Additive Number Theory Exercises 1.

1. Without giving full details, explain why in the first proof of the Hales-Jewett theorem it is in fact enough to find $y_1, \ldots, y_r$ and $A_1, \ldots, A_r$ with the following property: the colours of $(y_1 \oplus j_1 A_1, \ldots, y_r \oplus j_r A_r)$ and $(y_1 \oplus j_1' A_1, \ldots, y_r \oplus j_r' A_r)$ are equal whenever there exists t such that $j_i = j_i'$ for all $i < t$, j_t and j_t' are both less than k and $j_i = j_i' < k$ for all $i > t$. What effect does incorporating this observation have on the sequence $N_1, \ldots, N_r$?

2. (Not quite the usual proof of Ramsey's theorem.) Let κ be an r-colouring of $\mathbb{N}^{(k)}$, the set of all subsets of $\mathbb{N}$ of size k. Show how to pass to a subset X of $\mathbb{N}$ such that two subsets $A, B \subset X$ of size k have the same colour whenever their first $k-1$ elements are the same. Use this to prove Ramsey's theorem (that there is a subset Y of $\mathbb{N}$ such that all its subsets of size k have the same colour).

3. The Ackermann function is defined inductively by $A(1, n) = 2 + n$, $A(n, 1) = 2$ and $A(n, r) = A(n-1, A(n, r-1))$. Show that the bound for $HJ(k, 2)$ obtained in the first proof is comparable to $A(n, n)$, in the sense of being bounded above by a function of similar type. Show that the bound obtained by Shelah is comparable to $A(5, n)$. (I sketched these results in lectures.)

4. Give an explicit n for which you can prove (combinatorially) that if the set $\{1, 2, \ldots, n\}$ is coloured with three colours, then there is a monochromatic arithmetic progression of length three.

5. A subset A of $\mathbb{N}$ is called a *multiplicative basis of order* d if every $n \in A$ is the product of at most k elements of A. Show that if A is a multiplicative basis of order $d \geqslant 2$ then for every k there is an integer that can be written as a product of at most d elements of A in at least k different ways. (The corresponding question with multiplication replaced by addition is a well known open problem of Erdős.)

6. Prove that the following are equivalent, for a subset $A \subset \mathbb{Z}_N$:

(i) $|\hat{A}(r)| \geqslant c_1 N$ for some non-zero r;

(ii) there exists a mod-N arithmetic progression P of cardinality $\lfloor N/2 \rfloor$ such that $2|A \cap P| - |A| \geqslant c_2 N$.

What relationship is there, if any, between r and the common difference of the progression P? (By "equivalent" above, I mean that, given c_1, you can find a c_2 that works, and vice versa - but don't expect to recover your original c_1 if you follow the implication from (i) to (ii) and back again.)

7. Prove that for every lacunary sequence (n_k) there exist $\theta \in \mathbb{R}$ and $\epsilon > 0$ such that

$\|\theta n_k\| \geqslant \epsilon$ for every k. (A sequence (n_k) is *lacunary* if there exists $\alpha > 1$ such that $n_{k+1} \geqslant \alpha n_k$ for every k. This is a hard question, but if you can't do it as written, try it for $\alpha > 2$.)

8. Let A, B, C, D be four subsets of $\mathbb{Z}$ of size N. Suppose that there are αN^3 quadruples $(a, b, c, d) \in A \times B \times C \times D$ such that $a + b = c + d$. Prove that there are at least αN^3 quadruples (a, b, c, d) in A^4 with $a + b = c + d$.

9. Suppose A has size N and contains at least αN^2 arithmetic progressions of length three. Prove that there are at least αN^3 quadruples (a, b, c, d) in A^4 with $a + b = c + d$.

10. Show that there exists an absolute constant $c > 0$ with the following property. For every $a, b, c \in \mathbb{Z}_N$ there are $a', b', c' \in \mathbb{Z}_N$ such that $|a - a'|, |b - b'|$ and $|c - c'|$ are all at most N^{1-c} and $a'b' = c'$. (In other words, solutions of $xy = z$ are in some sense "dense" in $\mathbb{Z}_N^3$.)

11. What about solving $a'b' = c$? (I don't expect you to be able to solve this yet, though it's not impossible, but if you think about it now, you should be able to understand what is needed, and therefore properly appreciate a result that I hope to prove later in the course.)

12. Prove that there is an absolute constant C such that for every k, every N is the sum of at most $Ck \log \log N$ non-negative k^{th} powers.

13. (Random sets have small Fourier coefficients.) Choose a subset A of $\mathbb{Z}_N$ randomly by letting $x \in A$ with probability p, with all these events independent. Obtain an estimate for the largest value of $|\hat{A}(r)|$ with $r \neq 0$. (Technical hint: it is much easier first to replace A by the function $f(x) = A(x) - p$, so that expectation of $f(x)$ is zero, and to calculate $\sum_r |\hat{f}(r)|^4$.) Deduce that there exists a set A of cardinality between $N/4$ and $3N/4$ such that all $|\hat{A}(r)|$ are at most $C\sqrt{N}^{3/4}$, when $r \neq 0$. Obtain a lower bound for the size of the largest non-zero Fourier coefficient of such a set.

14. A standard result from probabilistic combinatorics implies that if $X_1, \ldots, X_N$ are independent random variables with mean zero and if their values are never more than 1 in modulus, then the probability that $|X_1 + \ldots + X_N| \geqslant t\sqrt{N}$ is at most $\exp(-ct^2)$ for some absolute constant $c > 0$. Use this result to improve the upper bound of the previous question to $C\sqrt{N \log N}$.

15. Let A be a subset of $\mathbb{Z}_N$ of size at most $(1/20) \log N$. Prove that there exists $r \neq 0$ such that $|\hat{A}(r)| \geqslant |A|/2$.

16. Convince yourself of the following extension to Roth's theorem. Let $a_1 + \ldots + a_k = 0$. Then for every $\delta > 0$ there exists N such that every set $A \subset [N]$ of cardinality at least δN

contains elements $x_1, \ldots, x_k$ not all equal such that $a_1x_1 + \ldots + a_kx_k = 0$. (I don't advise writing out the proof in full as it's similar to Roth's theorem.)