Solutions to Homework 3

Q.1. We show that $\mathcal{L}$ is c-irregular. It's a standard argument for making the jump from finite to infinite sets, which often goes by the name of a *compactness argument*. The only drawback is that it doesn't provide an 'explicit' c-coloring of $\mathbb{N}$.

Fix a choice of c colors and a c-coloring χ_n of $\{1, ..., n\}$ for every n, such that each χ_n avoids monochromatic non-trivial solutions to $\mathcal{L}$. We explain how a c-coloring χ of $\mathbb{N}$ may be constructed which does the job.

Since there are only finitely many colors, there must be an infinite subsequence $S_1 = (\chi_{n_i})_{i=1}^{\infty}$ each of which color the number 1 in the same color, say c_1. Choose any such infinite subsequence and set $\chi(1) = c_1$. Next, there must exist an infinite subsequence S_2 of S_1 s.t. each of the colorings in this sequence color 2 in the same color, say c_2. Put $\chi(2) = c_2$. We can continue indefinitely in this manner, and the resulting c-coloring χ of $\mathbb{N}$ will avoid monochromatic non-trivial solutions to $\mathcal{L}$.

Q.2. Let the colors be red, blue and green. Each $n \in \mathbb{N}$ can be written uniquely as $n = 2^{a_n} \cdot u$, where a_n is a non-negative integer and u is odd. Now color as follows:

Color the integer n red if $a_n \equiv 0 \pmod 3$, color n blue if $a_n \equiv 1 \pmod 3$ and color n green if $a_n \equiv 2 \pmod 3$.
It is easy to check that there will be no monochromatic solutions to $4x = 2y + z$.

Q.3 (i) First suppsoe A is skinny of order h. This means there exists a constant $C > 0$ such that $r_{A,h}(n) \leq C$ for all $n \in \mathbb{N}$. Now fix any $n \in \mathbb{N}$ and consider

$$S = S(n) := \sum_{t=1}^{hn} r_{A,h}(t).$$

On the one hand, skinnyness implies that this sum cannot exceed Chn. On the other hand, the sum is at least equal to the total number of unordered h-tuples $\{a_1, ..., a_h\}$ of elements of $A \cap \{1, ..., n\}$. Letting $A(n) := |A \cap \{1, ..., n\}|$, it follows from Lemma 17.3 in the lecture notes that

$$\binom{A(n) + h - 1}{h} \leq Chn.$$

Letting $n \to \infty$, it follows that

$$\limsup_{n\to\infty} \frac{A(n)}{n^{1/h}} \leq (Chh!)^{1/h},$$

which proves that A is thin.

(ii) I claim that none of the bases discussed in the Example after Theorem 17.5 are skinny. Fix $h \geq 2$ and consider the basis $A = \sqcup_{i=0}^{h-1} A_h$ of the Example. Let $n \in \mathbb{N}$ and let

$$x = x(n) = x_{nh-1} \cdots x_1 x_0$$

be the number consisting of nh binary digits, which is defined by setting

$$x_i = 1 \Leftrightarrow i \equiv -1 (\text{mod } h).$$

The number $x(n)$ has a total of n ones, and hence there are $f(n, h)$ ways to write it a sum $y_1 + \cdots + y_h = x(n)$ of h elements of A_{h-1}, where $f(n, h)$ is the number of unordered partitions $\{S_1, ..., S_h\}$ of $\{1, ..., n\}$ into h non-empty subsets. Here the sets in a partition correspond to the locations of the ones in $y_1, ..., y_h$.

Hence $r_{A,h}(x(n)) \geq f(n, h)$, and since it is clear that the function $f(n, h)$ goes to infinity with n, it follows that the basis A is not skinny.

Q.4. See the solution to Q.6 on the exam from 180811.

Q.5. For references and a proof of a much more general result, see Paper No. 23 on my research homepage.

Q.6 (i) This result was originally proven in the following paper :

P. ERDŐS AND R. GRAHAM, On bases with an exact order, *Acta Arith.* **37** (1980), 201-207.

(ii) Let A be an asymptotic basis. Suppose it contains infinitely many essential elements, written in increasing order as $e_1 < e_2 < \cdots$. For each i, let t_i be the smallest modulus of a non-trivial arithmetic progression containing $A \backslash \{e_i\}$. Hence $t_i > 1$ for each i. More importantly, note that the numbers t_i must be distinct. Now let $n \in \mathbb{N}$. Then $A \backslash \{e_1, ..., e_n\}$ is contained inside an arithmetic progression of modulus T_n, where $T_n = \text{LCM}\{t_i : 1 \leq i \leq n\}$. Since the numbers t_i are distinct, one has $d(T_n) \geq n$. But recall from Exercise 9 on Homework 1 that, for any $\epsilon > 0$, $d(T_n) = O(T_n^{\epsilon})$. Hence, $T_n = \Omega(n^{1/\epsilon})$ for any $\epsilon > 0$. Now suppose A is an asymptotic basis of order h. Then the numers $e_1, ..., e_n$ must form a basis for $\mathbb{Z}/T_n\mathbb{Z}$. But this is a priori only possible if $T_n = O(n^h)$. Hence, we get a contradiction by choosing $\epsilon < 1/h$.

(iii) Let $p_1 < p_2 < \cdots$ be the sequence of primes, written in increasing order. For each $k \geq 1$, let

$$P_k := \prod_{i=1}^{k} p_i$$

and for each $i = 1, ..., k$ set

$$q_{i,k} := \frac{P_k}{p_i}.$$

Fix k, and let A consist of all multiples of P_k, together with each of the numbers $q_{i,k}$, $i = 1, ..., k$. Then A is an asymptotic basis of order at most P_k, and it has exactly k essential elements, namely each of the numbers $q_{i,k}$.

(iv) The upper bound is also proven in the paper of Erdős and Graham referred to above. For the lower bound, let n be a 'large' positive integer and let a be the largest integer strictly less than $\sqrt{n}$ which is relatively prime to n. Let A be the subset of $\mathbb{N}_0$ consisting of zero, together with all positive integers which are congruent to either 1 or a (mod n). The order of A as an asymptotic basis for $\mathbb{N}$ equals that of the set $\{0, 1, a\}$ as a basis for $\mathbb{Z}/n\mathbb{Z}$. Similarly, if we let $B = A \backslash \{0\}$, then the order of B as an asymptotic basis equals that of $\{1, a\}$ as a basis for $\mathbb{Z}/n\mathbb{Z}$. Provided GCD$(a, n) = 1$, the order of B is exactly $n - 1$, for in that case if x_1, x_2, x_3, x_4 are non-negative integers satisfying $x_1 + x_2 = x_3 + x_4 = n - 1$, then $x_1 + x_2 a \equiv x_3 + x_4 a \pmod{n}$ if and only if $x_1 = x_3$ and $x_2 = x_4$. Since there are n solutions to the equation $x_1 + x_2 = n - 1$ in non-negative integers, it follows that all n congruence classes modulo n will be representable as $x_1 + x_2 a$, for some such pair (x_1, x_2).

Now consider A instead. Suppose $a = (1 - \epsilon)\sqrt{n}$. Then it is easy to see that there is an absolute constant $C > 0$ such that every number from 0 up to $n - 1$ can be written as $x_0 \cdot 0 + x_1 \cdot 1 + x_2 \cdot a$, where x_0, x_1, x_2 are non-negative integers such that $x_0 + x_1 + x_2 \leq (2 + C\epsilon)\sqrt{n}$. Hence the order of A, as an asymptotic basis, is at most $(2 + C\epsilon)\sqrt{n}$.

To summarise, we have shown that there is an absolute constant $C > 0$ such that, for all sufficiently large integers n, the following holds : There exists an asymptotic basis A_n, containing zero, of order less than $(2 + C\epsilon_n)\sqrt{n}$, where $a_n = (1 - \epsilon_n)\sqrt{n}$ is the largest integer up to $\sqrt{n}$ which is relatively prime to n, such that $A_n \backslash \{0\}$ is an asymptotic basis of order $n - 1$.

In particular, if n is prime for example, then $\epsilon_n \to 0$ as $n \to \infty$. This already implies that

$$\limsup_{h\to\infty} \frac{X(h)}{h^2/4} \geq 1.$$

To deduce that the same is true of the liminf can be accomplished by a suitable 'interpolation'. For example, one can show that for all sufficiently large h, one can find an n for which the basis A_n has order exactly h. I will leave further details to the reader.

Q.7 (i) If $|A| = n$ then

$$2n - 1 \leq |A - A| \leq n(n-1) + 1.$$

The upper bound is just one plus the number of ordered pairs of distinct elements of A. Since subtraction is non-commutative we need to consider ordered pairs, and the 'plus one' comes from the fact that $0 = a - a$ for any $a \in A$. For the lower bound, we just need to exhibit $2n-1$ distinct elements of $A - A$. If $A = \{a_1 < a_2 < \cdots < a_n\}$, then $\{\pm(a_i - a_1) : i = 1, ..., n\}$ froms such a collection of $2n - 1$ distinct elements of $A - A$.

(REMARK: In a similar manner to Q.9(i) below, one may also show that $|A - A| = 2n - 1$ if and only if A is an arithmetic progression).

(ii) The smallest such set has 8 elements, and it is unique up to affine transformation $x \mapsto ax+b,\ a, b \in \mathbb{Z}$. For example, $A = \{0, 2, 3, 4, 7, 11, 12, 14\}$ works. For further examples, see Paper No. 24 on my research homepage.

(iii) Let $a_1 + a_2 \in A + A$. There exists $a_3 \in A$ such that $a_2 = x - a_3$, hence $(a_1 + a_2) - x = (a_1 - a_3)$. Conversely, let $a_1 - a_2 \in A - A$. Then $a_1 - a_2 = (a_1 + a_3) - x$. The point is that there is a 1-1 correspondence between the elements of the sets $A - A$ and $(A + A) - \{x\}$. Thus, both sets have the same size and hence $|A + A| = |A - A|$.

(iv) Write the elements of A in increasing order, $A = \{a_1 < a_2 < \cdots < a_n\}$. Then $A \hat{+} A$ contains neither $a_1 + a_1$ nor $a_n + a_n$.

(v) By part **(iv)** it suffices to show that $|B + B| \leq |B - B| + 1$. Let y be such that $A = \{y\} - A$. Then

$$\begin{aligned} B + B = (A \cup \{x\}) + (A \cup \{x\}) &= (A + A) \cup (\{x\} + A) \cup \{2x\} = \\ &= [A + (\{y\} - A)] \cup [\{x\} + (\{y\} - A)] \cup \{2x\} = \\ = [\{y\} + [(A - A) \cup (\{x\} - A)]] \cup \{2x\} &\subseteq [\{y\} + (B - B)] \cup \{2x\}, \end{aligned}$$

which proves that $|B + B| \leq |B - B| + 1$.

(vi) This is first proven in the following paper:

G. MARTIN AND K. O'BRYANT, Many sets have more sums than differences. *Additive Combinatorics*, 287-305, CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI (2007).

A more general result is proven in Theorem 8 of Paper No. 24 on my homepage.

Q.8. It suffices to show that, for any $\epsilon > 0$, as $k \to \infty$ the number of integer solutions to $x^2 - y^2 = k$ is $O(k^\epsilon)$. Now we can factorise a difference of two squares, $x^2 - y^2 = (x+y)(x-y)$. It follows that there is a 2-1 correspondence between integer solutions to $x^2 - y^2 = k$ and integer factorisations $k = a \cdot b$. Indeed the correspondence is given by $x = (a \pm b)/2$, $y = (a \mp b)/2$. Now the number of such factorsations is just $2\tau(k)$, the factor two coming from the fact that we allow both positive and negative integer factorisations. As shown in Exercise 7 of Homework 1, one has $\tau(k) = O(k^\epsilon)$, for any $\epsilon > 0$. This completes the proof.

Q.9 (i) Write $A = \{a_1 < a_2 < \cdots < a_k\}$. If $k \leq 2$ then A is a priori an AP, so suppose $k \geq 3$. The following is an increasing sequence of $2k-1$ distinct elements of $A + A$:

$$2a_1 < a_1 + a_2 < 2a_2 < a_2 + a_3 < \cdots < 2a_{k-1} < a_{k-1} + a_k < 2a_k. \quad (1)$$

Next, for any i, one has

$$a_i + a_{i+1} < a_i + a_{i+2} < a_{i+1} + a_{i+2}. \quad (2)$$

Suppose there exists an i, with $1 \leq i \leq k-2$, such that

$$a_{i+2} - a_{i+1} \neq a_{i+1} - a_i. \quad (3)$$

In that case, $a_i + a_{i+2} \neq 2a_{i+1}$, so from (2) it follows that $a_i + a_{i+2}$ would be an element of $A + A$ not appearing in the sequence (1). Since $|A| = 2k-1$, it follows that (3) doesn't hold for any i and hence A is an AP.

(ii) This is a special case of the following theorem of Freiman:

Let A be a set of integers with $|A| = k \geq 3$. If $|2A| = (2k-1)+b \leq 3k-4$, then A is a subset of an arithmetic progression of length $k+b \leq 2k-3$.

For a proof, see Chapter 1 of the following book (which is in Chalmers library):

M.B. NATHANSON, Additive Number Theory : Inverse Problems and the Geometry of Sumsets, *Graduate Texts in Mathematics* **165**, Springer (1996).

Q.10. Such sets exist, for example the set $A_c = \{c^{-n} : n \in \mathbb{N}_0\}$, for any $c > 2$. Every infinite subset sum converges and it is easy to see that all subset sums, whether finite or infinite, are distinct, provided $c > 2$.

Q.11. See the attached scan of the proof reproduced from the book *The Probabilistic Method*, by Alon and Spencer.