C3.10 Additive and Combinatorial Number Theory, Hilary 2020 Exercises 4

Comment. This sheet is loosely based around proving the following result of Furstenberg and Sárközy.

Theorem 1. Let $\alpha > 0$. Suppose that $N > N_0(\alpha)$. Then any set $A \subset [N]$ with $|A| \geqslant \alpha N$ contains two different elements a, a' differing by a square.

I have divided the proof of the theorem up into exercises which all have something to do with other parts of the course, and which can hopefully be attempted more-or-less independently of one another. As the main purpose of this sheet is to practice technique, there is some redundancy.

The first set of questions concern the following theorem.

Theorem 2. We have

$$\lim_{N\to\infty} \sup_{\theta\in\mathbb{R}} \inf_{1\leqslant n\leqslant N} \|n^2\theta\|_{\mathbb{R}/\mathbb{Z}} = 0.$$

Statements like this are a little hard to parse, so let us reflect on the meaning: given $\theta \in \mathbb{R}$ and $\varepsilon > 0$, we can find $n \leqslant O_\varepsilon(1)$ such that $\|n^2\theta\|_{\mathbb{R}/\mathbb{Z}} \leqslant \varepsilon$, where the $O_\varepsilon(1)$ is uniform in θ.

Question 1. By considering sets of the form $\{n : \frac{n^2\theta}{2} (\mathrm{mod}\, 1) \in I\}$ for appropriate intervals I, deduce the theorem from Roth's theorem.

Solution 1. Let $\alpha = 1/M$ for some integer M. By the pigeonhole principle there is some interval I of length α such that there are at least αN values of $n \leqslant N$ such that $n^2\theta/2 \in I$. By Roth's theorem, if n is large enough in terms of α then this set contains three elements $n, n+d, n+2d$ in arithmetic progression, thus

$$\frac{n^2\theta}{2}, \frac{(n+d)^2\theta}{2}, \frac{(n+2d)^2\theta}{2} \in I.$$

But then

$$d^2\theta = \frac{n^2\theta}{2} - 2\frac{(n+d)^2\theta}{2} + \frac{(n+2d)^2\theta}{2} \in I - 2I + I = [-2\alpha, 2\alpha].$$

Since α can be made arbitrarily small, the result follows. $\square$

If $f : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ is an integrable function, we define the Fourier transform

$$\hat{f}(m) := \int_0^1 f(\theta)e(-\theta m).$$

In the next question, and in Question 4, $\varepsilon > 0$ is fixed and the dependence of implied constants on ε is not indicated.

Question 2. By considering the convolution of $1_{[-\varepsilon/2,\varepsilon/2]}$ with itself, show that there is a function $\psi : \mathbb{R}/\mathbb{Z} \to [0, \infty)$ with the following properties:

- ψ is supported on $[-\varepsilon, \varepsilon]$;
- $\hat{\psi}(0) = \int \psi = 1$;
- $\sum_{m\in\mathbb{Z}} |\hat{\psi}(m)| < \infty$.

Solution 2. Set

$$\psi(x) = f * f(x),$$

where $f(x) = \varepsilon^{-1} 1_{[-\varepsilon/2,\varepsilon/2]}(x)$.

Then

$$\mathrm{Supp}(\psi) \subset \mathrm{Supp}(f) + \mathrm{Supp}(f) = [-\varepsilon/2, \varepsilon/2] + [-\varepsilon/2, \varepsilon/2] = [-\varepsilon, \varepsilon],$$

and

$$\int \psi = (\int f)^2 = 1.$$

Now

$$|\hat{f}(m)| = |\frac{1}{2\pi i m\varepsilon}(e^{i\pi m\varepsilon} - e^{-i\pi m\varepsilon})| \ll_\varepsilon \frac{1}{|m|}$$

and so

$$|\hat{\psi}(m)| = |\hat{f}(m)|^2 \ll_\varepsilon \frac{1}{|m|^2},$$

so indeed

$$\sum_m |\hat{\psi}(m)| < \infty.$$

□

Question 3. With ψ as in Q2, prove the *inversion formula*

$$\psi(\theta) = \sum_m \hat{\psi}(m) e(\theta m).$$

(*You may use the uniqueness property of Fourier series in the following form: if $f : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ is continuous and if $\hat{f}(n) = 0$ for all n, then f is identically zero.*) Deduce that $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Solution 3. Define

$$\phi(\theta) := \sum_m \hat{\psi}(m) e(\theta m);$$

thus the aim is to show that $\phi = \psi$. Now since $\sum_m |\hat{\psi}(m)| < \infty$, we may evaluate $\hat{\phi}(m)$ by integrating term-by-term:

$$\begin{aligned}\hat{\phi}(n) &= \sum_m \hat{\psi}(m) \int_0^1 e(\theta(m-n)) d\theta \\ &= \hat{\psi}(n).\end{aligned}$$

Note also that ϕ is continuous, being a uniform limit of continuous functions (again because $\sum_m |\hat{\psi}(m)| < \infty$). Thus, if we define $f(\theta) := (\psi - \phi)(\theta)$, we have $\hat{f}(n) = 0$ for all $n \in \mathbb{Z}$. Moreover, f is continuous since both ψ and ϕ are (the latter by another application of the fact that $\sum_m |\hat{\psi}(m)| < \infty$), and so we may invoke uniqueness of Fourier series.

For the second part, take $\varepsilon = \frac{1}{2}$. Note that $(e^{i\pi m/2} - e^{-i\pi m/2})^2 = -4 \cdot 1_{m \,\mathrm{odd}}$, and so in this case

$$\hat{\psi}(m) = \frac{4}{\pi^2 m^2} 1_{m \,\mathrm{odd}} \tag{1}$$

for $m \neq 0$ by the computation from Question 2. By the inversion formula,

$$2 = \frac{1}{\varepsilon} = \psi(0) = \sum_{m \in \mathbb{Z}} \hat{\psi}(m)$$

Since $\hat{\psi}(0) = \int \psi = 1$, we see that

$$\sum_{m \neq 0} \hat{\psi}(m) = 1,$$

and so from (1)

$$\sum_{m \in \mathbb{Z}, m \,\mathrm{odd}} \frac{1}{m^2} = \frac{\pi^2}{4}.$$

Thus

$$\sum_{m \in \mathbb{N}, m \,\mathrm{odd}} \frac{1}{m^2} = \frac{\pi^2}{8}.$$

Finally,

$$\sum_{m \in \mathbb{N}} \frac{1}{m^2} = (1 + \frac{1}{2^2} + \frac{1}{2^4} + \frac{1}{2^6} + \cdots) \sum_{m \in \mathbb{N}, m \,\mathrm{odd}} \frac{1}{m^2} = \frac{\pi^2}{6}.$$

Question 4. Suppose that there is no $n \leqslant N$ such that $\|n^2\theta\|_{\mathbb{R}/\mathbb{Z}} \leqslant \varepsilon$.

(i) Using the result of Question 2, or otherwise, show that there is some $m = O(1)$, $m \neq 0$, such that

$$|\sum_{n \leqslant N} e(m\theta n^2)| \gg N.$$

(the implied constants here should be uniform in θ).

(ii) Using an appropriate result from the course, show that there is some nonzero $q = O(1)$ such that $\|q\theta\|_{\mathbb{R}/\mathbb{Z}} \ll N^{-2}$.

(iii) Give a second proof of Theorem 1.

Solution 4. (i) If there is no $n \leqslant N$ such that $\|n^2\theta\|_{\mathbb{R}/\mathbb{Z}}$ then

$$\sum_{n=1}^{N} \psi(n^2\theta) = 0.$$

Expanding into Fourier (as justified by the inversion formula and/or the solution to Question 3) it follows that

$$\sum_{m \in \mathbb{Z}} \hat{\psi}(m) \sum_{n=1}^{N} e(mn^2\theta) = 0,$$

the interchange in the order of summation and integration being justified by the fact that the sum over m is absolutely convergent. The contribution from $m = 0$ is N, and so

$$\sum_{m \in \mathbb{Z}\setminus\{0\}} |\hat{\psi}(m)|| \sum_{n \leqslant N} e(m\theta n^2)| \geqslant N.$$

Pick M such that $\sum_{|m|>M} |\hat{\psi}(m)| < \frac{1}{2}$ (such an M could be found completely explicitly using the estimates of Q 2, if desired). Then

$$\sum_{0<|m|\leqslant M} |\hat{\psi}(m)|| \sum_{n \leqslant N} e(m\theta n^2)| \geqslant N/2.$$

Since $|\hat{\psi}(m)| \leqslant \int \psi = 1$ for all m, it follows from the pigeonhole principle that there is some m, $0 < |m| < M$, such that

$$| \sum_{n \leqslant N} e(m\theta n^2)| \geqslant N/2M.$$

(ii) We may suppose that N is sufficiently large, the result being true trivially for $N = O(1)$ (by massaging the $\ll$ term). We will use the Weyl-type inequality, Proposition 4.3.1 in the notes. Applied here (with $L = N$, and $\delta = 1/2M \gg 1$), this states that if N is sufficiently large then there is some $q = O(1)$ such that $\|qm\theta\|_{\mathbb{R}/\mathbb{Z}} \ll N^{-2}$. Redefining q to be qm (and noting this is still $O(1)$) we obtain the result.

(iii) Let $\varepsilon > 0$. We have shown that if there is no $n \leqslant N$ such that $\|n^2\theta\|_{\mathbb{R}/\mathbb{Z}}$ then there is some $q = O(1)$ such that $\|q\theta\|_{\mathbb{R}/\mathbb{Z}} \ll N^{-2}$. But then $\|q^2\theta\|_{\mathbb{R}/\mathbb{Z}} \ll N^{-2}$ (with a worse implied constant), and if N is sufficiently large this is $< \varepsilon$, contrary to assumption. Therefore $N = O(1)$, a conclusion which is equivalent to the statement of Theorem 1. $\square$

Question 5. Sketch a proof of the following result. There is a function $\omega(N) \to \infty$ with the following property. There is a partition $[N] = P_1 \cup \cdots \cup P_m$ into progressions with square common difference, with $|P_i| \geqslant \omega(N)$ for all i, and such that $\mathrm{diam}_{P_i}(e(\theta\cdot)) \leqslant \omega(N)^{-1}$ for all i.

Solution 5. This follows by modifying the proof of Lemma 7.3.1 in the notes, but using Theorem 1 in place of Dirichlet's application of the pigeonhole principle. Thus let $d \leqslant N^{1/2}$ be a square with $\|\theta d\|_{\mathbb{R}/\mathbb{Z}} \leqslant \varepsilon(N^{1/2})$. Here $\varepsilon(M) \to 0$ as $M \to \infty$, and without loss of generality we may assume it does not do so too rapidly.

Set

$$\omega(N) := \frac{1}{100}\varepsilon(N^{1/2})^{-1/2}$$

(say). Then $\omega(N) \to \infty$, but $\omega(N) < N^{0.1}$ by our assumption that ε is not too small, and $\|\theta d\|_{\mathbb{R}/\mathbb{Z}} \leqslant 0.01\omega(N)^{-2}$. By the same argument as in lectures, if P is any progression with common difference d and length at most $10\omega(N)$, then $\mathrm{diam}_P(e(\theta\cdot)) \leqslant \omega(N)^{-1}$. Finally, by an argument essentially identical to the one in lectures, we may partition $[N]$ into progressions with common difference d and lengths between $\omega(N)$ and $10\omega(N)$. $\square$.

Given two functions $f_1, f_2 : [N] \to \mathbb{R}$, define

$$T(f_1, f_2) := \sum_{x,d} f_1(x) f_2(x+d) 1_X(d),$$

where $X = \{n^2 : n \leqslant N^{1/2}\}$ (as in the course, specialised to $k = 2$).

Question 6. Write an expression for $T(f_1, f_2)$ in terms of the Fourier transforms of f_1, f_2 and 1_X.

Solution 6. The formula is

$$\int_0^1 \hat{f}_1(\theta)\hat{f}_2(-\theta)\hat{1}_X(\theta)d\theta.$$

To verify it, substitute in the definitions of the Fourier transforms and use orthogonality. $\square$

Write $f_A = 1_A - \alpha 1_{[N]}$ for the balanced function of A.

Question 7. Suppose that A does not have any pair of elements differing by a square. Show that there are two 1-bounded[1] functions g_1, g_2, at least one of which is f_A, such that $|T(g_1, g_2)| \gg \alpha^2 N^{3/2}$. ($C$ can be whatever absolute constant you like to make the statement true; you don't have to specify it explicitly.)

Solution 7. The assumption is that $T(1_A, 1_A) = 0$. Expand this as a sum of four terms $E_1 + E_2 + E_3 + E_4$, where

$$E_1 = T(\alpha 1_{[N]}, \alpha 1_{[N]}),$$

$$E_2 = T(f_A, \alpha 1_{[N]}),$$

[1] That is, bounded pointwise by 1.

$$E_3 = T(\alpha 1_{[N]}, f_A),$$
$$E_4 = T(f_A, f_A).$$

Trivially
$$E_1 \gg \alpha^2 N^{3/2},$$
and so
$$|E_2| + |E_3| + |E_4| \gg \alpha^2 N^{3/2}.$$
But each of E_2, E_3, E_4 is of the form $T(g_1, g_2)$. The result follows. (This is very similar to the proof of Proposition 7.2.1 in lectures).

Question 8. Using any results from the course that you like, explain why there is a positive integer s such that
$$\int_0^1 |\hat{1}_X(\theta)|^{2s} d\theta \ll N^{s-1}.$$

Solution 8. Note that Hua's lemma (Sheet 5, Q2) gives this for $s = 2$, but with an extra factor of $N^{o(1)}$. There are (at least) two (related) ways to get the stronger statement asked for, with some large value of s.

Method 1 (easiest). Note that, by expanding out and using orthogonality, $\int_0^1 |\hat{1}_X(\theta)|^{2s} d\theta$ is the number of $(2s)$-tuples $(x_1, \cdots, x_{2s})$ with $x_i \leqslant N^{1/2}$ and $x_1^2 + \cdots + x_s^2 = x_{s+1}^2 + \cdots + x_{2s}^2$. In the notation of the course, this is
$$\sum_{n \leqslant sN} r_{2,s}(n)^2.$$
However, one of the main theorems of the course (Theorem 3.1.2 and Proposition 3.1.1) gives that $r_{2,s}(n) \ll n^{s/2-1}$ for $s \geqslant 10^4$. The claim follows.

Method 2 (harder). By Sheet 2, Q5 (with the exponent 5 there replaced by $2s$), we see that for $s \geqslant 3$ we need only worry about the major arcs. This can then be handled by minor adaptations of Chapter 5 of the notes (but there are quite a lot of them!).

Note that in both cases we only need the easier *upper* bound $\mathfrak{S}_{2,s}(N) \ll 1$ for the singular series, which means the reliance on Chapter 6 of the notes is minimal.

Question 9. Suppose that $g_1, g_2 : [N] \to \mathbb{R}$ are two 1-bounded functions. Suppose that $T(g_1, g_2) \geqslant \delta N^{3/2}$. Show that for $i = 1, 2$ we have $\sup_\theta |\hat{g}_i(\theta)| \gg_\delta N$. *Hint:* you may wish to use Hölder's inequality, which states that
$$\int_0^1 \prod_{i=1}^t \phi_i(\theta) d\theta \leqslant \prod_{i=1}^t \Big(\int_0^1 |\phi_i(\theta)|^{p_i} \Big)^{1/p_i}$$
whenever $p_1, \dots, p_t > 1$ and $\frac{1}{p_1} + \cdots + \frac{1}{p_t} = 1$.

Solution 9. From Question 6 we have

$$T(g_1, g_2) = \int_0^1 \hat{g}_1(\theta)\hat{g}_2(-\theta)\hat{1}_X(\theta)d\theta.$$

Thus, with s as in the solution to Question 8,

$$|T(g_1, g_2)| \leqslant \sup_\theta |\hat{g}_1(\theta)|^{1/s} \int_0^1 |\hat{g}_1(\theta)|^{(s-1)/s}|\hat{g}_2(\theta)||\hat{1}_X(\theta)|d\theta.$$

By Hölder's inequality with exponents $(p_1, p_2, p_3) = (\frac{2s}{s-1}, 2, 2s)$,

$$|T(g_1, g_2)| \leqslant \sup_\theta |\hat{g}_1(\theta)|^{1/s}\Big(\int_0^1 |\hat{g}_1(\theta)|^2\Big)^{(s-1)/2s}\Big(\int_0^1 |\hat{g}_2(\theta)|^2\Big)^{1/2}\Big(\int_0^1 |\hat{1}_X(\theta)|^{2s}\Big)^{1/2s}.$$

Using Parseval for the first two integrals and Question 8 for the third, we obtain

$$|T(g_1, g_2) \ll \sup_\theta |\hat{g}_1(\theta)|^{1/s} N^{3/2-1/s}.$$

Therefore if $|T(g_1, g_2)| \geqslant \delta N^{3/2}$, we have $|\hat{g}_1(\theta)| \gg \delta^s N$.

One may obtain the same bound for $\hat{g}_2$ by an essentially identical argument. □

Question 10. Outline a complete proof of the Furstenberg-Sárközy theorem by assembling the above ingredients.

Solution 10. We use a density increment argument, modelled very closely on the proof of Roth's theorem in lectures. Here, briefly, are the main steps. Suppose that $A \subset [N]$ is a set of density α and that A does not contain any pair of elements differing by a square. Suppose that N is sufficiently large in terms of α.

(i) By Question 7, $|T(g_1, g_2)| \gg \alpha^{3/2}N^{3/2}$, where at least one of g_1, g_2 is the balanced function f_A.

(ii) By Question 9, $\sup_\theta |\hat{f}_A(\theta)| \gg_\alpha N$ (in fact, $\gg \alpha^C N$ if one looks at the solution to the question, but this is not important if one's only interest is a qualitative bound).

(iii) Now we proceed as in Proposition 7.3.1 in the notes. However, where there we used the partition $[N] = \bigcup_i P_i$ coming from Lemma 7.3.1, now we use the solution to Question 5, which guarantees that all the P_i have square common difference.

(iv) Mimicking the argument in the lecture notes (that is, the proof of Proposition 7.3.1) we see that there is some progression P_i with square common difference, and with $|P_i| \geqslant \omega(N) \to \infty$, such that $\frac{|A \cap P_i|}{|P_i|} \geqslant \alpha + c\alpha^C$.

(v) Write $P_i = x + [N']d^2$, and set $A' := \{n \in [N'] : x + nd^2 \in A \cap P_i\}$. Then A' has no square common difference (or else A would), $|A' \subset [N']$, and $\alpha' := |A'|/N \geqslant \alpha + c\alpha^C$.

Thus is the basis for a density increment argument exactly as in lectures. $\square$

ben.green@maths.ox.ac.uk