidon set.

(b) Let $A = \{2^n, n \leqslant \lfloor \log_2 N \rfloor\}$. The proof that A is a Sidon set follows from the uniqueness of representation of a number in basis 2.

(c) -

(d) For $a \in A$, we prove that it is only possible that two elements of the set $\{a, a + N \cdot 2^{a+1}, a + N \cdot 2^{a+1}\}$ can belong to A''. Indeed, if $\{a, a + N \cdot 2^{a+1}, a - N \cdot 2^{a+1}\} \subset A''$ then we can write

$$a + a = a + N \cdot 2^{a+1} + a - N \cdot 2^{a+1},$$

which is a contradiction, because A'' is a Sidon set. Thus $|A''| \leqslant \frac{2}{3}|A'|$.

(e) Let $x_1, x_2, x_3, x_4 \in A''$, where $x_i = a_i + \varepsilon_i \cdot N2^{a_i+1}$, satisfying $a_i \in A$ and $\varepsilon_i \in \{-1, 0, 1\}$, for $i = 1, 2, 3, 4$, and suppose that

$$x_1 + x_2 = x_3 + x_4.$$

Then, it holds that

$$a_1 + \varepsilon_1 N \cdot 2^{a_1+1} + a_2 + \varepsilon_2 N \cdot 2^{a_2+1} = a_3 + \varepsilon_3 N \cdot 2^{a_3+1} + a_4 + \varepsilon_4 N \cdot 2^{a_4+1}.$$

Reducing the equation modulo $2N$ we get

$$a_1 + a_2 \bmod 2N = a_3 + a_4 \bmod 2N,$$

and since $a_i \leqslant N$ we can conclude that

$$a_1 + a_2 = a_3 + a_4.$$

(f) If $a_1 = a_3$ and $a_2 = a_4$ we have

$$a_1 + \varepsilon_1 N \cdot 2^{a_1+1} + a_2 + \varepsilon_2 N \cdot 2^{a_2+1} = a_1 + \varepsilon_3 N \cdot 2^{a_1+1} + a_2 + \varepsilon_4 N \cdot 2^{a_2+1}$$
$$(\varepsilon_1 - \varepsilon_3)2^{a_1} = (\varepsilon_4 - \varepsilon_2)2^{a_2}.$$

(g) If $\varepsilon_1 = \varepsilon_3$ then it is clear that $x_1 = x_3$. If $\varepsilon_2 = \varepsilon_4$ then it follows that $x_2 = x_4$ and thus $x_1 = x_3$.

(h) We can suppose, without loss of generality, that $\varepsilon_1 - \varepsilon_3 > 0$. Thus, $\frac{\varepsilon_4 - \varepsilon_2}{\varepsilon_1 - \varepsilon_3} \in \{\frac{1}{2}, 1, 2\}$. So, one of the three possibilities above holds

$$2^{a_1} = 2^{a_2-1}$$
$$2^{a_1} = 2^{a_2+1}$$
$$2^{a_1} = 2^{a_2}.$$

But since $A \subset 2\mathbf{Z}$, only the last option is true, so $a_1 = a_2 = a_3 = a_4$ and $(\varepsilon_1 - \varepsilon_3)2^{a_1} = (\varepsilon_4 - \varepsilon_2)2^{a_1}$ implies that $\varepsilon_1 + \varepsilon_2 = \varepsilon_3 + \varepsilon_4$.

(i) If $x_1 \notin \{x_3, x_4\}$ then, from the previous items, it holds that $a_1 = a_2 = a_3 = a_4$. We analyse the solutions considering the possibilities for $(\varepsilon_1, \varepsilon_3)$:

$$(\varepsilon_1, \varepsilon_3) = \begin{cases} (0,1) \\ (1,0) \\ (-1,1) \\ (1,-1) \\ (-1,0) \\ (0,-1.) \end{cases}$$

- if $(\varepsilon_1, \varepsilon_3) = (0, 1)$, using the equation $\varepsilon_1 + \varepsilon_2 = \varepsilon_3 + \varepsilon_4$ we conclude that the possibilities for $(\varepsilon_2, \varepsilon_4)$ are $(1, 0)$ or $(0, -1)$. The first one would imply that $x_2 = x_4$ which cannot hold, so only the second can hold, corresponding to the element $(a, a, a + N2^{a+1}, a - N2^{a+1})$.
- if $(\varepsilon_1, \varepsilon_3) = (1, 0)$ an analogous analysis implies that the unique possibility corresponds to the element $(a + N2^{a+1}, a - N2^{a+1}, a, a)$.
- if $(\varepsilon_1, \varepsilon_3) = (-1, 1)$ then we would have $(\varepsilon_2, \varepsilon_4) = (1, -1)$, which contradicts $x_1 \neq x_4$. The case $(\varepsilon_1, \varepsilon_3) = (1, -1)$ is analogous.
- if $(\varepsilon_1, \varepsilon_3) = (-1, 0)$, then the only possibility that works for $(\varepsilon_2, \varepsilon_4)$ is $(1, 0)$, correspoding to the element $(a - N2^{a+1}, a + N2^{a+1}, a, a)$.
- if $(\varepsilon_1, \varepsilon_3) = (0, -1)$, then the only possibility that works for $(\varepsilon_2, \varepsilon_4)$ is $(0, 1)$, correspoding to the element $(a, a, a - N2^{a+1}, a + N2^{a+1})$
- From the previous items, we conclude that $2|A''|^2 - |A''| \leqslant E(A'') = 2|A''|^2 - |A''| + 4|A''|$.