IASc-NASI-INSA SRPF 2012,
Final Report

SOME RESULTS IN ADDITIVE COMBINATORICS AND ANALYTIC NUMBER THEORY

MANJIL P. SAIKIA

Abstract. In this report we state and prove a few non-trivial theorems from additive combinatorics. We also give a very brief account of the circle method along with some prerequisites.

1. Introduction

This report is divided into three sections. This first section gives some basic notations, definitions and results that will be used in the next two sections of the report. The second section deals with additive combinatorics where many elementary results related to basic sumset estimates are proved. We also prove the Roth's Theorem, Varnavides Theorem, Plüneccke's Theorem and the Balog-Szemerédi-Gowers theorem among other related results in that section. The third section is devoted to analytic number theory, and we give a very brief introduction to the cicle method in that section. We prove Weyl's and Hua's theorems in that section.

We begin by giving a few notations and definitions that will be used in the remaining part of the report.

Notation 1.1. *$X \ll Y$ means that there exists an absolute constant $C > 0$ such that $|X| \leq CY$.*

Notation 1.2. $e(x) =: e^{2\pi ix} = \cos 2\pi x + i \sin 2\pi x, i = \sqrt{-1}$.

Notation 1.3. $||x|| = min\{|x - n| : n \in \mathbb{Z}\}$.

Definition 1.4. *The sumset of A and B is defined by*

$$A + B = \{x \in Z : x = a + b \text{ with some } a \in A, b \in b\}.$$

Typically we write $A + B = \{a + b : a \in A, b \in B\}$ with the understanding that the elements are not repeated in the set $A + B$.

Definition 1.5. *In a similar way we can define the following sets*

i. $kA = A + A + \ldots + A$,
ii. $b + A = \{b\} + A = \{b + a : a \in A\}$, *a translate of A,*
iii. $A - B = \{a - b : a \in A, b \in B\}$, *the difference set,*
iv. $A.B = \{ab : a \in A, b \in B\}$, *the product set,*
v. $A/B = \{a/b : a \in A, b \in B\}$, *the quotient set,*
vi. $k.A = \{k\}.A = \{ka : a \in A\}$, *a dilate of A.*

Reported by Manjil P. Saikia (MATS265).

Definition 1.6. *The representation functions are defined as follows*

i. $r_{A\pm B}(x) = |\{(a,b) \in A \times B : x = a \pm b\}|$,
ii. $r_{A.B}(x) = |\{(a,b) \in A \times B : x = ab\}|$,
iii. $r_{A/B}(x) = |\{(a,b) \in A \times B : x = a/b\}|$.

Definition 1.7 (e-transform)**.** *Let $e \in Z$ be arbitary, then we define the e-transform of (A,B) as the pair $(A(e), B(e))$ of subsets of Z given by $A(e) = A \cup (B+e)$ and $B(e) = B \cap (A-e)$ and where Z is an Abelian group.*

Definition 1.8. *A partition of the set of positive integers into r disjoint sets is called an r-coloring. The set of integers of the same colour is called a colour class. All the terms belonging to the same color class are called monochromatic.*

Definition 1.9 (Fourier Transform)**.** *The Fourier transform for $f : \mathbb{Z}_N \to \mathbb{C}$ is defined as $\hat{f} : \mathbb{Z}_N \to \mathbb{C}$ and by setting*

$$\hat{f}(r) = \sum_n f(n) e(-\frac{rn}{N}).$$

We now state some important facts that will be useful in our study.

Theorem 1.10 (Fourier Inversion)**.** *For a function $f : \mathbb{Z}_N \to \mathbb{C}$, we have*

$$f(n) = \frac{1}{N} \sum_n \hat{f}(r) e(\frac{rn}{N}).$$

Notation 1.11. *Given a set $A \in \mathbb{Z}_N$ we will use $I_A(n)$ to denote the characteristic function of A. That is $I_A(n) = 1$ if $n \in A$ and 0 otherwise. Also, we let f_A denote the balanced function $f_A(n) = I_A(n) - |A|/N$. Note that $I_{\hat{A}}(0) = |A|$ and that $\hat{f}_A(0) = 0$.*

Theorem 1.12 (Parseval's Identity)**.** *For any real or complex coefficients u_n, we have*

$$\int_0^1 |\sum_n u_n e(n\alpha)|^2 d\alpha = \sum_n |u_n|^2.$$

Proof. We prove the result for a finite sum, however by appropiate convergence we can show that the result is true for infinite sum also.

We have,

$$\int_0^1 |\sum_n u_n e(n\alpha)|^2 d\alpha = \int_0^1 \sum_n u_n e(n\alpha) \sum_m \overline{u_m} e(-m\alpha) d\alpha.$$

The above expression in turn equals,

$$\sum_n \sum_m u_n \overline{u_m} \int_0^1 e((n-m)\alpha) d\alpha = \sum_{n=m} u_n \overline{u_m} = \sum_n |u_n|^2.$$

□

Another varient of the above is,

Theorem 1.13.

$$N \sum_n f(n) \overline{g(n)} = \sum_k \hat{f}(k) \overline{\hat{g}(k)}.$$

And in the sepcial case of $f = g$ we have,

$$N\sum_n |f(n)|^2 = \sum_k |\hat{f}(k)|^2.$$

Theorem 1.14 (Dirichlet's Approximation Theorem)**.** *For integers $k \geq 1$, $Q \geq 1$ and $\alpha_1, \alpha_2, \ldots, \alpha_k$ real numbers, there is an integer q which satisfies $1 \leq q \leq Q^k$ such that*

$$||q\alpha_j|| \leq \frac{1}{Q}, \forall\ j = 1, 2, \ldots, k.$$

Proof. We split the k-dimensional unit cube into Q^k small cubes of side $\frac{1}{Q}$. We now use the box principle. These small cubes are the boxes. For $u = 0, 1, \ldots, Q^k$ we consider the vectors $(u\alpha_1, u\alpha_2, \ldots, u\alpha_k)$ modulo 1, that is we reduce all coordinates to the interval $[0, 1)$ by subtracting the largest not bigger integer from it. Each vector is in the unit circle and there are $Q^k + 1$ of them. At least one box should contain more than one vector. They belog to $u > v$ say. Here $q = u - v$ will do it as there are integers u_j and v_j such that for all $j = 1, 2, \ldots, k$ we have $|(u\alpha_j - u_j) - (v\alpha_j - v_j)| \leq \frac{1}{Q}$. □

There are numerous other ways to prove the above results, by using the geometry of numbers or Farey sequences and many more.

2. Additive Combinatorics

2.1. **Introduction.** Additive combinatorics is the theory of counting additive structures in sets. It is an amalgamation of combinatorics, additive number theory, analysis and some ergodic theory. The term 'additive combinatorics' was coined by Terence Tao a few years earlier, and since then this branch of mathematics has seen a massive development in the recent years. A fundamental task in this subject is to give some quantitative measures of additive structures in a set, and then investigate to what extend these measures are equivalent to each other. We begin with a few introductory theorems.

Theorem 2.1. *For two subsets A and B of the real numbers $\mathbb{R}$, we have*

$$|A| + |B| - 1 \leq |A + B| \leq |A||B|,$$

and the equality holds iff A and B are arithmetic progressions of the same difference.

Proof. The upper bound is readily obtained, when all the elements of the form $a+b$ are different, where $a \in A, b \in B$. This is possible if for example, let

$$A = \{0, 1, \ldots, r-1\},\ B = r.\{0.1, \ldots, s-1\} = \{0, r, 2r, \ldots, (s-1)r\},$$

and then $A + B = \{0, 1, \ldots, rs - 1\}$.

We now show that the lower bound is obtained. We can list the elements of the sets as

$$A = \{a_1 < a_2 < \cdots < a_r\}, B = \{b_1 < b_2 < \cdots < b_s\}.$$

Clearly the following chain contains $r + s - 1$ different elements of the set $A + B$,

$$a_1 + b_1 < a_1 + b_2 < a_1 + b_3 < \cdots < a_1 + b_s < a_2 + b_s < a_3 < b_s < \cdots < a_r + b_s.$$

This proves the lower bound, and it is not hard to see that if $A = \{1, \ldots, r\}$ and $B = \{1, \ldots, s\}$, then $A + B = \{2, \ldots, r + s\}$.

We can have several other examples of chains with $r+s-1$ elements of $A+B$ in increasing order, like

$$a_1+b_1<a_2+b_1<a_2+b_2<a_2+b_3<\cdots<a_2+b_s<a_3+b_s<\cdots<a_r+b_s.$$

If $A+B=r+s-1$, then the above two chains must be the same. The first terms and the last $r-1$ terms agree clearly. However if we rearrange the rest of the equations we shall get

$$\begin{aligned} b_2-b_1&=a_2-a_1,\\ b_3-b_2&=a_2-a_1,\\ &\vdots\\ b_s-b_{s-1}&=a_2-a_1. \end{aligned}$$

Thus the set B is indeed an AP with difference a_2-a_1. It is clear in the above that the roles of A and B are symmetric, and so we can show by a similar argument that the set A is also an AP with difference b_2-b_1. □

We can generalize the above result to the following,

Theorem 2.2. *For the subsets $A-1,\dots,A_k, k\geq 2$ of $\mathbb{R}$, we have*

$$|A_1|+\cdots+|A_k|-k+1\leq|A_1+\cdots+A_k|\leq|A_1|\cdots|A_k|,$$

and equality holds iff $A_1,\dots,A_k$ are arithmetic progressions of the same difference.

We omit the proof here, which is very simple to obtain via induction.

The following corollary follows from the preceeding discussion.

Corollary 2.3. *For a finite subset A of $\mathbb{R}$, and $k\geq 2, k\in\mathbb{Z}$ we have,*

$$k|A|-k+1\leq|kA|\leq|A|^k,$$

and equality holds iff A is an arithmetic progression.

Theorem 2.4. *For finite subsets A, B and C of $\mathbb{R}$, we have*

$$|A-C||B|\leq|A-B||B-C|.$$

Proof. For all $d\in A-C$, we fix a representation $d=a_d-c_d$ where $a_d\in A, c_d\in C$. We now define a map between $(A-C)\times B$ and $(A-B)\times(B-C)$, namely a pair (d,b), where $d\in A-C$ and $b\in B$ is mapped to the pair $(a_d-b, b-C-d)$ where $a_d-b\in A-B, b-c_d\in B-C$.

If (u,v) is an image under this map then $u+v$ should be d, and then a_d or c_d determine b such that $b=a_d-u$ or $b=c_d+v$. Thus the map is injective, that is an image determines its unique inverse.

The injectivity of this map now implies that the size of the image space should be bigger than or equal to the size of the domain, which is the stated inequality. □

On putting $C=A$ and $B=-A$ in the above we can readily get,

Corollary 2.5.

$$|A-A|\leq\frac{|A-B|^2}{|B|},\ for\ all\ B, \tag{2.1}$$

$$\frac{|A-A|}{|A|}\leq\frac{|A+A|^2}{|A|^2}. \tag{2.2}$$

We now state and prove the last theorem of this subsection.

Theorem 2.6. *For any finite subsets A and B of $\mathbb{R}$ there is a set $X \subset B$ such that $|X| \leq \frac{|A+B|}{|A|}$ and $B \subset A - A + X$.*

Proof. Let X be the largest subset such that the sets $A + x : x \in X$ are mutually disjoint. As $A+x \subset A+B$ for all $x \in B$ and $|A+x| = |A|$, we have $|X||A| \leq |A+B|$ as required.

Now for any $b \in B$ we have $(A + b) \cap (A + x) \neq \phi$ with some $x \in X$, otherwise b could be added to X. That is there are elements $a_1, a_2 \in A$ such that $a_1 + b = a_2 + x$ or $b = a_2 - a_1 + x \in A - A + X$ as required. □

2.2. **Plünnecke's Theorem.** We shall give below a simple elementary proof of Plünnecke's Theorem. But first we state and prove a few results that will be used in obtaining that.

Lemma 2.7. *For finite subsets A and B of $\mathbb{R}$ and $c > 0$ we have*

$$|A + B| = c|A|, \text{ while } |A' + B| \geq c|A'| \text{ for all } A' \subset A, \tag{2.3}$$

then for all finite subset C of the real numbers we have

$$|A + B + C| \leq c|A + C|. \tag{2.4}$$

Proof. We shall use induction on the size of C. If $C = 1$, that is if $C = \{x\}$ then

$$|A + B + x| = |A + B| = c|A| = c|A + x|,$$

and hence the statement in the theorem is true.

Let us now suppose that the statement (2.4) is true for a non-empty set C, and let $x \notin C$ be an arbitary real number, and also let $C' = C \cup \{x\}$.

We prove the statement for C'.

We define

$$A' = \{a \in A : a + x \in A + C\} = A \cap (A + C - x) \subset A.$$

We then have $A' + x = (A + x) \cap (A + C)$ and $A + C' = (A + C) \cup (A + x)$ and so

$$|A + C'| = |A + C| + |A + x| - |A' + x| = |A + C| + |A| - |A'|.$$

As $A' + x \subset A + C$, implies $A' + B + x \subset A + B + C$ and so

$$A+B+C' = (A+B+C) \cup (A+B+x) = (A+B+C) \cup [(A+B+x) \setminus (A'+B+x)],$$

and also

$$|A+B+C'| \leq |A+B+C| + |A+B+x| - |A'+B+x| = |A+B+C| + |A+B| - |A'+B|.$$

We now use the induction hypothesis (2.4) to estimate the first term on the right hand side and the two conditions of (2.3) to the other two terms thus obtaining

$$|A + B + C'| \leq c|A + C| + c|A| - c|A'| = c|A + C'|,$$

as is required to complete the induction. □

As a consequence of the above lemma we can prove the following.

Theorem 2.8. *For finite subsets A, B and C of $\mathbb{R}$ we have*

$$|A + C||B| \leq |A + B||B + C|.$$

Proof. We let $U \subset B$, such that the ratio $\frac{|U+A|}{|U|} = c$ is minimal. We have for any $U' \subset U$, $\frac{|U'+A|}{|U'|} \geq c$. The conditions of the above lemma are satisfied for the following choice

$$A \mapsto U,\ B \mapsto A,\ C \mapsto C,$$

getting

$$|U + A + C| \leq c|U + C|.$$

We have, $|A+C| \leq |U+A+C|, |U+C| \leq |B+C|$ and $c \leq |A+B|/|B|$, as B itself is considered when minimum is selected. Thus the theorem easily follows from the above inequalites. □

Writing $C = A$ and $B = -A$ we get (2.2). Again writing $C = (h-1)B$ to (2.4) we get $|A + hB| \leq c|A + (h-1)B|$, and an induction gives the following corollary.

Corollary 2.9. *For any finite subsets A and B of $\mathbb{R}$, and a $c > 0$ we have*

$$|A + B| = c|A|,\ \textit{while}\ |A' + B| \geq c|A'|\ \textit{for all}\ A' \subset A,$$

then for all positive integers h, we have

$$|A + hB| \leq c^h|A|.$$

Now we are in a position to state and prove Plünnecke's theorem.

Theorem 2.10 (Plünnecke)**.** *For a finite subset B of $\mathbb{R}$, satisfying $|B + B| \leq c|B|$ (or $|B - B| \leq c|B|$) and all non-negative integers m and n we have*

$$|mB - nB| \leq c^{m+n}|B|.$$

Proof. Let $\phi \neq A \subset B$ (*or* $\phi \neq A \subset -B$) be one of the sets that maximizes the ratio $|A + B|/|A|$, and we write $|A + B| = c'|A|$. Clearly $c' \leq c$. By this definition we have $|A' + B| \leq c'|A'|$ for all $A' \subset A$, and hence the conditions of the previous corollary is satisfied. We have,

$$|hB| \leq |A + hB| \leq (c')^h|A| \leq c^h|B|,$$

proving the statement for the case of $m = 0$ *or* $n = 0$.

For the general statement we use Theorem 2.4 and the transformations

$$A \mapsto mB,\ B \mapsto -A,\ C \mapsto nB.$$

Now Theorem 2.4 and the above corollary implies

$$|mB - nB||A| \leq |A + mB||A + nB| \leq (c')^m|A|(c')^n|A| \leq c^{m+n}|B||A|,$$

from which the theorem following upon simplying the term $|A|$. □

The original proof of Plünnecke was by using graph theory. Recently George Petridis [3] found another elementary proof somewhat similar to the one we have presented here.

2.3. **Cauchy-Davenport Theorem.** In the proof of Theorem 2.1 we used the ordering of the real numbers. However, we cannot generalize that proof for finite groups, say for the group of residue classes. In this subsection we shall concentrate on getting a lower bound for the size of $A+B$ if A and B are subsets of the additive group of residues modulo m. To describe all the extremal cases is an open question in general, but is solved for $\mathbb{Z}_p$, the group of residue classes modulo p, where p is a prime.

We begin with a few results which we shall use in proving the Cauchy-Davenport theorem.

Lemma 2.11. *For subsets A and B, of a finite Abelian group Z with $|A|+|B| \geq |Z|+t$, we have $r_{A+B}(z) \geq t, \forall z \in Z$.*

Proof. We consider the translates $z-B$, then we have

$$|Z| \geq |A \cup (z-B)| = |A| + |z-B| - |A \cap (z-B)| = |A| + |B| - |A \cap (z-B)|,$$

from which it follows that

$$|A \cap (z-B)| \geq |A| + |B| - |Z| \geq t.$$

There exists at least t distinct elements $a \in A$ and t distinct elements $b \in B$ such that $a = z - b$, proving $r_{A+B}(z) \geq t$. Since, $z \in Z$ was arbitary so this concludes the lemma. □

For $t = 1$ in the above we have,

Corollary 2.12. *For subsets A and B of the finite Abelian group Z such that $|A|+|B| \geq |Z|$ we have $A + B = Z$.*

Lemma 2.13. *For any two nonempty subsets A and B of the Abelian group Z and e be any element of Z we have,*

$$A(e) + B(e) \subset A + B, \tag{2.5}$$

$$A(e) \smallsetminus A = e + (B \smallsetminus B(e)), \tag{2.6}$$

$$|A(e)| + |B(e)| = |A| + |B|, \ if \ A \ and \ B \ are \ finite. \tag{2.7}$$

Proof. We have,

$$A(e) + B(e) = (A + B(e)) \cup (B + e + B(e)) \subset (A + B) \cup (B + e + A - e) \subset A + B$$

and thus (3.2) is established.

We also have,

$$A(e) \smallsetminus A = (B + e) \smallsetminus A = \{b + e : b \in B, b + e \notin A\}$$

and which in turn gives

$$A(e) \smallsetminus A = e + \{b \in B : b \notin A - e\} = e + \{b \in B : b \notin B(e)\} = e + (B \smallsetminus B(e)).$$

Thus (3.4) is proved. Finally we prove (3.3).

We note that clearly $A \subset A(e)$ and $B(e) \subset B$. For finite sets we have using (3.4),

$$|A(e)| - |A| = |A(e) \smallsetminus A| = |e + (B \smallsetminus B(e)| = |B| - |B(e)|.$$

□

We now state and prove the final theorem before we prove the Cauchy-Davenport theorem.

Theorem 2.14. *Let $m > 1$ be fixed, and if A and B are nonempty subsets of $\mathbb{Z}_m$ such that $0 \in B$, and $gcd(b, m) = 1, \forall b \in B \setminus \{0\}$, then we have*

$$|A + B| \geq min\{m, |A| + |B| - 1\}.$$

Proof. If $|A| + |B| - 1 \geq m$, then this follows from Corollary 2.12. So, we suppose $|A| + |B| \leq m$, and then prove this result by induction.

If $|B| = 1$, then $|A + B| = |A| = |A| + |B| - 1$, and hence the statement is true.

Let $|B| \geq 2$. Now we try to prove this theorem for B if it is true for any $B' \subset \mathbb{Z}_m$ with $|B'| < |B|$.

We select $b \in B, b \neq 0$. Now $A + b \neq A$, else starting from any arbitary $a_0 \in A$ we find that $a_1 = a_0 + b \in A$ and $a_2 = a_1 + b = a_0 + 2b \in A$ and so on, all $a_0 + jb \in A$. Using the fact that $gcd(b, m) = 1$ we find $\mathbb{Z}_m \subset A$ which is not possible since $|A| + |B| \leq m, |N| \geq 2$.

We can take an $e \in A$ such that $e + b \notin A$. We use the induction hypothesis on the pair $(A(e), B(e))$. As $A \subset A(e)$ and $0 \in B \cap (A - e)$ so, they are empty. Also $b \notin A - e$, so $B(e) \subsetneqq B$, and we conclude using (3.3) and (3.2) that

$$|A| + |B| - 1 = |A(e)| + |B(e)| - 1 \leq |A(e) + B(e)| \leq |A + B|.$$

□

Now, we are in a position to state and prove the Cauchy-Davenport theorem for the case of any two subsets of $\mathbb{Z}_p$.

Theorem 2.15 (Cauchy-Davenport)**.** *For a fixed prime p and subsets A and B of $\mathbb{Z}_p$ we have*

$$|A + B| \geq min\{p, |A| + |B| - 1\}.$$

Proof. We apply Theorem 3.5 with $B' = B - b$ for an arbitary element $b \in B$. Thus the theorem follows. □

We now extend the above result as follows,

Theorem 2.16 (Cauchy-Davenport)**.** *For a fixed prime p, $h \geq 2$ and nonempty subsets $A_1, A_2, \ldots, A_h$ of $\mathbb{Z}_p$ we have,*

$$|A_1 + A_2 + \cdots + A_h| \geq min\{p, |A_1| + |A_2| + \cdots + |A_h| - h + 1\}.$$

Proof. We prove this result using induction on h. The case for $h = 2$ is just the previous theorem. So, we let $h \geq 3$, and we suppose that the result is true for any $h-1$ subsets of $\mathbb{Z}_p$. We let $A_1, A_2, \ldots, A_h$ be nonempty subsets of $\mathbb{Z}_p$, and we write $B = A_1 + A_2 + \cdots + A_{h-1}$.

Now by the induction hypothesis we have,

$$|B| = |A_1 + A_2 + \cdots + A_{h-1}| \geq min\{p, |A_1| + |A_2| + \cdots + |A_{h-1}| - h + 2\},$$

and hence we have,

$$|A_1 + A_2 + \cdots + A_h| = |B + A_h| \geq min\{p, |B| + |A_h| - 1\}.$$

Thus we have

$$|A_1 + A_2 + \cdots + A_h| \geq min\{p, min\{p, |A_1| + |A_2| + \cdots + |A_{h-1}| - h + 2\} + |A_h| + 1\},$$

and hence we finally obtain the required result

$$|A_1 + A_2 + \cdots + A_h| \geq min\{p, |A_1| + |A_2| + \cdots + |A_h| - h + 1\}.$$

□

2.4. **Arithmetic Progressions.** In this subsection we shall state without proof some important results involving arbitary arithmetic progressions. We shall also state and prove three important results connected with arithmetic progressions in a set. An important class of problems in additive combinatorics is to determine whether a set A contains a non-trivial arithmetic progression of certain given length k. One reason for being interested in arithmetic progressions is because they are indestructible structures. They are preserved under translation and dilations of A.

We begin by stating some important results without proofs.

Theorem 2.17 (van der Waerden, 1927)**.** *For integers $k \geq 2, r \geq 2$, and any r-coloring of the positive integers, at least one color class contains a k-term arithmetic progression.*

There are other ways to state the above result, we give one such example below.

Theorem 2.18. *Given integers $k \geq 2$ and $r \geq 2$, there exists a positive integer $N = N(k, r)$ such that for any r-coloring of the set $\{1, 2, \ldots, N\}$, there is a monochromatic arithmetic progression of k terms.*

Erdös and Turán conjectured that van der Waerden's theorem must be true for density reasons, that is any large subset of the integers must contain long arithmetic progressions. Their conjecture was proved in 1975 by Szemerédi.

Theorem 2.19 (Szemerédi, 1975)**.** *Given an integer $k \geq 2$ and a real number δ such that $1 > \delta > 0$, there is a positive integer $N(k, \delta)$ such that if $N \geq N(k, \delta)$ and $A \subset \{1, 2, \ldots, N\}, |A| > \delta N$, then A contains a k-term arithmetic progression.*

The above theorem is the motivation behind the following recent theorem of Ben Green and Terence Tao.

Theorem 2.20 (Green-Tao)**.** *For any $k \geq 2$, the set of positive primes contains a k-term arithmetic progression.*

Before we state an prove an early result of Schur we need a special case of Ramsey's theorem, which says,

Lemma 2.21. *Suppose that the edges of the complete graph K_N are coloured using r colours, and if $N \geq N(r)$ then there is a monochromatic triangle for some natural number $N(r)$.*

Proof. We prove this by induction on r. It is very well known that if $r = 2$ and $N \geq 6$ then there is a monochromatic triangle. Let us now suppose that we know the result for $r - 1$ colourings, and we need $N \geq N(r - 1)$ for this. We now pick a vertex; there are $N - 1$ edges coming out of it. So for some colour there are more than $\lceil (N - 1)/r \rceil$ edges starting with the vertex having the same colour. Now the complete graph on the other vertices of these edges must be coloured using only $r - 1$ colours. Thus if $N \geq rN(r - 1) - r + 2$, we are done. □

We now state and prove Schur's theorem, which is not a consequence of Theorem 2.17. We know that from the density point of view, the set of positive odd integers is a large set, it is half the set of all positive integers. In spite of this, the equation $x + y = z$ cannot be solved in this large set. However, we have Schur's result which states,

Theorem 2.22 (Schur, 1916)**.** *Given any positive number r, if $N \geq N(r)$ for some $N(r)$ and the integers in $[1, N]$ are coloured using r colours then there is a monochromatic solution to $x + y = z$. Here $[1, N]$ denotes the set $\{1, 2, \ldots, N\}$.*

Proof. We consider the complete graph on N vertices labeled 1 through N. We colour the edge joining a and b using the colour of $|a - b|$. By Lemma 2.21, if N is large then there is a monochromatic triangle. If suppose its vertices are $a < b < c$, then $(c - a) = (c - b) + (b - a)$ is a solution proving our theorem. □

We now state without proof a result by Grüwald, which implies Theorem 2.17 upon taking $S = \{1, 2, \ldots, k\}$.

Theorem 2.23 (Grünwald)**.** *For an integer $r \geq 2$, a finite nonempty set of positive integers S and any r-colouring of $\mathbb{N}$, there exists integers $a \geq 1$ and b such that $a.S + b$ is monochromatic.*

We now state and prove an important theorem given by Roth which says,

Theorem 2.24 (Roth)**.** *There exists a positive constant C such that if $A \subset [1, N]$ with $|A| \geq CN/\log\log N$, then A has a non-trivial three term AP.*

We give a proof below that is due to Gowers.

Proof. Let $A \subset [1, N]$ with $|A| = \delta N$. We assume that N is odd, and we let B be the set of even or odd numbers in A whichever is larger. Now, we consider

$$\frac{1}{N} \sum_{r \pmod N} \hat{B}(r)^2 \hat{A}(-2r) = |\{x + y \equiv 2z \pmod N : x, y \in B, z \in A\}|.$$

Here $\hat{B}(r) = \sum_{b \in B} e(br/N)$, and similarly for $\hat{A}(r)$. By size and parity considerations, we find that $x + y \equiv 2z \pmod N$ and in fact implies that $x + y = 2z$ so that we have a three term AP. There are $|B|$ such trivial three term APs. So, the number of non-trivial three term APs is

$$\frac{1}{N} \sum_{r \pmod N} \hat{B}(r)^2 \hat{A}(-2r) - |B| = \frac{|B|^2|A|}{N} - |B| + \frac{1}{N} \sum_{r \neq 0} \hat{B}(r)^2 \hat{A}(-2r). \quad (2.8)$$

The proof is now in two parts: when A has no large Fourier coefficients (A is random), and when A has a large Fourier coefficient (A has a structure).

First we suppose that for all $r \neq 0$ we have $|\hat{A}(r)| \leq \delta^2 N/4$. In this case

$$\frac{1}{N} |\sum_{r \neq 0} \hat{B}(r)^2 \hat{A}(-2r)| \leq \frac{delta^2}{4} \sum_r |\hat{B}(r)|^2 = \frac{\delta^2}{4} N|B| \leq \frac{|A||B|^2}{2N}.$$

From (2.8) we can deduce that there are many three term APs in this case.

So, we suppose that there exists $r \neq 0$ such that $|\hat{A}(r)| \geq \delta^2 N/4$. Or equivalently we have,

$$|\sum_{a=1}^{N} (I_A(a) - \delta) e(ar/N)| \geq \frac{\delta^2}{4} N. \quad (2.9)$$

Let $1 \leq Q \leq N$ be a parameter, and we use Theorem 1.14 to find b/q where $q \leq Q$ and $(b, q) = 1$ such that $|r/N - b/q| \leq 1/qQ$. We then divide $[1, N]$ into progressions modulo q. There are q such progressions each with $N/q + O(1)$ elements. We now subsivide these progressions into M intervals each. Thus there are qM such intervals in all, and each interval contains about $N/(qM) + O(1)$

elements. let I denote one such interval. We claim that on I, $e(ar/N)$ is almost constant. It is $e(ab/q + a\theta)$ for some $|\theta| \leq 1/qQ$. Now, $e(ab/q)$ is constant as all elements of I are in the same progression modulo q. The variation in $e(a\theta)$ is at most $O(N|\theta|/M) = O(N/(qQM))$. Thus from (2.9) we have,

$$\frac{\delta^2 N}{4} \leq \sum_I |\sum_{a\in I}(I_A(a) - \delta)e(ar/N)| = \sum_I (|\sum_{a\in I}(I_A(a) - \delta)| + O(\frac{N|I|}{qQM})|$$

$$= \sum_I |\sum_{a\in I}(I_A(a) - \delta)| + O(\frac{N^2}{qQM}).$$

We choose $Q = \sqrt{N}$ and $M = C\sqrt{N}/(\delta^2 q)$ for a suitably large constant C. Then we obtain

$$\frac{\delta^2 N}{8} \leq \sum_I |\sum_{a\in I}(I_A(a) - \delta)|. \tag{2.10}$$

Again,

$$0 = \sum_I \sum_{a\in I}(I_A(a) - \delta),$$

so that from (2.10) we may deduce the existence of an I with

$$\sum_I (I_A(a) - \delta) \geq \frac{\delta^2 N}{16qM}.$$

We have I contains about $N/(qM)$ elements, and so the relative density of A within I is at least $\delta + \delta^2/16$. Now we take I and translate and dilate it so that it corresponds to the set $[1, N/qM]$. We note that APs are preserved under translation and dilations. We have thus extracted a set of density $\delta + \delta^2/16$ lying in $[1, N/(qM)] = [1, \delta^2\sqrt{N}/C]$, and it suffices to exhibit three term APs in this set. Now we repeat the above argument for this new set.

If we repeate this argument for D/δ times for an appropiate constant D then we can get a density> 0.9 when it is easy to exhibit three term APs. After these steps, the initial value of N would be reduced to $\delta^4 N^{1/2^L}/C^2$. We want the last quantity to be relatively large, like greater than say 10^3. Thus we would like $N \geq (10^3 C^2/\delta^4)^{2^{D/\delta}}$. Equivalently if $\delta > c/\log\log N$, then our arugument works. □

We now prove a stronger form of Roth's Theorem which counts the number of three term APs.

Theorem 2.25 (Varnivides)**.** *For every $\epsilon > 0$ there exists $C(\delta) > 0$ such that if $A \subset [1, N]$ with $|A| \geq \delta N$ then A contains at least $C(\delta)N^2$ three term progressions.*

Proof. By Roth's theorem we know that there exists $M = M(\delta)$ such that any set of $\delta M/2$ elements in $[1, M]$ has a non-trivial three term AP. Now, we consider progressions $P(a, d) = a + [1, M]d$ in $[1, N]$ where we allow $d \leq \delta N/M^2$ and $a \leq N(1 - \delta?M)$.

We claim that for many choices of a and d we have $|A\cap P(a, d)| \geq \delta M/@$. Indeed we have that for any given d,

$$\sum_{a\leq N(1-\delta/M)} |A \cap P(a, d)| \geq M \sum_{Md\leq a\leq N(1-\delta/M)} 1 \geq M(\delta N - 2N\delta/M).$$

It now follows that for each d there are $\gg \delta N$ values of a with $|A \cap P(a,d)| \geq \delta M/2$, so that in total there are $\gg \delta^2 N^2/M^2$ good progressions $P(a,d)$.

By Roth's theorem each good progression contributes at least one three term progression in A. But of course some of these progressions may be over counted. Suppose we are given a progression $x, x+y, x+2y$ in A. Clearly, when d is a divisor of y and $y/d \leq M$ then this progression belongs to $P(a.d)$. Therefore there are at most M choices for d. Each coice of d fixes a in at most M ways. Therefore, each progression is over counted at most M^2 times.

Thus we have exhibited $\gg \delta^2 N^2/M^4$ distinct three term APs, and this proves the theorem. □

Behrend has constructed a surprisingly large set in $[1, N]$ with no three term APs. We donot state or prove his result here.

2.5. **Balog-Szemerédi-Gowers Theorem.** Suppose we have sets A and B with $|A| = |B|$ and we know that for many choices of $(a,b) \in A \times B$ we get $a+b$ lying in a small set. Then can we form any conclusions about A? More precisely, we assume that we are given a subset G of $A \times B$ with $|G| \geq \alpha |A|^2$ and such that $S = \{a+b : (a,b) \in G\}$ is small. Then what can we say about A? The answer is that A contains a big subset A' and B contains a big subset B' such that $A' + B'$ is small. This is what the Balog-Szemerédi Theorem says.

We let the sets A and B be such hat $|A| = |B|$, and $|A + A| \leq C|A|$. From Definition 1.6 we note that

$$\sum_n r_{A+B}(b) = |A||B|,$$

and that $|A + B|$ equals the number of n such that $r_{A+B}(n) \neq 0$. Using the Cauchy-Schwarz inequality we have

$$\sum_n r_{A+B}(n)^2 \geq |A|^4/|A + B| \geq |A|^3/C.$$

The LHS of the above counts the number of *additive quadruples* (a_1, b_1, a_2, b_2) with $a_1 + b_1 = a_2 + b_2$. Thus having small $A + B$ implies the existence of many aditive quadruples.

Theorem 2.26 (Balog-Szemerédi-Gowers Theorem A)**.** *Let A and B be subsets of an abelian group with $|A| = |B|$. Suppose there are at least $\alpha|A|^3$ additive quadruples $(a_1, b_1, a_2, b_2) \in A \times B \times A \times B$ with $a_1 + b_1 = a_2 + b_2$. Then there are subsets A' of A and B' of B with $|A'| \geq \alpha^2|A|/(16\sqrt{2}), |B'| \geq \alpha^2|B|/16$, and $|A' + B'| \leq 2^{28}\alpha^{-13}|A|$.*

Theorem 2.27 (Balog-Szemerédi-Gowers Theorem B)**.** *Let A and B be two subsets of an abelian group with $|A| = |B|$. Let G be a subgraph of the complete bipartite graph between A and B, with G having at least $|A||B|/K$ edges. Suppose that $A +_G B = \{a+b : (a,b) \in G\}$ has cardinality $|A +_G B| \leq K_1|A|$. Then there exists subsets A' of A and B' of B with $|A'| \geq |A|/(4\sqrt{2}K), |B'| \geq |B|/(4K)$, and $|A' + B'| \leq 2^{15}K^5K_1^3|A|$.*

We now show that the above two versions are equivalent to each other. Suppose that we are given A and B with many additive quadruples. That is $\sum_n r_{A+B}(n)^2 \geq \alpha|A|^3$. Then there are at least $\alpha|A|/2$ popular sums n with $r_{A+B}(n) \geq \alpha|A|/2$. We now define the graph G by letting (a,b) be an edge in G precisely when $a+b$ is a

popular sum. The number of edges in G is at least $\alpha^2|A|^2/4$ and since there can be at most $2|A|/\alpha$ popular sums, we also have $|A +_G B| \leq 2|A|/\alpha$. Therefore version A follows from version B.

Conversely, we suppose that we are given a subgraph G as in version B. Then $\sum_n r_{A+_G B}(n) = |G|$, and so $sum_n r_{A+_G B}(n)^2 \geq |G|^2/|A +_G B|$ by the Cauchy-Schwarz inequality. Therefore there are at least $|G|^2/|A +_G B|$ additive quadruples, and hence we can deduce version B from vesrion A, upto constants.

We shall prove version B here, with the help of the following lemmas.

Lemma 2.28. *Let G be an undirected bipartite graph having two vertex sets A and B (that is, the edges connect points in A to points in B). Suppose that the edge set has cardinality $|A||B|/K$ for some $K \geq 1$. Given $\epsilon \in (0,1)$, there exists a subset A' of A with $|A'| \geq |A|/(\sqrt{2}K)$ such that for at least a proportion $(1-\epsilon)$ of the pairs $(a_1, a_2) \in A' \times A'$ we have at least $\epsilon|B|/(2K^2)$ paths of length 2 in G connecting $a-1$ and a_2.*

Proof. For $a \in A$ let $B(a)$ denote the points in B connected to a, and similarly for $b \in B$ let $A(b)$ denote the points in A connected to b. Let Ω denote the subset $A \times A$ consisting of pairs (a_1, a_2) for which there exists fewer than $\epsilon|B|/(2K^2)$ elements in $B(a_1) \cap B(a_2)$.

Clearly $\sum_{b\in B} |A(b)|$ equals the total number of edges $|A||B|/K$. By the Cauchy-Schwarz inequality we have,

$$\sum_{b\in B} \sum_{a_1,a_2 \in A(b)} 1 = \sum_{b\in B} |A(b)|^2 \geq |A|^2|B|/K^2.$$

Also,

$$\sum_{b\in B} \sum_{a_1,a_2\in A(b)(a_1,a_2)\in\Omega} 1 = \sum (a_1,a_2) \in \Omega \sum_{b\in B(a_1)\cap B(a_2)} 1$$
$$\leq |\Omega|\epsilon|B|/(2K^2) \leq \epsilon|A|^2|B|/(2K^2).$$

Now combining the above two relations we have,

$$\sum_{b\in B}(|A(b)|^2 - \frac{1}{\epsilon}(|A(b)^2 \cap \Omega|)) \geq \frac{|A|^2|B|}{2K^2},$$

so that for some $b \in B$ we have

$$|A(b)|^2 - \frac{1}{\epsilon}(|A(b)^2 \cap \Omega|) \geq |A|^2/(2K^2).$$

We obtain the lemma by taking A' to be this set $A(b)$. □

Lemma 2.29. *Let G be a bipartite graph as above, having an edge set of size $|A||B|/K$. We may extract a set A'' of A such that $|A''| \geq |A|/(4\sqrt{2}K)$, each vertex in A'' has degree at least $|B|/(2K)$, and for each $a_1 \in A''$ there exista at least $(a - a/(16K))|A''|$ vertices $a_2 \in A''$ such that a_1 and a_2 are joined by at least $|B|/(256K^3)$ paths of length 2.*

Proof. We remove from A all vertices with degree $\leq |B|/(2K)$. Let $\acute{A}$ denote the set of remaining vertices, and we consider the induced subgraph on vertex sets $\acute{A}$ and B. Since at most $|A||B|/(2K)$ edges are removed from our original graph, so our new graph has at least $|A||B|/(2K)$ edges. Futher, $|\acute{A}| \geq |A|/(2K)$.

We take $\epsilon = 1/(32K)$ in Lemma 2.28, and thus find a subset A' of $\acute{A}$ with $|A'| \geq |A|/(2\sqrt{2}K)$ such that for a proportion $1 - 1/(32K)$ of the pairs $(a_1, a_2) \in A' \times A'$

we have at least $|B|/(256K^3)$ paths of length 2 connecting a_1 and a_2. It follows that for at most half of values $a_1 \in A'$ can there exist more than $1/(16K)$ of values $a_2 \in A'$ with (a_1, a_2) not connected by many paths of length 2. Taking A'' to be the good half of A' we get the lemma. □

Lemma 2.30. *Let G be a bipartite graph as above having an edge set of size $|A||B|/K$. We may find subsets A' and B' of A and B with $|A'| \geq |A|/(4\sqrt{2}K)$ and $|B'| \leq |B|/(4K)$ such that for any $a \in A'$ and $b \in B'$ there exists $\geq |A||B|/(2^{15}K^5)$ paths of length three joining a and b.*

Proof. We take A' to be the set A'' extracted in Lemma 2.29. We now find the set B'. We will take B' to be the set of vertices adjacent to at least $|A'|/(8K)$ elements from A'. We note that the number of edges connecting A' to B is at least $|A'||B|/(2K)$. Therefore at least $|B|/(4K)$ of the vertices in B must be connected to $|A'|/(8L)$ vertices in A'. That is, $|B'| \geq |B|/(4K)$. If $a \in A'$ and $b \in B^prime$ then we have at least $|A'|/(8K)$ vertices in A' that are adjacent to b, and at most $|A'|/(16K)$ of these can have the property that there are few paths of length two connecting them to a. Thus there are at least $|A'|/(16K)$ vertices a_2 that are both adjacent to b, and have at least $|B|/(256K^3)$ paths of length two connecting a and a_2. Thus there are at least $|A||B|/(2^{15}K^5)$ paths of length three connecting a and b. □

Now we are in a position to prove Theorem 2.27.

Proof. By Lemma 2.30 we may extract large sets A' and B' with at least $\frac{|A||B|}{(2^{15}K^5)}$ paths of length 3 connecting any two elements in these sets. Thus given a and b in A' and B', we can find more than $|A||B|/(2^{15}K^5)$ bais b_1 and a_2 in B and A with $(a, b_1), (a_2, b_1), (a_2, b)$ all being edges in ou graph G. That is $a + b_1 = x, a_2 + b_1 = y$ and $a_2 + b = z$ are all elements in $A +_G B$. Now we note that

$$a + b = a + b_1 - (b_1 + a_2) + a_2 + b = x - y + z.$$

We know lots of solutions to this equation with x, y and z in $A +_G B$. But the total number of choices for x, y and z is at most $|A +_G B|^3 \leq K_1^3|A|^3$. Therefore the number of distinct possibilites for $a + b$ is at most

$$\frac{K_1^3|A|^3}{|A|^2/(2^{15}K^5)} = 2^{15}K^5K_1^3|A|.$$

Thus our proof is completed. □

3. Analytic Number Theory

3.1. **Introduction.** In this section we shall give a very brief introduction to the circle method in analytic number theory. The method had its genesis in a paper by G. H. Hardy and S. Ramanujan in the late 1910's dealing with the partition function. Later Hardy and Littlewood used this method in a variety of situations and hence it is sometimes also referred to as the Hardy-Littlewood method. The method has been used quite successfully in a variety of situations and is a very important tool in modern number theory. First we state and prove a simple result which shall be used in our study.

Theorem 3.1. $\int_0^1 e(n\alpha)d\alpha = \begin{cases} 1 \text{ if } n = 0 \\ 0 \text{ if } n \neq 0 \end{cases}$ *, for some α.*

Proof. This immediately follows from the fact that the complex valued function $e(x)$ is periodic modulo 1 and that the integral of the sin and cos functions over a full period is zero. □

The name of the method is reflected from the fact that the integral is over the unit circle, if we consider it on the complex plane. This analytic method was mainly developed by Hardy and Littlewood to tackle problems of the additive nature in number theory, like the representation of a large number as a sum of numbers of a specific kind. The most famous additive problem to which this method has been applied successfully is what is called the *Waring's problem*. The problem is that of representing a large number N as

$$N = x_1^k + x_2^k + \cdots + x_s^k, \tag{3.1}$$

where s and l are given and $x_1, x_2, \ldots, x_s$'s are positive integers.

This method was later on developed further by the Russian mathematician Vinogradov. The method itself has its genesis in a paper by Hardy and Ramanujan in 1917 as mentioned above on the asymptotic behaviour of $p(n)$, the total number of partitions of n. The function $p(n)$ increases like $e^{A\sqrt{n}}$, where A is a certain positive constant; and Hardy and Ramanujan obtained for it an asymptotic expansion which if one stops at the smallest term, gives $p(n)$ with an error. This was developed further by Rademacher in 1937. The method is not restricted to Diophantine equations like (3.1) only, it can be extended to various other situations.

3.2. **Weyl's Inequality.** The most important tool required in the investigation of Waring's problem and many other problems in number theory is Weyl's inequality, given by Weyl in 1916. This was given by Weyl in a less explicit form on the unifrom distribution of sequences of numbers to the modulus 1. Hardy and Littlewood later gave it in an explicit form for a polynomial, in terms of a rational approximation to the highest coefficient.

Theorem 3.2 (Weyl)**.** *Let $f(x)$ be a real polynomial of degree k with highest coefficient α:*

$$f(x) = \alpha x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k.$$

Suppose that α has a rational approximation a/q satisfying

$$(a, q) = 1, q > 0, |\alpha - \frac{a}{q}| \leq \frac{1}{q^2}.$$

Then, for any $\epsilon > 0$, we have

$$|\sum_{x=1}^{P} e(f(x))| \ll P^{1+\epsilon}(P^{-\frac{1}{K}} + q^{-\frac{1}{K}} + (\frac{P^k}{q})^{-\frac{1}{K}}),$$

where $K = 2^{k-1}$ and the implied constants depends only on k and ϵ.

Proof. Let

$$S_k(f) = \sum_{x=P_1+1}^{P_2} e(f(x)),$$

where $0 \leq P_2 - P_1 \leq P$, and where the suffix k indicates the degree of $f(x)$. Then we have,

$$|S_k(f)|^2 = \sum_{x_1} \sum_{x_2} e(f(x_2) - f(x_1)) = P_2 - P_1 + 2\mathcal{R} \sum_{x_1, x_2 x_2 > x_1} e(f(x_2) - f(x_1)).$$

We now put $x_2 = x_1 + y$, then $1 \leq y \leq P_2 - P_1$, and

$$f(x_2) - f(x_1) = f(x_1 + y) - f(x_1) = \Delta_y f(x_1).$$

Hence

$$|S_k(f)|^2 = P_2 - P_1 + 2\mathcal{R} \sum_{y=1}^{P} \sum_{x} e(\Delta_y f(x)),$$

where the summation in x is over an interval depending on y, but contained in $P_1 < x \leq P_2$. This interval may, for some values of y, be empty.

In particular,

$$|S_k(f)|^2 \leq P + 2 \sum_{y=1}^{P} |S_{k-1}(\Delta_y f)|,$$

where the interval S_{k-1} is of the nature just described. By repeating this process we get,

$$|S_{k-1}(\Delta_y f)|^2 \leq P + 2 \sum_{x=1}^{P} |S_{k-2}(\Delta_{y,z} f)|,$$

where the interval of summation in S_{k-2} depends on both y and z but is contained in $P_1 < x \leq P_2$. With the use of Cauchy-Schwarz inequality in the above two expressions we get,

$$|S_k(f)|^4 \ll P^2 + P \sum_{y=1}^{P} |S_{k-1}(\Delta_y f)|^2$$

$$\ll P^3 + P \sum_{y=1}^{P} \sum_{z=1}^{P} |S_{k-2}(\Delta_{y,z} f)|.$$

This process can be continued and finally we shall get,

$$|S_k(f)|^{2^v} \ll P^{2^v - 1} + P^{2^v - v - 1} \sum_{y_1=1}^{P} \cdots \sum_{y_v=1}^{P} |S_{k-v}(\Delta_{y_1,\ldots,y_v} f)|. \tag{3.2}$$

The above is obtained by using induction on v and using Cauchy-Schwarz inequality together with the basic operation described above which expresses $|S_{k-v}|^2$ in terms of S_{k-v-1}. The range of summation for x in S_{k-v} in (3.2) is an interval depending on $y_1, \ldots, y_v$, but contained in $P_1 < x \leq P_2$.

We take $v = k - 1$ and in the original S_k we take $P_1 = 0, P_2 = P$. We observe that

$$\Delta_{y_1,\ldots,y_{k-1}} f(x) = k! \alpha y_1 \ldots y_{k-1} x + \beta,$$

where β is the collection of terms independent of x. Hence we have,

$$|S_1(\Delta_{y_1,\ldots,y_{k-1}} f(x)| = |\sum_{x} e(k! \alpha y_1 \ldots y_{k-1} x)|.$$

The sum on the right, taken over any inteval of x of length at most P, may be of the form

$$|\sum_{x=x_1}^{x_2 - 1} e(\lambda x)| \leq \frac{2}{1 - e(\lambda)} = \frac{1}{|\sin \pi \lambda|} \ll \frac{1}{||\lambda||},$$

This fails if λ is an integer, and indeed gives a poor result if λ is very near to an integer, but we can supplement it by the upper bound P. Thus, (3.2) gives

$$|S_k(f)|^K \ll P^{K-1} + P^{K-k} \sum_{y_1=1}^{P} \cdots \sum_{y_{k-1}=1}^{P} min(P, ||k!\alpha y_1 \cdots y_{k-1}||^{-1}).$$

We shall now use a result from elementary number theory which will allow us to collect together all the terms in the sum for which $k!y_1 \cdots y_{k-1}$ has a given value, say m. The number of such terms is $\ll m^{\epsilon}$. To prove this, it is sufficient to show that,

$$d(m) \ll m^{\epsilon}, \tag{3.3}$$

for any integer m, where $d(m) = \sum_{d|m} 1$ is the divisor function. There are at most $d(m)$ possibilites for each of $y_1, \ldots, y_{k-1}$. To prove (3.3) we let $m = p_1^{\lambda_1} p_2^{\lambda_2} \cdots$, and we note that

$$\frac{d(m)}{m^{\epsilon}} = \prod_i \frac{\lambda_i + 1}{p_i^{\epsilon\lambda_i}} \leq \prod_{p_i \leq 2^{1/\epsilon}} \frac{\lambda_i + 1}{2^{\epsilon\lambda_i}} \leq C(\epsilon),$$

since $2^{-\epsilon\lambda}(\lambda + 1)$ is bounded above for $\lambda > 0$.

Collecting the terms as mentioned above, we get

$$|S_k(f)|^K \ll P^{K-1} + P^{K-k-\epsilon} \sum_{m=1}^{k!P^{k-1}} min(P, ||\alpha m||^{-1}).$$

It now remains to estimate the last sum of the rational approximation a/q to α. We divide the sum over m into blocks of q consecutive terms, the numbers of such blocks being

$$\ll \frac{P^{k-1}}{q} + 1.$$

We now consider the sum over any one block, which will be of the form

$$\sum_{m=0}^{q-1} min(P, ||\alpha(m_1 + m)||^{-1}),$$

, where m_1 is the first number in the block. We have

$$\alpha(m_1 + m) = \alpha m_1 + \frac{am}{q} + O(\frac{1}{q}),$$

since $|\alpha - a/q| \leq q^{-2}$ and $0 \leq m < q$. As m goes from 0 to $q - 1$, the number am runs through the complete set of residues modulo q. We put $am \equiv r \ (mod\ Q)$ and the then the sum is,

$$\sum_{r=0}^{q-1} min(P, \frac{1}{||(r + b)/q + O(1/q)||}),$$

where we have taken b to be the integer nearest to $q\alpha m_1$. There are $O(1)$ values of r in the sum for which the second expression in the minimum is of no use, namely those for which the absolutely least residue of $r + b \ (mod\ q)$ is small. For these, we must take P. For the other values of r, if s denotes the absolutely least residue of $r + b \ (mod\ q)$ we have

$$||\frac{r + b}{q} + O(\frac{1}{q})|| \gg \frac{s}{q}.$$

Hence the above sum is

$$+\sum_{s=1}^{q/2}\frac{q}{s} \ll P + q\log q.$$

Allowing for the number of blocks, we have

$$|S_k(f)|^{K\,K-1} + P^{K-k-}(\frac{P^{k-1}}{q}+1)(P+q\log q).$$

We can now absorb the factor $\log q$ in P, since we can suppose $q \leq P^k$, else the result of the theorem is trivial. Thus the RHS is

$$\ll P^{K+}(P^{-1}+q^{-1}+P^{-k}q),$$

proving the theore.

□

Remark 3.3. *The inequality in Weyl's inequality gives some improvement over the trivial upper bound P provided that $P^{\delta} \leq q \leq P^{k-\delta}$ for some fixed $\delta > 0$. If $P \leq q \leq P^{k-1}$, we get the estimate $P^{1-1/k+\epsilon}$, and it is under these condition that Weyl's inequality is most commonly applied. It is obviously impossible to extarct any better estimate than this from it. We note that Weyls' inequality fails to give any useful information if q is small, and this is natural because if $f(x) = \alpha x^k$ and α is very near to a rational number with small denominator, the sum is of a size which approaches P.*

Remark 3.4. *If, we apply the basic operation in its original form at the last stage of the proof of* (3.2)*, we get*

$$|S_k(f)|^{2^v} \ll P^{2^v-1} + P^{2^v-v-1}\sum_{y_1=1}^{P}\cdots\sum_{y_v=1}^{P}\mathcal{R}S_{k-v}(\Delta_{y_1,\ldots,y_v}f). \tag{3.4}$$

Here again, the range for x in S_{k-v} depends on $y_1,\ldots,y_v$ and may sometimes be empty.

Remark 3.5. *If k is large, then Vinogradov has given a much better estimate, in which 2^{k-1} is replaced by $4k^2\log k$.*

Corollary 3.6. *Let*

$$S_{a,q} = \sum_{z=1}^{q} e(az^k/q),$$

where $(a,q) = 1$ are integers and $q > 0$. Then

$$S_{a,q} \ll q^{1-1/K+}.$$

Proof. This is a special case of the theorem just proved with $\alpha = a/q$ and $P = q$. □

3.3. **Hua's Inequality.**

Theorem 3.7 (Hua)**.** *If*

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k),$$

then

$$\int_0^1 |T(\alpha)|^{2^k}\,d\alpha \ll P^{2^k-k+}$$

for any fixed > 0.

Proof. We write

$$I_v = \int_0^1 |T(\alpha)|^{2^v} d\alpha.$$

We now prove, by induction on v, that

$$I_v \ll P^{2^v - v +}, \ for\ v = 1, \dots, k, \tag{3.5}$$

the case $v = k$ being the theorem.

For $v = 1$, the hypothesis is correct. We have,

$$I_1 = \int_0^1 \sum_{x_1} e(\alpha x_i^k) \sum_{x_2} e(-\alpha x_2^k) d\alpha = P,$$

since the integral over α is 1 if $x_1 = x_2$ and 0 otherwise.

We suppose that (3.5) holds for a particular integer $v \le k-1$; we have to deduce that the corresponding result when v is replaced by $v+1$ holds. Using $T(\alpha)$ in place of $S_k(f)$ in (3.4) we have

$$|T(\alpha)|^{2^v} \ll P^{2^v - 1} + P^{2^v - v +} \mathcal{R} \sum_{y_1=1}^{P} \cdots \sum_{y_v=1}^{P} S_{k-v},$$

where

$$S_{k-v} = \sum_x e(\alpha \Delta_{y_1,\dots,y_v}(x^k)).$$

We note that the range of summation for x depends on the values of $y_1, \dots, y_v$, but is contained in $[1, P]$.

We multiply both sides of the inequality by $|T(\alpha)|^{2^v}$ and integrate from 0 to 1. We get,

$$I_{v+1} \ll P^{2^v - 1} I_v + P^{2^v - v - 1} \sum_{y_1,\dots,y_v} \mathcal{R} \int_0^1 S_{k-v} |T|^{2^v} d\alpha.$$

The last integral is

$$\int_0^1 \sum_x e(\alpha \Delta_{y_1,\dots,v}(x^k)) \sum_{u_1,\dots,u_{2^v-1} w_1,\dots,w_{2^v-1}} e(\alpha u_1^k + \cdots) e(-\alpha w_1^k + \cdots) d\alpha,$$

where the u_i and w_i go from 1 to P. This integral equals the number of solutions of

$$\Delta_{y_1,\dots,y_v}(x^k) + u_1^k + \cdots - w_1^k - \cdots = 0. \tag{3.6}$$

Summations over $y_1, \dots, y_v$ gives the number of solutions in all the variables. Hence,

$$I_{v+1} \ll P^{2^v - 1} I_v + P^{2^v - v - 1} N, \tag{3.7}$$

where N denotes the number of solutions of (3.6) in all the variables, these being now any integer in $[1, P]$.

We observe that since $y_1, \dots, y_v$ and x are positive, so

$$\Delta_{y_1,\dots,y_v}(x^k) > 0.$$

Also, this number is divisible by $y_1, \dots, y_v$. Thus, if we give u_i and w_i any values, the number of possiblities for each of y_i is $\ll P$ by (3.3). Then there is at most one possibility for x, since $\Delta_{y_1,\dots,y_v}(x^k)$ is a strictly increasing function of x. The number of possibilites for the u_i and w_i is
P^{2v}, thus it follows that

$$N \ll P^{2^v + v}.$$

Substituting this in (3.7) and using the induction hypothesis we have

$$I_{v+1} \ll P^{2^v-1}P^{2^v-v+} + P^{2^v-v-1}P^{2^v+v2^v+1-(v+1)_v}.$$

This is (3.5) with $v+1$ for v except for the change in which is of no significance.

Thus the result is proved. □

Acknowledgements. I would like to thank my guide Prof. R. Balasubramanian (IMSc, Chennai) for his immense help and guidance. He has been an inspiration and support in my learning. I would also like to thank the excellent facilities provided to me by The Institute of Mathematical Sciences (IMSc), Chennai during my stay here. My thanks also goes to Dr. Anirban Mukhopadhyay, Dr. Sanoli Gun, Dr. Debajit Kalita, Dr. Rajib Haloi, Sumit Giri, Ankush Goswami and Krittika Singhal for helping me in various ways.

References

[1] A. Balog; *Additive Combinatorics*, Lecture Notes, The Institute of Mathematical Sciences (2011).
[2] H. Davenport; *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, Second edition, Cambridge University Press (2005).
[3] T. Gowers; *A new way of proving sumset estimates*, http://www.gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/ (2011).
[4] K. Soundararajan; *Additive Combinatorics*, Lecture Notes, Stanford University (2007).
[5] T. Tao, V. H. Vu; *Additive Combinatorics*, Cambridge Studies in advanced mathematics, 105 (2006).
[6] R. C. Vaughan; *The Hardy-Littlewood method*, Second edition, Cambridge Tracts in Mathematics, 125 (1997).

Manjil P. Saikia[1]
Department of Mathematical Sciences, Tezpur University, Napaam, Assam, Pin 784028, India
Tel. +91-80119-02141
E-mail address: manjil_msi09@agnee.tezu.ernet.in, manjil@gonitsora.com

[1]Visiting Student, The Institute of Mathematical Sciences, Chennai, Pin 600113, India
E-mail address: manjilps@imsc.res.in