Additive

and

Combinatorial

Number Theory

Notes written by Jacques Verstraëte
Based on a course given by W.T. Gowers in Cambridge (1998)
Chapter 4 written by Tim Gowers

Contents

§1 The Hales-Jewett Theorem

The following theorem was proved in 1927 by van der Waerden [20], answering a conjecture of Schur:

Theorem 1.1. *If the natural numbers are partitioned into two sets, then one set must contain arbitrarily long arithmetic progressions.*

This result was proved before Ramsey's Theorem, and led to a number of generalizations, with implications in Ramsey Theory. Theorem 1.1 can be rewritten as follows: for any pair of positive integers k, r, there exists an integer $W = W(k, r)$ such that if $[W]$ is r-coloured, then we may find a monochromatic k-term arithmetic progression.

In this section, an important theorem known as the Hales-Jewett Theorem [8] is proved. Consider the following notation. For $x \in [k]^N$, $A \subset [N]$ and $j \in [k]$ define

$$(x \oplus jA)_i = \begin{cases} x_i & i \notin A \\ j & i \in A \end{cases}$$

A *Hales-Jewett line* is a set of the form $\{x \oplus jA : 1 \leq i \leq k\}$, for some $x \in [k]^N$ and $A \subset [N]$, $A \neq \emptyset$. The Hales-Jewett Theorem implies van der Waerden's Theorem. To see this, represent points in the cube $[k]^N$ by the coefficients in a base k expansion of non-negative integers less than k^N. Provided N is large enough, a monochromatic line exists, corresponding to a monochromatic arithmetic progression.

Hales-Jewett Theorem. *Let $k, r \in \mathbb{N}$. Then there exists N such that if $[k]^N$ is r-coloured, then it contains a monochromatic Hales-Jewett line.*

PROOF. Let $HJ(k, r)$ denote the smallest integer for which the theorem works. We must show $HJ(k, r)$ is always finite. If $k = 1$ set $N = 1$. Suppose that $N = HJ(i, r)$ has been found for each $i < k$ and set $i = k$. Let $N_1 = HJ(k - 1, r2^{r-1})$ and set

$$N_i = HJ(k - 1, r^{2^{r-i}k^{s_r}})$$

for $i = 1, 2, \ldots, r$, where $s_r = \sum_{i<r} N_i$. Let κ be an r-colouring of $[k]^{\sum N_i}$ (which gives a colouring of $[k]^{N_1} \times \cdots \times [k]^{N_r}$ in the natural way). For $x \in [k]^{N_r}$, we find a colouring κ_x on $[k]^{s_r}$ by sending $(x_1, \ldots, x_{r-1})$ to $\kappa(x_1, \ldots, x_{r-1}, x)$. The number of such

induced colourings κ_x is at most $r^{k^{s_r}}$ – the number of ways of colouring $[k]^{s_r}$ with r colours. Let the distinct ones be $\kappa_i : 1 \leq i \leq s$. We therefore obtain an s-colouring of $[k]^{N_r}$ where x is receives colour i if $\kappa_x = \kappa_i$. This induces an obvious s-colouring of $[k-1]^{N_r}$, as $[k-1]^{N_r} \subset [k]^{N_r}$. So, by definition of N_r, we can find $z_r \in [k]^{N_r}$ and $\emptyset \neq A_r \subset [N_r]$ such that $\kappa_{z_r \oplus jA_r}$ is the same function for $1 \leq j \leq k-1$. Set $L_r = \{z_r \oplus jA_r : 1 \leq j \leq k\}$. Let κ_x be the colouring of $[k]^{s_{r-1}} \times L_r$ induced by κ with $\kappa_x(x_1, x_2, \ldots, x_{r-2}, z_r \oplus jA_r) = \kappa(x_1, x_2, \ldots, x_{r-2}, x, z_r \oplus jA_r)$. The number of possible functions κ_x is now at most $r^{2k^{s_{r-1}}}$, where the factor of two appears since colourings don't change as $1 \leq j \leq k-1$ By definition of N_{r-1}, we find z_{r-1}, A_{r-1} such that $\kappa_{z_{r-1} \oplus jA_{r-1}}$ is constant over $j \in [k-1]$ (as before). Continue this procedure until we have $L_1 \times L_2 \times \cdots L_r$ with $\kappa(z_1 \oplus j_1 A_1, \ldots, z_r \oplus j_r A_r)$, depending only on $\{i : j_i = i\}$. If we r-colour the sets $\emptyset, \{1\}, \{1,2\}, \ldots, [r]$, we clearly find two of the same colour. Hence considering $J = \{i : j_i = k\}$ in this range, there exist t and u such that the colour assigned under κ is the same when $J = [t]$ as when $J = [u]$. If we let elements in any of the $A_i : t < i \leq u$ range from 1 to k, the colour assigned is still the same – we knew it wouldn't change up to $k-1$ and k is taken care of by definition of t and u. So, if

$$x = (z_1 \oplus kA_1, \ldots, z_t \oplus kA_t, z_{t+1} \oplus 1A_{t+1}, \ldots, z_u \oplus 1A_u, \ldots, z_r \oplus 1A_r)$$

and $A = \bigcup_{t<i\leq u} A_i$, then $\{x \oplus jA : 1 \leq j \leq k\}$ is a monochromatic line. □

This extends easily to a d-dimensional theorem. If we define a *d-dimensional Hales-Jewett subspace* of $[k]^N$ to be a set of the form

$$\{x \oplus j_1 A_1 \oplus j_2 A_2 \oplus \cdots \oplus j_d A_d : 1 \leq j_i \leq k\},$$

where $A_1, A_2, \ldots, A_d$ are disjoint and non-empty in $[N]$, then for every k, r, d there exists an N such that, however $[k]^N$ is r-coloured, there is a monochromatic d-dimensional Hales-Jewett subspace. Another way of viewing the Hales-Jewett theorem: if $[N]$ is coloured with r colours, then there exist disjoint sets $A_0, A_1, \ldots, A_k$ such that $A_0 \cup \bigcup_{i \in I} A_i$ are all monochromatic where $I \subset [k]$. The following remarkable inductive proof of the Hales-Jewett theorem is due to Shelah [14]:

PROOF. Let $M = HJ(k-1, r)$ and define $N_1 = r^{(k-1)^{M-1}}$ and $N_i = r^{(k-1)^{M-i}} k^{N_1 + \ldots + N_{i-1}}$ for $i = 2, 3, \ldots, r$. Let κ be an r-colouring of $[k]^{N_1} \times \cdots \times [k]^{N_M}$. Given $x \in [k]^{N_M}$, let κ_x

be the colouring of $[k]^{N_1} \times \cdots \times [k]^{N_{M-1}}$ induced by κ. There are at most $rk^{N_1+\ldots N_{M-1}}$ such colourings, so we can find two points x_1 and x_2 ,of the form $(k-1,\ldots,k-1,k,\ldots,k)$, such that $\kappa_{x_1} = \kappa_{x_2}$. If the first m and first n co-ordinates of x_1 and x_2 are $(k-1)$, respectively, and $A_m = (m,n]$, then $\kappa_{z_m} \oplus jA_m$ is the same for $j = k-1$ and $j = k$, where $z_m = x$. Let $L_M = \{z_M \oplus jA_M : 1 \leq j \leq k\}$. For each i, we have an induced colouring of $[k]^{N_1} \times \cdots \times [k]^{N_{i-1}} \times L_{i+1} \times \cdots \times L_M$. There are at most $r^{k^{N_1+\ldots+N_{i-1}}}(k-1)^{M-i}$ different colourings of this kind, so we find a line $L_i \subset [k]^{N_i}$, $L_i = \{z_i \oplus jA_i : 1 \leq j \leq k\}$ such that $\kappa_{z_i \oplus jA_i}$ is the same for $j = k-1, k$. At the end of this process, we construct $L_1 \times \cdots \times L_M$ so that κ, restricted to $L_1 \times \cdots \times L_M$ does not vary over co-ordinate change from $k-1$ to k. This completes the inductive step. $\square$

This proof was a breakthrough in that it was the first to give primitive recursive bounds on the van der Waerden numbers. Erdős and Turán [4] hoped this could be achieved by finding, for each $k \in \mathbb{N}$, an $o(N)$ function $n_k(N)$ such that every subset of $[N]$ of size at least $n_k(N)$ contains an arithmetic progression of length k. We now look at this problem more closely.

§2 Roth's Theorem

The following theorem was first proved by Szemerédi [17] using ingenious combinatorial techniques, and later by Fürstenburg [6], using methods in ergodic theory.

Szemerédi's Theorem. *Let A be a set of positive upper density in $\mathbb{N}$. Then A contains arbitrarily long arithmetic progressions.*

Szemerédi actually proved more than this. Let $n_k(N)$ denote the smallest integer such that any subset of $n_k(N)$ elements taken from $[N]$ contains an arithmetic progression of length k. Szemerédi established that $n_k(N) = o(N)$ for each k, thus proving a conjecture of Erdős and Turán [4]. The proof used van der Waerden's Theorem and Szemerédi's Regularity Lemma, therefore the upper bound on the order of $n_k(N)$ obtained can be no better than the bounds given by these theorems.

Roth [11] gave a remarkable analytic proof that $n_3(N) = o(N)$ in 1954. Szemerédi proved it for the more difficult case $k = 4$ [16] which then generalized to the above theorem, for general k. We present the theorem of Roth here. The interest in this proof is that it gives a good lower bound on $n_3(N) - n_3(N) \leq cN/\log\log N$ for some constant $c > 0$ – and that it offers the possibilty of generalization. Szemerédi's Theorem was proved by markedly different techniques and Fürstenburg's proof gives no bounds on the van der Waerden numbers.

Let $n \in \mathbb{N}$ and $f : \mathbb{Z}_N \to \mathbb{C}$. The *(discrete) Fourier transform* $\hat{f}$ of f is defined by $\hat{f}(r) = \sum_{s=0}^{N-1} f(s)\omega^{rs}$, where $\omega = \exp(2\pi i/N)$. We define the *convolution of f and g*, $f * g$ by $(f * g)(r) = \sum_{t-u=r} f(t)\overline{g(u)}$. The following properties are easily proved from the definition, and will be used throughout the material to follow. The first identity is known as *Parseval's Identity* and the third will be called the *convolution formula*.

Lemma 2.2. *The following properties hold for fourier transforms*

$$\begin{array}{ll}
(1) & \sum |\hat{f}(r)|^2 = N \sum |f(r)|^2 \\
(2) & \sum \hat{f}(r)\ \overline{\hat{g}}(r) = N \sum f(r)\ \overline{g}(r) \\
(3) & (f * g)\hat{} = \hat{f}\ \overline{\hat{g}} \\
(4) & N \sum |(f * g)(r)|^2 = \sum |\hat{f}(r)|^2 |\hat{g}(r)|^2 \\
(5) & \sum |\hat{f}(r)|^4 = N \sum_{a+b=c+d} f(a)f(b)\overline{f(c)f(d)}
\end{array}$$

An arithmetic progression in $\mathbb{Z}$ is called a $\mathbb{Z}$-*arithmetic progression* if it is an arithmetic progression when considered as a subset of $\mathbb{Z}$.

Lemma 2.3. *Let $a, d \in \mathbb{Z}_N$ with $d \neq 0$ and let $m \leq N$. Then the set $A = \{a, a + d, \ldots, a + (m-1)d\}$ can be partitioned into fewer than $3m^{1/2}$ subsets, which are $\mathbb{Z}$-arithmetic progressions.*

Proof. Let $\ell = \lfloor m^{1/2} \rfloor$ and consider the numbers $\{a, a+d, \ldots, a+(m-1)d\}$. At least two lie within N/ℓ of each other so there exists $s \in [\ell - 1]$ with $-N/\ell \leq sd \leq N/\ell$ such that we split A into subprogressions, each with common difference sd. If P is one of them, then P can be partitioned into $\mathbb{Z}$-arithmetic progressions, all but two of which have size at least $\ell \geq m^{1/2}$, as $|sd| \leq N/\ell$. So the whole set can be partitioned into at most $m/m^{1/2} + 2s \leq 3m^{1/2}$ $\mathbb{Z}$-arithmetic progressions. $\square$

The idea in the proof of Roth's Theorem is that if a set A does not contain an arithmetic progression of length three, then $\hat{A}$ has a large Fourier coefficient. This implies that A has an intersection with a long $\mathbb{Z}_N$-arithmetic progression, where the density of A increases. As the density is bounded above by 1, and $\mathbb{Z}_N$-arithmetic progressions are taken care of by the Lemma 2.3, this completes the argument, provided N is large enough.

Roth's Theorem. *There is a constant $c > 0$ such that for any $N \in \mathbb{N}$ and $A \subset [N]$ of size at least $cN/\log\log N$, A contains an arithmetic progression of length three.*

Proof. In general, if X, Y and Z are subsets of $\mathbb{Z}_N$ with densities α, β, γ respectively, then the number of triples $(x, y, z) \in X \times Y \times Z$ such that $x + z = 2y \pmod N$ is $N^{-1}|X||Y||Z| + \sum_r \hat{X}(r)\hat{Y}(-2r)\hat{Z}(r)$. Using Cauchy–Schwartz, the second term has modulus at most

$$N^{-1} \max_{r \neq 0} |\hat{X}(r)| \Big(\sum_r |\hat{Y}(-2r)|^2 \Big)^{1/2} \Big(\sum_r |\hat{Z}(r)|^2 \Big)^{1/2}.$$

Using Parseval's Identity for $\hat{Y}$ and $\hat{Z}$, this expression is $\beta\gamma N \max_{r \neq 0} |\hat{X}(r)|$. Provided $\max |\hat{X}(r)| \leq \frac{1}{2}\alpha\beta^{1/2}\gamma^{1/2}z^{1/2}N$, there are at least $\frac{1}{2}\alpha\beta\gamma N^2$ triples of the required form as $N^{-1}|X||Y||Z| = \alpha\beta\gamma N^2$. A non-trivial solution occurs if $\frac{1}{2}\alpha\beta\gamma N^2 > N$.

Now let A have density δ and $B = \{a \in A : \frac{N}{3} < x < \frac{2N}{3}\}$. We plan to show that A has a substantial intersection with, and higher density in, a long arithmetic progression P. If $|B| \leq \delta N/5$, then A has density at least $6\delta/5$ in $[0, N/3]$ or $[2N/3, N)$, and we have the required arithmetic progression P, of length $\lfloor N/3 \rfloor$ or $\lfloor N/3 \rfloor + 1$. Suppose $|B| \geq \delta N/5$. Then there exists a non-trivial solution $a + c = 2b$ with $(a, b, c) \in A \times B \times B$, or $|\hat{A}(r)| \geq \delta^2 N/10$ for some r. In the first case, we have a $\mathbb{Z}$-arithmetic progression of length three in A, as required.

Partition the unit circle into M consecutive equal intervals $I_1, I_2, \ldots, I_M$ of diameter as close to $\delta^2/20$ as possible. Define $P_j = \{x : \omega^{-rx} \in I_j\}$. Then each P_j is an arithmetic progression in $\mathbb{Z}_N$ with common difference $-r^{-1} \pmod N$ (the $\mathbb{Z}_N$ inverse of $-r$). Define $f(x) = A(x) - \delta$. Then $\sum f(x) = 0$ and $\hat{f} = \hat{A}$. So

$$\delta^2 N/10 \quad \leq \quad |\hat{f}(r)| = \Big|\sum_x f(x)\omega^{-rx}\Big| \leq \Big|\sum_j \sum_{x \in P_j} f(x)\omega^{-rx}\Big| \leq \sum_j \Big|\sum_{x \in P_j} f(x)\omega^{-rx}\Big|.$$

Now fix j and let $x_j \in P_j$. Then

$$\begin{aligned}
\Big|\sum_{x \in P_j} f(x)\omega^{-rx}\Big| \quad &\leq \quad \Big|\sum_{x \in P_j} f(x)\omega^{-rx_j}\Big| \; + \; \Big|\sum_{x \in P_j} f(x)\Big(\omega^{-rx} - \omega^{-rx_j}\Big)\Big| \\
&\leq \quad \Big|\sum_{x \in P_j} f(x)\Big| + \sum_{x \in P_j} \frac{\delta^2}{20} \\
&\leq \quad \Big|\sum_{x \in P_j} f(x)\Big| + \frac{\delta^2 |P_j|}{20}.
\end{aligned}$$

Summing over j, we find $\frac{\delta^2 N}{10} \leq \sum_{j=1}^M |\sum_{x \in P_j} f(x)| + \frac{\delta^2}{20} \sum_{j=1}^M |P_j|$. Since the last sum is N, we get $\sum_1^M |\sum_{P_j} f(x)| \geq \frac{\delta^2 N}{20}$. Recalling that $\sum f(x) = 0$, we find $\sum_1^M (|\sum_{P_j} f(x)| + \sum_{P_j} f(x))$ is at least $\frac{\delta^2 N}{20}$. So there exists j such that $\sum_{x \in P_j} f(x) \geq \frac{\delta^2 |P_j|}{40}$. As $A(x) = f(x) + \delta$, $|A(x) \cap P_j| \geq \delta(1 + \delta/40)|P_j|$. By Lemma 2.3, P_j may be partitioned into $r \leq 3|P_j|^{1/2}$ $\mathbb{Z}$-arithmetic progressions $Q_1, Q_2, \ldots, Q_r$. This gives

$$\sum_{i=1}^r \sum_{x \in Q_i} f(x) \geq \frac{\delta^2 |P_j|}{40}$$

and so there is k such that $\sum_{Q_k} f(x) \geq \delta^2 |Q_k|/80$ and $|Q_k| \geq \delta^2 |P_j|/80r \geq \delta^3 N^{1/2}/5000$. In other words, A has density $\delta(1+\delta/80)$ in the long arithmetic progression Q_k. We now repeat the argument on $A \cap Q_k$ in Q_k. As the density increases by a factor $\delta/80$ each time, this procedure must stop in $160/\delta$ steps. That is, A must contain an arithmetic progression of length three provided that $\delta \geq 500/\log\log N$. $\square$

Heath-Brown [9] and Szemerédi [18] have recently improved the denominator to $(\log N)^{-c}$, for some constant $c > 0$.

§3 Weyl's Inequality

Let $f : \mathbb{N} \to \mathbb{R}$ be a function and write $\{f(x)\}$ for the fractional part of $f(x)$. We say that f is *uniformly distributed* if for $\alpha \in (0,1]$,

$$\lim_{n\to\infty} |\{m \leq n : \{f(m)\} < \alpha\}| = \alpha$$

Weyl [23] established that if $f(x)$ is a polynomial that has at least one non-constant term with an irrational coefficient, then f is uniformly distributed. This theorem is proved using a fundamental inequality, known as *Weyl's Inequality*, involving exponential sums. We shall prove this theorem with $f(x) = \alpha x^k$: that is, $\{\alpha, 2^k\alpha, 3^k\alpha, \ldots\}$ is equidistributed modulo 1. As a consequence, if α is a real number then for any $\varepsilon > 0$ there exists N such that $N^2\alpha$ is at distance at most ε from an integer.

We derive the appropriate inequality to prove this result by establishing estimates for exponential sums. The statements here are written for simplicity, rather than for finding optimal bounds. We begin with the following elementary lemma:

Lemma 3.1. *Let $\alpha, \beta \in \mathbb{R}$. Then for $n \in \mathbb{N}$,*

$$\Big|\sum_{x=1}^{n} e(\alpha x + \beta)\Big| \leq \min\{n, (2\|\alpha\|)^{-1}\}$$

where $\|\alpha\|$ is the distance from α to the nearest integer.

Proof. The constant β does not affect the inequality. If $\alpha = 0$, then the sum is n. If $\alpha \neq 0$, then the sum is $e(\alpha)(1 - e(\alpha n))/(1 - e(\alpha))$. As $\sin z = \frac{1}{2i}(e^{iz} - e^{-iz})$, this is at most $|\sin \pi\alpha|^{-1}$. Since $|\sin \pi\alpha| \geq 2\|\alpha\|$, the inequality follows. □

Lemma 3.2. *Let $m, r, Q \in \mathbb{N}$ with $Q \geq 2$ and $m \leq r$. Let $\theta_1, \theta_2, \ldots, \theta_m$ be real numbers with $\|\theta_i - \theta_j\| \geq r^{-1}$ whenever $i \neq j$. Then*

$$\sum_{i=1}^{m} \min\Big\{\frac{1}{\|\theta_i\|}, Q\Big\} \leq 6 \log Q(Q + r).$$

Proof. Without loss of generality, $\theta_i \in [-1/2, 1/2]$ and the contribution S^+ to the sum from the non-negative θ_i is at least one half of the total. Suppose the positive θ_i are ordered: $0 < \theta_1 < \theta_2 < \ldots < \theta_k$. Then

$$\sum_{i=1}^{k} \min\Big\{\frac{1}{\|\theta_i\|}, Q\Big\} \;=\; \sum_{i=1}^{k} \min\{\theta_i^{-1}, Q\} \leq \sum_{i=1}^{k} \min\{r/(i-1), Q\} = \sum_{i=0}^{\lfloor r/Q \rfloor} Q + \sum_{r/Q < i < k} r/i.$$

Estimating the last term with logarithms, $S^+ \leq (1+r/Q)Q + 2r(\log k + \log Q - \log r) \leq Q + r + 2r\log Q$. Therefore the sum is at most $2S^+ \leq 6\log Q(Q+r)$. $\square$

The following lemma will be used in this and subsequent sections.

Lemma 3.3. *Let $q, Q, R \in \mathbb{N}$, $Q \geq 2$, and let $\alpha \in \mathbb{R}$ be chosen so that there exists $a \in \mathbb{N}$ with $(a, q) = 1$ and $|\alpha - a/q| \leq q^{-2}$. Then*

$$\sum_{x=0}^{R} \min\Big\{\frac{1}{\|\alpha x + \beta\|}, Q\Big\} \leq 48\log Q(Q + q + R + QR/q).$$

Proof. Let $s, t \geq 0$ be natural numbers. Then $\|s\alpha - t\alpha\| \geq \|(s-t)a/q\| - |s-t|q^{-2}$. If $0 < |s-t| \leq q/2$ then $a(s-t) \neq 0 \pmod q$, so is at least $1/q - q/2q^2 = 1/2q$. In the first case, suppose $R < q/2 - 1$. Then $\beta, \alpha+\beta, \ldots, R\alpha+\beta$ are all $(2q)^{-1}$-separated (mod 1), so by Lemma 3.2 with $r = 2q$,

$$\sum_{x=0}^{R} \min\Big\{\frac{1}{\|\theta_i\|}, Q\Big\} \leq 6\log Q(Q+2q).$$

In the second case, split the sum into segments of size at most $q/2$ – at most $4R/q$ segments in total. By Lemma 3.2, each contributes at most $6\log Q(Q+2q)$. Therefore the sum is at most $24\log Q(QR/q + 2R)$. In both cases, we obtain the upper bound $48\log Q(Q+q+R+QR/q)$, as required. $\square$

Theorem 3.4. *Let $q, Q \in \mathbb{N}$, $Q \geq 2$, let $(a, q) = 1$ and let $\alpha \in \mathbb{R}$ with $|\alpha - a/q| \leq q^{-2}$. Let $\phi(x) = x^2 + cx + d$. Then*

$$\Big|\sum_{x=0}^{Q} e(\alpha\phi(x))\Big| \leq 20\log Q(Q^{1/2} + q^{1/2} + Q/q^{1/2}).$$

Proof. Let $\psi_u(y) = \frac{1}{2u}[\phi(y+u) - \phi(y)] = y + u/2 + c/2$. Then

$$\begin{aligned}
\Big|\sum_{x=0}^{Q} e(\alpha\phi(x))\Big|^2 &= \sum_{y=0} Q \sum_{x=0}^{Q} e(\alpha\phi(x) - \alpha\phi(y)) \\
&= \sum_{y=0}^{Q}\sum_{u=-y}^{Q-y} e(\alpha\phi(y+u) - \alpha\phi(y)) \\
&= \sum_{u=-Q}^{-1}\sum_{y=Q+u}^{Q} e(\alpha\phi(y+u) - \alpha\phi(y)) + \sum_{u=0}^{Q}\sum_{y=0}^{Q-u} e(\alpha\phi(y+u) - \alpha\phi(y))
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{u=-Q}^{Q}\sum_{y\in I_u} e(2\alpha u\psi_u(y))\\
&\le \sum_{u=-Q}^{Q}\Big|\sum_{y\in I_u} e(2u\alpha y+\beta u)\Big|\\
&\le \sum_{u=-Q}^{Q}\min\{\|2u\alpha\|^{-1},Q\}\\
&\le \sum_{u=-2Q}^{2Q}\min\{\|u\alpha\|,Q\}\\
&\le 48\log Q(Q+q+2Q+1+Q(2Q+1)/q)\\
&\le 200\log Q(Q+q+Q^2/q).
\end{aligned}
$$

where I_u denotes the range of y-summation. This gives the desired bound. $\square$

In the next results, we will write $\underline{u}_j \equiv u_1,u_2,\ldots,u_j$, for convenience. The next lemma is the step required to prove Weyl's Inequality.

Lemma 3.5. *Let ϕ be a monic polynomial of degree k and let $0\le j\le k-1$. Let $f(\alpha)=\sum_{x=1}^{Q} e(\alpha\phi(x))$. Then*

$$|f(\alpha)|^{2^j} \le (2Q)^{2^j-j-1}\sum_{u_1\in I_1}\sum_{u_2\in I_2}\cdots\sum_{u_j\in I_j}\Big|\sum_{y\in I_{\underline{u}_j}} e(\alpha\phi_{\underline{u}_j}(y))\Big|$$

where $I_1,I_2,\ldots,I_j$ are integer intervals, contained in $(-Q,Q]$, such that I_i depends on $u_1,u_2,\ldots,u_{i-1}$, $I_{\underline{u}_j}$ is a sub-interval of $[Q]$ and $\phi_{\underline{u}_j}$ is a polynomial of degree $k-j$ with leading coefficient $k!/(k-j)!$.

Proof. By induction on j. For $j=0$, the result is clear. Now, as $(\sum a_i)\le n\sum a_i^2$,

$$
\begin{aligned}
|f(\alpha)|^{2^{j+1}} &\le (2Q)^{2^{j+1}-2j-2}(2Q)^j\Big|\sum_{y\in I_{\underline{u}_j}} e(\alpha\phi_{\underline{u}_j}(y))\Big|^2\\
&\le \sum_{u_{j+1}\in I_{j+1}}\cdot\sum_{y\in I_{\underline{u}_j}} e(\alpha[\phi_{\underline{u}_j}(y+u_{j+1})-\phi_{\underline{u}_j}(y)]),
\end{aligned}
$$

where I_{j+1} is a subset of $I_{\underline{u}_j}-I_{\underline{u}_j}\subset(-Q,Q]$ and $I_{\underline{u}_{j+1}}\subset I_{\underline{u}_j}$. Now $\phi_{\underline{u}_j}(y+u_{j+1})-\phi_{\underline{u}_j}(y)=\phi_{\underline{u}_{j+1}}(y)$ where $\phi_{\underline{u}_{j+1}}(y)$ has degree $k-j-1$. The leading coefficient of $\phi_{\underline{u}_{j+1}}(y)$ is $u_{j+1}(k-j)\cdot k!/(k-j)!\cdot u_1u_2\ldots u_j$. $\square$

We now state and prove Weyl's Inequality.

Theorem 3.6 Let $(a,q)=1$, $\alpha\in\mathbb{R}$, $|\alpha-a/q|\le q^{-2}$, $k,Q\in\mathbb{N}$, $Q\ge 2$. Then

$$\Big|\sum_{x=1}^{Q} e(\alpha\phi(x))\Big| \le 100(\log Q)^{k/2^{k-1}}Q(Q^{-1}+q^{-1}+qQ^{-k})^{1/(2^k-1)}.$$

Proof. Let $k\ge 2$. Given $n\in\mathbb{N}$, there are at most $(2\log_2 n)^{2(k-1)}$ ways of writing n as a product of $k-1$ integers. If $m=k!Q^{k-1}$, then

$$\begin{aligned}
|f(\alpha)|^{2^{k-1}} &\le (2Q)^{2^{k-1}-k}\cdot\sum_{u_1,\dots,u_{k-1}}\Big|\sum_y e(\alpha\phi_{\underline{u}_{k-1}}(y))\Big| \\
&\le (2Q)^{2^{k-1}-k}\cdot\sum_{\underline{u}_{k-1}}\Big|\sum_y e(\alpha\phi_{\underline{u}_{k-1}}(y))\Big| \\
&\le (2Q)^{2^{k-1}-k}\cdot 2^{k-1}(\log_2 Q)^{k-1}\sum_{-m+1}^{m}\min\{Q,\|\alpha x\|^{-1}\} \\
&\le (2Q)^{2^{k-1}-k}\cdot 2^{k-1}(\log_2 Q)^{k-1}\cdot 48\log Q(Q+2k!Q^{k-1}+q+2k!Q^k/q).
\end{aligned}$$

This is at most $100(\log Q)^k Q^{2^{k-1}}(Q^{-1}+q^{-1}+qQ^{-k})$. □

We briefly look at an important practical application of Weyl's Inequality, which will lead to Weyl's Theorem.

Proposition 3.7. *Let $\alpha\in\mathbb{R}, N\in\mathbb{N}$. Then there exists $q: 1\le q\le N$ such that $\|\alpha q\|\le N^{-1}$.*

Proof. Of the reals $\alpha, 2\alpha,\dots,N\alpha$, two lie within N^{-1} of each other (mod 1). Thus there exist $s,t: s\ne t$ with $\|(s-t)\alpha\|\le n^{-1}$. Set $q=|s-t|$. □

Lemma 3.8. *For $n\in\mathbb{N}$, the number of factors of n is at most $n^{4/(\log\log n)}$.*

Proof. Let $2\le t\le n$ and write $\tau(n)$ for the number of divisors of n. Then

$$\begin{aligned}
\tau(n) &= \prod_{\substack{p^a|n\\ p^{a+1}\nmid n}}(a+1) \le \prod_{\substack{p^a|n,p\le t\\ p^{a+1}\nmid n}}(a+1)\prod_{\substack{p^a|n,p>t\\ p^{a+1}\nmid n}}2^a \\
&\le \Big(1+\frac{\log n}{\log 2}\Big)^t\Big(\prod_{\substack{p^a|n\\ p^{a+1}\nmid n}}p^a\Big)^{\log 2/\log t} \\
&\le \exp\Big(t(2+\log\log n)+\log 2\cdot\log n/\log t\Big).
\end{aligned}$$

On choosing $t=\log n/(\log\log n)^3$, we obtain the result. □

Lemma 3.9. *Let $A \subset \mathbb{Z}_N$, $|A| = M$, and suppose that $A \cap (-2L, 2L] \neq \emptyset$. Then there exists r such that $0 < r < (N/L)^2$ and $|\hat{A}(r)| \geq LM/2N$.*

Proof. We have $x, y \in I = (-L, L]$ implies $x-y \in (-2L, 2L]$. Therefore if $(I*I)(s) \neq 0$ then $A(s) = 0$. So $\sum_s (I*I)(s)A(s) = 0$ and $\sum_r |\hat{I}|^2 \hat{A}(r) = 0$ implies $\sum_{r\neq 0} |\hat{I}(r)|^2 |\hat{A}(r)| \geq |\hat{I}(0)||\hat{A}(0)| = 4L^2M$. However $|\hat{I}(r)| = |\sum_I e(-rs)| \leq \min\{\|r/N\|, 2L\}$. If $-N/2 < r < N/2$, then this is $\min\{N/r, 2L\}$. Consequently

$$\begin{aligned}\sum_{r\neq 0} |\hat{I}(r)|^2 |\hat{A}(r)| &\leq \max_{0<|r|\leq (N/L)^2} |\hat{A}(r)| \sum_r |\hat{I}(r)|^2 + M \sum_{|r|>(N/L)^2} (N/r)^2 \\ &\leq 2LN \max_{0<r\leq (N/L)^2} |\hat{A}(r)| + 3MN^2/(N/L)^2.\end{aligned}$$

Therefore there exists r for which $|\hat{A}(r)| \geq LM/2N$. □

The next theorem, due to Weyl [23], is a well-known consequence of Weyl's Inequality:

Theorem 3.10. *For every $k \in \mathbb{N}$ there exists $\varepsilon > 0$ such that for all M sufficiently large and $\alpha \in \mathbb{R}$, there exists $q \leq M$ such that $\|q^k \alpha\| \leq 2M^{-\varepsilon}$.*

Proof. Approximate α arbitrarily closely by a rational a/N with N prime. Without loss of generality, $\alpha = a/N$. If the claim of the theorem is false, then $A = \{a, 2^k a, \ldots, M^k a\}$ and $(-2L, 2L]$ are disjoint when $L = \lfloor NM^{-\varepsilon} \rfloor$. Applying Lemma 3.9, we find r such that $0 < r \leq (N/L)^2 \leq 2M^{2\varepsilon}$, and such that $|\hat{A}(r)| \geq M^{1-\varepsilon}/2$. Now $|\hat{A}(r)| = |\sum_{s=1}^M e(\alpha r s^k)|$. Let $q \leq M$ with $|\alpha r - p/q| \leq (qM)^{-1}$. If $q \geq M^{2^{-k}}$, applying Weyl's inequality gives

$$\Big|\sum_{s=1}^{M} e(\alpha r s^k)\Big| \leq M^{1+\varepsilon} \cdot M^{-1/(2k2^{k-1})},$$

for M is sufficiently large. With $\varepsilon = 1/(k2^{k+3})$, this is a contradiction. If $q \leq M^{2^{-k}}$, then $\|\alpha q r\| \leq M^{-1}$, by Proposition 3.7. But then $\|\alpha(qr)^k\| \leq 2^k M^{-1/2} M^{2k\varepsilon} \leq 2M^{1-\varepsilon}$ for M sufficiently large. □

§4 Vinogradov's Three-Primes Theorem

Vinogradov's famous theorem asserts that every sufficiently large odd number is the sum of three primes. Together with Chen's theorem (every sufficiently large even number is the sum of p and q, where p is prime and q is the product of at most two primes) this is one of the strongest results in the direction of Goldbach's conjecture. In this section we shall see how to use exponential-sum estimates to prove Vinogradov's theorem, and we shall also gain some insight into why Goldbach's conjecture itself is out of reach.

We begin with some definitions and simple lemmas. Given $n \in \mathbb{N}$, let $\Lambda(n)$ be $\log p$ if $n = p^k$ with p prime, $k \geq 1$ and zero otherwise. Let $\mu(n) = (-1)^k$ if n is a product of k distinct primes (interpreting this as 1 when $n = 1$) and zero otherwise. These functions are called *von Mangoldt's function* and the *Möbius function respectively.*

Lemma 4.1. *Let $x \in \mathbb{N}$. Then $\sum_{d|x} \Lambda(d) = \log x$.*

Proof. Write x as a product of prime powers and it becomes obvious. □

Lemma 4.2. *Let $x \in \mathbb{N}$. Then $\sum_{d|x} \mu(d) = 0$ unless $x = 1$ in which case $\sum_{d|x} \mu(d) = 1$.*

Proof. Let $x \geq 2$ and write $x = p_1^{a_1} \dots p_k^{a_k}$. Then every subset $A \subset [k]$ contributes $(-1)^{|A|}$ to the sum $\sum_{d|x} \mu(d)$. But

$$\sum_{A \subset [k]} (-1)^{|A|} = \sum_{j=0}^{k} (-1)^j \binom{k}{j} = (1-1)^k = 0.$$

(Another way of looking at the last calculation is that a randomly chosen subset of $[k]$ has the same chance of being of even as of odd size.) □

Recall that $d(x)$ is defined to be the number of divisors of x. We know from the previous section that $d(x)$ is sometimes quite large. The next lemma shows that this does not happen all that often.

Lemma 4.3. *Let $n \in \mathbb{N}$. Then $\sum_{x \leq n} d(x)^2 \leq 2n(\log n)^3$.*

Proof. This is surprisingly easy to prove. Indeed,

$$\sum_{x \leq n} d(x)^2 \quad = \quad \sum_{x \leq n} \sum b|x \sum_{c|x} 1$$

$$
\begin{aligned}
&= \sum_{b\le n}\sum_{c\le n}\sum_{y.\mathrm{lcm}(a,b)\le n} 1 \\
&\le \sum_{a\le n}\sum_{d\le n/a}\sum_{e\le n/ad}\sum_{y\le n/ade} 1 \\
&\le \sum_{a\le n}\sum_{d\le n/a}\sum_{e\le n/ad} n/ade \\
&\le \sum_{a\le n}\sum_{d\le n/a} (n/ad)(\log n+1) \\
&\le \sum_{a\le n}(n/a)(\log n+1)^2 \\
&\le n(\log n+1)^3,
\end{aligned}
$$

which proves the lemma. □

It is easy to check that the number of ways of writing n as the sum of three primes is $\int F(\alpha)^3 e(-\alpha n)d\alpha$, where $F(\alpha)$ is the function $\sum_{p\le n} e(\alpha p)$. Roughly speaking, our aim will be to estimate $F(\alpha)$ for every α, and use this estimate to prove that the integral is non-zero. As in the previous section, $F(\alpha)$ turns out to be small when α is not too close to a rational with small denominator. When it is close to such a rational, we shall use results about the distribution of primes in an arithmetic progression to estimate $F(\alpha)$ directly.

There are, however, certain advantages in weighting the primes so that their density is approximately constant through the interval. Since the density near m is $(\log m)^{-1}$, the appropriate weight to give p is $\log p$. Accordingly, we shall estimate the function $f(\alpha) = \sum_{p\le n}\log p e(\alpha p)$. The integral $\int f(\alpha)^3 e(-\alpha n)d\alpha$ gives us the sum of $(\log p_1)(\log p_2)(\log p_3)$ over all triples (p_1,p_2,p_3) such that $p_1+p_2+p_3=n$, so for the purposes of Vinogradov's theorem it is enough to prove that this integral is non-zero for large enough odd n.

Finally, even this function is not always the most convenient to estimate. The next lemma shows that we may replace it by $g(\alpha) = \sum_{x\le n}\Lambda(x)e(\alpha x)$, with only a small error.

Lemma 4.4. *$|f(\alpha)-g(\alpha)|\le C\sqrt{n}$ for every α and some absolute constant C.*

Proof. $g(\alpha)-f(\alpha) = \sum_{p^k\le n, k\ge 2}\log p e(\alpha p^k)$ which in modulus is at most $(\log_2 n)\sum_{p\le\sqrt{n}} 1$. By Chebyshev's theorem the result follows. □

The next lemma is similar to the lemma we kept using during the proof of Weyl's inequality, and follows from it. Since we are about to prove several results with the same hypotheses, let us state them once and for all before starting. Thus, a and q will be positive integers with $(a,q)=1$ and α is a real number with $|\alpha - a/q| \le q^{-2}$.

Lemma 4.5. *Let Q, R be positive integers with $q \le Q$. Then*

$$\sum_{x=1}^{R} \min\{\|\alpha x\|^{-1}, Qx^{-1}\} \le 200 \log Q \log R(q + R + Qq^{-1}).$$

Proof. We know, from chapter 3, that the numbers $0, \alpha, 2\alpha, \ldots, \lfloor (q/2) \rfloor \alpha$ are $(2q)^{-1}$-separated. Therefore,

$$\sum_{x \le q/2} \min\{\|\alpha x\|^{-1}, Qx^{-1}\} \quad \le \quad 2 \sum_{x \le \lceil q/4 \rceil} 2q/x \le 4q \log q.$$

Given an integer i, let S_i be the sum $\sum_{x=2^{i-1}}^{2^i - 1} \min\{\|\alpha x\|^{-1}, Qx^{-1}\}$. Then

$$S_i \le \sum_{x=2^{i-1}}^{2^i-1} \min\{\|\alpha x\|^{-1}, Q/2^{i-1}\}$$

which, by Lemma 3.3 of the last chapter, is at most $48 \log Q(2^{-(i-1)}Q + 2^{i-1} + q + Qq^{-1})$. Summing over all i such that $2^i > q/2$ and $2^{i-1} \le R$, we obtain the desired result. □

We now prove an identity due to Vaughan [21], which will allow us to show that $g(\alpha)$ is small when α is not close to a rational with small denominator. This identity seems mysterious when it is just drawn out of a hat, but the mystery can be reduced with a few remarks.

We wish to show that $g(\alpha) = \sum_{x \le n} \Lambda(x) e(\alpha x)$ is appreciably smaller than n when q is not too small (or too large). The function which is hard to understand is of course Λ, but we know that Λ has the nice property that $\sum_{d|x} \Lambda(d) = \log x$, which is much more familiar. Therefore, we try to express $g(\alpha)$ as a sum of pieces of this form. As a first observation, we notice (or rather, it has been noticed) that

$$\sum_{x \le n} \sum_{y \le n/x} \Lambda(x) e(\alpha xy) = \sum_{u \le n} \sum_{x | u} \Lambda(x) e(\alpha u).$$

This is very promising, because

$$\sum_{x \le n} \Lambda(x) e(\alpha x) \quad = \quad \sum_{x \le n} \sum_{y \le n/x} \sum_{d|y} \mu(d) \Lambda(x) e(\alpha xy)$$

$$= \sum_{d\le n}\mu(d)\sum_{z\le n/d}\sum_{x\le n/zd}\Lambda(x)e(\alpha dxz)\ ,$$

which is a ± 1-combination of sums of the required form, and therefore seems to have a chance of being small.

Now it is clearly not easy to obtain a good estimate for the last quantity directly, because d takes n possible values and for each one we are not going to do better than a modulus of 1. It is therefore essential to restrict d. However, this introduces a new error term which must be shown to be small. Moreover, showing that this error term is small turns out not to be possible unless we also restrict x to be not too small. We now prove the identity by a process of trial and error, starting with the observations above.

Lemma 4.6. *Let* $X = n^{2/5}$. *Then* $g(\alpha) = \sum_{x\le n}\Lambda(x)e(\alpha x) = S - T - U + O(n^{2/5})$, *where*

$$S = \sum_{d\le X}\mu(d)\sum_{z\le n/d}\sum_{x\le n/zd}\Lambda(x)e(\alpha dxz)\ ,$$

$$T = \sum_{d\le X}\mu(d)\sum_{z\le n/d}\sum_{x\le X, x\le n/zd}\Lambda(x)e(\alpha dxz)$$

and

$$U = \sum_{X<u\le n}\sum_{d|u, d\le X}\mu(d)\sum_{X<x\le n/u}\Lambda(x)e(\alpha xu).$$

Proof. Let us write τ_u for $\sum_{d|u,d\le X}\mu(d)$. Then, by Lemma 4.2, we know that τ_u is 1 when $u = 1$ and 0 when $1 < u \le X$. Therefore,

$$\sum_{u\le n}\tau_u\sum_{X<x\le n/u}\Lambda(x)e(\alpha xu) = U + \sum_{X<x\le n}\Lambda(x)e(\alpha x).$$

But, by Chebyshev's theorem (as in the proof of Lemma 4.4),

$$\sum_{X<x\le n}\Lambda(x)e(\alpha x) = g(\alpha) + O(n^{2/5}).$$

We also know that

$$\begin{aligned}\sum_{u\le n}\tau_u\sum_{X<x\le n/u}\Lambda(x)e(\alpha xu) &= \sum_{u\le n}\sum_{d|u,d\le X}\mu(d)\sum_{X<x\le n/u}\Lambda(x)e(\alpha xu)\\ &= \sum_{d\le X}\mu(d)\sum_{z\le n/d}\sum_{X<x\le n/dz}\Lambda(x)e(\alpha xzd)\\ &= S - T.\end{aligned}$$

The identity follows. □

In the next three lemmas, we show that each of S, T and U is small. Notice that S is the sum we originally expected to be able to bound, and is therefore in a sense the important one, while T and U are error terms that we were unable to avoid introducing.

Lemma 4.7. $|S| \leq 80(\log n)^3(q + X + n/q)$.

PROOF. Writing u for xz, we have

$$|S| = \Big|\sum_{d\leq X} \mu(d) \sum_{u\leq n/d} \sum_{x|u} \Lambda(x)e(\alpha du)\Big| \leq \sum_{d\leq X}\Big|\sum_{u\leq n/d} \log ue(\alpha du)\Big|$$

by Lemma 4.1. But

$$\begin{aligned}\Big|\sum_{u\leq n/d} \log ue(\alpha du)\Big| &= \Big|\sum_{u\leq n/d} \int_1^u e(\alpha du)\, dt/t\Big| \\ &\leq \textstyle\int_1^{n/d}\Big|\sum_{t\leq u\leq n/d} e(\alpha du)\Big|\, dt/t \\ &\leq \textstyle\int_1^{n/d} \min\{\|\alpha d\|^{-1}, n/d\}\, dt/t \\ &\leq \log n \min\{\|\alpha d\|^{-1}, n/d\}.\end{aligned}$$

Summing over $d \leq X$ and applying Lemma 4.5 (taking into account that $\log X = (2/5)\log n$) we obtain the bound claimed. □

Lemma 4.8. $|T| \leq 160(\log n)^3(q + X^2 + n/q)$.

PROOF. Interchanging the order of summation of z and x in the definition of T, and using the fact that $|\mu(d)| \leq 1$, we have

$$|T| \leq \sum_{d\leq X} \sum_{x\leq X} \Lambda(x)\Big| \sum_{z\leq n/dx} e(\alpha dxz)\Big|.$$

Now let $y = dx$, and this becomes

$$\sum_{y\leq X^2} \sum_{x\leq X, x|y} \Lambda(x)\Big| \sum_{z\leq n/y} e(\alpha yz)\Big|.$$

By Lemma 4.1, $\sum_{x\leq X,x|y} \Lambda(x) \leq \log y \leq \log n$, so we can bound this above by

$$\log n \sum_{k\leq X^2} \min\{\|\alpha y\|^{-1}, n/y\}$$

which is at most the bound stated, by Lemma 4.5. □

Lemma 4.9. $|U| \leq 40(\log n)^4(n^{1/2}q^{1/2} + n/X^{1/2} + nq^{-1/2})$.

PROOF. Given a positive integer i, let U_i be the sum

$$\sum_{u=2^{i-1}}^{2^i-1} |\tau_u| \Big| \sum_{X<x\leq n/u} \Lambda(x)e(\alpha xu)\Big|.$$

Notice that $U_i = 0$ when $2^{i-1} \geq n/X$ (because it is then impossible to satisfy the inequality $X < x \leq n/u$), and that $|U|$ is therefore at most the sum of all U_i over all i such that $2^i > X$ and $2^{i-1} < n/X$. It is easy to check that there are at most $\log n$ such values of i. (The fact that 2^i is between roughly $n^{2/5}$ and roughly $n^{3/5}$ more than compensates for the replacement of $\log_2 n$ by $\log n$.) We shall estimate the U_i separately. By the Cauchy-Schwarz inequality,

$$U_i^2 \leq \Big(\sum_{u=2^{i-1}}^{2^i-1} |\tau_u|^2\Big)\Big(\sum_{u=2^{i-1}}^{2^i-1} \Big| \sum_{X<x\leq n/u} \Lambda(x)e(\alpha xu)\Big|^2\Big).$$

Now $|\tau_u|$ is obviously at most $d(u)$, so

$$\begin{aligned}\sum_{u=2^{i-1}}^{2^i-1} |\tau_u|^2 &\leq \textstyle\sum_{u=2^{i-1}}^{2^i-1} d(u)^2 \\ &\leq \textstyle\sum_{u=1}^{2^i} d(u)^2 \ ,\end{aligned}$$

which is at most $2^i(\log n)^3$, by Lemma 4.3. As for the other bracket, if we expand out the modulus squared, we find that it equals

$$\sum_{u=2^{i-1}}^{2^i-1} \sum_{X<x\leq n/u} \sum_{X<y\leq n/u} \Lambda(x)\Lambda(y)e(\alpha(x-y)u).$$

Interchanging the sum over u with those over x and y, we find that this is at most

$$\sum_{X<x\leq n/2^{i-1}} \sum_{X<y\leq n/2^{i-1}} \Lambda(x)\Lambda(y)\Big| \sum_{2^{i-1}\leq u<2^i, u\leq \min\{n/x,n/y\}} e(\alpha(x-y)u)\Big|$$

which is at most

$$\sum_{X<x\leq n/2^{i-1}} \sum_{X<y\leq n/2^{i-1}} \Lambda(x)\Lambda(y)\min\{\|\alpha(x-y)\|^{-1}, 2^{i-1}\}.$$

Writing z for $x-y$ and observing that each z occurs at most $n/2^{i-1}$ times, we can bound this sum above by

$$(\log n)^2(n/2^{i-1}) \sum_{n/2^{i-1}<z\leq n/2^{i-1}} \min\{\|\alpha z\|^{-1}, 2^{i-1}\} \ ,$$

which, by Lemma 3.3 of the last chapter, is at most

$$(\log n)^2.48\log n(q+n/2^{i-2}+2^{i-1}+2n/q).$$

Multiplying the two estimates together, we have shown that

$$U_i^2\leq 96n(\log n)^6(q+4n/2^i+2^{i-1}+2n/q)\ ,$$

which implies, since $n/2^i$ and 2^{i-1} are at most n/X, that

$$U_i\leq 40(\log n)^3(n^{1/2}q^{1/2}+n/X^{1/2}+nq^{-1/2}).$$

Since there are at most $\log n$ values of i such that U_i contributes to U, the result follows. $\square$

Remarks. It may look complicated to split the sum into $\log n$ (or so) further pieces, but this was a good (and standard) thing to do because we were estimating something of the form $\sum_u f(u)g(u)$, where $f(u)$ appeared to be roughly proportional to u and $g(u)$ roughly proportional to u^{-1}. So applying the Cauchy-Schwarz inequality straight away would have been disastrous. Note that the choice of $X=n^{2/5}$ was made in order to minimize $\max\{X^2,nX^{-1/2}\}$.

If we put together Lemmas 4.4 and 4.6 to 4.9 we obtain the following result.

Theorem 4.10. *Let a,q be positive integers with $(a,q)=1$ and let α be a real number such that $|\alpha-a/q|\leq 1/q^2$. Then $\sum_{x\leq n}\Lambda(x)e(\alpha x)$ and $\sum_{p\leq n}\log p\, e(\alpha p)$ are both at most $50(\log n)^4(n^{1/2}q^{1/2}+n^{4/5}+nq^{-1/2})$, when n is sufficiently large.*

We have now managed to show that $f(\alpha)$ is small, provided that q is not too small. The usual approach to the rest of the proof is to estimate $f(\alpha)$ when α *is* close to a rational with small denominator, using the Siegel-Walfisz theorem (see [19]), and then combine these results to obtain a fairly accurate estimate for $\int f(\alpha)^3e(-\alpha n)\,d\alpha$ (in particular, accurate enough to show that it is non-zero). In these notes, a different argument is used, which is believed to explain, in a more intuitive way, why the integral comes out to be positive. It has the added advantage that we do not actually need to estimate the integral at all accurately, although it is possible to work harder in order to do so.

The main idea is to work out exactly what is meant by the familiar idea that the primes are somehow randomly distributed. A minor problem to worry about first is that there are more small primes than large ones, but we have already dealt with that by weighting a prime p by $\log p$. Now, in chapter 2, we thought of a subset A of $\{1, 2, \ldots, n\}$ as being random if the Fourier coefficients $\hat{A}(r)$ were all much smaller than n, for non-zero r. However, it is clear that the primes are not random in this sense, because, for example, only one prime is a multiple of five.

Which constraints of this kind have an effect on Fourier coefficients? It is an easy exercise to show that congruence conditions mod q have an effect if and only if q is small. Motivated by this observation, we let $p_1, \ldots, p_k$ be the primes less than or equal to $(\log n)^A$, in ascending order, and define Q to be the set of integers less than or equal to n that are not multiples of any p_i. Here, A is an absolute constant (in fact we shall choose $A = 16$), but there is some freedom in the argument, and we could have made p_k quite a bit larger. What we shall do in the rest of the section is show that the weighted primes behave like a random subset of Q.

It is not hard to work out how to interpret this statement. It means that the Fourier transforms $f(\alpha) = \sum_{p \leq n} \log p\, e(\alpha p)$ and $h(\alpha) = \sum_{x \in Q} e(\alpha x)$ are roughly proportional. This implies that integrals involving these functions are also roughly proportional, so that, roughly speaking, whatever is true for Q is true for the weighted primes as well. (That "roughly speaking" is important: a good exercise is to see why Lemma 4.20 below does not translate into a solution of the Goldbach conjecture.)

We begin by obtaining an estimate similar to Theorem 4.10 for the function $h(\alpha)$. The proof is much simpler, however.

Lemma 4.11. *Suppose that $(a, q) = 1$ and $|\alpha - a/q| \leq q^{-2}$. Then*

$$|h(\alpha)| \leq 100(\log n)^2(n^{1/2} + q + nq^{-1} + n^{1-1/4A}).$$

PROOF. Notice first that

$$h(\alpha) = \sum_{s=0}^{k}(-1)^s \sum_{1 \leq i_1 \leq \ldots \leq i_s \leq k} \; \sum_{y \leq n/p_{i_1} \ldots p_{i_s}} e(\alpha p_{i_1} \ldots p_{i_s} y).$$

The justification of this is similar to the proof of Lemma 4.2. If $z \in Q$ then $e(\alpha z)$ is added when $s = 0$, and otherwise does not appear. If $z \notin Q$ then $z = p_{j_1}^{a_1} \ldots p_{j_r}^{a_r} w$

for some $w \in Q$, and $a_i \geq 1$, and $e(\alpha z)$ is added $(-1)^{|B|}$ times for every subset B of $\{j_1, dots, j_r\}$, giving a total contribution of zero.

The inner sum is at most $\min\{\|\alpha p_{i_1} \dots p_{i_s}\|^{-1}, n/p_{i_1} \dots p_{i_s}\}$. Let $t = \log n / 2A \log\log n$ and note that $p_k^t \leq \sqrt{n}$. These estimates and the fundamental theorem of arithmetic imply that

$$\Big|\sum_{s=0}^{t}(-1)^s \sum_{1 \leq i_1 \leq \dots \leq i_s \leq k} \; \sum_{y \leq n/p_{i_1} \dots p_{i_s}} e(\alpha p_{i_1} \dots p_{i_s} y)\Big|$$

is at most $\sum_{x \leq \sqrt{n}} \min\{\|\alpha x\|^{-1}, n/x\}$, which, by Lemma 4.5, is at most $100(\log n)^2(n^{1/2} + q + nq^{-1})$.

The rest of the sum is, in modulus, at most

$$\sum_{s=t+1}^{k} \sum_{1 \leq i_1 \leq \dots \leq i_s \leq k} n \prod_{j=1}^{s} p_{i_j}^{-1} \ ,$$

which is at most

$$n \sum_{s=t+1}^{k} (s!)^{-1}(p_1^{-1} + \dots + p_k^{-1})^s .$$

It is well known (and follows from the prime number theorem) that $p_1^{-1} + \dots + p_k^{-1}$ is about $\log\log k$, and so at most $2\log\log\log n$, when n is sufficiently large. Approximating $s!$ by $(s/e)^s$, we obtain an upper bound of $2n(2e\log\log\log n/t)^t$, since $t \geq 4e\log\log\log n$. It is not hard to check that this is at most $n^{-1/4A}$ when n is sufficiently large. This, together with the first estimate, proves the lemma. $\square$

We now turn to the "major-arcs" estimates, that is, estimates for $f(\alpha)$ and $h(\alpha)$ when α is close to a rational with small denominator. It turns out that such estimates are more or less equivalent to estimating $\sum_{p \in X} \log p$ and $|X \cap Q|$ for certain long arithmetic progressions X. In the case of the primes themselves, we shall appeal to known estimates of this type, as given in the next result, the Siegel-Walfisz theorem.

Siegel-Walfisz Theorem. *Let A be a positive real number, let x be an integer, let $q \leq (\log x)^A$ be another integer and let $(a, q) = 1$. Then*

$$\sum_{p \leq x, p \equiv a\,(q)} \log p = \frac{x}{\phi(q)} + O(\exp(-C\sqrt{\log x})) \ ,$$

where C is a constant depending on A only.

Notice that from the Siegel-Walfisz Theorem it follows that, if $q \leq (\log n)^A$, and X is the arithmetic progression $\{a, a+q, \ldots, a+(m-1)q\}$, where $(a,q)=1$ and $1 \leq a \leq n-(m-1)q$, then for any constant B, we have

$$\sum_{p \in X} \log p = \frac{mq}{\phi(q)} + O(n/(\log n)^B) \ ,$$

with the implied constant in the error term depending on A and B only.

We shall now obtain an estimate for $|X \cap Q|$, when X is an arithmetic progression of the kind above.

Lemma 4.13. *Let $q \leq (\log n)^A$, let $X = \{a, a+q, \ldots, a+(m-1)q\}$ be a subset of $[N]$ with $m \geq N^{1/2}$ and suppose that $(q,a)=1$. Then*

$$|X \cap Q| = \frac{mq}{\phi(q)} \prod_{i=1}^{k} (1-p_i^{-1}) + O(mn^{-1/4A}).$$

PROOF. Let $x \in X$ be chosen uniformly at random, and for each i let X_i be the event $p_i|x$. Then the probability of X_i is $p_i^{-1} + O(m^{-1})$ if $p_i \not| q$ and $O(m^{-1})$ if $p_i|q$. More generally, for any choice $1 \leq i_1 \leq \ldots \leq i_s \leq k$ we have

$$\mathrm{Prob}(X_{i_1} \cap \ldots \cap X_{i_s}) = \prod_{j=1}^{s} \epsilon_{i_j}/p_{i_j} + O(m^{-1}) \ ,$$

where $\epsilon_i = 1$ if $p_i \not| q$ and 0 if $p_i|q$. It follows from this and the inclusion-exclusion formula that, for any t,

$$1 - \mathrm{Prob}\Big(\bigcup_{i=1}^{k} X_i\Big) = \sum_{s=0}^{t} (-1)^s \sum_{1 \leq i_1 \leq \ldots \leq i_s \leq k} \prod_{j=1}^{s} \epsilon_{i_j}/p_{i_j} + O(m^{-1}) \sum_{s=1}^{t} \binom{k}{s} .$$

Now

$$\prod_{i=1}^{k} (1-\epsilon_i/p_i) = \sum_{s=0}^{k} (-1)^s \sum_{1 \leq i_1 \leq \ldots \leq i_s \leq k} \prod_{j=1}^{s} \epsilon_{i_j}/p_{i_j}$$

and

$$\begin{aligned} \sum_{1 \leq i_1 \leq \ldots \leq i_s \leq k} \prod_{j=1}^{s} \epsilon_{i_j}/p_{i_j} &\leq (s!)^{-1}(p_1^{-1} + \ldots + p_k^{-1})^s \\ &\leq (4e \log\log\log n/s)^s \end{aligned}$$

when n is sufficiently large. If $t \geq 8e \log\log\log n$, then this quantity summed from $t+1$ to k is at most $(4e \log\log\log n/t)^t$. Furthermore, $\sum_{s=1}^{t} \binom{k}{s}$ is easily seen to be at most k^t. It follows that

$$1 - \mathrm{Prob}\Big(\bigcup_{i=1}^{k} X_i\Big) = \prod_{i=1}^{k} (1-\epsilon_i/p_i) + O((\log n)^{At} + (4e \log\log\log n/t)^t).$$

Choosing t to be $\log n/2A\log\log n$ gives an error of at most $O(n^{-1/4A})$, as in the proof of Lemma 4.11. Note finally that

$$\begin{aligned}\prod_{i=1}^{k}(1-\epsilon_i/p_i) &= \prod_{i=1}^{k}(1-1/p_i)\prod_{p_i|q}(1-1/p_i)^{-1}\\ &= \prod_{i=1}^{k}(1-1/p_i)\prod_{p|q}(1-1/p)^{-1}\\ &= \frac{q}{\phi(q)}\prod_{i=1}^{k}(1-p_i^{-1}).\end{aligned}$$

Multiplying everything by m proves the lemma. □

Corollary 4.14. *Let a,q,X be as in Lemma 4.13, let $K=\prod_{i=1}^{k}(1-p_i^{-1})^{-1}$ and let B be any positive constant. Then*

$$K|X\cap Q|-\sum_{p\in X}\log p=O(n(\log n)^{-B}).$$

Proof. This follows immediately from Lemma 4.13 and the remark following Lemma 4.12. (Strictly speaking one must consider what happens if $(a,q)\neq 1$ but then it is easy to see that both $K|X\cap Q|$ and $\sum_{p\in X}\log p$ are very small.) □

Lemma 4.15. *Let $q\leq(\log n)^A$, let $(b,q)=1$ and let α be a real number such that $|\alpha-b/q|\leq(\log n)^A/qn$. Let G be a function from $\{1,2,\dots,n\}$ to $\mathbb{R}$ such that $|G(x)|\leq\log n$ for every x and such that*

$$\Big|\sum_{x\in X}G(x)\Big|=O(n(\log n)^{-B})$$

for every arithmetic progression $X=\{a,a+q,\dots,a+(m-1)q\}$, where $B\geq 4A+2$. Then

$$\Big|\sum_{x\leq n}G(x)e(\alpha x)\Big|=O(n(\log n)^{-A}).$$

Proof. Let $\beta=\alpha-b/q$ and let X be one of the arithmetic progressions of the above type. Notice that, if $x,y\in X$, then

$$|e(\beta x)-e(\beta y)|=|1-e(\beta(x-y))|\leq 2\pi|x-y||\beta|\leq 2\pi m(\log n)^A/n.$$

Therefore, letting x_0 be an arbitrary element of X, we have

$$\Big|\sum_{x\in X}G(x)e(\alpha x)\Big| = \Big|\sum_{x\in X}G(x)e(bx/q)e(\beta x)\Big|$$

$$
\begin{aligned}
&\le \left|e(ab/q)\sum_{x\in X} G(x)(e(\beta x)-e(\beta_0 x))\right| + \left|e(ab/q)e(\beta x_0)\sum_{x\in X} G(x)\right| \\
&= \left|\sum_{x\in X} G(x)(e(\beta x)-e(\beta x_0))\right| + \left|\sum_{x\in X} G(x)\right| \\
&\le (2\pi m(\log n)^A/n)m\log n + O(n(\log n)^{-B}) \\
&= O((\log n)^{A+1}m^2n^{-1} + n(\log n)^{-B}).
\end{aligned}
$$

But we can partition $[n]$ into $2n/m_0$ arithmetic progressions of the form of X, with $m \le m_0$ in each case. Therefore, choosing $m_0 = n(\log n)^{-B/2}$ and summing over all these, we find that

$$\left|\sum_{x\le n} G(x)e(\alpha x)\right| = O(n(\log n)^{A+1-B/2})$$

which proves the result. □

Recall that $f(\alpha) = \sum_{p\le n}\log p\, e(\alpha p)$. Let us define $h_1(\alpha)$ to be $K\sum_{x\in Q} e(\alpha x) = Kh(\alpha)$.

Corollary 4.16. *Let $A = 16$. Then, for every real number α, $f(\alpha) - h_1(\alpha) = O(n(\log n)^{-A/4})$.*

Proof. Let α be a real number. Then we can find $q \le n(\log n)^{-A}$ and b with $(b,q) = 1$ such that $|\alpha - b/q| \le (\log n)^A/nq$. If $q \ge (\log n)^A$, then Theorem 4.10 implies that $f(\alpha) = O(n(\log n)^{4-A/2})$, while Lemma 4.11 (with an easy estimate for K) implies that $h_1(\alpha) = O(n(\log n)^{3-A})$, so the result holds.

If on the other hand $q \le (\log n)^A$, then set $G(x) = \log x - KQ(x)$ if x is prime, and $-KQ(x)$ otherwise. Corollary 4.14 tells us that G satisfies the conditions for Lemma 4.15. But $\sum_{x\le n} G(x)e(\alpha x) = f(\alpha) - h_1(\alpha)$, so Lemma 4.15 gives us the result in this case. □

This is all we need for the three-primes theorem. However, it is perhaps of some interest to obtain an actual estimate for $f(\alpha)$ and $h_1(\alpha)$ when q is small, rather than merely showing that they are close. So the next two lemmas are here for interest only.

For notational convenience, when we write $(a,q) = 1$ in the next lemma we shall mean that a and q are coprime and that $1 \le a \le q$.

Lemma 4.17. *For every q, $\sum_{(a,q)=1} e(a/q) = \mu(q)$.*

PROOF. If $q = 1$ then the result holds. If q is a prime, then

$$\sum_{(a,q)=1)} e(a/q) = \sum_{1\leq a<q} e(a/q) = 0 - 1 = -1.$$

If $q = p^k$ with p prime and $k \geq 2$, then

$$\sum_{(a,q)=1} e(a/q) = \sum_{1\leq a\leq q} e(a/q) - \sum_{1\leq b\leq p^{k-1}} e(b/p^{k-1}) = 0 - 0 = 0.$$

Finally, if q and r are coprime, then

$$\sum_{(a,q)=1} e(a/q) \sum_{(b,r)=1} e(b/r) = \sum_{(a,q)=1,(b,r)=1} e(ar + bq/qr).$$

But $ar+bq$ runs through all residues mod qr, and $(ar+bq, qr) = 1$ if and only if $(a,q) = 1$ and $(b,r) = 1$. So the sum is $\sum_{(a,qr)=1} e(a/qr)$.
These properties of the left hand side force it to equal μ.

$\square$

Now, given $q \leq (\log n)^A$, let us define a function $H_q : [n] \to \mathbb{R}$ by letting $H_q(x)$ equal $q/\phi(q)$ if $(x,q) = 1$ and zero otherwise.

Lemma 4.18. *Let $q \leq (\log n)^A$, let $(b,q) = 1$ and let α be a real number such that $|\alpha - b/q| \leq (\log n)^A/nq$. Let $\beta = \alpha - b/q$. Then*

$$\sum_{x\leq n} H_q(x)e(\alpha x) = \frac{\mu(q)}{\phi(q)} \sum_{x\leq n} e(\beta x) + O((\log n)^{2A}).$$

PROOF. Let us write X_a for the set of integers less than or equal to n and congruent to a mod q. If $(a,q) \neq 1$, then clearly $\sum_{x\in X_a} H_q(x)e(\alpha x) = 0$. On the other hand, if $(a,q) = 1$, then

$$\begin{aligned}\sum_{x\in X_a} H_q(x)e(\alpha x) &= \frac{q}{\phi(q)} \sum_{x\in X_a} e(bx/q)e(\beta x) \\ &= \frac{q}{\phi(q)} e(ab/q) \sum_{x\in X_a} e(\beta x).\end{aligned}$$

Now, if $a_1, a_2 \leq q$, then

$$\Big|\sum_{x\in X_{a_1}} e(\beta x) - \sum_{x\in X_{a_2}} e(\beta x)\Big| \leq 1 + \Big|\sum_{x\in X_{a_1}} e(\beta x)\Big||1 - e(\beta(a_1 - a_2))|.$$

Since $|a_1 - a_2| \leq q$, we know that $1 - e(\beta(a_1 - a_2)) = O((\log n)^A/n)$, so this shows that, for every a,

$$\sum_{x \in X_a} e(\beta x) = q^{-1} \sum_{x \leq n} e(\beta x) + O((\log n)^A).$$

(In words, the numbers $\sum_{x \in X_a} e(\beta x)$ are all approximately equal, and therefore all approximately equal to their average.) It follows that

$$\sum_{0 \leq a < q} \sum_{x \in X_a} H_q(x) e(\alpha x) = \frac{q}{\phi(q)} \sum_{(a,q)=1} e(ab/q) \Big(q^{-1} \sum_{x \leq n} e(\beta x) + O(\log n)^A \Big).$$

Since $(b, q) = 1$, the result follows from Lemma 4.17. □

Corollary 4.19. *Let α, b, q and β be as in Lemma 4.18. Then $f(\alpha)$ and $h_1(\alpha)$ are both equal to $(\mu(q)/\phi(q)) \sum_{x \leq n} e(\beta x) + O(n(\log n)^{-A})$.*

Proof. This follows easily from Theorem 4.12 and Lemmas 4.13, 4.15 and 4.18. Let $P(x)$ be the function $\log x$ if x is prime and zero otherwise. Setting $G(x) = P(x) - H_q(x)$, Theorem 4.12 tells us that the conditions for Lemma 4.15 are satisfied. But this implies that $f(\alpha) = \sum_{x \leq n} H_q(x) e(\alpha x) + O(n(\log n)^{-A})$. Then Lemma 4.18 gives us our estimate for $f(\alpha)$. The same argument works for $h_1(\alpha)$ if we use Lemma 4.13 instead of Theorem 4.12. □

After that diversion, let us now finish the proof of the three-primes theorem. There are two steps to the proof. First, we show that every sufficiently large odd integer is the sum of three elements of Q (or fake primes) in many ways, using the Brun sieve once again. Then we deduce, from the fact that f and h_1 are uniformly close, that the same is true of the genuine primes.

Lemma 4.20. *Let m be an integer. Then the number of ways of writing $m = x + y$ with x and y both in Q is at least $m \prod_{i=1}^{k} (1 - r_i/p_i) + O(m^{-1} n^{1/2} + mn^{-1/4A})$, where $r_i = 1$ if $p_i | m$ and 2 otherwise.*

Proof. Choose x randomly and uniformly from the set $[m]$. For each i let X_i be the event that $p_i | x$ or $p_i | m - x$. As in the proof of Lemma 4.13, it is easy to show that $\text{Prob}(X_i) = r_i/p_i + O(m^{-1})$. (The point about the r_i is that the events $p_i | x$ and $p_i | m - x$ are the same if $p_i | m$ and mutually exclusive otherwise.) More generally, it is not hard to show that

$$\text{Prob}(X_{i_1} \cap \ldots \cap X_{i_s}) = \prod_{j=1}^{s} \frac{r_{i_j}}{P_{i_j}} + O(m^{-1}).$$

Therefore, by the inclusion-exclusion formula,

$$1 - \mathrm{Prob}\Big(\bigcup_{i=1}^{k} X_i\Big) = \sum_{s=0}^{t}(-1)^s \sum_{1\le i_1\le\ldots\le i_s\le k}\prod_{j=1}^{s} r_{i_j}/p_{i_j} + O(m^{-1})\sum_{s=1}^{t}\binom{k}{s}.$$

But

$$\prod_{i=1}^{k}(1 - r_i/p_i) = \sum_{s=0}^{k}(-1)^s \sum_{1\le i_1\le\ldots\le i_s\le k}\prod_{j=1}^{s} r_{i_j}/p_{i_j}$$

and

$$\begin{aligned}\sum_{1\le i_1\le\ldots\le i_s\le k}\prod_{j=1}^{s} r_{i_j}/p_{i_j} &\le (s!)^{-1}(2p_1^{-1} + \ldots + 2p_k^{-1})^s \\ &\le (8e\log\log\log n/s)^s.\end{aligned}$$

As in the proof of Lemma 4.13, it follows that

$$1 - \mathrm{Prob}\Big(\bigcup_{i=1}^{k} X_i\Big) = \prod_{i=1}^{k}(1 - r_i/p_i) + O(m^{-1}(\log n)^{At} + (8e\log\log\log n/t)^t)$$

for any $t \ge 16e\log\log\log n$. Choosing t to be $\log n/2A\log\log n$ implies the lemma. $\square$

Corollary 4.21. *If n is sufficiently large and odd, then the number of ways of writing n as the sum of three elements of Q is at least $(n^2/16)K^{-1}\prod_{i=2}^{k}(1-2p_i^{-1})$.*

PROOF. Note first that Lemma 4.13 implies that the number of elements of Q less than or equal to $n/2$ is at least $K^{-1}n/4$ (when n is sufficiently large). For every odd $z \le n/2$, the number of ways of writing $n - z$ as the sum of two elements of Q is, by Lemma 4.20, at least $(n/4)\prod_{i=2}^{k}(1 - 2/p_i)$. The result follows. $\square$

It is possible to be much more careful and work out the number of ways of writing n as the sum of three elements of Q to within a factor $1 + o(1)$, but we do not need this.

Vinogradov's Three-Primes Theorem. *Every sufficiently large odd integer is the sum of three primes.*

PROOF. Note first that $(16K)^{-1}\prod_{i=2}^{k}(1-2p_i^{-1})$ is easily shown to be at least $(\log n)^{-1}$ when n is sufficiently large, so the number of ways of writing n as the sum of three elements of Q is at least $n^2/\log n$. On the other hand, it is also $\int h(\alpha)^3 e(-\alpha n)\,d\alpha$, so we certainly have $\int h_1(\alpha)^3 e(-\alpha n)\,d\alpha \ge n^2/\log n$.

As we commented at the beginning, it is sufficient for our purposes to establish that $\int f(\alpha)^3 e(-\alpha n)\, d\alpha \neq 0$. But, by Corollary 4.16,

$$\begin{aligned}
\Big|\int f(\alpha)^3 e(-\alpha n)\, d\alpha \;&-\; \int h_1(\alpha)^3 e(-\alpha n)\, d\alpha\Big| \\
&= O(n(\log n)^{-A/4}) \int |f(\alpha)^2 + f(\alpha)h_1(\alpha) + h_1(\alpha)^2|\, d\alpha \\
&= O(n(\log n)^{-A/4}) \int |f(\alpha)|^2 + |h_1(\alpha)|^2\, d\alpha \\
&= O(n(\log n)^{-A/4}) \;\Big(\sum_{p \leq n} (\log p)^2 + K^2|Q|\Big) \\
&= O(n^2 \log n (\log n)^{-A/4}).
\end{aligned}$$

Since we chose A to be 16, this and our estimate for the integral with h_1 are enough to prove the theorem. □

§5 The Geometry of Numbers

A *lattice* in $\mathbb{R}^n$ is a subgroup generated by n linearly independent vectors. A *basis* for a lattice Λ is a linearly independent set in Λ that generates Λ.

Lemma 5.1. *Let Λ be a lattice and let $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ be distinct bases of Λ. Let $\alpha : x_i \mapsto y_i$ be linear. Then $det(\alpha) = 1$.*

Proof. Each y_i is an integer combination of x_i so both α and α^{-1} are non-singular and have integer determinants. $\square$

Let Λ be a lattice with basis $x_1, x_2, \ldots, x_n$. The *fundamental parallellopiped* of Λ with respect to $x_1, x_2, \ldots, x_n$ is the set $P = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n : 0 \leq a_i < 1\}$. Note that the sets $x + P$, $x \in \Lambda$ are disjoint and their union is $\mathbb{R}^n$. The *determinant* $\det(\Lambda)$ of Λ is the volume of P, which is well-defined by the Lemma 5.1. Alternatively, $\det(\Lambda)$ is $|\det(A)|$, where $A = (x_1, x_2, \ldots, x_n)$ and the x_i are column vectors with respect to the canonical basis for $\mathbb{R}^n$. A *convex body* is a bounded convex open subset of $\mathbb{R}^n$.

Lemma 5.2. *Let Λ be a lattice and suppose that K is a convex body in $\mathbb{R}^n$. Then $vol(K) = \lim_{t\to\infty} |\Lambda \cap tK| det(\Lambda)/t^n$.*

Proof. Let Q be a translate of a fundamental parallellopiped P of Λ. Then tQ contains exactly t^n points in Λ if t is an integer. However, $|\Lambda \cap tQ|$ lies between $\lfloor t \rfloor^n$ and $\lceil t \rceil^n$. Therefore the result is true for all sets of the form $z + \rho P$ with $z \in \mathbb{R}^n$ and $\rho > 0$. As K is convex, it can be approximated by finite unions of such sets. $\square$

A *sublattice* of a lattice Λ in $\mathbb{R}^n$ is a subgroup $M \subset \Lambda$ which is also a lattice.

Lemma 5.3. *Let Λ be a lattice and let M be a sublattice of Λ. Then the index of M as a subgroup of Λ is $det(M)/det(\Lambda)$.*

Proof. Let P be a fundamental parallellopiped for M. Then every vector $x \in \mathbb{R}^n$ can be written uniquely as $y + z$, where $y \in M$ and $z \in P$. Therefore every $x \in \Lambda$ can be written uniquely as $y + z$ with $y \in M$ and $z \in \Lambda$. So the index of M is $|P \cap \Lambda|$. If t is an integer, $|tP \cap \Lambda| = t^n|P \cap \Lambda|$. Thus $\mathrm{vol}P = |P \cap \Lambda|\det(\Lambda)$, by Lemma 5.2, and it follows that $\det(M) = |P \cap \Lambda|\det(\Lambda)$. $\square$

Blichfeldt's Lemma. *Let $K \subset \mathbb{R}^n$ be a measurable set, Λ a lattice and suppose vol$(K) >$ det(Λ). Then $K - K$ contains a non-zero lattice point.*

Proof. Let $x_1, x_2, \ldots, x_n$ be a basis for Λ and let $Q = \{a_1x_1 + \ldots + a_nx_n : -1 \leq a_i < 1\}$. Then $\mathrm{vol}(K) = 2^n \mathrm{det}(\Lambda)$ and Q contains 2^n points of Λ. Provided M is sufficiently large, $\mathrm{vol}(K \cap MQ)$ is still greater than $\det(\Lambda)$. So $K \subset MQ$. Let N be an integer, chosen such that $(1 + M/N)^n < \mathrm{vol}(K)/\det(\Lambda)$. If the lemma were false, then the sets $x + K, x \in \Lambda \cap NQ$ are disjoint. The union of these sets is contained in $(M + N)Q$ and has volume $(2N)^n \mathrm{vol}(K)$, since there are $(2N)^n$ lattice points in Q. Therefore $(2N)^n \mathrm{vol}(K) \leq (2(N + M))^n \det(\Lambda)$. By the choice of M, this is a contradiction. □

Minkowski's First Theorem. *Let Λ be a lattice and let K a centrally symmetric convex body with vol$(K) > 2^n$det(Λ). Then K contains a non-zero point of Λ.*

Proof. As K is convex and centrally symmetric, $K = \frac{1}{2}K - \frac{1}{2}K$. However, $\mathrm{vol}\frac{1}{2}K > \det(\Lambda)$, so the result follows by Blichfeldt's Lemma. □

Let Λ be a lattice, let K be a centrally symmetric convex body. Define $0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$ by $\lambda_k = \inf\{\lambda : \lambda K$ contains k linearly independent vectors in $\Lambda\}$. The numbers $\lambda_1, \lambda_2, \ldots, \lambda_n$ are called the *successive minima of K with respect to* Λ. Note that we can find vectors $b_1, b_2, \ldots, b_k \in \mathbb{R}^n$ such that $b_k \in \lambda_k \overline{K} \cap \Lambda$ for each $k \leq n$. These b_i actually form a basis for Λ.

Minkowski's Second Theorem. *Let Λ be a lattice and let K be a convex body. Suppose $0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$ are the successive minima of K with respect to Λ. Then $\lambda_1\lambda_2 \ldots \lambda_nvol(K) \leq 2^ndet(\Lambda)$.*

Proof. Let $b_1, b_2, \ldots, b_n$ be a basis as defined above. Set $V_1 = \{0\}$ and, for each i, set $V_i = \langle b_1, b_2, \ldots, b_{i-1}\rangle$ and $W_i = \langle b_i, b_{i+1}, \ldots, b_n\rangle$. Define a map $c_i : iK \to K$ by setting $c_i(x)$ equal to the centre of gravity of $(x + V_i) \cap K$. We note that c_i is continuous (K is open) and $c_i(x)$ does not depend on the first $i-1$ co-ordinates of x. Also $c_i(x) - x \in V_i$ and so if $c_i(x)_j$ is the jth co-ordinate of $c_i(x)$ with respect to $b_1, b_2, \ldots, b_n$, then $c_i(x)_j = x_j$ for $j \geq i$. Now define $\phi(x) = \sum_{i=1}^n (\lambda_i - \lambda_{i-1})c_i(x)$, with $\lambda_0 = 0$. Then, expanding $\phi(x)$,

$$\begin{aligned}
\phi(x) &= \sum_{i=1}^{n} (\lambda_i - \lambda_{i-1}) \sum_{j=1}^{n} c_i(x)_j b_j \\
&= \sum_{j=1}^{n} b_j \Big[\sum_{i=1}^{j} c_i(x)_j (\lambda_i - \lambda_{i-1})\Big]
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=1}^{n} b_j\Big[\sum_{i=1}^{j} x_j(\lambda_j - \lambda_{j-1}) + \sum_{i=j+1}^{n} c_i(x)_j(\lambda_i - \lambda_{i-1})\Big] \\
&= \sum_{j=1}^{n} b_j(\lambda_j x_j + \phi_j(x_{j+1}, \dots, x_n),
\end{aligned}
$$

where ϕ_j is some continuous function. The next claim is that $\mathrm{vol}\phi(K) = \lambda_1\lambda_2\dots\lambda_n\mathrm{vol}(K)$. First note that $\phi(x)_n = \lambda_n x_n$. For fixed t, let $K(t)$ denote the cross section $\{x \in K : x_n = t\}$ of K. Then ϕ restricted to $K(t)$ can be represented by a formula

$$
\phi(\sum_{i=1}^{n-1} x_i b_i + t b_n) = \lambda_n t b_n + \sum_{j=1}^{n-1} b_j(\lambda_j x_j + \psi_j(x_{j+1}, \dots, x_{n-1})
$$

as t is fixed, so by induction $\mathrm{vol}(\phi(K(t))) = \mathrm{vol}\{y \in \phi(K) : y_n = \lambda_n t\} = \lambda_1\lambda_2\dots\lambda_{n-1}$. Applying Fubini's theorem, the theorem is proved. □

For further reading on Minkowski's Theorems, see [15].

Let $r_1, r_2, \dots, r_k \in \mathbb{Z}_n$ and $\delta > 0$. Then the *Bohr neighbourhood* $B(r_1, r_2, \dots, r_k; \delta)$ is the set $\{s \in \mathbb{Z}_n : |r_i s| \leq \delta N, i = 1, 2, \dots, k\}$ where $|r_i s|$ is the distance from $r_i s$ to the nearest multiple of N. A *d-dimensional arithmetic progression* is a subset of $\mathbb{Z}$ or $\mathbb{Z}_N$ of the form $\{x_0 + \sum_{i=1}^{d} a_i x_i : 0 \leq a_i < s_i\}$. It is *proper* if the numbers $\sum_{i=1}^{d} a_i x_i$ are all distinct. It will be seen, in §6, that Bohr neighbourhoods can be used as a step in finding arithmetic progressions, using Fourier transforms.

Theorem 5.7. *Let $r_1, r_2, \dots, r_k \in \mathbb{Z}_N$ and $0 < \delta < 1/2$. Then the Bohr neighbourhood $B(r_1, \dots, r_k, \delta)$ contains a proper k-dimensional arithmetic progression of cardinality at least $(\delta/k)^k N$.*

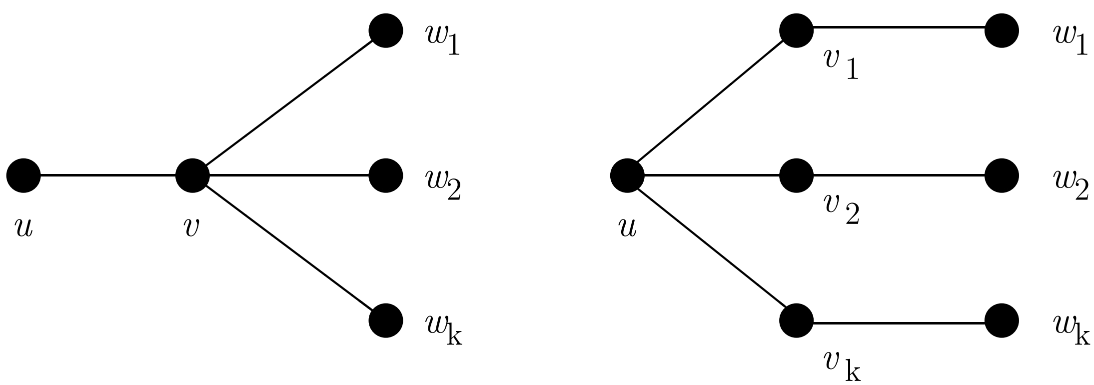
Proof. We have $s \in B(r_1, r_2, \dots, r_k; \delta)$ if and only if $(r_1 s, r_2 s, \dots, r_k s)$ lies within ℓ_∞^k-distance δN of a point in $N\mathbb{Z}^k$. Or, equivalently, $(r_1 s, r_2 s, \dots, r_k s) + N\mathbb{Z}^k$ contains a point x with $\|x\|_\infty \leq \delta N$. Let Λ be the lattice generated by $N\mathbb{Z}^k$ and $(r_1, r_2, \dots, r_k)$. The index of $N\mathbb{Z}^k$ is clearly N^k, and it has index N in Λ. Therefore Λ has index N^{k-1} in $\mathbb{Z}^k$, implying $\det(\Lambda) = N^{k-1}$ by Lemma 5.3. Let $K = \{(a_1, a_2, \dots, a_k) : -1 < a_i < 1\}$; we apply Minkowski's Second Theorem to K and Λ, to obtain a basis $b_1, b_2, \dots, b_k$ of $\mathbb{R}^k$ with $b_i \in \Lambda$ and b_i having $\|b\|_\infty = \lambda_i$, where $\lambda_1\lambda_2\dots\lambda_k\mathrm{vol}(K) \leq \det(\Lambda) \cdot 2^k$. Therefore $\lambda_1\lambda_2\dots\lambda_k \leq N^{k-1}$. Now notice that if $a_1, a_2, \dots, a_k$ are integers with $|a_i| \leq \delta N/k\lambda_i$, then $\|\sum a_i b_i\| \leq \sum(\delta N/\lambda_i k) \cdot \lambda_i = \delta N$. However b_i is a vector of the form

$(r_1 s_i, r_2 s_i, \dots, r_k s_i)$. So $|\sum a_i s_i r_j| \le \delta N$, $j = 1, 2, \dots, k$. Let P be the k-dimensional arithmetic progression $\{\sum_{i=1}^k a_i s_i : |a_i| \le \delta N / k\lambda_i\}$. As the vectors $b_1, b_2, \dots, b_k$ are independent and $\|\sum a_i b_i\| \le \delta N$, P is proper – no two terms are equal (mod N). The number of integers a_i in the interval $[-\delta N/k\lambda_i, \delta N/k\lambda_i]$ is at least $\delta N/k\lambda_i$, therefore $|P| \ge \prod \delta N/k\lambda_i = (\delta/k)^k N^k \cdot (\lambda_1 \lambda_2 \dots \lambda_k)^{-1} \ge (\delta/k)^k N$. $\square$

A *layered graph* is a graph G with vertex set comprising a disjoint union $V_0 \cup V_1 \cup \dots \cup V_n$ of sets such that each edge lies between V_i and V_{i+1} for some $i \in [0, n-1]$. It will often be convenient to have an implicit orientation of the edges, from V_i to V_{i+1} for each i. A layered graph G is called a *Plünnecke Graph* if it satisfies the following two conditions:

(1) For $u \in V_{i-1}$, $v \in V_i$ and distinct $w_1, w_2, \dots, w_k \in V_{i+1}$ with $uv, vw_i \in E(G)$, $i = 1, 2, \dots, k$ then there exist distinct $v_1, v_2, \dots, v_k \in V_i$ such that uv_i and $v_i w_i \in E(G)$.

(2) For distinct $u_1, u_2, \dots, u_k \in V_{i-1}$, $v \in V_i$ and $w \in V_{i+1}$, $u_i v, v_i w \in E(G)$ there exist distinct $v_1, v_2 \dots, v_k$ such that $u_i v_{i-1}, v_i w \in E(G)$.



Given two layered graphs G, H with vertex sets $V_0 \cup V_1 \cup \dots \cup V_n$ and $W_0 \cup W_1 \dots \cup W_n$, the product graph $G \times H$ has vertex set $V_0 \times W_0 \cup V_1 \times W_1 \cup \cdots \cup V_n \times W_n)$ and (v, w) joined to (v', w') if and only if $vv' \in E(G)$ or $ww' \in E(G)$. It is easily seen that $G \times H$ is a Plünnecke Graph if G and H are. The *ith magnification ratio* $D_i(G)$ of a layered graph G with vertex set $V_0 \cup V_1 \cup \dots \cup V_n$ is defined to be

$$\min\Big\{\frac{|\mathrm{Im}_i(Z)|}{|Z|} : Z \subset V_0, Z \ne \emptyset\Big\}$$

where $\mathrm{Im}_i(Z) = \{y \in V_i :$ there is a directed path from some $z \in Z$ to $y\}$.

Lemma 5.8. *Let G, H be layered graphs. Then $D_i(G \times H) = D_i(G)D_i(H)$.*

Proof. Suppose G, H have vertex sets $V_0 \cup V_1 \cup \ldots \cup V_n$ and $W_0 \cup W_1 \cup \ldots \cup W_n$ respectively. Let $Y \subset V_0$, $Z \subset W_0$ satisfy $|\mathrm{Im}_i(Y)|/|Y| = D_i(G)$ and $|\mathrm{Im}_i(Z)|/|Z| = D_i(H)$. Then $(v, w) \in \mathrm{Im}_i(Y \times Z)$ if and only if there are paths from some $y \in Y$ to v and some $z \in Z$ to w – equivalently $(v, w) \in \mathrm{Im}_i(Y) \times \mathrm{Im}_i(Z)$. Therefore $D_i(G \times H) \leq D_i(G)D_i(H)$.

Conversely, if F is a layered graph with vertex set $P \cup Q \cup R$ and $D(P, Q), D(Q, R)$ and $D(P, R)$ are the magnification ratios in the layered subgraphs between P, Q, Q, R and P, R respectively, then $D(P, R) \geq D(P, Q)D(Q, R)$. Define layered graph F and vertex sets P, Q and R as follows: let $P = V_0 \times W_0$, $Q = V_0 \times W_i$ and $R = V_i \times W_i$. Join $(v, w) \in V_0 \times W_0$ to $(v', w') \in V_0 \times W_i$ in F if $v = v'$ and $w' \in \mathrm{Im}_i(\{w\})$. Similarly, join $(v, w) \in V_0 \times W_i$ to $(v', w') \in V_i \times W_i$ if $w = w'$ and $v' \in \mathrm{Im}_i(\{v\})$. Then there exists a path from $(v, w) \in P$ to $(v', w') \in Q$ if and only if there exists a path from (v, w) to (v', w') in $G \times H$. Hence $D(P, R) = D_i(G \times H)$. We next show that $D(P, Q) = D_i(H)$. If $C \subset W_0$ with $|\mathrm{Im}_i(C)|/|C| = D_i(H)$, let $v \in V_0$ and $C' = \{v\} \times C$. This shows $D(P, Q) \leq D_i(H)$. Conversely, let $C \subset P = V_0 \times W_0$. For each $x \in V_0$, let $C_x = \{y : (x, y) \in C\}$. Then $|\mathrm{Im}_Q(C_x)|/|C_x| \geq D_i(H)$ hence $D(P, Q) = D_i(H)$ – note that C_x and $\mathrm{Im}_Q(C_x)$ are disjoint and non-empty and C is arbitary. Similarly $D(Q, R) = D_i(G)$. Therefore $D_i(G)D_i(H) \leq D_i(G \times H)$. $\square$

Menger's Theorem. *Let G be a graph and let $a, b \in V(G)$. Then the maximum number of internally disjoint a-b paths equals the size of a smallest set of vertices separating a from b.*

Lemma 5.10. *Let G be a Plünnecke Graph, on $V_0 \cup V_1 \cup \ldots \cup V_n$, such that $D_n(G) \geq 1$. Then there are $|V_0|$ disjoint paths from V_0 to V_n and, in particular, $D_i \geq 1$ for all $i \leq n$.*

Proof. Add a vertex a joined to all of V_0 and a vertex b joined to all of V_h. Let m be the maximum number of disjoint a-b paths. There exists a set $S = \{s_1, s_2, \ldots, s_m\}$ of size m separating a from b, by Menger's Theorem. Set $S_i = S \cap V_i$. Choose S such that $M = \sum_s iS_i(s)$ is a minimum. We claim that $S \subset V_0 \cup V_n$. Suppose this is false; there exists $i : 1 \leq i < n$ such that $S \cap V_i = \{s_1, s_2, \ldots, s_q\} \neq \emptyset$. Let $P_1, P_2, \ldots, P_m$ be disjoint paths from V_0 to V_n. Each P_i contains exactly one s_i, by the minimality of m. Let s_i^- and s_i^+ denote the predecessor and successor of s_i on the path containing

s_i, oriented from V_0 to V_n, $1 \le i \le q$. By the minimality of M, we cannot replace any elements of S with predecessors on the paths. So we find a path P from V_0 to V_n that misses $\{s_1^-, s_2^-, \ldots, s_q^-, s_{q+1}, \ldots, s_m\}$. This path must intersect S, as S is a separating set. Let $\{r\} = P \cap V_{i-1}$. Then the next vertex of P must be s_i for some $i : 1 \le i \le q$.

We claim that every path from $\{s_1^-, s_2^-, \ldots, s_q^-, r\}$ to $s_1^+, s_2^+, \ldots, s_q^+$ passes through the vertices $s_1, s_2, \ldots, s_q$. Suppose that this claim is false. If there exists a path Q from s_i^- to s_j^+ missing $s_1, s_2, \ldots, s_q$, then the path comprises the segment of P_i to s_i^-, the segment of Q to s_j^+ and the segment of P_j onwards, misses S. This contradicts the fact that S is a separating set. Therefore the graph induced by $\{s_1^-, \ldots, s_q^-, r\}, \{s_1, \ldots, s_q\}$ and $\{s_1^+, \ldots, s_q^+\}$ is a Plünnecke Graph. In this subgraph, let $d^+(x)$ and $d^-(X)$ be the in- and out-degrees of x. Since s_i^- is joined to s_i, $d^+(s_i^-) \ge d^+(s_i)$. Similarly, $d^-(s_i) \ge d^-(s_i^+)$. Also $\sum_{i=1}^q d^+(s_i) = \sum_{i=1}^q d^-(s_i^+)$ by counting edges, and $d^+(r) + \sum d^+(s_i^-) = \sum d^-(s_i)$. Since $d^+(r) > 0$, we have a contradiction. Therefore $S \subset V_0 \cup V_n$ and, by minimality, $S = (V_0 \cap S) \cup (\mathrm{Im}_n(V_0 \backslash S)$ and $|S| = |V_0 \cap S| + |\mathrm{Im}_n(V_0 \backslash S)| \ge |V_0 \cap S| + |V_0 \backslash S| = |V_0|$.

Plünnecke's Theorem. *Let G be a Plünnecke Graph on $V_0 \cup V_1 \cup \ldots \cup V_n$. Then $D_1 \ge D_2^{1/2} \ge \ldots \ge D_n^{1/n}$.*

Proof. It is enough to show $D_i^{1/i} \ge D_n^{1/n}$ for $i < n$. When $D_n = 1$, this holds. Suppose $D_n < 1$. Choose a positive integer r; then $D_n(G^r) = D_n^r$, by Lemma 5.8. Given an integer m, we can find a set $\{b_1, b_2, \ldots, b_m\} \subset \mathbb{Z}$ such that all sums $b_{j_1} + b_{j_2} + \ldots + b_{j_i}$, with $i \le m$ and $j_1 \le \ldots \le j_i$, are distinct. The number of these sums, given i, is $\binom{m+i-1}{i}$ – between $m^i/i!$ and m^i. Let $B = \{b_1, b_2, \cdots b_m\}$, $A = \{0\}$ and H_m be the natural layered graph with layers $A, A+B, \ldots, A+nB$. Let m be minimal such that $m^n D_n^r/m! \ge 1$. Then $m = \lceil (n! D_n^{-r})^{1/n} \rceil \le (n! D_n^{-r})^{1/n} + 1$. By the choice of m, $D_m(G^r \times H_m) \ge 1$ so by Lemma 5.10, $D_i(G^r \times H_m) \ge 1$, and $D_i(G)^r \cdot D_i(H_m) \ge 1$. However, $D_i(H_m) \le m^i$ so

$$D_i = D_i(G) \ge m^{-i/r} \ge \left[(n! D_n^{-r})^{1/n} \right]^{-i/r} \to D_n^{i/n}.$$

This completes the proof when $D_n < 1$. If $D_n > 1$, consider the reverse I_n of H_n – vertex sets $A+nB, A+(n-1)B, \ldots, A+B, A$. Then $D_n(I_m) \ge \binom{m+n-1}{m}^{-1}$ and

$$D_i(I_m) \le \binom{m+n-i-1}{m-i} \cdot \binom{m+n-1}{m}^{-1} \le n! m^{n-i}/m^n = n! m^{-i}.$$

Let r be a positive integer and m maximal such that $D_n^r m^{-n} \ge 1$. Then $m = \lfloor D_n^{-r/n} \rfloor \ge D_n^{r/n} - 1$. Then $D_n(G^r \times I_m) \ge 1$ so $D_i(G^r \times I_m) \ge 1$. However $D_i(G^r \times I_m) \le D_i^r n! m^{-i}$ so $D_i^r \ge m^i n!^{-1}$ implying $D_i \ge [(D_n^{r/n} - 1)^i n!^{-1}]^{1/r} \to D_n^{i/n}$, as required. $\square$

Corollary 5.12. *Let A and B be non-empty subsets of $\mathbb{Z}_N$ such that $|A+iB| \leq C|A|$. For $h \geq i$, there is a $\emptyset \neq A' \subset A$ such that $|A'+hB| \leq C^{h/i}|A'|$.*

Proof. Let G be the natural Plünnecke Graph. If the result were false, then $D_h(G) > C^{h/i}$ so $D_i(G) > C$ which implies that $|A'+iB| > C|A|$, a contradiction. $\square$

Corollary 5.13. *If A is a non-empty subset of $\mathbb{Z}$ and $|A+A| \leq C|A|$, then $|kA| \leq C^k|A|$ for each $k \geq 3$.*

Proof. Take $i = 1$ and $B = A$ in the preceding Corollary. This implies that there exists a non-empty $A' \subset A$ such that $|A'+kA| \leq C^k|A'| \leq C^k|A|$, but $|A'+kA| \geq |kA|$, so the result is proved. $\square$

Lemma 5.14. *Let $U, V, W \subset \mathbb{Z}$. Then $|U||V-W| \leq |U+V||U+W|$.*

Proof. Define, for $x \in V-W$, $\phi(u,x) = (u+v(x), u+w(x))$ where $v(x) \in V$, $w(x) \in W$ satisfy $v(x) - w(x) = x$. Then ϕ is an injection $U \times (V-W) \to (U+V) \times (U+W)$. $\square$

Theorem 5.15. *Let $A, B \subset \mathbb{Z}$ such that $|A+B| \leq C|A|$ and let k and l be natural numbers with $l \geq k$. Then $|kB - lB| \leq C^{k+l}|A|$.*

Proof. Suppose $l \geq k \geq 1$. By Corollary 5.12, there exists $A' \subset A$ with $|A'+kB| \leq C^k|A'|$. Again there exists $A'' \subset A'$ with $|A''+lB| \leq C^l|A''|$. Using Lemma 5.14, $|A''||kB-lB| \leq |A''+kB||A''+lB| \leq C^{k+l}|A'||A''|$ and the result follows on dividing by $|A''|$. $\square$

In the next chapter, we will see the use of Theorem 5.15. In essence, the arithmetic properties of kA for large k are easier to deal with than when k is small. Theorem 5.15 also allows one to deal with distinct set sums $A+B$ by converting the problem to a single set difference problem $kB - lB$.

§6 Freiman's Theorem

Freiman's Theorem [5] describes the structure of a set A under the condition that $A+A$ has size close to that of A. We define a *generalised arithmetic progression* to be a sum P of ordinary arithmetic progressions (see Theorem 5.7). If P is a subset of a small generalised arithmetic progression then $|P+P|$ is close to $|P|$. Freiman's Theorem states the converse: if $|P+P|$ is close to P then P must be contained in a small generalized arithmetic progression.

We now proceed to the proof of Freiman's Theorem, using a remarkable and ingenious approach due to Ruzsa [12].

Let $A \subset \mathbb{Z}_s$ or $A \subset \mathbb{Z}$ and $B \subset \mathbb{Z}_t$. Then $\phi : A \to B$ is called a *(Freiman) k-homomorphism* if whenever $x_1 + x_2 + \ldots + x_k = y_1 + y_2 + \ldots + y_k$, with $x_i, y_i \in A$, $\sum \phi(x_i) = \sum \phi(y_i)$. In addition, ϕ is called a *k-isomorphism* if ϕ is invertible and ϕ and ϕ^{-1} are k-homomorphisms.

Note that ϕ is a k-homomorphism if the map $\psi : (x_1, \ldots, x_k) \mapsto \sum \phi(x_i)$ induced by ϕ is a well defined map $kA \to kB$, and a k-isomorphism if ψ is a bijection. Our interest will be in 2-isomorphisms, as these preserve arithmetic progressions – a set 2-isomorphic to an arithmetic progression is clearly an arithmetic progression. We use the following notation: if $\phi : A \to B$ and $A' \subset A$, then $\phi|_{A'}$ denotes the restriction of ϕ to A'.

Lemma 6.1. *Let $A \subset \mathbb{Z}$ and suppose $|kA - kA| \le C|A|$. Then, for any prime $N > C|A|$, there exists $A' \subset A$ with $|A'| \ge |A|/k$ that is k-isomorphic to a subset of $\mathbb{Z}_N$.*

Proof. We may suppose $A \subset \mathbb{N}$ and select a prime $p > k \max A$. Then the quotient map $\phi_1 : \mathbb{Z} \to \mathbb{Z}_p$ is a homomorphism of all orders, and $\phi_1|_A$ is a k-isomorphism. Now let q be a random element of $[p-1]$ and define $\phi_2 : \mathbb{Z}_p \to \mathbb{Z}_p$ by $\phi_2(x) = qx$. Then ϕ_2 is an isomorphism of all orders, and hence a k-isomorphism. Let $\phi_3(x) = x$ where $\phi_3 : \mathbb{Z}_p \to \mathbb{Z}$. Then for any j, $\phi_3|_{I_j}$ is a k-isomorphism where

$$I_j = \{x \in \mathbb{Z}_p : \frac{j-1}{k} p \le x < \frac{j}{k} p - 1\}.$$

For, if $\sum_{i=1}^k x_i = \sum_{i=1}^k y_i \pmod p$ with $x_i, y_i \in I_j$, then $\sum_{i=1}^k x_i = \sum_{i=1}^k y_i$ in $\mathbb{Z}$. By the pigeonhole principle, there exist $A' \subset A$ with $|A'| \ge |A|/k$ (depending on q) and

$\phi_2\phi_1[A'] \subset I_j$ for some j. Restricted to A', $\phi_3\phi_2\phi_1$ is a k-homomorphism. Finally, let ϕ_4 be the quotient map (a k-homomorphism) $\mathbb{Z} \to \mathbb{Z}_N$. Then with $\phi = \phi_4\phi_3\phi_2\phi_1$, $\phi(x) = qx \pmod p \pmod N$ and $\phi|_{A'}$ is a k-homomorphism, as it is the composition of k-homomorphisms.

The only way $\phi|_{A'}$ is not a k-isomorphism is if there are $a_1, a_2, \ldots, a_k, a'_1, a'_2, \ldots, a'_k \in A'$ such that $\sum_{i=1}^k \phi(a_i) = \sum_{i=1}^k \phi(a'_i)$ but $\sum_{i=1}^k \phi(a_i) \neq \sum_{i=1}^k \phi(a'_i)$. Now $\sum_i a_i \neq \sum_i a'_i$ implies $\sum_i a_i \neq \sum_i a'_i \pmod p$ so we have $q(\sum_i a_i - \sum_i a'_i) \pmod p$ is a multiple of N. The probability of this event is at most $|kA - kA|/N < 1$ since $|kA - kA| \leq C|A|$ and $N > C|A|$. So for some q, $\phi|_{A'}$ is a k-isomorphism. □

The next theorem, due to Bogolyubov [3], shows that we may find long arithmetic progressions with small dimension in $2A - 2A$. The proof is surprisingly simple.

Theorem 6.2 *Let $A \subset \mathbb{Z}_N$ with $|A| \geq \alpha N$. Then $2A - 2A$ contains an arithmetic progression of length at least $(\alpha^2/4)^{\alpha^{-2}} N$ and dimension at most α^{-2}.*

Proof. Let $g(x)$ be the number of ways of writing $x = (a-b)-(c-d)$ with $a, b, c, d \in A$. That is, $g = (A * A) * (A * A)$ and $x \in 2A - 2A$ if and only if $g(x) \neq 0$. Now $g(x) = N^{-1} \sum_r |\hat{A}(r)|^4 \omega^{rx}$, by Lemma 2.2 (3). Let $K = \{r \neq 0 : \hat{A}(r) \geq \alpha^{3/2} N\}$. Then

$$\sum_{\substack{r \neq 0 \\ r \notin K}} |\hat{A}(r)|^4 \leq \max_{\substack{r \neq 0 \\ r \notin K}} |\hat{A}(r)|^2 \sum_r |\hat{A}(r)|^2 < \alpha^3 N^2 \cdot \alpha N^2 = \alpha^4 N^4.$$

Therefore, if x is such that $\mathrm{Re}(\omega^{rx}) \geq 0$ for all $r \in K$, then

$$\mathrm{Re}\Big(\sum_r |\hat{A}(r)|^4 \omega^{rx}\Big) > |\hat{A}(0)|^4 - \alpha^4 N^4 = 0.$$

Therefore $g(x) \neq 0$ and $2A - 2A$ contains the Bohr neighbourhood $B(K; 1/4) - \mathrm{Re}(\omega^{rs}) \geq 0$ if and only if $-N/4 \leq rs \leq N/4$. Now $\sum_{r \in K} |\hat{A}(r)|^2 \geq k\alpha^3 N^2$ and $\sum_{r \in K} |\hat{A}(r)|^2 \leq \alpha N^2$. By Theorem 5.7, $2A - 2A$ contains the required arithmetic progression. □

We now present Ruzsa's proof of Freiman's Theorem.

Freiman's Theorem. *Let $A \subset \mathbb{Z}_N$ be a set such that $|A + A| \leq C|A|$. Then A is contained in a d-dimensional arithmetic progression P of cardinality at most $k|A|$ where d and k depend on C only.*

Proof. By Theorem 5.15, $|8A-8A| \leq C^{16}|A|$. By Lemma 6.1, A contains a subset A' of cardinality at least $|A|/8$ which is 8-isomorphic to a a set $B \subset \mathbb{Z}_N$ with $C^{16}|A| < N \leq 2C^{16}|A|$, where N is prime and $C|A| < N \leq 2C|A|$, using Bertrand's Postulate. So $|B| = \alpha N$ with $\alpha \geq (16C^{16})^{-1}$. By Theorem 6.2, $2B-2B$ contains an arithmetic progression of dimension at most α^{-2} and cardinality at least $(\alpha^2/4)^{\alpha^{-2}}N \geq (\alpha^2/4)^{\alpha^{-2}}|A|$. Since B is 8-isomorphic to A', $2B-2B$ is 2-isomorphic to $2A'-2A'$. Any set 2-isomorphic to a d-dimensional arithmetic progression is a d-dimensional arithmetic progression. Therefore $2A'-2A'$, and hence $2A-2A$, contains an arithmetic progression Q of dimension at most α^{-2} and cardinality $\gamma|A|$, where $\gamma \geq (\alpha^2/4)^{\alpha^{-2}}$. Now let $X = \{x_1, x_2, \ldots, x_k\} \subset A$ be maximal such that $x, y \in X$, $x \neq y$ imply $x-y \in Q-Q$. Equivalently, all the sets $x+Q$ are disjoint, so $X+Q = |X||Q|$. Since X is maximal, $A \subset X+(Q-Q)$ and X is contained in the k-dimensional arithmetic progression $R = \left\{\sum_{i=1}^{k} a_i x_i : 0 \leq a_i \leq 1\right\}$. Clearly $|R| \leq 2^k$. Therefore A is contained in the arithmetic progression $R+(Q-Q)$, of dimension at most $\alpha^{-2}+k$. We know that $X+(Q-Q) \subset A+(4A-4A) = A+2A-2A+2A-2A$, and that $X+Q \subset A+2A-2A = 3A-2A$. So $|X+Q| \leq |3A-2A| \leq C^5|A|$, by Theorem 5.15. So $k \leq C^5|A|/|Q| \leq C^5\gamma^{-1}$. Finally, $|Q-Q| \leq 2^{\alpha^{-2}}|Q|$, by d-dimensionality. So A is contained in an arithmetic progression of dimension at most $\alpha^{-2}C^5\gamma^{-1}$, and cardinality at most $2^k 2^{\alpha^{-2}}|Q| \leq 2^k 2^{\alpha^{-2}}|2A-2A| \leq kC^4 2^{\alpha^{-2}}|A|$. □

The constants from this theorem can be chosen to be $d = \exp(C^\alpha)$ and $k = \text{expexp}(C^\beta)$, where $\alpha, \beta > 0$ are absolute constants. Using a refinement of the same approach, a better result can be obtained for set *differences* of the same set (see [2]):

Theorem 6.4. *Let C be a positive real number. Suppose A is a set of integers satisfying $|A-A| \leq C|A|$ and $|A| \geq \frac{\lfloor C\rfloor\lfloor C+1\rfloor}{2(\lfloor C+1\rfloor - C)}$. Then A is a subset of an arithmetic progression of dimension at most $\lfloor C-1\rfloor$ and cardinality at most expexp(C^γ) where $\gamma > 0$ is an absolute constant.*

It is likely that a result with very much the same constants is true for $A+A$. These theorems can be generalized to theorems about abelian groups [4], [13]. We now turn to results concerning difference sets, which will eventually aid in finding four-term arithmetic progressions in the next chapter.

Lemma 6.5. *Let $A_1, A_2, \ldots, A_m$ be subsets of $[N]$, $\alpha > 0$ and suppose that $\sum_{i=1}^{m} |A_i| \geq \alpha mN$. Then there exists $B \subset [m]$, of cardinality at least $\alpha^5 m/2$, such that for at least* *ninety percent of pairs* $(i,j) \in B \times B$, $|A_i \cap A_j| \geq \alpha^2 N/2$.

Proof. Let $x_1, x_2, \ldots, x_5$ be chosen randomly and independently from $[N]$. Let $B = \{i : \{x_1, x_2, \ldots, x_5\} \subset A\}$. Then $\mathrm{Prob}[i \in B] = (|A_i|/N)^5$ and thus the expected size of B is $\sum_{i=1}^m (|A_i|/N)^5 \geq m(\sum |A_i|/mN)^5 \geq \alpha^5 m$, by Jensen's Inequality. By Cauchy-Schwartz, $\mathsf{E}[|B|^2] \geq \alpha^{10} m^2$. If $|A_i \cap A_j| \leq \alpha^2 N/2$, then $\mathrm{Prob}[i \in B, j \in B] < \alpha^{10}/32$. So if $C = \{i, j \in B \times B : |A_i \cap A_j| < \alpha^2 N/2\}$, then $\mathsf{E}[|C|] < \alpha^{10} m^2/32$. It follows that the expected value of $\mathsf{E}[|B|^2 - 16|C|] > \alpha^{10} m^2/2$. Hence there exist $x_1, x_2, \ldots, x_5$ such that $|B|^2 > \alpha^{10} m^2/2$ and $|B|^2 \geq 16|C|$. $\square$

The following theorem is due to Balog and Szemerédi [1]:

Theorem 6.6. *Let A be a subset of an abelian group. Suppose $\alpha > 0$ and that there are at least $\alpha|A|^3$ quadruples $(a,b,c,d) \in A \times A \times A \times A$ such that $a - b = c - d$. Then A contains a subset A' such that $|A'| \geq c|A|$ and $|A' - A'| \leq C|A|$ where c and C depend on α only.*

Proof. Set $|A| = n$. Let $f(x) = (A * A)(x)$, the number of ways of writing $x = a - b$ with $a, b \in A$. Then $\sum_x f(x) = n^2$, $\sum_x f(x)^2 \geq \alpha n^3$ and $\max f(x) \leq n$. It follows that $f(x) \geq \alpha n/2$ for at least $\alpha n/2$ values of x: otherwise let $B = \{x : f(x) < \alpha n/2\}$ and note $\sum_B f(x)^2 < \max_B f(x) \sum_B f(x) < \alpha n^3/2$ which implies $\sum_x f(x)^2 < \alpha n^3$. Let x be called a *popular difference* if $f(x) \geq \alpha n/2$. Define a graph G with vertex set A and edge set $\{ab : a - b \text{ is a popular difference}\}$ – note that f *is* symmetric. There are at least $\alpha^2 n^2/8$ edges in G, by the first part of the proof. Let $\Gamma(a)$ denote the open neighbourhood of a vertex a in G. Then $\sum_{a \in A} |\Gamma(a)| \geq \alpha^2 n^2/4$ so, by the preceding lemma, we can find $B \subset A$ of cardinality at least $\alpha^{10} n/2^{11}$ such that $|\Gamma(a) \cap \Gamma(b)| \geq \alpha^4 n/32$ for at least ninety percent of pairs $(a,b) \in B \times B$.

Define a new graph H with vertex set B and edge set $\{ab : |\Gamma(a) \cap \Gamma(b)| \geq \alpha^4 n/32\}$. Since the average degree in H is at least $9|B|/10$, at least $4|B|/5$ vertices have degree at least $4|B|/5$. Let A' be the set of all such vertices; this will be the desired set. Let $a, b \in A'$. There are at least $3|B|/5$ numbers $c \in B$ such that ac and bc are edges of H, by definition of A'. If ac is an edge of H, then $|\Gamma(a) \cap \Gamma(c)| \geq \alpha^4 n/32$, so there are at least $\alpha^4 n/32$ numbers d such that ad and cd are edges of G, and similarly for bc. If ad is an edge of G then there are at least $\alpha n/2$ pairs $(x,y) \in A \times A$ such that $y - x = d - a$

so $a+y-x=d$, and similarly for other edges of G. Therefore there are at least

$$\frac{3}{5}\cdot\frac{\alpha^{10}}{2^{11}}n\cdot\Big(\frac{\alpha^4 n}{32}\Big)^2\Big(\frac{\alpha n}{2}\Big)^4$$

distinct octuples $(x_1,y_1,x_2,y_2,\ldots,x_4,y_4)\in\prod_{i=1}^8 A$ such that $a+y_1-x_1+y_2-x_2+y_3-x_3+y_4-x_4=b$. If we choose a different pair $(a',b')\in A'\times A'$ such that $b'-a'\neq b-a$, then the corresponding set of octuples is disjoint. Using the above inequality, $|A'-A'|\le n^8$ and so $|A'-A'|\le 2^{26}\alpha^{-22}n$. Setting $c=\alpha^{10}/(5\cdot 2^9)$ and $C=2^{26}\alpha^{-22}$ completes the proof. $\square$

Corollary 6.7. *Let $A\subset\mathbb{Z}^k$ with $|A|=m$ and such that the number of quadruples $(a,b,c,d)\in A\times A\times A\times A$, with $a-b=c-d$, is at least cm^3. Then there exists an arithmetic progression P of cardinality at most Cm and dimension at most d such that $|A\cap Q|\ge cm$, where C and d depend only on c.*

Proof. This follows directly from the preceding result and Freiman's Theorem. $\square$

This corollary, or rather a derivative of it, will be very useful in studying four-term arithmetic progressions in the next chapter. In fact, this result is equivalent to Freiman's Theorem.

Any integer quadruple (a,b,c,d) such that $a-b=c-d$ is called an *additive quadruple*. For a function $\phi: B\to\mathbb{Z}_N$, where $B\subset\mathbb{Z}_N$, we say $(a,b,c,d)\in B\times B\times B\times B$ is an additive quadruple of ϕ if (a,b,c,d) is an additive quadruple and $(\phi(a),\phi(b),\phi(c),\phi(d))$ is an additive quadruple. If $B\subset\mathbb{Z}^d$, then $(A*A)(x)$ is the number of representations of x as $y-z$. Therefore the number of quadruples $(a,b,c,d)\in A\times A\times A\times A$ with $a-b=c-d$ is $\|A*A\|_2^2$. The result we shall use in the next chapter is the following:

Corollary 6.8. *Let $B\subset\mathbb{Z}_N$ be a set of cardinality βN, and let $\phi: B\to\mathbb{Z}_N$ be a function with at least αN^3 additive quadruples. Then there exist constant γ and η, depending only on β and c, a $\mathbb{Z}_N$-arithmetic progression P of cardinality at least N^γ and a linear function $\psi: P\to\mathbb{Z}_N$ such that $\psi(s)=\phi(s)$ for at least $\eta|P|$ values of $s\in P$.*

Proof. Let Γ denote the graph of ϕ in $\mathbb{Z}\times\mathbb{Z}$. By Theorem 6.6, there are constants c and C, depending only on α, and a set $A'\subset A$ of cardinality at least $c|A|$ such that $|A'-A'|\le C|A|$. A result of Ruzsa shows that if A is any set with $|A-A|\le C|A|$, then there exists a $\mathbb{Z}$-arithmetic progression Q of dimension at most $2^{18}C^{32}$ and size at least

$(2^{20}C^{32})^{-2^{18}C^{32}}|A|$, such that $|A \cap Q| \geq C^{-5}2^{-d}|Q|$. Applying this result to A', we get a d-dimensional $\mathbb{Z}$-arithmetic progression Q of cardinality at most CN, with $|\Gamma \cap Q| \geq cN$, where d, c, C depend on α and β only. If $Q = Q_1 + Q_2 + \ldots + Q_d$, then at least one P_i has cardinality at least $(CN)^{1/d} \geq (cN)^{1/d}$, so Q can be partitioned into one-dimensional arithmetic progressions of cardinality at least $(cN)^{1/d}$. Therefore there is an arithmetic progression $R \subset \mathbb{Z} \times \mathbb{Z}$, of cardinality at least $(cN)^{1/d}$ such that $|R \cap \Gamma| \geq cC^{-1}|R|$. As Γ is the graph of a function, R is not vertical unless $|R \cap \Gamma| = 1$ in which case the result is proved. So there exists an arithmetic progression $P \subset \mathbb{Z}$ of the same size as R and a linear function ψ such that Γ contains at least $cC^{-1}|P|$ pairs $(s, \psi(s))$. Reducing modulo N gives the required result. $\square$

Following Ruzsa's proof of Freiman's Theorem, we may take $\gamma = \alpha^K$ and $\eta = \exp(-\alpha^{-K})$, where $K > 0$ is an absolute constant.

§7 Szemerédi's Theorem

To prove Szemerédi's Theorem [16] for four term arithmetic progressions, following Gowers [7], a two case argument: we consider first sets which behave roughly like random sets, and then those which do not. Then, if a set does not behave in the first sense above, it can be restricted to an arithmetic progression, of reasonable length, in which its density increases. This argument applies a finite number of times as the density is bounded above by 1. Notice the similarities in approach with the proof of Roth's Theorem. The difference is that a stronger condition, namely *quadratic uniformity* is required for random-like behaviour with regards to four term arithmetic progressions. The difficult part is finding an arithmetic progression of reasonable length in which the density increases.

We now define the concept of quadratic uniformity. Let $f : \mathbb{Z}_N \to \{z \in \mathbb{C} : |z| \leq 1\}$ and $\alpha > 0$. Then f is *α-uniform* if $\sum_r |\hat{f}(r)|^4 \leq \alpha N^4$. If $A \subset \mathbb{Z}_N$, $|A| = \delta N$ and $f(x) = A(x) - \delta$, then A is α-uniform if f is α-uniform – A is α-uniform if $\sum_r |\hat{A}(r)|^4 \leq (\delta^4 + \alpha)N^4$. The concept of α-uniformity is not quite strong enough, in terms of containing the expected number of arithmetic progressions of length four. We say f is *quadratically α-uniform* if

$$\sum_k \sum_r |\hat{\Delta}(f;k)(r)|^4 \leq \alpha N^5$$

where $\Delta(f;k)(x) = f(x)\overline{f(x-k)}$. We generally define

$$\Delta(f; k_1, k_2, \ldots, k_r) = \Delta(\Delta(f; k_1, k_2, \ldots, k_{r-1}); k_r).$$

This is independent of the order of the k_i. Also

$$\begin{aligned}
\sum_k \sum_r |\hat{\Delta}(f;k)(r)|^4 &= N \sum_{x,k,l,m} \Delta(f;k)(x)\overline{\Delta(f;k)(x-\ell)\Delta(f;k)(x-m)}\Delta(f;k)(x-l-m) \\
&= \sum_{x,k,l,m} \Delta(f;k,l,m)(x) \\
&= N \sum_{k,l} \Big| \sum_x \Delta(f;k,l)(x) \Big|^2.
\end{aligned}$$

In this chapter, D will denote the unit disc in the complex plane.

Lemma 7.1 *Let $f : \mathbb{Z}_N \to \mathbb{D}$. Then f is α-uniform if and only if for any function $g : \mathbb{Z} \to \mathbb{C}$,*

$$\sum_k \Big| \sum_s f(s)\overline{g(s-k)}\Big|^2 \le \sqrt{\alpha} N^2 \|g\|_2^2.$$

Also, f is α-uniform if $\max_r |\hat{f}(r)| \le \alpha^{1/2} N$.

PROOF. For the first part, we know that

$$\begin{aligned}
\sum_k |\sum_s f(s)\overline{g(s-k)}|^2 &= \sum_k |f * g)k)|^2 \\
&= N^{-1} \sum_r |(f * g)\hat{}(r)|^2 \\
&= N^{-1} \sum_r |\hat{f}(r)|^2 |\hat{g}(r)|^2 \\
&\le \Big(\sum_r |\hat{f}(r)|^4\Big)^{1/2} \Big(\sum_r |\hat{g}(r)|^4\Big)^{1/2},
\end{aligned}$$

by the Cauchy-Schwartz inequality, and Lemma 2.2. Since $\left(\sum_r |\hat{g}(r)|^4\right)^{1/2} \le \sum_r |\hat{g}(r)|^2$, if f is α-uniform then the inequality in f and g above must hold. For the second part, we use the fact that $\sum_r |\hat{f}(r)|^4 \le \max_r |\hat{f}(r)|^2 \sum_r |\hat{f}(r)|^2$, and Parseval's Identity from Lemma 2.2 to obtain $\sum_r |\hat{f}(r)|^2 \le N^2$ and the result follows. □

The first few results lead to showing that quadratically α-uniform sets do contain four-term arithmetic progressions. We begin by proving a number of technical lemmas concerning α-uniformity. The following lemma shows that a quadratically uniform set is also uniform.

Lemma 7.2. *If f is quadratically α-uniform, then f is $\alpha^{1/2}$-uniform.*

PROOF.
$$\begin{aligned}
\Big(\sum_r |\hat{f}(r)|^4\Big)^2 &= \Big(N \sum_{x,k,l} f(x)\overline{f(x-k)f(x-l)}f(x-k-l)\Big)^2 \\
&= N^2 \Big(\sum_{x,k,l} \Delta(f;k,l)(x)\Big)^2 \\
&\le N^4 \sum_{k,l} \Big|\sum_x \Delta(f;k,l)(x)\Big|^2 \\
&= N^3 \sum_{k,r} |\hat{\Delta}(f;k)(r)|^4 \le \alpha N^8.
\end{aligned}$$
□

Lemma 7.3. *Let $f_1, f_2, f_3 : \mathbb{Z}_N \to \mathbb{D}$. Suppose that f_3 is α-uniform. Then we have* $|\sum_{a,d} f_1(a) f_2(a+d) f_3(a+2d)| \le \alpha^{1/4} N^2$.

Proof. If $S = \sum_{a,d} f_1(a)f_2(a+d)f_3(a+2d)$ then

$$\begin{aligned}
|S| &= \Big|\sum_{a+c=2b} f_1(a)f_2(b)f_3(c)\Big| \\
&= \Big|N^{-1}\sum_r \hat{f}_1(r)\hat{f}_2(-2r)\hat{f}_3(r)\Big| \\
&\leq N^{-1}\max_r \hat{f}_3(r)\cdot\Big(\sum_r |\hat{f}_1(r)|^2\Big)^{1/2}\cdot\Big(\sum_r |\hat{f}_2(r)|^2\Big)^{1/2} \\
&\leq N^{-1}\cdot\alpha^{1/4}N\cdot N^2 = \alpha^{1/4}N^2. \qquad \square
\end{aligned}$$

Lemma 7.4. *Let $f_1, f_2, f_3, f_4 : \mathbb{Z}_N \to \mathbb{D}$ and $\alpha > 0$. Suppose f_4 is quadratically α-uniform. Then $|\sum_{a,d} f_1(a)f_2(a+d)f_3(a+2d)f_4(a+3d)| \leq \alpha^{1/8}N^2$.*

Proof. Let S be the sum we are estimating. Then

$$\begin{aligned}
|S|^2 &\leq N\sum_a\Big|\sum_d f_1(a)f_2(a+d)f_3(a+2d)f_4(a+3d)\Big|^2 \\
&\leq N\sum_a\Big|\sum_d f_2(a+d)f_3(a+2d)f_4(a+3d)\Big|^2 \\
&\leq \sum_a\sum_{d,e} f_2(a+d)\overline{f_2(a+e)}f_3(a+2d)\overline{f_3(a+2e)}f_4(a+3e)\overline{f_4(a+3e)} \\
&= N\sum_a\sum_{d,k}\Delta(f_2;k)(a+d)\Delta(f_3;2k)(a+2d)\Delta(f_3;3k)(a+3d) \\
&= N\sum_a\sum_{d,k}\Delta(f_2;k)(a)\Delta(f_3;2k)(a+2d)\Delta(f_3;3k)(a+3d).
\end{aligned}$$

Since f_4 is quadratically α-uniform, there are $\alpha(k)$, $k \in \mathbb{Z}_N$ such that for each k, $\Delta(f_4;k)$ is $\alpha(k)$-uniform and $N^{-1}\sum_k \alpha(k) = \alpha$. By Lemma 7.3, the above expression is at most

$$\begin{aligned}
N\sum_k \alpha(3k)^{1/4}N^2 &= N\sum_k \alpha(k)\alpha(k)^{1/4}N^2 \\
&\leq N\alpha^{1/4}NN^2 = \alpha^{1/4}N^4. \qquad \square
\end{aligned}$$

Theorem 7.5. *Let $A_1, A_2, A_3, A_4 \subset \mathbb{Z}_N$ with $|A_i| = \delta_i N$. Suppose that A_3 is $\alpha^{1/2}$-uniform and A_4 is quadratically α-uniform. Then $\sum_{a,d} A_1(a)A_2(a+d)A_3(a+2d)A_4(a+3d) - \delta_1\delta_2\delta_3\delta_4 N^2 \leq 12\alpha^{1/8}N^2$.*

Proof. Set $f_i(x) = A_i(x) - \delta_i$. Replace the $A_i(\cdot)$ with $f_i(\cdot) + \delta_i$ in the sum we wish to estimate. The sum splits into sixteen parts. We think of δ_i as constant functions and apply the two preceding lemmas. If we choose f_4 in applying Lemma 7.4, then the sum is at most $\alpha^{1/8}N^2$. If we do not choose f_4, but choose f_3, then the sum is at most $(\alpha^{1/2})^{1/4}N^2 = \alpha^{1/8}N^2$, by Lemma 7.3. If neither f_3 nor f_4 is chosen, we use the identity

$$\sum_{a,d} g_1(a) g_2(a+d) = \sum_{a,b} g_1(a) g_2(b) = \Big(\sum_a g_1(a)\Big)\Big(\sum_b g_2(b)\Big).$$

This shows that all of the remaining terms are zero, apart from the constant term, which is $\sum_{a,d} \delta_1\delta_2\delta_3\delta_4 = N^2\delta_1\delta_2\delta_3\delta_4$. This completes the proof of Theorem 7.5. $\square$

Corollary 7.6. *Let $A \subset [N]$, $|A| = \delta N$ where $\delta > 0$. Suppose that A is quadratically α-uniform. If $\alpha \leq \delta^{32}/2^{88}$ and $N \geq 200/\delta^4$, then A contains an arithmetic progression of length four or we can find a subprogression where A has density at least $\frac{9}{8}\delta$.*

PROOF. Let $A_1 = A_2 = A \cap [2N/5, 3N/5]$ and $A_3 = A_4 = A$. If $|A| \leq \delta/10$, we have $A \cap [0, 2N/5]$ or $A \cap [3N/5, N)$ of cardinality at least $\delta(9N/20)$. By Theorem 7.5, $A_1 \times A_2 \times \cdots \times A_4$ contains at least $(\delta^4/100 - 12\alpha^{1/8})N^2$ $\mathbb{Z}_N$ arithmetic progressions of length four. Provided this is greater than N, we have a $\mathbb{Z}$-arithmetic progression – all $\mathbb{Z}_N$ arithmetic progressions in $A_1 \times A_2 \times A_3 \times A_4$ are $\mathbb{Z}$-arithmetic progressions. $\square$

We now turn to the case where f is *not* quadratically uniform. If A is the corresponding set of density δ, then we plan to show that A intersects a $\mathbb{Z}$-arithmetic progression $P \subset \{1, 2, \ldots, N\}$ of size at least N^d and such that $|A \cap P| \geq (\delta + \varepsilon)|P|$ where ε and d depend only on α and δ.

Lemma 7.7. *Suppose that f is not quadratically α-uniform. Then there exists a set B, of cardinality at least $\alpha N/2$, and a function $\phi : B \to \mathbb{Z}_N$ such that*

$$\sum_{k \in B} |\hat{\Delta}(f;k)(\phi(k))|^2 \geq (\alpha/2)^2 N^3.$$

PROOF. Since f is not quadratically α-uniform, $\sum_k \sum_r |\hat{\Delta}(f;k)(r)|^4 > \alpha N^5$. So there must be more than $\alpha N/2$ values of k for which $\sum_r |\hat{\Delta}(f;k)(r)|^4 \leq \alpha N^3/2$. So there are more than $\alpha N/2$ values of k such that $\max_r |\hat{\Delta}(f;k)(r)| \geq (\alpha/2)^{1/2} N$, by the second part of Lemma 7.1. Therefore there exists a set B, of cardinality at least $\alpha N/2$, and a function ϕ such that $|\hat{\Delta}(f;k)(r)| \geq (\alpha/2)^{1/2} N$ for all $k \in B$. Summing this over $k \in B$ gives the required result. $\square$

Recall the definition of an additive quadruple, given in the last part of the last chapter.

Lemma 7.8. *Suppose that $f : \mathbb{Z}_N \to \mathbb{D}$, $B \subset \mathbb{Z}_N$ and $\phi : \mathbb{Z}_N$ is a function such that, for some $\alpha > 0$,*

$$\sum_{k\in B} |\hat{\Delta}(f;k)(\phi(k))|^2 \geq \alpha N^3.$$

Then there exist at least $\alpha^4 N^3$ quadruples $(a,b,c,d) \in B\times B\times B\times B$ such that $a+b=c+d$ and $\phi(a)+\phi(b)=\phi(c)+\phi(d)$.

Proof. Expanding the left hand side of the inequality, we get:

$$\begin{aligned}
&\sum_{k\in B} |\hat{\Delta}(f;k)(\phi(k))|^2 \geq (\alpha/2)^2 N^3 \\
\Rightarrow\ &\sum_{k\in B}\sum_{s,t} f(s)\overline{f(s-k)f(t)}f(t-k)\omega^{-\phi(k)(s-t)} \geq \alpha N^3 \\
\Rightarrow\ &\sum_{k\in B}\sum_{s,u} f(s)\overline{f(s-k)f(s-u)}f(s-k-u)\omega^{-\phi(k)u} \geq \alpha N^3 \\
\Rightarrow\ &\sum_{u,s}\Big|\sum_{k\in B} \overline{f(s-k)}f(s-k-u)\omega^{-\phi(k)u}\Big| \geq \alpha N^3 \\
\Rightarrow\ &\sum_{u,s}\Big|\sum_{k\in B} \overline{f(s-k)}f(s-k-u)\omega^{-\phi(k)u}\Big|^2 \geq \alpha^2 N^4.
\end{aligned}$$

Let $\gamma(u)$ satisfy $\sum_s|\sum_B \overline{f(s-k)}f(s-k-u)\omega^{-\phi(k)u}|^2 = \gamma(u)N^3$. Using the first part of Lemma 7.1, we deduce that $B(k)\omega^{\phi(k)u}$ is not $\gamma(u)^2$-uniform, and therefore (by definition) $\sum_r|\sum_B \omega^{\phi(k)u-rk}|^4 \geq \gamma(u)^2N^4$. By the above inequalities, $\sum_u \gamma(u) \geq \alpha^2 N$ so $\sum_u \gamma(u)^2 \geq \alpha^4 N$. Therefore

$$\sum_u \sum_r |\sum_{k\in B} \omega^{\phi(k)u-rk}|^4 \geq \alpha^4 N^5.$$

Expanding the left hand side we find that:

$$\sum_{u,r}\sum_{a,b,c,d\in B} \omega^{(\phi(a)+\phi(b)-\phi(c)-\phi(d))u}\omega^{-r(a+b-c-d)} \geq \alpha^4 N^5.$$

However, the left side is N^2 times the number of quadruples $(a,b,c,d) \in B\times B\times B\times B$ for which $a+b=c+d$ and $\phi(a)+\phi(b)=\phi(c)+\phi(d)$. $\square$

We recall the definition of additive quadruples for a function ϕ, from the end of chapter six.

Lemma 7.9. *Suppose that $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ has at least αN^3 additive quadruples. Then there exist η, γ, depending only on α, and an arithmetic progression P of length at least N^γ such that for some λ and μ,*

$$\sum_{k\in P}|\hat{\Delta}(f;k)(\lambda k+\mu)|^2 \geq \eta N^2|P|.$$

PROOF. This follows from Corollary 6.8 with $\gamma=\alpha^K$ and $\eta=\exp(-\alpha^{-K})$. □

Lemma 7.10. *Let $f:\mathbb{Z}_N\to\mathbb{D}$. Let $\eta>0$ and $P\subset\mathbb{Z}_N$ be an $\mathbb{Z}_N$-arithmetic progression such that, with $\lambda,\mu\in\mathbb{Z}_N$,*

$$\sum_{k\in P}|\Delta(f;k)\hat{\ }(2\lambda k+\mu)|^2 \geq \eta|P|N^2$$

Then, for $|P|\leq N^{1/2}$, there exists a partition of $\mathbb{Z}_N$ into translates $P_1,P_2,\ldots,P_M$ of P or P with an endpoint removed, such that for each i we can find $r_i\in\mathbb{Z}_N$ such that

$$\sum_i|\sum_{x\in P_i}f(x)\omega^{-\lambda x^2-r_ix}|\geq \eta|P|N/2.$$

PROOF.
$$\begin{aligned}
&\sum_{k\in P}\Big|\sum_x f(x)\overline{f(x-k)}\omega^{-(2\lambda k+\mu)x}\Big|\geq\eta|P|N^2\\
\Rightarrow\ &\sum_{k\in P}\sum_x\sum_y f(x)\overline{f(x-k)f(y)}f(y-k)\omega^{-(2\lambda k+\mu)(x-y)}\geq\eta|P|N^2\\
\Rightarrow\ &\sum_{k\in P}\sum_x\sum_u f(x)\overline{f(x-k)f(x-u)}f(x-k-u)\omega^{-(2\lambda k+\mu)u}\geq\eta|P|N^2.
\end{aligned}$$

Every $u\in\mathbb{Z}_N$ can be written in exactly $|P|$ ways as $v+l$ with $v\in\mathbb{Z}_N$ and $l\in P$, therefore,

$$\sum_{k\in P}\sum_{l\in P}\sum_x\sum_v f(x)\overline{f(x-k)f(x-v-l)}f(x-v-k-l)\omega^{-(2\lambda k+\mu)(v+l)}\geq\eta|P|^2N^2.$$

Hence we can find $v\in\mathbb{Z}_N$ such that

$$\Big|\sum_{k\in P}\sum_{l\in P}\sum_x f(x)\overline{f(x-k)g(x-l)}g(x-k-l)\omega^{-(2\lambda vk+\mu v+2\lambda kl+\mu l)}\Big|\geq\eta|P|^2N$$

where $g(x)=f(x-v)$. Now with $2\lambda vk=2\lambda v(x-l-(x-k-l))$, $\mu l=\mu(x-(x-l))$ and $2\lambda kl=\lambda(x^2-(x-k)^2-(x-l)^2+(x-k-l)^2)$,

$$\Big|\sum_{k\in P}\sum_{l\in P}\sum_x h_1(x)\overline{h_2(x-k)h_3(x-l)}h_4(x-k-l)\Big|\geq\eta|P|^2N$$

where $h_1(x) = f(x)\omega^{-\lambda x^2-\mu x}$, $h_2(x) = f(x)\omega^{-\lambda x^2}$, $h_3(x) = g(x)\omega^{-\lambda x^2+(2\lambda v-\mu)x}$ and $h_4(x) = g(x)\omega^{-\lambda x^2+2\lambda vx}$. This implies that

$$\sum_x\Big|\sum_{k\in P}\sum_{l\in P} h_1(x)\overline{h_2(x-k)h_3(x-l)}h_4(x-k-l)\Big| \geq \eta|P|^2N.$$

For each x, define $\eta(x)$ by $|\sum_{k\in P}\sum_{l\in P}\overline{h_2(x-k)h_3(x-l)}h_4(x-k-l)| = \eta(x)|P|^2$. Then

$$\begin{aligned} N^{-1} \quad &\Big|\sum_r\sum_{k\in P}\sum_{l\in P}\sum_{m\in P+P}\overline{h_2(x-k)h_3(x-l)}h_4(x-m)\omega^{r(k+l-m)}\Big| \geq \eta(x)|P|^2 \\ \Rightarrow \quad &\sum_r\Big|\sum_{k\in P} h_2(x-k)\omega^{-rk}\Big|\cdot\Big|\sum_{l\in P} h_3(x-l)\omega^{-rl}\Big|\cdot\Big|\sum_{m\in P+P} h_4(x-m)\omega^{-rm}\Big| \geq \eta(x)|P|^2N. \end{aligned}$$

However $\sum_r|\sum_{l\in P} h_3(x-l)\omega^{-rl}|^2 = N\sum_{l\in P}|h_3(x-l)|^2 \leq N|P|$ and similarly for h_4. Applying Cauchy-Schwartz,

$$\max_r\Big|\sum_{k\in P} h_2(x-k)\omega^{-rk}\Big|\cdot 2^{1/2}N|P| \geq \eta(x)|P|^2N.$$

So there exists r_x such that $|\sum_{k\in P} h_2(x-k)\omega^{r_xk}| \geq \eta|P|2^{-1/2}$. That is,

$$\Big|\sum_{k\in P} f(x-k)\omega^{-\lambda(x-k)^2+r_x(x-k)}\Big| \geq \eta(x)|P|2^{-1/2}.$$

Summing over all x, we obtain $\sum_x|\sum_{y\in x-P} f(y)\omega^{-\lambda y^2+r_xy}| \geq \eta|P|N2^{-1/2}$. An easy averaging argument then shows that we can partition $\mathbb{Z}_N$ into translates of copies of P (or P with an endpoint removed), which we call $P_1, P_2, \cdots, P_M$ with

$$\sum_i\Big|\sum_{y\in P_i} f(y)\omega^{-\lambda y^2-r_iy}\Big| \geq \eta N|P|/2.$$

The division by $2^{1/2}$ is to ensure that the P_i differ in length by at most 1. $\square$

Let $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ be a function. We define, for $S \subset \mathbb{Z}_n$, $\text{diam}\phi(S) = \max\{\phi(x)-\phi(y) : x, y \in S\}$.

Lemma 7.11. *Let $m, r, l \in [N]$ and let P be a $\mathbb{Z}_N$-arithmetic progression of length m. Let $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ be a linear function. Then, provided that $l \leq (m/r)^{1/3}$, P can be partitioned into subprogressions $P_i, i \geq 1$ of lengths l or $l-1$, such that diam$\phi(P_i) \leq N/r$ for each i.*

Proof. Without loss of generality, suppose $P = [0, m-1]$. By the pigeonhole principle, there exists $d \leq rl$ such that $|\phi(d)-\phi(0)| \leq N/rl$. Set $Q = \{x, x+d, \ldots, x+(l-1)d\}$.

Then $|\phi(x+ld)-\phi(x)| \leq l|\phi(d)-\phi(0)| \leq N/r$ so $\text{diam}\phi(Q) \leq N/r$. As each congruence class modulo d has size at least $m/d \geq m/rl \geq l^2$, we can split P into copies P_i of Q, differing in length by at most one. $\square$

In the next lemma, we apply Weyl's Theorem (Theorem 3.10):

Lemma 7.12. *Let $m \in [N]$. and let $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ be a quadratic function and let P be a $\mathbb{Z}_N$-arithmetic progression of length m. Then for any $l \leq m^{1/18.128}$, P can be partitioned into subprogressions P_i, $i \geq 1$, of lengths l or $l-1$, with $\text{diam}\phi(P_i) \leq Cm^{-1/6.128}N$.*

PROOF. Suppose $\phi(x) = ax^2+bx+c$ and $P = [m]$. Choose $d \leq m^{1/2}$ such that, modulo N, $|ad^2| \leq m^{-1/128}N$: this is possible, by Theorem 3.10 with $k = 2$. Let $t \leq m^{1/3.128}$ and $Q_i = \{x, x+d, \ldots, x+(t-1)d\}$. Then $\phi(x+td)-\phi(x) = (2axd+bd)t+ad^2t^2$. We note that $|ad^2t^2| \leq Cm^{-1/3.128}N$ modulo N. Applying Lemma 7.11 to Q_i, with $r = m^{1/6.128}$, for $l \leq m^{1/18.128}$, Q_i can be partitioned into subprogressions R_{ij} of sizes l or $l-1$ with $\text{diam}\phi(R_{ij}) \leq N/r = Cm^{-1/6.128}N$. Considering a partition of P into Q_is, the R_{ij} form the required arithmetic progressions. $\square$

Lemma 7.13. *Let $\phi : \mathbb{Z}_N \to \mathbb{Z}_N$ be a quadratic polynomial and $r \leq N$. Then there exists $m \leq Cr^{1-1/18.128}$ such that $[0, r-1]$ can be partitioned into arithmetic progressions $P_1, P_2, \ldots, P_m$, of lengths differing by at most 1, and such that, if $f : \mathbb{Z}_N \to \mathbb{D}$ is any function with*

$$\Big|\sum_{x=0}^{r-1} f(x)\omega^{-\phi(x)}\Big| \geq \eta r,$$

then

$$\sum_{j=1}^{m}\Big|\sum_{x\in P_j} f(x)\Big| \geq \eta r/2.$$

PROOF. By Lemma 7.12, we find $P_1, P_2, \ldots, P_m$ such that $\text{diam}\phi(P_i) \leq CNr^{-1/6.128}$. Provided N is sufficiently large, this is at most $\eta N/4\pi$. By the triangle inequality,

$$\sum_{j=1}^{m}\Big|\sum_{x\in P_j} f(x)\omega^{-\phi(x)}\Big| \geq \eta r.$$

Let $x_j \in P_j$. The estimate on the diameter of $\phi(P_i)$ implies that $|\omega^{-\phi(x)} - \omega^{-\phi(x_j}| \leq \eta/2$ for all $x \in P_j$. So

$$\begin{aligned}\sum_{j=1}^{m}\Big|\sum_{x\in P_j} f(x)\Big| &= \sum_{j=1}^{m}\Big|\sum_{x\in P_j} f(x)\omega^{-\phi(x_j)}\Big| \\ &\geq \sum_{j=1}^{m}\Big|\sum_{x\in P_j} f(x)\omega^{-\phi(x)}\Big| - \sum_{j=1}^{m}(\eta/2)|P_j| \geq \eta r/2.\end{aligned}$$

This completes the proof. □

Szemerédi's Theorem. *There exists an absolute constant $c > 0$ such that if $A \subset [N]$, $|A| = \delta N$ and $\delta \geq (\log\log\log N)^c$, then A contains an arithmetic progression of length four.*

Proof. Regard A as a subset of $\mathbb{Z}_N$. If A is quadratically $\alpha = \delta^{32}/2^{88}$-uniform, then the theorem is proved, by Corollary 7.6. Let $f(x) = A(x) - \delta$ and suppose f is not quadratically α-uniform. By Lemma 7.7, there exists a set B of cardinality at least $\alpha N/2$ and a function $\phi : B \to \mathbb{Z}_N$ such that

$$\sum_{k\in B} |\hat{\Delta}(f;k)(\phi(k))| \geq (\alpha/2)^2 N^3.$$

By Lemma 7.8, ϕ has at least $(\alpha/2)^8 N^3$ additive quadruples and so, by Lemma 7.9, there exists an arithmetic progression P with $|P| \geq N^\gamma$ and

$$\sum_{k\in P} |\Delta(f;k)\hat{}(2\lambda k + \mu)|^2 \geq \eta |P| N^2$$

By Ruzsa's proof of Freiman's Theorem, we may choose $\gamma = \alpha^K$ and $\eta \geq \exp(-\alpha^{-K})$ where $K > 0$ is an absolute constant. By Lemma 7.10, we then have

$$\sum_i \Big|\sum_{x\in P_i} f(x)\omega^{-\lambda x^2 - r_i x}\Big| \geq \eta |P| N/2,$$

where the P_i are as in Lemma 7.10. Apply Lemma 7.13 in each P_i to obtain further progressions P_{ij}, of cardinalities differing by at most 1, and with average lengths $C|P|^{1/18.128}$ (for some constant $C > 0$) and such that

$$\sum_i \sum_{j=1}^{m} \Big|\sum_{x\in P_{ij}} f(x)\Big| \geq \eta N |P|/4.$$

A consequence of Lemma 7.12 is that we can insist that the P_{ij} are $\mathbb{Z}$-arithmetic progressions, except that (by Lemma 2.3) the average length of P_{ij} is $C|P|^{1/2.18.128}$, where $C > 0$ is a constant and no P_{ij} has more than twice this length.

Relabel the P_{ij}s as $Q_1, Q_2, \ldots, Q_M$, where $M = N^{-\gamma/2.18.128}$ and the Q_i have average length $N^{\gamma/2.18.128}$. As $\sum f(x) = 0$, we have

$$\sum_i \Big(\Big|\sum_{x\in Q_i} f(x)\Big| + \sum_{x\in Q_i} f(x)\Big) \geq \eta N/4.$$

The contribution of Q_i with $|Q_i| \leq \sqrt{N/M}$ is at most $2N/\sqrt{M} \leq \eta N/8$, therefore there exists Q_i such that $|Q_i| \geq \sqrt{N/M}$ such that $|\sum_{x \in Q_i} f(x)| + \sum_{x \in Q_i} f(x) \geq \eta |Q_i|/8$. This implies that $\sum_{x \in Q_i} f(x) \geq \eta |Q_i|/16$.

So we have shown that there exists an arithmetic progression Q, of length at least $\sqrt{N/M} \geq N^{\gamma/4.18.128} = N^{\delta^c}$ such that $|A \cap Q| \geq (\delta + \exp[-\delta^c])|Q|$, where $c > 0$ is a constant. Rewriting this in terms of δ, a four-term arithmetic progression must be found when $\delta \geq (\log\log\log N)^{-c}$ for some $c > 0$. $\square$

References

[1] A. Balog and E. Szemerédi, *A statistical theorem of set addition*, Combinatorica **14**(3) (1994) 263–268.

[2] Y. Bilu, *Structure of sets with small sumset*, Structure Theory of Set Addition, Astérisque **258** (1999) 77–108.

[3] N. N. Bogolyubov, Zap. Kafedry Mat. Fizi. **4** (1939) 185.

[4] P. Erdős and P. Turán, *On some sequences of integers*, J. London Math. Soc. **11** (1936) 261–264.

[5] G. R. Freiman, Foundations of a Structural Theory of Set Addition, Translations of Mathematical Monographs **37**, Amer. Math. Soc., Providence, R. I., USA.

[6] H. Fürstenburg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204–256.

[7] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998) (3) 529–551.

[8] A. W. Hales, R. I. Jewett, *Regularity and positional games*, Trans. Amer. Math. Soc. **106** (1963), 222–229.

[9] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. (2) **35** (1987), 385–394.

[10] N. M. Korobov, Exponential Sums and their Applications, Mathematics and its Applications **80**, Kluwer, (1992).

[11] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 245–252.

[12] I. Ruzsa, *Generalized arithmetic progressions and sumsets*, Acta Math. Hungar. **65** (1994), 379–388.

[13] I. Ruzsa, *An analog of Freiman's Theorem for abelian groups*, Structure Theory of Set Addition, Astérisque **258** (1999) 323–326.

[14] S. Shelah, *Primitive recursive bounds for van der Waerden Numbers*, J. Amer. Math. Soc. **1**(3) (1988) 683–697.

[15] C. F. Siegel, Lectures on Geometric Number Theory,

[16] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta Math. Acad. Sci. Hungar. **20** (1969), 89–104.

[17] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. Hungar. **27** (1975), 299–345.

[18] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. **56** (1990) 155–158.

[19] G. Tenenbaum, Introduction to analytic and probabilistic number theory, Cam. Studies in Advanced Math. **46** Cam. Univ. Press (1995).

[20] B. L. van der Waerden, *Beweis einer Baudetschen vermutung*, Nieuw Arch. Wisk. **15** (1927), 212–216.

[21] R. C. Vaughan, The Hardy-Littlewood Method, 2nd Ed. Cam. Tracts in Math. **125** Cam. Univ. Press (1997).

[22] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Trav. Inst. Math. Steklof **23** (1947).

[23] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Annalen **77** (1913), 313–352.

Notation

A	general integer set
$A+B$	sum set $\{a+b : a \in A, b \in B\}$
$\|\alpha\|$	distance from α to the nearest integer
$\{\alpha\}$	fractional part of α
A^*	set of subset sums $\{\sum \varepsilon_i a_i : \varepsilon_i \in \{0,1\}, a_i \in A\}$
$B(K,\delta)$	Bohr neighbourhood
$\mathbb{C}$	field of complex numbers
$c(q)$	$\min\{c : \|A\| \geq c, A \subset \mathbb{Z}_q \Rightarrow A^* = \mathbb{Z}_q\}$
c, C	constant
Γ	graph of a function
$\Gamma(a)$	neighbourhood of a vertex a
d	dimension of arithmetic progression
$\mathbb{D}$	unit disc in $\mathbb{C}$
$D_i(G)$	ith magnification ratio
$\det(\Lambda)$	determinant of lattice Λ
$\Delta(f;k)(r)$	$f(r)\overline{f(r-k)}$
$e(\alpha)$	$\exp(2\pi i\alpha)$
E	expectation
δ	density
$f * g$	convolution
$\hat{f}$	fourier transform of f
$\|g\|_2$	ℓ^2-norm of function g
$G \times H$	product of layered graphs
$HJ(k,r)$	Hales-Jewett numbers
i, j, k	counting variables
$\mathrm{Im}_i(Y)$	image of Y in ith layer

kA	k-fold sum $A + A + \ldots + A$ of A
K	convex body or absolute constant
$K(t)$	tth cross-section of body K
$\Lambda(x)$	von Mangoldt's function
$(m, n]$	integers greater than m and less than or equal n
$\mu(x)$	Möbius function
$n_k(N)$	number of elements required in $[N]$ for a k-term progression
N	large integer
$[N]$	$\{1, 2, \ldots, N\}$
$\mathbb{N}$	natural numbers
Prob	probability
$\mathbb{R}$	real numbers
$\tau(n)$	divisor function
$\mathrm{vol}(K)$	volume of K
$W(k, r)$	van der Waerden numbers
$x \oplus jA$	Hales-Jewett line
$\mathbb{Z}$	set of integers
ω^r	$\exp(2\pi ir/N)$