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).

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

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

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 $h \neq 0$.

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

$$\mathbf{E}\Big(\Big|\sum_{x \in A} e\Big(\frac{hx}{q}\Big)\Big|^2\Big) = q\alpha.$$