Additive Number Theory

James Maynard

Mathematical Institute, Oxford
Email address: maynard@maths.ox.ac.uk

Contents

Chapter 1. The geometry of numbers 1
1.1. Minkowski's first theorem and sums of squares 2
1.2. Minkowski's second theorem 4

Chapter 2. Sumset inequalities 9

Chapter 3. Equations in $\mathbb{Z}/q\mathbb{Z}$ 13

Chapter 4. Introduction to circle method 21
4.1. The Fourier Transform over $\mathbb{Z}$ and $\mathbb{R}$ 21
4.2. A warm-up example 22
4.3. The circle method 25

Chapter 5. Waring's Problem 27
5.1. Major Arcs for Waring's problem 28
5.2. Minor Arcs for Waring's problem 32

Chapter 6. Roth's Theorem 37
6.1. The density increment strategy 37
6.2. Circle method and large Fourier coefficients 38

Chapter 7. Freiman's Theorem 43
7.1. Modelling integers sets with cyclic groups 45
7.2. Structure in sumsets 47

Appendix A. Asymptotic estimates 51

Appendix B. Analytic identities 53

CHAPTER 1

The geometry of numbers

The geometry of numbers studies the integers by viewing them geometrically as a *lattice* in $\mathbb{R}$ (or $\mathbb{R}^n$).

DEFINITION (Lattices and their key parameters).

(1) A lattice Λ *in* $\mathbb{R}^n$ *is a set*

$$\Lambda = \mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_r\mathbb{Z}$$

for some linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbb{R}^n$*. We say* $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ *is the* basis *of the lattice and* r *is the rank of the lattice. We say* Λ *is* full-rank *if* $r = n$*.*

(2) The fundamental parallelepiped *of a lattice* Λ *with respect to the basis* $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ *of* Λ *is the set*

$$P_{\mathbf{v}} := \{x_1\mathbf{v}_1 + \cdots + x_r\mathbf{v}_r : x_1, \ldots, x_r \in [0, 1]\}.$$

(3) The determinant $\det(\Lambda)$ *is the* r*-dimensional volume of a fundamental parallelepiped.*

There are many possible choices of a basis for any given lattice, but quantities like the rank and determinant do not depend on the choice of basis.

LEMMA 1.1 (Basic properties of lattices).

(1) (Additive subgroup) If $\mathbf{x}, \mathbf{y} \in \Lambda$ *then* $\mathbf{x} \pm \mathbf{y} \in \Lambda$*.*

(2) (Discreteness) There is a constant $\delta > 0$ *such that if* $\mathbf{x} \neq \mathbf{y} \in \Lambda$ *then* $|\mathbf{x} - \mathbf{y}| \geq \delta$*.*

(3) (Determinant well-defined) If $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ *and* $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ *are two bases of a lattice* Λ*, then* $r = k$ *and* $\mathrm{vol}(P_{\mathbf{v}}) = \mathrm{vol}(P_{\mathbf{w}})$*. If* Λ *has full rank then* $\det(\Lambda) = |\det(\mathbf{v}_1, \ldots, \mathbf{v}_k)|$*.*

PROOF. (1) This is immediate from the definition.

(2) If $\mathbf{x} = \sum_{i=1}^{k} a_i\mathbf{v}_i \in \Lambda$ has $\mathbf{x} \neq \mathbf{0}$ then $|a_j| \geq 1$ for some j since $a_j \in \mathbb{Z}$. Let $\mathbf{v}_j^* \in \mathbb{R}^n$ be the component of $\mathbf{v}_j$ orthogonal to the other $\mathbf{v}_i$. Then $|\mathbf{v}_j^* \cdot \mathbf{x}| = |a_j||\mathbf{v}_j^*|^2 \geq |\mathbf{v}_j^*|^2$. Thus for all $\mathbf{x} \in \Lambda$ we have $|\mathbf{x}| \geq \min_j |\mathbf{v}_j^*| > 0$.

(3) Since the vectors $\mathbf{v}_i$ are linearly independent and the $\mathbf{w}_i$ are, we see that $r = k = \dim(\mathrm{span}_{\mathbb{R}}(\Lambda))$. Since $\{\mathbf{v}_i\}_{i=1}^{r}$ form a basis for Λ and

$\{\mathbf{w}_j\}_{j=1}^k \subseteq \Lambda$, there is an $r \times r$ matrix M with integer entries such that $\mathbf{w}_i = \sum_j M_{i,j}\mathbf{v}_j$. But since $\{\mathbf{w}_i\}_{i=1}^k$ also forms a basis there is a $k \times k$ integer matrix N such that $\mathbf{v}_i = \sum_i N_{i,j}\mathbf{w}_j$. Thus we see that $M^{-1} = N$, so both matrixes have determinant ± 1 and $\mathrm{vol}(P_{\mathbf{v}}) = \mathrm{vol}(P_{\mathbf{w}})$. If $r = n$ then it is easy to see from a change variables $\mathrm{vol}(P_{\mathbf{v}}) = |\det(\mathbf{v}_1, \dots, \mathbf{v}_k)|$. □

1.1. Minkowski's first theorem and sums of squares

Definition (Convex sets and successive minima).

(1) *A* convex *set $K \subseteq \mathbb{R}^n$ is a set such that if $\mathbf{x}, \mathbf{y} \in K$ then the line segment connecting $\mathbf{x}$ and $\mathbf{y}$ is also contained in K.*
(2) *A* centrally symmetric *set is a set S such that $-\mathbf{x} \in S$ whenever $\mathbf{x} \in S$.*
(3) *Given a lattice and a centrally symmetric convex set K of positive volume, the i^{th} successive minima of K with respect to Λ is*

$$\lambda_i = \inf\{\lambda \in \mathbb{R}_{>0} : \lambda K \cap \Lambda \text{ contains } i \text{ linearly independent vectors}\}.$$

If K is the unit ball, we say $\lambda_1 \leq \cdots \leq \lambda_k$ are the successive minima of the lattice Λ.

Lemma 1.2 (Blichfeldt's lemma). *Let $K \subseteq \mathbb{R}^n$ be a measurable set and $\Lambda \subseteq \mathbb{R}^n$ be full rank lattice with $\mathrm{vol}(K) > \det(\Lambda)$. Then there are distinct points $\mathbf{x}, \mathbf{y} \in K$ with $\mathbf{x} - \mathbf{y} \in \Lambda$.*

Proof. Assume for a contradiction that there are no such $\mathbf{x}, \mathbf{y}$. Let P be the fundamental parallelepiped of Λ. Then for every $\mathbf{t} \in P$, there is at most one $\mathbf{v} \in \Lambda$ such that $\mathbf{t} + \mathbf{v} \in K$. On the other hand, every point in $\mathbb{R}^n$ can be written as $\mathbf{t} + \mathbf{v}$ for some $\mathbf{t} \in P$, $\mathbf{v} \in \Lambda$. Thus

$$\mathrm{vol}(K) = \int_P \#\{\mathbf{v} \in \Lambda : \mathbf{t} + \mathbf{v} \in K\} d\mathbf{t} \leq \int_P 1 d\mathbf{t} = \mathrm{vol}(P) = \det(\Lambda). \qquad \square$$

Theorem 1.3 (Minkowski's first Theorem). *Let K be a centrally symmetric convex set and $\Lambda \subseteq \mathbb{R}^n$ a full rank lattice with $\mathrm{vol}(K) > 2^n \det(\Lambda)$. Then K contains a non-zero lattice point of Λ.*

Proof. $\mathrm{vol}(\frac{1}{2} \cdot K) = 2^{-n}\mathrm{vol}(K) > \det(\Lambda)$, so by Blichfeldt's Lemma there are $\mathbf{x} \neq \mathbf{y} \in \frac{1}{2} \cdot K$ such that $\mathbf{x} - \mathbf{y} \in \Lambda$. But if $\mathbf{x}, \mathbf{y} \in \frac{1}{2} \cdot K$ then $2x, 2y \in K$, so $\mathbf{x} - \mathbf{y} \in (2\mathbf{x} - 2\mathbf{y})/2 \in K$ since K is centrally symmetric and convex. Thus $\mathbf{0} \neq \mathbf{x} - \mathbf{y} \in K \cap \Lambda$. □

Proposition 1.4 (Sums of two squares). *An integer q can be written as the sum of two squares if and only if all primes factors of q which are $3 \pmod 4$ occur with even multiplicity.*

PROOF. If $p \equiv 3 \pmod 4$, the only solutions to $x^2 + y^2 = 0 \pmod p$ are $x \equiv y \equiv 0 \pmod p$, which means that $x^2 + y^2$ is divisible by p^2. It follows that there are no solutions to $x^2+y^2 = q$ unless every prime factor of q which is 3 (mod 4) occurs with even multiplicity, and any such solutions must have x^2 and y^2 a multiple of all of these factors. By restricting to x, y a multiple of d whenever $d^2|q$ and then dividing through by all square factors of q, it suffices to consider the case when q is squarefree and has no prime factors which are 3 (mod 4).

Let $b \in \mathbb{Z}$ be such that $b^2 = -1 \pmod q$. Consider the centrally smmetric convex set $K \subseteq \mathbb{R}^2$ and lattice Λ given by

$$K = \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + x_2^2 < 2q\},$$
$$\Lambda = \{(x_1, x_2) \in \mathbb{Z}^2 : x_1 \equiv bx_2 \pmod q\} = \begin{pmatrix} b \\ 1 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 0 \\ q \end{pmatrix} \mathbb{Z}.$$

Then we have $\mathrm{vol}(K) = 2\pi q$ and $\det(\Lambda) = q$, so Minkowski's first theorem applies and there is a non-zero point in $(x_1, x_2) \in \Lambda \cap K$. But then $x_1^2 + x_2^2 \equiv 0 \pmod q$ and $0 < x_1^2 + x_2^2 < 2q$, so $x_1^2 + x_2^2 = q$, as required. □

LEMMA 1.5 (Sums of 4 squares). *Every positive integer can be written as the sum of four integer squares.*

PROOF. We note the identity

$$\begin{aligned}(a_1^2+a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2,\end{aligned}$$

so the set of integers representable as the sum of four squares is closed under multiplication. In particular, it suffices to show the result for all primes p. The result is trivial for $p = 2$, so we just consider odd p. Let

$$\mathcal{A} := \{1 - x^2 \pmod p : x \in \mathbb{Z}\}, \qquad \mathcal{B} := \{x^2 \pmod p : x \in \mathbb{Z}\}.$$

Then $|\mathcal{A}| = |\mathcal{B}| = (p+1)/2$ and so $\mathcal{A} \cap \mathcal{B} \neq \emptyset$. In particular, there are $r, s \in \mathbb{Z}$ such that $r^2 + s^2 + 1 = 0 \pmod p$. Let $\Lambda \subseteq \mathbb{Z}^4$ be the lattice

$$\Lambda := \begin{pmatrix} p \\ 0 \\ 0 \\ 0 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 0 \\ p \\ 0 \\ 0 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} r \\ s \\ 1 \\ 0 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} s \\ -r \\ 0 \\ 1 \end{pmatrix} \mathbb{Z} = \left\{ \mathbf{x} \in \mathbb{Z}^4 : \begin{array}{l} x_1 = rx_3 + sx_4 \pmod p \\ x_2 = sx_3 - rx_4 \pmod p \end{array} \right\},$$

so that if $\mathbf{x} \in \Lambda$ coming from $\mathbf{a} \in \mathbb{Z}^4$ then

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = (pa_1 + ra_3 + sa_4)^2 + (pa_2 + sa_3 - ra_4)^2 + a_3^2 + a_4^2$$
$$\equiv (1 + r^2 + s^2)(a_3^2 + a_4^2) \equiv 0 \pmod{p}.$$

We see that $\det(\Lambda) = p^2$. Let K be the centrally symmetric convex region

$$K := \{\mathbf{x} \in \mathbb{R}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p\}$$

so that $\mathrm{vol}(K) = \pi^2(\sqrt{2}p)^4/2 = 2\pi^2 p^2 > 2^4 p^2$. Thus Minkowski's first Theorem applies and so Theorem 1.3 implies that there is $\mathbf{x} \in \Lambda \cap K \setminus \{\mathbf{0}\}$, and hence satisfies

$$0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p, \qquad x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0 \pmod{p}.$$

Thus $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$, as required. □

LEMMA 1.6 (Dirichlet). *Let $\theta_1, \dots, \theta_r \in \mathbb{R}$. Then for any choices of $M \geq 1$ and $\epsilon_1, \dots, \epsilon_r \in (0, 1/2)$ with $\prod_{i=1}^r \epsilon_i \geq 1/M$ there is an integer $0 < m \leq M$ such that*

$$\|m\theta_i\| \leq \epsilon_i \qquad \text{for all } 1 \leq i \leq r.$$

PROOF. Choose $M' > M$ such that $M' < \lfloor M \rfloor + 1$. Let K be the centrally symmetric convex set

$$K := \Big\{(x, y_1, \dots, y_r) \in \mathbb{R}^{r+1} : |x| \leq M', |\theta_i x - y_i| < \epsilon_i \, \forall i\Big\}.$$

Then $\mathrm{vol}(K) = 2^{r+1} M' \prod_{i=1}^r \epsilon_i \geq 2^{r+1} M'/M > 2^{r+1}$. Thus, by Minkowski's Theorem $K \cap \mathbb{Z}^{r+1}$ contains a non-zero point. Either the x-coordinate or its negative then gives the result (noting that all integers $\leq M'$ are $\leq M$). □

1.2. Minkowski's second theorem

THEOREM 1.7 (Reduced basis of a lattice). *Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of rank r. Then there are linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_r$ such that*

(1) (Basis of the lattice) We have that

$$\Lambda = \mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_r\mathbb{Z}.$$

(2) (Quasi-orthogonality) For any $a_1, \dots, a_r \in \mathbb{R}$ we have

$$|a_1\mathbf{v}_1 + \cdots + a_r\mathbf{v}_r| \geq 2^{-r^4}(|a_1\mathbf{v}_1| + \cdots + |a_r\mathbf{v}_r|).$$

(3) (Minkowski's second theorem) Let Λ have successive minima $\lambda_1 \leq \cdots \leq \lambda_n$. Then $|\mathbf{v}_i| \leq 2^{i-1}\lambda_i$ and if Λ has full rank

$$2^{-n^3}\lambda_1 \dots \lambda_n \leq \det(\Lambda) \leq 2^{n^2}\lambda_1 \dots \lambda_n.$$

PROOF. We begin by constructing the basis of Λ. First we choose $\mathbf{v}_1 \neq \mathbf{0} \in \Lambda$ to be a vector of minimal length. By minimiality, we then see that $\Lambda \cap \mathrm{span}_{\mathbb{R}}(\mathbf{v}_1) = \mathbf{v}_1\mathbb{Z}$ and that $|\mathbf{v}_1| = \lambda_1$.

Imagine $\mathbf{v}_1, \dots, \mathbf{v}_j$ have already been chosen (with $j < r$) such that $\Lambda \cap \mathrm{span}_{\mathbb{R}}(\mathbf{v}_1, \dots, \mathbf{v}_j) = \mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_j\mathbb{Z}$ and such that $|\mathbf{v}_i| \leq 2^{i-1}\lambda_i$. We wish to select $\mathbf{v}_{j+1}$. Let

$$H := \mathrm{span}_{\mathbb{R}}(\mathbf{v}_1, \dots, \mathbf{v}_j),$$

and choose $\mathbf{w} \in \Lambda \backslash H$ of shortest length (which exists since if $\Lambda = \Lambda \cap H$ we have a basis so $j = r$). Let P be the closed parallelepiped

$$P := \{x_1\mathbf{v}_1 + \cdots + x_j\mathbf{v}_j + x_{j+1}\mathbf{w} : 0 \leq x_i \leq 1\}.$$

Since Λ is discrete, $\Lambda \cap P$ is a finite set. Now choose $\mathbf{v}_{j+1}$ to be a vector in $\Lambda \cap P \backslash H$ which minimises the distance to a vector in H. Then clearly $\mathbf{v}_1, \dots, \mathbf{v}_{j+1}$ are linearly independent (since $\mathbf{v}_{j+1} \notin H$) and $\mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_{j+1}\mathbb{Z} \subseteq \Lambda$ (since $\mathbf{v}_{j+1} \in \Lambda$). Moreover, we see that $\mathbf{v}_{j+1}$ minimises the distance to H amongst all vectors in $\mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_{j+1}\mathbb{Z} \backslash H$.

Now we show $\mathrm{span}_{\mathbb{R}}(\mathbf{v}_1, \dots, \mathbf{v}_{j+1}) \cap \Lambda = \mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_{j+1}\mathbb{Z}$. If

$$\mathbf{x} = x_1\mathbf{v}_1 + \cdots + x_{j+1}\mathbf{v}_{j+1} \in \mathrm{span}_{\mathbf{R}}(\mathbf{v}_1, \dots, \mathbf{v}_{j+1}) \cap \Lambda,$$

then let $\mathbf{x}' := \mathbf{x} - \lfloor x_{j+1} \rfloor \mathbf{v}_{j+1}$. We see that the distance of $\mathbf{x}'$ from H is $(x_{j+1} - \lfloor x_{j+1} \rfloor) < 1$ times the distance of $\mathbf{v}_{j+1}$ from H. However, $\mathbf{v}_{j+1}$ minimizes this distance amongst vectors not in H, so we must have that $x_{j+1} \in \mathbb{Z}$ and $\mathbf{x}' \in \mathrm{span}_{\mathbb{R}}(\mathbf{v}_1, \dots, \mathbf{v}_j) \cap \Lambda = \mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_j\mathbb{Z}$. Thus $x_i \in \mathbb{Z}$ for all i, so

$$\mathrm{span}_{\mathbb{R}}(\mathbf{v}_1, \dots, \mathbf{v}_{j+1}) \cap \Lambda = \mathbf{v}_1\mathbb{Z} + \cdots + \mathbf{v}_{j+1}\mathbb{Z}.$$

Since $\mathbf{w}$ had minimal length in Λ and was linearly independent of $\mathbf{v}_1, \dots, \mathbf{v}_j$, we see that $|\mathbf{w}| \leq \lambda_{j+1}$. By the triangle inequality, any element of P therefore has size at most

$$\sum_{i=1}^{j} |\mathbf{v}_i| + |\mathbf{w}| \leq \sum_{i=1}^{j} 2^{i-1}\lambda_i + \lambda_{j+1} \leq 2^j\lambda_{j+1}.$$

In particular, $|\mathbf{v}_{j+1}| \leq 2^j\lambda_{j+1}$, as requried. Repeating this we obtain a basis of Λ with $|\mathbf{v}_i| \leq 2^{i-1}\lambda_i$. By reordering if necessary, we may assume that $|\mathbf{v}_i| \geq \lambda_i$.

Having constructed our basis, we now show it has the required properties. If

$$|\mathbf{v}_{k+1} - \mu_1\mathbf{v}_1 - \cdots - \mu_k\mathbf{v}_k| \leq \epsilon|\mathbf{v}_{k+1}|$$

for some $\mu_1, \dots, \mu_k \in \mathbb{R}$, then by Lemma 1.6 we can choose $m \leq M$ such that $\|m\mu_i\| \leq M^{-1/k}$ for all i. Then we see that

$$\begin{aligned}|m\mathbf{v}_{k+1} - \lfloor m\mu_1 \rfloor \mathbf{v}_1 - \cdots - \lfloor m\mu_k \rfloor \mathbf{v}_k| &\leq m\epsilon|\mathbf{v}_{k+1}| + M^{-1/k}\sum_{i=1}^{k}|\mathbf{v}_i| \\ &\leq 2^k\lambda_{k+1}M\epsilon + M^{-1/k}\sum_{i=1}^{k}2^{i-1}\lambda_i \\ &\leq 2^k\lambda_{k+1}(M\epsilon + M^{-1/k}).\end{aligned}$$

On the other hand, the vector on the left hand side is clearly in Λ with non-zero $\mathbf{v}_{k+1}$ coefficient, so of size at least λ_{k+1}. Taking $M = \epsilon^{-k/(k+1)}$ gives the inequality $1 \leq 2^{k+1}\epsilon^{-1/(k+1)}$, so $\epsilon \geq 2^{-(k+1)^2}$. Thus the distance from $\mathbf{v}_{k+1}$ to $\operatorname{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ is at least $2^{-(k+1)^2}|\mathbf{v}_{k+1}|$.

Let let $\mathbf{v}_j^*$ be the component of $\mathbf{v}_j$ orthogonal to $\mathbf{v}_1, \dots, \mathbf{v}_{j-1}$. We then have $|\mathbf{v}_i^*| \geq 2^{-i^2}|\mathbf{v}_i| \geq 2^{-i^2}\lambda_i$. If Λ has full rank, then $\det(\Lambda) = |\det(\mathbf{v}_1, \dots, \mathbf{v}_n)| = \prod_{i=1}^{n}|\mathbf{v}_i^*|$, and so

$$|\det(\mathbf{v}_1, \dots, \mathbf{v}_k)| \geq \prod_{i=1}^{n} 2^{-i^2}\lambda_i \geq 2^{-n^3}\lambda_1 \cdots \lambda_n.$$

$$|\det(\mathbf{v}_1, \dots, \mathbf{v}_k)| \leq \prod_{i=1}^{n}|\mathbf{v}_i| \leq \prod_{i=1}^{n} 2^{i-1}\lambda_i \leq 2^{n^2}\lambda_1 \cdots \lambda_n.$$

Moreover, this implies that the component of $\mathbf{v}_j$ orthogonal to all of the other $\mathbf{v}_i$ has length at least $2^{-r^3}|\mathbf{v}_j|$. Thus

$$|a_1\mathbf{v}_1 + \cdots + a_r\mathbf{v}_r| \geq 2^{-r^3}\sup_i |a_i\mathbf{v}_i| \geq 2^{-r^4}(|a_1\mathbf{v}_1| + \cdots + |a_r\mathbf{v}_r|). \qquad \square$$

DEFINITION (Generalized arithmetic progression). *A generalized arithmetic progression of dimension d and size S is a set of the form*

$$G = \{w_0 + a_1w_1 + \cdots + a_dw_d : 0 \leq a_i < L_i,\ a_i \in \mathbb{Z}\}$$

for some $w_0, \dots, w_d \in \mathbb{Z}$ and $L_1, \dots, L_d$ with $L_1 \cdots L_d = S$. If $|G| = S$ (so that all expressions $w_0 + a_1w_1 + \cdots + a_dw_d$ with $0 \leq a_i < L_i$ are distinct) we say that G is proper.

LEMMA 1.8 (Bohr sets contain generalized arithmetic progressions). *Let $\eta \in (0, 1/2)$, $M > 1$ and $\theta_1, \dots, \theta_k \in [0, 1]$. Define*

$$B_\theta := \{x \in \mathbb{Z} : \|x\theta_i\| < \eta \text{ for } i = 1, \dots, k,\ |x| \leq M\}.$$

Then there are $w_1, \dots, w_k \in \mathbb{Z}$ and constants $L_1, \dots, L_k > 0$ such that the set

$$S = \{a_1w_1 + \cdots + a_kw_k : a_i \in \mathbb{Z},\ |a_i| \leq L_i\}$$

is contained in B_θ, has size at least $2^{-2k^3}\eta^k M$, and all elements $a_1w_1 + \cdots + a_kw_k$ are distinct.

PROOF. Let $\Lambda_1 = \mathbb{Z}^{k+1}$ and

$$K = \{(x, y_1, \ldots, y_k) \in \mathbb{R}^{k+1} : |x| \leq M, |x\theta_i - y_i| \leq \eta\}.$$

Then we see that every point of B_θ corresponds to a point in $\Lambda \cap K$. To apply Theorem 1.7 we apply a linear transformation so K is comparable to the unit ball. Let

$$\Lambda_2 := \begin{pmatrix} 1/M \\ \theta_1/\eta \\ \vdots \\ \theta_k/\eta \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 0 \\ 1/\eta \\ \vdots \\ 0 \end{pmatrix} \mathbb{Z} + \cdots + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1/\eta \end{pmatrix} \mathbb{Z}.$$

Then we see that every point in $\Lambda_2 \cap B(0,1)$ gives rise to a point of B_θ, and Λ has determinant $M^{-1}\eta^{-k}$. By Theorem 1.7, there is a reduced basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ for Λ_2, and by the triangle inequality

$$\left\{a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k : a_i \in \mathbb{Z}, |a_i| \leq \frac{1}{k|\mathbf{v}_i|}\right\} \subseteq \Lambda_2 \cap B(0,1).$$

Letting $w_j \in \mathbb{Z}$ be the first component of $M\mathbf{v}_j$ and $L_i = 1/(k|\mathbf{v}_i|)$, we then see that the set S defined in the lemma is contained in B_θ. Moreover, since there are at least t integers in the interval $[-t, t]$, we see that the number of choices of $a_1, \ldots, a_k$ is at least

$$\prod_{i=1}^{k} L_i = \frac{1}{k^k} \prod_{i=1}^{k} \frac{1}{|\mathbf{v}_i|} \geq \frac{2^{-k^2}}{k^k} \prod_{i=1}^{k} \frac{1}{\lambda_i} \geq \frac{2^{-k^2}2^{-k^3}}{k^k \det(\Lambda_2)} \geq 2^{-2k^3} M\eta^k.$$

Finally, we need to check that two distinct choices of coefficients a_i cannot give the same point in S. If

$$a_1w_1 + \cdots + a_kw_k = b_1w_1 + \ldots b_kw_k = x,$$

then since there are unique choices of $y_1, \ldots, y_k$ satisfying $|\theta_i x - y_i| < \eta$, we see that we must have

$$a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k = b_1\mathbf{v}_1 + \ldots b_k\mathbf{v}_k.$$

But this implies that $(a_1, \ldots, a_k) = (b_1, \ldots, b_k)$ by the linear independence of $\mathbf{v}_i$. The the size of S is at least $2^{-2k^3}M\eta^k$, as required. □

CHAPTER 2

Sumset inequalities

DEFINITION (Sumsets). *Given sets $\mathcal{A}, \mathcal{B}$ in some additive group , we write*

$$\mathcal{A} + \mathcal{B} := \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\},$$
$$\mathcal{A} - \mathcal{B} := \{a - b : a \in \mathcal{A}, b \in \mathcal{B}\}.$$

Given an integer $k \geq 1$ we define the k-fold iterated sumset

$$k\mathcal{A} = \underbrace{\mathcal{A} + \cdots + \mathcal{A}}_{k \text{ times}} = \{a_1 + \cdots + a_k : a_i \in \mathcal{A}\},$$

Throughout this chapter, we will implicitly assume that we are working inside a fixed additive group; in practice we will always be interested in sets in $\mathbb{Z}$ or $\mathbb{Z}/q\mathbb{Z}$.

LEMMA 2.1 (Ruzsa's Triangle inequality). *We have*

$$|\mathcal{A}||\mathcal{B} - \mathcal{C}| \leq |\mathcal{A} - \mathcal{B}||\mathcal{A} - \mathcal{C}|.$$

PROOF. For each $d \in \mathcal{B} - \mathcal{C}$, fix a representative $b_d \in \mathcal{B}$ and $c_d \in \mathcal{C}$ such that $d = b_d - c_d$. Then define $\phi : \mathcal{A} \times (\mathcal{B} - \mathcal{C})$ by

$$\phi((a, d)) = (a - b_d, a - c_d).$$

ϕ is injective since we can recover (a, d) from its image; if $\phi((a, d)) = (x, y)$ then $d = y - x$ and $a = x + b_{y-x}$. Thus the size of the domain is at most the size of the codomain, giving the result. □

LEMMA 2.2 (Ruzsa's covering lemma). *Suppose that $|\mathcal{A} + \mathcal{B}| \leq K|\mathcal{A}|$. Then there is a set $\mathcal{X}$ with $|\mathcal{X}| \leq K$ such that*

$$\mathcal{B} \subseteq \mathcal{A} - \mathcal{A} + \mathcal{X}.$$

PROOF. Choose a subset $\mathcal{X} \subseteq \mathcal{B}$ of maximal size such that the sets $\{\mathcal{A} + x : x \in \mathcal{X}\}$ are all disjoint. Then the union of these sets contains exactly $|\mathcal{A}||\mathcal{X}|$ elements and is contained in $\mathcal{A} + \mathcal{B}$, so $|\mathcal{A}||\mathcal{X}| \leq |\mathcal{A} + \mathcal{B}| \leq K|\mathcal{A}|$ and hence $|\mathcal{X}| \leq K$. For every $b \in \mathcal{B}$, the set $b + \mathcal{A}$ must intersect $x + \mathcal{A}$ for some $x \in \mathcal{X}$ by maximality of $\mathcal{X}$. Therefore there exists $a_1, a_2 \in \mathcal{A}$ such that $b + a_1 = x + a_2$, so $b = x + a_2 - a_1 \in \mathcal{X} + \mathcal{A} - \mathcal{A}$. □

LEMMA 2.3 (Petridis' lemma/Subset-minimality implies sumsets-maximality). *Suppose that*

$$\frac{|\mathcal{A}+\mathcal{B}|}{|\mathcal{A}|} \leq \frac{|\mathcal{A}'+\mathcal{B}|}{|\mathcal{A}'|} \quad \text{for all non-empty } \mathcal{A}' \subseteq \mathcal{A}.$$

Then

$$\frac{|\mathcal{A}+\mathcal{B}|}{|\mathcal{A}|} \geq \frac{|\mathcal{A}+\mathcal{B}+\mathcal{C}|}{|\mathcal{A}+\mathcal{C}|} \quad \text{for all } \mathcal{C}.$$

PROOF. We prove this by induction on $|\mathcal{C}|$. If $|\mathcal{C}| = 1$ then the result is automatic since $|\mathcal{A}+\mathcal{B}+\mathcal{C}| = |\mathcal{A}+\mathcal{B}|$ and $|\mathcal{A}+\mathcal{C}| = |\mathcal{A}|$. Now assume that the result holds for all $|\mathcal{C}| \leq m$, and consider $\mathcal{C}'$ of size $m+1$. Let $\mathcal{C}' = \mathcal{C} \cup \{c\}$ for a set $\mathcal{C}$ of size m. Thus we wish to show

$$\frac{|\mathcal{A}+\mathcal{B}+(\mathcal{C}\cup\{c\})|}{|\mathcal{A}+(\mathcal{C}\cup\{c\})|} \leq \frac{|\mathcal{A}+\mathcal{B}|}{|\mathcal{B}|}$$

Since $|\mathcal{A}+\mathcal{B}+(\mathcal{C}\cup\{c\})| = |\mathcal{A}+\mathcal{B}+\mathcal{C}| + |(\mathcal{A}+\mathcal{B}+c)\backslash(\mathcal{A}+\mathcal{B}+\mathcal{C})|$ (and similarly for the denominator), and by the induction hypothesis we see that it suffices to show

$$|(\mathcal{A}+\mathcal{B}+c)\backslash(\mathcal{A}+\mathcal{B}+\mathcal{C})| \leq \frac{|\mathcal{A}+\mathcal{B}|}{|\mathcal{A}|}|(\mathcal{A}+c)\backslash(\mathcal{A}+\mathcal{C})|.$$

We have

$$\begin{aligned}|(\mathcal{A}+\mathcal{B}+c)\backslash(\mathcal{A}+\mathcal{B}+\mathcal{C})| &= \{a+b+c:\ a\in\mathcal{A},\, b\in\mathcal{B},\, a+b+c\notin A+B+C\}\\ &\subseteq \{a+b+c:\ a\in\mathcal{A},\, b\in\mathcal{B},\, a+B+c\not\subseteq A+B+C\}.\end{aligned}$$

Therefore, if we let

$$\mathcal{D} := \{a\in\mathcal{A}:\ a+c+\mathcal{B}\subseteq\mathcal{A}+\mathcal{B}+\mathcal{C}\},$$

we have

$$\{a+b+c:\ a\in\mathcal{A},\, b\in\mathcal{B},\, a+B+c\not\subseteq A+B+C\} = (A+B+c)\backslash(D+B+c).$$

In particular,

$$|(\mathcal{A}+\mathcal{B}+c)\backslash(\mathcal{A}+\mathcal{B}+\mathcal{C})| \leq |\mathcal{A}+\mathcal{B}| - |\mathcal{D}+\mathcal{B}|.$$

Moreover, if $a\in\mathcal{A}$ has $a+c\in\mathcal{A}+\mathcal{C}$, then $a+c+\mathcal{B}\subseteq\mathcal{A}+\mathcal{B}+\mathcal{C}$ so $a\in\mathcal{D}$. Thus

$$|(\mathcal{A}+c)\backslash(\mathcal{A}+\mathcal{C})| \geq |\mathcal{A}| - |\mathcal{D}|.$$

Putting this together, it suffices to show that

$$|\mathcal{A}+\mathcal{B}| - |\mathcal{D}+\mathcal{B}| \leq \frac{|\mathcal{A}+\mathcal{B}|}{|\mathcal{A}|}(|\mathcal{A}| - |\mathcal{D}|).$$

But this follows immediately from the hypothesis applied to $\mathcal{A}' = \mathcal{D} \subseteq \mathcal{A}$. □

LEMMA 2.4 (Plünnecke's inequality). *Let $|\mathcal{A}+\mathcal{B}| \leq K|\mathcal{A}|$. Then for all integers $m, n \geq 0$*

$$|m\mathcal{B} - n\mathcal{B}| \leq K^{m+n}|\mathcal{A}|.$$

In particular, if $|\mathcal{A}+\mathcal{A}| \leq K|\mathcal{A}|$ then $|m\mathcal{A} - n\mathcal{A}| \leq K^{m+n}|\mathcal{A}|$.

PROOF. Choose $\mathcal{X} \subseteq \mathcal{A}$ to minimize $|\mathcal{X}+\mathcal{B}|/|\mathcal{X}|$. Then we have

$$\frac{|\mathcal{X}+\mathcal{B}|}{|\mathcal{X}|} \leq \frac{|\mathcal{Y}+\mathcal{B}|}{|\mathcal{Y}|} \quad \text{for all non-empty } \mathcal{Y} \subseteq \mathcal{X},$$
$$\frac{|\mathcal{X}+\mathcal{B}|}{|\mathcal{X}|} \leq \frac{|\mathcal{A}+\mathcal{B}|}{|\mathcal{A}|} \leq K.$$

Thus, by Lemma 2.3 applied to $C = n\mathcal{B}$, we have for any integer $n \geq 0$

$$\frac{|\mathcal{X}+(n+1)\mathcal{B}|}{|\mathcal{X}+n\mathcal{B}|} \leq K.$$

Therefore, by induction we find $|\mathcal{X}+n\mathcal{B}| \leq K^n|\mathcal{X}|$. Finally, applying Lemma 2.1 we have

$$|m\mathcal{B} - n\mathcal{B}| \leq \frac{|\mathcal{X}+n\mathcal{B}||\mathcal{X}+m\mathcal{B}|}{|\mathcal{X}|} \leq K^{m+n}|\mathcal{X}| \leq K^{m+n}|\mathcal{A}|. \qquad \square$$

LEMMA 2.5 (GAPs in sumsets and small doubling means contained in a GAP). *Let $|2\mathcal{A}| \leq K|\mathcal{A}|$ and $Q \subseteq \ell\mathcal{A} - \ell\mathcal{A}$ be a generalised arithmetic progression of dimension d and size $|\mathcal{A}|/S$.*

Then there is a constant $C = C(K, d, S, \ell)$ such that $\mathcal{A}$ is contained in a generalised arithmetic progression of dimension at most C and size at most $C|\mathcal{A}|$.

PROOF. Since $Q \subseteq \ell\mathcal{A} - \ell\mathcal{A}$, we have $Q + \mathcal{A} \subseteq (\ell+1)\mathcal{A} - \ell\mathcal{A}$. Thus, by Lemma 2.4

$$|Q+\mathcal{A}| \leq |(\ell+1)\mathcal{A} - \ell\mathcal{A}| \leq K^{2\ell+1}|\mathcal{A}| \leq SK^{2\ell+1}|\mathcal{Q}|.$$

Thus, by Lemma 2.2, there is a set $\mathcal{X} \subseteq \mathcal{A}$ such that $|\mathcal{X}| \leq SK^{2\ell+1}$ and $\mathcal{A} \subseteq \mathcal{X} + Q - Q$.

By using two elements in each direction, $\mathcal{X}$ is contained in a generalised arithmetic progression of dimension $|\mathcal{X}| - 1$ and size $2^{|\mathcal{X}|-1}$. Since Q is a generalised arithmetic progression with dimension d and size $\leq |\ell\mathcal{A} - \ell\mathcal{A}| \leq K^{2\ell}|\mathcal{A}|$, we see that $Q - Q$ is a generalised arithmetic progression with dimension d and volume at most $2^d K^{2\ell}|\mathcal{A}|$. Thus $\mathcal{A} \subseteq \mathcal{X} + Q - Q$ is contained in a generalised arithmetic progression of dimension at most

$$d + |\mathcal{X}| - 1 \leq d + SK^{2\ell+1}$$

and size at most

$$2^{|\mathcal{X}|-1+d}K^{2\ell}|\mathcal{A}| \leq 2^{d+SK^{2\ell+1}}K^{2\ell}|\mathcal{A}|. \qquad \square$$

LEMMA 2.6 (Cauchy-Davenport). *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}/q\mathbb{Z}$. If $0 \in \mathcal{B}$ and for all $b \in \mathcal{B}\backslash\{0\}$ we have $(b, q) = 1$, then we have*

$$|\mathcal{A} + \mathcal{B}| \geq \min\Big(q, |\mathcal{A}| + |\mathcal{B}| - 1\Big).$$

PROOF. The result is trivial if $|\mathcal{A}| = q$, so assume $|\mathcal{A}| < q$. We prove the result by induction on $s = |\mathcal{B}|$; the case $s = 1$ is trivial. Assume that the result holds whenever $|\mathcal{B}| < s$. We claim that $\mathcal{A} + \mathcal{B} \neq \mathcal{A}$. Indeed, if $\mathcal{A} + b = \mathcal{A}$ for some $b \in \mathcal{B}\backslash\{0\}$ then

$$\sum_{a\in\mathcal{A}}(a + b) = \sum_{a\in\mathcal{A}} a \pmod q,$$

which implies that $|\mathcal{A}|b = 0 \pmod q$, which is impossible since $|\mathcal{A}| < q$ and $(b, q) = 1$. Therefore there is an $a_0 \in \mathcal{A}$ and $b_0 \in \mathcal{B}$ that $a_0 + b_0 \notin \mathcal{A}$. Let

$$\mathcal{B}_1 := \{b \in \mathcal{B} : b + a_0 \in \mathcal{A}\}, \qquad \mathcal{A}_1 := \mathcal{A} \cup \{a_0 + b : b \in \mathcal{B}, a_0 + b \notin \mathcal{A}\}.$$

Then $|\mathcal{A}_1| + |\mathcal{B}_1| = |\mathcal{A}| + |\mathcal{B}|$, $0 \in \mathcal{B}_1$ and $|\mathcal{B}_1| < |\mathcal{B}|$ since $b_0 \notin \mathcal{B}_1$. Moreover, we see that

$$\mathcal{A}_1 + \mathcal{B}_1 \subseteq \mathcal{A} + \mathcal{B}.$$

Thus the induction hypothesis now gives the result. □

CHAPTER 3

Equations in $\mathbb{Z}/q\mathbb{Z}$

DEFINITION (Discrete Fourier transform on $\mathbb{Z}/q\mathbb{Z}$). *Let $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$. Then we define the Fourier transform $\widehat{f} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ by*

$$\widehat{f}(m) := \frac{1}{q} \sum_{a \in \mathbb{Z}/q\mathbb{Z}} f(a)e(-am/q),$$

where $e(x) := e^{2\pi i x}$, noting that (with some abuse of notation) $x \to e(x/q)$ can be viewed as a well-defined function on $\mathbb{Z}/q\mathbb{Z}$.

LEMMA 3.1 (Properties of the discrete Fourier transform). *Let $f, g : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$.*

- *(Orthogonality of characters). For any $b \in \mathbb{Z}$ we have*
$$\frac{1}{q} \sum_{a \pmod q} e(ab/q) = \begin{cases} 1, & \text{if } b \equiv 0 \pmod q, \\ 0, & \text{otherwise.} \end{cases}$$
- *(Inversion formula). We have*
$$f(x) = \sum_{a \pmod q} \widehat{f}(a)e(ax/q).$$
- *(Parseval).*
$$\sum_{x \pmod q} f(x)\overline{g(x)} = q \sum_{a \pmod q} \widehat{f}(a)\overline{\widehat{g}(a)}.$$
- *(Convolutions). Let $h(x) := \sum_{a+b=x \pmod q} f(a)g(b)$. Then*
$$\widehat{h}(a) = q\widehat{f}(a)\widehat{g}(a).$$

PROOF. These all follow quickly from the definitions. If $b \equiv 0 \pmod q$ then $e(ab/q) = 1$ for all a, so the result is trivial in this case. If $b \not\equiv 0 \pmod q$ we can sum the geometric series

$$\sum_{a \pmod q} e(ab/q) = \frac{e(ab) - 1}{e(b) - 1} = 0$$

since $e(ab) = 1$.

Using the above formula, by expanding the definition of $\widehat{f}$ and swapping the order of summation

$$\sum_{a \pmod q} \widehat{f}(a)e(ax/q) = \frac{1}{q}\sum_{a,b \pmod q} f(b)e(a(x-b)/q)$$
$$= \sum_{b \pmod q} f(b)\mathbf{1}_{b\equiv x \pmod q} = f(x).$$

Using the inversion formula, we have

$$\sum_x f(x)\overline{g(x)} = \sum_{a,b,x} \widehat{f}(a)\widehat{\overline{g}}(b)e\Big(\frac{x(b+a)}{q}\Big).$$

By orthogonality of characters, the x sum vanishes unless $a = -b \pmod q$. Thus this is equal to

$$q\sum_a \widehat{f}(a)\widehat{\overline{g}}(-a).$$

We then note that $\widehat{\overline{g}}(-a) = \overline{\widehat{g}(a)}$ from the definition.

Substituting the definitions

$$\widehat{h}(a) = \frac{1}{q}\sum_b \sum_{c+d=b} f(c)g(d)e(-ab/q) = \frac{1}{q}\sum_{c,d} f(c)g(d)e(-ac/q)e(-ad/q)$$
$$= q\widehat{f}(a)\widehat{g}(a).$$

□

Definition (Pseudorandom functions and sets).

- *Given a set $\mathcal{A} \subseteq \mathbb{Z}/q\mathbb{Z}$, the* balanced function *of $\mathcal{A}$ is the function*
$$f_{\mathcal{A}}(x) = \mathbf{1}_{x\in\mathcal{A}} - \frac{|A|}{q}.$$
- *Given a constant $\eta > 0$, a 1-bounded function $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is called* η-pseudorandom *if $|\widehat{f}(m)| \le q^{-\eta}$ for all $m \in \mathbb{Z}/q\mathbb{Z}$.*
- *A set $\mathcal{A} \subseteq \mathbb{Z}/q\mathbb{Z}$ is called η-pseudorandom if the balanced function $f_{\mathcal{A}}(m)$ is* η-pseudorandom.

Note: Much of the above notation, in particular the notation of 'η-pseudorandom' is not standard in the wider literature. There is a somewhat arbitrary choice of normalisation for the Fourier transform, so elsewhere it is sometimes defined as $\widehat{f}(a) = \sum_b f(a)e(-ba/q)$ without the $1/q$ factor.

Proposition 3.2 (Solutions to equations in pseudorandom sets). *Let $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$. Then we have for any $x \in \mathbb{Z}/q\mathbb{Z}$*

$$\Big|\sum_{a_1+\cdots+a_k=x} f(a_1)\cdots f(a_k) - q^{k-1}\widehat{f}(0)^k\Big| \le q^{k-1}\sum_{b\neq 0 \pmod q} |f(b)|^k.$$

In particular, if $\mathcal{A}$ is an η-pseudorandom set, then

$$\Big|\#\Big\{a_1,\dots,a_k\in\mathcal{A}:\ a_1+\cdots+a_k=x\Big\}-\frac{|\mathcal{A}|^k}{q}\Big|\le q^{k-k\eta}.$$

PROOF. By orthogonality of characters, the left hand side is

$$\begin{aligned}\sum_{a_1,\dots,a_k} f(a_1)\dots f(a_k)\frac{1}{q}\sum_{b\pmod q} e\Big(\frac{b(x-a_1-\cdots-a_k)}{q}\Big)&\\ =\frac{1}{q}\sum_{b\pmod q} e(bx/q)\Big(\sum_a f(a)e(-ab/q)\Big)^k&\\ =q^{k-1}T\sum_{b\pmod q} e(bx/q)\widehat{f}(b)^k.&\end{aligned}$$

We separate out the term $b=0$ which contributes $q^{k-1}\widehat{f}(0)^k$, giving

$$q^{k-1}\frac{\widehat{f}(0)^k}{q}+q^{k-1}\sum_{\substack{b\pmod q\\ b\neq 0}} e(bx/q)\widehat{f}(b)^k.$$

The triangle inequality now gives the first result.

For the second result, we apply the above with $f(a)=\mathbf{1}_{a\in\mathcal{A}}$. We note that $\widehat{f}(0)=|\mathcal{A}|/q$ and

$$\widehat{f}(b)=\frac{1}{q}\sum_{a\pmod q} f_{\mathcal{A}}(a)e(ab/q)+\frac{|A|}{q^2}\sum_{a\pmod q} e(ab/q).$$

When $b\neq 0\pmod q$ the second term is 0 by orthogonality of characters. The first term is $\widehat{f_{\mathcal{A}}}(b)$. Thus we find that

$$\begin{aligned}\Big|\#\Big\{a_1,\dots,a_k\in\mathcal{A}:\ a_1+\cdots+a_k=x\Big\}-\frac{|\mathcal{A}|^k}{q}\Big|&\le q^{k-1}\sum_{\substack{b\pmod q\\ b\neq 0}}\Big|\widehat{f_{\mathcal{A}}}(b)\Big|^k\\ &\le q^k\sup_{b\pmod q}|f_{\mathcal{A}}(b)|^k.\end{aligned}$$

Clearly if $\mathcal{A}$ is η-pseudorandom then $|f_{\mathcal{A}}(b)|<q^{-\eta}$ which gives the result. □

LEMMA 3.3 (Squares are pseudorandom $\pmod q$). *If $(a,q)=1$ then*

$$\Big|\sum_{b\pmod q} e(ab^2/q)\Big|\le\begin{cases}\sqrt{q}, & 2\nmid q,\\ \sqrt{2q}, & 2|q.\end{cases}$$

PROOF. We square the sum in question, expand, and write $x_2 = x_1 + h$. This gives

$$\Big|\sum_{b \pmod q} e(ab^2/q)\Big|^2 = \sum_{x_1,x_2 \pmod q} e\Big(\frac{a(x_1^2 - x_2^2)}{q}\Big)$$
$$= \sum_{h \pmod q} \sum_{x_1 \pmod q} e\Big(\frac{2ahx_1 + ah^2}{q}\Big).$$

By orthogonality of characters, the inner sum vanishes unless $2ah = 0 \pmod q$. Since $(a, q) = 1$, this implies that $2h = 0 \pmod q$. Thus there are at most 2 choices of $h \pmod q$ if $2|q$ and one choice of $2 \nmid q$. Thus we obtain the bound

$$q \sum_{\substack{h \pmod q \\ 2h \equiv 0 \pmod q}} e\Big(\frac{ah^2}{q}\Big) \le \begin{cases} 2q, & 2|q \\ q & 2 \nmid q \end{cases}. \qquad \square$$

COROLLARY 3.4 (Representations as sums of squares $\pmod q$). *Let q be odd. Then every residue class $a \pmod q$ can be represented as a sum of three squares $\pmod q$.*

(There are easier ways of proving this, but we use it to demonstrate the basic method.)

PROOF. By the Chinese remainder theorem, it suffices to show the result for q being a prime power p^j. First, using the Proposition with

$$f(x) = \#\{b \pmod q : b^2 \equiv x\},$$

we find for any $x \in \mathbb{Z}/q\mathbb{Z}$

$$\Big|\#\{a_1^2 + a_2^2 + a_3^2 = x \pmod q\} - q^2\Big| \le \frac{1}{q} \sum_{\substack{a \pmod q \\ a \neq 0}} |\widehat{f}(a)|^3.$$

We then see that, using Lemma 3.3, if p is odd then

$$\frac{1}{q} \sum_{\substack{a \pmod q \\ a \neq 0}} \Big|\sum_{x \pmod q} e(ax^2/q)\Big|^3 \le \frac{1}{q} \sum_{1<d|q} d\frac{p-1}{p} \sup_{\substack{a \pmod d \\ (a,d)=1}} \Big(\frac{q}{d}\Big| \sum_{x \pmod d} e(ax^2/d)\Big|\Big)^3$$
$$\le q^2 \frac{p-1}{p} \sum_{1<d|q} \frac{1}{d^{1/2}}$$
$$\le \frac{q^2(p-1)}{p(p^{1/2}-1)}.$$

Thus the number of solutions is at least

$$q^2 - \frac{q^2(p-1)}{p(p^{1/2}-1)} > 0$$

for $p \ge 3$. $\square$

LEMMA 3.5 (Polynomial values are pseudorandom $\pmod q$). *Let $P(x) \in \mathbb{Z}/q\mathbb{Z}[x]$ be a polynomial of degree d with leading coefficient a. Then*

$$\Big|\sum_{b \pmod q} e(P(b)/q)\Big| \le 2^{\omega(q)}(q, d!a_0)^{1/2^{d-1}} q^{1-1/2^{d-1}}.$$

PROOF. We prove the result by induction. The statement holds for $d = 2$ by Lemma 3.3. Assume the statement holds for all polynomials of degree less than $d \ge 3$. We square the sum, and write $b_2 = b_1 + h$. This gives

$$\Big|\sum_{b \pmod q} e(P(b)/q)\Big|^2 = \sum_{b_1,b_2 \pmod q} e\Big(\frac{P(b_2) - P(b_1)}{q}\Big) = \sum_{b_1,h} e\Big(\frac{Q_h(b_1)}{q}\Big)$$

where $Q_h(b_1) = P(b_1 + h) - P(b_1)$ is a polynomial in b_1 of degree $d - 1$, with lead coefficient $a_0 hd$. Thus, by the induction hypothesis

$$\sum_{b_1} e\Big(\frac{Q_h(b_1)}{q}\Big) \le 2^{\omega(q)}(d!ah, q)^{1/2^{d-2}} q^{1-1/2^{d-2}}.$$

We now sum this over all $h \pmod q$, giving a bound

$$\begin{aligned}
&2^{\omega(q)}(d!a, q)^{1/2^{d-2}} q^{1-1/2^{d-2}} \sum_{h \pmod q} (h, q)^{1/2^{d-2}} \\
&\le 2^{\omega(q)}(d!a, q)^{1/2^{d-2}} q^{1-1/2^{d-2}} \sum_{e|q} e^{1/2^{d-2}} \phi(q/e) \\
&\le 2^{\omega(q)}(d!a, q)^{1/2^{d-2}} q^{2-1/2^{d-2}} \prod_{p|q} \Big(\frac{1 - 1/p}{1 - p^{1/2^{d-2}-1}}\Big).
\end{aligned}$$

We have that $(1 - 1/p)/(1 - p^{1/2^{d-2}-1}) \le (1 - 1/p)/(1 - 1/p^{1/2}) \le 2$ since $d \ge 3$. Thus the product is bounded by $2^{\omega(q)}$. This gives the bound

$$\Big|\sum_{b \pmod q} e(P(b)/q)\Big|^2 \le \Big(2^{\omega(q)}(d!a, q)^{1/2^{d-1}} q^{1-1/2^{d-1}}\Big)^2,$$

as required. □

LEMMA 3.6. *Let $k \ge 4d$ and*

$$N(m, q) := \#\{a_1, \dots, a_k \in \mathbb{Z}/q\mathbb{Z} : a_1^d + \cdots + a_k^d = m \pmod q\}.$$

Then for all m, q we have

$$N(m, q) \ge q^{k-4d}.$$

PROOF. By the Chinese remainder theorem, we have that $N(m, q_1q_2) = N(m, q_1)N(m, q_2)$ if $(q_1, q_2) = 1$. Therefore it suffices to prove the result for prime powers $q = p^j$. Let $\mathcal{B} = \{b^d \pmod{p^j} : (b, p) = 1\} \cup \{0\} \subseteq \mathbb{Z}/p^j\mathbb{Z}$. Since $(\mathbb{Z}/p^j\mathbb{Z})^\times$ is cyclic for $p > 2$

and $\cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{j-2}\mathbb{Z})$ if $p = 2$ and $j \geq 3$, we have

$$|\mathcal{B}| = \begin{cases} \frac{p^j(p-1)}{(d,p^j(p-1))}, & p > 2, \\ \frac{2^{j-2}}{(d,2^{j-2})}, & p = 2 \text{ and } j \geq 2 \text{ and } 2|d, \\ 2^{j-1}, & p = 2 \text{ and } (j = 1 \text{ or } 2 \nmid d). \end{cases}$$

Regardless, $|\mathcal{B}| - 1 \geq p^j/(4d)$. Now, by repeatedly applying Lemma 2.6 we find that for any integer r

$$|r\mathcal{B}| \geq \min(p^j, r(|\mathcal{B}| - 1)).$$

In particular, $4d\mathcal{B} = \mathbb{Z}/p^j\mathbb{Z}$, so every residue class $\pmod q$ can be represented as the sum of $4d$ d^{th} powers. We then see that by fixing the first $k - 4d$ variables in $N(p^j)$, we have that

$$\sum_{a_1,\dots,a_{k-4d} \pmod{p^j}} \#\{(b_1, \dots, b_{4d} \pmod{p^j} : b_1^d + \cdots + b_{4d}^d = m - a_1^d - \dots a_{k-4d}^d \pmod{p^j}\}$$
$$\geq (p^j)^{k-4d}. \qquad \square$$

PROPOSITION 3.7 (Sums of d^{th} powers modulo q). *Let $k > d2^{d+1}$ and*

$$N(m, q) := \#\{a_1, \dots, a_k \in \mathbb{Z}/q\mathbb{Z} : a_1^d + \cdots + a_k^d = m \pmod q\}.$$

Then for $0 \leq j_1 < j_2$ we have

$$\Big|\frac{N(m, p^{j_1})}{p^{j_1(k-1)}} - \frac{N(m, p^{j_2})}{p^{j_2(k-1)}}\Big| \leq 2^{k+1} p^{-j_1 k/2^d}.$$

In particular

$$\beta_p(m) = \lim_{j\to\infty} \frac{N(m, p^j)}{p^{j(k-1)}}$$

exists and $|\beta_p(m) - 1| \leq 2^{k+1} p^{-k/2^d}$ and $\beta_p(m) \geq p^{-d2^{d+3}}$.

PROOF. By Fourier inversion and then splitting the sum according to the gcd with p^j, we have that

$$\begin{aligned} N(m, p^j) &= \frac{1}{p^j} \sum_{b \pmod{p^j}} e\Big(\frac{mb}{p^j}\Big)\Big(\sum_{a \pmod{p^j}} e\Big(\frac{-a^d b}{p^j}\Big)\Big)^k \\ &= \frac{1}{p^j} \sum_{0\leq \ell \leq j} \sum_{\substack{b \pmod{p^j} \\ (b,p^j)=p^{j-\ell}}} e\Big(\frac{m(b/p^{j-\ell})}{p^\ell}\Big)\Big(p^{j-\ell} \sum_{a \pmod{p^\ell}} e\Big(\frac{-a^d(b/p^{j-\ell})}{p^\ell}\Big)\Big)^k \\ &= p^{j(k-1)} \sum_{0\leq \ell \leq j} \sum_{\substack{b' \pmod{p^\ell} \\ (b',p)=1}} e\Big(\frac{mb'}{p^\ell}\Big)\Big(p^{-\ell} \sum_{a \pmod{p^\ell}} e\Big(\frac{-a^d b'}{p^\ell}\Big)\Big)^k. \end{aligned}$$

Thus if $j_1 < j_2$

$$\Big|\frac{N(m,p^{j_1})}{p^{j_1(k-1)}} - \frac{N(m,p^{j_2})}{p^{j_1(k-1)}}\Big| \le \sum_{j_1<\ell\le j_2}\sum_{\substack{b' \pmod{p^\ell}\\(b',p)=1}} \Big|p^{-\ell}\sum_{a \pmod{p^\ell}} e\Big(\frac{-a^d b'}{p^\ell}\Big)\Big|^k.$$

By Lemma 3.5, the inner sum over a is bounded by $2(p^\ell)^{1-1/2^{d-1}}$. There are p^ℓ choices of b'. Thus we have

$$\Big|\frac{N(m,p^{j_1})}{p^{j_1(k-1)}} - \frac{N(m,p^{j_2})}{p^{j_1(k-1)}}\Big| \le \sum_{j_1<\ell\le j_2} 2^k p^{-\ell(k/2^{d-1}-1)} \le 2^{k+1}p^{-j_1(k/2^{d-1}-1)}.$$

Since the right hand side tends to 0 as $j_1, j_2 \to \infty$, the limit $\beta_p(m)$ exists. Using the inequality with $j_1 = 0$ $j_2 \to \infty$ gives the bound $|\beta_p(m) - 1| \le 2^{k+1}p^{-k/2^d}$. This automatically shows that $\beta_p(m) > 0$ for $p > 2^{2^d}$. For smaller p we use the main inequality with $j_2 \to \infty$ and Lemma 3.6 to give

$$\begin{aligned}\beta_p(m) \ge \frac{N(p^j)}{p^{j(k-1)}} - 2^{k+1}p^{-j(k/2^{d-1}-1)} &\ge \frac{p^{j(k-4d)}}{p^{j(k-1)}} - 2^{k+1}p^{-j(k/2^{d-1}-1)}\\ &\ge p^{j(1-4d)}\Big(1 - 2^{k+1}p^{-j(k/2^{d-1}-4d)}\Big).\end{aligned}$$

Since we have assumed $k \ge d2^{d+2}$, we see that $k/2^{d-1} - 4d \ge k/2^d$. Thus choosing $j = 2^d + 1$ gives

$$\beta_p(m) \ge p^{(2^d+1)(1-4d)}(1 - 2p^{-4d}) \ge p^{(2^d+1)(1-4d)}(1 - 2p^{-4d}) \ge p^{-d2^{d+3}}. \qquad \square$$

Corollary 3.8 (Waring's problem modulo p). *Let $k > d2^{d+1}$. Then we have that for any $m \in \mathbb{Z}/p\mathbb{Z}$*

$$\#\{a_1, \dots, a_k \in \mathbb{Z}/p\mathbb{Z} : a_1^d + \cdots + a_k^d = m \pmod p\} = p^{k-1} + O_k(p^{k-1-k/2^d}).$$

CHAPTER 4

Introduction to circle method

4.1. The Fourier Transform over $\mathbb{Z}$ and $\mathbb{R}$

We now generalise much of the previous chapter to the more complicated situation of equations over $\mathbb{Z}$

DEFINITION (Fourier transform on $\mathbb{Z}$). *Let $f : \mathbb{Z} \to \mathbb{C}$ be supported on $|x| < N$. Then we define the Fourier transform $\widehat{f} : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ by*

$$\widehat{f}(\theta) := \sum_{a \in \mathbb{Z}} f(a)e(-a\theta),$$

where $e(x) := e^{2\pi ix}$, noting that (with some abuse of notation) $x \to e(x)$ can be viewed as a well-defined function on $\mathbb{R}/\mathbb{Z}$.

LEMMA 4.1 (Properties of the integer Fourier transform). *Let $f, g : \mathbb{Z} \to \mathbb{C}$.*

- *(Orthogonality of characters). For any $b \in \mathbb{Z}$ we have*
$$\int_0^1 e(b\theta)d\theta = \begin{cases} 1, & \text{if } b = 0, \\ 0, & \text{otherwise.} \end{cases}$$
- *(Inversion formula). We have*
$$f(n) = \int_0^1 \widehat{f}(\theta)e(n\theta)d\theta.$$
- *(Parseval).*
$$\sum_{x \in \mathbb{Z}} f(x)\overline{g(x)} = \int_0^1 \widehat{f}(\theta)\overline{\widehat{g}(\theta)}d\theta.$$
- *(Convolutions). Let $h(x) := \sum_{a+b=x} f(a)g(b)$. Then*
$$\widehat{h}(\theta) = \widehat{f}(\theta)\widehat{g}(\theta).$$

PROOF. These all follow quickly from the definitions in an identical way to Lemma 3.1. If $b = 0$ then $e(b\theta) = 1$ for all θ, so the result is trivial in this case. If $b \neq 0$ we can integrate

$$\int_0^1 e(b\theta)d\theta = \frac{e(b) - 1}{2\pi i} = 0$$

since $e(b) = 1$.

Using the above formula, by expanding the definition of $\widehat{f}$ and swapping the order of summation and integration

$$\int_0^1 \widehat{f}(\theta)e(x\theta) = \sum_b f(b)\int_0^1 e(\theta(x-b))d\theta = f(x).$$

Using the definition, and orthogonality we have

$$\int_0^1 \widehat{f}(\theta)\overline{\widehat{g}(\theta)}d\theta = \sum_{a,b\in\mathbb{Z}} f(a)\overline{g(b)}\int_0^1 e(\theta(b-a))d\theta = \sum_{a\in\mathbb{Z}} f(a)\overline{g(a)}.$$

Subtituting the definitions

$$\begin{aligned}\widehat{h}(\theta) = \sum_b \sum_{c+d=b} f(c)g(d)e(-b\theta) &= \sum_{c,d} f(c)g(d)e(-c\theta)e(-d\theta)\\ &= \widehat{f}(\theta)\widehat{g}(\theta).\end{aligned}$$

□

Definition (Fourier transform on $\mathbb{R}$). *Let $f \in L^1(\mathbb{R})$. Then we define the Fourier transform $\widehat{f} : \mathbb{R} \to \mathbb{C}$ by*

$$\widehat{f}(\xi) := \int_{-\infty}^{\infty} f(u)e(-u\theta)du.$$

Lemma 4.2 (Properties of the real Fourier transform). *Let $f, g, fg \in L^1(\mathbb{R})$.*

- *(Inversion formula). If $\widehat{f}(\xi) \in L^1(\mathbb{R})$ and f is continuous at x, then*
$$f(x) = \int_{-\infty}^{\infty} \widehat{f}(\xi)e(x\xi)d\xi.$$
- *(Parseval). If $\widehat{f}\widehat{g} \in L^1(\mathbb{R})$ then*
$$\int_{-\infty}^{\infty} f(t)\overline{g(t)}dt = \int_{-\infty}^{\infty} \widehat{f}(\xi)\overline{\widehat{g}(\xi)}d\xi.$$
- *(Convolutions). Let $h(x) := \int_{-\infty}^{\infty} f(t)g(x-t)dt$. Then*
$$\widehat{h}(\xi) = \widehat{f}(\xi)\widehat{g}(\xi).$$

Proof. Non-examinable, see appendix. □

Note: As with the Fourier transform on $\mathbb{Z}/q\mathbb{Z}$, different authors use slightly different normalisations for their definition of the Fourier Transform. In some previous versions of the course (and in C3.8) the Fourier transfrom on $\mathbb{R}$ has been defined as $\widehat{f}(\xi) = \int_{\mathbb{R}} f(t)e^{-it\xi}dt$ which is $\widehat{f}(\xi/(2\pi))$ in our notation.

4.2. A warm-up example

It is a trivial combinatorial counting problem that if $N > m$ then

$$\#\{(x_1,\dots,x_k) \in \mathbb{Z}_{>0}^k : x_1+\cdots+x_k = m,\ |x_i| \le N\} = \binom{m+k-1}{k-1} = \frac{m^{k-1}}{(k-1)!} + O(m^{k-2}).$$

(We will view k as fixed and allow any implied constants to depend on k). We now reprove this in the spirit of the circle method, which generalises more readily to when the x_i lie in more complicated sets.

4.2.1. Using orthogonality. Let $f : \mathbb{Z} \to \mathbb{C}$ be given by $f(x) = \mathbf{1}_{1\leq x\leq N}$. Then the orthogonality relation

$$\int_0^1 e(\theta(m - x_1 - \cdots - x_n))d\theta = \begin{cases} 1, & \text{If } x_1 + \cdots + x_n = m, \\ 0, & \text{If } x_1 + \cdots + x_n - m \in \mathbb{Z}\backslash\{0\}. \end{cases}$$

gives

$$\begin{aligned} &\#\{(x_1, \dots, x_k) \in \mathbb{Z}_{>0}^k : x_1 + \cdots + x_k = m, |x_i| \leq N\} \\ &\qquad = \sum_{x_1,\dots,x_k} f(x_1) \cdots f(x_k)\mathbf{1}_{x_1+\cdots+x_k=m} \\ &\qquad = \sum_{x_1,\dots,x_k} f(x_1) \cdots f(x_k) \int_0^1 e(\theta(m - x_1 - \cdots - x_k))d\theta \\ &\qquad = \int_0^1 \widehat{f}(\theta)^k e(m\theta)d\theta. \end{aligned}$$

4.2.2. Splitting the integral according to the size of the Fourier transform. We see that since $|e(\theta) - 1| = 2|\sin(\pi\theta)| \geq \|\theta\|$

$$\widehat{f}(\theta) = \sum_{x=1}^{N} e(-x\theta) = \frac{e(-\theta(N + 1)) - 1}{e(-\theta) - 1} = O\Big(\frac{1}{\|\theta\|}\Big).$$

Therefore $\widehat{f}(\theta)$ is small unless θ is very close to 0 (mod 1). With this in mind we split the integral according to whether $\|\theta\| \leq \eta$ or not. We see that

$$\int_{\|\theta\|>\eta} \widehat{f}(\theta)^k e(m\theta)d\theta \ll \int_{\|\theta\|>\eta} \frac{d\theta}{\|\theta\|^k} \ll \frac{1}{\eta^{k-1}}.$$

When $\|\theta\| \leq \eta$

$$\widehat{f}(\theta) = \frac{e(-\theta(N + 1)) - 1}{e(-\theta) - 1} = \frac{e(-\theta(N + 1)) - 1}{-2\pi i\theta(1 + O(\eta))} = \int_0^{N+1} e(-\theta t)dt + O(\eta N).$$

Substituting this back in, we find

$$\begin{aligned} &\#\{(x_1, \dots, x_k) \in \mathbb{Z}_{>0}^k : x_1 + \cdots + x_k = m, |x_i| \leq N\} \\ &\qquad = \int_{|\theta|<\eta} e(m\theta)\Big(\int_0^{N+1} e(-\theta u)du\Big)^k d\theta + O(\eta^2 N^k) + O(\eta^{-(k-1)}). \end{aligned} \tag{4.1}$$

4.2.3. Understanding main term as a local factor. Ignoring the error terms, this is just an analytic integral only involving real numbers (and so just an analytic quantity with no number-theoretic properties). It essentially counts the

measure number of *real* solutions to the equation $u_1 + \cdots + u_k = m$. Indeed, since

$$\int_0^{N+1} e(-\theta u)du \ll \frac{1}{|\theta|}$$

we can extend the integral in (4.1) to $\theta \in \mathbb{R}$ at the cost of a $\eta^{-(k-1)}$ error term. But then, if $g(x) = \mathbf{1}_{x\in[0,N+1]}$ we see that the integral is given by

$$\int_{-\infty}^{\infty} e(m\theta)\widehat{g}(\theta)^k d\theta + O(\eta^{-(k-1)}).$$

We recall from Lemma 4.1 that

$$\underbrace{\widehat{(f * \cdots * f)}}_{k \text{ times}}(\xi) = \widehat{f}(\xi)^k, \qquad f(x) = \int_{-\infty}^{\infty} \widehat{f}(\xi)e(\xi x)d\xi$$

so we see that

$$\int_{-\infty}^{\infty} e(m\theta)\widehat{g}(\theta)^k d\theta = (g * \cdots * g)(m) = \int_{\substack{u_1,\ldots,u_k\in[0,N+1]\\ u_1+\cdots+u_k=m}} 1.$$

Thus, for any choice of $\eta > 0$ we have

$$\begin{aligned}\#\{(x_1,\ldots,x_k) \in \mathbb{Z}_{>0}^k : x_1 + \cdots + x_k = m,\, |x_i| \le N\}& \\ = \int_{\substack{u_1,\ldots,u_k\in[0,N+1]\\ u_1+\cdots+u_k=m}} 1 + O(\eta^2 N^k) + O(\eta^{-(k-1)}).&\end{aligned}$$

We can choose $\eta = N^{-k/(k+1)}$ to balance the error terms and obtain an asymptotic

$$\frac{m^{k-1}}{(k-1)!} + O(m^{k-2+2/(k+1)}).$$

If we instead counted solutions where $x_1, \ldots, x_k$ were all a multiple of a prime p, then there would only be solutions if m is a multiple of p. If now $f(x) = \mathbf{1}_{1\le x\le N,\, p|x}$ then

$$\widehat{f}(\theta) = \frac{e(-p\theta(\lfloor N/p\rfloor + 1) - 1}{e(-p\theta) - 1} = O\Big(\frac{1}{\|p\theta\|}\Big).$$

As before, we can discard $\|p\theta\| > \eta$ at the cost of a $O(\eta^{-(k-1)})$ error term. Now, however, we also have to take into acount values of θ near $1/p$, $2/p$ etc. This gives

$$\begin{aligned}&\#\{(x_1,\ldots,x_k) \in \mathbb{Z}_{>0}^k : x_1 + \cdots + x_k = m,\, |x_i| \le N\, p|x_i\} \\ &\qquad = \frac{1}{p}\sum_{a \pmod p} \int_{|\delta|<\eta} e\Big(m\Big(\frac{a}{p} + \delta\Big)\Big)\Big(\int_0^{N+1} e(-\delta u)du\Big)^k d\theta + O(\eta^2 N^k) + O(\eta^{-(k-1)}).\end{aligned}$$

The arithmetic fact that there are no solutions modulo p to the equation unless $p|m$ is now accounted for by the contribution from these other rationals. Indeed

the main term factorises as

$$\Big(\frac{1}{p}\sum_{a \pmod p} e(am/p)\Big)\Big(\int_{|\delta|<\eta} e(m\delta)\Big(\int_0^{N+1} e(-\delta u)du\Big)^k d\theta\Big)$$
$$= \Big(\frac{\#\{x_1+\cdots+x_k = m \pmod p\}}{p^{k-1}}\Big)\cdot \int_{\substack{u_1,\dots,u_k\in[0,N+1]\\ u_1+\cdots+u_k=m}} 1.$$

Therefore now the main term is a product of the density of solutions $\pmod p$ and the density of solutions over $\mathbb{R}$.

4.3. The circle method

By Fourier inversion, we have that for any function $f : \mathbb{Z} \to \mathbb{C}$ with compact support

$$\sum_{a_1+\cdots+a_k=n} f(a_1)\cdots f(a_k) = \int_0^1 e(-n\theta)\widehat{f}(\theta)^k d\theta.$$

If $\widehat{f}(\theta)$ is small for all θ, this shows that the weighted count of solutions is small (which is what we would expect if f looked like a random ± 1 function, for example). However, it is less clear how to extract a 'main term' when f is the indicator function of a set. The Hardy-Littlewood *circle method* splits the integral in 'major arcs' $\mathfrak{M}$ where the Fourier transform is large, and 'minor arcs' $\mathfrak{m} = [0,1]\backslash\mathfrak{M}$ where the Fourier transform is small. Although the precise choice of $\mathfrak{M}$ can vary depending on the situation, in most number-theoretic applications the most natural choice depends on Diophantine properties of θ. In this case, the major arc contribution is essentially a product of densities of solutions in all places.

CHAPTER 5

Waring's Problem

The aim of this chapter is to establish

THEOREM 5.1 (Asymptotic formula for the number of representations as the sum of k d^{th} powers). *Let $k \geq 20d2^d$. Then we have*

$$\#\{n_1^d + \cdots + n_k^d = m\} = m^{k/d-1}\Big(\beta_\infty(m)\prod_p \beta_p(m) + O(m^{-1/2d})\Big).$$

where $\beta_\infty(m)\prod_p \beta_p(m)$ converges to a constant, which is bounded away from 0 uniformly in m. In particular, every sufficiently large integer can be written as the sum of $20d2^d$ positive d^{th} powers, and there is a number $g(d)$ such that every integer can be represented by at most $g(d)$ d^{th} powers

Rather better bounds are known in this problem; we can get the same asymptotic formula when $k \geq d^2$, and the fact that there exists at least one representation for large integers occurs when $k > d\log d + 5d$. If we wish to represent *every* integer then $2^d\lfloor(3/2)^d\rfloor - 1$ requires at least $2^d + \lfloor(3/2)^d\rfloor - 2$, and it is known that every integer can be expressed as essentially this many d^{th} powers.

PROPOSITION 5.2 (Major arc contribution). *Let $k \geq d2^{d+2}$, $N \geq m^{1/d}$, $Q \geq 1$ and $\mathfrak{M}$ be given by*

$$\mathfrak{M} = \bigcup_{q\leq Q}\bigcup_{(a,q)=1}\Big[\frac{a}{q} - \frac{Q}{N^d}, \frac{a}{q} + \frac{Q}{N^d}\Big].$$

Then we have

$$\int_{\mathfrak{M}}\Big(\sum_{n\leq N} e(\theta n^d)\Big)^k e(-m\theta)d\theta = m^{k/d-1}\beta_\infty(m)\prod_p \beta_p(m) + O\Big(N^{k-d}\Big(\frac{Q^5}{N} + \frac{1}{Q^{k/2^{d-1}-2}}\Big)\Big),$$

where

$$\beta_p(m) := \lim_{j\to\infty}\frac{\#\{b_1,\ldots,b_k \pmod{p^j} : b_1^d + \cdots + b_k^d = m \pmod{p^j}\}}{p^{j(k-1)}},$$

$$\beta_\infty(m) := \frac{\Gamma(1+1/d)^k}{\Gamma(k/d)},$$

and $\beta_\infty(m)\prod_p \beta_p(m)$ converges to a positive constant bounded away from 0 uniformly in m.

PROPOSITION 5.3 (Minor arc contribution). *Let $\mathfrak{m} = [0,1]\backslash\mathfrak{M}$. Then for $Q \le N$ we have*

$$\int_{\mathfrak{m}} \Big|\sum_{n\le N} e(\theta P(n))\Big|^k d\theta \ll \frac{N^{k+o(1)}}{Q^{k/2^d}}.$$

PROOF OF THEOREM 5.1 ASSUMING PROPOSITION 5.2 AND PROPOSITION 5.3. Using orthogonality (Lemma 4.1 we have

$$\#\{n_1^d + \cdots + n_k^d = m,\ 0 \le n_i \le N\} = \int_0^1 \Big(\sum_{n\le N} e(\theta n^d)\Big)^k e(-m\theta) d\theta.$$

Let $\mathfrak{M}$ be as given in Proposition 5.2, and $\mathfrak{m} = [0,1]\backslash\mathfrak{M}$ as in Proposition 5.3. Then, splitting the integral according to whether $\theta \in \mathfrak{M}$ or not, the above is equal to

$$\int_{\mathfrak{M}} \Big(\sum_{n\le N} e(\theta n^d)\Big)^k e(-m\theta) d\theta + \int_{\mathfrak{m}} \Big(\sum_{n\le N} e(\theta n^d)\Big)^k e(-m\theta) d\theta.$$

Applying Propostion 5.2 to estimate the first integral and Proposition 5.3 to bound the second one, we find that for $k > d2^{d+2}$ this is

$$m^{k/d-1}\beta_\infty(m)\prod_p \beta_p(m) + O\Big(N^{k-d}\Big(\frac{Q^5}{N} + \frac{1}{Q^{k/2^{d-1}-2}} + \frac{N^d}{Q^{k/2^d}}\Big)\Big).$$

We now choose $N = m^{1/d}$, $Q = N^{1/10}$, and see that for $k \ge 20d2^d$ the error term is $O(m^{k/d-1-1/2d})$ which is much smaller than $m^{k/d-1}$. Thus we have

$$\#\{n_1^d + \cdots + n_k^d = m\} = m^{k/d-1}\Big(\beta_\infty(m)\prod_p \beta_p(m) + O(m^{-1/2d})\Big). \qquad \square$$

Thus we are left to establish Proposition 5.2 and Proposition 5.3.

5.1. Major Arcs for Waring's problem

LEMMA 5.4 (Polynomial exponential sum when close to a rational with small denominator). *Let $\theta = a/q + \epsilon$ and $P(x) \in \mathbb{Z}[x]$ be an integer polynomial of degree d. Then we have*

$$\sum_{n\le N} e(\theta P(n)) = \Big(\frac{1}{q}\sum_{b \pmod q} e(aP(b)/q)\Big)\Big(\int_0^N e(\epsilon P(u))du\Big) + O(q\epsilon N^d).$$

PROOF. We note that $e(aP(n)/q)$ only depends on the residue class $n \pmod q$. Therefore, splitting into residue classes

$$\sum_{n\in[N,2N]} e(\theta P(n)) = \sum_{b \pmod q} e(aP(b)/q) \sum_{\substack{n\in[N,2N]\\ n\equiv b \pmod q}} e(\epsilon P(n)).$$

Since ϵ is small, $e(\epsilon P(n))$ only really depends on the rough size of $P(n)$, and so we can approximate the sum by an integral. Since P has degree d, we see that

$|P'(t)| = O(N^{d-1})$ for $|t| \le N$. Thus, if $|u-v| \le q$ and $u, v \le N$ then

$$|P(v) - P(u)| \le |v-u| \sup_{|t|\le N} P'(t) = O(qN^{d-1}).$$

Therefore, for $b \le q$, $b + rq \le 2N$

$$\begin{aligned}\Big|e(\epsilon P(b+rq)) - \frac{1}{q}\int_{rq}^{(r+1)q} e(\epsilon P(u))du\Big| &\le \sup_{u\in[rq,(r+1)q]}\Big|2\pi i\epsilon\int_{P(u)}^{P(b+rq)} e(\epsilon t)dt\Big| \\ &= O(\epsilon q N^{d-1}).\end{aligned}$$

Thus

$$\sum_{n\in[N,2N]} e(\theta P(n)) = \Big(\frac{1}{q}\sum_{b \pmod q} e(aP(b)/q)\Big)\Big(\int_N^{2N} e(\epsilon P(u))du\Big) + O(\epsilon q N^d). \quad \square$$

LEMMA 5.5 (Completion of local factors). *Let $k > 2^d$ and $\mathfrak{M}$ be as in Proposition 5.2. Then we have*

$$\int_{\mathfrak{M}}\Big(\sum_{n\le N} e(\theta n^d)\Big)^k e(-m\theta)d\theta = \mathfrak{S}(m)J(m) + O\Big(N^{k-d}\Big(\frac{Q^5}{N} + \frac{1}{Q^{k/2^{d-1}-2}}\Big)\Big),$$

where

$$\begin{aligned}\mathfrak{S}(m) &:= \sum_q \sum_{(a,q)=1}\Big(\frac{1}{q}\sum_{b \pmod q} e(ab^d/q)\Big)^k e(-am/q), \\ J(m) &:= \int_{-\infty}^{\infty}\Big(\int_{u\le N} e(-vu^d)du\Big)^k e(vm)dv.\end{aligned}$$

PROOF. By Lemma 5.4, we have for $\theta \in \mathfrak{M}$

$$\Big(\sum_{n\le N} e(\theta n^d)\Big)^k = \Big(\frac{1}{q}\sum_{b \pmod q} e(ab^d/q)\Big)^k\Big(\int_0^N e(\epsilon u^d)du\Big)^k + O(Q^2N^{k-1}).$$

We note that the measure of $\mathfrak{M}$ is $O(Q^3/N^d)$, so the error term contributes a total $O(Q^5N^{k-d-1})$ to the integral. The first factor depends on a, q but not on ϵ, whereas the second factor depends only on ϵ. Thus

$$\int_{\mathfrak{M}}\Big(\sum_{n\le N} e(\theta n^d)\Big)^k e(-m\theta)d\theta = \mathfrak{S}^*(m;Q)J^*(m,Q) + O(Q^5N^{k-d-1}),$$

where

$$\begin{aligned}\mathfrak{S}^*(m;Q) &:= \sum_{1\le q\le Q}\sum_{(a,q)=1}\Big(\frac{1}{q}\sum_{b \pmod q} e(ab^d/q)\Big)^k e(-am/q), \\ J^*(m,Q) &:= \int_{-Q/N^d}^{Q/N^d}\Big(\int_{u\le N} e(\epsilon u^d)du\Big)^k e(-\epsilon m)d\epsilon.\end{aligned}$$

We first concentrate on the arithmetic piece $\mathfrak{S}(m,Q)$. By Lemma 3.5 we have

$$\sum_{(a,q)=1}\Big(\frac{1}{q}\sum_{b\pmod q} e(ab^d/q)\Big)^k \ll q^{1-k/2^{d-1}}.$$

Therefore, since $k>2^d$, we can extend the sum to all q at the cost of a correction term of size $Q^{2-k/2^{d-1}}$. This gives

$$\mathfrak{S}^*(m,Q)=\mathfrak{S}(m)+O(Q^{2-k/2^{d-1}}).$$

We now wish to similarly approximate the Archimedean factor $J^*(m,Q)$ with $J(m)$. We first note that, by letting $v=\epsilon u^d$

$$\int_{u\le N} e(\epsilon u^d)du=\frac{1}{d\epsilon^{1/d}}\int_0^{\epsilon N^d} v^{1/d-1}e(v)\ll\frac{1}{\epsilon^{1/d}}.$$

We can therefore extend the integration in $J^*(m,Q)$ to all of $\mathbb{R}$ at the cost of an error term of size

$$\ll\int_{|\epsilon|>Q/N^d}\frac{d\epsilon}{|\epsilon|^{k/d}}\ll\frac{N^{k-d}}{Q^{k/d-1}}.$$

Thus

$$J^*(m,Q)=J(m)+O\Big(\frac{N^{k-d}}{Q^{k/d-1}}\Big).$$

Putting these estimates together (alongside the trivial bounds $J^*(m,Q)\ll N^{k-d}$ and $\mathfrak{S}(m,Q)\ll Q^2$) then gives the result. □

LEMMA 5.6 (Singular series). *For each prime p, let*

$$\beta_p(m)=\lim_{j\to\infty}\frac{\#\{b_1,\dots,b_k \pmod{p^j} : b_1^d+\cdots+b_k^d=m \pmod{p^j}\}}{p^{j(k-1)}}$$

as in Proposition 3.7. Then we have

$$\mathfrak{S}(m)=\prod_p\beta_p(m)$$

which converges to a positive real number which is lower bounded uniformly in m.

PROOF. If $q=p_1^{e_1}\cdots p_j^{e_j}$ then, by the Chinese remainder theorem, we have

$$\sum_{(a,q)=1}\Big(\frac{1}{q}\sum_{b\pmod q}e\Big(\frac{ab^d}{q}\Big)\Big)^k e\Big(\frac{-am}{q}\Big)$$
$$=\prod_{i=1}^{j}\sum_{\substack{a_i\pmod{p_i^{e_i}}\\(a_i,p_i)=1}}\Big(\frac{1}{p_i^{e_i}}\sum_{b\pmod{p_i^{e_i}}}e\Big(\frac{a_ib^d}{p_i^{e_i}}\Big)\Big)^k e\Big(\frac{-a_im}{p_i^{e_i}}\Big).$$

Letting $q_i = p_i^{e_i}$, the sum over a_i is

$$\sum_{a_i \pmod{q_i}} \Big(\frac{1}{q_i} \sum_{b \pmod{q_i}} e\Big(\frac{a_i b^d}{q_i}\Big)\Big)^k e\Big(\frac{-a_i m}{q_i}\Big) - \sum_{\substack{a_i \pmod{q_i} \\ p_i | a_i}} \Big(\frac{1}{q_i} \sum_{b \pmod{q_i}} e\Big(\frac{a_i b^d}{q_i}\Big)\Big)^k e\Big(\frac{-a_i m}{q_i}\Big).$$

Expanding out and using orthogonality (mod q_i), the first sum above is

$$\frac{1}{q_i^k} \sum_{b_1,\dots,b_k \pmod{q_i}} \sum_{a_i \pmod{q_i}} e\Big(\frac{a_i(b_1^d + \dots b_k^d - m)}{q_i}\Big) = \frac{N(q_i)}{q_i^{k-1}},$$

where

$$N(q) := \#\{b_1, \dots, b_k \pmod q : b_1^d + \dots + b_k^d = m \pmod q\}.$$

Similarly, the second term is $-N(q_i/p_i)/(q_i/p_i)^{k-1}$. Thus we find

$$\sum_{(a,q)=1} \Big(\frac{1}{q} \sum_{b \pmod q} e\Big(\frac{ab^d}{q}\Big)\Big)^k e\Big(\frac{-am}{q}\Big) = \prod_{i=1}^{j} \Big(\frac{N(q_i)}{q_i^{k-1}} - \frac{N(q_i/p_i)}{(q_i/p_i)^{k-1}}\Big).$$

We note that by the Chinese Remainder Theorem that $N(q_1 q_2) = N(q_1)N(q_2)$ if q_1, q_2 are coprime, so the above expression is multiplicative in q. Thus, summing over all q we obtain

$$\sum_{q} \sum_{(a,q)=1} \Big(\frac{1}{q} \sum_{b \pmod q} e\Big(\frac{ab^d}{q}\Big)\Big)^k e\Big(\frac{-am}{q}\Big) = \prod_{p} \Big(1 + \sum_{j \geq 1} \big(\frac{N(p^j)}{p^{j(k-1)}} - \frac{N(p^{j-1})}{p^{(j-1)(k-1)}}\big)\Big)$$

(we note that these expressions converge absolutely thanks to Proposition 3.7). Since the inner sum telescopes and converges, we see that

$$1 + \sum_{j \geq 1} \Big(\frac{N(p^j)}{p^{j(k-1)}} - \frac{N(p^{j-1})}{p^{(j-1)(k-1)}}\Big) = \lim_{j \to \infty} N(p^j) = \beta_p(m).$$

Thus

$$\mathfrak{S}(m) = \prod_p \beta_p(m).$$

Again, the absolute convergence follows from $|\beta_p(m) - 1| \leq 2^{k+1} p^{-k/2^d}$ by Proposition 3.7. Indeed, alongside $\beta_p(m) \geq p^{-d2^{d+1}}$, this shows the uniform lower bound

$$\mathfrak{S}(m) \geq \prod_{p \leq 2^{2^d}} \Big(\frac{1}{p^{d2^{d+3}}}\Big) \prod_{p > 2^{2^d}} \Big(1 - \frac{2^{k+1}}{p^{k/2^d}}\Big). \qquad \square$$

LEMMA 5.7 (Singular Integral). *Let $N \geq m^{1/d}$. Then we have*

$$J(m) = \int_{\substack{u_1,\dots,u_k \in [0, m^{1/d}] \\ u_1^d + \dots + u_k^d = m}} 1 = \frac{\Gamma(1 + 1/d)^k}{\Gamma(k/d)} m^{k/d - 1}.$$

Here the integral above is interpreted as with respect to the $(k-1)$ dimensional measure induced from $du_1 \dots du_k$, and $\Gamma(z) := \int_0^\infty x^{z-1} e^{-x} dx$ is the Gamma function.

PROOF. Let $f(u) = d^{-1}u^{1/d-1}\mathbf{1}_{0\le u\le N}$. Then, by a change of variables $v_i = u_i^d$

$$\int_{\substack{u_1,\dots,u_k\in[0,N]\\ u_1^d+\cdots+u_k^d=m}} du_1\dots du_{k-1} = \int_{\substack{v_1,\dots,v_k\in[0,N^d]\\ v_1+\cdots+v_k=m}} \frac{(v_1\cdots v_k)^{1/d-1}}{d^k} dv_1\dots dv_k$$
$$= (f*\cdots*f)(m).$$

We see from Lemma 4.1 and integration by parts that the Fourier transform is given by

$$\widehat{f}(\xi) = \frac{1}{d}\int_0^{N^d} v^{1/d-1}e(-\xi v)dv = \frac{1}{d\xi^{1/d}}\int_0^{\xi N^d} v^{1/d-1}e(-v)dv \ll \frac{1}{\xi^{1/d}},$$
$$\widehat{(f*\cdots*f)}(\xi) = \widehat{f}(\xi)^k \ll \frac{1}{|\xi|^{k/d}}.$$

Therefore, by Fourier inversion we have

$$(f*\cdots*f)(m) = \int_{-\infty}^{\infty} e(m\xi)\widehat{f}(\xi)^k d\xi = J(m).$$

We now show that this integral is $\frac{\Gamma(1+1/d)^k}{\Gamma(k/d)}n^{k-d}$ by induction on k. Letting $w_i = v_i/m^{1/d}$ we see that

$$J(m) = m^{k/d-1}\int_{\substack{w_1,\dots,w_k\in[0,1]\\ w_1+\cdots+w_k=1}} \frac{dw_1\dots dw_{k-1}}{d^k w_1^{1-1/d}\cdots w_k^{1-1/d}}.$$

Thus $J(m) = m^{k/d-1}C(k,d)$ for some positive constant $C(k,d)$. It isn't really important for us what this is, but Lemma B.2 shows that this constant is

$$\frac{\Gamma(1/d)^k}{d^k\Gamma(k/d)} = \frac{\Gamma(1+1/d)^k}{\Gamma(k/d)}.$$ □

5.2. Minor Arcs for Waring's problem

LEMMA 5.8 (Fractional parts can't be small too often). *Let $|\theta - a/q| \le 1/q^2$ with $(a,q)=1$. Then for any $\beta\in\mathbb{R}$ we have*

$$\sum_{|h|\le H} \min\Big(N, \frac{1}{\|h\theta+\beta\|}\Big) \ll \frac{HN}{q} + H\log q + N + q\log q.$$

PROOF. Let $\theta = a/q+\epsilon$. If $\epsilon = 0$ then $\|\theta h\|$ would be periodic with period q, taking values which are $1/q$-seaprated. Moreover, ϵh would be small compared with $1/q$ if h is a bit smaller than q. We therefore split the sum over h into $\lceil 4H/q\rceil$ sums of length $q/2$ (potentially increasing the number of terms slightly for an upper bound). Thus

$$\sum_{|h|<H} \min\Big(N, \frac{1}{\|\theta h+\beta\|}\Big) \le \sum_{m=1}^{\lceil 2H/q\rceil}\sum_{r=1}^{q/2} \min\Big(N, \frac{1}{\|\beta_m+\theta r\|}\Big),$$

where $\beta_m = \theta mq + \beta$ doesn't depend on r. Finally, we note that if $r_1, r_2 \le q/2$ with $r_1 \neq r_2$ then $a(r_1 - r_2) \neq 0 \pmod q$ since $(a,q) = 1$, so $\|a(r_1 - r_2)/q\| \ge 1/q$. Therefore, since $|\epsilon| \le 1/q^2$

$$\|\theta r_1 - \theta r_2\| = \Big\|\frac{a(r_1 - r_2)}{q} + \epsilon(r_1 - r_2)\Big\| \ge \frac{1}{q} - \frac{|\epsilon| q}{2} \ge \frac{1}{2q}.$$

Thus the values $\beta_m + \theta r \pmod 1 \in [-1/2, 1/2]$ for $1 \le r \le q/2$ are separated by $1/(2q)$, so the j^{th} smallest non-negative value is at least $(j-1)/(2q)$. In particular, for any m we have

$$\sum_{r=1}^{q/2} \min\Big(N, \frac{1}{\|\beta_m + \theta r\|}\Big) \le N + 2\sum_{j=1}^{q/2-1} \frac{2q}{j} \ll N + q\log q.$$

Recalling that there are $\ll H/q + 1$ such sums we obtain the result. □

LEMMA 5.9 (Minor arc bound for squares). *If $\theta = a/q + \epsilon$ with $(a,q) = 1$ and $|\epsilon| \le 1/q^2$, then*

$$\Big|\sum_{n \le N} e(\theta n^2)\Big| \ll \frac{N}{q^{1/2}} + N^{1/2}\log q + q^{1/2}\log q.$$

PROOF. We square the sum in question, expand, and write $n_2 = n_1 + h$. This gives

$$\begin{aligned}\Big|\sum_{n \le N} e(\theta n^2)\Big|^2 &= \sum_{n_1, n_2 \le N} e(\theta(n_2^2 - n_1^2)) \\ &= \sum_{|h| < N} e(\theta h^2) \sum_{\max(1,-h) \le n_1 \le \min(N, N-h)} e(\theta h n_1).\end{aligned}$$

By summing the geometric series, we have that

$$\Big|\sum_{\max(1,-h) \le n_1 \le \min(N,N-h)} e(\theta h n_1)\Big| \le \min\Big(N, \frac{2}{|e(\theta h) - 1|}\Big) \ll \min\Big(N, \frac{1}{\|\theta h\|}\Big).$$

Now, applying Lemma 5.8 gives

$$\Big|\sum_{n \le N} e(\theta n^2)\Big|^2 \ll \sum_{|h| \le N} \min\Big(N, \frac{1}{\|h\theta\|}\Big) \ll \Big(\frac{N}{q} + 1\Big)(N + q\log q).$$

This gives the result. □

LEMMA 5.10 (Divisor Bound). *Let $\tau_k(n)$ be the number of ways of writing n as a product $n_1 \dots n_k$ of k positive integers. Then*

$$\tau_k(n) \le n^{o_k(1)}.$$

PROOF. If $n = p_1^{e_1} \cdots p_r^{e_r}$ then for any $\epsilon > 0$

$$\tau_k(n) = \prod_{i=1}^{r} \binom{e_i + k}{k} \le \prod_{i=1}^{r} (e_i + 1)^k \le n^{\epsilon} \prod_{i=1}^{r} \frac{(e_i+1)^k}{p_i^{\epsilon e_i}}.$$

If $p > 2^{k/\epsilon}$ then $(e_i+1)^k \le 2^{ke_i} \le p^{\epsilon e_i}$. If $p \le 2^{k/\epsilon}$ then we see that

$$\frac{(e+1)^k}{p^{\epsilon e}} \le \frac{(e+1)^k}{2^{\epsilon e}} \le C(\epsilon,k)$$

for some constant $C(\epsilon,k)$ independent of e. Thus

$$\tau_k(n) \le N^\epsilon \prod_{p \le 2^{r/\epsilon}} C(\epsilon,k) \le N^\epsilon C(\epsilon,k)^{2^{k/\epsilon}}. \qquad \square$$

LEMMA 5.11 (Minor arc bound for polynomials). *Let $P(x) \in \mathbb{Z}[x]$ be a polynomial of degree d and $\theta = a/q + \epsilon$ for $(a,q) = 1$ and $|\epsilon| \le 1/q^2$. Then*

$$\Big|\sum_{n\le N} e(\theta P(n))\Big| \ll_P N^{1-1/2^{d-1}+o(1)} + N^{1+o(1)}q^{-1/2^{d-1}} + N^{1+o(1)}\Big(\frac{q}{N^d}\Big)^{1/2^{d-1}}.$$

PROOF. We claim that if $P(x)$ has degree d and lead coefficient a_0, then for any interval $\mathcal{I} \subseteq [1,N]$ we have

$$\Big|\sum_{n\in\mathcal{I}} e(\theta P(n))\Big|^{2^{d-1}} \ll N^{2^{d-1}-d} \sum_{|h_1|,\dots,|h_{d-1}|\le N} \min\Big(N, \frac{1}{\|d!a_0h_1\cdots h_{d-1}\theta\|}\Big).$$

Assume that this is true for all polynomails of degree at most k, and we wish to show it for $P(x)$ of degree $k+1$ and lead coefficient a_0. We see that

$$\begin{aligned}\Big|\sum_{n\in\mathcal{I}} e(\theta P(n))\Big|^2 &= \sum_{n_1,n_2\in\mathcal{I}} e(\theta(P(n_1)-P(n_2)))\\ &= \sum_{|h|\le N}\sum_{n_1\in\mathcal{J}_h} e(\theta Q_h(n_1)), \qquad (5.1)\end{aligned}$$

where $\mathcal{J}_h = \mathcal{I}\cap(\mathcal{I}-h)$ and $Q_h(n) = P(n+h)-P(n)$. Then $Q_h(n)$ has degree k and lead coefficient $(k+1)a_0h$ and $\mathcal{J}_h$ is an interval, so by the induction hypothesis

$$\Big|\sum_{n_1\in\mathcal{J}_h} e(\theta Q_h(n_1))\Big|^{2^{k-1}} \ll N^{2^{k-1}-k} \sum_{|h_1|,\dots,|h_{k-1}|\le N} \min\Big(N, \frac{1}{\|(k+1)!a_0hh_1\cdots h_{k-1}\theta\|}\Big). \qquad (5.2)$$

Now Hölder's inequality gives

$$\sum_{|h|\le N}\sum_{n_1\in\mathcal{J}_h} e(\theta Q_h(n_1)) \le N^{1-1/2^{k-1}}\Big(\sum_{|h|\le N}\Big|\sum_{n_1\in\mathcal{J}_h} e(\theta Q_h(n_1))\Big|^{2^{k-1}}\Big)^{1/2^{k-1}}.$$

Substituting in (5.1) and (5.2) (and relabelling h as h_k) gives

$$\Big|\sum_{n\in\mathcal{I}} e(\theta P(n))\Big|^{2^k} \ll N^{2^k-k-1} \sum_{|h_1|,\dots,|h_k|\le N} \min\Big(N, \frac{1}{\|(k+1)!a_0h_1\cdots h_k\theta\|}\Big).$$

This establishes the claim.

Let $h = (k+1)!a_0h_1\dots,h_k \ll N^k$. The number of choices of $h_1,\dots,h_k$ given h is $O(N^{o(1)})$ by the divisor bound when $h \ne 0$, and $O(N^{k-1})$ when $h = 0$. Thus

by Lemma 5.8 we obtain

$$\Big|\sum_{n\in\mathcal{I}} e(\theta P(n))\Big|^{2^k} \ll N^{2^k-k-1}\Big(N^{o(1)}\sum_{0<|h|\ll N^k}\min\Big(N,\frac{1}{\|h\theta\|}\Big)+N^k\Big)$$
$$\leq N^{2^k-1+o(1)}+\frac{N^{2^k+o(1)}}{q}+N^{2^k-k-1+o(1)}q. \qquad \square$$

Proof of Proposition 5.3. By Dirichlet's Theorem in Diphantine approximation (Lemma 1.6, any $\theta\in[0,1]$ has an approximation

$$\theta=\frac{a}{q}+\epsilon, \qquad q\leq\frac{N^d}{Q}, \qquad (a,q)=1, \qquad |\epsilon|\leq\frac{Q}{qN^d}\leq\frac{1}{q^2}.$$

If there is such an approximation with $q\leq Q$ then clearly $\theta\in\mathfrak{M}$. Therefore if $\theta\in\mathfrak{m}$ we see that $q\in[Q,N^d/Q]$, in which case Lemma 5.11 gives

$$\Big|\sum_{n\leq N} e(\theta P(n))\Big|\ll\frac{N^{1+o(1)}}{Q^{1/2^d}}.$$

Integrating the k^{th} power of this bound over all $\theta\in\mathfrak{m}$ gives

$$\int_{\mathfrak{m}}\Big|\sum_{n\leq N} e(\theta P(n))\Big|^k d\theta\ll\frac{N^{k+o(1)}}{Q^{k/2^d}}. \qquad \square$$

CHAPTER 6

Roth's Theorem

A k-term arithmetic progression is a sequence a, $a+d$, $\dots$, $a+(k-1)d$. We call this non-trivial if $d \neq 0$.

THEOREM 6.1 (Roth's Theorem). *There is a constant $C \geq 1$ such that any subset $\mathcal{A} \subseteq \{1, \dots, N\}$ with $|\mathcal{A}| \geq CN/\sqrt{\log\log N}$ contains a non-trivial 3-term arithmetic progression.*

6.1. The density increment strategy

PROPOSITION 6.2 (Density increment). *Let $\alpha \in (0,1)$ and $N \geq (10/\alpha)^{10}$. Let $\mathcal{P} \subseteq \mathbb{Z}$ be an arithmetic progression of length N, and $\mathcal{A} \subseteq \mathcal{P}$ a set with $|\mathcal{A}| \geq \alpha N$. Then at least one of the following holds:*

(1) $\mathcal{A}$ contains a non-trivial 3-term arithmetic progression.

(2) There is an arithmetic progression $\mathcal{P}' \subseteq \mathcal{P}$ of length $N' \geq N^{1/5}$ such that $\mathcal{A}' := \mathcal{A} \cap \mathcal{P}'$ satisfies

$$\frac{|\mathcal{A}'|}{|\mathcal{P}'|} \geq \alpha + \frac{\alpha^2}{60}.$$

PROOF OF THEOREM 6.1 ASSUMING PROPOSITION 6.2. By increasing the constant C if necessary, we may assume that $N > N_0$ for any fixed choice of N_0. Assume for a contradiction that there is a set $\mathcal{A} \subseteq \{1, \dots, N\}$ containing no non-trivial three term arithmetic progressions, but with density $\alpha \geq 1/\sqrt{\log\log N}$. Then no subset of $\mathcal{A}$ contains non-trivial 3-term progressions. Let $\mathcal{A}_1 := \mathcal{A}$ and $\mathcal{P}_1 := \{1, \dots, N\}$. We now repeatedly apply Proposition 6.2 to obtain a sequence of arithmetic progressions $\mathcal{P}_1 \supseteq \mathcal{P}_2 \supseteq \cdots \supseteq \mathcal{P}_J$ together with sets $\mathcal{A}_1 \supseteq \mathcal{A}_2 \supseteq \cdots \supseteq \mathcal{A}_J$ where $\mathcal{A}_j := \mathcal{A} \cap \mathcal{P}_j$ has density $\alpha_j := |\mathcal{A}_j|/|\mathcal{P}_j|$. We do this until we can no longer apply Proposition 6.2, which must mean that

$$|\mathcal{P}_J| < (10/\alpha_J)^{10}. \tag{6.1}$$

By the bounds from Proposition 6.2, we have that

$$|\mathcal{P}_j| \geq N^{1/5^j}, \qquad \alpha_{j+1} \geq \alpha_j + \frac{\alpha_j^2}{60} \geq \alpha_j\Big(1 + \frac{\alpha}{60}\Big). \tag{6.2}$$

We see that α_j are increasing, and so we cannot have many terms in the sequence since the density of a set cannot increase above 1. Let $m := \lceil 60/\alpha \rceil$. Since $\alpha_{j+1} \geq$

$\alpha_j(1+\alpha/60)$, we see that

$$\alpha_{1+jm} \geq \alpha\Big(1+\frac{\alpha}{60}\Big)^{jm} \geq \alpha\Big(1+\frac{1}{m}\Big)^{jm} \geq \alpha 2^j.$$

However, all densities must be at most 1, so we must have that $j \leq 2\log(1/\alpha)$. Thus, recalling $\alpha \geq 1/\sqrt{\log\log N}$, if N_0 is large enough the number J of terms in the sequence satisfies

$$J \leq 1 + 2\lceil\frac{60}{\alpha}\rceil \log\frac{1}{\alpha} \leq \frac{\log\log N}{100}$$

terms in the sequence. However, this is incompatible with our bounds on $|\mathcal{P}_J|$. The lower bound (6.2) then implies (for N large enough)

$$|\mathcal{P}_J| \geq N^{1/5^J} \geq \exp\Big((\log N)^{1-\log 5/10}\Big) \geq \Big(10\sqrt{\log\log N}\Big)^{10},$$

but the upper bound (6.1) implies

$$|\mathcal{P}_J| < (10/\alpha)^{10} < \Big(10\sqrt{\log\log N}\Big)^{10},$$

a contradiction. Thus $\mathcal{A}$ must have contained a non-trivial three term arithmetic progression. □

6.2. Circle method and large Fourier coefficients

To prove Proposition 6.2 we wish to analyse the count of the number of three term arithmetic progressions in $\mathcal{A}$. We see that, using orthogonality,

$$\begin{aligned}\sum_{\substack{a,d\leq N\\ a,a+d,a+2d\in\mathcal{A}}} 1 &= \sum_{\substack{a_1,a_2,a_3\in\mathcal{A}\\ a_1+a_3=2a_2}} 1\\ &= \int_0^1 \Big(\sum_{a\in\mathcal{A}} e(a\theta)\Big)^2\Big(\sum_{a\in\mathcal{A}} e(-2a\theta)\Big)d\theta.\end{aligned}$$

For any set $\mathcal{A}\subseteq\{1,\dots,N\}$ we have that $\sum_{a\in\mathcal{A}} e(a\theta)$ is large when θ is a small multiple of $1/N$. For a random set, it would only be these arcs near 0 which make a meaningful contribution, and these would contribute roughly α^3N^2. Therefore there must be a significant contribution from somewhere else to cancel this if there are actually no arithmetic progressions in $\mathcal{A}$. To keep track of things more easily we work with the balanced function $f_{\mathcal{A}}(n) := \mathbf{1}_{\mathcal{A}}(n) - \alpha$ rather than the indicator function. Given functions $f_1, f_2, f_3 : \mathbb{Z}\to\mathbb{C}$, let

$$\begin{aligned}T(f_1,f_2,f_3) &= \int_0^1 \Big(\sum_{n\leq N} f_1(n)e(n\theta)\Big)\Big(\sum_{n\leq N} f_3(n)e(n\theta)\Big)\Big(\sum_{n\leq N} f_2(n)e(-2n\theta)\Big)d\theta\\ &= \sum_{\substack{n_1,n_2,n_3\leq N\\ n_1+n_3=2n_2}} f_1(n_1)f_2(n_2)f_3(n_3).\end{aligned}$$

LEMMA 6.3. *Let $f_1, f_2, f_3 : \mathbb{Z} \to \mathbb{C}$ be supported on $\{1, \dots, N\}$ and satisfy $\sum_{n \le N} |f_i(n)|^2 \le \beta N$. Then for any $j \in \{1, 2, 3\}$*

$$T(f_1, f_2, f_3) \le \beta N \sup_\theta |\widehat{f_j}(\theta)|.$$

PROOF. We prove the result for $j = 1$; the other cases are completely analogous. We have that

$$\begin{aligned} T(f_1, f_2, f_3) &= \int_0^1 \widehat{f_1}(\theta)\widehat{f_3}(\theta)\widehat{f}(2\theta))d\theta \\ &\le \sup_\theta |\widehat{f_1}(\theta)| \int_0^1 |f_2(2\theta) f_3(\theta)| d\theta \\ &\le \sup_\theta |\widehat{f_1}(\theta)| \Big(\int_0^1 |f_2(2\theta)|^2 d\theta \Big)^{1/2} \Big(\int_0^1 |f_3(\theta)|^2 d\theta \Big)^{1/2}. \end{aligned}$$

By Parseval (Lemma 4.1) we have

$$\int_0^1 |\widehat{f_j}(\theta)|^2 d\theta = \sum_n |f_j(n)|^2 \le \beta N.$$

Substituting this in above gives the result. □

LEMMA 6.4.

$$\sum_{\substack{a,d \le N \\ a, a+d, a+2d \in \mathcal{A}}} 1 \ge \frac{\alpha^3 N^2}{2} - 7\alpha N \sup_\theta |\widehat{f_{\mathcal{A}}}(\theta)|.$$

PROOF. Clearly T is trilinear, so by writing $\mathbf{1}_{\mathcal{A}}(n) = f_{\mathcal{A}}(n) + \alpha$, we have

$$\begin{aligned} T(\mathbf{1}_{\mathcal{A}}, \mathbf{1}_{\mathcal{A}}, \mathbf{1}_{\mathcal{A}}) - T(\alpha, \alpha, \alpha) = {} & T(f_{\mathcal{A}}, f_{\mathcal{A}}, f_{\mathcal{A}}) + T(f_{\mathcal{A}}, f_{\mathcal{A}}, \alpha) + T(f_{\mathcal{A}}, \alpha, f_{\mathcal{A}}) \\ & + T(\alpha, f_{\mathcal{A}}, f_{\mathcal{A}}) + T(f_{\mathcal{A}}, \alpha, \alpha) + T(f_{\mathcal{A}}, \alpha, f_{\mathcal{A}}) \\ & + T(\alpha, \alpha, f_{\mathcal{A}}). \end{aligned}$$

Each term on the right hand side involves at least one copy of $f_{\mathcal{A}}$ as an argument to T. We note that

$$\sum_n |\mathbf{1}_{\mathcal{A}}(n)|^2 = \alpha N, \qquad \sum_n |f_{\mathcal{A}}|^2 = \alpha(1-\alpha)N,$$

so by Lemma 6.3 we have

$$\Big| T(\mathbf{1}_{\mathcal{A}}, \mathbf{1}_{\mathcal{A}}, \mathbf{1}_{\mathcal{A}}) - T(\alpha, \alpha, \alpha) \Big| \le 7\alpha N \sup_\theta |\widehat{f_{\mathcal{A}}}(\theta)|.$$

By direct estimation we see that

$$T(\alpha, \alpha, \alpha) = \alpha^3 \sum_{\substack{n_1, n_2, n_3 \le N \\ n_1 + n_3 = 2n_2}} 1 \ge \alpha^3 \frac{N^2}{2}.$$

Therefore

$$T(\mathbf{1}_{\mathcal{A}}, \mathbf{1}_{\mathcal{A}}, \mathbf{1}_{\mathcal{A}}) \geq \frac{\alpha^3 N^2}{2} - 7\alpha N \sup_{\theta} |\widehat{f_{\mathcal{A}}}(\theta)|. \qquad \square$$

LEMMA 6.5 (Sets without 3APs have large Fourier coefficients). *Let $\alpha \geq 1/\sqrt{\log\log N}$ and N be sufficiently large. Then at least one of the following holds:*

(1) $\mathcal{A}$ contains a non-trivial three-term arithmetic progression.
(2) $\sup_\theta |\widehat{f_{\mathcal{A}}}(\theta)| \geq \alpha^2 N/20$.

PROOF. The number of trivial three term progressions in $\mathcal{A}$ is just $|\mathcal{A}| = \alpha N$. Therefore, by Lemma 6.4, the number of non-trivial three term arithmetic progressions is at least

$$\frac{\alpha^3 N^2}{2} - 7\alpha N \sup_{\theta} |\widehat{f_{\mathcal{A}}}(\theta)| - \alpha N.$$

Since $\alpha \geq 1/\sqrt{\log\log N}$, we see that for N large enough $\alpha^3 N^2/2 - \alpha N \geq 2\alpha^3 N^2/5$. Therefore if $|\widehat{f_{\mathcal{A}}}(\theta)| \leq \alpha^2 N/20$ for all θ, the number of non-trivial three term arithmetic progressions is at least

$$\frac{2\alpha^3 N^2}{5} - \frac{\alpha^3 N^2}{20} > 0. \qquad \square$$

LEMMA 6.6 (Large Fourier coefficients imply density increments). *Let $|f_{\mathcal{A}}(\theta)| \geq \alpha^2 N/20$. Then there is an arithmetic progression $\mathcal{P} \subseteq \{1, \dots, N\}$ such that*

$$\frac{|\mathcal{A} \cap \mathcal{P}|}{|\mathcal{P}|} \geq \alpha + \frac{\alpha^2}{60}, \qquad |\mathcal{P}| \geq N^{1/5}.$$

PROOF. By Lemma 1.6, there is a $q \leq N^{1/2}$ such that

$$\theta = \frac{b}{q} + \epsilon, \qquad |\epsilon| \leq \frac{1}{qN^{1/2}}, \qquad (b, q) = 1.$$

We first split $\{1, \dots, N\}$ into congruence classes $\pmod q$, and then split each of these into arithmetic progressions containing between $N^{1/5}$ and $2N^{1/5}$ consecutive terms in the congruence class. If $\mathcal{P} = \{c + qr : r \leq N_1\}$ is one of these arithmetic progressions, then we see that

$$\sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) e(n\theta) = e(c\theta) \sum_{r \leq N_1} f_{\mathcal{A}}(c + rq) e(\epsilon rq).$$

We have that

$$|e(\epsilon rq) - 1| = |2\sin(\pi \epsilon rq)| \leq 2\pi \epsilon rq \leq \frac{2\pi N_1}{N^{1/2}} \leq \frac{4\pi}{N^{3/10}}.$$

Thus, for N large enough

$$\Big| \sum_{r \leq N_1} f_{\mathcal{A}}(c + rq) e(\epsilon rq) - \sum_{r \leq N_1} f_{\mathcal{A}}(c + rq) \Big| \leq \frac{4\pi N_1}{N^{3/10}} \leq 1.$$

On the other hand, by assumption $|\widehat{f_{\mathcal{A}}}(\theta)| \geq \alpha^2 N/20$. Thus, since the $\mathcal{P}$ partition $\{1, \dots, N\}$, by the triangle inequality

$$\sum_{\mathcal{P}} \Big| \sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) e(n\theta) \Big| \geq \Big| \sum_{n \leq N} f_{\mathcal{A}}(n) e(n\theta) \Big| \geq \frac{\alpha^2 N}{20}.$$

Combining these gives (for N sufficiently large)

$$\sum_{\mathcal{P}} \Big| \sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) \Big| \geq \frac{\alpha^2 N}{30}.$$

Since $\sum_{n \leq N} f_{\mathcal{A}}(n) = 0$, and $\sum_{\mathcal{P}} |\mathcal{P}| = N$, we have

$$\sum_{\mathcal{P}} \Big(\Big| \sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) \Big| + \sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) \Big) \geq \frac{\alpha^2}{30} \sum_{\mathcal{P}} |\mathcal{P}|.$$

Thus there is some $\mathcal{P}$ such that

$$\Big| \sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) \Big| + \sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) \geq \frac{\alpha^2}{30} |\mathcal{P}|.$$

We see $\sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n)$ is real, and must be positive for the left hand side to be positive. Thus

$$\sum_{n \in \mathcal{P}} f_{\mathcal{A}}(n) \geq \frac{\alpha^2}{60} |\mathcal{P}|.$$

Recalling the definition of $f_{\mathcal{A}}$, the left hand side is $|\mathcal{A} \cap \mathcal{P}| - \alpha |\mathcal{P}|$. This then gives the result. □

We can now prove Proposition 6.2, and so complete the proof of Theorem 6.1.

Proof of Proposition 6.2. Assume that $\mathcal{A}$ contains no non-trivial 3-term arithmetic progressions. After an affine rescalining, we may assume that $\mathcal{P} = \{1, \dots, N\}$ since affine rescalings don't change whether a set is a 3AP, and preserves cardinalities.

Then, applying Lemma 6.5, we deduce that $\mathcal{A}$ has a large Fourier coefficient in the sense that

$$\Big| \widehat{f}_{\mathcal{A}}(\theta) \Big| \geq \frac{\alpha^2 N}{30}.$$

Now applying Lemma 6.6, we see that this implies that there is an arithmetic progression $\mathcal{P} \subseteq \{1, \dots, N\}$ of length at least $N^{1/5}$ such that

$$\frac{|\mathcal{A} \cap \mathcal{P}|}{|\mathcal{P}|} \geq \alpha + \frac{\alpha^2}{60}.$$

□

CHAPTER 7

Freiman's Theorem

THEOREM 7.1 (Freiman's Theorem). *Let $\mathcal{A} \subseteq \mathbb{Z}$ satisfy $|\mathcal{A}+\mathcal{A}| \leq K|\mathcal{A}|$. Then there is a constant $C(K) > 0$ such that $\mathcal{A}$ is contained in a generalised arithmetic progression of dimension $C(K)$ and size $C(K)|\mathcal{A}|$.*

DEFINITION (Freiman Homomorphism). *Let $\mathcal{A}, \mathcal{B}$ be sets in (possibly different) additive groups, and $\phi : \mathcal{A} \to \mathcal{B}$. Let $s \geq 2$ be an integer. We say that ϕ is a Freiman homomorphism of order s if*

$$\phi(a_1) + \cdots + \phi(a_s) = \phi(a'_1) + \cdots + \phi(a'_s)$$

whenever $a_1 + \cdots + a_s = a'_1 + \cdots + a'_s$. We say that ϕ is a Freiman s-isomorphism if ϕ is a bijection and both ϕ and ϕ^{-1} are Freiman s-homomorphisms.

Thus Freiman homomorphisms respect s-fold sum relations.

LEMMA 7.2 (Basic properties of Freiman homomorphisms).

(1) *(Preserved under composition) If $\phi_1 : \mathcal{A} \to \mathcal{B}$ and $\phi_2 : \mathcal{B} \to \mathcal{C}$ are both Freiman s-homomorphisms, then $\phi_2 \circ \phi_1 : \mathcal{A} \to \mathcal{C}$ is a Freiman s-homomorphism. Moreover, if ϕ_1, ϕ_2 are both Freiman s-isomorphisms then so is $\phi_2 \circ \phi_1$.*
(2) *(Hierarchy) If ϕ is a Freiman s-homomorphism it is a Freiman t-homomorphism for all $t \leq s$.*
(3) *(Interactions with sumsets) If $\phi : \mathcal{A} \to \mathcal{B}$ is a Freiman s-homomorphism, then it induces $\tilde{\phi}_{k,\ell} : k\mathcal{A} - \ell\mathcal{A} \to k\mathcal{B} - \ell\mathcal{B}$, which is a Freiman $\tilde{s}$-homomorphism for any $\tilde{s} \leq s/(k+\ell)$.*
(4) *(Weakening of homomorphism) If ϕ is a homomorphism from $\langle A \rangle \to \langle B \rangle$ then ϕ is a Freiman s-homomorphism for all s.*
(5) *(Dependency on additive structure of underlying sets) If $\mathcal{A}$ has no non-trivial solutions to $a_1 + \cdots + a_s = a'_1 + \cdots + a'_s$ then every map $\phi : \mathcal{A} \to \mathcal{B}$ is a Freiman s-homomorphism.*
(6) *(Preserves GAPs) If $\phi : \mathcal{A} \to \mathcal{B}$ is a Freiman 2-isomorphism and $Q \subseteq \mathcal{A}$ is a proper generalised arithmetic progression of dimension d and size S,*

then $\phi(Q)$ is a proper generalised arithmetic progression of dimension d and size S.

PROOF. These all follow quickly from the definitions. If $a_1+\cdots+a_s = a'_1+\cdots+a'_s$ then $\phi_1(a_1)+\cdots+\phi_1(a_s) = \phi_1(a'_1)+\cdots+\phi_1(a'_s)$ since ϕ_1 is a Freiman s-homomorphism, which then means $\phi_2(\phi_1(a_1))+\cdots+\phi_2(\phi_1(a_s)) = \phi_2(\phi_1(a'_1))+\cdots+\phi_2(\phi_1(a'_s))$ since ϕ_2 is a Freiman s-homomorphism, and so $\phi_2\circ\phi_1$ is a Freiman s-homomorphism.

If $a_1+\cdots+a_{s-1} = a'_1+\cdots+a'_{s-1}$ then (choosing $a_s\in\mathcal{A}$ arbitrarily) $a_1+\cdots+a_s = a'_1+\cdots+a'_{s-1}+a_s$, so $\phi(a_1)+\cdots+\phi(a_s) = \phi(a'_1)+\cdots+\phi(a'_{s-1})+\phi(a_s)$ (since ϕ is an s-homomorphism), so $\phi(a_1)+\cdots+\phi(a_{s-1}) = \phi(a'_1)+\cdots+\phi(a'_{s-1})$ and ϕ is a Freiman $(s-1)$-homomorphism. Repeating this gives the result.

We define $\tilde{\phi}$ by

$$\tilde{\phi}(a_1+\cdots+a_k-a'_1-\cdots-a'_\ell) = \phi(a_1)+\cdots+\phi(a_k)-\phi(a'_1)-\cdots-\phi(a'_\ell).$$

We need to check that this is well-defined; if $a_1+\cdots+a_k-a'_1-\cdots-a'_\ell = a''_1+\cdots+a''_k-a'''_1-\cdots-a'''_\ell$ then $a_1+\cdots+a_k+a'''_1+\cdots+a'''_\ell = a''_1+\cdots+a''_k+a'_1+\cdots+a'_\ell$. Since $k+\ell\le s$ and ϕ is a Freiman s-homomorphism we then see that

$$\phi(a_1)+\cdots+\phi(a_k)-\phi(a'_1)-\cdots-\phi(a'_\ell) = \phi(a''_1)+\cdots+\phi(a''_k)-\phi(a'''_1)-\cdots-\phi(a'''_\ell),$$

so $\tilde{\phi}$ is independent of the choice of representative and is well-defined. Similarly if $n_1+\cdots+n_{\tilde{s}} = n'_1+\cdots+n'_{\tilde{s}}$ with $n_i,n'_i\in k\mathcal{A}-\ell\mathcal{A}$ then, picking representatives $n_i = a_1^{(i)}+\cdots+a_k^{(i)}-b_1^{(i)}-\cdots-b_\ell^{(i)}$ we find that

$$\sum_{i=1}^{\tilde{s}}\Big(\sum_{j=1}^{k}a_j^{(i)}+\sum_{j=1}^{\ell}b'^{(i)}_j\Big) = \sum_{i=1}^{\tilde{s}}\Big(\sum_{j=1}^{k}a'^{(i)}_j+\sum_{j=1}^{\ell}b_j^{(i)}\Big).$$

Since $\tilde{s}\le s/(k+\ell)$, there are at most s terms on either side, so

$$\tilde{\phi}(n_1)+\cdots+\tilde{\phi}(n_{\tilde{s}}) = \sum_{i=1}^{\tilde{s}}\Big(\sum_{j=1}^{k}\phi(a_j^{(i)})-\sum_{j=1}^{\ell}\phi(b_j^{(i)})\Big) = \tilde{\phi}(n'_1)+\cdots+\tilde{\phi}(n'_{\tilde{s}})$$

If ϕ is a genuine homomorphism of additive groups then $\phi(a_1+\cdots+a_s) = \phi(a_1)+\cdots+\phi(a_s)$ so the result is immediate.

If $\mathcal{A}$ only has the trivial solutions then $a_1+\cdots+a_s = a'_1+\cdots+a'_s$ implies $\{a_1,\dots,a_s\} = \{a'_1,\dots,a'_s\}$ so certainly $\phi(a_1)+\cdots+\phi(a_s) = \phi(a'_1)+\cdots+\phi(a'_s)$ without requiring any properties about the map ϕ.

We see x_1,x_2,x_3 being in arithmetic progression is equivalent to $x_1+x_3 = 2x_2$. If this holds then $\phi(x_1)+\phi(x_3) = 2\phi(x_2)$, so $\phi(x_1),\phi(x_2),\phi(x_3)$ are in arithmetic progression. It follows that $\phi(Q)$ is a generalised arithmetic progression of dimension d. □

LEMMA 7.3. *If $\mathcal{A} \subseteq \mathbb{Z}$ satisfies*

$$\sup_{a,b\in\mathcal{A}} |a-b| < \frac{N}{s},$$

then $\mathcal{A}$ is Freiman s-isomorphic to its image $\pmod N$.

PROOF. The reduction mod N map is a group homomorphism, so certainly a Freiman s-homomorphism. Therefore we just need to consider the inverse map. Imagine $a_1, \dots, a_s, a_1', \dots, a_s' \in \mathcal{A}$ are such that

$$(a_1 + \cdots + a_s) - (a_1' + \cdots + a_s') = 0 \pmod N.$$

By assumption on $\mathcal{A}$, we see that $(a_1 + \cdots + a_s) - (a_1' + \cdots + a_s')$ is an integer of size less than N. But then the only such integer which is 0 $\pmod N$ is 0 itself, so we must have $a_1 + \cdots + a_s = a_1' + \cdots + a_s'$ whenever these are congruent $\pmod N$. □

7.1. Modelling integers sets with cyclic groups

A big difficulty of using Fourier analysis to study an arbitrary set $\mathcal{A}\mathbb{Z}$ is that this is typically very weak if $\mathcal{A}$ is very sparse. Therefore, to address this issue it is very benefitial if we can find a set $\mathcal{B}$ with similar additive structure to $\mathcal{A}$ (such as being s-isomorphic to $\mathcal{A}$, or a large subset of $\mathcal{A}$) but which is dense. One cannot hope to find such a dense set $\mathcal{B}$ in $\mathbb{Z}$ (since an additive relations over $\mathbb{Z}$ encode information about the relative size of integers), but we can find sets $\mathcal{B}$ is a cyclic group $\mathbb{Z}/N\mathbb{Z}$ (where there is no longer a notion of size).

Clearly you cannot hope to find a set $\mathcal{B} \subseteq \mathbb{Z}/N\mathbb{Z}$ s-isomorphic to $\mathcal{A}$ if $N < |s\mathcal{A} - s\mathcal{A}|$. If $N \geq |s\mathcal{A} - s\mathcal{A}|$ and $s\mathcal{A} - s\mathcal{A}$ contains no non-zero elements which are a multiple of N, then for any interval $\mathcal{I} \subseteq \mathbb{Z}/N\mathbb{Z}$ of length N/s, and $\mathcal{B} = \{b \in \mathcal{I} : b \in \mathcal{A} \pmod N\}$ is s-isomorphic to $\mathcal{A}$ by Lemma 7.3. By the pigeonhole principle we can choose $\mathcal{I}$ such that $\mathcal{B}$ contains at least $|\mathcal{A}|/s$ elements. We wish to find a substitute for this construction when $s\mathcal{A} - s\mathcal{A}$ does contain non-zero elements which are a multiple of N.

LEMMA 7.4. *Let $\mathcal{A} \subseteq \mathbb{Z}$, and $s, N \geq 2$. If we have that*

$$|s\mathcal{A} - s\mathcal{A}| \leq N,$$

then there is a prime p and a subset $\mathcal{B} \subseteq \mathbb{Z}$ such that:

- *If $d \in (s\mathcal{B} - s\mathcal{B})\backslash\{0\}$ then $N \nmid d$.*
- *$\mathcal{B}$ is Freiman s-isomorphic to a subset $\mathcal{A}'$ of $\mathcal{A}$.*
- *$|\mathcal{B}| \geq |\mathcal{A}|/s$.*
- *$\mathcal{B}$ is contained in an interval of length p/s.*
- *$\mathcal{B} = \lambda\mathcal{A}' \pmod p$ for some $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$.*

PROOF. The idea is to take a large prime p, and first choose $\mathcal{B}' \subseteq [0, p-1]$ such that $\mathcal{B}' = \lambda \cdot \mathcal{A} \pmod p$ is congruent to the dilation of $\mathcal{A} \pmod p$ by a well-chosen element $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$ to ensure nothing is a multiple of N. This is an isomorphism if we view everything $\pmod p$, and we then restrict $\mathcal{B}'$ to a short interval to ensure that this is an s-isomorphism over the integers.

Fix a very large prime $p > \max(s\mathcal{A} - s\mathcal{A})$. Let $\phi_1 : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be the reduction mod p map, let $\phi_{2,\lambda} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be $\phi_{2,\lambda}(x) = \lambda x$ and $\phi_3 : \mathbb{Z}/p\mathbb{Z} \to \{0, \dots, p-1\}$ the lift inverting ϕ_1 on $\{0, \dots, p-1\}$. Then, for each choice of $\lambda \in \{1, \dots, p-1\}$, we define

$$\phi_\lambda := \phi_3 \circ \phi_{2,\lambda} \circ \phi_1.$$

First we want to show that there exists a choice of $\lambda \in \{1, \dots, p-1\}$ such that $\phi_\lambda(d)$ is not a multiple of N for any $d \in (s\mathcal{A} - s\mathcal{A})\backslash\{0\}$. Let $\mathcal{S}_N$ be the set of non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ mapped to multiples of N by ϕ_3, so $|\mathcal{S}_N| \leq (p-1)/N$. We see that

$$\sum_{\lambda \in \{1,\dots,p-1\}} \#\Big\{d \in s\mathcal{A} - s\mathcal{A}\backslash\{0\} : N|\phi_\lambda(d)\Big\} = \sum_{d \in s\mathcal{A}-s\mathcal{A}\backslash\{0\}} \sum_{b \in S_N} \sum_{\substack{\lambda \in \{1,\dots,p-1\} \\ \phi_\lambda(d)=b}} 1.$$

Since d is non-zero and $p > \max(s\mathcal{A} - s\mathcal{A}) \geq d$, we see that d is coprime to p. Therefore there is a unique choice of λ such that $\phi_\lambda(d) = b$ (namely $\lambda \equiv bd^{-1} \bmod p$). Thus

$$\sum_{\lambda \in \{1,\dots,p-1\}} \#\Big\{d \in s\mathcal{A}-s\mathcal{A}\backslash\{0\} : N|\phi_\lambda(d)\Big\} < |\mathcal{S}_N||s\mathcal{A}-s\mathcal{A}| \leq \frac{p-1}{N}|s\mathcal{A}-s\mathcal{A}| \leq p-1,$$

on recalling that $|s\mathcal{A} - s\mathcal{A}| \leq N$. In particular, this means we cannot have that $\#\{d \in s\mathcal{A} - s\mathcal{A}\backslash\{0\} : N|\phi_\lambda(d)\} \geq 1$ for all λ, so there must be some choice of λ such that $\phi_\lambda(d)$ is not a multiple of N for all $d \in s\mathcal{A} - s\mathcal{A}$. Thus if we choose

$$\mathcal{B}' = \phi_\lambda(\mathcal{A})$$

then $\mathcal{B}' = \lambda \cdot \mathcal{A} \pmod p$ and no non-zero element of $s\mathcal{B}' - s\mathcal{B}'$ is a multiple of N and $|\mathcal{B}'| = |\mathcal{A}|$.

Finally, by the pigeonhole principle, we can find an interval $\mathcal{I} \subseteq \{0, \dots, p-1\}$ of length at most p/s such that

$$\mathcal{B} := \mathcal{B}' \cap \mathcal{I}$$

contains at least $|\mathcal{B}'|/s = |\mathcal{A}|/s$ elements. By Lemma 7.3, both $\mathcal{A}'$ and $\mathcal{B}$ are s-isomorphic to their images $\pmod p$ (since $\mathcal{A}' \subseteq \mathcal{A} \subseteq [0, p/s]$, and these images are isomorphic, so $\mathcal{A}'$ and $\mathcal{B}$ are s-isomorphic. □

LEMMA 7.5 (Rusza modelling lemma). *Let $\mathcal{A} \subseteq \mathbb{Z}$, and $s, N \geq 2$. If we have that*

$$|s\mathcal{A} - s\mathcal{A}| \leq N$$

then there is an $\mathcal{A}' \subseteq \mathcal{A}$ such that $|\mathcal{A}'| \geq |\mathcal{A}|/s$ and $\mathcal{A}'$ is Freiman s-isomorphic to a subset of $\mathbb{Z}/N\mathbb{Z}$.

PROOF. By Lemma 7.4 there is a subset $\mathcal{A}'$ of $\mathcal{A}$ of size at least $|\mathcal{A}|/s$ and an s-isomorphism ϕ such that $s\phi(\mathcal{A}') - s\phi(\mathcal{A}')$ contains no non-zero elements which are a multiple of N and $\phi(\mathcal{A}') = \lambda \cdot \mathcal{A}' \pmod p$ and $\phi(\mathcal{A}')$ is contained in an interval of length p/s.

It suffices to show that $\phi(\mathcal{A}')$ is Freiman s-isomorphic to its image $\pmod N$. Let ψ be the composition of ϕ with the reduction $\pmod N$ map. Clearly ψ is a Freiman s-homomorphism (since it is a composition of Freiman s-homomorphisms). Thus it suffices to show that $\psi(a_1) + \cdots + \psi(a_s) = \psi(a_1') + \cdots + \psi(a_s')$ implies $a_1 + \cdots + a_s = a_1' + \cdots + a_s'$. If $\psi(a_1) + \cdots + \psi(a_s) = \psi(a_1') + \cdots + \psi(a_s')$, then

$$y := \phi(a_1) + \cdots + \phi(a_s) - \phi(a_1') - \cdots - \phi(a_s') \in N\mathbb{Z}.$$

Without loss of generality, we may assume that $y > 0$ (by swapping the a_i with the a_i' if necessary). Since $\phi(\mathcal{A}')$ is contained in an interval of length p/s, we see that $0 \leq y < p$. Let

$$x := a_1 + \cdots + a_s - a_1' - \cdots - a_s' \in s\mathcal{A}' - s\mathcal{A}'.$$

Since $\phi(t) = \lambda t \pmod p$, working $\pmod p$ we have

$$\phi(x) = \lambda a_1 + \cdots + \lambda a_s - \lambda a_1' - \cdots - \lambda a_s' = y \pmod p.$$

Thus $\phi(x) = y \pmod p$ and $\phi(x), y \in [0, p)$, so $\phi(x) = y$. But $N|y$ and we have constructed ϕ such that $\phi(x) \notin N\mathbb{Z}$ for all non-zero $x \in s\mathcal{A} - s\mathcal{A}$. Thus we must have that $x = 0$, and so ψ is indeed a Freiman s-isomorphism. □

7.2. Structure in sumsets

DEFINITION (Bohr sets in $\mathbb{Z}/q\mathbb{Z}$). *Given $\mathcal{R} = \{r_1, \ldots, r_k\} \subseteq \mathbb{Z}/q\mathbb{Z}$ and $\epsilon > 0$, define*

$$B(\mathcal{R}, \epsilon) := \{x \in \mathbb{Z}/q\mathbb{Z} : \left\| \frac{r_i x}{q} \right\| \leq \epsilon \, \forall i\}.$$

LEMMA 7.6 (Bogolyubov Lemma). *Let $\mathcal{A} \subseteq \mathbb{Z}/q\mathbb{Z}$ be a set of size αq. Then there is an integer $k \leq 4/\alpha^2$ and a set $\mathcal{R} = \{r_1, \ldots, r_k\} \subseteq \mathbb{Z}/q\mathbb{Z}$ such that $2\mathcal{A} - 2\mathcal{A}$ contains $B(\mathcal{R}, 1/10)$.*

PROOF. Let $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ be given by

$$f(x) = \sum_{\substack{a_1,a_2,a_3,a_4 \in \mathcal{A} \\ a_1+a_2-a_3-a_4=x}} 1 = (\mathbf{1}_{\mathcal{A}} * \mathbf{1}_{\mathcal{A}} * \mathbf{1}_{-\mathcal{A}} * \mathbf{1}_{-\mathcal{A}})(x).$$

Then f is supported on $2\mathcal{A}-2\mathcal{A}$. By the convolution identity (Lemma 3.1) we have

$$\widehat{f}(r) = q^3 |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^4.$$

Thus, by Fourier inversion (Lemma 3.1 again) and the fact that f is real, we have

$$f(x) = \Re(f(x)) = \Re\Big(q^3 \sum_r |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^4 e\Big(\frac{rx}{q}\Big)\Big) = q^3 \sum_r |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^4 \cos\Big(\frac{2\pi rx}{q}\Big).$$

We now choose $\mathcal{R}$ to be the set of large Fourier frequencies

$$\mathcal{R} := \{r \in \mathbb{Z}/q\mathbb{Z} : |\widehat{\mathbf{1}_{\mathcal{A}}}(r)| \geq \alpha^{3/2}/2\}.$$

Then by Parseval's identity

$$|\mathcal{R}|\frac{\alpha^3}{4} \leq \sum_{r\in\mathcal{R}} |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^2 \leq \sum_{r\in\mathbb{Z}/q\mathbb{Z}} |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^2 = \frac{1}{q}\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \mathbf{1}_{\mathcal{A}}(x)^2 = \alpha.$$

Thus $|\mathcal{R}| \leq 4/\alpha^2$. To complete the proof it suffices to show that $f(x) > 0$ if $x \in B(\mathcal{R}, 1/10)$ since $f(x) > 0$ only on $2\mathcal{A} - 2\mathcal{A}$. We split the Fourier expansion into three parts: the term $r = 0$, the terms $r \in \mathcal{R}$ and the terms $r \notin \mathcal{R} \cup \{0\}$.

$$f(x) = q^3|\widehat{\mathbf{1}_{\mathcal{A}}}(0)|^4 + q^3 \sum_{r\in\mathcal{R}} |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^4 \cos\Big(\frac{2\pi rx}{q}\Big) + q^3 \sum_{r\notin\mathcal{R}\cup\{0\}} |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^4 \cos\Big(\frac{2\pi rx}{q}\Big).$$

We see that $\widehat{\mathbf{1}_{\mathcal{A}}}(0) = \alpha^4$, and that since $|\widehat{\mathbf{1}_{\mathcal{A}}}(r)| \leq \alpha^{3/2}/2$ for $r \notin \mathcal{R} \cup \{0\}$

$$\Big|\sum_{r\notin\mathcal{R}\cup\{0\}} |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^4 \cos\Big(\frac{2\pi rx}{q}\Big)\Big| \leq \frac{\alpha^3}{4} \sum_{r\notin\mathcal{R}\cup\{0\}} |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^2 \leq \frac{\alpha^3}{4}\sum_r |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^2 \leq \frac{\alpha^4}{4}.$$

Finally, if $x \in B(\mathcal{R}, 1/10)$ then for all $r \in \mathcal{R}$ we have that $\|rx/q\| \leq 1/10$, so $\cos(2\pi rx/q) \geq 0$. In particular

$$\sum_{r\in\mathcal{R}} |\widehat{\mathbf{1}_{\mathcal{A}}}(r)|^4 \cos\Big(\frac{2\pi rx}{q}\Big) \geq 0.$$

Putting this together, we find that for $x \in B(\mathcal{R}, 1/10)$ we have

$$f(x) \geq q^3\alpha^4 + 0 - q^3\frac{\alpha^4}{4} = \frac{3q^3\alpha^4}{4} > 0. \qquad \square$$

PROOF OF THEOREM 7.1.

(1) By Plünnecke's Theorem (Lemma 2.4) we have $|8\mathcal{A} - 8\mathcal{A}| \leq K^{16}|\mathcal{A}|$.
(2) Choose N to be a prime with $K^{16}|\mathcal{A}| \leq N \leq 2K^{16}|\mathcal{A}|$.
(3) By Rusza's modelling lemma (Lemma 7.5), there is a subset $\mathcal{A}' \subseteq \mathcal{A}$ with $|\mathcal{A}'| \geq |\mathcal{A}|/8$ such that $\mathcal{A}'$ is Frieman 8-isomorphic to a subset $\mathcal{B}$ of $\mathbb{Z}/N\mathbb{Z}$.

We see that

$$\frac{|\mathcal{B}|}{N} = \frac{|\mathcal{A}'|}{N} \geq \frac{|\mathcal{A}|}{8N} \geq \frac{1}{16K^{16}}.$$

(4) By Bogolubov's lemma (Lemma 7.6) we then see that $2\mathcal{B} - 2\mathcal{B}$ contains a Bohr set $B(\mathcal{R}, 1/10)$ for some set $\mathcal{R} \subseteq \mathbb{Z}N\mathbb{Z}$ of cardinality at most $256K^{32}$.

(5) By the geometry of numbers (Lemma 1.8) $B(\mathcal{R}, 1/10)$ contains a proper generalised arithmetic progression G of dimension $d \leq 256K^{32}$ and size at least $c_K N$ for some constant $c_K > 0$ depending only on K.

(6) Since $\mathcal{B}$ is Freiman 8-isomorphic to $\mathcal{A}'$, $2\mathcal{B} - 2\mathcal{B}$ is Freiman 2-isomorphic to $2\mathcal{A}' - 2\mathcal{A}'$ by Lemma 7.2.

(7) Generalised arithmetic progressions are preserved by Freiman 2-isomorphisms (by Lemma 7.2). Thus G is mapped to a proper generalised arithmetic progression $Q \subseteq 2\mathcal{A}' - 2\mathcal{A}'$, with the same dimension $d \leq 256K^{32}$ and size at least $c_K N$.

(8) By Lemma 2.5, this implies that $\mathcal{A}$ is contained in a generalised arithmetic progression of dimension $C(K)$ and size $C(K)|\mathcal{A}|$. This gives the result.

□

APPENDIX A

Asymptotic estimates

We will repeatedly encounter interesting number-theoretic objects which are complicated, such as the counting function of the primes. To understand these complicated functions, we want to approximate them by much simpler functions, such as a continuous function with no number-theoretic properties. To do this we need to control the error in such approximations, and the following notation is very useful to keep us focused on what is going on.

DEFINITION (Big Oh notation). *We write '$O(h(x))$' to denote a function $g(x)$ which satisfies*

$$|g(x)| \leq C \cdot h(x)$$

for some constant $C > 0$ and all x under consideration.

Since the function g and the constant C are unspecified, multiple uses of $O(\cdot)$ can specify different functions. Moreover, this can lead to some initally confusing issues when used with the $=$ sign, since $f(x) = O(h(x))$ and $g(x) = O(h(x))$ does not imply that $f(x) = g(x)$. Moreover, we will use $O(h(x))$ inside various expressions, so given functions f, g, h, when we write '$f(x) = g(x) + O(h(x))$ for $x \in \mathcal{S}$' we mean there exists a constant $C > 0$ (which depends only on $f, g, h, \mathcal{S}$) such that

$$|f(x) - g(x)| \leq C \cdot h(x)$$

for all $x \in \mathcal{S}$. If the set $\mathcal{S}$ is clear from the context (as is normally the case), we just write '$f(x) = g(x) + O(h(x))$'. We sometimes call $g(x)$ the 'main term' and $h(x)$ the 'error term' in an approximation to f.

EXAMPLE A.1.

- $x = O(x^2)$ *for* $x \geq 1$. *(Since* $x \leq x^2$ *for* $x \geq 1$.*)*
- $x^2 = O(x)$ *for* $0 \leq x \leq 10$. *(Since* $x^2 \leq 10x$ *for* $0 \leq x \leq 10$.*)*
- *It is not the case that* $x^2 = O(x)$ *for* $x \geq 1$ *(since as* $x \to \infty$, $x^2/x \to \infty$.*)*
- $(x+1)^2 = x^2 + O(x)$ *for* $x \geq 1$ *(since* $|(x+1)^2 - x^2| \leq 3x$ *for* $x \geq 1$.*)*
- $\lfloor x \rfloor = \sup\{n \in \mathbb{Z} : n \leq x\} = x + O(1)$ *for* $x \in \mathbb{R}$. *(Since* $x - 1 \leq \lfloor x \rfloor \leq x$, *so* $|\lfloor x \rfloor - x| \leq 1$.*)*

- $\sqrt{x+1} = \sqrt{x} + \frac{1}{2\sqrt{x}} - \frac{1}{8x^{3/2}} + O\Big(\frac{1}{x^{5/2}}\Big)$ *for* $x \geq 1$. *(Since for* $f(x) = \sqrt{x}$, $f(x+1) = f(x) + f'(x) + f''(x)/2 + f'''(y)/6$ *for some* $y \in [x, x+1]$ *by Taylor's Theorem, and* $f'''(y) = 3/(8y^{5/2}) \leq 6/(8x^{5/2})$ *for* $x \geq 1$.*)*

LEMMA A.2 (Properties of Big Oh notation).

(1) Non-negativity of error term:
If $f(x) = O(g(x))$ *then* $g(x) \geq 0$.

(2) Transitivity:
If $f(x) = O(g(x))$ *and* $g(x) = O(h(x))$ *then* $f(x) = O(h(x))$.

(3) Additivity:
If $f_1(x) = g_1(x) + O(h_1(x))$ *and* $f_2(x) = g_2(x) + O(h_2(x))$ *then* $f_1(x) + f_2(x) = g_1(x) + g_2(x) + O(h_1(x) + h_2(x))$.

PROOF. These follow immediately from the definition. □

DEFINITION (Further asymptotic notation).

- *Little Oh notation:*
Given $h(x) > 0$, *when considering a limit* $x \to a$ *we write '*$o(h(x))$*' to denote a function* $g(x)$ *which satisfies*

$$\lim_{x \to a} \frac{g(x)}{h(x)} \to 0.$$

If we don't explicitly mention the limit point a then it is assumed $a = \infty$.

- *Vinogradov notation:*
We have the binary relation $f(x) \ll g(x)$ *if* $f(x) = O(g(x))$.

Although the Vinogradov notation overlaps with Big Oh notation, the Big Oh notation should be thought of as a placeholder for some unspecified function, whereas the $\ll$ is an inequality which can exploit the transitivity of $O(\cdot)$, so we might write things like $f(x) \ll g(x) \ll h(x)$.

APPENDIX B

Analytic identities

DEFINITION (Schwarz functions on $\mathbb{R}$). *We let $\mathcal{S}(\mathbb{R})$ be the space of infinitely differentiable functions $f : \mathbb{R} \to \mathbb{C}$ such that for all integers $j, k > 0$*

$$|f^{(j)}(x)| \ll_{j,k} |x|^{-k}.$$

LEMMA B.1 (Properties of the real Fourier transform). *Let $f, g \in \mathcal{S}(\mathbb{R})$.*

- *(Fourier transform is smooth with rapid decay) $\widehat{f} \in \mathcal{S}(\mathbb{R})$.*
- *(Gaussian is egenfunction of Fourier operator)If $f(x) = e^{-\pi x^2}$ then $\widehat{f}(\xi) = e^{-\pi \xi^2}$.*
- *(Inversion formula). We have*

$$f(t) = \int_{-\infty}^{\infty} \widehat{f}(\xi) e(t\xi) d\xi.$$

- *(Parseval).*

$$\int_{-\infty}^{\infty} f(t)\overline{g(t)}dt = \int_{-\infty}^{\infty} \widehat{f}(\xi)\overline{\widehat{g}(\xi)}d\xi.$$

- *(Convolutions). Let $h(x) := \int_{-\infty}^{\infty} f(t)g(x-t)dt$. Then*

$$\widehat{h}(\xi) = \widehat{f}(\xi)\widehat{g}(\xi).$$

PROOF. A bit of care is required because convergence issues can come into play. Let

$$\phi_\epsilon(x) = \frac{1}{\epsilon} e^{-\pi(x/\epsilon)^2}$$

be an approximation of the identity. Clearly $\phi_\epsilon \in \mathcal{S}(\mathbb{R})$. Let

$$f_\epsilon(x) := e^{-\pi(\epsilon x)^2}(f * \phi_\epsilon)(x) = e^{-\pi(\epsilon x)^2} \int_{-\infty}^{\infty} \phi_\epsilon(x-t) f(t) dt.$$

Then $f_\epsilon \in \mathcal{S}(\mathbb{R})$ since $f * \phi_\epsilon$ is infinitely differentiable and $e^{-\pi(\epsilon x)^2}$ has rapid decay. We see that for $|x| < \epsilon^{-1/2}$

$$f_\epsilon(x) = f(x) + O(\epsilon) + O(\sup_{|y-x|<\epsilon^{1/2}} |f(y) - f(x)|).$$

In particular $f_\epsilon(x) \to f(x)$ as $\epsilon \to 0$ if x is a point of continuity of f. Thus, since the conditions on f, g ensure that all integrals in the lemma are absolutely

convergent, it suffices to establish the results for f_ϵ, g_ϵ in place of f, g, so we only need to consider $f, g \in \mathcal{S}(\mathbb{R})$.

- First note that since $f \in \mathcal{S}(\mathbb{R})$, we have that $f(x) = O(|x|^{-k})$ for $|x| \geq 1$. Thus $\hat{f}(\xi)$ is given by an absolutely convergent integral, and

$$\frac{\hat{f}(\xi+\epsilon) - \hat{f}(\xi)}{\epsilon} = \int_{|x|<\epsilon^{-1/2}} f(x)e^{-2\pi i x\xi}\Big(\frac{e^{-2\pi i x\epsilon}-1}{\epsilon}\Big)dx + \int_{|x|\geq\epsilon^{-1/2}} O\Big(\frac{|f(x)|}{\epsilon}\Big)dx.$$

  In the first integral we use the Taylor expansion $e^{-2\pi i x\epsilon} = 1 - 2\pi i x\epsilon + O(x^2\epsilon^2)$. Thus, taking out a term $-2\pi i x f(x)e^{-2\pi i x\xi}$ from both integrals, we find

$$\begin{aligned}\frac{\hat{f}(\xi+\epsilon) - \hat{f}(\xi)}{\epsilon} &= \int_{-\infty}^{\infty} -2\pi i x f(x)e^{-2\pi i x\xi} + O\Big(\int_{|x|<\epsilon^{-1/2}} \epsilon x^2|f(x)|dx\Big) \\ &\qquad + O\Big(\int_{|x|\geq\epsilon^{-1/2}} |f(x)|(\frac{1}{\epsilon}+x)dx\Big) \\ &= \int_{-\infty}^{\infty} -2\pi i x f(x)e^{-2\pi i x\xi} + O\Big(\int_{|x|<\epsilon^{-1/2}} \epsilon dx\Big) + O\Big(\int_{|x|\geq\epsilon^{-1/2}} \frac{1}{x^4\epsilon} + \frac{1}{x^3}\Big)dx\Big) \\ &= \int_{-\infty}^{\infty} -2\pi i x f(x)e^{-2\pi i x\xi} + O(\epsilon^{1/2}).\end{aligned}$$

  This converges as $\epsilon \to 0$, showing $\hat{f}'(\xi)$ is the Fourier transform of $-2\pi i x f(x)$. Since $-2\pi i x f(x) \in \mathcal{S}(\mathbb{R})$ whenever $f \in \mathcal{S}(\mathbb{R})$, we can repeat the above argument and find that $\hat{f}^{(j)}$ is the Fourier transform of $(-2\pi i x)^j f(x)$ for all $j \in \mathbb{Z}_{>0}$.

  By differentiating by parts k times, we see that

$$\hat{f}^{(j)}(\xi) = \int_{-\infty}^{\infty} \frac{e^{-2\pi i x\xi}}{(2\pi i\xi)^k}\frac{\partial^k}{\partial x^k}\Big((-2\pi i x)^j f(x)\Big)dx \ll_{j,k} \frac{1}{|\xi|^k}.$$

  Thus $\hat{f} \in \mathcal{S}(\mathbb{R})$.

- By completing the square, we have

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} e^{-\pi x^2 - 2\pi i x\xi}dx = e^{-\pi\xi^2}\int_{-\infty}^{\infty} e^{-\pi(x+i\xi)^2}dx.$$

  By Cauchy's residue theorem

$$\int_{-R+i\xi}^{R+i\xi} f(z)dz + \int_{R+i\xi}^{R} f(z)dz + \int_{R}^{-R} f(z)dz + \int_{-R}^{-R+i\xi} f(z)dz = 0,$$

  where the integrals are straight line contours. Since $|f(z)| \leq e^{-\pi(\Re(z)^2 - \Im(z)^2)}$, we see that the second and fourth terms both tend to 0 as $R \to \infty$. Thus we find that

$$\int_{-\infty}^{\infty} e^{-\pi(x+i\xi)^2}dx = \lim_{R\to\infty}\int_{-R+i\xi}^{R+i\xi} f(z)dz = -\int_{\infty}^{-\infty} f(z)dz = \int_{-\infty}^{\infty} e^{-\pi x^2}dx.$$

The result follows on recalling the identity $\int_{-\infty}^{\infty} e^{-\pi u^2} du = 1$.

- Let $\phi_\epsilon(x) = e^{-\pi(x/\epsilon)^2}/\epsilon$. Then, by a change of variables and the previous result, we see that

$$\widehat{\phi_\epsilon}(\xi) = \int_{-\infty}^{\infty} \frac{e^{-\pi(x/\epsilon)^2}}{\epsilon} dx = e^{-\pi\xi^2\epsilon^2} = \frac{\phi_{1/\epsilon}(\xi)}{\epsilon},$$

$$\int_{-\infty}^{\infty} \widehat{\phi_\epsilon}(\xi) e(x\xi) d\xi = \frac{1}{\epsilon}\int_{-\infty}^{\infty} \phi_{1/\epsilon}(\xi) e(x\xi) = \frac{\widehat{\phi_{1/\epsilon}}(-x)}{\epsilon} = \phi_\epsilon(x).$$

Then we see that

$$\begin{aligned} f * \phi_\epsilon(t) &= \int_{-\infty}^{\infty} f(t-u) \int_{-\infty}^{\infty} \widehat{\phi_\epsilon}(\xi) e(\xi u) d\xi du \\ &= \int_{-\infty}^{\infty} \widehat{\phi_\epsilon}(\xi) e(\xi t) \int_{-\infty}^{\infty} f(t-u) e(-\xi(t-u)) du d\xi \\ &= \int_{-\infty}^{\infty} \widehat{\phi_\epsilon}(\xi) \widehat{f}(\xi) e(\xi t) d\xi. \end{aligned}$$

Rcalling that $f, \widehat{f} \in \mathcal{S}(\mathbb{R})$, we see that letting $\epsilon \to 0$ then gives

$$f(t) = \lim_{\epsilon\to 0}(f * \phi_\epsilon)(t) = \lim_{\epsilon\to 0} \int_{-\infty}^{\infty} \widehat{\phi_\epsilon}(\xi)\widehat{f}(\xi) e(\xi t) d\xi = \int_{-\infty}^{\infty} \widehat{f}(\xi) e(\xi t) d\xi.$$

- Substituting the defintions and then $t = u + v$ gives (recalling $f, g \in \mathcal{S}(\mathbb{R})$ so everything converges absolutely)

$$\begin{aligned} \widehat{h}(\xi) &= \int_{-\infty}^{\infty} \Big(\int_{-\infty}^{\infty} f(u) g(t-u) du \Big) e(-t\xi) dt \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(u) g(v) e(-u\xi) e(-\xi v) du dv = \widehat{f}(\xi)\widehat{g}(\xi). \end{aligned}$$

□

LEMMA B.2 (Gamma and Beta function identities). *For $\Re(s) > 0$, let $\Gamma(s) := \int_0^\infty x^{s-1}e^{-x}dx$ be the Gamma function. Then for $\Re(s), \Re(\alpha_1), \dots, \Re(\alpha_k) > 0$*

$$\Gamma(s) = \frac{\Gamma(s+1)}{s},$$

$$\int_{x_1+\cdots+x_k=1} x_1^{\alpha_1-1}\cdots x_k^{\alpha_k-1} dx_1 \dots dx_{k-1} = \frac{\Gamma(\alpha_1)\cdots\Gamma(\alpha_k)}{\Gamma(\alpha_1+\cdots+\alpha_k)}.$$

PROOF. This is just an exercise in basic analysis. By integrating by parts, for $\Re(s) > 0$

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx = \int_0^\infty \frac{x^s}{s} e^{-x} dx = \frac{\Gamma(s+1)}{s}.$$

For the second part, first we note that by a change of variables $y_i = x_i/(x_2+\cdots+x_k)$ for $i \geq 2$ the integral is

$$\int_0^1 x_1^{\alpha_1-1}(1-x_1)^{\alpha_2+\cdots+\alpha_k-1} dx_1 \int_{y_2+\cdots+y_k=1} y_2^{\alpha_2-1}\cdots y_k^{\alpha_k-1} dy_2 \dots y_{k-1}.$$

By applying this repeatedly we see that the integral in question is

$$B(\alpha_1, \alpha_2 + \cdots + \alpha_k)B(\alpha_2, \alpha_3 + \cdots + \alpha_k) \cdots B(\alpha_{k-1}, \alpha_k),$$

where $B(z_1, z_2) = \int_0^1 x^{z_1-1}(1-x)^{z_2-1}dx$, so it suffices to show

$$B(z_1, z_2) = \frac{\Gamma(z_1)\Gamma(z_2)}{\Gamma(z_1 + z_2)}.$$

We see that

$$\Gamma(z_1)\Gamma(z_2) = \int_0^\infty \int_0^\infty u_1^{z_1-1} u_2^{z_2-1} e^{-u_1-u_2} du_1 du_2.$$

By a change of variables $s = u_1 + u_2$, $t = u_1/(u_1 + u_2)$ (so $u_1 = st$, $u_2 = s(1-t)$ and the Jacobian factor is s) we find this is

$$\Gamma(z_1)\Gamma(z_2) = \int_0^\infty s^{z_1+z_2-1} e^{-s} ds \int_0^1 t^{z_1-1}(1-t)^{z_2-1} dt = \Gamma(z_1 + z_2)B(z_1, z_2),$$

as required. □