Exercise sheet 1

1. (a) Give some concrete examples to show that Cauchy's Theorem does not hold for subsets of $\mathbf{Z}/q\mathbf{Z}$ in general, if $q \geqslant 1$ is arbitrary (i.e., find examples of q and A, B non-empty subsets of $\mathbf{Z}/q\mathbf{Z}$ such that $|A+B| < \min(q, |A|+|B|-1)$.)

   (b) Let $q \geqslant 1$ be a positive integer, let $A \subset \mathbf{Z}/q\mathbf{Z}$ be any subset and let $B \subset \mathbf{Z}/q\mathbf{Z}$ be such that $0 \in B$. Show that

$$|A+B| \geqslant \min(q, |A|+|B^\times|-1),$$

   where $B^\times$ is the set of elements of B which are invertible in $\mathbf{Z}/q\mathbf{Z}$ (i.e., those $b \in B$ which are residue classes of integers coprime to q).

Solutions.

(a) Let $q = 2n$ for $n \geqslant 2$, and let $A = B + \{0, 2, \ldots, 2(n-1)\}$. Observe that $A+B = A$ and $|A+B| = |A| = k$. On the other hand $|A|+|B|-1 = 2k-1$ so $|A+B| < |A|+|B|-1 < 2n$.

(b) We first observe that $A + B^\times \cup \{0\} \subset A + B$ since $B^\times \cup \{0\} \subset B$. So, it holds that $|A+B| \geqslant |A+B^\times \cup \{0\}|$ and we can suppose, without loss of generality, that $B = B^\times \cup \{0\}$.

To prove the result, we follow the outlines of Cauchy's Theorem's proof. One can assume that $A \neq \mathbf{Z}/q\mathbf{Z}$ and the result holds when $|B| = 1$. The argument follows by induction on the size of B. The key point of the proof is that for all $b_0 \in B\backslash\{0\}$ there exists $a_0 \in A$ such that $b_0 + a_0 \notin A$. If such an element a_0 didn't exist then, for all $k \in \mathbf{Z}$, it would follow that $kb_0 + a_0 \in A$. Since b_0 is invertible, any $n \in \mathbf{Z}/q\mathbf{Z}$ could be written as

$$n = (n-a_0)b_0^{-1} \cdot b_0 + a + 0,$$

which is a contradiction since $A \neq \mathbf{Z}/q\mathbf{Z}$. The rest of the proof follows as in the proof of Cauchy's Theorem.

2. Let $q \geqslant 1$ and $k \geqslant 1$ be integers. Let $A \subset \mathbf{Z}/q\mathbf{Z}$ be a non-empty set, and let $A^{(k)} = A + \cdots + A$ (with k-summands) be the set of elements of the form $a_1 + \cdots + a_k$ with $a_i \in A$. For $x \in \mathbf{Z}/q\mathbf{Z}$, define

$$r_k(x) = |\{(a_1, \ldots, a_k) \in A^k \mid a_1 + \cdots + a_k = x\}|.$$

(a) Show that

$$r_k(x) = \frac{|A|^k}{q} + \frac{1}{q} \sum_{1 \leqslant h < q} W_A(h)^k e\Big(\frac{hx}{q}\Big)$$

where

$$W_A(h) = \sum_{a \in A} e\Big(-\frac{ah}{q}\Big).$$

(b) For $k \geqslant 2$, deduce that

$$r_k(x) \geqslant \frac{|A|^k}{q} - |A| \sup_{h \neq 0} |W_A(h)|^{k-2}.$$

(c) Assume there exists $\delta > 0$ such that $|W_A(h)| \leqslant q^\delta$ for all h. Assuming $k \geqslant 2$, show that $A^{(k)} = \mathbf{Z}/q\mathbf{Z}$ if

$$|A| > q^{\frac{1+(k-2)\delta}{k-1}}.$$

Solutions.

(a) We expand $r_k(x)$ in the orthogonal character basis. Observe that

$$\begin{aligned}
< r_k, e\left(\frac{h}{q}\cdot\right) > &= \frac{1}{q} \sum_{1 \leqslant n \leqslant q} r_k(n) e\left(-\frac{hn}{q}\right) \\
&= \frac{1}{q} \sum_{1 \leqslant n \leqslant q} \sum_{\substack{(a_1,\dots,a_k) \in A^k \\ a_1 + \dots a_k = n}} e\left(-\frac{hn}{q}\right) \\
&= \frac{1}{q} \sum_{(a_1,\dots a_k) \in A^k} e\left(\frac{-h(a_1 + \ldots + a_k)}{q}\right) \cdot \sum_{\substack{1 \leqslant n \leqslant q \\ n = a_1 + \dots + a_k}} 1 \\
&= \frac{1}{q} \left(\sum_{a \in A} e\left(-\frac{ha}{q}\right) \right)^k .
\end{aligned}$$

For $h \neq 0$, the sum above is equal to $W_A(h)^k$ and for $h = 0$ it is equal to $|A|^k/q$. Thus,

$$r_k(x) = \frac{|A|^k}{q} + \frac{1}{q} \sum_{1 \leqslant h < q} W_A(h)^k e\Big(\frac{hx}{q}\Big).$$

(b) Observe that, since $k \geqslant 2$, it holds that

$$r_k(x) \geqslant \frac{|A|^k}{q} - \sup_{h \neq 0} |W_A(h)|^{k-2} \sum_{1 \leqslant h < q} |W_A(h)|^2.$$

To conclude, we observe that

$$\sum_{1\leqslant h<q} |W_A(h)|^2 \leqslant \sum_{1\leqslant h\leqslant} |W_A(h)|^2 = \sum_{1\leqslant h\leqslant q}\sum_{a,b\in A} e\left(\frac{h(b-a)}{q}\right)$$
$$\sum_{a,b\in A}\sum_{1\leqslant h\leqslant q} e\left(\frac{h(b-a)}{q}\right),$$

and the inner sum is non zero if and only if $b-a\neq 0$, so

$$\sum_{a,b\in A}\sum_{1\leqslant h\leqslant q} e\left(\frac{h(b-a)}{q}\right)\ \sum_{a\in A} q = q|A|,$$

concluding the proof.

(c) It suffices to prove that $r_k(x)>0\ \forall x\in \mathbf{Z}/q\mathbf{Z}$. From the previous items, this follows in case

$$\frac{|A|^k}{q} - |A|\sup_{h\neq 0}|W_A(h)|^{k-2} > 0 \Leftrightarrow |A|^{k-1} > q\sup_{h\neq 0}|W_A(h)|^{k-2}.$$

Since $|W_A(h)|\leqslant q^\delta$ the result holds whenenver

$$|A|^{k-1} > q^{1+(k-2)\delta},$$

which is one of the hypothesis.

3. Let p be an odd prime number, and let Q be the set of non-zero squares in $\mathbf{Z}/p\mathbf{Z}$. It has $(p-1)/2$ elements.

   (a) If $p\equiv 3 \bmod 4$, show that $Q+Q\neq \mathbf{Z}/p\mathbf{Z}$.

For $h\in\mathbf{Z}/p\mathbf{Z}$, denote

$$W(h) = \sum_{x\in Q} e\Big(\frac{hx}{p}\Big).$$

   (b) Show that

$$W(h) = \frac{1}{2}\sum_{x\in\mathbf{Z}/p\mathbf{Z}} e\Big(\frac{hx^2}{p}\Big) - \frac{1}{2}.$$

   (c) Show that

$$\Big|\sum_{x\in\mathbf{Z}/p\mathbf{Z}} e\Big(\frac{hx^2}{p}\Big)\Big|^2 = \sum_{u\in\mathbf{Z}/p\mathbf{Z}}\sum_{v\in\mathbf{Z}/p\mathbf{Z}} e\Big(\frac{huv}{p}\Big).$$

(d) Deduce that

$$|W(h)| \leqslant \frac{1}{2}(\sqrt{p}+1) \leqslant \sqrt{p}$$

for all $h \neq 0$.

Solution.

(a) We prove that if $p \equiv 3 \bmod 4$ then $0 \not\equiv x^2 + y^2 \bmod p$ for all $x, y \in \mathbf{Z}/p\mathbf{Z}$. Suppose that there are x, y such that $0 \equiv x^2 + y^2 \bmod p$. Then $(y^{-1}x)^2 \equiv -1 \bmod p$. But we can prove that such an element $w = y^{-1}x$ cannot exists. Indeed, from Fermat's Little Theorem, $w^{p-1} \equiv 1 \bmod p$. Thus

$$1 \equiv w^{p-1} \equiv (w^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \bmod p,$$

which is a contradiction.

(b) Observe that for every $y \in \mathbf{Z}/p\mathbf{Z}$ it holds that $y^2 \equiv (p-y)^2 \bmod p$ and $y \not\equiv p - y \bmod p$. On the otherhand, since $|Q| = \frac{p-1}{2}$, we get that

$$p - 1 = \sum_{x \in Q} |y \in \mathbf{Z}/p\mathbf{Z}\backslash\{0\} : y^2 = x| \geqslant 2 \cdot \frac{p-1}{2},$$

so the last inequality has to be an equality, and we conclude that running through all $x \in \mathbf{Z}/p\mathbf{Z}\backslash\{0\}$ we will obtain every $y \in Q$ exactly twice.

$$W(h) = \frac{1}{2} \sum_{x \in \mathbf{Z}/p\mathbf{Z}\backslash\{0\}} e\left(\frac{hx^2}{p}\right) = \frac{1}{2} \sum_{x \in \mathbf{Z}/p\mathbf{Z}} e\left(\frac{hx^2}{p}\right) - \frac{1}{2}.$$

(c) Observe that

$$\begin{aligned} \Big| \sum_{x \in \mathbf{Z}/p\mathbf{Z}} e\Big(\frac{hx^2}{p}\Big) \Big|^2 &= \sum_{x,y \in \mathbf{Z}/p\mathbf{Z}} e\left(\frac{h(x^2-y^2)}{p}\right) \\ & \sum_{x,y \in \mathbf{Z}/p\mathbf{Z}} e\left(\frac{h(x+y)(x-y))}{p}\right) \\ &= \sum_{u \in \mathbf{Z}/p\mathbf{Z}} \sum_{v \in \mathbf{Z}/p\mathbf{Z}} e\Big(\frac{huv}{p}\Big), \end{aligned}$$

where in the last equality we changed variables $x + y = u$ and $x - y = v$.

(d) We observe that

$$\sum_{u \in \mathbf{Z}/p\mathbf{Z}} \sum_{v \in \mathbf{Z}/p\mathbf{Z}} e\Big(\frac{huv}{p}\Big) = p,$$

since the inequality is non-zero if and only if $u = 0$ or $v = 0$. Thus, using the previous item, we conclude that

$$\Big| \sum_{x \in \mathbf{Z}/p\mathbf{Z}} e\Big(\frac{hx^2}{p}\Big) \Big| = \sqrt{p}.$$

Together with the expression in item b) and triangle inequality, we conclude the result.

4. Let $q \geqslant 1$ be an integer and let $\alpha \in]0,1[$ be a real numnber. We define a *random subset* A of $\mathbf{Z}/q\mathbf{Z}$ by the condition that each $x \in \mathbf{Z}/q\mathbf{Z}$ (independently) belongs to A with probability α.

   (a) For any subset $X \subset \mathbf{Z}/q\mathbf{Z}$, show that
   $$\mathbf{P}(A = X) = \alpha^{|X|}(1-\alpha)^{q-|X|}.$$

   (b) Show that the average of the size of A is equal to $q\alpha$, or in other words
   $$\mathbf{E}(|A|) = q\alpha.$$

   (c) For any $h \in \mathbf{Z}/q\mathbf{Z} - \{0\}$, show that
   $$\mathbf{E}\Big(\Big|\sum_{x \in A} e\Big(\frac{hx}{q}\Big)\Big|^2\Big) = q\alpha.$$

   Solution.

   (a) Let $X = \{x_1, \ldots, x_{|X|}\}$ and $\mathbf{Z}/q\mathbf{Z} \backslash X = \{y_1, \ldots y_{q-|X|}\}$ and observe that
   $$\mathbf{P}(A = X) = \prod_{i=1}^{|X|} \mathbf{P}(x_i \in X) \prod_{j=1}^{q-|X|} \mathbf{P}(y_j \in X) = \alpha^{|X|}(1-\alpha)^{q-|X|}.$$

   (b)
   $$\begin{aligned}
   \mathbf{E}(|A|) &= \sum_{i=1}^{q} i \cdot \mathbf{P}(|A| = i) = \sum_{i=1}^{q} i \sum_{\substack{X \subset \mathbf{Z}/q\mathbf{Z} \\ |X|-i}} \mathbf{P}(A = X) \\
   &= \sum_{i=1}^{q} i\alpha^1(1-\alpha)^{q-i} \sum_{\substack{X \subset \mathbf{Z}/q\mathbf{Z} \\ |X|-i}} 1 \\
   &= \sum_{i=1}^{q} i\alpha^i(1-\alpha)^{q-i}\binom{q}{i} = \sum_{i=0}^{q-1}(i+1)\alpha^{i+1}(1-\alpha)^{q-i-1}\binom{q}{i+1} \\
   &= \alpha q \sum_{i=0}^{q-1} \alpha^i(1-\alpha)^{q-1-i}\binom{q-1}{i},
   \end{aligned}$$
   and the inner sum is the binomial identity for $(\alpha + 1 - \alpha)^{q-1} = 1$.

(c)

$$\mathbf{E}\Big(\Big|\sum_{x\in A} e\Big(\frac{hx}{q}\Big)\Big|^2\Big) = \sum_{i=1}^{q} \sum_{\substack{X\subset \mathbf{Z}/q\mathbf{Z}\\ |X|=i}} \Big|\sum_{x\in X} e\Big(\frac{hx}{q}\Big)\Big|^2 \mathbf{P}(A=X)$$

$$= \sum_{i=1}^{q} \sum_{\substack{X\subset \mathbf{Z}/q\mathbf{Z}\\ |X|=i}} \alpha^i(1-\alpha)^{q-i} \sum_{x,y\in X} e\left(\frac{h(x-y)}{q}\right)$$

$$= \sum_{i=2}^{q} \alpha^i(1-\alpha)^{q-i} \sum_{x\neq y\in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{h(x-y)}{q}\right) \sum_{\substack{X\subset \mathbf{Z}/q\mathbf{Z}\\ |X|=i\\ x\neq y\in X}} 1$$

$$+ \sum_{i=1}^{q} \alpha^i(1-\alpha)^{q-i} \sum_{x\in \mathbf{Z}/q\mathbf{Z}} 1 \sum_{\substack{X\subset \mathbf{Z}/q\mathbf{Z}\\ |X|=i\\ x\in X}} 1.$$

We observe that

$$\sum_{\substack{X\subset \mathbf{Z}/q\mathbf{Z}\\ |X|=i\\ x\neq y\in X}} 1 = \binom{q-2}{i-2}$$

is independent of x, y, thus

$$\sum_{i=2}^{q} \alpha^i(1-\alpha)^{q-i} \sum_{x\neq y\in \mathbf{Z}/q\mathbf{Z}} e\left(\frac{h(x-y)}{q}\right) \sum_{\substack{X\subset \mathbf{Z}/q\mathbf{Z}\\ |X|=i\\ x\neq y\in X}} 1 = 0.$$

We conclude that

$$\mathbf{E}\Big(\Big|\sum_{x\in A} e\Big(\frac{hx}{q}\Big)\Big|^2\Big) = \sum_{i=1}^{q} \alpha^i(1-\alpha)^{q-i} \sum_{x\in \mathbf{Z}/q\mathbf{Z}} 1 \sum_{\substack{X\subset \mathbf{Z}/q\mathbf{Z}\\ |X|=i\\ x\in X}} 1$$

$$= q\sum_{i=1}^{q} \alpha^i(1-\alpha)^{q-i}\binom{q-1}{i-1}$$

$$= q\alpha \sum_{i=0}^{q-1} \alpha^i(1-\alpha)^{q-1-i}\binom{q-1}{i},$$

where the inner sum is equal to 1 because it is the binomial representation of $(\alpha+1-\alpha)^{q-1}$.