# Rudin Inequality, Chang Theorem, primes and squares

Olivier Ramaré

January 9, 2025

*Dedicated to George Andrews and Bruce Berndt for their $85^{th}$ birthdays*

**Abstract**

We prove that the set of large values of the trigonometric polynomial over a subset of density of the primes has some additive structure, similarly to what happens for subsets of densities in $\mathbb{Z}/N\mathbb{Z}$ but in a weaker form. To do so, we prove large sieve inequalities for *dissociate sets* $\mathcal{X}$ of circle points and functions $f$ whose support $S$ is finite and respectively in an interval, in the set of primes or in the set of squares. Set $T(f,x) = \sum_n f(n)\exp(2i\pi nx)$. These inequalities are of the shape $\sum_{x\in\mathcal{X}} |T(f,x)|^2 \ll |S|\|f\|_2^2 \log(8R/|S|)$ where $R$ is respectively $N$, $N/\log N$ and $\sqrt{N}$. The implied constants depend on the spacement between sumsets of $\mathcal{X}$.

## 1 Introduction and results

One of the main outcome of the present paper is that the set of large values of the trigonometric polynomial over a subset of density of the primes has some additive structure, similarly to what happens for subsets of densities in $\mathbb{Z}/N\mathbb{Z}$. In the case of squares, which is extreme with respect to the method employed, we reach only an improved large sieve inequality.

Such a property has been proved for dense subsets of integers by M. Chang [5] as a consequence of an inequality attributed to W. Rudin, explaining our title; the setting generally employed is the one of finite abelian groups, see for instance the survey paper [8] by B. Green or the book [24] by T. Tao & V.H. Vu. We consider here subsequences of the primes from $[1,N]$ and want to rely on sieve techniques. These rely crucially on the fact that the primes are invertible (if we omit the initial ones) in $\mathbb{Z}/q\mathbb{Z}$ for any $q \le \sqrt{N}$; this fact is not naturally expressible inside $\mathbb{Z}/\mathcal{O}(N)\mathbb{Z}$, so we first establish some results on integer sequences lying in $[1,N]$. These are not new in spirit, though some constants may be improved with respect to the published ones. The author does not know of any ancestors to the case of primes and of squares that is examined later.

A main definition on this query comes from harmonic analysis. In accordance with the book [10, Definition 2.5] by J. López & K. Ross, a finite set $\mathcal{X} \subset \mathbb{R}/\mathbb{Z}$ is called *dissociate* when the equation $\sum_{x\in\mathcal{X}} \epsilon(x)x = 0$ has no non-trivial solution with $(\epsilon(x)) \in \{0,\pm 1\}^{\mathcal{X}}$; a natural example is the set $\{\frac{1}{U}, \frac{2}{U}, \cdots, \frac{2^H}{U}\}$ for some

positive integers $U$ and $H$. We present more methological and historical points below. An inequality of Rudin involving such sets of points and that is usually traced to [19] plays an important role in our proof. The paper [23] by I. Shkredov has a very informative first part with many references and may be used as an introduction to the subject. We somehow displace the center of gravity of the questions at hand towards an improved large sieve inequality over such sets. The usual large sieve inequality says that (see [11] by H.L. Montgomery), for any finite subset $\mathcal{X} \subset \mathbb{R}/\mathbb{Z}$, we have

$$\sum_{x\in\mathcal{X}} \Big| \sum_{n\leq N} f(n)e(nx)\Big|^2 \leq (N+\delta^{-1})\,\|f\|_2^2 \tag{1}$$

where $\|f\|_2^2 = \sum_b |f(n)|^2$, $e(y) = \exp(2i\pi y)$ and

$$\delta = \min\big\{\|x-x'\|_{\mathbb{R}/\mathbb{Z}} : x, x' \in \mathcal{X}, x \neq x'\big\}. \tag{2}$$

Notation $\|u\|_{\mathbb{R}/\mathbb{Z}}$ stands for the distance on the unit circle, i.e.

$$\|u\|_{\mathbb{R}/\mathbb{Z}} = \min_{k\in\mathbb{Z}} |u-k|. \tag{3}$$

In the case of applications, we have $\delta \gg 1/N$. By assuming a quantitative separation condition on the points of $\mathcal{X}$, namely that $\delta_\star \gg 1/N$, where $\delta_\star$ is defined in (4), we prove the improved large sieve like inequality given in Theorem 1.1. It is stronger in that, in essence, we replace the $N+\delta^{-1}$ above by the length of the support of $f$.

When working over finite abelian groups, say over $\mathbb{Z}/U\mathbb{Z}$, it is enough to use the condition that all the sumsets of $\mathcal{X}$ are distincts. In the case of an interval, and since we do not restrict our attention to circle points of the shape $u/U$, the quantitative information provided to us by $\delta_\star$ is needed.

For primes, we require a stronger and more arithmetical quantity, namely $\delta_*(z, z_0)$ defined in (5). For intervals, the linear forms in the points of $\mathcal{X}$ with coefficients $\{0, \pm 1\}$ had to be away from 0. We now need these forms to be away from any rational $a/q$ with a not-too-large denominator. Of course asking for $\delta_*(z, z_0) > 0$ is stronger than asking that $\delta_\star > 0$, but applications ask in fact for $\delta_*(z, z_0) \gg 1/N$ which is this time much stronger than the condition $\delta_\star \gg 1/N$. We show in Corollary 1.3 below how to treat this requirement geometrically. The parameter $z_0$ is included to allow some small prime factors in $U$. Having this parameter $\delta_*(z, z_0)$ at hand, we prove two improved large sieve inequalities that link dissociate sets on one side and subset of density either of primes or of squares on the other side. Notice that this means a two-fold saving: first we need to save the density of the primes (or of the squares) with respect to the integers as in [6] by B. Green & T. Tao and more efficiently in [17], and then the relative density of the support of $f$ with respect to the primes (or to the squares).

This is achieved by using an *enveloping sieve*, as developed in [12], in [16] and in [15] (see also [14] for a reminder). We further employ a Fourier analytic device (Lemma 3.1) to reduce the arithmetical input to a minimum (in the proof of Theorem 1.2 and 1.5, we evaluate only a density and do not have to handle any error term). The enveloping sieve for the squares is much less used, so we spend some time putting it in place.

## The case of intervals

We proceed by producing a general enough proof than will prove at the same time several Rudin's like inequalities, infer a large sieve inequality from a dual version of it and deduce a Chang's theorem from there. We first prove an interval version.

**Theorem 1.1.** *Let $\mathcal{X} \subset \mathbb{R}/\mathbb{Z}$ be a finite set. Let*

$$\delta_\star = \min\Big\{ \Big\| \sum_{x\in\mathcal{A}} x - \sum_{x\in\mathcal{B}} x \Big\|_{\mathbb{R}/\mathbb{Z}} : \mathcal{A} \neq \mathcal{B} \subset \mathcal{X} \Big\}. \tag{4}$$

*Assume that $\delta_\star > 0$. When $f$ has support inside $S \subset \{1,\dots,N\}$, we have*

$$\sum_{x\in\mathcal{X}} \Big| \sum_{n\le N} f(n) e(nx) \Big|^2 \le 9\,|S|\,\|f\|_2^2\,\log\frac{8(N+\delta_\star^{-1})}{|S|}.$$

*More generally, for any real number $\ell \ge 1$, we have*

$$\Big( \sum_{x\in\mathcal{X}} \Big| \sum_{n\le N} f(n) e(nx) \Big|^{\ell+1} \Big)^2 \le 9\,|S|\,\|f\|_2^2 \sum_{x\in\mathcal{X}} \Big| \sum_{n\le N} f(n) e(nx) \Big|^{2\ell} \log\frac{8(N+\delta_\star^{-1})}{|S|}.$$

Let us compare with the large lieve inequality (1): we have here $|S|\log\frac{8N}{|S|}$ instead of $N$, on assuming that $\delta_\star \gg 1/N$. The dependence in $\mathcal{X}$ is however much worse. The parameter $\delta_\star$ is absent from the theory developed on finite abelian groups. See Corollary 1.3 for a result without this parameter. The corresponding Rudin's inequality is given in Lemma 2.3.

I. Shkredov establishes in [23, Theorem 1.3] the analogous of the inequality with $\ell$, save that he requires the condition $\ell \ge 2$ that we can wave in our proof. The $\ell$-part for $\ell > 2$ may also be proved by using the case $\ell = 2$: we apply the Cauchy inequality to the scalar product $\langle u|v\rangle = \sum_x |T(f,x)|^2 u(x)\overline{v(x)}$ and the variables $u = \mathbb{1}$ and $v = |T(f,x)|^{\ell-1}$, where $T(f,x) = \sum_n f(n)\exp(2i\pi nx)$. Though we do not specify it, the extension to $\ell \ge 1$ is valid for Theorem 1.2 and 1.5 and for Corollary 1.3.

## The case of primes

Here our first main result, namely the counterpart of Theorem 1.1 for primes.

**Theorem 1.2.** *Let $\mathcal{X} \subset \mathbb{R}/\mathbb{Z}$ be a finite set. Let $N \ge z_0 \ge 2$ be two parameters and define $P(z_0) = \prod_{p<z_0} p$. We set*

$$\delta_*(z,z_0) = \min\Big\{ \Big\| \sum_{x\in\mathcal{A}} x - \sum_{x\in\mathcal{B}} x - \frac{a}{q} \Big\|_{\mathbb{R}/\mathbb{Z}} : \mathcal{A} \neq \mathcal{B} \subset \mathcal{X}, a \in \mathbb{Z}, q \le z, (q, P(z_0)) = 1 \Big\}. \tag{5}$$

*Let $\kappa \in (0, 1/2]$. Assume that $\delta_*(N^\kappa, z_0) > 0$. For any function $f$ with support inside a subset $S$ of the primes of $\{N^\kappa,\dots,N\}$, we have*

$$\sum_{x\in\mathcal{X}} \Big| \sum_{p\le N} f(p) e(xp) \Big|^2 \le c(\kappa)|S|\,\|f\|_2^2\,\log\frac{8N}{|S|\log N}.$$

*where*

$$c(\kappa) = 9\frac{\log\Big(64\frac{N+\delta_*^{-1}(N^\kappa,z_0)}{\kappa|S|\log N}\log z_0\Big)}{\log\frac{8N}{|S|\log N}}.$$

The corresponding inequality in [17] has essentially $N(\log N)^{-1}\log|\mathcal{X}|$ when the above with $z_0 = 2$ has $N(\log N)^{-1}(\log K)/K$, with $K = N/(|S|\log N)$. On assuming that $c$ is indeed bounded above (i.e. that $\delta_*(\sqrt{N}, z_0) \gg 1/N$), the saving is thus two-fold: we save (almost all) the relative density $K$ of the subset $|S|$ and the $\log|\mathcal{X}|$.

This result is more easily read on rational circle points with a denominator with a large prime divisor, where we recover the group structure on one component. Here is a sample result.

**Corollary 1.3.** *Let $N \geq 2$ and let $U \geq N$ be an integer with a prime divisor $U_1 \in [N^{1/4}, N^{3/4}]$. Let $\mathcal{U} \subset \mathbb{Z}/U\mathbb{Z}$ all whose sumsets modulo $U_1$ are distinct. For any function $f$ with support inside a subset $S$ of the primes of $\{N^{1/4}, \dots, N\}$, we have*

$$\sum_{u\in\mathcal{U}}\Big|\sum_{p\leq N} f(p)e\Big(\frac{up}{U}\Big)\Big|^2 \leq 30\,|S|\,\|f\|_2^2\,e^{U/N}\,\log\frac{8N}{|S|\log N}.$$

From the facts that the number of subsets of $\mathcal{U}$ is $2^{|\mathcal{U}|}$ and that each such subset corresponds to only one sum modulo $U_1$, we infer that $|\mathcal{U}| \leq (\log U_1)/\log 2$. This bound is optimal as the example $\{1, 2, \cdots, 2^H\}$ shows. We may also replace $e^{U/N}$ by $e^{U/(N\log 8K)}$; we chose simplicity.

Here is now a results in the line of M. H. Chang in [5, Lemma 3.1], but for dense prime subsets.

**Theorem 1.4** (Chang's theorem for primes)**.** *Let $N \geq 2$ and let $U_1$ and $U_2$ be two distinct primes such that $U_1, U_2 \in [N^{1/4}, N^{3/4}]$. Set $U = U_1U_2$. Let $S$ be a subset of the primes of $\{N^{1/4}, \dots, N\}$ and let $A \geq 1$ be given. Set $K = N/(|S|\log N)$. For $i \in \{1, 2\}$, there exists $\mathcal{D}_i \subset \mathbb{Z}/U_i\mathbb{Z}$ of cardinality at most $30A^2\log(8K)e^{U/N}$ such that*

$$\Big\{u \in \mathbb{Z}/U\mathbb{Z} : \Big|\sum_{p\in S} e(pu/U)\Big| \geq |S|/A\Big\} \subset \prod_{i=1}^{2}\Big\{\sum_{a\in\mathcal{D}_i}\epsilon(a)a : (\epsilon(a)) \in \{0, \pm 1\}^{\mathcal{D}_i}\Big\}.$$

It is a consequence of the material exposed in [17] that, in case $U \ll N$, the set on the left hand side, say $\mathscr{C}$, has cardinality at most $\mathcal{O}(A^2K\log 2A)$. The above theorem therefore exhibits some non-trivial additive structure of the set $\mathscr{C}$ when $A$ is small with respect to $K$. The set $\mathcal{D}$ may indeed be smaller in size than $\mathscr{C}$, though the set of the right-hand side above may have cardinality $9^{\mathcal{O}(A^4\log^2(8K))}$.

Let us end this part with a counter-example that explains why we do not restrict our attention to a dissociate set $\mathcal{D}_1 \times \mathcal{D}_2$. The projection of the dissociate set $\mathcal{D} = \{(1,1), (1,4), (3,2), (3,3)\} \subset \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ on $\mathbb{Z}/5\mathbb{Z}$ is the dissociate set $\{1, 3\}$, but there are not dissociate subset $\mathcal{A}$ of $\mathbb{Z}/6\mathbb{Z}$ such that $\mathcal{D} \subset \{1, 3\} \times \mathcal{A}$.

## The case of squares

Theorem 1.2 can immediately be generalized to any sieve context of finite dimension, as in [6] by B. Green & T. Tao. As it turns out, the Selberg sieve has

teeth even for sieving squares, and still provides there an upper bound that is only a constant times bigger than expected. This is not the case anymore if we sieve prime squares. All that has been developped and used in [13, Theorem 5.4]. It leads readily to the next theorem.

**Theorem 1.5.** *With hypothesis and notation as in Theorem 1.2 with $z_0 = 2$. For any function $f$ with support inside a subset $S$ of the squares of $\{1, \dots, N\}$, we have*

$$\sum_{x\in\mathcal{X}}\Big|\sum_{n\le\sqrt{N}} f(n)e(xn^2)\Big|^2 \le c|S|\|f\|_2^2\,\log\frac{8\sqrt{N}}{|S|}.$$

*where the quantity $c$ is given by*

$$c = 9\frac{\log\Big(64\frac{N+\delta_*^{-1}(\sqrt{N},2)}{|S|\sqrt{N}}\Big)}{\log\frac{8\sqrt{N}}{|S|}}.$$

The squares in the context of $\Lambda(p)$-sets have been intensively examined. In this extreme case, we need to sieve truely up to $\sqrt{N}$, so we cannot afford a parameter $\kappa$ as in the case of primes, and that ruins any corollary like Corollary 1.3.

## Some methological and historical notes

Following [24, Section 4.5] of the book by T. Tao & V. Vu, we define the $\Lambda(p)$-constant of a subset $S \subset \mathbb{Z}/U\mathbb{Z}$ to be the smallest $K$ such that

$$\Big(\frac{1}{U}\sum_{u \bmod U}\Big|\sum_{s\in S} c(s)e(su/U)\Big|^p\Big)^{1/p} \le K\Big(\frac{1}{U}\sum_{u \bmod U}\Big|\sum_{s\in S} c(s)e(nu/U)\Big|^2\Big)^{1/2}. \tag{6}$$

This inequality should hold for any choice $(c(s))$; $S$ is a subset of the dual group of the initial goup ($X$ in the notation of the reference book [10] by J. López & K. Ross, the initial group being denoted by $G$). Such an inequality is close to what we call a generic Rudin's inequality in Lemma 2.3 below and is generally traced back to [19, Theorem 3.1] by W. Rudin. In harmonic analysis over groups, see for instance Definition 5.2 in [10], a subset $S$ is called a $\Lambda(p)$-set if any such constant exists, but in the finite set context, only an upper bound for the attached constant is meaningful.

When we replace $\mathbb{Z}/U\mathbb{Z}$ by the interval $[1, N]$, it is clear that we stay close to the definition (6), but the counterparts with primes or squares are less readable in this context. The other variable, which is from $\mathcal{X}$ in our notation, comes naturally from the character group of $\mathbb{Z}$, and may be also seen, when containing only rational points, as a subset of the character group of some $\mathbb{Z}/U\mathbb{Z}$. This one corresponds truely to the $s$-variable in (6).

The notion of dissociate set appears only in the 1969-paper [9] by E. Hewitt & H. Zuckerman, about ten years after the Rudin paper. However [19, Theorem 2.4] contains points that shows that a dissociate set is a *Sidon* set. Yet again, the notion of Sidon sets is somewhat difficult in the context of finite structure. One definition used in number theory is that no point of a Sidon set equals to a sum of two points from this set. This is not the notion used harmonic analysis, but there are translations of the harmonic analytic definition in arithmetical context,

see for instance [19, Theorem 2.4] or the book [20, Theorem 5.7.5] again by W. Rudin. Yet again, this definition looses its impact in finite structures if one does not follow the size of the implied finite parts.

The intermediate notion of $\Lambda(p)$-*sets* seems more appropriate in the context of finite sets, save for the caveat that web search engines have difficulties with such a name! We refer to the survey paper [3] by J. Bourgain. In this paper, Eq. (3.7) defines as an *independent* set what appears to be a dissociate set, bar the possibility of characters of order 2. To add to this joyful confusion, it seems modern terminology prefers *dissociated* to *dissociate*.

As we have seen, the notion of dissociate sets which is instrumental in our work appears in earlier work only on the character group side, and the same holds for the notion of Sidon sets. There are deep questions therein concerning squares, dissociate sets and Sidon sets. Our Theorem 1.5 which mixes this kind of conditions on both variables is thus rather new.

### Extensions and acknowledgements

In [4], J. Bourgain proves an extension to Theorem 1.1 to sumsets of a dissociated set. The reader may read [22] by I. Shkredov for a proper introduction to the subject. The possibility of such an extension to the case of primes or of squares are open questions.

We decided to use a rather low-level style of writing so as to be accessible to both communities of number theorists and harmonic analysists. We hope this will be helpful to the readers.

A large part of this work was completed when the author was enjoying the hospitality of the Indian Statistical Institute in Kolkata. It has also has been partially supported by the Indo-French IRL Relax and by the joint FWF-ANR project Arithrand: FWF: I 4945-N and ANR-20-CE91-0006. The author also thanks warmly H. Queffélec and I. Shkredov for their fruitful comments.

## 2 An abstract machinery

We want to prove things on the integers and then mimick the proof to reach corresponding results on the primes. On looking closely, one sees that one input differs and the rest follows.

In this section, we consider a finite sequence $\mathcal{N}$ of integers, a finite sequence $\mathcal{X}$ of points of $\mathbb{R}/\mathbb{Z}$. We assume that there exists a constant $H \geq |\mathcal{N}|$ such that, for every complex sequence $(c(x))_{x\in\mathcal{X}}$, we have

$$\log \sum_{n\in\mathcal{N}} \left| \exp\Big( \sum_{x\in\mathcal{X}} c(x)e(xn) \Big) \right| \leq \tfrac{1}{2} \sum_{x\in\mathcal{X}} |c(x)|^2 + \log H. \tag{Hyp.}$$

**Remark:** On choosing $c(x) = 0$ when $x \neq 0$, for some chosen $x_0$ from $\mathcal{X}$, the above inequality reduces to $-(\frac{1}{2} - c(x_0))^2 + \frac{1}{4} \leq \log H$.

We may deduce distributional inequalities from this hypothesis.

**Lemma 2.1.** *Under the hypothesis (Hyp.), we have*

$$\left| \Big\{ n \in \mathcal{N} : \ \Big| \sum_{x\in\mathcal{X}} c(x)e(nx) \Big| \geq \lambda \sqrt{\sum_{x\in\mathcal{X}} |c(x)|^2} \Big\} \right| \leq 4He^{-\lambda^2/4}.$$

See the second half of [24, Lemma 4.33] by T. Tao & V. Vu. As these inequalities may be compared with the classical Chernoff bound for sums of independent random variables, one may say that this shows the $e(nx)$ behaves "independently".

*Proof.* Let us use Hypothesis $(Hyp.)$ on $\tilde{c}(x) = e(\theta)\sigma\, c(x)$ for a positive parameter $\sigma$ and a phase $\theta$ that we may choose. Set $C = \sum_x |c(x)|^2$. We find that

$$\Big|\big\{n \in \mathcal{N}, \sigma \Re e(\theta) \sum_x c(x)e(nx) \geq \sigma\lambda\sqrt{C}\big\}\Big| \, \exp(\sigma\lambda\sqrt{C}) \leq H \exp(\sigma^2 C/2).$$

On selecting $\sigma = \lambda/\sqrt{C}$, we reach

$$\big|\big\{n \leq \mathcal{N}, \Re e(\theta) \sum_x c(x)e(nx) \geq \lambda\sqrt{C}\big\}\big| \leq He^{-\lambda^2/2}. \tag{7}$$

To infer inequalities on the modulus, let us notice that

$$\max\Big(\big|\Re \sum_x c(x)e(nx)\big|, \big|\Im \sum_x c(x)e(nx)\big|\Big)\sqrt{2} \geq \big|\sum_x c(x)e(nx)\big|.$$

Therefore

$$\begin{aligned}(1/\sqrt{2})\Big|\sum_x c(x)e(nx)\Big| \leq \max\Big(&\Re \sum_x c(x)e(nx), \Re(-1)\sum_x c(x)e(nx),\\ &\Re i\sum_x c(x)e(nx), \Re(-i)\sum_x c(x)e(nx)\Big),\end{aligned}$$

so inequality (7) applies (which $\lambda/\sqrt{2}$ rather than $\lambda$). The lemma is proved. □

**Lemma 2.2.** *When $x > 0$, there exists $\theta \in (0,1)$ such that*

$$|\Gamma(x+1)| = \sqrt{2\pi}|x|^{x+\frac{1}{2}} \exp\Big(-x + \frac{\theta}{12x}\Big).$$

This is from the book [1, (6.1.38)] by M. Abramowitz and I.A. Stegun.

We now turn towards $\mathrm{L}^p$-inequalities. The next one is the very similar, when replacing the summation over a finite abelian group by $n \leq N$, of [23, Theorem 1.1] by I. Shkredov, which this author calls Rudin's inequality.

**Lemma 2.3.** *Under the hypothesis $(Hyp.)$ and for any real number $p \geq 1$, we have*

$$\sum_{n\in\mathcal{N}}\Big|\sum_{x\in\mathcal{X}} c(x)e(nx)\Big|^p \leq 4(\tfrac{9}{5}\sqrt{p})^p H\left(\sum_{x\in\mathcal{X}}|c(x)|^2\right)^{p/2}.$$

In [8, Proposition 1], B. Green proves a resembling inequality on $\mathbb{Z}/N\mathbb{Z}$, with the slightly worse constant $(12\sqrt{p})^p$.

*Proof.* Set $f(n) = \sum_x c(x)e(nx)$ and $F = \sqrt{\sum_x |c(x)|^2}$. We define

$$\mathcal{N}(\lambda) = \big\{n \in \mathcal{N} : |f(n)| \geq \lambda F\big\}$$

as well as $N(\lambda) = |\mathcal{N}(\lambda)|$. Let $0 \le \lambda_1 < \lambda_2 < \cdots < \lambda_K$ be the sequence of values taken by $|f(n)|/F$, and we set $N(\lambda_{K+1}) = 0$ as well as $\lambda_0 = 0$. We readily find that

$$\sum_{n\in\mathcal{N}} |f(n)|^p/F^p = \sum_{k\le K} \lambda_k^p\big(N(\lambda_k) - N(\lambda_{k+1})\big) = \sum_{k\le K} N(\lambda_k)(\lambda_k^p - \lambda_{k-1}^p)$$
$$= \sum_{k\le K} N(\lambda_k) \int_{\lambda_{k-1}}^{\lambda_k} pt^{p-1}dt = \int_0^\infty pN(t)t^{p-1}dt.$$

We may apply Lemma 2.1 to majorize $N(t)$. We are thus led to find an upper bound for $\int_0^\infty pe^{-t^2/4}t^{p-1}dt$. Set $u = t^2/4$, so that $dt = du/\sqrt{u}$, and get that

$$\int_0^\infty pe^{-t^2/4}t^{p-1}dt = 2^{p-1}p\int_0^\infty u^{p/2}e^{-u}du/u = p2^{p-1}\Gamma(p/2)$$
$$= 2^p\Gamma\Big(1+\frac{p}{2}\Big) \le \sqrt{2\pi}2^p(p/2)^{\frac{p+1}{2}}e^{-p/2}e^{1/(6p)}$$
$$\le \sqrt{\pi}2^{p/2}p^{\frac{p+1}{2}}e^{-p/2}e^{1/(6p)} \le (\tfrac{9}{5}\sqrt{p})^p$$

by Pari/GP. □

**Theorem 2.4.** *Under the hypothesis (Hyp.), let $f$ be a function over $\mathcal{N}$ with support inside a given subset $S$. We have*

$$\sum_{x\in\mathcal{X}}\Big|\sum_{n\in\mathcal{N}} f(n)e(nx)\Big|^2 \le 9\,|S|\,\|f\|_2^2\,\log\frac{8H}{|S|}.$$

*More generally, for any real number $\ell \ge 1$, we have*

$$\Big(\sum_{x\in\mathcal{X}}\Big|\sum_{n\in\mathcal{N}} f(n)e(nx)\Big|^{\ell+1}\Big)^2 \le 9\,|S|\,\|f\|_2^2\sum_{x\in\mathcal{X}}\Big|\sum_{n\in\mathcal{N}} f(n)e(nx)\Big|^{2\ell}\log\frac{8H}{|S|}.$$

*Proof.* Let us start, with an obvious notation, from

$$\Big|\sum_x\sum_n f(n)e(nx)g(x)\Big| \le \Big(\sum_n |f(n)|^q\Big)^{1/q}\Big(\sum_n\Big|\sum_x g(x)e(nx)\Big|^p\Big)^{1/p}$$
$$\le \Big(\sum_n |f(n)|^q\Big)^{1/q}\Big(4(\tfrac{9}{5}\sqrt{p})^pH\Big(\sum_x |g(x)|^2\Big)^{p/2}\Big)^{1/p}$$

where Lemma 2.3 was used in the second step. We select $g(x) = \sum_n \overline{f(n)}e(-nx)$ to obtain

$$\sum_{x\in\mathcal{X}}\Big|\sum_{n\in\mathcal{N}} f(n)e(nx)\Big|^2 \le \big(\tfrac{9}{5}\big)^2\Big(\sum_n |f(n)|^q\Big)^{2/q} p\,H^{2/p}.$$

This is the dual form of Lemma 2.3. Let us now use the hypothesis on the support of $f$. We assume that $p > 2$, i.e. $q < 2$. Let us again us the Hölder inequality, this time with exponents $a = 2/q$ and $b$ defined $1/b = 1 - q/2$. We find that

$$\Big(\sum_n |f(n)|^q\Big)^{2/q} \le \sum_n |f(n)|^2|S|^{1-\frac{2}{p}}.$$

Therefore

$$\sum_{x\in\mathcal{X}}\Big|\sum_{n\in\mathcal{N}} f(n)e(nx)\Big|^2 \le \big(\tfrac{9}{5}\big)^2 p(H/|S|)^{2/p}|S|\sum_n |f(n)|^2.$$

The choice $p=\log(8H/|S|)\ge 2$ gives the first inequality. We may also take $g(x)=\sum_n \overline{f(n)}e(-nx)|\sum_n f(n)e(nx)|^{\ell-1}$ for some $\ell\ge 1$. Then we use

$$\Big(\sum_x |g(x)|^2\Big)^{1/2} = \Big(\sum_x\Big|\sum_n f(n)e(nx)\Big|^{2\ell}\Big)^{1/2}.$$

This ends the proof of our theorem. □

# 3 A quantitative version of Rudin's inequality

The handling of the integers from $[1,N]$ will almost exclusively on the next lemma. It is due to A. Selberg, see [21, Section 20] or [25] by J.D. Vaaler.

**Lemma 3.1.** *Let $M\in\mathbb{R}$, and $N$ and $\delta$ be positive real number. There exists a smooth function $\psi$ on $\mathbb{R}$ such that*

- *The function $\psi$ is non-negative.*
- *When $t\in[M,M+N]$, we have $\psi(t)\ge 1$.*
- *$\psi(0)=N+\delta^{-1}$.*
- *When $|\alpha|>\delta$, we have $\hat{\psi}(\alpha)=0$.*
- *We have $\psi(t)=\mathcal{O}_{M,N,\delta}(1/(1+|t|^2))$.*

**Lemma 3.2.** *Under the hypotheses of Theorem 2.3, we have*

$$\log\sum_{n\le N}\Big|\exp\Big(\sum_{x\in\mathcal{X}} c(x)e(xn)\Big)\Big| \le \tfrac{1}{2}\sum_{x\in\mathcal{X}}|c(x)|^2+\log(N+\delta_\star^{-1}).$$

Let us specify that the summation is over positive $n$. We follow the proof of Lemma 4.33 in [24] by T. Tao & V.H. Vu. See also [7, Proposition 17] by B. Green. There are $2^{|\mathcal{X}|}$ subsums $\sum_{x\in\mathcal{A}} x$. As they are suposed to be all distincts in $\mathbb{R}/\mathbb{Z}$, the minimal spacement is at most $2^{-|\mathcal{X}|-1}$.

*Proof.* Let us consider

$$\Sigma=\sum_{n\le N}\Big|\exp\Big(\sum_{x\in\mathcal{X}} c(x)e(xn)\Big)\Big| = \sum_{n\le N}\exp\Big(\Re\sum_{x\in\mathcal{X}} c(x)e(xn)\Big). \tag{8}$$

Let us write $c(x)=|c(x)|e(\theta_x)$. As

$$\forall y\ge 0,\forall t\in[-1,1],\quad e^{ty}\le \operatorname{ch} y + t\operatorname{sh} y, \tag{9}$$

we find that

$$\exp\big(|c(x)|\Re e(xn+\theta_x)\big)\le \operatorname{ch}(|c(x)|)+\operatorname{sh}(|c(x)|)\Re e(xn+\theta_x). \tag{10}$$

We gather these inequalities to reach that $\Sigma$ is bounded above by

$$\sum_{n\in\mathbb{Z}}\psi(n)\prod_{x\in\mathcal{X}}\Big(\mathrm{ch}(|c(x)|)+\tfrac{1}{2}\,\mathrm{sh}(|c(x)|)e(xn+\theta_x)+\tfrac{1}{2}\,\mathrm{sh}(|c(x)|)e(-xn-\theta_x)\Big). \quad (11)$$

Let $(\mathcal{A},\mathcal{B},\mathcal{C})$ range over partitions of $\mathcal{X}$. By using (compare Taylor series)

$$\mathrm{ch}\, y\le e^{y^2/2},$$

we reach

$$\begin{aligned}\Sigma&\le\Big(N+\sum_{(\mathcal{A},\mathcal{B},\mathcal{C})\neq(\emptyset,\emptyset,\mathcal{X})}\delta_\star^{-1}2^{-|\mathcal{A}|-|\mathcal{B}|}\Big)e^{\sum_{x\in\mathcal{X}}|c(x)|^2/2}\\&\le\big(N+\delta_\star^{-1}2^{|\mathcal{X}|}\big)e^{\sum_{x\in\mathcal{X}}|c(x)|^2/2}.\end{aligned}$$

Indeed, we had to sum $\sum_{n\in\mathbb{Z}}\psi(n)e(ny)$ for $y=\sum_{x\in\mathcal{A}}x-\sum_{x\in\mathcal{B}}x\neq 0$. □

*Proof of Theorem 1.1.* Lemma 3.2 is prepared to apply Theorem 2.4 which is precisely what we claimed. □

# 4 Rudin's inequality on primes

We shall handle the primality condition via an enveloping sieve, as initially in [16], but with an additional parameter introduced in [17, Section 4, (8)]. This is more fully described in the future paper [18, Section 3]. As a matter of fact, the reader may proceed without this paramater. It is included only for some applications we have in mind where it will be required. The proof is not more difficult.

We proceed as in the case of integers and establish the following inequality.

**Lemma 4.1.** *Under the hypothesis and notation of Theorem 1.2, we have*

$$\sum_{N^\kappa<p\le N}\Big|\exp\Big(\sum_{x\in\mathcal{X}}c(x)e(xp)\Big)\Big|\le 8\frac{N+\delta_*^{-1}(\sqrt{N},z_0)}{\kappa\log N}(\log z_0)e^{\frac{1}{2}\sum_{x\in\mathcal{X}}|c(x)|^2}.$$

*Proof.* We proceed as in the proof of Lemma 3.2 until we reach (11). There we bound above the characteristic function of the primes by the enveloping sieve of [17, Section 4] with $z=N^{\kappa/2}$. This leads to

$$\begin{aligned}\sum_{(\mathcal{A},\mathcal{B},\mathcal{C})}\prod_{x_a\in\mathcal{A}}\frac{|c(x_a)|}{2}\prod_{x_b\in\mathcal{B}}\frac{|c(x_b)|}{2}\prod_{x_c\in\mathcal{C}}|c(x_c)|\\ \sum_{n\in\mathbb{Z}}\beta_{z_0,z}(n)e\big((x_\mathcal{A}-x_\mathcal{B})n+\theta_\mathcal{A}-\theta_\mathcal{B}\big)\psi(n)\end{aligned}\quad (12)$$

where $x_\mathcal{A}=\sum_{a\in\mathcal{A}}x_a$, similarly for $x_\mathcal{B}$ and $\theta_\mathcal{A}=\sum_{a\in\mathcal{A}}\theta_a$, and similarly for $\theta_\mathcal{B}$, with the notation of (10) and (11). Since $\beta_{z_0,z}(n)=(\sum_{d|n}\lambda_d)^2$, this may also be rewritten as

$$\begin{aligned}\sum_{(\mathcal{A},\mathcal{B},\mathcal{C})}\prod_{x_a\in\mathcal{A}}\frac{|c(x_a)|}{2}\prod_{x_b\in\mathcal{B}}\frac{|c(x_b)|}{2}\prod_{x_c\in\mathcal{C}}|c(x_c)|\\ \sum_{d_1,d_2\le z}\lambda_{d_1}\lambda_{d_2}\sum_{m\in\mathbb{Z}}e\big((x_\mathcal{A}-x_\mathcal{B})m[d_1,d_2]+\theta_\mathcal{A}-\theta_\mathcal{B}\big)\psi([d_1,d_2]m).\end{aligned}$$

Poisson summation formula enables us to rewrite the sum over $m$ in the form

$$\frac{e(\theta_{\mathcal{A}}-\theta_{\mathcal{B}})}{[d_1,d_2]}\sum_{k\in\mathbb{Z}}\hat{\psi}\Big(\frac{k-(x_{\mathcal{A}}-x_{\mathcal{B}})[d_1,d_2]}{[d_1,d_2]}\Big).$$

This shows that this sum sum vanishes when $x_{\mathcal{A}}-x_{\mathcal{B}}\neq 0$ and equals

$$(N+\delta_*^{-1}(z_0,z))\sum_{d_1,d_2\leq z}\frac{\lambda_{d_1}\lambda_{d_2}}{[d_1,d_2]}=\frac{N+\delta_*^{-1}(z,z_0)}{G(z;z_0)} \tag{13}$$

otherwise. We conclude the proof as we did for the one of Lemma 3.2. [17, Lemma 2.6] provides us with a lower bound for $G(z;z_0)$. We thus reach the upper bound

$$\Big(e^{\gamma}\frac{N+\delta_*^{-1}(z,z_0)}{\log z}\log(2z_0)\Big)e^{\frac{1}{2}\sum_x|c(x)|^2}.$$

We notice that $2e^{\gamma}\frac{N}{\log N}\log(2z_0)\leq 8\frac{N}{\log N}\log z_0$. The proof is complete. □

*Proof of Theorem 1.2.* Lemma 4.1 is prepared to apply Theorem 2.4. We obtain the inequality

$$\sum_{x\in\mathcal{X}}\Big|\sum_{p\leq N}f(p)e(px)\Big|^2\leq 9\,|S|\,\|f\|_2^2\,\log\Big(32\frac{N+\delta_*^{-1}(\sqrt{N},z_0)}{\kappa|S|\log N}\log z_0\Big).$$

Theorem 1.2 follows swiftly from there. □

*Proof of Corollary 1.3.* We use Theorem 1.2 with $z_0=2$ and $\kappa=1/4$. We have $\delta_*(N^{\kappa},z_0)>1/(N^{1/4}U_1)\geq 1/U$. Therefore, with $K=\frac{N}{|S|\log N}$, we find that

$$c\leq 9\exp\frac{\log\Big(64\frac{2UK}{N}\log 2\Big)}{\log 8K}\leq 30e^{U/N}.$$

The proof is complete. □

# 5 Proof of Theorem 1.4

*Proof of Theorem 1.4.* Indeed, for $i\in\{1,2\}$, take for $\mathcal{D}_i=\{a_1(i),\cdots,a_{K(i)}(i)\}$ a maximal set inside $\mathscr{C}/U_i\mathbb{Z}\subset\mathbb{Z}/U_i\mathbb{Z}$ that is *dissociate*, i.e. such that all its sumset sums are distinct. Consider the lift of $\mathcal{E}=\mathcal{D}_\infty\times\mathcal{D}_2$ by the Chinese Remainder Theorem map $\varphi:\mathbb{Z}/U_1U_2\mathbb{Z}\to\mathbb{Z}/U_1\mathbb{Z}\times\mathbb{Z}/U_2\mathbb{Z}$. For any $a_k(2)$, the set $\varphi^{-1}(\mathcal{D}_\infty\times\{a_k(2)\})$ satisfies the assumptions of Corollary 1.3, so its cardinality $K(1)$ is bounded by $30A^2\log(8K)e^{U_1U_2/N}$. Any further point $x'\in\mathcal{C}$ has that, for $i\in\{1,2\}$, the set $\{x',a_1(i),\cdots,a_{K(i)}(i)\}/U_i\mathbb{Z}$ is not dissociate, from which the reader will readily conclude that there exists $\mathcal{A},\mathcal{B}\in\mathcal{D}_i$ such that

$$x'+\sum_{x\in\mathcal{A}}x=\sum_{x\in\mathcal{B}}x.$$

The lemma follows swiftly from there. □

# 6 On the Selberg sieve for squares

How to use the Selberg sieve for squares is completely described in the conventional setting in [13, Chapter 11]. The involved quantities are used and evaluated already in [13, Theorem 5.4].

## Pointwise upper bound

We define, for any positive integer $q$, the set $\mathcal{K}_q \subset \mathbb{Z}/q\mathbb{Z}$ ro be the set of squares modulo $q$. For simplicity we restrict our attention to moduli $q$ that are odd and square-free. The function $q \mapsto |\mathcal{K}_q|$ is multiplicative and takes the value $(p+1)/2$ at the prime $p$. We seek real parameters $(\lambda_q^\sharp)_{q\le Q}$ that are such that $\sum_q \lambda_q^\sharp = 1$ and whose support in on odd square-free integers. We chose them so as to optimize the main term in the upper bound:

$$\sum_{\substack{n\le N\\ n \text{ is a square}}} 1 \le \sum_{n\le N}\Big(\sum_{\substack{q\le z\\ n\in\mathcal{K}_q}} \lambda_q^\sharp\Big)^2. \tag{14}$$

This main term is

$$\mathrm{MT} = N\sum_{q_1,q_2\le Q} \frac{|\mathcal{K}_{[q_1,q_2]}|}{[q_1,q_2]}\lambda_{q_1}^\sharp\lambda_{q_2}^\sharp = N\sum_{q_1,q_2\le Q}\frac{(q_1,q_2)}{|\mathcal{K}_{(q_1,q_2)}|}\frac{|\mathcal{K}_{q_1}|\lambda_{q_1}^\sharp}{q_1}\frac{|\mathcal{K}_{q_2}|\lambda_{q_2}^\sharp}{q_2}. \tag{15}$$

We introduce the multiplicative function $h$ which vanishes on non square-free integers and whose value on primes is given by $h(2)=0$ and $h(p)=(p-1)/(p+1)$ when $p$ is an odd prime. This function satisfies the convolution identity

$$\frac{q}{|\mathcal{K}_q|} = \sum_{d|q} h(q)$$

when $q$ is odd and square-free. Therefore

$$\mathrm{MT} = N\sum_{d\le Q} h(d)\Big(\sum_{\substack{q\le z\\ d|q}}\frac{|\mathcal{K}_q|\lambda_q^\sharp}{q}\Big)^2.$$

We are thus led, as in the classical Selberg approach, to a quadratic optimization problem under a linear constraint. We cut the story short and select

$$\lambda_q^\sharp = \frac{q}{|\mathcal{K}_q|}\sum_{\substack{d\le z\\ q|d}}\mu(d/q)/G^\sharp(z), \quad G^\sharp(z)=\sum_{q\le z}h(\delta). \tag{16}$$

We simply check that

$$\begin{aligned} G^\sharp(z)\sum_{q\le z}\lambda_q^\sharp &= \sum_{q\le z}(\mathbb{1}\star h)(q)\sum_{\substack{d\le z\\ q|d}}\mu(d/q)\\ &= \sum_{d\le z}(\mu\star\mathbb{1}\star h)(q) = G^\sharp(Q). \end{aligned}$$

The coefficient $(\lambda_q^\sharp)$ are thus very similar to the Selberg coefficients $(\lambda_d)$ except that are *not* bounded. How to recover the Selberg coefficients from these is described fully in [13, Chapter 11] and in a paragraph below. Both may be skipped here as we shall only use the density $G^\sharp(z)$.

## Fourier decomposition of the sieve

The sets $\mathcal{K}_d$ are subsets of $\mathbb{Z}/d\mathbb{Z}$, which is not apparent in the writing. We now propose a decomposition that makes this point foremost. Here is how it goes:

$$\beta_z(n) = \Big(\sum_{q\le z} \lambda_q^\sharp \mathbb{1}_{\mathcal{K}_q}(n)\Big)^2 = \sum_{q_1,q_2\le z} \lambda_{q_1}^\sharp \lambda_{q_2}^\sharp \mathbb{1}_{\mathcal{K}_{q_1}}(n)\mathbb{1}_{\mathcal{K}_{q_2}}(n).$$

The next step is to notice that $\mathbb{1}_{\mathcal{K}_{q_1}}\mathbb{1}_{\mathcal{K}_{q_2}} = \mathbb{1}_{\mathcal{K}_{[q_1,q_2]}}$ where $[q_1,q_2]$ is the lcm of $q_1$ and $q_2$. We develop this function in Fourier series

$$\mathbb{1}_{\mathcal{K}_q}(n) = \frac{1}{q}\sum_{a \bmod q} \eta(q;a)e(na/q)$$

for some coefficients $\eta(q;a)$. We next introduce *primitive* additive characters via

$$\mathbb{1}_{\mathcal{K}_q}(n) = \sum_{d|q}\sum_{a \bmod^* d} \eta(q;bq/d)e(nb/d)$$

where $b \bmod^* d$ denotes a sum over integers $b$ in $\{1,\cdots,d\}$ that are coprime to $d$. After some shuffling, we reach

$$\beta_z(n) = \sum_{d\le z^2}\sum_{b \bmod^* d} w_d(\mathcal{K},b/d)e(na/d), \tag{17}$$

with

$$w_d(\mathcal{K},b/d) = \sum_{\substack{q_1,q_2\le z\\ d|[q_1,q_2]}} \frac{\lambda_{q_1}^\sharp \lambda_{q_2}^\sharp}{[q_1q_2]}\eta([q_1,q_2];b[q_1,q_2]/d). \tag{18}$$

One could study there coefficients much more but their sole existence will be enough below. We call Eq. (17) the *Fourier expansion* of $\beta$, as in [15, End of subsection 4.1]. The weights $\beta_{z_0,z}(n)$ would be defined in just that same manner but carrying a condition $(q,P(z_0))=1$ throughout. This condition is trivial when $z_0=2$.

## Recovering the usual Selberg coefficients

The material of this subsection is not used in this paper, it is only included for the readers to see properly the connections between different viewpoints.

A classical presentation of the sieve, as for instance in the book [2] by E. Bombieri, starts from sets $\Omega_p \subset \mathbb{Z}/p\mathbb{Z}$ that are to be *avoided*. We then look typicall at the integers $n\le N$ that are so that $n\notin\Omega_p$ for every $p$ into consideration. Reverting to the above notation, we have $\Omega_p = \mathbb{Z}/p\mathbb{Z}\setminus\mathcal{K}_p$. In [13], we extended the notion of $(\Omega_p)$ to $(\Omega_q)$, where $q$ is any modulus, called this one the *bordering sytem* and in fact denoted it by $(\mathcal{L}_q)$. But let us stick in this short presentation to the notation $\Omega_q$. The set $\Omega_q$ is simply obtained[1] by glueing together the $\Omega_p$ for $p|q$ via the Chinese remainder Theorem, but $n\notin\Omega_p$

[1] This is because we restrict our attention to square-free moduli $q$'s.

for $p|q$ *does not translate* in $n \notin \Omega_q$. We may solve this difficulty by resorting to indicator functions. We have $\mathbb{1}_{\mathcal{K}_p} = \mathbb{1} - \mathbb{1}_{\Omega_p}$ and therefore, when $d$ is square-free:

$$\mathbb{1}_{\mathcal{K}_d} = \sum_{\ell|d} \mu(\ell) \mathbb{1}_{\Omega_\ell}. \tag{19}$$

We continue and infer that

$$\sum_{q:n\in\mathcal{K}_q} \lambda_q^\sharp = \sum_q \lambda_q^\sharp \mathbb{1}_{\mathcal{K}_q}(n) = \sum_\ell \lambda_\ell \mathbb{1}_{\Omega_\ell}(n)$$

where $\lambda_\ell = \mu(\ell) \sum_{q:\ell|q} \lambda_q^\sharp$, so that

$$G^\sharp(z)\lambda_\ell = \mu(\ell) \sum_{q:\ell|q} (\mathbb{1} \star h)(q) \sum_{\substack{d\le z\\ q|d}} \mu(d/q) = \mu(\ell)(1\star h)(\ell) \sum_{\substack{m\le z/\ell\\ (m,\ell)=1}} h(m). \tag{20}$$

These coefficients $(\lambda_\ell)$ are exactly the ones that we obtain in the classical presentation of the Selberg sieve, the condition $\sum_q \lambda_q^\sharp = 1$ translating in $\lambda_1 = 1$. Yet again the method of [26] by J.E. van Lint and H.E. Richert may be adapted to show that $|\lambda_\ell| \le 1$, but the situation changes dramatically here because we in fact have (on anticipating on the evaluation of $G^\sharp(z)$ in the next paragraph)

$$\lambda_\ell \ll 2^{\omega(\ell)}/\ell, \tag{21}$$

as simple consequence of the bound $\sum_{\substack{m\le z/\ell\\ (m,\ell)=1}} h(m) \le z/\ell$.

### Density evaluation

We want to sieve up $z = \sqrt{N}$ and the main quantity to be evaluated (minorized is enough) is:

$$G^\sharp(z) = \sum_{q\le z} h(\delta) = \sum_{\substack{q\le z\\ (q,2)=1}} \mu^2(q) \prod_{p|q} \frac{p-1}{p+1} \tag{22}$$

denoted by $G_d(z)$ at the bottom of [13], for $d = 1$. The function $h$ therein is indeed the one we have defined above. The estimation given page 49 with $f = 1$ and $u = 0$, so the function $a$ reduces to the function $h$, gives us

$$G^\sharp(z) = B(1)\big(z + \mathcal{O}^*(6.7\, z^{3/4})\big) \ge 0.35(1 - 6.7/z^{1/4})z \ge 0.326\, z \tag{23}$$

when $z \ge 10^8$. A Pari/GP script rapidly shows that $G^\sharp(z)/z \ge 0.304$ when $z \le 10^9$, the minimum being reached just before $z = 179$. We will use the bound $G^\sharp(z)/z \ge 0.304 \ge 1/8$ for $z \ge 1$ so as to get numerics exactly similar to the ones in the case of the primes.

## 7 Rudin's inequality for squares

The Selberg sieve for squares is briefly described in Section 6.

**Lemma 7.1.** *Under the hypothesis and notation of Theorem 1.2, we have that*

$$\sum_{n\le\sqrt{N}} \left| \exp\Big( \sum_{x\in\mathcal{X}} c(x) e(xn^2) \Big) \right| \le 8 \frac{N + \delta_*^{-1}(\sqrt{N}, 2)}{\sqrt{N}} e^{\frac{1}{2}\sum_{x\in\mathcal{X}} |c(x)|^2}.$$

*Proof.* The proof follows faithfully the one of Theorem 4.1 until Eq. (12), where we dispense of the parameter $z_0$ and employ the decomposition given in (17). Our upper bound becomes

$$\sum_{(\mathcal{A},\mathcal{B},\mathcal{C})} \prod_{x_a\in\mathcal{A}} \frac{|c(x_a)|}{2} \prod_{x_b\in\mathcal{B}} \frac{|c(x_b)|}{2} \prod_{x_c\in\mathcal{C}} |c(x_c)| \\ \sum_{d\leq z^2} \sum_{b \bmod^* d} w_d(\mathcal{K}, b/d) \sum_{n\in\mathbb{Z}} e\Big((x_{\mathcal{A}} - x_{\mathcal{B}})n + \theta_{\mathcal{A}} - \theta_{\mathcal{B}} + \frac{bn}{d}\Big)\psi(n).$$

Yet again, Poisson summation formula enables us to rewrite the sum over $n$ in the form

$$e(\theta_{\mathcal{A}} - \theta_{\mathcal{B}}) \sum_{k\in\mathbb{Z}} \hat{\psi}\Big(\frac{dk - b - (x_{\mathcal{A}} - x_{\mathcal{B}})d}{d}\Big).$$

At this level, we simply need to put another evaluation for the sieve density $G(z; z_0)$, and replace it by (23) for $Q = \sqrt{N}$. The lemma follows readily. □

*Proof of Theorem 1.5.* Lemma 7.1 is prepared to apply Theorem 2.4. As it is exactly similar to Lemma 4.1, the reader will complete the proof without any difficulty. □

# References


[1] M. Abramowitz and I.A. Stegun. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, volume 55 of *National Bureau of Standards Applied Mathematics Series*. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964. `http://mintaka.sdsu.edu/faculty/wfw/ABRAMOWITZ-STEGUN`.

[2] E. Bombieri. *Le grand crible dans la théorie analytique des nombres*, volume 18. 1987/1974.

[3] Jean Bourgain. $\Lambda_p$-sets in analysis: results, problems and related aspects. In *Handbook of the geometry of Banach spaces, Vol. I*, pages 195–232. North-Holland, Amsterdam, 2001.

[4] Jean Bourgain. Roth's theorem on progressions revisited. *J. Anal. Math.*, 104:155–192, 2008.

[5] Mei-Chu Chang. A polynomial bound in Freiman's theorem. *Duke Math. J.*, 113(3):399–419, 2002.

[6] B. Green and T. Tao. Restriction theory of the Selberg sieve, with applications. *J. Théor. Nombres Bordx*, 18(1):147–182, 2006. Available at `http://fr.arxiv.org/pdf/math.NT/0405581`.

[7] Ben Green. Structure theory of set addition. page 27 pp, Edinburgh March 25 – April 5, 2002. ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis.

[8] Ben Green. Spectral structure of sets of integers. In *Fourier analysis and convexity*, Appl. Numer. Harmon. Anal., pages 83–96. Birkhäuser Boston, Boston, MA, 2004.

[9] Edwin Hewitt and Herbert S. Zuckerman. Some singular Fourier-Stieltjes series. *Proc. London Math. Soc. (3)*, 19:310–326, 1969.

[10] Jorge M. López and Kenneth A. Ross. *Sidon sets*, volume Vol. 13 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1975.

[11] H.L. Montgomery. The analytic principle of the large sieve. *Bull. Amer. Math. Soc.*, 84(4):547–567, 1978.

[12] O. Ramaré. *Contribution au problème de Goldbach : tout entier $> 1$ est d'au plus 13 nombres premiers*. 1–70pp, Université Bordeaux I, 1991.

[13] O. Ramaré. *Arithmetical aspects of the large sieve inequality*, volume 1 of *Harish-Chandra Research Institute Lecture Notes*. Hindustan Book Agency, New Delhi, 2009. With the collaboration of D. S. Ramana.

[14] O. Ramaré. A note on additive properties of dense subsets of sifted sequences. *Bull. Lond. Math. Soc.*, 45(4):677–682, 2013.

[15] O. Ramaré and I.M. Ruzsa. Additive properties of dense subsets of sifted sequences. *J. Théorie N. Bordeaux*, 13:559–581, 2001.

[16] Olivier Ramaré. On Snirel'man's constant. *Ann. Scu. Norm. Pisa*, 22:645–706, 1995.

[17] Olivier Ramaré. Notes on restriction theory in the primes. *Israel J. Math.*, 261(2):717–738, 2024.

[18] Olivier Ramaré. Cusps of dense subsets of the prime – bypassing the $w$-trick. page 26pp, 2025.

[19] Walter Rudin. Trigonometric series with gaps. *J. Math. Mech.*, 9:203–227, 1960.

[20] Walter Rudin. *Fourier analysis on groups*, volume No. 12 of *Interscience Tracts in Pure and Applied Mathematics*. Interscience Publishers (a division of John Wiley & Sons, Inc.), New York-London, 1962.

[21] A. Selberg. Collected papers. *Springer-Verlag*, II:251pp, 1991.

[22] I. D. Shkredov. On sumsets of dissociated sets. *Online J. Anal. Comb.*, (4):26, 2009.

[23] Ilya D. Shkredov. Some applications of W. Rudin's inequality to problems of combinatorial number theory. *Unif. Distrib. Theory*, 6(2):95–116, 2011.

[24] T. Tao and V.H. Vu. *Additive Combinatorics*. Cambridge Univ. Press, 2006.

[25] J.D. Vaaler. Some Extremal Functions in Fourier Analysis. *Bull. A. M. S.*, 12:183–216, 1985.

[26] J.E. van Lint and H.E. Richert. On primes in arithmetic progressions. *Acta Arith.*, 11:209–216, 1965.