Additive Number Theory Examples Sheet 2. W. T. G.

1. Let k be a real number. Prove that there exist an integer N and a subset $A \subset \mathbb{Z}_N$ of size δN (say) such that $|\hat{A}(r)| \leqslant \delta N/k$ whenever $r \neq 0$, and such that the convolution $A * A$ is not approximately constant. (This means that there is some absolute constant $\eta > 0$ such that $|A * A(x) - \delta^2 N| \geqslant \eta\delta^2 N$ for at least ηN values of x.) What relationship must hold between k and δ for this to be possible?

2. Let $B = \{e_1, \ldots, e_m\}$ be a basis for an m-dimensional vector space. Prove that $|nB| = \binom{m+n-1}{n}$.

3. Let G be a Plünnecke graph with vertex set $V_0 \cup V_1 \cup \ldots \cup V_n$. Suppose that $|V_0| = 1$, $|V_1| = m$ and that the vertex in V_0 is joined to every vertex in V_1. Assume first that $n = 2$, and prove that $|V_n| \leqslant \binom{m+n-1}{n}$, with equality if and only if G is isomorphic to the graph defined in lectures with vertex set $\{0\} \cup B \cup \ldots \cup nB$. Is this result true for $n > 2$? [I have only recently thought of this question and do not know the answer to the last part. If the answer is yes then it seems hardish but shouldn't be impossible.]

4. Let Λ be a lattice, let K be a centrally symmetric convex body and let $\lambda_1, \ldots, \lambda_n$ be the successive minima of K with respect to Λ. Is it necessarily possible to choose a basis $b_1, \ldots, b_n$ of Λ (as opposed to $\mathbb{R}^n$) such that $b_i \in \lambda_i \overline{K}$ for every i?

5. In the proof of Minkowski's second theorem, why would it not be possible to replace the map ϕ by the simpler map $\sum_{i=1}^n x_i b_i \mapsto \sum_{i=1}^n \lambda_i x_i b_i$?

6. Let Λ be a lattice and let K be a centrally symmetric convex body. Define a *grid* to be a set of the form $\{\sum_{i=1}^n a_i x_i : r_i \leqslant a_i \leqslant s_i\}$, where $x_1, \ldots, x_n$ are independent vectors in Λ. Prove that K contains a grid of cardinality $c|K|/\det\Lambda$, where c is a constant depending on n only, and $|K|$ stands for the volume of K.

7. Let $G \subset \mathbb{R}^n$ be a discrete subgroup (meaning that there is a neighbourhood of zero with no non-zero point of G in it) containing n linearly independent vectors. Prove that G is a lattice. Prove the converse (which is easier).

8. Let P be the arithmetic progression $(a, a+d, \ldots, a+(m-1)d)$. Map P to $\mathbb{Z}$ as follows. First multiply everything by r. Then map to $\mathbb{Z}_N$ via the usual quotient map from $\mathbb{Z}$, where $N > m^2$ (this condition is not very important) is prime and r is not a multiple of N. Finally, embed into $\mathbb{Z}$ in the usual way. Show that the image of P under this map is contained in a two-dimensional arithmetic progression of size at most $C|P|$, where C is an absolute constant.

9. (Easier Waring's problem.) Prove that for every k there is a constant $C = C(k)$ such that every integer can be written as $\pm x_1^k \pm \ldots \pm x_m^k$ with $m \leqslant C$. [Hint: think about the proof of Weyl's inequality.]

10. A set A of integers is called a *Sidon set* if no integer can be written in more than one way as $a + b$ with $a, b \in A$, $a \leqslant b$. Show that there is a constant $c > 0$ such that, for every N, the set $\{1, 2, \ldots, N\}$ has a subset of size at least $c\sqrt{N}$ which is a Sidon set. [Hint: consider the set of points of the form (x, x^2) in $\mathbb{Z}_p^2$.]

11. Show that for every C there is a centrally symmetric convex body in $\mathbb{R}^2$ of area at least $1/100$ and diameter at least C which contains no non-zero points in $\mathbb{Z}^2$.

12. Check the following simple facts, some of which I assumed in lectures.

(i) For every pair of positive integers k and d, every finite subset of $\mathbb{Z}^d$ is isomorphic of order k to a subset of $\mathbb{Z}$.

(ii) The composition of two homomorphisms/isomorphisms of order k is a homomorphism/isomorphism of order k.

(iii) $\phi : A \to B$ is an isomorphism of order k if and only if ϕ induces a bijection (in the obvious way) between kA and kB.

(iv) If $I = \{x \in \mathbb{Z}_p : (j-1)p/k \leqslant x < jp/k\}$, then the "identity map" from I to $\mathbb{Z}$ is an isomorphism of order k.

(v) If A is a d-dimensional arithmetic progression and B is isomorphic (of order 2) to A, then B is a d-dimensional arithmetic progression.

(vi) If A and B are finite subsets of $\mathbb{Z}$ and A is isomorphic of order k to B for every k, then there exist integers $a \neq 0$ and b such that the map $x \mapsto ax + b$ is a bijection from A to B.

(vii) If A is isomorphic of order rs to B and $k + l = r$, then $kA - lA$ is isomorphic of order s to $kB - lB$.

(viii) If A is a proper d-dimensional arithmetic progression, then $|rA - sA| \leqslant (r + s)^d |A|$.

(ix) If A is a proper d-dimensional arithmetic progression, then $A - A$ is contained in a union of 2^d translates of A.

(x) A d-dimensional arithmetic progression of cardinality n contains a one-dimensional arithmetic progression of cardinality at least $n^{1/d}$.

13. Disprove the following statement. There exists an absolute constant B such that, whenever A is a finite subset of $\mathbb{Z}$ with $|A + A| \leqslant C|A|$, we also have $|A - A| \leqslant BC|A|$. [I

think it is possible to prove an upper bound of the form $C^\alpha|A|$ for some $\alpha < 2$, but this is quite a bit harder.]

14. Prove that if $B \subset \{1, 2, \ldots, n\}$ is a set of cardinality at least $99n/100$ and $\phi : B \to \mathbb{Z}$ is a homomorphism, then ϕ is an affine map.

15. Let X be a subset of size n of an abelian group G. Suppose that X^4 contains at least $99n^3/100$ quadruples (a, b, c, d) such that $a + b = c + d$. Prove that X is contained in a coset of a subgroup of G of size at most $11n/10$. (These numbers are off the top of my head, and therefore unnecessarily generous.)

16. For the following two unitary maps from $\mathbb{C}^{\mathbb{Z}_N}$ to $\mathbb{C}^{\mathbb{Z}_N}$, find an orthonormal basis of eigenvectors and calculate the corresponding eigenvalues.

(i) $f \mapsto g$, where $g(x) = f(x - 1)$.

(ii) $f \mapsto N^{-1/2}\hat{f}$.

Comments/corrections to wtg10@dpmms.