ADDITIVE ENERGY OF DENSE SETS OF PRIMES AND MONOCHROMATIC SUMS

D S Ramana, Olivier Ramaré

ADDITIVE ENERGY OF DENSE SETS OF PRIMES AND MONOCHROMATIC SUMS

D.S. RAMANA AND O. RAMARÉ

Abstract. When $K \geq 1$ is an integer and S is a set of prime numbers in the interval $(\frac{N}{2}, N]$ with $|S| \geq \pi^*(N)/K$, where $\pi^*(N)$ is the number of primes in this interval, we obtain an upper bound for the additive energy of S, which is the number of quadruples (x_1, x_2, x_3, x_4) in S^4 satisfying $x_1 + x_2 = x_3 + x_4$. We obtain this bound by a variant of a method of Ramaré and I. Ruzsa. Taken together with an argument due to N. Hegyvári and F. Hennecart this bound implies that when the sequence of prime numbers is coloured with K colours, every sufficiently large integer can be written as a sum of no more than $CK \log\log 4K$ prime numbers, all of the same colour, where C is an absolute constant. This assertion is optimal upto the value of C and answers a question of A. Sárközy.

1. Introduction

A consequence of Vinogradov's classical three primes theorem is the assertion that every sufficiently large integer may be expressed as a sum of no more than four prime numbers. Following A. Sárközy [8] one may ask for a monochromatic version of this assertion. More precisely, let $\mathcal{P}$ denote the sequence of prime numbers and suppose that for an integer $K \geq 1$, $\mathcal{P} = \cup_{1 \leq i \leq K} \mathcal{P}_i$ is a partition of the sequence of prime numbers into K subsequences $\mathcal{P}_i$. Then the problem is to determine upper bounds in terms of K for the smallest integer $t(K)$ with the property that for each sufficiently large integer n there is an i, $1 \leq i \leq K$, such that n can be expressed as a sum of no more than $t(K)$ prime numbers all belonging to $\mathcal{P}_i$. Indeed, Sárközy remarks on page 29 of [8] that it is easily seen that there exists an integer analogous to $t(K)$ in the corresponding question for the sequence of squares and poses the problem of finding upper bounds, in terms of K, for this integer and for $t(K)$.

In [4], N. Hegyvári and F. Hennecart devised an essentially elementary method for attacking the problem of Sárközy for both the sequence of squares and the sequence of prime numbers. Applying their method to the sequence of prime numbers, they obtained the bound $t(K) \leq 1500K^3$. The method of [4] for this bound relies on an averaged form of the inequality

$$|2A|\, E(A) \geq |A|^4\,, \tag{1.1}$$

2010 *Mathematics Subject Classification.* Primary 11N36; Secondary 11P99.

Key words and phrases. additive energy, monochromatic sums of primes, large sieve.

where A is any finite subset of the integers, $2A$ denotes the set of integers of the form $x_1 + x_2$ with $(x_1, x_2) \in A^2$, and $E(A)$, the additive energy of A, is the number of quadruples $(x_1, x_2, x_3, x_4) \in A^4$ satisfying the relation $x_1 + x_2 = x_3 + x_4$. We recall here that the inequality (1.1) results on noting that $\sum_n r_A(n) = |A|^2$, where $r_A(n)$ is the number of pairs $(x_1, x_2) \in A^2$ such that $n = x_1 + x_2$, for any integer n, and using the Cauchy-Schwarz inequality.

Let us now summarize the method of Hegyvári and Hennecart [4] for their bound for $t(K)$. Thus let N be an integer and let P be the set of all primes in the interval $(\frac{N}{2}, N]$. Further, for each i, let P_i denote the set of terms of $\mathcal{P}_i$ contained this interval. Then the sets P_i are a partition of P. On applying (1.1) to each P_i and adding the resulting inequalities we have

$$\max_i |2P_i| \ \geq \ \frac{\sum_i |P_i|^4}{\sum_i E(P_i)} \ \geq \ \frac{|P|^4}{K^3\, E(P)} \ , \tag{1.2}$$

where the last inequality results from applying Hölder's inequality in the form $K^3 \sum_i |P_i|^4 \geq |P|^4$ and using the trivial bound $E(P) \geq \sum_i E(P_i)$. Hegyvári and Hennecart then observe that by a well-known application of the circle method we have $E(P) \leq \frac{N^3}{5(\log N)^4}$. Taken together with (1.2) and the bound $|P| \geq \frac{N}{20^{1/4} \log N}$, obtained from the Prime Number Theorem, this implies that for each sufficiently large integer N there is an i such that

$$|2P_i| \ \geq \ \frac{N}{4K^3} \ . \tag{1.3}$$

In other words, there is an i such that $P_i + P_i$ is a set of density at least $1/4K^3$ in the interval $(N, 2N]$. A finite analogue of Kneser's theorem, again due to A. Sárközy, now shows that there is an integer h not exceeding $500K^3$ such that for each sufficiently large N there is an i such that $2hP_i$ contains an arithmetical progression of length N to a modulus bounded in terms of K. Hegyvári and Hennecart then elegantly combine this conclusion with the fact that P_i comprises prime numbers to deduce the stated upper bound for $t(K)$.

In the present article we replace the averaging argument expressed by (1.2) with the simple observation that there exists an i such that $|P_i| \geq \pi^*(N)/K$, where $\pi^*(N) = |P|$ is the number of prime numbers in $(\frac{N}{2}, N]$. For such a subset P_i of the primes in $(\frac{N}{2}, N]$ we shall prove the upper bound for its additive energy given by the following theorem, which is our principal conclusion.

Theorem 1.1. *Given an integer $K \geq 1$ there is an integer $N(K)$ such that such that for all $N \geq N(K)$ and any subset S of the prime numbers in the interval $(\frac{N}{2}, N]$ with $|S| \geq \pi^*(N)/K$ we have*

$$E(S) \ \leq \ \frac{M}{\phi(M)} \frac{|S|^3}{\log\left(\frac{N}{2}\right)} \exp\left(\frac{16}{\log\log 4K}\right) \ , \tag{1.4}$$

where we have denoted by M the product of all prime numbers not exceeding $(4\log 4K \log\log 4K)^2$.

By Merten's theorem we have $\frac{M}{\phi(M)} \sim 2e^{\gamma}\log\log K$ when $K \to +\infty$. It then follows from Theorem 1.1 that there is an absolute constant C such that for a given $K \geq 1$ and all $N \geq N(K)$ and any subset S of the prime numbers in the interval $(\frac{N}{2}, N]$ with $|S| \geq \pi^*(N)/K$ we have the bound

$$E(S) \ \leq \ \frac{C|S|^3}{4\log N} \log\log 4K \ . \tag{1.5}$$

Applying (1.1) and (1.5) to P_i we see that for any $K \geq 1$ and all sufficiently large N we have

$$|2P_i| \ \geq \frac{4|P_i|\log N}{C\log\log 4K} \ \geq \ \frac{N}{CK\log\log 4K} \ , \tag{1.6}$$

since $\pi^*(N) \geq N/4\log N$ for all sufficiently large N, by the Prime Number Theorem. With (1.3) replaced by (1.6), and arguing as on pages 321 and 322 of [4] using the finite analogue of Kneser's theorem mentioned above, we obtain the following theorem. For the sake of completeness, we provide the details of this argument, in a form adequate for our purpose, at the end of Section 3.

Theorem 1.2. *Let $K \geq 1$ be an integer and let $\mathcal{P} = \cup_{1\leq i\leq K}\mathcal{P}_i$ be a partition of the sequence of prime numbers $\mathcal{P}$ into K subsequences $\mathcal{P}_i$. Then for each sufficiently large integer n there is an i such that n can be expressed as a sum of no more than $1700CK\log\log 4K$ terms of $\mathcal{P}_i$.*

In other words, we have $t(K) \leq 1700CK\log\log 4K$. This bound is optimal up to the value of C, as shown by the example on page 322 of [4], which depends on considering the partition of the primes induced by congruence classes to a modulus M of the shape $\prod_{p\leq L} p$ for an integer $L \geq 1$. In the light of this example it is interesting to compare the upper bound for $E(S)$ given by Theorem 1.1 with the asymptotic formula for $E(S)$ obtained from the circle method when S is the set of all primes in $(\frac{N}{2}, N]$ lying in a given congruence class modulo such an M. Indeed, on making the necessary modifications to the method of [1] we obtain for such S the asymptotic formula

$$E(S) \sim \frac{M}{\phi(M)^4} \prod_{p>L}\left(1 + \frac{1}{(p-1)^3}\right) \frac{N^3}{12\,(\log N)^4} \tag{1.7}$$

as N tends to $+\infty$. By the Prime Number Theorem for arithmetical progressions we have that $|S| \sim \pi^*(N)/K$ as N tends to $+\infty$, where we have

set $K = \phi(M)$. On noting that $L \sim \log M \sim \log K$, rearranging terms in (1.7) and using Merten's formula we conclude that

$$E(S) \sim \frac{2}{3}\, e^{\gamma} \frac{|S|^3}{\log N} \log\log K\ , \tag{1.8}$$

when L and N tend to $+\infty$. On the other hand, Theorem 1.1 and Merten's formula give, for any set primes S in $(\frac{N}{2}, N]$ with $|S| \geq \pi^*(N)/K$, the bound

$$E(S) \leq (2+\epsilon)\, e^{\gamma} \frac{|S|^3}{\log N} \log\log K\ , \tag{1.9}$$

for any $\epsilon > 0$ and all K and N sufficiently large. In particular, we see that Theorem 1.1 is optimal in its dependence on K and N when these parameters tend to $+\infty$. We do not know if the $2+\epsilon$ in (1.9) may be replaced with $\frac{2}{3}+\epsilon$, which, on account of (1.8), would suggest the intutively appealing conclusion that $E(S)$ is essentially the largest possible when S is a set of primes in an arithmetical progression.

Independently of the problem of bounding $t(K)$, Ramaré and I. Ruzsa [6] studied the question of representing all sufficiently large integers as the sum of the terms of a dense subsequence of a sufficiently sifted sequence. The fundamental example of a sufficiently sifted sequence is the sequence $\mathcal{P}$ of prime numbers. Yet, as noted by Hegyvári and Hennecart on page of 315 of [4], the main result of Ramaré and Ruzsa is not applicable to the problem of bounding $t(K)$ since none of the $\mathcal{P}_i$ may be a dense subsequence of $\mathcal{P}$. Nevertheless, and in consonance with the remarks of B. J. Green in the review [2] of [4], the *method* of [6] may well be adapted to treat this problem. It is in fact possible to obtain an inequality of the shape (1.9) by the method of [6], although with the $2+\epsilon$ replaced with a constant that is at least $16+\epsilon$, on account of essential restrictions on certain parameters in [6]. For this reason, we prove Theorem 1.1 here by an alternate method which at first proceeds in the manner of the proof of Vinogradov's three primes theorem presented in Chapter 10 of the book [7] and then draws on key devices from the method of Ramaré and Ruzsa. Moreover, the present method also appears to have the advantage of being much simpler in its details than the method of [6].

Let us then sketch the proof of Theorem 1.1, deferring the details to Section 3. We begin by remarking that the proof of Theorem 1.1 reduces to the majorisation of the sum

$$\sum_{(x_1,x_2,x_3)\in S^3} \Lambda(x_1+x_2-x_3)\ , \tag{1.10}$$

where $\Lambda(n)$ is the Van Mangoldt function. We estimate this sum with the aid of the sieve identity for $\Lambda(n)$ given by the relation

$$\Lambda(n) = -\sum_{d|n} \mu(d)\log d = -\sum_{\substack{d|n,\\ d\le L.}} \mu(d)\log d - \sum_{\substack{d|n,\\ d>L.}} \mu(d)\log d \tag{1.11}$$

for any $L \geq 2$. With $L = N^{1/2}$, we substitute (1.11) into (1.10) and obtain two sums, one over $d \leq L$ and the other over $d > L$. We first show that the sum over $d > L$ is majorised by the right hand side of (1.4). This step is a standard application of Davenport's classical bound for $\sum_n \mu(n)e(nt)$. Following this, we use properties of the arithmetical function $\omega(q, L)$ defined for integers $q, L \geq 1$ by

$$\omega(q, L) \;=\; -\sum_{\substack{1\le l\le L,\\ l\equiv 0 \bmod q.}} \frac{\mu(l)\log l}{l} \tag{1.12}$$

to show that the majorisation of the sum over $d \leq L$ amounts to that of

$$\sum_{1\le q\le (\log N)^4} \frac{\mu(q)}{\phi(q)} \sum_{a \bmod^* q} \sum_{(x_1,x_2,x_3)\in S^3} e\left(\frac{a(x_1+x_2-x_3)}{q}\right) . \tag{1.13}$$

Let us remark here that required properties of $\omega(d, L)$, recalled in Subsection 2.1, are much simpler to establish than the corresponding ones for the Selberg sieve coefficients used in [6]. Finally, we treat the sum (1.13) by means of devices from the method of [6], recalled in Subsections (2.2) through (2.4) below.

Throughout this article AB will denote, for subsets A and B of a group, the set of all ab with a in A and b in B. When the group is commutative we will write $A + B$ in place of AB and write nA for $A + A + \ldots + A$, with n summands. On the other hand, $n.A$ will denote the set of all na, for a in A and n an integer. Finally, $e(z)$ denotes $e^{2\pi iz}$, for any complex number z, while $\exp(z)$ and e^z retain their usual meanings.

2. PRELIMINARIES

2.1 Bounds for $\omega(q, L)$.— Plainly, $\omega(q, L) \neq 0$ only when q is a squarefree integer, which we shall assume for the rest of this subsection. Then on writing $l = qk$ and rearranging terms in (1.12) we obtain

$$\omega(q, L) \;=\; -\frac{\mu(q)}{q} \sum_{\substack{1\le k\le L/q,\\ (k,q)=1.}} \frac{\mu(k)\log qk}{k} . \tag{2.1}$$

On applying the triangle inequality to (2.1) and ignoring the condition $(k, d) = 1$ we obtain, for all $q, L \geq 1$, the upper bound

$$|\omega(q, L)| \leq \frac{1}{q}(\log L)(1 + \log(L/q)) \leq \frac{(\log 2L)^2}{q} . \tag{2.2}$$

When $1 \le q \le L^{1/2}$ preceding bound may be refined to the asymptotic formula

$$\omega(q, L) = \frac{\mu(q)}{\phi(q)} + O\left(\frac{2^{\nu(q)} \log q}{q(\log L)^A}\right) \tag{2.3}$$

for any $A \ge 1$, where the implied constant in the O symbol depends only on A. In effect, let $P(s) = \prod_{p|q}(1 - p^{-s})$. Then the sum on the right hand side of (2.1) is a partial sum of the coefficients of the Dirichlet series for $f(s) \log q - f'(s)$ where $f(s) = \frac{1}{P(s+1)\zeta(s+1)}$. The asymptotic formula (2.3) results on applying Perron's formula as, for example, in Satz 3.1, page 376 of [5] to this function and arguing as in the proof of the prime number theorem with the aid of the bounds

$$\left|\frac{P'(s)}{P(s)}\right| \le 2\zeta(2\sigma) \log q \quad \text{and} \quad \left|\frac{1}{P(s)}\right| \le \zeta(2\sigma) 2^{\nu(q)} \ , \tag{2.4}$$

when $\sigma > 1/2$, where $\sigma = \mathrm{Re}(s)$ and $\nu(q)$ is the number of prime divisors of q.

2.2 An improved large sieve inequality for primes.— The following proposition is the same as Theorem 5.3 on page 43 of the book [7], which, in turn is deduced from Theorem 5 on page 571 of [6].

Proposition 2.1. *Let $N \ge 100$ be an integer and u_n be a finite sequence of complex numbers supported on integers all of whose prime factors exceed $N^{\frac{1}{2}}$. Then for any Q satisfying $1 \le Q \le N^{\frac{1}{2}}$ we have*

$$\sum_{1 \le q \le Q} \sum_{a \bmod^* q} \left| \sum_n u_n e\left(\frac{an}{q}\right) \right|^2 \le 7 \log Q \frac{N}{\log N} \sum_n |u_n|^2 \ . \tag{2.5}$$

Proposition 2.1 improves upon the bound supplied by the classical large sieve inequality by the factor $\log Q / \log N$. For Q much smaller than N this factor is significant and will allow us to save a crucial factor $\log N$ in the argument leading to the proof of Theorem 1.1.

2.3 A simple optimisation principle.— In this subsection we formalise the discussion following (5.13) on page 578 of [6].

Suppose that $n \ge 1$ is an integer and that c_{ij} for $1 \le i, j \le n$ are real numbers. Further, let P and T be positive real numbers and assume that the subset K of points $x = (x_1, x_2, \dots, x_n)$ in $\mathbf{R}^n$ satisfying the conditions

$$\sum_{1 \le i \le n} x_i = P \ \text{ and } \ 0 \le x_i \le T \ \text{ for all } i \ . \tag{2.6}$$

is not empty. Plainly, K is a non-empty, compact and convex subset of $\mathbf{R}^n$.

Proposition 2.2. *Let $f(x,y) = \sum_{1\le i,j\le n} c_{ij}x_iy_j$ from $\mathbf{R}^n \times \mathbf{R}^n$ to $\mathbf{R}$ be a bilinear form with real coefficients c_{ij}. Then there exist extreme points x^* and y^* of the convex set K such that $f(x,x) \le f(x^*,y^*)$ for all x in K.*

Proof.— Indeed, suppose that $f(x,y)$ attains its maximum on the compact set $K \times K$ at (z,w). Then the map $x \mapsto f(x,w)$ is linear and thus attains its maximum on the compact convex set K at an extreme point of K, say x^*. We must necessarily have $f(x^*,w) = f(z,w)$. Arguing similarly with the linear map $y \mapsto f(x^*,y)$ we obtain y^*, also an extreme point of K, such that $f(x^*,y^*) = f(x^*,w) = f(z,w)$. In particular, we have $f(x,x) \le f(z,w) = f(x^*,y^*)$ for all x in K.

To apply this proposition we will require a description of the extreme points of K, which we take up now. Let x be a point of K with two of its co-ordinates x_i and x_j with respect to the canonical basis $\{e_1, e_2, \dots, e_n\}$ of $\mathbf{R}^n$ lying in the interior of the interval $[0,T]$. If $y = x + \delta(e_i - e_j)$ and $z = x - \delta(e_i - e_j)$ then for all small enough δ distinct from 0, the points y and z lie in K but are distinct from x and satisfy $x = (y+z)/2$. Therefore x is not an extreme point of K. In other words, if x is an extreme point of K then, excepting at most one, all co-ordinates of x are equal to either 0 or T. Moreover, if k is the number of co-ordinates of x that are distinct from 0 then we have from (2.6) that k is determined by $kT \ge P \ge (k-1)T$.

2.4 Pairs of points with co-ordinates distinguished by translations.— Let G be the product of a finite family of finite groups $\{G_i\}_{i\in I}$ and A and B be non-empty subsets of G. Given a subset J of I and, for each $i \in J$, a subset Ω_i of G_i, we write Ω to denote the family $\{\Omega_i\}_{i\in J}$. Then the proposition below gives an upper bound for the number $\mathcal{T}_{J,\Omega}(A,B)$ of pairs (a,b) in $A \times B$ such that

$$a_i^{-1}b_i \notin \Omega_i \text{ for all } i \in J\ , \tag{2.7}$$

where a_i and b_i are the co-ordinates of index i of a and b.

Proposition 2.3. *Let A and B be non-empty subsets of $G = \prod_{i\in I} G_i$ as above and let Ω_i be a subset of G_i for all $i \in J$, a subset of I. Further, let us set*

$$L(A,B) = \log\left(\frac{|G|^2}{|A||B|}\right) \quad \text{and} \quad w_J(\Omega) = \sum_{i\in J} \frac{|\Omega_i||\Omega_i\Omega_i^{-1}|}{|G_i|^2}\ . \tag{2.8}$$

Then for any integer t satisfying $1 \le t \le \inf_{i\in J}\left(\frac{|G_i|}{|\Omega_i|}\right)^{\frac{1}{2}}$ we have that

$$\mathcal{T}_{J,\Omega}(A,B) \le |A||B| \exp\left(-\sum_{i\in J}\frac{|\Omega_i|}{|G_i|}\right)\exp\left(\frac{L(A,B)}{t} + tw_J(\Omega)\right)\ . \tag{2.9}$$

Proposition 2.3 is a generalisation of Theorem 3 on page 563 of [6] but follows easily by the same method as that given by Ramarè and Ruzsa for

Theorem 3 of [6]. Since, however, the presentation of this method in [6] contains an error (see Remark 2.4 below), we give here a complete proof of Proposition 2.3.

A word of caution on our notation in the proof below : for any a in G we will continue to write a_i for its component of index i, but a_j and a_k will denote components of tuples of elements of G !

Proof of Proposition 2.3.— Let us set, for each i in J and (a,b) in $G\times G$, $\epsilon_i(a,b)=1$ when $a_i^{-1}b_i\notin\Omega_i$ and to be 0 otherwise. Then we have that

(2.10)
$$\mathcal{T}_{J,\Omega}(A,B)=\sum_{b\in B}\sum_{a\in A}\prod_{i\in J}\epsilon_i(a,b)\le |B|^{1-\frac1t}\left(\sum_{b\in B}\left(\sum_{a\in A}\prod_{i\in J}\epsilon_i(a,b)\right)^t\right)^{\frac1t},$$

where we have applied Hölder's inequality to exponent t to the sum over $b\in B$ in the second term in (2.10). We replace the sum over $b\in B$ in the third term of (2.10) with the sum over $b\in G$, expand the summand and interchange summations to obtain

$$\mathcal{T}_{J,\Omega}(A,B)\le |B|^{1-\frac1t}\left(\sum_{(a_1,a_2,\dots,a_t)\in A^t}\sum_{b\in G}\prod_{i\in J}\prod_{1\le j\le t}\epsilon_i(a_j,b)\right)^{\frac1t}. \tag{2.11}$$

Let us endow G with the uniform probability measure. Then on remarking that for any $(a_1,a_2,\dots,a_t)\in A^t$ the random variables $b\mapsto\prod_{1\le j\le t}\epsilon_i(a_j,b)$, as i varies over J, are mutually independent we deduce that the right hand side of (2.11) is the same as

$$|B|\left(\frac{|G|}{|B|}\right)^{\frac1t}\left(\sum_{(a_1,a_2,\dots,a_t)\in A^t}\prod_{i\in J}\mathbb{E}\left(\prod_{1\le j\le t}\epsilon_i(a_j,b)\right)\right)^{\frac1t}, \tag{2.12}$$

where $\mathbb{E}$ denotes expectation over the variable b. To bound this expectation, we first set $\delta_i(a,b)=1-\epsilon_i(a,b)$ and apply the truncation inequality

$$\prod_{1\le j\le t}(1-\delta_i(a_j,b))\le 1-\sum_{1\le j\le t}\delta_i(a_j,b)+\sum_{1\le j<k\le t}\delta_i(a_j,b)\delta_i(a_k,b)\,. \tag{2.13}$$

For any a and a' in G and i in J we set $\gamma_i(a,a')$ to be 1 when $a_i\Omega_i$ meets $a_i'\Omega_i$ and to be 0 otherwise. Then we have

$$\mathbb{E}\left(\delta_i(a,b)\right)=\frac{|\Omega_i|}{|G_i|}\quad\text{and}\quad\mathbb{E}\left(\delta_i(a,b)\delta_i(a',b)\right)\le\frac{|\Omega_i|\gamma_i(a,a')}{|G_i|}\,. \tag{2.14}$$

Passing to expectation with respect to b in (2.13) and using (2.14) we then deduce for all i in J and any $(a_1,a_2,\dots,a_t)$ in A^t the bound

$$\mathbb{E}\left(\prod_{1\le j\le t}\epsilon_i(a_j,b)\right)\le 1-\frac{|\Omega_i|}{|G_i|}t+\frac{|\Omega_i|}{|G_i|}\sum_{1\le j<k\le t}\gamma_i(a_j,a_k). \tag{2.15}$$

Thus on using the inequality $1+x\le\exp(x)$, valid for all real x, for the right hand side of (2.15), substituting into the expression (2.12) and rearranging the terms we conclude that (2.12) does not exceed

$$|B|\exp\left(-\sum_{i\in J}\frac{|\Omega_i|}{|G_i|}\right)\left(\frac{|G|}{|B|}\right)^{\frac{1}{t}}\left(\sum_{(a_1,a_2,\dots,a_t)\in A^t}\prod_{1\le j<k\le t}\exp\left(\psi(a_j,a_k)\right)\right)^{\frac{1}{t}} \tag{2.16}$$

where we have set $\psi(a,a')=\sum_{i\in J}\frac{|\Omega_i|\gamma_i(a,a')}{|G_i|}$ for any a and a' in A. We now observe that the inequality of arithmetic and geometric means, in the form $x_1x_2\dots x_n\le(x_1^n+x_2^n+\dots+x_n^n)/n$, implies that

$$\prod_{1\le j<k\le t}\exp\left(\psi(a_j,a_k)\right)\le\frac{1}{\binom{t}{2}}\left(\sum_{1\le j<k\le t}\exp\left(\binom{t}{2}\psi(a_j,a_k)\right)\right) \tag{2.17}$$

With the aid of (2.17) together with the remark that a given pair (a,a') appears as (a_j,a_k) in $|A|^{t-2}\binom{t}{2}$ tuples $(a_1,a_2,\dots,a_t)$, and on recalling the definition of $\psi(a,a')$, we easily see that the sum over A^t in (2.16) does not exceed

$$|A|^{t-2}|G|\sum_{a'\in A}\mathbb{E}\left(\prod_{i\in J}\exp\left(\binom{t}{2}\frac{|\Omega_i|\gamma_i(a,a')}{|G_i|}\right)\right), \tag{2.18}$$

where the expectation is over the variable a.

For any a', the random variable $a\mapsto\gamma_i(a,a')$ takes only values 1 or 0. Moreover, it takes value 1 only when $a_i\in a_i'\Omega_i\Omega_i^{-1}$. Consequently, we have $\mathbb{E}(\gamma_i(a,a'))=|\Omega_i\Omega_i^{-1}|/|G_i|$ and

$$\mathbb{E}\left(\exp\left(\lambda\gamma_i(a,a')\right)\right)=1+\left(\exp(\lambda)-1\right)\mathbb{E}(\gamma_i(a,a'))\le\exp\left(\frac{2\lambda|\Omega_i\Omega_i^{-1}|}{|G_i|}\right) \tag{2.19}$$

for any λ in $[0,1/2]$, on noting that $1+x(\exp(\lambda)-1)\le\exp(2\lambda x)$ for such λ and all real x. Indeed, the mean value theorem gives $0\le\exp(\lambda)-1\le 2\lambda$ for λ in $[0,1/2]$, from which the stated inequality follows.

Let us set $\lambda=\binom{t}{2}|\Omega_i|/|G_i|$, which, by the hypothesis on t, is in $[0,1/2]$. The bound supplied by (2.19) applied with this λ then shows that

(2.20)
$$|A|^{t-2}|G| \sum_{a' \in A} \prod_{i \in J} \mathbb{E}\left(\exp\left(\binom{t}{2}\frac{\delta_i(a,a')}{|\Omega_i|}\right)\right) \le |A|^{t-1}|G| \exp\left(t^2 w_J(\Omega)\right) \ .$$

By independence, the product over $i \in J$ may be interchanged with taking expectation in (2.20). Therefore, the left hand side of (2.20) is the same as (2.18), which we have shown to be an upper bound for the sum over A^t in (2.16). On substituting the right hand side of (2.20) for this sum in (2.16) and recalling that (2.16) is an upper bound for the right hand side of (2.11), we obtain (2.9) after a rearrangement of terms.

Remark 2.4. The proof of Theorem 3 in [6] is correct up to the point corresponding to inequality in (2.19) above, which is inequality (2.10) in [6]. The error lies in the conclusion of the optimization argument that follows this point. It is asserted there that $xb^x + 1 - x \le b^{x^2}$, where $0 \le x \le 1$ and $b \ge 1$ and, in particular, that $(\exp(t/q) - 1)/q + 1 \le \exp(t/q^2)$ for all t positive and $q \ge 1$. These inequalities are false in general and in fact the argument in [6] verifies the opposite inequalities.

3. The Proofs

We first prove Theorem 1.1. Throughout the proof we let K be an integer that is at least 1. Also, we will assume, as we may, that N is sufficiently large, its actual size varying to suit our requirements at various stages of our argument. We begin by noting that $E(S)$ is majorised by the number of triples (x_1, x_2, x_3) in S^3 such that $x_1 + x_2 - x_3$ is a prime number exceeding $\frac{N}{2}$. Consequently, we have

$$E(S) \log\left(\frac{N}{2}\right) \le \sum_{(x_1,x_2,x_3) \in S^3} \Lambda(x_1 + x_2 - x_3) \ , \tag{3.1}$$

Let us estimate the sum on the right hand side of the above relation. We set $L = N^{1/2}$ and, following [3], we write $\Lambda(n) = \Lambda^\sharp(n) + \Lambda^\flat(n)$, where $\Lambda^\sharp(n)$ and $\Lambda^\flat(n)$ are, respectively, the sums over $d \le L$ and $d > L$, together with the sign, in (1.11). Substituting into (3.1) and writing $r(n)$, for any integer n, to be the number of triples (x_1, x_2, x_3) in S^3 such that $x_1 + x_2 - x_3 = n$, we have that

$$E(S) \log\left(\frac{N}{2}\right) \le \sum_n r(n)\Lambda^\sharp(n) + \sum_n r(n)\Lambda^\flat(n) \ . \tag{3.2}$$

Let us first dispose of the second sum on the right hand side of the above relation. Since $r(n) = 0$ for n outside the interval $[1, 2N]$, we have that

$$\sum_n r(n)\Lambda^\flat(n) \ = \ \int_0^1 \left(\sum_n r(n)e(-nt)\right)\left(\sum_{1 \le n \le 2N} \Lambda^\flat(n)e(nt)\right) dt \ , \tag{3.3}$$

by orthogonality of the functions $t \mapsto e(nt)$. On recalling the definition of $\Lambda^\flat(n)$ and setting $n = dk$, we easily see by an interchange of summation that

$$\sum_{1\le n\le 2N} \Lambda^\flat(n)e(nt) \;=\; -\sum_{1\le k<\frac{2N}{L}} \sum_{L<d\le\frac{2N}{k}} \mu(d)\log d\, e(dkt)\,. \tag{3.4}$$

For conciseness, let us write $T(u)$ to denote, for a given k and t, the sum $\sum_{1\le d\le u}\mu(d)e(dkt)$ for any $u \ge 1$. Then we have

$$\sum_{L<d\le\frac{2N}{k}} \mu(d)\log d\, e(dkt) = \int_L^{\frac{2N}{k}} \log u\; dT(u)\,. \tag{3.5}$$

Davenport's classical bound given, for example, by Theorem 13.10, page 348 of [3], tells us that for any $A \ge 0$ we have $T(u) \ll u(\log u)^{-A}$ for all $u \ge 2$, uniformly in k and t. In this bound the implied constant depends only on A. Thus, on integrating by parts and applying this bound with $A = 4$ we have

$$\int_L^{\frac{2N}{k}} \log u\; dT(u) \;\le\; 3\log(2N) \max_{L\le d\le\frac{2N}{k}} |T(u)| \ll \frac{N}{k(\log N)^3}\,, \tag{3.6}$$

on remarking that $\log u$ is an increasing function for $L < u \le \frac{2N}{k}$ and recalling that $L = N^{1/2}$. From (3.4) through (3.6) we then see that

$$\sum_{1\le n\le 2N} \Lambda^\flat(n)e(nt) \;\ll\; \frac{N}{(\log N)^3} \sum_{1\le n\le 2N} \frac{1}{k} \;\ll \frac{N}{(\log N)^2}\,, \tag{3.7}$$

for all t in $[0,1]$. From the definition of $r(n)$ it immediately follows that $\sum_n r(n)e(-nt) = |\widehat{S}(t)|^2\widehat{S}(-t)$, where $\widehat{S}(t) = \sum_{n\in S} e(nt)$. Consequently, we have from (3.3) and (3.7) that

$$\sum_n r(n)\Lambda^\flat(n) \;\ll\; \frac{N}{(\log N)^2}\int_0^1 |\widehat{S}(t)|^2|\widehat{S}(-t)|\,dt \;\ll\; \frac{N|S|^2}{(\log N)^2}\,, \tag{3.8}$$

where the last inequality follows on using the trivial bound $|\widehat{S}(-t)| \le |S|$ together with the Parseval relation. The implied constant in (3.8) is absolute.

We now turn to the first sum on the right hand side of (3.2). On recalling the definition of $\Lambda^\sharp(n)$ we obtain

$$\sum_n r(n)\Lambda^\sharp(n) = -\sum_{1\le d\le L} \mu(d)\log d \sum_{n\equiv 0 \bmod d} r(n)\,, \tag{3.9}$$

after an interchange of summations. We note that

(3.10)
$$\sum_{n\equiv 0 \bmod d} r(n) \;=\; \frac{1}{d}\sum_{a \bmod d}\sum_{n} r(n) e\left(\frac{an}{d}\right) \;=\; \frac{1}{d}\sum_{q|d}\sum_{a \bmod^* q}\sum_{n} r(n) e\left(\frac{an}{q}\right),$$

by orthogonality of characters on the group $\mathbf{Z}/d\mathbf{Z}$. On combining (3.10) with (3.9), interchanging summations and recalling the definition of $\omega(q, L)$ from (1.12) we deduce that

$$\sum_{n} r(n)\Lambda^\sharp(n) = \sum_{1\le q\le L} \omega(q,L) \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \widehat{S}\left(\frac{a}{q}\right). \tag{3.11}$$

Let us estimate the contribution to the sum on the right hand side of (3.11) from q satisfying $(\log N)^4 < q \le L$ by verifying that

$$\sum_{(\log N)^4<q\le L} \omega(q,L) \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \widehat{S}\left(\frac{a}{q}\right) \le \frac{2N|S|^2}{(\log N)^2}. \tag{3.12}$$

Indeed, on using the bound for $\omega(q, L)$ given by (2.2) together with the trivial bound $|\widehat{S}(a/q)| \le |S|$ we have that the absolute value of the left hand side of (3.12) does not exceed

$$\frac{(\log 2L)^2|S|}{(\log N)^4} \sum_{1\le q\le L}\sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \le \frac{(\log 2L)^2(N+L^2)|S|^2}{(\log N)^4}, \tag{3.13}$$

where we have extended the range of summation in the sum over q in (3.13) back to $1 \le q \le L$ and applied the classical large sieve inequality given, for example, by Theorem 7.28, page 178 of [3]. Since $L = N^{1/2}$, we have $\log 2L \le \log N$ for $N \ge 4$. Thus, (3.12) follows from (3.13).

Passing to the contribution to the sum on the right hand side of (3.11) from q in the range $1 \le q \le (\log N)^4$, let us set

$$T = \sum_{1\le q\le (\log N)^4} \omega(q,L) \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \widehat{S}\left(\frac{a}{q}\right), \tag{3.14}$$

and use the asymptotic formula for $\omega(q, L)$ given by (2.3), which is applicable since $L = N^{1/2}$ and $(\log N)^4 \le N^{1/2}$ for all sufficiently large N. In effect, on using the trivial bounds $|\widehat{S}(a/q)| \le |S|$ and $2^{\nu(q)} \log q \le \tau(q) \log q \le 4q$, for any $q \ge 1$ we have

$$\sum_{1\le q\le (\log N)^4} \frac{2^{\nu(q)}\log q}{q(\log L)^2} \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \left|\widehat{S}\left(\frac{a}{q}\right)\right| \le \frac{8N|S|^2}{(\log L)^2}, \tag{3.15}$$

by the classical large sieve inequality, as before. Consequently, on using (2.3) with $A = 2$ we obtain

$$T = \sum_{1\le q\le (\log N)^4} \frac{\mu(q)}{\phi(q)} \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \widehat{S}\left(\frac{a}{q}\right) + O\left(\frac{N|S|^2}{(\log N)^2}\right) \tag{3.16}$$

where the implied constant is absolute.

Let us set $a = 4^{11}K^2$ and write U to denote the product of all primes not exceeding a. Then for sufficiently large N, we have $U \le (\log N)^4$ and we set $T(U)$ to be the sum over q on the right hand side of (3.16) restricted to those q that divide U. Since all other q then satisfy $q > a$, we have by the triangle inequality applied to (3.16) that

$$|T - T(U)| \le |S| \sum_{a<q\le (\log N)^4} \frac{1}{\phi(q)} \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 + O\left(\frac{N|S|^2}{(\log N)^2}\right) . \tag{3.17}$$

We shall estimate the sum over q in the above relation by the improved large sieve inequality of Proposition 2.1. To this end, let us write h to denote the integer satisfying $2^h a \le (\log N)^4 \le 2^{h+1}a$. Then the sum over q in (3.17) does not exceed

$$\sum_{0\le n\le h} \sum_{2^n a<q\le 2^{n+1}a} \frac{1}{\phi(q)} \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \tag{3.18}$$

For any $q \ge 1$ we have the trivial bounds $q/\phi(q) \le \nu(q) + 1 \le 2\log 2q$. Thus on writing $E(u)$ to denote $\sum_{1\le q\le u}\sum_{a \bmod^* q} |\widehat{S}(a/q)|^2$ for any $u \ge 1$ and remarking that $t \mapsto (\log 2t)/t$ is monotonically decreasing for $t \ge a$, we see that the above sum is majorised by

$$2 \sum_{0\le n\le h} \frac{\log(2^{n+1}a)E(2^{n+1}a)}{2^n a} . \tag{3.19}$$

Since S is a set of primes in $(\frac{N}{2}, N]$ and since for all sufficiently large N we have $2(\log N)^4 \le N^{1/2}$, an application of Proposition 2.1 gives us the bound $E(u) \le 7N|S|\log u/\log N$ for all u with $1 \le u \le 2(\log N)^4$. Also, for any $n \ge 1$ we have $\log(2^n a) \le n \log 2a$, since $a \ge 1$. Substituting these bounds into (3.19) we deduce that

$$\sum_{a<q\le (\log N)^4} \frac{1}{\phi(q)} \sum_{a \bmod^* q} \left|\widehat{S}\left(\frac{a}{q}\right)\right|^2 \le \frac{28N|S|(\log 2a)^2}{a\log N} \sum_{n\ge 1} \frac{n^2}{2^n} . \tag{3.20}$$

Recalling that $a = 4^{11}K^2$ we see that $\log(2a) \le 12\log 4K$. Also, we have $\sum_{n\ge 1} \frac{n^2}{2^n} = 6$. We then conclude from (3.17) and (3.20) that

$$|T - T(U)| \le \frac{(\log 4K)^2 N|S|^2}{128K^2 \log N} + O\left(\frac{N|S|^2}{(\log N)^2}\right) , \tag{3.21}$$

Before commencing our final step in the proof of Theorem 1.1, which is to estimate $T(U)$, let us gather together the bounds obtained thus far. Indeed, on combining (3.21), (3.12) and (3.8), we conclude by an application of the triangle inequality that

$$\left| \sum_{(x_1,x_2,x_3)\in S^3} \Lambda(x_1+x_2-x_3) - T(U) \right| \leq \frac{(\log 4K)^2}{64K^2} \frac{N|S|^2}{\log N} \ . \tag{3.22}$$

for every $N \geq N(K)$, where $N(K)$ depends on K. To estimate $T(U)$ we begin by remarking that

$$T(U) = \frac{U}{\phi(U)} \left| \{(x_1,x_2,x_3) \in S^3 \,|\, (x_1+x_2-x_3, U) = 1\} \right| . \tag{3.23}$$

In effect, since U is a squarefree integer, we have for any integer $n \neq 0$ the identity

$$\sum_{q|U} \frac{\mu(q)}{\phi(q)} \sum_{a \bmod^* q} e\left(\frac{an}{q}\right) \ = \ \frac{U}{\phi(U)} \sum_{q|(U,n)} \mu(q) \ , \tag{3.24}$$

which is easily verified using classical properties of Ramanujan sums. Since by the Möbius inversion formula the right hand side of (3.24) is $U/\phi(U)$ when $(n,U)=1$ and is 0 otherwise, we have on recalling the definition of $T(U)$ that

$$T(U) = \sum_{q|U} \frac{\mu(q)}{\phi(q)} \sum_{a \bmod^* q} \sum_{n} r(n) e\left(\frac{an}{q}\right) \ = \ \frac{U}{\phi(U)} \sum_{(n,U)=1} r(n) \ , \tag{3.25}$$

where the last sum is nothing but the right hand side of (3.23).

For any integer z and any subset Z of the integers, let $\tilde{z}$ and $\tilde{Z}$ denote their canonical images in $\mathbf{Z}/U\mathbf{Z}$. Further, for any residue class a modulo U, let $m(a)$ be the number of elements of the set S that belong to this residue class. If D denotes $\frac{N}{\phi(U)\log N}$, we then have that

$$\sum_{a\in\tilde{S}} m(a) = |S| \ \text{ and } \ 0 \leq m(a) \leq D \tag{3.26}$$

for all sufficiently large N, where the upper bound for $m(a)$ follows from the prime number theorem for arithmetical progressions on recalling that S is a set of prime numbers in the interval $(\frac{N}{2}, N]$. Finally, for any integer z and residue classes a, b modulo U let us set $C_z(a,b)$ to be 1 when $a+b-\tilde{z}$ is invertible in $\mathbf{Z}/U\mathbf{Z}$ and to be 0 otherwise. Then (3.23) tells us that

$$T(U) = \frac{U}{\phi(U)} \sum_{z\in S} \sum_{(a,b)\in\tilde{S}^2} C_{\tilde{z}}(a,b)\, m(a)m(b) \ . \tag{3.27}$$

Let us bound the inner sum on the right hand side of (3.27) with the aid of the optimization principle given in Subsection 2.2. From the discussion in that subsection we then have that

$$\sum_{(a,b)\in\tilde{S}^2} C_{\tilde{z}}(a,b)\, m(a)m(b) \le \sum_{(a,b)\in\tilde{S}^2} C_{\tilde{z}}(a,b)\, x_a^* y_b^*\,, \tag{3.28}$$

for some x_a^* and y_b^*, with a and b varying over $\tilde{S}$, satisfying the following conditions. All the x_a^*, and similarly all the y_b^*, are either 0 or D excepting at most one, which must lie in $(0, D)$. Moreover, if A and B denote, respectively, the subsets of $\tilde{S}$ for which $x_a^* \neq 0$ and $y_b^* \neq 0$ then $|A|D \ge |S| \ge (|A|-1)D$ and the same inequalities hold with $|A|$ replaced by $|B|$.

By the Prime Number Theorem we have $|S| \ge N/4K\log N$ for sufficiently large N. Moreover, it is easily verified that $\phi(U) \ge 64K^2$. Therefore we have $|S|/D \ge \phi(U)/4K \ge 16K$ when N is sufficiently large. From the preceding paragraph we have that $|A|$ and $|B|$ are at least $|S|/D$. Thus, in particular, we have $|A|, |B| \ge 16K$. These remarks allow us to deduce that

$$D^2 \;\le\; \frac{|S|^2}{(|A|-1)(|B|-1)} \;\le\; \frac{|S|^2}{|A||B|}\exp\left(\frac{1}{4K}\right)\,, \tag{3.29}$$

where we have used the inequality $(1-x)^{-1} \le 1+2x \le \exp(2x)$ when x is in $[0, 1/2]$, applied with x taken to be $1/|A|$ and then to be $1/|B|$. Finally, since $C_{\tilde{z}}(a,b)$ is always positive, we conclude using (3.28) and (3.29) that the sum on the left hand side of (3.28) does not exceed

$$D^2 \sum_{(a,b)\in A\times B} C_{\tilde{z}}(a,b) \;\le\; \frac{|S|^2}{|A||B|}\exp\left(\frac{1}{4K}\right) \sum_{(a,b)\in A\times B} C_{\tilde{z}}(a,b)\,, \tag{3.30}$$

the sum on the right hand side in (3.30) counts the number of pairs (a,b) in $A\times B$ such that $a+b-\tilde{z}$ is an invertible residue class modulo U. We shall presently bound the sum on this sum by means Proposition 2.3.

Let I be the set of prime numbers not exceeding $a = 4^{11}K^2$. By means of the Chinese remainder theorem we identify the group $\mathbf{Z}/U\mathbf{Z}$ with the group G, the product of the groups $\mathbf{Z}/p\mathbf{Z}$ with p varying over I. For any a in $\mathbf{Z}/U\mathbf{Z}$ and p in I, let us denote the canonical image of a in $\mathbf{Z}/p\mathbf{Z}$ by a_p. Then the sum on the right hand side in (3.30) is the same as the number of pairs (a,b) in $A\times B$ such that $a_p + b_p \neq \tilde{z}_p$ for all p in I. Thus, if we set $Q = 4\log 4K \log\log 4K$ and let J be the subset of I comprising the primes in I that exceed Q^2, then we certainly have

$$\sum_{(a,b)\in A\times B} C_{\tilde{z}}(a,b) \le \left|\{(a,b)\in A\times B \,|\, a_p + b_p \notin \Omega_p \text{ for all } p\in J\}\right|\,. \tag{3.31}$$

where $\Omega_p = \{\tilde{z}_p\}$, for each p in J.

Since we have $|A| \geq \phi(U)/4K$ we obtain that $|G|/|A| \leq 4KU/\phi(U)$. Using the trivial bound $U/\phi(U) = \prod_{p\leq a}(1-p^{-1}) \geq 1/a$ we then deduce that $|G|/|A| \leq 4^{12}K^3$. Similarly, we also have $|G|/|B| \leq 4^{12}K^3$ and consequently that $L(A,B) \leq 24\log 4K$, where $L(A,B)$ is as in Proposition 2.3. Next, we see that in our case $\omega_J(\Omega)$ of Proposition 2.3 is $\sum_{p>Q^2}\frac{1}{p^2} \leq \frac{2}{Q^2}$. Finally, on writing P to denote the product of the primes in J, we note that

$$\exp\left(-\sum_{p\in J}\frac{1}{p}\right) \leq \exp\left(\sum_{p\in J}\frac{2}{p^2}\right)\prod_{p\in J}(1-p^{-1}) \leq \frac{\phi(P)}{P}\exp\left(\frac{4}{Q^2}\right), \tag{3.32}$$

by the inequality $-\log(1-x) \leq x + 2x^2$ valid for $0 \leq x \leq 1/2$.

Thus on applying Proposition 2.3 to bound the right hand side of (3.31) we deduce that for any integer t with $1 \leq t \leq Q$ we have

$$\sum_{(a,b)\in A\times B} C_{\tilde{z}}(a,b) \leq \frac{\phi(P)}{P}|A||B|\exp\left(\frac{24\log 4K}{t}+\frac{6t}{Q^2}\right). \tag{3.33}$$

Since $Q = 4\log 4K\log\log 4K \geq 1$, there is an integer $t \geq 1$ such that $Q/2 \leq t \leq Q$. Taking t to be such an integer we see that the expression in the brackets on the right hand side of (3.33) does not exceed

$$\frac{48\log 4K}{Q}+\frac{6}{Q} \leq \frac{14}{\log\log 4K}. \tag{3.34}$$

On combining (3.30) and (3.33) with the bound above and recalling that the left hand side of (3.30) is an upper bound for the left hand side of (3.28), we obtain that

$$\sum_{(a,b)\in\tilde{S}^2} C_{\tilde{z}}(a,b)\, m(a)m(b) \leq \frac{\phi(P)}{P}|S|^2\exp\left(\frac{14}{\log\log 4K}+\frac{1}{4K}\right), \tag{3.35}$$

uniformly in z. Finally, taking (3.35) together with (3.27) and noting that M as defined in the statement of Theorem 1.1 is nothing but $\frac{U}{P}$, we conclude that

$$T(U) \leq \frac{M}{\phi(M)}\,|S|^3\exp\left(\frac{14}{\log\log 4K}+\frac{1}{4K}\right), \tag{3.36}$$

for all sufficiently large N. Finally, on recalling that for sufficiently large N we have $|S| \geq N/4K\log N$ by the prime number theorem, we obtain from (3.1), (3.22) and (3.36) that

$$E(S) \leq \frac{M}{\phi(M)}\,\frac{|S|^3}{\log\left(\frac{N}{2}\right)}\exp\left(\frac{14}{\log\log 4K}+\frac{1}{4K}\right)\left(1+\frac{(\log 4K)^2}{16K}\right). \tag{3.37}$$

Theorem 1.1 follows from (3.37) on using the inequality $1 + x \leq \exp(x)$ with $x = \frac{(\log 4K)^2}{16K}$ and noting that $(\log 4K)^2 \log\log 4K \leq 16K$ and that $\log\log 4K \leq 4K$ since $K \geq 1$.

Let us now take up Theorem 1.2 and begin by recalling the notation used in its statement. Then with $P_i = \mathcal{P}_i \cap (\frac{N}{2}, N]$ we have for each sufficiently large N that there is an i, with $1 \leq i \leq K$, such that $|P_i| \geq \pi^*(N)/K$. As we have already remarked in Section 1 (see (1.6)), Theorem 1.1 and the inequality (1.1) now show that for this P_i we have $|2P_i| \geq N/CK \log\log 4K$, where C is an absolute constant. Let us set $L \geq 1$ to be the smallest integer such that

$$|2P_i| \geq \frac{N}{CK \log\log 4K} > \frac{N}{L} + 1 \, . \tag{3.38}$$

When N is sufficiently large we have $L \leq 2CK \log\log 4K$.

To complete the proof of Theorem 1.2 from here, we follow [4] with some modifications. Since $2P_i$ is a subset of $(N, 2N]$, Sárközy's finite addition theorem (see Theorem 1, page 115 of [9]) applied to $2P_i - N$ tells us that for each sufficiently large N there is an arithmetical progression $\mathcal{A}$ with N terms and common difference d contained in $2hP_i$, where the integers h and d satisfy $1 \leq d \leq L - 1$ and $1 \leq h \leq 118L$. Since $2hP_i$ is contained in $(hN, 2hN]$, we have in particular that $0 \leq a \leq 236LN$ for any term a of $\mathcal{A}$.

Let p be any element of P_i. Then p is a prime number in $(N/2, N]$ and if $N \geq 236L$, we certainly have $d < p$ from the bound on d. In particular, p is coprime to d. Since the modulus of the arithmetical progression $\mathcal{A}$ is d and since it contains $N \geq p$ terms, it follows that $\mathcal{A}$ contains a complete system of residue classes modulo p. Therefore for every integer n there is an a in $\mathcal{A}$ and an integer b such that $n = a + bp$. Further, if n lies in the interval $I(N) = [236LN, 237LN]$ then we have $0 \leq b \leq 574L$, since $0 \leq a \leq 236LN$ and $N/2 < p$. On recalling that a is in $2hP_i$ and p is in P_i, we conclude that every integer in the interval $I(N)$ can be written as the sum of no more than $810L$ elements of P_i. In other words, for all sufficiently large N, every integer in $I(N)$ has a monochromatic representation as sum of no more than $1700C \log\log 4K$ prime numbers. Finally, on noting that as N varies over all sufficiently large integers, the union of the intervals $I(N)$ contains all sufficiently large integers, we obtain Theorem 1.2.

Acknowledgment : We are grateful to Professor Antal Balog for spending his time with various drafts of this article. The first named author thanks the Université Lille I and the SYM project of the Harish-Chandra Research Institute for their generous support during the course of this work.

References

[1] R. Ayoub, On Rademachers extension of the Goldbach-Vinogradov theorem, *Trans. Amer. Math. Soc.*,Vol. 74 , 1953, pp. 482-491.

[2] B.J. Green, *MR2321364 (2008d:11007)*, A.M.S. Math Reviews.

[3] H. Iwaniec and I.Kowalski, Analytic Number Theory, American Mathematical Society Colloquium Publications 53, A.M.S., 2004.
[4] N. Hegyvári and F. Hennecart, On monochromatic sums of squares and primes, *Journal of Number Theory*, Vol. 124, 2007, pp. 314-324.
[5] K. Prachar, Primzahlverteilung, Grundlehren der Mathematischen Wissenschaften 91, Springer Verlag, 1957.
[6] O. Ramaré and I. Ruzsa, Additive properties of dense subsets of sifted sequences, *Journal de Theorie des Nombres de Bordeaux,*Volume 13, pp. 559 -581, 2001.
[7] O. Ramaré, Arithmetical aspects of the large sieve inequality. With the collaboration of D. S. Ramana. *Harish-Chandra Research Institute Lecture Notes, 1.*, Hindustan Book Agency, New Delhi, 2009.
[8] A. Sárközy, Unsolved Problems in Number Theory, *Period. Math. Hungar.*, Vol. 42, pp. 17-35, 2001.
[9] A. Sárközy, Finite Addition Theorem I, *Journal of Number Theory*, Vol. 48, pp. 197-218, 1994.

Harish-Chandra Research Institute, Jhunsi, Allahabad -211 019, India.
E-mail address: suri@hri.res.in

Laboratoire Paul Painlevé, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France.
E-mail address: ramare@math.univ-lille1.fr