Additive Number Theory Examples Sheet 3. W. T. G.

1. (i) Deduce the following extension of Roth's theorem from Ruzsa's lemma (and Plünnecke's inequality). For every C there exists n such that, if $A \subset \mathbb{Z}$, $|A| \geqslant n$ and $|A+A| \leqslant C|A|$, then A contains an arithmetic progression of length three.

(ii) Using the Balog-Szemerédi theorem, deduce a further extension.

2. Let $A \subset \mathbb{Z}_N$. Define a k-cube in A to be a mapping $\phi : \{0,1\}^k \to \mathbb{Z}_N$ of the form $\phi(\epsilon) = x_0 + \sum_{i=1}^k \epsilon_i x_i$, where $x_0, x_1, \dots, x_k$ belong to $\mathbb{Z}_N$ and the image of ϕ lies in A. (For example, a 2-cube can be thought of as a quadruple $(a, a+b, a+c, a+b+c) \in A^4$.)

(i) Let A have size δN. Prove that A contains at least $\delta^{2^k} N^{k+1}$ k-cubes.

(ii) Suppose that A is quadratically α-uniform. Prove that A contains at most $(\delta^8 + c(\alpha))N^4$ 3-cubes, where $c(\alpha)$ tends to zero as α tends to zero.

3. Obtain a decent lower bound (without appealing to the geometry of numbers) for the size of the Bohr neighbourhood $B(r_1, \dots, r_k; \delta)$.

4. Let A be a subset of $\mathbb{Z}_N$ of cardinality δN. Prove that $A+A+A$ contains an arithmetic progression (mod N) of length N^c, where c depends on δ only. Give an example of a set A such that the longest arithmetic progression in $A+A+A$ has length $N^{c'}$ for some c' that tends to zero with δ. (You ought to be able to get c proportional to δ^2 and c' proportional to $\log(1/\delta)$. Closing the gap between these two bounds is an important open problem.)

5. (Hard - in fact, probably an unsolved problem.) Let $\epsilon > 0$, let N be prime and let A and B be subsets of $\mathbb{Z}_N$ of size $\lceil N/2 \rceil$. If N is large enough (as a function of ϵ), prove that there exists some $x \in \mathbb{Z}_N$ such that $A \cap (B+x)$ has cardinality between $(\frac{1}{4} - \epsilon)N$ and $(\frac{1}{4} + \epsilon)N$. What can go wrong if N is not prime?

6. Let f be an increasing function. Obtain an estimate for $\left|\sum_{x \leqslant n} f(x) e(\alpha x + \beta)\right|$ under the assumption that $(a,q) = 1$ and $|\alpha - a/q| \leqslant q^{-2}$.

7. By carrying out the following steps, prove that the subset $A = \{x : |x^2| \leqslant N/10000\}$ of $\mathbb{Z}_N$ discussed in lectures satisfies $\max_{r \neq 0} |\hat{A}(r)| = O(\sqrt{N} \log N)$.

(i) Prove that if $f(x) = \omega^{ax^2}$ then $|\hat{f}(r)| = \sqrt{N}$ for every r.

(ii) Set $M = \lfloor N/10000 \rfloor$, let $I = [-M, M]$ and notice that $A(x) = I(x^2)$ for every x. Use the inversion formula to write an expression for $A(x)$ in terms of the Fourier coefficients of I.

(iii) Finish off by using (i) and a simple estimate for the sizes of the Fourier coefficients of I.

8. Prove also that A contains significantly more than $10^{-16}N^2$ arithmetic progressions (in $\mathbb{Z}_N$) of length four. (You should find 7(ii) helpful here as well.)

9. Let A be a subset of $I = \{x \in \mathbb{Z} : |x| \leqslant n\}$ of cardinality δN. Prove that there is a constant k, depending on δ only, such that $kA - kA$ contains the whole of I. (I'm not quite sure how to do this question but I know it's known.)

10. Show that there are constants $0 < \beta < \alpha^3 \leqslant 1$ such that, for infinitely many N, $\mathbb{Z}_N$ contains a set of size αN with at most βN^2 triples of the form $(a, a+d, a+2d) \pmod N$.

11. Let $A \subset \mathbb{N}$. Suppose that

$$\forall \alpha \in \mathbb{R}\ \forall \epsilon > 0\ \exists q \in A\ \|q\alpha\| \leqslant \epsilon\ .$$

Prove that

$$\forall \epsilon > 0\ \exists N \in \mathbb{N}\ \forall \alpha \in \mathbb{R}\ \exists q \leqslant N\ \|q\alpha\| \leqslant \epsilon\ .$$

(That is, obtain a result which is uniform over α.)