Journal de Théorie des Nombres
de Bordeaux **13** (2001), 559–581

Additive properties of dense subsets of sifted sequences

par Olivier RAMARÉ et Imre Z. RUZSA

Résumé. Nous nous intéressons aux propriétés additives des sous-suites de densité de suites "bien criblées" et montrons en particulier que, sous des hypothèses très générales, une telle suite est une base additive asymptotique dont l'ordre est très bien contrôlé.

Abstract. We examine additive properties of dense subsets of sifted sequences, and in particular prove under very general assumptions that such a sequence is an additive asymptotic basis whose order is very well controlled.

1. Introduction

The sequence $\mathcal{P}$ of primes is known to be an asymptotic basis of order at most 4 (due to Vinogradov's work) and its expected order is 3. Taking an infinite sequence of primes $\mathcal{P}^*$ which contains a positive proportion of primes we answer two additive questions concerning this sequence. As shown by Sárközy in [20], such a sequence is an asymptotic basis, and thus an essential component. We give an upper bound for its order as an asymptotic basis and a lower bound for its "impact", this word being understood in the spirit of Plünnecke and Ruzsa (cf. [19]). None of the sequence of integers we consider contains zero and as usual in additive number theory, if $\mathcal{A}$ is a sequence of integers, we denote by $A(X)$ the number of its elements that are less than X. Since our methods are fairly elementary (partly inherited from [16]) we prove a wide generalisation of these results to any "sufficiently sifted sequence" and its dense subsequences, namely Theorem 1 below.

More precisely, we say that the sequence $\mathcal{A}$ of integers is sufficiently sifted if there exist $X_0 \geq 1$, $c_1, c_2 > 0$, $\kappa \geq 0$, $s_0 \geq 2$, $\xi \in [0, \frac{1}{2}[$, $\alpha > 0$, a function r such that $r(X) = o(X(\operatorname{Log} X)^{-\kappa})$, a sequence $(\mathcal{K}_p)_{p\in\mathcal{P}}$ such that $\mathcal{K}_p \subset \mathbb{Z}/p\mathbb{Z}$ and a sequence $(\mathcal{A}_X)_{X\geq 1}$ of subsets of $\mathcal{A}$ such that

(H_1) $A(X) \geq c_1 X/\operatorname{Log}^\kappa X$ for $X \geq X_0$.

(H_2) $A_X(X) = A(X) + r(X)$.

Manuscrit reçu le 2 juillet 1999.

(H_3) $\forall p \le X^{1/s_0}$, $\mathcal{A}_X + p\mathbb{Z} \subset \mathcal{K}_p$.
(H_4) $\sum_{p\le X}(1-|\mathcal{K}_p|/p)\operatorname{Log} p = \kappa \operatorname{Log} X + \mathcal{O}(1)$.
(H_5) We have $|\mathcal{K}_p| \ge p - c_2 p^{\xi}$.
Note that (H_5) implies that

$$\sum_{p>L}\bigl(1-|\mathcal{K}_p|/p\bigr)^2 \ll L^{2\xi-1} \tag{1.1}$$

and the fact the $\mathcal{A}$ is infinite implies that $\mathcal{K}_p \ne \emptyset$. As examples of sufficiently sifted sequences, let us mention the sequence of integers ($\kappa = 0$), the sequence of primes ($\kappa = 1$) , the sequence of integers that are sums of two squares ($\kappa = \frac{1}{2}$), the sequence of integers n that are sums of two coprime squares and such that $n+1$ also has this property ($\kappa = 1$, cf. [10]) or the sequence of those prime numbers p such that p can be written as $p = 1 + m^2 + n^2$ with $(m,n) = 1$ ($\kappa = \frac{3}{2}$, cf. [11] and also [7] for related sequences). As far as orders as asymptotic bases are concerned the examples above have an order C which verifies respectively $C = 1$, $3 \le C \le 4$, $C = 2$, $2 \le C < \infty$ and $C < \infty$. We mention a last example: the sequence of integers n that are product of $s_0 - 1$ primes each being larger than n^{1/s_0} (here $\kappa = 1$).

The parameter κ occurring in (H_1) and (H_4) above is called the dimension of the sequence. Since (as we show below), $\mathcal{A}$ is essentially the result of sieving the integers by a sieve of dimension κ, we see that $A(X) \asymp X/\operatorname{Log}^{\kappa} X$ which provides an intrinsic definition of κ. Given such a sufficiently sifted sequence $\mathcal{A}$, we shall consider subsequences $\mathcal{A}^* \subset \mathcal{A}$ which are dense with respect to $\mathcal{A}$, i.e. such that $A^*(X) \ge A(X)/k$ for $X \ge X_1$ for a given constant $k \ge 1$. Note that such a subsequence is again a sufficiently sifted sequence and of same dimension, but we are interested in the dependence in k. Our main result is

Theorem 1. *For $i \in \{1,2\}$, let $\mathcal{A}_i$ be a sufficiently sifted sequence of dimension κ_i, let $k_i \ge 1$ be a real number and let $\mathcal{A}_i^* \subset \mathcal{A}_i$ be such that $A_i^*(X) \ge A_i(X)/k_i$ for $X \ge X_1$. Then we have*

$$(\mathcal{A}_1^* + \mathcal{A}_2^*)(X) \gg_{\mathcal{A}_1,\mathcal{A}_2} X/\bigl(k_1(\operatorname{Log}\operatorname{Log} 3(k_1+k_2))^{\kappa_1}\bigr).$$

By $\gg_{\mathcal{A}_1,\mathcal{A}_2}$, we mean that the implied constant may depend on all the parameters required to define the sufficiently sifted sequences $\mathcal{A}_1$ and $\mathcal{A}_2$.

This result is fully asymmetrical in its statement as in its proof, only the starting hypotheses being similar. We shall reduce the problem to a finite one by treating the first sequence via Selberg sieve while the other one will be treated by appealing to an improved version of the large sieve inequality. The known "duality" between these two processes explains the similarity of hypotheses. Moreover to treat the final problem, the second sequence has to be not too badly distributed in arithmetic progression to finite moduli, which is built in in this setting.

We have restricted our attention to finite dimensional sieves, but the method used to prove Theorem 1 can most probably be extended to cover the case when one of the sifted sequences is as sparse as the sequence of squares. Both sequences cannot be that sparse since the set of sums of two squares do not have positive lower density. But the method would never be able to tackle for instance the sequence consisting of sums of a prime and a cube, though this sequence does have positive lower density [17, 4].

Here are some corollaries:

Corollary 1. *Let $\mathcal{A}$ be a sufficiently sifted sequence of dimension κ. Let $k \geq 1$ be a real number and $\mathcal{A}^* \subset \mathcal{A}$ be such that $A^*(X) \geq A(X)/k$ for $X \geq X_1$. If $\mathcal{A}^*$ is not included in any subgroup of $\mathbb{Z}$, then $\mathcal{A}^*$ is an asymptotic basis of order $\ll_{\mathcal{A}} k(\operatorname{Log}\operatorname{Log} 3k)^{\kappa}$. Moreover this bound is best possible for a sequence of k going to infinity, aside from the constant implied in the $\ll_{\mathcal{A}}$-symbol.*

By Theorem 1, the set of integers that are sums of two elements of $\mathcal{A}^*$ has positive lower density, say δ. We then conclude by using Kneser's Theorem that $\mathcal{A}^*$ is an asymptotic basis of order $\mathcal{O}(1/\delta)$ (statement and proof of Kneser's Theorem may be found in [9, chapter I, paragraph 7, Theorem 16′]).

Thus Corollary 1 says that, except if some local obstructions occur, a sufficiently sifted sequence is an asymptotic basis and that the same property holds for all its dense subsequences. Though this result seems surprising, an adaptation of Schnirelman's approach ([21])would most probably be enough to establish it. However the fact that the order should be so well bounded is new. For instance for the sequence of primes, Sárközy got the bound $\ll k^4$ and we do not see how his approach could provide anything better than the bound $\ll k^2$. Note that he conjectured our result for this sequence.

Being an asymptotic additive basis, a theorem of Erdős asserts that $\mathcal{A}^*$ is an essential component i.e. for any sequence of integers $\mathcal{B}$ of asymptotic lower density $\geq 1/\ell$, the asymptotic lower density of $\mathcal{B}+\mathcal{P}$ is $> 1/\ell$ (see [9] for instance). For the sequence of primes Ruzsa [18] has shown that this phenomenom was particularly pronounced if ℓ is large since the asymptotic lower density of $\mathcal{B}+\mathcal{P}$ is $\geq c/\operatorname{Log}\operatorname{Log}(3\ell)$ for some positive constant c. Since a sequence of positive lower density is a dense subsequence of the sufficiently sifted sequence of natural intergers, Theorem 1 readily yields

Corollary 2. *Let $\mathcal{A}^* \subset \mathcal{A}$ be two sequences verifying the assumptions of Corollary 1. There exists a constant $c_3(\mathcal{A}) > 0$ such that for all $\ell \geq 1$ and every sequence of integers $\mathcal{B}$ of asymptotic lower density $\geq 1/\ell$, the* *asymptotic lower density of $\mathcal{B}+\mathcal{A}^*$ is greater than $c_3/[k(\operatorname{Log}\operatorname{Log} 3(\ell+k))^\kappa]$. This result is optimal for a sequence of k going to infinity, as far as the value of c_3 is not concerned.*

We of course do not need to assume that $\mathcal{A}^*$ is not included in any subgroup of $\mathbb{Z}$ (since Kneser's Theorem is not required).

The corresponding finite problems sound as follows. Let m be a modulus. Let $\mathcal{K}_m$ be a subset of $\mathbb{Z}/m\mathbb{Z}$. For any $\ell|m$, we define $\mathcal{K}_\ell = \mathcal{K}_m/\ell\mathbb{Z}$. We say that $\mathcal{K}_m$ is multiplicatively split if we have $|\mathcal{K}_{h\ell}| = |\mathcal{K}_h||\mathcal{K}_\ell|$ whenever $(h,\ell) = 1$ and $h\ell|m$. In other words, the canonical isomorphism from $\mathbb{Z}/h\ell\mathbb{Z}$ to $\mathbb{Z}/h\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ maps $\mathcal{K}_{h\ell}$ to $\mathcal{K}_h\times\mathcal{K}_\ell$. Given such a subset and a subset $\mathcal{K}_m^*$ of $\mathcal{K}_m$ such that $|\mathcal{K}_m^*| \geq |\mathcal{K}_m|/k$ and such that $\mathcal{K}_m^*$ is not included in any subgroup of $\mathbb{Z}/m\mathbb{Z}$, how can we bound the order of $\mathcal{K}_m^*$ as an additive basis of $\mathbb{Z}/m\mathbb{Z}$? And what is the impact of this set ? We give satisfactory answers to both questions in the next two results. For the sake of simplicity we shall restrain our attention to "squarefree" $\mathcal{K}_m$, by which we mean that $\mathcal{K}_{p^\nu}$ is the inverse image by the canonical projection of $\mathcal{K}_p$. Thus squarefree moduli carry all the information about this set. To be able to have asymptotical results, we need a family of $\mathcal{K}_m$, which we get by considering a compact subset $\mathcal{K}$ of $\hat{\mathbb{Z}}$ (the projective limit of $\mathbb{Z}/n\mathbb{Z}$) and defining $\mathcal{K}_m = \mathcal{K}/m\hat{\mathbb{Z}}$. We assume that $\mathcal{K}_m$ is multiplicatively split for all m which we shorten by saying that $\mathcal{K}$ is multiplicatively split. The data $\mathcal{K}$ is equivalent to a sequence $(\mathcal{K}_m)$ such that the $\mathcal{K}_m \subset \mathbb{Z}/m\mathbb{Z}$ and $\mathcal{K}_\ell = \mathcal{K}_m/\ell\mathbb{Z}$ for $\ell|m$. Since Corollary 3 below is fairly intricate in general, for the two applications we have in mind we shall further restrict our attention to moduli M of the shape $M = \prod_{p\leq\lambda} p$ and to compacta $\mathcal{K}$ verifying (H_4) and (H_5). This is by no means necessary but shall render our results more readable.

Theorem 2. *Take a compact $\mathcal{K}$ as above and a sequence $(\mathcal{B}_M)_M$ of subsets of $\mathbb{Z}/M\mathbb{Z}$ where M ranges moduli of the shape $M = \prod_{p\leq\lambda} p$. Then we have*

$$|\mathcal{B}_M + \mathcal{K}_M^*| \gg_{\mathcal{K}} M/\big(k\big(\operatorname{Log}\operatorname{Log}(M/|\mathcal{B}_M|)\big)^\kappa\big).$$

It is important to note that the implied constant is independant of k and $\mathcal{B}_M$.

Taking for B_M a subset of density of $\mathbb{Z}/M\mathbb{Z}$, we get immediately a measure of the "impact" of $\mathcal{K}_M^*$.

Combining the proof of Theorem 1 together with Theorem 2, we reach

Corollary 3. *Notations being as above, if the set $\mathcal{K}_M^*$ is not included in any subgroups of $\mathbb{Z}/M\mathbb{Z}$, then it is a basis of order $\mathcal{O}(k(\operatorname{Log}\operatorname{Log}(3k))^\kappa)$.*

Taking $\mathcal{K}$ to be the set of invertible elements ($\kappa = 1$), Corollary 3 is an appreciable improvement (but with stronger hypotheses) on a theorem of Cauchy-Davenport-Chowla (cf. [9] chapter 1, paragraph 6 Theorem 15) which would give the order to be $\mathcal{O}(k \cdot \operatorname{Log} \lambda)$.

While the results pertaining to the sieve are exposed in Section 4, we state here the result concerning the finite part of the proof, where we do not make any special assumption about $\mathcal{K}$, aside from the fact that it should be multiplicatively split.

Theorem 3. *Let m be an integer and $\mathcal{A}$ and $\mathcal{B}$ be two subsets of $\mathbb{Z}/m\mathbb{Z}$. Then*

$$\left|\{(a,b) : a \in \mathcal{A}, b \in \mathcal{B}, a+b \in \mathcal{K}_m\}\right| \leq 3\eta \cdot |\mathcal{A}| \cdot |\mathcal{B}| \cdot \frac{|\mathcal{K}_m|}{m}$$

where

$$\eta = \frac{m}{|\mathcal{K}_m|} \min_{\mathcal{D}} \exp \sum_{q \in \mathcal{D}} \left(-\frac{|\mathcal{L}'_q|}{q} + \left(1 + \operatorname{Log} \frac{m^2}{|\mathcal{A}||\mathcal{B}|}\right) \frac{|\mathcal{L}'_q|^2}{q^2} \right)$$

where $\mathcal{D}$ ranges the set of subsets of exact prime power divisors of m and $\mathcal{L}'_q = \mathbb{Z}/q\mathbb{Z} \setminus \mathcal{K}_q$.

An "exact prime power divisor of m" is a power of a prime, say $q > 1$, such that m/q is prime to q.

The organisation of this paper. In Section 2, we prove Theorem 3 and in Section 3, we prove Theorem 2. In Section 4, we gather information about Selberg sieve and the large sieve in order to build an upper bound for the characteristic function of a sufficiently sifted sequence and to prove a large sieve estimate that will be required to prove Theorem 1, this proof being displayed in Section 5. Section 6 shows how Theorem 2 and the proper uniformity in the proof of Theorem 1 implies Corollary 3. In Section 7, we give examples showing that the bounds given are optimal.

2. Sums coprime to a fixed number. Proof of Theorem 3

Throughout this proof p shall denote a prime factor of m. Define $|\mathcal{A}| = n \leq |\mathcal{B}| = n'$ and

$$S = \left|\{(a,b) : a \in \mathcal{A}, b \in \mathcal{B}, a+b \in \mathcal{K}_m\}\right|. \tag{2.1}$$

We define further

$$s(x) = \left|\{a \in \mathcal{A} : a + x \in \mathcal{K}_m\}\right|. \tag{2.2}$$

We have

$$S = \sum_{b \in \mathcal{B}} s(b).$$

By the power-mean inequality, we infer

$$S \le (n')^{1-1/t}\Big(\sum_{x\in\mathbb{Z}/m\mathbb{Z}} s(x)^t\Big)^{1/t} \tag{2.3}$$

with any positive integer t.

Now $s(x)^t$ is the number of those t-tuples $a_1,\dots,a_t \in \mathcal{A}$ for which $a_i+x \in \mathcal{K}_m$ for all i. So if we write

$$F(a_1,\dots,a_t) = \big|\{y \in Z_m : a_i + y \in \mathcal{K}_m \text{ for all } i\}\big|,$$

then

$$\sigma_t = \sum_{x\in Z_m} s(x)^t = \sum_{a_1,\dots,a_t\in\mathcal{A}} F(a_1,\dots,a_t). \tag{2.4}$$

For a prime power q let $\mathcal{L}'_q$ be the complementary set of $\mathcal{K}_q$ in $\mathbb{Z}/q\mathbb{Z}$ and

$$\omega_q(a_1,\dots,a_t) = \big|\bigcup_i (a_i + \mathcal{L}'_q)\big|. \tag{2.5}$$

We have

$$F(a_1,\dots,a_t) = \prod_q (q - \omega_q(a_1,\dots,a_t)) = m\prod_q (1 - \omega_q(a_1,\dots,a_t)/q).$$

Hence

$$\sigma_t = m\sum_{a_1,\dots,a_t\in\mathcal{A}}\prod_q\Big(1 - \frac{\omega_q(a_1,\dots,a_t)}{q}\Big). \tag{2.6}$$

Let $\mathcal{D}$ be a subset of exact prime power divisors of m. We estimate $1-\omega_q(a_1,\dots,a_t)/q$ as follows. For $q\in\mathcal{D}$ we use the elementary inequality valid for $x\ge 0$

$$1 - \frac{x}{q} \le \exp -\frac{x}{q} = \exp -\frac{t|\mathcal{L}'_q|}{q}\exp\frac{t|\mathcal{L}'_q| - x}{q},$$

while for $q\notin\mathcal{D}$ we use the trivial estimate $1-\omega_q(a_1,\dots,a_t)/q \le 1$. We also observe that by inclusion-exclusion

$$t|\mathcal{L}'_q| - \omega_q(a_1,\dots,a_t) \le \sum_{i<j}\big|(a_i+\mathcal{L}'_q)\cap(a_j+\mathcal{L}'_q)\big|.$$

Hence with the notation

$$\psi(a,a') = \sum_{q\in\mathcal{D}}\frac{\big|(a+\mathcal{L}'_q)\cap(a'+\mathcal{L}'_q)\big|}{q} \tag{2.7}$$

we obtain

$$\sigma_t \le m\exp\Big(-t\sum_{q\in\mathcal{D}}|\mathcal{L}'_q|/q\Big)\sum_{a_1,\dots,a_t\in\mathcal{A}}\exp\sum_{i<j}\psi(a_i,a_j). \tag{2.8}$$

To estimate the last sum we use the inequality of geometric and arithmetic mean:

$$\exp \sum_{i<j} \psi(a_i, a_j) \le \binom{t}{2}^{-1} \sum_{i<j} \exp \binom{t}{2} \psi(a_i, a_j),$$

hence

$$\sum_{a_1,\dots,a_t \in \mathcal{A}} \exp \sum_{i<j} \psi(a_i, a_j) \le n^{t-2} \sum_{a,a' \in \mathcal{A}} \exp t^2 \psi(a, a'). \tag{2.9}$$

We thus have to evaluate this latter double sum Σ. To do that we fix a and let a' range $\mathbb{Z}/m\mathbb{Z}$. We get

$$\begin{aligned} \Sigma &\le \sum_{a \in \mathcal{A}} m \prod_{q \in \mathcal{D}} \left(\frac{1}{q} \sum_{c \bmod q} \exp\left(\frac{t^2}{q} \big| (a + \mathcal{L}'_q) \cap (c + \mathcal{L}'_q) \big| \right)\right) \\ &\le mn \prod_{q \in \mathcal{D}} \left(\frac{1}{q} \sum_{c \bmod q} \exp\left(\frac{t^2}{q} \big| \mathcal{L}'_q \cap (c + \mathcal{L}'_q) \big| \right)\right). \end{aligned} \tag{2.10}$$

To go any further, consider the following optimisation problem:

$$\text{Maximum of } S(x_1, \dots, x_q) = \sum_{i=1}^{q} \theta^{x_i}$$
$$\text{under} \quad \sum_i x_i = H^2, \quad x_i \in \mathbb{N}, \qquad (\forall i,\ 0 \le x_i \le H)$$

for $\theta > 1$. This corresponds to the sum we have to bound with $\theta = \exp(t^2/q)$, $x_i = \big|\mathcal{L}'_q \cap (i + \mathcal{L}'_q)\big|$ and $H = |\mathcal{L}'_q|$. Assume $(x_1, \dots, x_q)$ verify the proper inequalities and it is such that there exist x_i and x_j with $i \ne j$ and both $\in [1, H-1]$. We can further assume that $x_i \ge x_j$ and $i = 1$, $j = 2$. The q-tuple $(x_1 + 1, x_2 - 1, x_3, \dots, x_q)$ gives a larger value for S since the difference between the two values is

$$\theta^{x_1+1} - \theta^{x_1} + \theta^{x_2-1} - \theta^{x_2} = (\theta - 1)(\theta^{x_1} - \theta^{x_2-1}) > 0.$$

Using this remark, we get that the maximum is reached when H^2/H of the x_i are equal to H and the other are 0. The maximal value is thus

$$H\ \theta^H + q - H \le q\ \theta^{\frac{H^2}{q}}$$

this inequality coming from $xb^x + 1 - x - b^{x^2} \le 0$ for $0 \le x \le 1$ and $b \ge 1$ (the derivative in b is ≥ 0, and the inequality is obvious for $b = 1$).

Applying this latter result to each term of the product appearing in the right-hand side inequality of (2.10), we reach the upper bound

$$\Sigma \le mn \prod_{q \in \mathcal{D}} \left(\exp\left(t^2 |\mathcal{L}'_q|^2 / q\right)\right)$$

from which we infer (collecting (2.3), (2.4), (2.8) and (2.9))

$$S \le nn'\Big(\frac{m^2}{nn'}\Big)^{1/t}\exp\Big(-\sum_{q\in\mathcal{D}}|\mathcal{L}'_q|/q\Big)\exp\Big(\sum_{q\in\mathcal{D}}\frac{t|\mathcal{L}'_q|^2}{q^2}\Big).$$

We put $t=[1+\log(m^2/nn')]$, which makes the factor $(m^2/nn')^{1/t}$ bounded by 3.

3. Proof of Theorem 2

This results is an easy consequence of Theorem 3 but the estimates proved here shall prepare the ground for the proof of Theorem 1. Put

$$r_2(n)=\sum_{k+b=n}1 \tag{3.1}$$

where $k\in\mathcal{K}^*_M$ and $b\in\mathcal{B}_M$. We have

$$|\mathcal{K}^*_M||\mathcal{B}_M|=\sum_n r_2(n)\le\sum_{\substack{b,n\\ n-b\in\mathcal{K}_M,r_2(n)\neq 0}}1\ll|\mathcal{B}_M|\,\delta\cdot M\cdot\frac{|\mathcal{K}_M|}{M}\cdot\eta \tag{3.2}$$

by applying Theorem 3 to $\mathcal{B}=-\mathcal{B}_M$ and to $\mathcal{A}=\{n\in\mathbb{Z}/M\mathbb{Z},\ r_2(n)\neq 0\}=\mathcal{K}^*_M+\mathcal{B}_M$ of cardinality δM, and where η is defined in Theorem 3. In order to evaluate η, let us first notice that here $\mathcal{L}_p=\mathcal{L}'_p$ and that partial summation together with (H_4) give

$$\sum_{p\le P}|\mathcal{L}_p|/p=\kappa\,\mathrm{Log}\,\mathrm{Log}\,P+\mathcal{O}(1),\qquad (P\ge 3). \tag{3.3}$$

Furthermore, we have

$$\begin{aligned}|\mathcal{K}_M|/M&=\prod_{p\le\lambda}\Big(1-|\mathcal{L}_p|/p\Big)\\ &=\exp\Big(-\sum_{p\le\lambda}|\mathcal{L}_p|/p+\mathcal{O}\big(\sum_{p\ge 2}|\mathcal{L}_p|^2/p^2\big)\Big)\end{aligned}$$

hence using (1.1) and (3.3), we get

$$|\mathcal{K}_M|/M\asymp(\mathrm{Log}\,\lambda)^{-\kappa}. \tag{3.4}$$

Notice next that

$$\mathrm{Log}(M^2/(|\mathcal{A}||\mathcal{B}|))\le\mathrm{Log}(\delta^{-1}M/|\mathcal{B}_M|)\le 2\,\mathrm{Log}(M/|\mathcal{B}_M|)$$

since $\delta^{-1}\le M/|\mathcal{B}_M|$. Taking $\mathcal{D}=\{p\in]L,\lambda]\}$ with

$$L=\big(\mathrm{Log}(M/|\mathcal{B}_M|)\big)^{1/(1-2\xi)},$$

and recalling (3.3), we get

$$\eta\ll_{\mathcal{K}}(\mathrm{Log}\,L)^{-\kappa}\ll_{\mathcal{K}}(\mathrm{Log}\,\mathrm{Log}(3M/|\mathcal{B}_M|))^{-\kappa}. \tag{3.5}$$

Inserting this value in (3.2), we reach

$$1/\big(k(\operatorname{Log}\operatorname{Log}(3M/|\mathcal{B}_M|))^\kappa\big) \ll \delta = |\mathcal{K}_M^* + \mathcal{B}_M|/M \tag{3.6}$$

as required. Such a proof is correct if L is less than λ, but extends automatically to the other case, for we then have

$$\big(\operatorname{Log}\operatorname{Log}(M/|\mathcal{B}_M|)\big)^\kappa \geq \big((1-2\xi)\operatorname{Log}\lambda\big)^\kappa$$

so that (3.6) is weaker than

$$|\mathcal{K}_M^* + \mathcal{B}_M|/M \gg \big(\operatorname{Log}\lambda\big)^{-\kappa}$$

which is already certainly true.

4. Sieve results

In Section 4.1 which can be read independently, we present Selberg sieve in a way that is convenient for this paper and which allows one to sieve by non-squarefree integers. The reader is assumed to be familiar with the large sieve and the classical Selberg upper Λ^2-sieve. Under an additional hypothesis, we use this approach to recover Selberg's upper bound for an interval through the large sieve, following an idea of Bombieri and Davenport and deduce an improvement of the large sieve inequality for sifted sequences which is an essential tool for the proof of Theorem 1. We furthermore prove several technical lemmas that are required to use this sieving device as an enveloping sieve (i.e. essentially as a preliminary sieve).

In Section 4.2, we explain rapidly how we build an enveloping sieve in the context of this paper.

4.1. Remarks on Selberg sieve and the large sieve.

∘∘ *The supporting compact* $\mathcal{K}$. Our first data is a non empty compact subset $\mathcal{K}$ of $\hat{\mathbb{Z}} = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z}$ which is supposed to be multiplicatively split (a notion that has been defined between Theorem 1 and Theorem 2). This is equivalent to a sequence $(\mathcal{K}_{p^\nu})$ with $\mathcal{K}_{p^\nu} \subset \mathbb{Z}/p^\nu\mathbb{Z}$ and such that the canonical projection $\sigma_{p^\nu} : \mathbb{Z}/p^\nu\mathbb{Z} \to \mathbb{Z}/p^{\nu-1}\mathbb{Z}$ maps $\mathcal{K}_{p^\nu}$ to $\mathcal{K}_{p^{\nu-1}}$. As a matter of notation, we put $\mathcal{K}_d = \mathcal{K}/d\hat{\mathbb{Z}}$.

A sequence $(\varphi_n)_{n\geq 1}$ is said to be supported by $\mathcal{K}$ up to the level D if

$$\varphi_n \neq 0 \implies \forall d \leq D, n \in \mathcal{K}_d. \tag{4.1.1}$$

∘∘ *The bordering system* $(\mathcal{L}_d)_d$. We shall need another sequence of sets $(\mathcal{L}_d)_{d\geq 1}$ complementary to $\mathcal{K}$: we put $\mathcal{L}_1 = \{1\}$ and $\mathcal{L}_{p^\nu} = \mathcal{K}_{p^{\nu-1}} - \mathcal{K}_{p^\nu}$, i.e. it is the set of elements $x \in \mathbb{Z}/p^\nu\mathbb{Z}$ such that $\sigma_{p^\nu}(x) \in \mathcal{K}_{p^{\nu-1}}$ but that do not belong to $\mathcal{K}_{p^\nu}$. We then define $\mathcal{L}_d$ by split multiplicativity. The notation $n \in \mathcal{K}_d$ (resp. $n \in \mathcal{L}_d$) means that the image of n in $\mathbb{Z}/d\mathbb{Z}$ is in $\mathcal{K}_d$ (resp. in $\mathcal{L}_d$) and the function $1_{\mathcal{K}_d}$ is the characteristic function of such integers. Note that contrarily to what happens with $\mathcal{K}$, we do not have $\mathcal{L}_\ell = \mathcal{L}_d/\ell\mathbb{Z}$ if $\ell|d$. By definition we have

$$1_{\mathcal{K}_d} = \prod_{p^\nu|d}\left(1 - 1_{\mathcal{L}_p} - 1_{\mathcal{L}_{p^2}} - \cdots - 1_{\mathcal{L}_{p^\nu}}\right) = \sum_{\delta|d}(-1)^{\omega(d)}1_{\mathcal{L}_\delta}, \tag{4.1.2}$$

where $\omega(d)$ denotes as usual the number of prime divisors of d and is in no way connected to the ω defined by (2.5) (this latter will not be used any more).

∘∘ *The G-functions.* We set

$$G_d(z) = \sum_{d|q\leq z}\left(\sum_{d|f|q}\mu(q/f)\frac{f}{|\mathcal{K}_f|}\right) \tag{4.1.3}$$

which is a sum of non-negative terms since the summand can also be written

$$\prod_{\substack{p^\nu\|q\\ p^\nu\nmid d}}\left(\frac{p^\nu}{|\mathcal{K}_{p^\nu}|} - \frac{p^{\nu-1}}{|\mathcal{K}_{p^{\nu-1}}|}\right)\prod_{\substack{p^\nu\|q\\ p^\nu|d}}\frac{p^\nu}{|\mathcal{K}_{p^\nu}|} \tag{4.1.4}$$

We introduce the solution h of $q/|\mathcal{K}_q| = 1 \star h(q)$. It is given explicitly by

$$h(\delta) = \prod_{p^\nu\|\delta}\left(\frac{p^\nu}{|\mathcal{K}_{p^\nu}|} - \frac{p^{\nu-1}}{|\mathcal{K}_{p^{\nu-1}}|}\right) \geq 0. \tag{4.1.5}$$

Introducing h in the expression defining G_d, we get

$$G_d(z) = \sum_{\delta\leq z,[d,\delta]\leq z} h(\delta), \tag{4.1.6}$$

where $[d,\delta]$ stands for the lcm of d and δ. From this expression, we immediately get the following generalisation of a Lemma of van Lint & Richert (cf. [13]):

Lemma 1. *If $\ell|d$ then $G_\ell(z\ell/d) \leq G_d(z) \leq G_\ell(z)$.*

Note that these G-functions have been studied thoroughly in the context of Selberg sieve and the reader will find relevant informations in [8].

∘∘ *Selberg's weights.* We set

$$\lambda_d^* = \frac{d}{|\mathcal{K}_d|}\frac{\sum_{q\leq z/d}\mu(q)}{G_1(z)} \quad \text{and} \quad \lambda_d = (-1)^{\omega(d)}\frac{G_d(z)}{G_1(z)}. \tag{4.1.7}$$

These two sets of weights are solutions of the following extremal problems:

$$\begin{cases} \sum_d \lambda_d^* = 1 \quad , \quad \lambda_d^* = 0 \quad \text{if } d \geq z \\ \text{Main Term of } \sum_{N_0<n\leq N_0+N}\left(\sum_{d/n\in\mathcal{K}_d}\lambda_d^*\right)^2 \quad \text{minimal} \end{cases} \tag{4.1.8}$$

and

$$(4.1.9)\qquad \begin{cases} \lambda_1 = 1 \quad , \quad \lambda_d = 0 \quad \text{if } d \geq z \\ \text{Main Term of } \sum_{N_0 < n \leq N_0+N} \left(\sum_{d/n \in \mathcal{L}_d} \lambda_d \right)^2 \quad \text{minimal.} \end{cases}$$

We go from one problem to the other by using (4.1.2) and the first one is fairly trivial to solve. We note for future use that

$$(4.1.10)\qquad \begin{cases} (-1)^{\omega(d)}\lambda_d = \sum_{d|\ell} \lambda_\ell^* \quad , \quad \lambda_\ell^* = \sum_{\ell|d} \mu(d/\ell)(-1)^{\omega(d)}\lambda_d, \\ \beta(n) = \left(\sum_{d/n \in \mathcal{K}_d} \lambda_d^* \right)^2 \quad , \quad \sum_{d/n \in \mathcal{L}_d} \lambda_d = \sum_{d/n \in \mathcal{K}_d} \lambda_d^*. \end{cases}$$

We refer to [22] and [15] for another exposition and to [6] for related material.

∘∘ *Dimension of the sieve.* It is not the purpose of this note to evaluate the G-functions and we shall only say that we have a sieve of dimension $\kappa \geq 0$ whenever we have

$$(4.1.11)\qquad G_1(z) = C(\mathcal{K}) \operatorname{Log}^\kappa z + \mathcal{O}(\operatorname{Log}^{\kappa-1} z)$$

where $C(\mathcal{K})$ is a positive constant. We refer to [8] and [6] for more details. Though everything we do is made for this case, most of it is valid under more general conditions and holds for infinite dimensional sieves as well. Note that (H_4) is enough to ensure (4.1.11), as shown in [8].

∘∘ *An identity.* We now assume that $\mathcal{K}$ satisfies a condition introduced by Johnsen (cf. [6] and [22]) and which reads

$$(4.1.12)\qquad \begin{array}{l} \forall p \geq 2, \forall \nu \geq 1, \forall a \in \mathcal{K}_{p^\nu} \text{ the quantity } |\{n \in \mathcal{K}_{p^{\nu+1}} \ : \ n \equiv a\,[p^\nu]\}| \\ \qquad \text{is independent of } a. \end{array}$$

Then we have the following identity which generalises already known ones (cf. [1], [14] and [2])

Theorem 4. *Assume $\mathcal{K}$ verifies the Johnsen condition* (4.1.12)*. Let* (φ_n) *be a sequence supported by $\mathcal{K}$ up to the level Q. Then we have*

$$\sum_{q \leq Q} \sum_{a \bmod^* q} \left| \sum_n \varphi_n e(\frac{na}{q}) \right|^2 = \sum_{q \leq Q} G_q(Q) |\mathcal{K}_q| \sum_{b \in \mathcal{K}_q} \left| \sum_{\ell | q} \mu(\frac{q}{\ell}) \frac{|\mathcal{K}_\ell|}{|\mathcal{K}_q|} \sum_{m \equiv b[\ell]} \varphi_n \right|^2$$

where the summation over a is restricted to invertible classe modulo q.

It can be shown that the Johnsen condition is indeed required. Note that in order to be able to handle non-squarefree q, we need to have a proper definition of G_q which comes naturally when studying Selberg sieve with non-squarefree moduli.

Proof. Let us denote by $\Delta(Q)$ the LHS of the equality above. We have

$$\Delta(Q) = \sum_{m,n} \varphi_m \overline{\varphi_n} \sum_{d|m-n} d \sum_{q \leq Q/d} \mu(q)$$

and we recognize the inner summation as being $G_1(Q)|\mathcal{K}_d|\lambda_d^*$. Expressing λ^* in terms of λ, we get

$$\Delta(Q) = \sum_q G_q(Q) \Big\{ \sum_{d|q} \mu(q/d)|\mathcal{K}_d| \sum_{m \equiv n[d]} \varphi_m \overline{\varphi_n} \Big\}.$$

We now define

$$\Theta(q) = |\mathcal{K}_q| \sum_{b \in \mathcal{K}_q} \Big| \sum_{\ell|q} \mu(q/\ell) \frac{|\mathcal{K}_\ell|}{|\mathcal{K}_q|} \sum_{m \equiv b[\ell]} \varphi_n \Big|^2$$

which we expand in

$$\Theta(q) = \sum_{\ell_1,\ell_2|q} \mu(q/\ell_1)\mu(q/\ell_2) \sum_{m,n} \varphi_m \overline{\varphi_n} \frac{|\mathcal{K}_{\ell_1}||\mathcal{K}_{\ell_2}|}{|\mathcal{K}_q|} \sum_{\substack{b \in \mathcal{K}_q \\ b \equiv m[\ell_1] \\ b \equiv n[\ell_2]}} 1.$$

The inner summation is evaluated by appealing to the fact that $\mathcal{K}$ is multiplicatively split: for this sum not to be zero, we need $m \equiv n[(\ell_1,\ell_2)]$. Under this condition b is uniquely determined modulo $[\ell_1,\ell_2]$, and by using the Johnsen condition, we infer that this sum equals $|\mathcal{K}_q|/|\mathcal{K}_{[\ell_1,\ell_2]}|$. By split multiplicativity again, we have

$$|\mathcal{K}_{[\ell_1,\ell_2]}||\mathcal{K}_{(\ell_1,\ell_2)}| = |\mathcal{K}_{\ell_1}||\mathcal{K}_{\ell_2}|.$$

We thus get

$$\Theta(q) = \sum_{d|q} \sum_{m \equiv n[d]} \varphi_m \overline{\varphi_n} |\mathcal{K}_d| \sum_{\substack{\ell_1|q, \ell_2|q \\ (\ell_1,\ell_2)=d}} \mu(q/\ell_1)\mu(q/\ell_2).$$

We only have to compute the inner sum. We have

$$\begin{aligned} \sum_{\substack{\ell_1|q,\ell_2|q \\ (\ell_1,\ell_2)=d}} \mu(q/\ell_1)\mu(q/\ell_2) &= \sum_{r_1|q/d, r_2|q/d} \mu((q/d)/r_1)\mu((q/d)/r_2) \sum_{\substack{\delta|r_1 \\ \delta|r_2}} \mu(\delta) \\ &= \mu(q/d) \end{aligned}$$

as required. □

Note that by using the above Theorem together with the large sieve inequality, we recover the upper bound given by Gallagher in [6] in the spirit of the paper [3] by Bombieri & Davenport.

∘∘ *An improved large sieve inequality.* The first named author is indebted to Professor H. Iwaniec for useful discussions which led to the following result.

Theorem 5. *Assume $\mathcal{K}$ verifies the Johnsen condition* (4.1.12).
Let $(\varphi_n)_{n\leq N}$ be a sequence supported by $\mathcal{K}$ up to the level Q. Then for $Q_0 \leq Q$ we have

$$\sum_{q\leq Q_0}\sum_{a \bmod^* q}\left|\sum_n \varphi_n e(na/q)\right|^2 \leq \frac{G_1(Q_0)}{G_1(Q/Q_0)}\sum_n |\varphi_n|^2(N+Q^2)$$

Proof. Let us call $\Sigma(Q_0)$ the LHS of the inequality to be shown. By Theorem 4.1.2 and using the notation $\Theta(q)$ from its proof, we have

$$\begin{aligned}\Sigma(Q_0) &= \sum_{q\leq Q_0} G_q(Q)\frac{G_q(Q_0)}{G_q(Q)}\Theta(q) \leq \max_{q\leq Q_0}\left(\frac{G_q(Q_0)}{G_q(Q)}\right)\sum_{q\leq Q_0} G_q(Q)\Theta(q)\\ &\leq \max_{q\leq Q_0}\left(\frac{G_q(Q_0)}{G_q(Q)}\right)\sum_{q\leq Q} G_q(Q)\Theta(q) = \max_{q\leq Q_0}\left(\frac{G_q(Q_0)}{G_q(Q)}\right)\Sigma(Q)\end{aligned}$$

and we conclude the proof by applying Lemma 4.1.1. □

∘∘ *Equidistribution of Selberg's weights in arithmetic progressions.* We assume $\mathcal{K}$ satisfies the Johnsen condition (4.1.12). We now define for a coprime to q

$$\begin{aligned}w(a/q) &= \lim_{Y\to\infty}\frac{1}{Y}\sum_{n\leq Y}\left(\sum_{n\in\mathcal{K}_d}\lambda_d^*\right)^2 e(na/q)\\ &= \sum_{q|[d_1,d_2]}\frac{\lambda_{d_1}^*\lambda_{d_2}^*}{[d_1,d_2]}\sum_{b\in\mathcal{K}_{[d_1,d_2]}} e(ab/q)\\ &= \sum_{q|[d_1,d_2]}\frac{\lambda_{d_1}^*\lambda_{d_2}^*}{[d_1,d_2]}|\mathcal{K}_{[d_1,d_2]}|\frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|}\\ &= w_q^\sharp\frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|}\end{aligned}\tag{4.1.13}$$

say. Replacing λ^* by its value, we get

$$\begin{aligned}G_1(z)^2 w_q^\sharp &= \sum_{q|[d_1,d_2]}\frac{(d_1,d_2)}{|\mathcal{K}_{(d_1,d_2)}|}\sum_{d_1|\ell_1\leq z}\sum_{d_2|\ell_2\leq z}\mu(\ell_1/d_1)\mu(\ell_2/d_2)\\ &= \sum_{\ell_1,\ell_2\leq z}\sum_{\substack{d_1|\ell_1, d_2|\ell_2\\ q|[d_1,d_2]}}\frac{(d_1,d_2)}{|\mathcal{K}_{(d_1,d_2)}|}\mu(\ell_1/d_1)\mu(\ell_2/d_2)\end{aligned}$$

i.e.

$$G_1(z)^2 w_q^\sharp = \sum_{\delta\le z} h(\delta) \sum_{\ell_1,\ell_2\le z} \sum_{\substack{\delta|d_1|\ell_1\\ \delta|d_2|\ell_2\\ q|[d_1,d_2]}} \mu(\ell_1/d_1)\mu(\ell_2/d_2) \tag{4.1.14}$$
$$= \sum_{\delta\le z} h(\delta)\rho_z(q,\delta)$$

with

$$\rho_z(q,\delta) = \sum_{\ell_1',\ell_2'\le z/\delta} \sum_{\substack{d_1|\ell_1',d_2|\ell_2'\\ q/(\delta,q)|[d_1,d_2]}} \mu(\ell_1'/d_1)\mu(\ell_2'/d_2)$$

and we now evaluate the inner sum by multiplicativity. Its value is 0 as soon as there is a prime p which divides ℓ_1' or ℓ_2' but not $q/(\delta,q)$. Let then p be a prime such that $p^a\|\ell_1'$, $p^b\|\ell_2'$ and $p^c\|q/(\delta,q)$ with $c\ge 1$. We check successively that the value of the inner sum is 0 if $c\le \max(a,b)-1$, or if $c=\max(a,b)>\min(a,b)\ge 1$. Its value is 1 if $c=\max(a,b)>\min(a,b)=0$ and -1 if $c=a=b$. We can thus write $\ell_1'=q_1q_3$, $\ell_2'=q_2q_3$ with $q=q_1q_2q_3$ and $(q_1,q_2)=(q_1,q_3)=(q_2,q_3)=1$ and the value of the inner sum is $(-1)^{\omega(q_3)}$. Hence

$$\rho_z(q,\delta) = \sum_{\substack{q/(\delta,q)=q_1q_2q_3\\ (q_1,q_2)=(q_1,q_3)=(q_2,q_3)=1\\ \max(q_1q_3\delta,q_2q_3\delta)\le z}} (-1)^{\omega(q_3)}. \tag{4.1.15}$$

Note that $\rho_z(q,\delta)=1$ if $q\delta\le z$ and is 0 if $\sqrt{q\delta}>z$ (since $\max(q_1q_3,q_2q_3)\ge\sqrt{q/\delta}$). Moreover we check that $|\rho_z(q,\delta)|\le 3^{\omega(q/(\delta,q))}$.

If we have a sieve of dimension κ, then recalling (4.1.6), expression (4.1.14) estimated via (4.1.15) and Lemma 4.1.1 yields

$$G_1(z)w_q^\sharp = G_1(z/q) + \mathcal{O}\big(3^{\omega(q)}(G_1(z)-G_1(z/q))\big)$$

which we combine with (4.1.11) to infer the first line of

$$\begin{cases} w_q^\sharp = \frac{1}{G_1(z)}\big(1+\mathcal{O}(3^{\omega(q)}/\operatorname{Log} z)\big), & (q\le z),\\ |G_1(z)w_q^\sharp| \ll 3^{\omega(q)}. \end{cases} \tag{4.1.16}$$

the second line being a direct consequence of (4.1.14)–(4.1.15). For the sake of simplicity, we shall convert the $\mathcal{O}(3^{\omega(q)}/\operatorname{Log} z)$ into $\mathcal{O}_\varepsilon(q^\varepsilon/\operatorname{Log} z)$, valid for any $\varepsilon>0$. The implied constant also depends on $\mathcal{K}$, as far as the asymptotic expression (4.1.11) of G_1 depends on $\mathcal{K}$.

To conclude this part, we consider $\sum_{b\in\mathcal{K}_q} e(ab/q)$. First as an easy application of the chinese remainder theorem, we have

$$\Big|\sum_{b\in\mathcal{K}_q} e(ab/q)\Big| \le \prod_{p^\nu|q}\big(p^\nu - |\mathcal{K}_{p^\nu}|\big). \tag{4.1.17}$$

Next if $c/M = a/q$ with $(a,q)=1$, then note that

$$\frac{1}{|\mathcal{K}_M|}\sum_{b\in\mathcal{K}_M} e(cb/M) = \frac{1}{|\mathcal{K}_q|}\sum_{b\in\mathcal{K}_q} e(ab/q).$$

∘∘ *Distribution of Selberg's weights in arithmetic progressions.* We assume $\mathcal{K}$ satisfies the Johnsen condition (4.1.12) and is of dimension κ (cf. (4.1.11)). We further assume that

$$p^\nu - |\mathcal{K}_{p^\nu}| \le c p^{\nu\xi} \tag{4.1.18}$$

for some $c>0$ and $\xi \in [0,\frac12[$ which implies (see (4.1.13), (4.1.16) and (4.1.17))

$$|G_1(z)w(a/q)| \ll q^{-1/2}. \tag{4.1.19}$$

We then get by using additive characters

$$\begin{aligned}\sum_{n\le X}\Big(\sum_{n\in\mathcal{K}_d}\lambda_d\Big)^2 e(na/q) &= Xw_q^{\#}\frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|} + \mathcal{O}(z^2)\\ &= \frac{X}{G_1(z)}\frac{\sum_{b\in\mathcal{K}_q} e(ab/q)}{|\mathcal{K}_q|} + \mathcal{O}\Big(z^2 + \frac{X\sqrt{q}}{|\mathcal{K}_q|G_1(z)\operatorname{Log} z}\Big)\end{aligned}$$

the last equality comimg from (4.1.16), (4.1.17) and (4.1.18). As an easy consequence, we get

$$\sum_{\substack{n\le X\\ n\equiv b[q]}}\Big(\sum_{n\in\mathcal{K}_d}\lambda_d\Big)^2 = \begin{cases}\frac{X}{G_1(z)|\mathcal{K}_q|} & \text{if } b\in\mathcal{K}_q\\ 0 & \text{else}\end{cases} + \mathcal{O}\Big(z^2 + \frac{X\sqrt{q}}{|\mathcal{K}_q|G_1(z)\operatorname{Log} z}\Big). \tag{4.1.20}$$

∘∘ *Squarefree sieves.* When $\sigma_{p^\nu}^{-1}(\mathcal{K}_{p^{\nu-1}}) = \mathcal{K}_{p^\nu}$ for $\nu\ge 2$ we say that $\mathcal{K}$ is squarefree. We are then in the usual condition of the (squarefree) Selberg sieve. Note that the Johnsen condition (4.1.12) is automatically satisfied. Under this assumption we have $\mathcal{L}_{p^\nu}=\emptyset$ for $\nu\ge 2$. Note further that, though λ_d is defined and non-zero for squarefree $d\le z$, non-squarefree values of d do not occur in (4.1.9) if $\mathcal{K}$ is squarefree. In particular $w(a/q)=0$ if q is not squarefree which can be seen in two ways: by replacing λ_d^* by λ_d in (4.1.13) or by noticing that by the chinese remainder theorem $\sum_{b\in\mathcal{K}_q} e(ab/q) = 0$. In particular (H_4) is enough in this case to claim (4.1.19) and (4.1.20). We finally refer to [6] for examples of non-squarefree sieves.

∘∘ *Fourier expansion of* β. In order to have a confortable setting to evaluate sums of the type $\sum_n \beta(n)F(n)$ where β is defined in (4.1.10), we seek another expression of β as in [16]. We assume (4.1.12). We have

$$\beta(n) = \Big(\sum_{d/n\in\mathcal{K}_d} \lambda_d^*\Big)^2 = \sum_{d_1,d_2} \lambda_{d_1}^*\lambda_{d_2}^* 1_{\mathcal{K}_{[d_1,d_2]}}(n).$$

We now express the inner characteristic function by using additive characters and get

$$\begin{aligned}\beta(n) &= \sum_{d_1,d_2} \frac{\lambda_{d_1}^*\lambda_{d_2}^*}{|\mathcal{K}_{[d_1,d_2]}|} \sum_{a \bmod [d_1,d_2]} e(an/[d_1,d_2]) \sum_{b\in\mathcal{K}_{[d_1,d_2]}} e(-ab/[d_1,d_2]) \\ &= \sum_{d_1,d_2} \frac{\lambda_{d_1}^*\lambda_{d_2}^*}{|\mathcal{K}_{[d_1,d_2]}|} \sum_{q|[d_1,d_2]} \sum_{a \bmod^* q} e(an/q) \sum_{b\in\mathcal{K}_{[d_1,d_2]}} e(-ab/q)\end{aligned}$$

hence we reach the fundamental identity

$$\beta(n) = \sum_{q\le z^2} \sum_{a \bmod^* q} w(a/q)e(an/q). \tag{4.1.21}$$

4.2. An enveloping sieve. We fix a real number $X \ge 1$ and seek an upper bound β for the characteristic function $1_{\mathcal{A}}$ of $\mathcal{A}$ up to X which we can work with in a very explicit way. We recalled in Section 4.1 how Selberg sieve provides such a function.

We define $z = X^{1/s}$, $s \ge s_0$, s_0 being the parameter occuring in the definition of a sufficiently sifted sequence. We consider the bordering system $(\mathcal{L}_d)_d$. If d is not squarefree, we have $\mathcal{L}_d = \emptyset$. We then put (cf. (4.1.7) and (4.1.10))

$$\beta(n) = \Big(\sum_{d/n\in\mathcal{L}_d} \lambda_d\Big)^2, \qquad \lambda_d = \mu(d)G_d(z)/G_1(z), \tag{4.2.1}$$

where (cf. (4.1.3) and (4.1.6))

$$G_d(z) = \frac{d}{|\mathcal{L}_d|} \sum_{d|\ell\le z} \frac{\mu^2(\ell)|\mathcal{L}_\ell|}{|\mathcal{K}_\ell|}. \tag{4.2.2}$$

We thus have for $n \le X$

$$1_{\mathcal{A}}(n) \le 1_{\mathcal{A}_X}(n) + 1_{\mathcal{A}-\mathcal{A}_X}(n) \quad , \quad 1_{\mathcal{A}_X}(n) \le \beta(n). \tag{4.2.3}$$

Recall further the classical estimate (cf. (4.1.11))

$$G_1(z) = C(\mathcal{K})(\operatorname{Log} z)^\kappa + \mathcal{O}\big((\operatorname{Log} z)^{\kappa-1}\big) \tag{4.2.4}$$

for some positive constant $C(\mathcal{K})$. To go further and still following Section 4.1, we define for a coprime to q

$$\begin{aligned} w(a/q) &= \lim_{Y\to\infty} \frac{1}{Y} \sum_{n\le Y} \beta(n) e(na/q) \\ &= \sum_{q|[d_1,d_2]} \frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]} \sum_{b\in\mathcal{L}_{[d_1,d_2]}} e(ab/q). \end{aligned} \tag{4.2.5}$$

We need some information about $w(a/q)$ which are similar to those proved in [16]. By (4.1.15) and (4.1.19) we infer

$$|G_1(z)w(a/q)| \ll_{\mathcal{K},s} q^{-1/2}. \tag{4.2.6}$$

If $q|M$ and $q \le z$, we have

$$G_1(z)w(a/q) = \frac{1}{|\mathcal{K}_M|}\big(1 + \mathcal{O}_{\mathcal{K},s,\varepsilon}(q^{\varepsilon} \operatorname{Log}^{-1} z)\big) \sum_{b\in\mathcal{K}_M} e(ab/M) \qquad (\varepsilon > 0). \tag{4.2.7}$$

In fact, the $\mathcal{O}$-symbol depends also on the parameters ξ and c_2. We shall need this expression with s fixed, $\mathcal{K}$, ξ and c_2 fixed and hence we shall drop most of the dependences, except the one in q in the $\mathcal{O}$-symbol. In Section 4.1 we also established in (4.1.20) that the weighted sequence $(\beta(n))$ is properly distributed in arithmetic progressions and thus

$$\sum_{a\le X, a\in\mathcal{A}_X, a\equiv b[M]} 1 \ll_{\mathcal{K}} \frac{X}{|\mathcal{K}_M|(\operatorname{Log} X)^{\kappa}} \qquad (M \le (\operatorname{Log} z)^2) \tag{4.2.8}$$

for $b \in \mathcal{K}_M$ and provided $s > 2$ (the implied constant may depend on s, but is bounded for all $s \in]s_1, \infty]$, for any $s_1 > 2$). If $b \notin \mathcal{K}_M$, the above sum is 0. We finally recall the following identity (cf. (4.1.21) for a proof)

$$\beta(n) = \sum_{q\le z^2} \sum_{a \bmod^* q} w(a/q) e(an/q). \tag{4.2.9}$$

5. Proof of Theorem 1

In this part, i will always denote an index that ranges $\{1,2\}$. Let us fix a large enough number X. We put $z = X^{\min(1/s_0^{(1)},1/(3s_0^{(2)}))}$ where $s_0^{(i)}$ is the parameter s_0 appearing in (H_3) for $\mathcal{A}_i$. All the constants may depend on the host sequences $\mathcal{A}_i$, and more precisely on the particular choice of parameters being chosen to verify conditions (H_1)—(H_5). We consider two subsequences $\mathcal{A}_i^*$ of $\mathcal{A}_i$ as in Theorem 1. X being fixed, we can replace $\mathcal{A}_i^*$ by $\tilde{\mathcal{A}}_i^* = \mathcal{A}_i^* \cap [1, X/2] \cap \mathcal{A}_{iX}$. This sequence satisfies

$$\frac{X}{k_i(\operatorname{Log} X)^{\kappa_i}} \ll \tilde{A}_i^*(X/2) = |A_i^*| \ll \frac{X}{k_i(\operatorname{Log} X)^{\kappa_i}}. \tag{5.0}$$

To avoid accumulating notations, we shall still use $\mathcal{A}_i^*$ instead of $\tilde{\mathcal{A}}_i^*$. This change is of no consequence since $\tilde{\mathcal{A}}_i^*$ is at most a constant time sparser than $\mathcal{A}_i^*$. Define

$$r_2(n) = \sum_{\substack{a_1+a_2=n\\ a_i\in\mathcal{A}_i^*}} 1. \tag{5.1}$$

We have readily

$$\sum_{n\le X} r_2(n) = |\mathcal{A}_1^*||\mathcal{A}_2^*| \gg \frac{X^2}{k_1k_2(\operatorname{Log} X)^{\kappa_1+\kappa_2}} \tag{5.2}$$

where the implied constant depends only on the ones appearing in (5.0). Define

$$\delta = \delta(X) = \frac{1}{X}\sum_{\substack{n\le X\\ r_2(n)\neq 0}} 1. \tag{5.3}$$

We have

$$\begin{aligned}\left(\frac{X^2}{k_1k_2(\operatorname{Log} X)^{\kappa_1+\kappa_2}}\right)^2 &\ll \big(\sum_{n\le X} r_2(n)\big)^2 \le 2\delta X\sum_{n\le X} r_2(n)^2\\ &\ll \delta X \sum_{a_1-a_1'+a_2-a_2'=0} 1.\end{aligned}$$

Define

$$T_i(\alpha) = \sum_{a_i\in\mathcal{A}_i^*} e(a_i\alpha), \tag{5.4}$$

Loosening the condition $a_1\in\mathcal{A}_1^*$ into $a_1\in\mathcal{A}_{1X}$ and sieving the resulting a_1 by the process described in Section 3 (cf. (4.2.9)), we get

$$\begin{aligned}\sum_{a_1-a_1'+a_2-a_2'=0} 1 &\le \sum_{a_1',a_2,a_2'} \beta(a_1'-a_2+a_2')\\ &\le \sum_{d\le z^2}\sum_{a \bmod^* d} w(a/d)e\big((a_1'-a_2+a_2')a/d\big)\\ &\le \sum_{d\le z^2}\sum_{a \bmod^* d} w(a/d)|T_2(a/d)|^2T_1(a/d)\end{aligned}$$

where $w(a/q)$ depends on z and $\mathcal{K}^{(1)}$, where $\mathcal{K}^{(i)}$ is the compact corresponding to $\mathcal{A}_i$. We thus have reached the inequality

$$\frac{X^3}{\delta k_1^2k_2^2(\operatorname{Log} X)^{2(\kappa_1+\kappa_2)}} \ll \sum_{d\le z^2}\sum_{a \bmod^* d} w(a/d)|T_2(a/d)|^2T_1(a/d) \tag{5.5}$$

where the implied constant depends only on the ones appearing in (5.0). The improved large sieve inequality (Theorem 4.1.13) gives us

$$(5.7)\quad \sum_{d\le D}\sum_{a \bmod^* d} |T_2(a/d)|^2 \ll_{\mathcal{A}_2} \left(\frac{\operatorname{Log} D}{\operatorname{Log}(X^{1/s_0^{(2)}}/D)}\right)^{\kappa_2} T_2(0)(X+X^{2s_0^{(2)}})$$

for any $D < X^{1/s_0^{(2)}}$. In our case D is at most z^2 which is not more than $X^{2/(3s_0^{(2)})}$, so that $\operatorname{Log}(X^{1/s_0^{(2)}}/D) \ge (\operatorname{Log} X)/(3s_0^{(2)})$. Furthermore, we have assumed that $s_0^{(2)} \ge 2$, so that (5.7) implies

$$(5.8)\qquad \sum_{d\le D}\sum_{a \bmod^* d} |T_2(a/d)|^2 \ll_{\mathcal{A}_2} \left(\frac{\operatorname{Log} D}{\operatorname{Log} X}\right)^{\kappa_2} T_2(0)X \quad (\forall D < z^2).$$

Introduce $M = \prod_{p\le\lambda} p$. Using the bounds $|(\operatorname{Log} X)^{\kappa_1} w(a/d)| \ll d^{-0.5}$ (cf. (4.2.6)), $|T_1(a/d)| \le T_1(0)$, and (5.8), we get

$$\begin{aligned}\sum_{\substack{d\le z^2\\ d\nmid M}}\sum_{a \bmod^* d} &|w(a/d)||T_2(a/d)|^2|T_1(a/d)| \\ &\le \sum_{\lambda<d\le z^2}\sum_{a \bmod^* d} |w(a/d)||T_2(a/d)|^2|T_1(a/d)| \\ &\ll \frac{X}{k_1(\operatorname{Log} X)^{\kappa_1}}\frac{X}{k_2(\operatorname{Log} X)^{\kappa_2}}\left(\frac{\operatorname{Log}\lambda}{\operatorname{Log} X}\right)^{\kappa_2}\frac{X}{\lambda^{0.5}(\operatorname{Log} X)^{\kappa_1}}\end{aligned}$$

where this time the implied constant depends on $\mathcal{A}_1$ and $\mathcal{A}_2$ and on all the parameters defining them as sufficiently sifted sequences. Since $\delta \le 1$, we can take $\lambda = k_1^3 k_2^3$, and get

$$(5.9)\qquad \frac{X^3}{\delta k_1^2 k_2^2 (\operatorname{Log} X)^{2(\kappa_1+\kappa_2)}} \ll \sum_{d|M}\sum_{a \bmod^* d} w(a/d)|T_2(a/d)|^2 T_1(a/d)$$

and we are thus left with a finite problem. We can furthermore replace $w(a/d)$ by its asymptotic expression (4.2.7) with admissible error term

$$\mathcal{O}_\varepsilon\left(\frac{M^\varepsilon}{\operatorname{Log}^{1+\kappa_1} X}\frac{X}{k_1 \operatorname{Log}^{\kappa_1} X}\frac{MX^2}{|\mathcal{K}_M^{(2)}|\operatorname{Log}^{2\kappa_2} X}\right)$$

got by using $|T_1(a/d)| \le T_1(0)$, Parseval equality on T_2 and (4.2.8) on $\mathcal{K}^{(2)}$, provided

$$(5.10)\qquad M \le \operatorname{Log}^2 z,$$

which we assume. By using (3.4) on $\mathcal{K}^{(2)}$, and bounding M^ε by $M \le \operatorname{Log}^{2\varepsilon} z$, we get that this error term is admissible (i.e. smaller than the RHS of (5.5)) at least if

$$(5.11)\qquad (k_1k_2)^3 \le \operatorname{Log} X, \quad (X \ge X_2(\mathcal{A}_1, \mathcal{A}_2))$$

which we assume. We have reached

$$\frac{X^3}{\delta k_1^2 k_2^2 (\operatorname{Log} X)^{\kappa_1+2\kappa_2}} \ll \sum_{d|M}\sum_{a \bmod^* d} \frac{\sum_{t\in\mathcal{K}_M^{(1)}} e(at/d)}{|\mathcal{K}_M^{(1)}|}|T_2(a/d)|^2 T_1(a/d)$$
$$= \sum_{c \bmod M} \frac{\sum_{t\in\mathcal{K}_M^{(1)}} e(ct/M)}{|\mathcal{K}_M^{(1)}|}|T_2(c/M)|^2 T_1(c/M)$$

This latter sum is a number of representations. Expanding $T_1(c/M)$ and $T_2(c/M)$, we get

$$\frac{X^3}{\delta k_1^2 k_2^2 (\operatorname{Log} X)^{\kappa_1+2\kappa_2}} \ll \frac{M}{|\mathcal{K}_M^{(1)}|} \sum_{\substack{a_2-a_2'-a_1\in\mathcal{K}_M^{(1)}\\ a_2,a_2'\in\mathcal{A}_2^*, a_1\in\mathcal{A}_1^*}} 1$$
$$\ll \frac{M}{|\mathcal{K}_M^{(1)}|} \sum_{\substack{a_2'\in\mathcal{A}_2^*\\ a_2'\le X}} \sum_{\substack{x,y\in\mathbb{Z}/M\mathbb{Z}\\ (x-a_2')+y\in\mathcal{K}_M^{(1)}}} \Big(\sum_{\substack{a_2\in\mathcal{A}_2^*\\ a_2\le X, a_2\equiv x[M]}} 1\Big)\Big(\sum_{\substack{a_1\in\mathcal{A}_1^*\\ a_1\le X, a_1\equiv -y[M]}} 1\Big). \tag{5.12}$$

□ Conclusion. We define

$$\Phi_M(\phi,\psi) = \sum_{x+y\in\mathcal{K}_M^{(1)}} \phi(x)\psi(y). \tag{5.13}$$

Writing

$$T_i(\alpha) = \sum_m t_i(m)e(m\alpha) \tag{5.14}$$

and

$$f(a) = \sum_{m\equiv a[M]} t_1(m)/T_1(0), \qquad g(b) = \sum_{-n\equiv b[M]} t_2(n)/T_2(0), \tag{5.15}$$

the inequality (5.12) reads

$$\frac{X}{\delta k_1 k_2 (\operatorname{Log} X)^{\kappa_2}} \ll \frac{M}{|\mathcal{K}_M^{(1)}|} \sum_{r\in\mathcal{A}_2^*} t_2(r)\Phi_M(f,g_r)$$

where $g_r(x) = g(r-t)$. We have the conditions (cf. (4.2.8) and (5.10))

$$\begin{cases} \sum_{a \bmod M} f(a) = 1\ , \quad 0\le f(a) \le c_6\frac{k_1}{|\mathcal{K}_M^{(1)}|} \\ \sum_{b \bmod M} g_r(b) = 1\ , \quad 0\le g_r(b) \le c_7\frac{k_2}{|\mathcal{K}_M^{(2)}|}. \end{cases} \tag{5.16}$$

We seek an upper bound for $\Phi_M(f,h)$ under (5.16) (replace g_r by h). Let us take a maximal solution (f,h). We first show that we can assume that $f(a) = c_6k_1/|\mathcal{K}_M^{(1)}|$ or 0 except in at most one point and similarly for h. For otherwise, h being fixed, assume $f(a_1)$ and $f(a_2)$ both in the open interval $]0, c_6k/|\mathcal{K}_M^{(1)}|[$ and that $h(a_1)\le h(a_2)$. Increasing $f(a_2)$ by

$\min(-f(a_2)+c_6k/|\mathcal{K}_M^{(1)}|, f(a_1))$ and decreasing $f(a_1)$ by the same amount, we reach a better couple (f,h) while still verifying the constraints.

We thus have

$$\Phi_M(f,h) \ll \frac{k_1k_2}{|\mathcal{K}_M^{(1)}||\mathcal{K}_M^{(2)}|} \max \sum_{a+b\in\mathcal{K}_M^{(1)}, a\in\mathfrak{A}, b\in\mathfrak{B}} 1$$

this latter maximum being taken over the sets $\mathfrak{A}$ of cardinality $\leq 1 + |\mathcal{K}_M^{(1)}|/(c_6k)$ and $\mathfrak{B} \subset \mathbb{Z}/M\mathbb{Z}$ of cardinality $\leq 1 + |\mathcal{K}_M^{(2)}|/(c_7\ell)$. We shall now apply Theorem 3 and first estimate $|\mathcal{K}_M^{(i)}|/M$. By (3.4), we have

$$|\mathcal{K}_M^{(i)}|/M \asymp (\mathrm{Log}\,\lambda)^{-\kappa_i}. \tag{5.17}$$

We then estimate the coefficient η. We have $\mathrm{Log}(M^2/|\mathfrak{A}||\mathfrak{B}|) \ll \mathrm{Log}(3(k_1+k_2))$. We choose $\mathcal{D} = \{p \leq \lambda, p > L\}$. We use (1.1) with $L = \alpha(\mathrm{Log}(k_1+k_2))^{1/(1-2\xi_1)}$ where $\alpha > 0$ is independent of k_1 and k_2 and is being chosen so that $L \leq \lambda$. We finally get

$$\Phi_M(f,h) \ll \frac{|\mathcal{K}_M^{(1)}|}{M}(\mathrm{Log}\,\mathrm{Log}(k_1+k_2))^{\kappa_1}. \tag{5.18}$$

Collecting our estimates, we reach

$$\frac{1}{\delta k_1} \ll (\mathrm{Log}\,\mathrm{Log}(k_1+k_2))^{\kappa_1} \tag{5.19}$$

as required.

6. Proof of Corollary 3

We shall need two parameters M so we change at once the notations of Corollary 3. We shall work with $\mathcal{K}_N^*$ with $N = \prod_{p\leq\mu}$.

If $k \geq \mathrm{Log}\,\mu$ then Theorem 2 readily implies Corollary 3, simply by taking $\mathcal{B}_M = \mathcal{K}_M^*$. If k is smaller, the proof is more difficult and is in fact pretty similar to the one required for Theorem 1. Let $\mathcal{A}_1^* = \mathcal{A}_2^*$ being the lift of $\mathcal{K}_N^*$ over $\mathbb{N}$. Put $X = \mu^2$ and look at intervals of length $X/2$ intersected with $\mathcal{A}_1$. One of these intervals contains more elements than the average density which is $\gg 1/(k(\mathrm{Log}\,\mu)^\kappa)$. Discard elements so that the remaining set $\mathcal{B}$ verifies

$$|\mathcal{B}| \asymp \frac{X}{k(\mathrm{Log}\,X)^\kappa}. \tag{6.1}$$

Now (6.1) is the equivalent of (5.0) and the proof of Section 5 can be pursued with $\mathcal{B} = \tilde{\mathcal{A}}_i^*$, the only difference being that we sieve an interval which does not start at 1. This of no consequence whatsoever while sieving intervals.

However, we cannot let X be as large as need be and we have to control its size in terms of $k_1 = k$ and $k_2 = k$. The two conditions are (5.10) and (5.11). They read

$$\begin{cases} k^6 = (k_1k_2)^3 = \lambda \ll \mu^2, \\ k^6 = (k_1k_2)^3 \ll \mu. \end{cases}$$

This is more than enough since we had a proof already for $k \geq \operatorname{Log}\mu$.

7. Counterexamples

We give here examples pertaining to the optimality of our results. To do so first note that Corollary 1 applies only when $\mathcal{A}$ is an asymptotic basis, hence there exist a_1, a_2 in $\mathcal{A}$ that are coprime. Next consider $m = \prod_{p\leq\lambda} p = \exp(\lambda(1+o(1)))$. For a sufficiently sifted sequence $\mathcal{A}$, we have

$$\begin{cases} r(X) + \sum_{\overline{a}_0\in\mathcal{K}_m} \left|\{a\in\mathcal{A}, a\leq X, a\equiv\overline{a}_0[m]\}\right| \geq c_4X(\operatorname{Log}X)^{-\kappa}, \\ c_5X(\operatorname{Log}X)^{-\kappa}/|\mathcal{K}_m| \geq \left|\{a\in\mathcal{A}, a\leq X, a\equiv\overline{a}_0[m]\}\right|, \end{cases}$$

the latter inequality following from (4.2.8). If we chose $X_2 \geq X_0$ such that $c_4X(\operatorname{Log}X)^{-\kappa} - r(X) \geq \frac{1}{2}c_4X(\operatorname{Log}X)^{-\kappa}$ as soon as $X \geq X_2$, and select a positive real c number strictly less than $c_4/2$ (which is $\leq c_5$), we infer that the set defined by

$$\tilde{\mathcal{K}}_m = \Big\{\overline{a}_0\in\mathcal{K}_m, \forall X\geq X_2, \\ \left|\{a\in\mathcal{A}, a\leq X, a\equiv\overline{a}_0[m]\}\right| \geq cX(\operatorname{Log}X)^{-\kappa}/|\mathcal{K}_m|\Big\}$$

verifies

$$|\tilde{\mathcal{K}}_m| \gg |\mathcal{K}_m|.$$

We then select $\overline{a}_0 \in \tilde{\mathcal{K}}_m$ and take

$$\mathcal{A}^* = \{a_1, a_2\} \cup \{a\in\mathcal{A}, a\equiv\overline{a}_0[m]\}.$$

We have $|A^*(X)| \geq cX(\operatorname{Log}X)^{-\kappa}/|\mathcal{K}_m|$ and $\mathcal{A}^*$ is an asymptotic basis (by our Theorem) of order at least m. Translating these bounds in terms of $k = |\mathcal{K}_m|$, we see that the order of $\mathcal{A}^*$ is $\gg k(\operatorname{Log}\operatorname{Log}k)^\kappa$.

To deal with the optimality of Corollary 2, we use a remark which we own to D. R. Heath-Brown: by Theorem 1, $\mathcal{B} = \mathcal{A}^* + \mathcal{A}^*$ is of positive density $\gg 1/(k(\operatorname{Log}\operatorname{Log}(3k))^\kappa) = 1/\ell$ and the inverse of the lower density of $\mathcal{B}+\mathcal{A}^*$ is an upper bound for the order of $\mathcal{A}^*$, the optimality of Corollary 1 thus implies the optimality of Corollary 2, at least when $\ell = ck(\operatorname{Log}\operatorname{Log}(3k))^\kappa$. Theorem 3 is optimal for the same reason.

For similar reasons, Theorem 2 and Corollary 3 are optimal.

References

[1] M.B. BARBAN, *The "large sieve" method and its application to number theory*, (Russian). Uspehi Mat. Nauk **21** (1966), 51–102.

[2] E. BOMBIERI *Le grand crible dans la théorie analytique des nombres.* Astérisque **18** (1987).

[3] E. BOMBIERI, H. DAVENPORT, *On the large sieve method.* Abh. aus Zahlentheorie und Analysis zur Erinnerung an Edmund Landau, Deut. Verlag Wiss., Berlin (1968), 11–22.

[4] J. BRÜDERN, A. PERELLI, *The addition of primes and power* Can. J. Math. **48** (1996), 512–526.

[5] P. X. GALLAGHER, *The large sieve.* Mathematika **14** (1967), 14–20.

[6] P. X. GALLAGHER, *Sieving by prime powers.* Acta Arith. **24** (1974), 491–497.

[7] G. GREAVES, *On the representation of a number in the form $x^2+y^2+p^2+q^2$ where p and q are primes.* Acta Arith. **29** (1976), 257–274.

[8] H. HALBERSTAM, H. E. RICHERT, *Sieves methods.* London Mathematical Society Monographs **4**, Academic Press, London-New York, 1974.

[9] H. HALBERSTAM, K. F.ROTH, *Sequences*, Second edition. Springer-Verlag, New York-Berlin, 1983.

[10] K. H. INDLEKOFER, *Scharfe Abschätchung für die Anzahlfunction der B-Zwillinge.* Acta Arith. **26** (1974/75), 207–212.

[11] H. IWANIEC *Primes of the type $\varphi(x,y)+A$ where φ is a quadratic form.* Acta Arith. **21** (1972), 203–234.

[12] Y. V. LINNIK, *The large sieve.* C. R. (Doklady) Acad. Sci. URSS (N.S.) **30**(1941), 292–294.

[13] J. E. VAN LINT, H. E. RICHERT, *On primes in arithmetic progressions* Acta Arith. **11** (1965), 209–216.

[14] H. L. MONTGOMERY, *Topics in Multiplicative Number Theory.* Lecture Notes in Math. **227**, Springer-Verlag, Berlin-New York, 1971.

[15] Y. MOTOHASHI, *Lectures on sieve methods and prime number theory.* Tata Institute of Fundamental Research Lectures on Mathematics and Physics **72**, Published for the Tata Institute of Fundamental Research, Bombay; by Springer-Verlag, Berlin, 1983.

[16] O. RAMARÉ, *On Snirel'man's constant.* Ann. Scu. Norm. Pisa **21** (1995), 645–706.

[17] N. P. ROMANOFF, *Über einige Sätze der additiven Zahlentheorie.* Math. Ann. **109** (1934), 668–678.

[18] I. Z. RUZSA, *On an additive property of squares and primes.* Acta Arith. **49** (1988), 281–289.

[19] I. Z. RUZSA, *Essential Components.* Proc. London Math. Soc. **34** (1987), 38–56.

[20] A. SÁRKÖZY, *On finite addition theorems.* Astérisque **258** (1999), 109–127.

[21] L. G. SCHNIRELMAN, *Über additive Eigenschaften von Zahlen.* Math. Annalen **107** (1933), 649–690.

[22] A. SELBERG, *Remarks on multiplicative functions.* Number theory day (Proc. Conf., Rockefeller Univ., New York, 1976), 232–241, Lecture Notes in Math. **626**, Springer, Berlin, 1977.

Olivier RAMARÉ
UFR de Mathématiques URA CNRS 751
Université de Lille 1
59655 Villeneuve d'Ascq Cedex
France
E-mail : `ramare@agat.univ-lille1.fr`

Imre Z. RUZSA
Mathematical Institute
Hungarian Academy of Sciences
Budapest, Pf. 127, H-1364
Hungary
E-mail : `ruzsa@math-inst.hu.fr`