

THE TRIGONOMETRIC POLYNOMIAL ON SUMS OF TWO SQUARES, AN ADDITIVE PROBLEM AND GENERALISATION

OLIVIER RAMARÉ AND G.K. VISWANADHAM

ABSTRACT. Let \mathfrak{B} be the set of odd integers that are sums of two coprime squares. We prove that the trigonometric polynomial $S(\alpha; N) = \sum_{b \in \mathfrak{B}, b \leq N} e(b\alpha)$ satisfies

$$\frac{S(\alpha; N)}{N/\sqrt{\log N}} \ll_{A, A'} \frac{1}{\varphi(q)} + \sqrt{\frac{q}{N}} (\log N)^7 + \frac{1}{(\log N)^A}$$

for any $A, A' \geq 0$ and when $(a, q) = 1$ and $|q\alpha - a| \leq (\log N)^{A'}/N$. We use this estimate together with a variant of the circle method influenced by Green and Tao's Transference Principle to obtain the number of representations of a large enough odd integer N as a sum $b + b_1 + b_2$, where $b \in \mathfrak{B}$ while b_1 (resp. b_2) belongs to a general subset \mathfrak{B}_1 (resp. \mathfrak{B}_2) of \mathfrak{B} of relative positive density. We further show that the above bound is effective when $0 \leq A < 1/2$.

CONTENTS

1. Introduction and results	1
2. Proof of Theorem 1.1	7
3. Proof of Theorem 1.3	9
4. A Simple Sieve Identity	10
5. Using the Simple Sieve Identity	11
6. Recovering the Harman Sieve	13
7. The trigonometric polynomial around $\alpha = 0$	14
8. Distribution in 'small' arithmetic progressions via analytical means	15
9. A local model	21
10. The trigonometric polynomial in the large	23
11. The trigonometric polynomial at rationals with small denominator	25
12. A global bound for the trigonometric polynomial, proof of Theorem 1.5	29
13. An additive application, Proof of Theorem 1.6	29
14. A challenge. Proof of Theorem 1.7	31
15. Bounds on multiples. Proof of Theorem 1.8	32
16. Diophantine approximation and proof of Theorem 1.9	33
17. Appendix: some estimates with primes congruent to 3 modulo 4	34
References	35

1. INTRODUCTION AND RESULTS

In 1922, the part III of the series *Partitio Numerorum* [26] by G.H. Hardy & J.E. Littlewood opened a new era saluted for instance by E. Landau in his review for *ZentralBlatt*. In this paper, the authors developed the circle method introduced by G.H. Hardy & S. Ramanujan in a series of papers, see [25] to handle additive questions on primes. They proved in particular that, under the Generalized Riemann Hypothesis, every large enough odd integer is a sum of three primes, a result

2010 *Mathematics Subject Classification.* Primary: 11L07, Secondary: 11M26, 11N25, 11P55.

Key words and phrases. Sums of two squares, Transference principle, Trigonometric polynomial.

that was largely out of reach. Around the same time, V. Brun in [4] initiated what was to become the combinatorial sieve. Influenced by both works, I.M. Vinogradov simplified in [61] Hardy & Littlewood's method to use only the finite trigonometric polynomials on the primes, i.e. $\sum_{p \leq N} e(pa)$, and introduced a decomposition of this sum in what he called type I or type II sums (also referred to as linear and bilinear contribution), making possible to handle the minor arcs without appealing to the Generalized Riemann Hypothesis. This is a landmark in the study of primes. Later and simplifying considerably this initial work, P.X. Gallagher in [15] and R.C. Vaughan in [59] used convolution identities to obtain another type I/type II decomposition. We finally mention that B. Green & T. Tao in a series of papers around [22] developed a dynamical understanding of this trigonometric polynomial; the restriction to primes still relies on combinatorial tools, as is surely easier to grasp from the paper [3] by J. Bourgain, P. Sarnak & T. Ziegler (see [5] by M. Cafferata, A. Perelli & A. Zaccagnini). The survey paper [44] gives more details, but let us retain that two approaches compete to handle the trigonometric polynomials on the primes: via combinatorial tools or via convolution identities. Notice that the combinatorial tools are inherited from sieve techniques which rely heavily on non-negativity.

A first aim of this paper is to try to disentangle the role of sieve from the one of convolution identities. The trigonometric polynomial $S(\alpha; N)$ on sums of two squares is our trying ground. To stay in a clean sieve situation, we restrict our attention to the subset \mathfrak{B} of odd integers that are sums of two coprime squares: these are simply the odd integers that are free of primes $\equiv 3[4]$ and their characteristic function is written $n \mapsto b(n)$. The sieve dimension is just borderline for the sieve to be very efficient, see Chapter 14 of [14] by J. Friedlander & H. Iwaniec. Convenient convolution identities are missing. We show that the initial Vinogradov idea (but not the one from Theorem 3, Chapter IX of [60], see also [63]) and the central identity of the combinatorial sieve may be used to produce adequate decompositions; we are able to cope with a more general case that we describe below, the two innovative steps being Theorem 1.1 and 1.4. We shall complete and improve on the latter in a forthcoming paper but decided here to stay focused on the trigonometric polynomial $S(\alpha; N)$; we produce a finer bound for $S(\alpha; N)$ when α is close to a rational with a small denominator in Lemma 11.3. We do not reach the maximal precision one gets for the primes, see [43], but miss it by a mere $(\log \log N)^{\frac{1}{2}+\varepsilon}$. We end this study by a more classical asymptotic for $S(\alpha; N)$ when α is close to a rational with a small denominator. This work is supplemented by two applications, one to a ternary additive problem for which we prove an L^p -bound for $p > 2$ for $S(\alpha; N)$ and another one to a quantitative measure of the equidistribution of $b\alpha$ when α is quadratic irrational and $b \in \mathfrak{B}$, for which we have to prove an average bound over $r \in \{1, 2, \dots, R\}$ for $S(r\alpha; N)$.

Let us now give more details. It is easier to introduce now a notation: $f = \mathcal{O}^*(g)$ means that $|f| \leq g$. We recall that $n \mapsto b(n)$ is the characteristic function of the set \mathfrak{B} and we record that the function ρ is defined in Eq. (3).

Bilinear representations for characteristic functions of sifted sets. To cover several cases as one, we introduce an infinite set of primes \mathfrak{P} that has a density $\kappa \in (0, 1]$ in the sense that

$$(1) \quad \sum_{\substack{p \leq X \\ p \in \mathfrak{P}}} \frac{\log p}{p} = \kappa \log X + \mathcal{O}(1).$$

When investigating the set \mathfrak{B} of odd integers that may be written as sums of two coprime squares, \mathfrak{P} is the set of primes congruent to 3 modulo 4. Let us notice that

the elements of \mathfrak{B} are all congruent to 1 modulo 4. This implies in particular that if a prime $p \equiv 3[4]$ divides such an element, then at least another prime $\equiv 3[4]$ does so (which may be the same, says p , meaning that p^2 divides our candidate). As a conclusion, the odd integers below N that are in \mathfrak{B} are the integers below N that are congruent to 1 modulo 4 and do not have prime divisors $p \leq \sqrt{N}$ congruent to 3 modulo 4. We can encompass also the case of primitive Loeschian integers, i.e. integers n than can be written as $n = u^2 + uv + v^2$ with u and v coprime by sieving the set of integers congruent to 1 modulo 3 by the set \mathfrak{P} of primes congruent to 2 modulo 3. As in [13] by É. Fouvry, C. Levesque and M. Waldschmidt, we may also consider the set of integers that are both odd primitive Gaussian integers and primitive Loeschian integers in which case the set \mathfrak{P} is the set of primes not congruent to 1 mod 12. It is typographically expedient to define

$$(2) \quad \mathfrak{P}(z) = \prod_{\substack{p < z \\ p \in \mathfrak{P}}} p$$

and the special case $P_{4;3}(z) = \prod_{\substack{p < z \\ p \equiv 3[4]}} p$. Let us present our first identity that introduces few loss and, as may be expected, leads to only a moderate saving. It results from a combination of the initial method of I. M. Vinogradov together with Rankin's trick. We state this initial result in a format close to the one employed by H. Iwaniec and E. Kowalski in [33, Proposition 13.1].

Theorem 1.1. *Let $2 \leq z \leq D \leq \sqrt{N}$ and $Z \geq z$. For any sequence of complex numbers (u_n) , we have*

$$\sum_{\substack{n \leq N \\ (n, \mathfrak{P}(Z))=1}} u_n = \sum_{\substack{d | \mathfrak{P}(z) \\ d \leq D}} \mu(d) \sum_{n \equiv 0[d]} u_n - \sum_{\substack{mp \leq N \\ z \leq p < Z}} \rho(m) \mathbf{1}_{p \in \mathfrak{P}} u_{mp} + \mathcal{O}^*(E)$$

where

$$(3) \quad \rho(m) = \frac{\mathbf{1}_{(m, \mathfrak{P}(z))=1}}{1 + \#\{p' \in [z, Z] \cap \mathfrak{P} : p' | m\}} \in [0, 1]$$

and with

$$(4) \quad E = \sqrt{N \sum_n |u_n|^2} \left(\frac{1}{\sqrt{z}} + \exp\left(\frac{-\log D}{\log z}\right) (\log 3z)^{31} \right).$$

In case $|u_n| \leq 1$, the first term of the error term E may be improved to N/z .

This is proved in Section 2. Here is a consequence of it for the readers to visualize better.

Corollary 1.2. *Let $2 \leq z \leq D \leq \sqrt{N}$. For any sequence of complex numbers $(u_n)_{n \leq N}$ supported on the integers congruent to 1 modulo 4, we have*

$$\sum_{n \leq N} b(n) u_n = \sum_{\substack{d | P_{4;3}(z) \\ d \leq D}} \mu(d) \sum_{n \equiv 0[d]} u_n - \sum_{\substack{mp \leq N \\ z \leq p \leq \sqrt{N}}} \rho(m) \mathbf{1}_{p \equiv 3[4]} u_{mp} + \mathcal{O}^*(E).$$

In case $|u_n| \leq 1$, the first term of the error term E may be improved to N/z .

The non-negativity of $\rho(m)$ is noteworthy: it is an inheritance from the sieve background. The explicit form to the error is here to explicitate the dependencies in the parameters; neither the constants, nor the power of logarithm have been optimized.

Here is a more specific and interval oriented version of the previous result.

Theorem 1.3. Let $10 \leq z \leq D \leq \sqrt{N}$ and $U \in [D, N]$ be another parameter. For any sequence of complex numbers (u_n) supported in $[N - U, N]$ and such that $|u_n| \leq 1$, Theorem 1.1 for $\mathfrak{P}(Z) = P_{4,3}(\sqrt{N})$ holds with E replaced by $\mathcal{O}(E')$ where

$$E' = \frac{U}{z} + N \exp\left(\frac{-\log D}{\log z} \log \frac{\log D}{2 \log z}\right) \sqrt{\log z}.$$

This is proved in Section 3. We complete our weaponry with a somewhat less precise but much stronger bilinear decomposition that combines the principle of Theorem 1.1 with what we call the *Simple sieve bilinear decomposition* contained in Lemma 4.2 and Theorem 5.2.

Theorem 1.4. For any set of parameters $\max(2, z) \leq Z \leq N$ and $2 \leq M_0 \leq M$, there exist sequences $(\alpha_\ell(t))$ and $(\beta_k(t))$ such that, for any sequence $(u_n)_{n \leq N}$, we have

$$\begin{aligned} \sum_{(n, \mathfrak{P}(Z))=1} u_n &= \sum_{\substack{d < M \\ d \mid \mathfrak{P}(z)}} \mu(d) \sum_{n \equiv 0 \pmod{d}} u_n - \sum_{\substack{mp \leq N \\ z \leq p < Z}} \rho(m) \mathbf{1}_{p \in \mathfrak{P}} u_{mp} \\ &\quad - \int_0^1 \sum_{\substack{k\ell \geq M \\ M_0 \leq \ell \leq M_0 z}} \alpha_\ell(t) \beta_k(t) u_{k\ell} dt + \mathcal{O}\left(\sqrt{\frac{N \sum_n |u_n|^2}{z}}\right) \end{aligned}$$

where $|\alpha_\ell(t)| \leq 1$ and $|\beta_k(t)| \leq 16\tau_3(k) \log N$ and $\alpha_\ell(t)$ vanishes on indices ℓ that do not divide $\mathfrak{P}(z)$, while $\rho(m) \in [0, 1]$ is defined in Theorem 1.1. In case $|u_n| \leq 1$, the error term may be improved to $\mathcal{O}(N/z)$.

This is proved at the end of Section 5. The function τ_3 is classically the second Piltz function, namely $\tau_3(k) = \sum_{d_1 d_2 d_3 = k} 1$. We show in Theorem 6.1 that we may recover from the above decomposition a version of the Harman sieve. This version has a smaller admissible range for one of the variables.

Discrepancies between the case of primes and the case of sums of two squares. Let us recall that the characteristic function of elements of \mathfrak{B} (we shall refer to them as *odd primitive Gaussian integers*) is denoted by $n \mapsto b(n)$. One of our aim is to understand the trigonometric polynomial

$$(5) \quad S(\alpha; N) = \sum_{n \leq N} b(n) e(n\alpha).$$

Though one may think this polynomial over sums of two squares is easier to handle than the one on the primes, the sieving dimension being less, combinatorial identities à la Gallagher-Vaughan are not available in this context. Indeed we only have

$$\sum_{\substack{d \mid n \\ d \mid P_{4,3}(\infty)}} \mu(d) = \begin{cases} 1 & \text{when } (n, P_{4,3}(\infty)) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

while, in the case of the primes, we may rely on $\sum_{d \mid n} \mu(d) = \mathbf{1}_{n=1}$.

The trigonometric polynomial on sums of two squares. The above machinery gives us access to sharp bounds for $S(\alpha; N)$ defined in (5). By combining that with results on the distribution of sums of two squares in arithmetic progressions to small modulus, we reach the next theorem.

Theorem 1.5. Let $A \geq 0$. Let $|\alpha - \frac{a}{q}| \leq \frac{(\log N)^{2A+14}}{qN}$ with $(a, q) = 1$ and $q \leq N/(\log N)^{2A+14}$. We have

$$\frac{S(\alpha; N)}{N/\sqrt{\log N}} \ll_A \frac{1}{\varphi(q)} + \sqrt{\frac{q}{N}} (\log N)^7 + \frac{1}{(\log N)^A}.$$

The implied constant can be effectively computed when $A < 1/2$.

This is proved in Section 12. See also Lemma 10.4 and 11.3. There are two ranges of estimation of $S(\alpha; N)$: when q is small and when q is large. We cover the large range by using Theorem 1.4 while the smaller range of q is dealt with analytic methods, though uneffectively. Effectivity can be recovered when $A < 1/2$ by using Corollary 1.2.

Additive problems with subsequences of sums of two squares. A theorem of Fermat in 1625 asserts that a positive integer n can be written as a sum of two coprime squares if and only if it is either odd and not divisible by any prime $\equiv 3[4]$ or it is the double of such a number. For the history of results on this subject, we refer the readers to the Chapter VI of Volume II of the book [10] by L. E. Dickson. In [36], E. Landau proved that

$$(6) \quad B(N) = \sum_{n \leq N} b(n) \sim \frac{CN}{\sqrt{\log N}}, \quad C = \sqrt{2} \prod_{p \equiv 3[4]} (1 - 1/p^2)^{-1/2}.$$

Please note that such integers are $\equiv 1[4]$. Our notation $b(n)$ is in accordance with Section 14.3 of the reference book [14] by J. Friedlander and H. Iwaniec, see in particular Theorem 14.1 therein for the value of C . Our aim is to study some additive questions concerning subsets of \mathfrak{B} . Their behaviour as essential components and similar questions have already been treated in [42, 46] but only upper bounds were required in such works. The half-dimensional sieve and sieve reversal principle may also be put to work when it comes to the full sequence \mathfrak{B} , see [32, Corollary 2] by H. Iwaniec, [16] by G. Greaves and Section 14.5 of [14]. Queries requiring lower bounds or even equality were successfully treated for rather general subsequences of the primes in a series of works initiated by B. Green in [21], followed by [18, 20] by B. Green and T. Tao to cite but a few of these results. We should mention specifically [52, 53] by X. Shao, [39] by K. Matomäki and X. Shao, [55] by J. Teräväinen or more recently [1] by C. Bauer as they are close to our main result. In these pieces of work, the *transference principle*, as defined in [19] by B. Green and T. Tao, is put to work. We are interested at avoiding this method but to stick to the more precise circle method. We do so below at the price of assuming that one variable is ‘more regular’: X. Shao [52] is able to handle sums of three primes, each belonging to a dense subset of primes, whereas we constrain one of our variables to belong to the full set. As a result, we avoid the W -trick (but use restriction estimates, see Lemma 13.1 below) and get a close to asymptotic expression for the required number of representations. The theorem we have in view is the following.

Theorem 1.6. *Let $N \equiv 3[4]$ be an integer, $K \in [2, \log \log N]$ be a parameter, and \mathcal{B}_1 and \mathcal{B}_2 be two sets of odd primitive Gaussian integers. With $M = P_{4,3}(K)$, we have*

$$\sum_{\substack{n+b_1+b_2=N \\ b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2}} b(n) = \frac{CM/\varphi(M)}{\sqrt{\log N}} \sum_{\substack{b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2 \\ b_1+b_2 \leq N \\ (N-(b_1+b_2), M)=1}} 1 + \mathcal{O}_{\mathcal{B}_1, \mathcal{B}_2} \left(\frac{N^2}{\sqrt{K}(\log N)^{3/2}} \right)$$

where C is defined in (6).

This is proved at the end of Section 13. The variables b_1 and b_2 are controlled by the restriction estimate recalled in Lemma 13.1. We may therefore replace \mathcal{B}_1 and \mathcal{B}_2 by any subsequence of relative positive density of a *sufficiently sifted set*, as defined in [46], e.g. the sequence of primes, or of primes p such that $p+2$ is in \mathfrak{B} as in [32, Corollary 2] by H. Iwaniec (see also [31] by K. H. Indlekofer), or of Chen primes as in [19].

Sketching the proof of Theorem 1.6. It is classical in the circle method to “interpret” the singular series as the product of so-called “local densities”. We go one step further and provide a geometrical meaning to this philosophy: we indeed approximate our function on the major arcs by a function that is periodical modulo M , for some large modulus M , that we call the *local model*.

More precisely, the proof of Theorem 1.6 goes by the circle method in which:

- (1) The major arcs defined in (31) are arcs around a/q for a prime to q and $q \in P_{4,3}(K) \cup 2P_{4,3}(K) \cup 4P_{4,3}(K)$ for some parameter K .
- (2) We approximate one copy of $S(\alpha; N)$ by the trigonometric polynomial $S_K^\flat(\alpha; N)$ of a local model of \mathfrak{B} on the major arcs. This approximation is the result of the comparison of Lemma 8.1 and 9.3).
- (3) The contribution of the minor arcs is shown to be negligible by combining two facts: (a) the L^ℓ -inequality given in Lemma 13.1 for some $\ell > 2$ and (b) the L^∞ -bound given in Theorem 1.5. This idea is very much related with the work of B. Green & T. Tao, see Eq. (5.15) in [19].
- (4) The expression with one copy of $S_K^\flat(\alpha; N)$ and two copies of $S(\alpha; N)$ (though restricted to subsequences) is written back in terms of the coefficients, so $N = b_1 + b_2 + n$ with n coming from the local model. The existence of such a writing amounts to a congruence condition of $N - b_1 - b_2$ to some modulus $M = 4P_{4,3}(K)$, as in the first two lines on top of page 578 in [46].

The size of M , hence of K , is of utmost importance. The above scheme enables us to take K to be as small as a (large) constant if we rely on Theorem 1.5, i.e. if we allow analytical means. If we want to use only combinatorial means, so as to be able to generalize the proof, then Lemma 11.3 looses $\Theta = C\sqrt{\log \log N} \log \log \log N$, where C is some positive constant; K has to be larger than Θ^2 , implying that M is larger than any power of $\log N$.

Notice that the same proof holds if the three variables are primes (or belonging to dense subsets of these for two of them) thanks, for the L^∞ -estimate, to the Vinogradov estimates on the minor arcs coupled with ‘log’-free estimates for the major arcs, as can be found in [7] by H. Daboussi or in [43] (see [49] for the latest best estimate) and, for the L^ℓ -estimate, to the Bourgain-Green estimate found in Theorem 1.5 of [23]. On using the same setting as before, we may again take K to be a constant. This gives another Dirichlet L -function-free proof of Vinogradov’s three primes theorem, after the one of X. Shao [53].

A challenge. Here is a result to measure the strength of our method in the middle range.

Theorem 1.7. *We have $S(\sqrt{2}; N) \ll N^{5/6}(\log N)^{13/2}$.*

This is proved in Section 14. Our process would give the same for primes, while the Gallagher-Vaughan Identity immediately provides an exponent $4/5$ rather than $5/6$. We could use any quadratic number rather than $\sqrt{2}$ as the required property is that $\sqrt{2}$ has convergent denominators of any given size, i.e. a substitute to Lemma 14.1.

The trigonometric polynomial on the family of multiples. The bilinear decomposition of Theorem 1.4 enables us to handle sums of $e(b\alpha)$, but also of other oscillating functions like $b \mapsto e(rba)$ for some integer r . Additional gain may be obtained by studying these functions on average over a large range of values of r , and this leads to the next result.

Theorem 1.8. *Let α be a point of \mathbb{R}/\mathbb{Z} given with a rational approximation $\alpha = \frac{a}{q} + \beta$ where $q^2|\beta| \leq 1$. For $N \geq 1$ and any $\varepsilon > 0$, we have*

$$\sum_{r \leq R} |S(r\alpha; N)| \ll_{\varepsilon} \frac{RN}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{1}{R^{1/3}N^{1/6}} + \frac{R^{1/3}}{N^{1/3}} \right) N^{\varepsilon}.$$

This is proved in Section 15. It can be compared with [62, Theorem 3] by I. M. Vinogradov, or with [57, Theorem 1] by R. C. Vaughan. Specializing $R = 1$ recovers the result of Lemma 10.4, save for the $(\log N)^7$ that is here degraded in N^{ε} .

A Diophantine usage. Here is a direct consequence of Theorem 1.8.

Theorem 1.9. *Let α be a quadratic irrational and let $\lambda \in (0, 1/4)$. The number of integers $b \in \mathfrak{B}$ with $b \leq N$ and $\|b\alpha - \beta\| \leq 1/N^{\lambda}$ is asymptotic to $2\mathfrak{B}(N)/N^{\lambda}$.*

This is proved in Section 16. In the case of primes, R. Vaughan in [57] obtained a similar result. See also [29, Theorem 2.2 and 3.2] in the book of G. Harman. More refined approaches by G. Harman in [27, 28] and by C. H. Jia in [34, 35] led to the exponent $\lambda = 7/22$, though being unable to provide an asymptotic formula in the case α quadratic irrational. In case $\beta = 0$, this exponent has been further reduced to $1/3$ after the successive contributions of R. Heath-Brown & C. H. Jia in [30] and of K. Matomäki in [38]. Notice that, if we had only used Theorem 1.5 rather than Theorem 1.8, the exponent λ would be constrained to $\lambda < 1/6$.

Thanks and acknowledgments. Thanks are due to the referee for his/her very careful reading. The authors gratefully acknowledge funding from ReLaX, CNRS IRL 2024 and by NBHM, and support and hospitality of IISER Berhampur and of I2M in Aix-Marseille University.

2. PROOF OF THEOREM 1.1

Here is the first step.

Lemma 2.1. *Under the hypotheses of Theorem 1.1, we have*

$$\sum_{\substack{n \leq N \\ (n, \mathfrak{P}(Z))=1}} u_n = \sum_{\substack{n \leq N \\ (n, \mathfrak{P}(z))=1}} u_n - \sum_{\substack{z \leq p \leq Z \\ p \in \mathfrak{P}}} \sum_{m \leq N/p} \rho(m) u_{mp} + \mathcal{O}^* \left(\sqrt{\frac{N}{z}} \sum_n |u_n|^2 \right).$$

In case we have $|u_n| \leq 1$, the error term may be improved to $\mathcal{O}^*(N/z)$.

Proof. A moment of thought leads to our first formula:

$$\sum_{\substack{n \leq N \\ (n, \mathfrak{P}(Z))=1}} u_n = \sum_{\substack{n \leq N \\ (n, \mathfrak{P}(z))=1}} u_n - \sum_{\substack{z \leq p \leq Z \\ p \in \mathfrak{P}}} \sum_{\substack{m \leq N/p \\ (m, \mathfrak{P}(z))=1}} \frac{u_{pm}}{\omega^{\sharp}(pm)}$$

where

$$\omega^{\sharp}(pm) = \sum_{\substack{p' \in \mathfrak{P} \\ p'|pm \\ z \leq p' \leq Z}} 1.$$

As this counting is done without multiplicities, we have $\omega^\sharp(pm) = 1 + \omega(m)$ when $(m, p) = 1$ and $\omega^\sharp(pm) = \omega^\sharp(m)$ otherwise. Hence

$$\begin{aligned} \sum_{\substack{n \leq N \\ (n, \mathfrak{P}(Z))=1}} u_n &= \sum_{\substack{n \leq N \\ (n, \mathfrak{P}(z))=1}} u_n - \sum_{\substack{z \leq p \leq Z \\ p \in \mathfrak{P}}} \sum_{\substack{m \leq N/p \\ (m, \mathfrak{P}(z))=1}} \frac{u_{pm}}{1 + \omega^\sharp(m)} \\ &\quad - \sum_{\substack{z \leq p \leq Z \\ p \in \mathfrak{P}}} \sum_{\substack{\ell \leq N/p^2 \\ (\ell, \mathfrak{P}(z))=1}} \frac{u_{p^2\ell}}{(1 + \omega^\sharp(p\ell))\omega^\sharp(p\ell)}. \end{aligned}$$

We discard the last term in the following manner. First we notice that

$$(7) \quad \sum_{\substack{z \leq p \leq Z \\ p \in \mathfrak{P}}} \left| \sum_{\substack{\ell \leq N/p^2 \\ (\ell, \mathfrak{P}(z))=1}} \frac{u_{p^2\ell}}{(1 + \omega^\sharp(p\ell))\omega^\sharp(p\ell)} \right| \leq \frac{1}{2} \sum_{m \leq N} |u_m| \left(\sum_{\substack{p^2|m \\ z \leq p \leq Z}} 1 \right).$$

We apply the Cauchy-Schwarz inequality to this last quantity and use

$$\begin{aligned} \sum_{m \leq N} \left(\sum_{\substack{p^2|m \\ z \leq p \leq Z}} 1 \right)^2 &\leq \sum_{z \leq p_1 \neq p_2 \leq Z} \frac{N}{p_1^2 p_2^2} + \sum_{z \leq p_1 \leq Z} \frac{N}{p_1^2} \\ &\leq N \left(\frac{2}{z} \right)^2 + \frac{2N}{z} \leq \frac{4N}{z}. \end{aligned}$$

by using $\sum_{p \geq A} 1/p^2 \leq 2/A$, valid for any $A \geq 1$ and since we may assume that $z \geq 2$. This proves our lemma with the first version of the error term. When the sequence (u_n) is bounded in absolute value by 1, we may proceed more efficiently as in Theorem 26.2 of [47] by P. Moree, O. Ramaré & A. Sedunova. Indeed we readily find that

$$(8) \quad \sum_{\substack{z \leq p \leq Z \\ p \in \mathfrak{P}}} \left| \sum_{\substack{\ell \leq N/p^2 \\ (\ell, \mathfrak{P}(z))=1}} \frac{u_{p^2\ell}}{(1 + \omega^\sharp(p\ell))\omega^\sharp(p\ell)} \right| \leq \sum_{\substack{z \leq p \leq Z \\ p \in \mathfrak{P}}} \frac{N}{2p^2} \leq \frac{N}{z}.$$

The proof is now to an end. \square

Proof of Theorem 1.1. We first appeal to Lemma 2.1. The first term may be studied by a straightforward usage of the Erathostenes sieve by Legendre, i.e. we write

$$\begin{aligned} \sum_{\substack{n \leq N \\ (n, \mathfrak{P}(z))=1}} u_n &= \sum_{n \leq N} u_n \sum_{\substack{d|\mathfrak{P}(z) \\ d|n}} \mu(d) \\ &= \sum_{\substack{d|\mathfrak{P}(z) \\ d \leq D}} \mu(d) \sum_{n \equiv 0[d]} u_n + \sum_{\substack{d|\mathfrak{P}(z) \\ d > D}} \mu(d) \sum_{n \equiv 0[d]} u_n. \end{aligned}$$

We treat the second summand in a similar manner to what we did to bound the first error term, i.e. we write

$$(9) \quad \sum_{\substack{d|\mathfrak{P}(z) \\ d > D}} \mu^2(d) \sum_{n \equiv 0[d]} |u_n| = \sum_{n \leq N} |u_n| \sum_{\substack{d|\mathfrak{P}(z) \\ d > D \\ d|n}} 1$$

to which we apply Cauchy's inequality to bound it above by the squareroot of

$$\sum_{n \leq N} |u_n|^2 \sum_{n \leq N} \left(\sum_{\substack{d|\mathfrak{P}(z) \\ d > D \\ d|n}} 1 \right)^2.$$

We can handle the last sum, say Σ , via Rankin's trick:

$$\begin{aligned} \Sigma &\leq \sum_{\substack{D < d_1, d_2 \leq N, \\ [d_1, d_2] \leq N \\ d_1, d_2 \nmid \mathfrak{P}(z)}} \frac{N}{[d_1, d_2]} \leq N \sum_{\substack{D < d \leq N, \\ d \mid \mathfrak{P}(z)}} \frac{3^{\omega(d)}}{d} \leq ND^{-2\varepsilon} \prod_{p \leq z} \left(1 + \frac{3p^{2\varepsilon}}{p}\right) \\ &\leq ND^{-2\varepsilon} \prod_{p \leq z} \left(1 + \frac{3p^{3\varepsilon}}{p^{1+\varepsilon}}\right) \leq ND^{-2\varepsilon} \zeta(1 + \varepsilon)^{3z^{3\varepsilon}} \end{aligned}$$

for any positive ε . We select $\varepsilon = 1/\log z$. Since $\zeta(1 + \varepsilon) \leq 1 + 1/\varepsilon$, this finally amounts to

$$\begin{aligned} \sum_{\substack{n \leq N \\ (n, \mathfrak{P}(Z))=1}} u_n &= \sum_{\substack{d \mid \mathfrak{P}(z) \\ d \leq D}} \mu(d) \sum_{n \equiv 0[d]} u_n - \sum_{\substack{mp \leq N \\ z \leq p < z \\ p \in \mathfrak{P}}} \rho(m) u_{mp} \\ &\quad + \mathcal{O}^* \left(\sqrt{N \sum_n |u_n|^2} \left(\frac{1}{\sqrt{z}} + \exp\left(\frac{-\log D}{\log z}\right) (1 + \log z)^{31} \right) \right). \end{aligned}$$

This ends the proof of Theorem 1.1. \square

3. PROOF OF THEOREM 1.3

Before embarking into the proof, we recall a lemma due to H. Daboussi and J. Rivat in this particular precise form. This is [8, Lemma 4], and is inspired by [11, around page 81] by P.D.T.A. Elliott.

Lemma 3.1. *Let f be a non-negative multiplicative function, and $z \geq 2$ be some real parameter. We define*

$$S = \sum_{p < z} \frac{f(p)}{1 + f(p)} \log p.$$

We assume $S > 0$ and write $K(t) = \log t - 1 + 1/t$ for $t \geq 1$. Then for any y such that $\log y \geq S$, we have

$$\sum_{\substack{d \geq y \\ d \mid \mathfrak{P}(z)}} \mu^2(d) f(d) \leq \prod_{p < z} (1 + f(p)) \exp\left(-\frac{\log y}{\log z} K\left(\frac{\log y}{S}\right)\right).$$

When $\log y \geq 7S$, we have $K((\log y)/S) \geq 1$. The function $t \mapsto K(t)$ is non-decreasing when $t \geq 1$.

Here is the consequence of Lemma 3.1 that we are interested in.

Lemma 3.2. *When $z \geq 10$ and $2 \log D \geq \log z$, we have*

$$\sum_{D < d \mid P_{4;3}(z)} \frac{\mu^2(d)}{d} \ll \sqrt{\log z} \exp\left(-\frac{\log D}{\log z} \log \frac{\log D}{2 \log z}\right).$$

Proof. We apply Lemma 3.1 with the multiplicative function f defined on primes by

$$(10) \quad f(p) = \begin{cases} 1/p & \text{when } p \equiv 3[4] \\ 0 & \text{otherwise.} \end{cases}$$

The values on prime powers are irrelevant, so we set $f(p^k) = 0$ when $k \geq 2$ to be semantically correct. We use Lemma 17.1 to compute that

$$S = \sum_{p < z} \frac{f(p) \log p}{1 + f(p)} = \sum_{\substack{p < z \\ p \equiv 3[4]}} \frac{\log p}{p + 1} \leq \frac{1}{2} \log z - \frac{1}{4} \log 3 \leq \frac{\log z}{2}.$$

By monotonicity, we get, when $z \geq 10$ and $2 \log D \geq \log z$

$$\begin{aligned} K\left(\frac{\log D}{S}\right) &\geq K\left(\frac{2 \log D}{\log z}\right) \geq \log \frac{2 \log D}{\log z} - 1 \\ &\geq \log \frac{\log D}{2 \log z}. \end{aligned}$$

This concludes the lemma. \square

Proof of Theorem 1.3. We follow the proof of Theorem 1.1. Since $|u_n| \leq 1$, we get that the first error term is bounded by $\frac{U}{z}$. The next discrepancies appear after (9). We again use the fact that $|u_n| \leq 1$ to bound above $|\sum_{n:d|n} u_n|$ by N/d . We then appeal to Lemma 3.2 to get the required result. \square

4. A SIMPLE SIEVE IDENTITY

The main result of this section is Lemma 4.2 to which we provide two proofs. Let us start by a more general version of it.

Lemma 4.1. *Let ∇ be a function such that (1) ∇ takes only the values 0 and 1, (2) the set on which $\nabla(d) = 1$ is divisor-closed and (3) $\nabla(1) = 1$. Then for any sequence ψ , we have*

$$\begin{aligned} \sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d) &= \sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d)\nabla(d) + \sum_{\ell|\mathfrak{P}(z)} \mu(\ell)\psi(\ell)\bar{\nabla}(\ell) \\ &\quad - \sum_{\ell|\mathfrak{P}(z)} \bar{\nabla}(\ell)\mu(\ell) \sum_{\substack{p' < P^-(\ell) \\ p' \in \mathfrak{P}}} \sum_{d|\mathfrak{P}(p')} \mu(d)\psi(\ell p' d) \end{aligned}$$

where

$$(11) \quad \bar{\nabla}(\ell) = \begin{cases} 0 & \text{when } \ell = 1 \\ \nabla(\ell/P^-(\ell)) - \nabla(\ell) & \text{when } \ell > 1. \end{cases}$$

We recall that $P^-(m)$ denotes the least prime factor of the integer m . We shall see that the binding condition $p' < P^-(\ell)$ is easy to remove. On specializing ∇ (and some shuffling), we get the next simpler identity.

Lemma 4.2. *For any sequence ψ and $M \geq M_0 \geq 1$, we have*

$$\begin{aligned} \sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d) &= \sum_{\substack{d|\mathfrak{P}(z) \\ d < M}} \mu(d)\psi(d) + \sum_{\substack{\ell|\mathfrak{P}(z) \\ M \leq \ell < M_0 P^-(\ell)}} \mu(\ell)\psi(\ell) \\ &\quad - \sum_{\substack{\ell|\mathfrak{P}(z) \\ M_0 \leq \ell < M_0 P^-(\ell)}} \mu(\ell) \sum_{\substack{p' < P^-(\ell) \\ p' \in \mathfrak{P}(z)}} \sum_{\substack{d|\mathfrak{P}(p') \\ \ell dp' \geq M}} \mu(d)\psi(\ell dp'). \end{aligned}$$

When specializing $M = M_0$, this identity takes a simpler look, which is directly inferred from Lemma 4.1. The distinction between the parameters M and M_0 may be useful.

Proof of Lemma 4.1. Let us recall the Fundamental Sieve Identity. This is, in raw form, Eq. (1.8) of [24, Chapter 2] by H. Halberstam and H.-E. Richert, and, more explicitly, Lemma 2.1 of [9] of H. Diamond, H. Halberstam and H.-E. Richert (reproduced with some notational changes in Lemma 2 of [12] by K. Ford and H. Halberstam). It reads:

$$\sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d) = \sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d)\nabla(d) + \sum_{\ell|\mathfrak{P}(z)} \bar{\nabla}(\ell) \sum_{\delta|\mathfrak{P}(P^-(\ell))} \mu(\ell\delta)\psi(\ell\delta).$$

We have used Lemma 2 of [12] with $h(d) = \mu(d)\psi(d)$ and $D = \mathfrak{P}(z)$; then in the second sum, d and t are replaced by ℓ and δ respectively. Notice that $\mu(\ell\delta) = \mu(\ell)\mu(\delta)$. As δ and ℓ are linked in a tricky manner, we use the Buchstab Identity (see Eq. (1.9) of [24, Chapter 2] or (13) below) to write

$$\begin{aligned} \sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d) &= \sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d)\nabla(d) + \sum_{\ell|\mathfrak{P}(z)} \bar{\nabla}(\ell)\mu(\ell)\psi(\ell) \\ &\quad - \sum_{\ell|\mathfrak{P}(z)} \bar{\nabla}(\ell)\mu(\ell) \sum_{\substack{p' < P^-(\ell) \\ p' \in \mathfrak{P}}} \sum_{d|\mathfrak{P}(p')} \mu(d)\psi(\ell p' d) \end{aligned}$$

which is exactly what we announced. \square

Proof of Lemma 4.2. When $M = M_0$, the selection $\nabla(d) = \mathbf{1}_{d < M}$ in Lemma 4.1 yields Lemma 4.2. For the general case, use Lemma 4.1 on $\psi(d)\mathbf{1}_{d \geq M}$ and $\nabla(d) = \mathbf{1}_{d < M_0}$. The reader will swiftly recover the claimed identity. \square

Lemma 4.2 is at the heart of our proof, and it is methodologically interesting to note that it may be derived directly from the next decomposition.

Lemma 4.3. *Let $M_0 \geq 1$ be a real parameter and let $d \geq M_0$ be a squarefree integer. Then there exists a unique couple (δ, ℓ) such that $d = \delta\ell$, $\delta|\mathfrak{P}(P^-(\ell))$ and $M_0 \leq \ell < M_0 P^-(\ell)$.*

Proof. Let us write $d = p_1 p_2 \cdots p_r$ where $p_1 > p_2 > \cdots > p_r$. Since $M_0 \leq d$, there exists a t_0 such that $p_1 \cdots p_{t_0-1} < M_0 \leq p_1 \cdots p_{t_0}$. We choose $\ell = p_1 \cdots p_{t_0-1} p_{t_0}$ and $\delta = p_{t_0+1} \cdots p_r$. Clearly $M_0 \leq \ell = p_1 \cdots p_{t_0}$ and $M_0 p_{t_0} > p_1 \cdots p_{t_0} = \ell$. Suppose there is another decomposition of ℓ as $\ell = \delta_1 \ell_1$ with the same properties. Then there exists an $s \leq r$ such that $\ell_1 = p_1 \cdots p_s$ and $\delta_1 = p_{s+1} \cdots p_r$. We have

$$p_1 p_2 \cdots p_{t_0-1} < M_0 \leq p_1 \cdots p_s$$

which implies $t_0 \leq s$. On the other hand $\ell_1 = p_1 \cdots p_s < M_0 p_s < p_1 \cdots p_{t_0} p_s$. If $s \geq t_0 + 1$, we get that $\prod_{i=t_0+1}^{s-1} p_i < 1$, a contradiction. \square

Second proof of Lemma 4.2. By Lemma 4.3, we find that

$$(12) \quad \sum_{d|\mathfrak{P}(z)} \mu(d)\psi(d) = \sum_{\substack{d|\mathfrak{P}(z) \\ d < M}} \mu(d)\psi(d) + \sum_{\substack{\ell|\mathfrak{P}(z) \\ M_0 \leq \ell < M_0 P^-(\ell)}} \mu(\ell) \sum_{\substack{\delta|\mathfrak{P}(P^-(\ell)) \\ \delta \ell \geq M}} \mu(\delta)\psi(\ell\delta).$$

Once this identity is established, the binding condition $\delta|\mathfrak{P}(P^-(\ell))$ on δ and ℓ can be handled using the Buchstab Identity:

$$(13) \quad \sum_{\delta|\mathfrak{P}(P^-(\ell))} \mu(\delta)\mathbf{1}_{\ell\delta \geq M} \psi(\ell\delta) = \mathbf{1}_{\ell \geq M} \psi(\ell) - \sum_{\substack{p' < P^-(\ell) \\ p' \in \mathfrak{P}}} \sum_{d|\mathfrak{P}(p')} \mu(d) \mathbf{1}_{\ell dp' \geq M} \psi(\ell dp').$$

This ends the proof. \square

5. USING THE SIMPLE SIEVE IDENTITY

We use Fourier analysis to separate ℓ and p' in Lemma 4.1.

Lemma 5.1. *Let $u, v > 0$ with $v \neq u$, and let $T \geq 1$. We have*

$$\frac{4}{\pi} \int_{1/T}^T \sin^2(vt/2) \frac{\sin ut}{t} dt = \mathbf{1}_{u < v} + \mathcal{O}\left(\frac{1}{T|v-u|} + \frac{1}{Tu} + \frac{v^2 u}{T^3}\right).$$

Proof. The formula

$$\frac{1}{\pi} \int_{-T}^T e^{ivt} \frac{\sin ut}{t} dt = 1_{u>v} + \mathcal{O}\left(\frac{1}{T|v-u|}\right)$$

is classical and can for instance be found in [29, Lemma 2.2] (and it is already used in this context by R. Vaughan, see top of page 114 of [58]). We then write

$$\begin{aligned} \frac{1}{\pi} \int_{-T}^T e^{ivt} \frac{\sin ut}{t} dt &= \frac{2}{\pi} \int_0^T (\cos(vt) - 1) \frac{\sin ut}{t} dt + \frac{2}{\pi} \int_0^T \frac{\sin ut}{t} dt \\ &= \frac{-4}{\pi} \int_0^T \sin^2(vt/2) \frac{\sin ut}{t} dt + 1 + \mathcal{O}\left(\frac{1}{Tu}\right). \end{aligned}$$

We use $|\sin vt| \leq vt$ as well as $|\sin ut| \leq ut$ for the integral on the segment $[0, 1/T]$. The lemma follows readily. \square

Theorem 5.2. *For any sequence θ , any $T \geq 1$ and any $M \geq M_0 \geq 1$, we have*

$$\begin{aligned} \sum_{(n, \mathfrak{P}(z))=1} \theta(n) &= \sum_{d \mid \mathfrak{P}(z)} \mu(d) \sum_{d \mid n} \theta(n) + \sum_{M \leq \ell \leq M_0 z} \tilde{a}_\ell \theta(k\ell) - \int_{1/T}^T \sum_{\substack{k\ell \geq M \\ M_0 \leq \ell \leq M_0 z}} a_\ell(t) b_k(t) \theta(k\ell) \frac{dt}{t} \\ &\quad + \mathcal{O}\left(\frac{z}{T} \sum_{\ell \mid \mathfrak{P}(z)} \sum_{\substack{d \mid \mathfrak{P}(z) \\ \ell d \mid n}} \left| \sum_{M_0 \leq \ell < M_0 z} \theta(n) \right| \right) \end{aligned}$$

where

$$\tilde{a}_\ell = \begin{cases} \mu(\ell) & \text{if } \ell \mid \mathfrak{P}(z) \text{ and } M_0 \leq \ell < M_0 P^-(\ell), \\ 0 & \text{otherwise,} \end{cases}, \quad b_k(t) = \sum_{\substack{p' dm = k \\ p' < z, p' \in \mathfrak{P} \\ d \mid \mathfrak{P}(p')}} \mu(d) \sin(t \log p'),$$

and

$$a_\ell(t) = \begin{cases} \frac{4}{\pi} \mu(\ell) \sin^2(\log(P^-(\ell) - \frac{1}{2}) t/2) & \text{if } \ell \mid \mathfrak{P}(z) \text{ and } M_0 \leq \ell < M_0 P^-(\ell), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We use Lemma 4.2 with $\psi(d) = \sum_{d \mid n} \theta(n)$. We use Lemma 5.1 on $\log p'$ and $\log(P^-(\ell) - \frac{1}{2})$ of Lemma 4.2 and get

$$\begin{aligned} &\sum_{\substack{\ell \mid \mathfrak{P}(z) \\ M_0 \leq \ell < M_0 P^-(\ell)}} \mu(\ell) \sum_{\substack{p' < P^-(\ell) \\ p' \in \mathfrak{P}(z)}} \sum_{\substack{d \mid \mathfrak{P}(p') \\ dp' \ell \geq M}} \mu(d) \psi(\ell dp') \\ &= \frac{4}{\pi} \int_{1/T}^T \sum_{\substack{\ell \mid \mathfrak{P}(z) \\ M_0 \leq \ell < M_0 P^-(\ell)}} \mu(\ell) \sin^2(\log(P^-(\ell) - \frac{1}{2}) t/2) \sum_{\substack{p' < z, p' \in \mathfrak{P}(z) \\ d \mid \mathfrak{P}(p')} \\ dp' \ell \geq M}} \mu(d) \sin(t \log p') \psi(\ell dp') \frac{dt}{t} \\ &\quad + \mathcal{O}\left(\sum_{\substack{\ell \mid \mathfrak{P}(z) \\ M_0 \leq \ell < M_0 P^-(\ell)}} \sum_{\substack{p' < z, p' \in \mathfrak{P}(z) \\ d \mid \mathfrak{P}(p')} \\ dp' \ell \geq M}} |\psi(\ell dp')| \left(\frac{z}{T} + \frac{\log^3 z}{T^3}\right)\right). \end{aligned}$$

The theorem follows readily after the change of notation $dp' \rightarrow d$ in the last sum. \square

Proof of Theorem 1.4. We first use Lemma 2.1 to reduce Z to z and then appeal to Theorem 5.2.

First reduction. We simplify the error term by assuming that $\theta(n) = 0$ when $n > N$ and by first noticing that

$$\left| \sum_{\ell d | n} \theta(n) \right| \leq \sqrt{\frac{N}{d\ell}} \|\theta\|_2,$$

getting the error term to be \mathcal{O} of

$$\frac{z\sqrt{N}\|\theta\|_2}{T} \sum_{\substack{\ell |\mathfrak{P}(z) \\ M_0 \leq \ell < M_0 z}} \sum_{\substack{d |\mathfrak{P}(z) \\ \ell d \leq N}} \frac{1}{\sqrt{d\ell}} \ll \frac{z\sqrt{N}\|\theta\|_2}{T} \sum_{\substack{\ell |\mathfrak{P}(z) \\ M_0 \leq \ell < M_0 z}} \frac{\sqrt{N/\ell}}{\sqrt{\ell}} \ll \frac{zN\|\theta\|_2}{T} \log(M_0 z).$$

We select $T = N^3 \log N$.

Second reduction. On the integral over $[1/T, 1]$, we apply the change of variable $t \mapsto 1/t$ so that we now have the sum

$$\int_1^T \sum_{\substack{k\ell \geq M \\ M_0 \leq \ell \leq M_0 z}} a_\ell(t) b_k(t) \theta(k\ell) \frac{dt}{t} + \int_1^T \sum_{\substack{k\ell \geq M \\ M_0 \leq \ell \leq M_0 z}} a_\ell(1/t) b_k(1/t) \theta(k\ell) \frac{dt}{t}.$$

We reduce each to the interval $[0, 1]$ by the change of variable $t \mapsto e^{y \log T}$, getting

$$\int_0^1 \sum_{\substack{k\ell \geq M \\ M_0 \leq \ell \leq M_0 z}} a_\ell(T^y) b_k(T^y) \theta(k\ell) dy + \int_0^1 \sum_{\substack{k\ell \geq M \\ M_0 \leq \ell \leq M_0 z}} a_\ell(T^{-y}) b_k(T^{-y}) \log T \theta(k\ell) dy.$$

We then displace the second range of integration from 1 to 2, so that we may join both integrals with a proper definition of a_ℓ and b_k . We further write

$$\sum_{M \leq \ell \leq M_0 z} \tilde{a}_\ell \theta(k\ell) = \int_2^3 \sum_{M \leq \ell \leq M_0 z} \tilde{a}_\ell \theta(k\ell) dy$$

so that the sum of our three bilinear contributions can be folded in a single integral from 0 to 3 with coefficients $a_\ell(t)$ and $b_k(t)$ respectively bounded in absolute value by $4/\pi$ and $\tau_3(k) \log T \leq 4\tau_3(k) \log N$. It looks better to have an integration ranging from 0 to 1, something we achieve by change of variable $y' = y/3$, and divide $a_\ell(t)$ by $4/\pi$, a factor we transfer in $b_k(t)$, concluding the proof. \square

6. RECOVERING THE HARMAN SIEVE

In [27, 28], G. Harman developed his so called *Alternative Sieve* for primes. Here we provide another proof of a weak version of it.

Theorem 6.1 (Harman sieve, a weak version). *Let $z \geq 1$, \mathcal{A} and \mathcal{B} be two subsets of points on $[1, N]$ for which there exist four parameters $D \geq 1$, $\alpha \in (0, 1)$, $\lambda \in \mathbb{C}$ and $Y \geq 2$ that verify the following assumptions.*

- For any sequence of complex numbers $a(d)$ with $|a(d)| \leq 1$, we have

$$\sum_{\substack{d < D, n \in \mathcal{A} \\ d|n}} a(d) = \lambda \sum_{\substack{d < D, n \in \mathcal{B} \\ d|n}} a(d) + \mathcal{O}(Y).$$

- For any two sequences of complex numbers $a(\ell)$ and $b(m)$ such that $|a(\ell)| \leq 1$ and $|b(m)| \leq \tau_6(m)$, we have

$$\sum_{\substack{N^\alpha < \ell \leq zN^\alpha \\ m: \ell m \in \mathcal{A}}} a(\ell)b(m) = \lambda \sum_{\substack{N^\alpha < \ell \leq zN^\alpha \\ m: \ell m \in \mathcal{B}}} a(\ell)b(m) + \mathcal{O}(Y).$$

Then, for any sequence $(c_r)_{r \leq R}$ verifying $|c_r| \leq 1$ and $N^\alpha R \leq D$, we have

$$\sum_{r \leq R} c_r \sum_{\substack{n \in \mathcal{A} \\ (n, \mathfrak{P}(z))=1 \\ r|n}} 1 = \lambda \sum_{r \leq R} c_r \sum_{\substack{n \in \mathcal{B} \\ (n, \mathfrak{P}(z))=1 \\ r|n}} 1 + \mathcal{O}\left(Y \log N + \frac{RN}{z}\right).$$

We call this version “weak” as the range in R is smaller than in the full theorem of Harman, but the case $R = 1$ is already of interest. There are several versions of this theorem according to the bounds we assume on the coefficients a and b . They are all essentially equivalent in practice.

Proof. Let us use Theorem 1.4 with $Z = z$ and $M = M_0 = N^\alpha$ twice with u_n being the characteristic function of \mathcal{A} and of \mathcal{B} . Let us notice first that we may discard those r ’s which are not coprime with $\mathfrak{P}(z)$.

Linear part. We need to bound

$$\begin{aligned} \Delta_1 &= \sum_r c_r \sum_{\substack{d|\mathfrak{P}(z) \\ d < M}} \mu(d) \sum_{\substack{n \in \mathcal{A} \\ [d,r]|n}} 1 - \lambda \sum_r c_r \sum_{\substack{d|\mathfrak{P}(z) \\ d < M}} \mu(d) \sum_{\substack{n \in \mathcal{B} \\ [d,r]|n}} 1 \\ &= \sum_{s < MR} c_s^* \left(\sum_{\substack{n \in \mathcal{A} \\ s|n}} 1 - \lambda \sum_{\substack{n \in \mathcal{B} \\ s|n}} 1 \right) \end{aligned}$$

where

$$c_s^* = \sum_{\substack{[r,d]=s \\ d|\mathfrak{P}(z), d < M \\ r \leq R}} c_r \mu(d).$$

Please notice that at most one decomposition $s = [r, d]$ may occur as $d|\mathfrak{P}(z)$ and $(r, \mathfrak{P}(z)) = 1$. Therefore our first hypothesis applies with $D = RM = RN^\alpha$, gives the error term $\mathcal{O}(Y)$, provided that $R \leq D/N^\alpha$.

Bilinear part. We have

$$\Delta_2 = \sum_r c_r \left(\sum_{\substack{M_0 \leq \ell \leq M_0 z \\ r|k\ell \\ k\ell \in \mathcal{A}}} \alpha_\ell(t) \beta_k(t) - \lambda \sum_{\substack{M_0 \leq \ell \leq M_0 z \\ r|k\ell \\ k\ell \in \mathcal{B}}} \alpha_\ell(t) \beta_k(t) \right).$$

As $\alpha_\ell(t)$ has its support on $\ell|\mathfrak{P}(z)$, and c_r has its support outside of this set, the condition $r|k\ell$ reduces to $r|k$. Hence

$$\Delta_2 = \sum_{\substack{M_0 \leq \ell \leq M_0 z \\ rm\ell \in \mathcal{A}}} \alpha_\ell(t) c_r \beta_{rm}(t) - \lambda \sum_{\substack{M_0 \leq \ell \leq M_0 z \\ rm\ell \in \mathcal{B}}} \alpha_\ell(t) c_r \beta_{rm}(t)$$

from which we deduce

$$\Delta_2 = \sum_{\substack{M_0 \leq \ell \leq M_0 z \\ k\ell \in \mathcal{A}}} \alpha_\ell(t) \beta_k^*(t) - \lambda \sum_{\substack{M_0 \leq \ell \leq M_0 z \\ k\ell \in \mathcal{B}}} \alpha_\ell(t) \beta_k^*(t)$$

where $\beta_k^*(t) = \beta_k(t) \sum_{r|k} c_r$ obviously verifies $|\beta_k^*(t)| \ll \tau_6(k) \log N$. The theorem follows swiftly. \square

7. THE TRIGONOMETRIC POLYNOMIAL AROUND $\alpha = 0$

We want to approximate $S(\beta; N)$ with enough uniformity in β . This can be achieved by using small interval results that we take from [6] by Z. Cui and J. Wu.

Lemma 7.1. *We have*

$$\sum_{n \leq N} b(n)e(n\beta) = 4C \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} + \mathcal{O}\left(\frac{N}{(\log N)^{3/2}}(1 + |\beta|N^{7/10})\right).$$

The initial sum carried in fact on integers that are congruent to 1 modulo 4. The constant that appears is indeed $4C$ because the sum over n is restricted to such integers.

Proof. As an application of Theorem 1.1 of [6] with $\kappa = \alpha = 1/2$, $w = 0$, $\delta = 1/3$ (by Weil's bound for $\zeta(s)$), we get for $y \in [x^{7/10}/\log x, x]$ that

$$\sum_{x < n \leq x+y} b(n) = \frac{Cy}{\sqrt{\log x}} + \mathcal{O}\left(\frac{y}{(\log x)^{3/2}}\right).$$

It is not difficult to deduce from this estimate that

$$\sum_{x < n \leq x+y} b(n) = 4C \sum_{\substack{x < n \leq x+y \\ n \equiv 1[4]}} \frac{1}{\sqrt{\log n}} + \mathcal{O}\left(\frac{y}{(\log x)^{3/2}}\right).$$

We write, with $y = N^{7/10}/\log N$,

$$\begin{aligned} \sum_{N < n \leq 2N} b(n)e(n\beta) &= \sum_{0 \leq k \leq N/y} \sum_{N+ky < n \leq N+(k+1)y} b(n)e(n\beta) + \mathcal{O}(y) \\ &= \sum_{0 \leq k \leq N/y} e(\beta(N+ky)) \sum_{N+ky < n \leq N+(k+1)y} b(n) \\ &\quad + \mathcal{O}\left(\frac{|\beta|yN}{\sqrt{\log N}} + \frac{N}{(\log N)^{3/2}}\right) \end{aligned}$$

and after easy steps, our lemma follows. \square

8. DISTRIBUTION IN ‘SMALL’ ARITHMETIC PROGRESSIONS VIA ANALYTICAL MEANS

The distribution of Gaussian integers have been studied in several works, starting by the main Theorem of [41] of K. Prachar, then Satz 1 of [50] by G. J. Rieger and it is also treated in [32] by H. Iwaniec, or in Theorem 14.7 of [14] by J. Friedlander & H. Iwaniec.

We need a better error term for Theorem 1.5, similar to the one obtained in the paper [6]. It seems this case has not been considered, so we provide some details, though the technique in itself is not new, see [51] by J. P. Serre for instance. The Selberg-Delange method as exposed in Chapter 5, Part II of [54] by G. Tenenbaum, and more precisely in Theorem 3 of Section 5.3, would also lead to a solution. We use a path that is intermediate and relies on [50] by G. J. Rieger. Throughout this section, we use the following decomposition of the modulus $q \geq 1$:

$$(14) \quad q = q_2 q_*, \quad \text{where } q_2 \text{ is a power of 2 and } (q_*, 2) = 1.$$

Here is the main result of this section.

Lemma 8.1. *Let $\tau > 0$ and $A \geq 1$. Let $q = q_2 q_* \leq (\log N)^\tau$ and a be prime to q . When $q_* | P_{4;3}(\infty)$ and $q_2 \neq 4$, we have*

$$\begin{aligned} S\left(\frac{a}{q} + \beta; N\right) &= \frac{4C\mu(q)}{\varphi(q)} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} \\ &\quad + \mathcal{O}\left(\frac{N2^{\omega(q)} \log q}{\varphi(q)(\log N)^{3/2}} (1 + |\beta|N^{4/5})\right) + \mathcal{O}_{\tau,A}\left(\frac{N(1 + N|\beta|)}{(\log N)^A}\right). \end{aligned}$$

When $q_* | P_{4;3}(\infty)$ and $q_2 = 4$, we have

$$\begin{aligned} S\left(\frac{a}{q} + \beta; N\right) &= \frac{4Ci\chi_4(a)\mu(q_*)}{\varphi(q_*)} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} \\ &\quad + \mathcal{O}\left(\frac{N2^{\omega(q)} \log q}{\varphi(q)(\log N)^{3/2}} (1 + |\beta|N^{4/5})\right) + \mathcal{O}_{\tau,A}\left(\frac{N(1 + N|\beta|)}{(\log N)^A}\right). \end{aligned}$$

When $q_* \nmid P_{4;3}(\infty)$, we have

$$S\left(\frac{a}{q} + \beta; N\right) \ll \frac{N2^{\omega(q)} \log q}{\varphi(q)(\log N)^{3/2}} (1 + |\beta|N^{4/5}) + \frac{N(1 + N|\beta|)}{(\log N)^A}.$$

The implied constant is not effective when $\tau \geq 2$ but can be explicitly computed otherwise.

To prove this, we first prove the following lemma whose gist is that $S(\frac{a}{q} + \beta; N)$ is independent of a .

Lemma 8.2. *Let $\tau > 0$ and $A \geq 1$. Let $q \leq (\log N)^\tau$ and a be prime to q . Let $\beta \in \mathbb{R}$. We have*

$$S\left(\frac{a}{q} + \beta; N\right) = \mathcal{O}_{\tau,A}\left(\frac{N(1 + N|\beta|)}{(\log N)^A}\right) + \begin{cases} \sum_{n \leq N} \frac{c_q(n)}{\varphi(q)} b(n)e(n\beta) & \text{when } q_2 \neq 4, \\ i\chi_4(a) \sum_{n \leq N} \frac{c_{q_*}(n)}{\varphi(q_*)} b(n)e(n\beta) & \text{when } q_2 = 4. \end{cases}$$

The implied constant is not effective when $\tau \geq 2$ but can be explicitly computed otherwise.

We reproduce the necessary lemmas from [50]. In this paper, we have $T = \exp(\sqrt{\log N})$ as written on Line 6, page 207. There are two Dirichlet characters that behave like the principal character on our sequence \mathfrak{B} : the trivial character (and its induced versions) and the only non-trivial character modulo 4, say χ_4 , and its induced versions also denoted by χ_4 , as all the elements of \mathfrak{B} are congruent to 1 modulo 4. This character is denoted by χ_1 in [50]. Recall that, when n is odd, we have $\chi_4(n) = (-1)^{\frac{n-1}{2}}$. Here is a combination/adaptation of Hilfssatz 11 and 12 therein.

Lemma 8.3. *There exist two positive constants c_1 and c_2 such that, for $N \geq 100$, $q \leq \exp(\sqrt{\log N})$ and χ not induced modulo q either by the trivial character modulo 1 or by χ_4 , the non-principal character modulo 4, we have*

$$\begin{aligned} \sum_{n \leq N} \chi(n)b(n) &\ll N \exp(-c_1 \sqrt{\log N}) \\ &\quad + \begin{cases} N^{\beta(q)} (\log N)^{c_2} & \text{when } \chi \text{ is exceptional} \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

We can say under the hypothesis of Lemma 8.3 that for any $A > 0$, we have

$$\sum_{n \leq N} \chi(n)b(n) \ll_A \frac{N}{(\log N)^A}.$$

We have modified somewhat the statement of [50]: the modulus k therein is q for us. However we allow q to be even at the price of ruling out the non-principal character modulo 4. On relying on [50], Hilfssatz 2 therein tells us that a polar contribution at $s = 1$ occurs only in the two cases that we exclude. We do not provide more details on what an exceptional character is. We note that $\beta(q) = 1 - \mathcal{O}_\epsilon(1/q^\epsilon)$ for any positive ϵ by a famous Theorem of C. L. Siegel, but in an ineffective manner. Since we shall use this theorem, some of our results are ineffective.

An important consequence emerges from this lemma: the error term is indeed very small when we consider the non-principal character. We now have to consider the contribution of the principal character, but we see that its contribution is going to be independent of a , for (16). As the principal character is indeed real valued, we can now rely on [51] or on the Selberg-Delange Method.

Lemma 8.4. *We have $\tau_q(\chi_0) = \mu(q)$, and, when $4|q$, we have $\tau_q(\chi_4) = -2i\mu(q/2)$, where $\tau_q(\chi) = \sum_{b \bmod^* q} \chi(b)e(b/q)$.*

Proof. The value of the Gauss sum on the trivial character is classical. Concerning χ_4 , we split the modulus q in $q = q_2q'$ where q' is odd and q_2 is a power of 2. We have $\tau_q(\chi_4) = \tau_{q_2}(\chi_4)\tau_{q'}(\chi_0)$. We readily check that $\tau_{q_2}(\chi_4) = 0$ when $8|q_2$. Finally, we see that $\tau_4(\chi_4) = e(1/4) - e(3/4) = 2i$. We may fold these results in the formula $\tau_q(\chi_4) = -2i\mu(q/2)$, concluding the proof of this lemma. \square

Proof of Lemma 8.2. We set $\alpha = \frac{a}{q} + \beta$. Let $q \geq 3$ be a modulus and a be prime to q . Let us define

$$(15) \quad S_q(\alpha; N) = \sum_{\substack{n \leq N \\ (n, q)=1}} b(n)e(n\alpha).$$

The reader should notice that S_q depends only on the prime factors of q and not on the actual value of this parameter. With the aim of evaluating this function, we replace the additive character with a linear combination of multiplicative ones. To do this, we first notice that, for n prime to q , we have:

$$\begin{aligned} e(na/q) &= \sum_{c \bmod^* q} \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \bar{\chi}(c)\chi(n)e(ca/q) \\ &= \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \sum_{c \bmod^* q} \bar{\chi}(c)e(ca/q)\chi(n) \\ &= \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \tau_q(\bar{\chi})\chi(a)\chi(n). \end{aligned}$$

Therefore

$$(16) \quad S_q(a/q; N) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \tau_q(\bar{\chi})\chi(a) \sum_{n \leq N} b(n)\chi(n).$$

Please note that each Gauss sum $\tau_q(\bar{\chi})$ is of modulus at most \sqrt{q} .

By Lemma 8.3 with $A + \tau/2$ rather than A , when $4 \nmid q$, we have

$$(17) \quad S_q(a/q; N) - \frac{\mu(q)}{\varphi(q)} S_q(0; N) \ll_{\tau, A} \frac{N}{(\log N)^A}$$

valid for any $A \geq 0$, any $q \leq (\log N)^\tau$ and any a prime to q .

When $4|q$, then $\mu(q) = 0$ but the character χ_4 has some effect and recalling Lemma 8.4, we get

$$(18) \quad S_q(a/q; N) + \frac{2i\mu(q/2)\chi_4(a)}{\varphi(q)} S_q(0; N) \ll_{\tau, A} \frac{N}{(\log N)^A}.$$

Let us set

$$(19) \quad s(q, a) = \begin{cases} \mu(q) & \text{when } q_2 \neq 4 \\ -2i\chi_4(a)\mu(q/2) & \text{when } q_2 = 4. \end{cases}$$

First extension. We need to extend this inequality to $S_{qq'}(a/q; N)$ for any integer q' prime to q . It is better for later usage to change the notation. For integers u and v with $(u, v) = 1$, we have

$$\begin{aligned} S_{uv}(f/u; N) &= \sum_{w|v} \mu(w)b(w)S_u(fw/u; N/w) \\ &= \frac{1}{\varphi(u)} \sum_{w|v} \mu(w)b(w)s(u, fw)S_u(0; N/w) + \mathcal{O}_{A, \tau}\left((\log v)\frac{N}{(\log N)^A}\right) \\ (20) \quad &= M_1(N, u, uv, f \bmod 4) + \mathcal{O}_{A, \tau}\left((\log v)\frac{N}{(\log N)^A}\right) \end{aligned}$$

for some function M_1 . When $u_2 \neq 4$, we readily find that $M_1(N, u, uv, f \bmod 4) = \mu(u)S_{uv}(0; N)/\varphi(u)$, while, when $u_2 = 4$, the expression is a bit more intricate, but still only depends on $f \bmod 4$.

Second extension. We now have to dispense with the coprimality condition $(n, q) = 1$. To do so, we write $\delta|q^\infty$ to say that the prime factors of δ divide q . It is possible to write every integer n in the form $n = \delta m$ with $\delta|q^\infty$ and $(m, q) = 1$, and this can be done in a unique manner. Since the function $d \mapsto b(d)$ is completely multiplicative, we find that

$$S(a/q; N) = \sum_{\substack{\delta|q^\infty \\ \delta \leq N/3}} b(\delta)S_q(a\delta/q; N/\delta).$$

Notice that we may assume δ to be odd. We have

$$S_q(a\delta/q; N/\delta) = S_q\left(\frac{a\delta/(q, \delta)}{q/(q, \delta)}; N/\delta\right) = S_{\frac{q}{(q, \delta)}r_q(\delta)}\left(\frac{a\delta/(q, \delta)}{q/(q, \delta)}; N/\delta\right)$$

where $r_q(\delta) = \prod_{p|q, p \nmid q/(q, \delta)} p$. Notice that $r_q(\delta)$ may be smaller than (q, δ) , which is why we need this extra notation. Let us resume the main evaluation:

$$\begin{aligned} (21) \quad S(a/q; N) &= \sum_{\substack{\delta|q^\infty \\ \delta \leq N/3}} b(\delta)S_{\frac{q}{(q, \delta)}r_q(\delta)}\left(\frac{a\delta/(q, \delta)}{q/(q, \delta)}; N/\delta\right) \\ &= M_2(q, N) + \mathcal{O}\left(N \sum_{\substack{\delta|q^\infty \\ \delta \leq N/3}} \frac{1}{\delta} \frac{1}{(\log(N/\delta))^A}\right) \end{aligned}$$

where $M_2(q, N)$ is the 'main term' and is defined as

$$(22) \quad M_2(q, N) = \sum_{\substack{\delta|q^\infty \\ \delta \leq N/3 \\ (\delta, 2)=1}} b(\delta)M_1\left(N, \frac{q}{(q, \delta)}, \frac{q}{(q, \delta)}r_q(\delta), \frac{a\delta}{(q, \delta)} \bmod 4\right)$$

by appealing to (20). We find again that, when $q_2 \neq 4$, this main term is independent of a , while, when $q_2 = 4$, it depends only on the class of a modulo 4. Concerning the error term in (21), when $\delta \geq \sqrt{N}$, we use

$$\begin{aligned} \sum_{\substack{\delta|q^\infty \\ \sqrt{N} \leq \delta \leq N/3}} \frac{1}{\delta} \frac{1}{(\log(N/\delta))^A} &\leq \sum_{\delta|q^\infty} \frac{1}{\delta} \left(\frac{\delta}{\sqrt{N}} \right)^{1/2} \\ &\leq \frac{1}{N^{1/4}} (1 - 1/\sqrt{2})^{-\omega(q)} \ll \frac{1}{N^{1/4}} 4^{\frac{\log q}{\log 2}} \\ &\ll \frac{1}{N^{1/4}} 8^{\tau \log \log N} \ll_{\tau,A} \frac{1}{(\log N)^A} \end{aligned}$$

since $q \leq (\log N)^\tau$. For the smaller δ , we use

$$\sum_{\substack{\delta|q^\infty \\ \delta \leq \sqrt{N}}} \frac{1}{\delta} \frac{1}{\log(N/\delta)^A} \ll \frac{1}{(\log N)^A} \prod_{p|q} (1 + 1/p) \ll \frac{\log q}{(\log N)^A}.$$

We conclude that

$$S(a/q; N) - M_2(q, N) \ll_{\tau,A} \frac{N \log q}{(\log N)^A}.$$

The expression for $M_2(q, N)$ is rather unwieldy but discloses that this quantity does not depend on a . We may therefore sum over a' congruent to a modulo q/q_* , and prime to q_* . On changing A to $A + \tau + 1$, we find that

$$(23) \quad S(a/q; N) = \mathcal{O}_{\tau,A} \left(\frac{N}{(\log N)^A} \right) + \begin{cases} \sum_{n \leq N} \frac{c_q(n)}{\varphi(q)} b(n) & \text{when } q_2 \neq 4, \\ i\chi_4(a) \sum_{n \leq N} \frac{c_{q_*}(n)}{\varphi(q_*)} b(n) & \text{when } q_2 = 4. \end{cases}$$

Analytic variations.

We readily get:

$$\begin{aligned} S(\alpha; N) &= \sum_{n \leq N} b(n) e(na/q) e(n\beta) \\ &= \sum_{n \leq N} b(n) e(na/q) \left(2i\beta\pi \int_0^n e(\beta t) dt + 1 \right) \\ &= 2i\pi\beta \int_0^N e(\beta t) (S(a/q; N) - S(a/q; t)) dt + S(a/q; N). \end{aligned}$$

On using (23), $c_q(n) = \sum_{d|n, d|q} d\mu(q/d)$ and the fact that the $d \mapsto b(d)$ function is completely multiplicative, we find that

$$\begin{aligned} S(\alpha; N) &= \sum_{d|q} \frac{\mu(q/d)db(d)}{\varphi(q)} \left(2i\pi\beta \int_0^N e(\beta t) \left(B\left(\frac{N}{d}\right) - B\left(\frac{t}{d}\right) dt + B\left(\frac{N}{d}\right) \right) \right. \\ &\quad \left. + \mathcal{O}_{\tau,A} \left(\frac{N(1 + N|\beta|)}{(\log N)^A} \right) \right) \end{aligned}$$

where $B(t) = \sum_{n \leq t} b(n)$ is defined in (6). The integral may also be written in the form

$$\int_0^{N/d} e(d\beta u) (B(N/d) - B(u)) du + B(N/d).$$

Lemma 8.2 follows swiftly. \square

We now first restate Lemma 8.2 in the format used in Lemma 7.1.

Lemma 8.5. *Let $\tau > 0$ and $A \geq 1$. Let $q \leq (\log N)^\tau$, a prime to q and let q^* be the largest divisor of q such that $b(q^*) = 1$. When $q_2 \neq 4$, we have*

$$\begin{aligned} S\left(\frac{a}{q} + \beta; N\right) &= 4C \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} \frac{\mu(q/q^*)c_{q^*}(n)}{\varphi(q)} \\ &\quad + \mathcal{O}\left(\frac{N2^{\omega(q)} \log q}{\varphi(q)(\log N)^{3/2}} (1 + |\beta|N^{4/5})\right) + \mathcal{O}_{\tau,A}\left(\frac{N(1 + N|\beta|)}{(\log N)^A}\right). \end{aligned}$$

When $q_4 = 4$, we have

$$\begin{aligned} S\left(\frac{a}{q} + \beta; N\right) &= 4Ci\chi_4(a) \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} \frac{\mu(q_*/q^*)c_{q^*}(n)}{\varphi(q_*)} \\ &\quad + \mathcal{O}\left(\frac{N2^{\omega(q)} \log q}{\varphi(q)(\log N)^{3/2}} (1 + |\beta|N^{4/5})\right) + \mathcal{O}_{\tau,A}\left(\frac{N(1 + N|\beta|)}{(\log N)^A}\right). \end{aligned}$$

Proof. Let us set, for this proof,

$$M(q, N, \beta) = \sum_{d|q} \frac{\mu(q/d)db(d)}{\varphi(q)} S(d\beta; N/d).$$

This is the main term obtained in Lemma 8.2 when $q_2 \neq 4$. Otherwise the main term is $\chi_4(a)M(q_*, N, \beta)$. By Lemma 7.1, we find that, when $q \leq N^{1/10}$, we have

$$M(q, N, \beta) = 4C \sum_{d|q} \frac{\mu(q/d)db(d)}{\varphi(q)} \sum_{\substack{3 \leq n \leq N/d \\ n \equiv 1[4]}} \frac{e(nd\beta)}{\sqrt{\log n}} + \mathcal{O}\left(\frac{N2^{\omega(q)}(1 + |\beta|N^{4/5})}{\varphi(q)(\log N)^{3/2}}\right).$$

To replace $\log n$ by $\log(nd)$, we note that

$$\frac{1}{\sqrt{\log n}} - \frac{1}{\sqrt{\log(nd)}} = \frac{\log d}{\sqrt{(\log n)(\log(nd))}(\sqrt{\log n} + \sqrt{\log(nd)})} \leq \frac{\log d}{(\log n)^{3/2}},$$

from which we deduce that

$$\begin{aligned} M(q, N, \beta) &= 4C \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} \sum_{\substack{d|q \\ d|n}} \frac{\mu(q/d)db(d)}{\varphi(q)} + \mathcal{O}\left(\frac{N2^{\omega(q)} \log q}{\varphi(q)(\log N)^{3/2}} (1 + |\beta|N^{4/5})\right) \\ &= 4C \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} \frac{\mu(q/q^*)c_{q^*}(n)}{\varphi(q)} + \mathcal{O}\left(\frac{N2^{\omega(q)} \log q}{\varphi(q)(\log N)^{3/2}} (1 + |\beta|N^{4/5})\right). \end{aligned}$$

as announced. \square

Lemma 8.5 can be simplified.

Proof of Lemma 8.1. Our main remark is the following estimate, valid provided $d \nmid 2$:

$$\sum_{\substack{n \leq M \\ n \equiv 1[4]}} c_d(n) = \sum_{\substack{n \leq M \\ n \equiv 1[4]}} \sum_{\delta|n, \delta|d} \mu(d/\delta)\delta = \sum_{\delta|d} \delta \mu(d/\delta) \sum_{\substack{n \leq M \\ n \equiv 1[4] \\ \delta|n}} 1 \ll \phi_+(d)$$

where

$$(24) \quad \phi_+(d) = d \prod_{p|d} (1 + 1/p).$$

We deduce for this bound that $\sum_{\substack{n \leq M \\ n \equiv 1[2]}} e(n\beta)c_d(n) \ll (1 + |\beta|N)\phi_+(d)$. Hence, the main term given in Lemma 8.5 is small when $q^* \neq 1$. \square

9. A LOCAL MODEL

We consider some (large) positive real number K and put

$$(25) \quad S_K^\flat(\alpha; N) = 4C \prod_{\substack{p \leq K \\ p \equiv 3[4]}} \left(1 - \frac{1}{p}\right)^{-1} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} \frac{e(n\alpha)}{\sqrt{\log n}}.$$

Lemma 9.1. *When $4\alpha \notin \mathbb{Z}$, we have $\sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(\alpha n)}{\sqrt{\log n}} \ll 1/\|4\alpha\|$.*

Proof. Indeed, by summation by parts, we find that the sum, say $\Sigma(\alpha)$, may be rewritten as

$$\Sigma(\alpha) = \int_3^N \sum_{\substack{3 \leq n \leq t \\ n \equiv 1[4]}} e(\alpha n) \frac{dt}{t(\log t)^{3/2}} + \frac{1}{\sqrt{\log N}} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} e(\alpha n) \ll 1/\|4\alpha\|.$$

\square

Lemma 9.2. *When $\alpha = \frac{a}{q} + \beta$, $q|4d$ and $d|P_{4;3}(\infty)$, let us definewe have*

$$\Sigma_d(N; \alpha) = \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ d|n}} \frac{e(n\alpha)}{\sqrt{\log n}}.$$

We have $\Sigma_d(N; \alpha) = e(aq_*/q_2)\Sigma_q(N; \beta)$ which is therefore independent on a prime to q when $q_2 \neq 4$ and depends only on a mod 4 when $q_2 = 4$.

Proof. Let $n_0 \geq 3$ be the smallest integer solution to $n \equiv 1[4]$ and $d|n$. Let us write

$$\frac{a}{q} \equiv \frac{a_2}{q_2} + \frac{a_*}{q_*} \pmod{1}.$$

We have

$$\begin{aligned} \frac{na}{q} &\equiv \frac{n_0 a}{q} + \frac{(n - n_0)a}{q} \equiv \frac{n_0 a}{q} \pmod{1} \\ &\equiv \frac{n_0 a_2}{q_2} + \frac{n_0 a_*}{q_*} \equiv \frac{n_0 a_2}{q_2} \pmod{1} \end{aligned}$$

because $q_*|d|n_0$. We also know that $q_2|4$ (as $q|4d$), that $n_0 \equiv 1[4]$ and that $a_2 \equiv aq_*^{-1}[q_2] \equiv aq_*[q_2]$ because, modulo 2 or 4, a class equals its inverse class. \square

Lemma 9.3. *Let $Q = P_{4;3}(K)$. Let $\alpha \in \mathbb{R}/\mathbb{Z}$ be given with a rational approximation $\alpha - a/q = \beta$, where q is a positive integer, a is coprime with q and $qQ|\beta| \leq 1$. Write $q = q_2q_*$ with q_2 a power of 2 and q_* odd. We have, when $q_2 \nmid 4$ or $q_* \nmid P_{4;3}(K)$:*

$$S_K^\flat(\alpha; N) \ll qe^K.$$

When $q_2 \neq 4$ and $q_ | P_{4;3}(K)$, we find that*

$$S_K^\flat(\alpha; N) = \frac{4\mu(q)C}{\varphi(q)} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} + \mathcal{O}\left(\frac{e^{-K/4}N}{q\sqrt{\log N}} + qe^{K/4}\right).$$

When $q_2 = 4$ and $q_* \mid P_{4;3}(K)$, we find that

$$S_K^b(\alpha; N) = \frac{4\mu(q_*)Ci\chi_4(a)}{\varphi(q_*)} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} + \mathcal{O}\left(\frac{e^{-K/4}N}{q\sqrt{\log N}} + qe^{K/4}\right).$$

Proof. We set $\delta(K) = \varphi(P_{4;3}(K))/P_{4;3}(K)$. We readily find that

$$\begin{aligned} \delta(K) \frac{S_K^b(\alpha; N)}{4C} &= \sum_{d \mid P_{4;3}(K)} \mu(d) \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ d \mid n}} \frac{e(n\alpha)}{\sqrt{\log n}} \\ &= \sum_{\substack{d \mid P_{4;3}(K) \\ q \mid 4d}} \mu(d) \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ d \mid n}} \frac{e(n\alpha)}{\sqrt{\log n}} + \mathcal{O}\left(\sum_{d \mid P_{4;3}(K)} q\right) \end{aligned}$$

by Lemma 9.1. Notice that, by the prime number theorem modulo 4, we have $\sum_{d \mid P_{4;3}(K)} 1 \ll e^{(1+o(1))(\log 2)^{\frac{K}{2\log K}}} \ll_\varepsilon e^{\varepsilon K}$ for any $\varepsilon > 0$. Let us write $q = q_2 q_*$ where q_2 is a power of 2 and q_* is odd. The first sum of course is empty when $q_* \nmid P_{4;3}(K)$ or when $q_2 \nmid 4$. Lemma 9.2 implies that the main term above does not depend on a when $q_2 \neq 4$, and only on $a \pmod 4$ when $q_2 = 4$. In the first case, we may thus average over all a prime to q , and over all a' in $(\mathbb{Z}/4q_*\mathbb{Z})^\times$ congruent to a modulo 4. In the first case, this gives us, when $q_* \mid P_{4;3}(K)$:

$$\delta(K) \frac{S_K^b(\alpha; N)}{4C} = \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} \frac{e(n\beta)c_q(n)}{\varphi(q)\sqrt{\log n}} + \mathcal{O}_\varepsilon(qe^{\varepsilon K}).$$

But as q and n are coprime, the dependence in q can simply be factored out, getting

$$\delta(K) \frac{S_K^b(\alpha; N)}{4C} = \frac{\mu(q)}{\varphi(q)} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} \frac{e(n\beta)}{\sqrt{\log n}} + \mathcal{O}(qe^{\varepsilon K}).$$

To further study the main term, we assume that $\mu(q) \neq 0$. We use summation by parts to infer that

$$\begin{aligned} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} \frac{e(n\beta)}{\sqrt{\log n}} &= \int_3^N \sum_{\substack{3 \leq n \leq t \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} 1 \left(2i\pi\beta \frac{e(t\beta)}{\sqrt{\log t}} + \frac{e(\beta t)}{2t(\log t)^{3/2}} \right) dt \\ &\quad + \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} 1 \frac{e(\beta N)}{\sqrt{\log N}}. \end{aligned}$$

We employ the approximation $\sum_{\substack{3 \leq n \leq t, n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} 1 = \delta(K) \frac{t}{4} + \mathcal{O}_\varepsilon(e^{\varepsilon K})$ and reach

$$\begin{aligned} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} \frac{e(n\beta)}{\sqrt{\log n}} &= \delta(K) \int_3^N \sum_{\substack{3 \leq n \leq t \\ n \equiv 1[4]}} 1 \left(2i\pi\beta \frac{e(t\beta)}{\sqrt{\log t}} + \frac{e(\beta t)}{2t(\log t)^{3/2}} \right) dt \\ &\quad + \delta(K) \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} 1 \frac{e(\beta N)}{\sqrt{\log N}} + \mathcal{O}_\varepsilon\left(\frac{e^{\varepsilon K}(1 + N|\beta|)}{\sqrt{\log N}}\right). \end{aligned}$$

The approximation is the same quantity with $K = 1$, therefore

$$\mu(q)\varphi(q)\delta(K) \frac{S_K^b(\alpha; N)}{4C} = \delta(K) \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4]}} \frac{e(n\beta)}{\sqrt{\log n}} + \mathcal{O}_\varepsilon \left(\frac{e^{\varepsilon K} |\beta| N}{\sqrt{\log N}} + q e^{\varepsilon K} \right).$$

Finally, we notice that $\delta(K)^{-1} \ll \log K$ and that $|\beta| \ll e^{-K/3}/q$. The lemma is proved in the case $q_2 \neq 4$.

When $q_2 = 4$, we skip some steps and reach

$$\delta(K) \frac{S_K^b(\alpha; N)}{4C} = i\chi_4(a) \frac{\mu(q_*)}{\varphi(q_*)} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[4] \\ (n, P_{4;3}(K))=1}} \frac{e(n\beta)}{\sqrt{\log n}} + \mathcal{O}(qe^{\varepsilon K}).$$

The lemma follows readily. \square

Lemma 9.4. *For any $\ell > 2$ and $K \geq 2$, we have*

$$\int_0^1 \left| S_K^b(\alpha; N) \right|^\ell d\alpha \ll \sqrt{\log K} \frac{N^{\ell-1}}{(\log N)^{\ell/2}}.$$

Anticipating on Lemma 13.1, the above loses a factor $\sqrt{\log K}$.

Proof. We simply use Parseval:

$$\begin{aligned} \int_0^1 \left| S_K^b(\alpha; N) \right|^\ell d\alpha &\leq (S_K^b(0; N))^{\ell-2} C^2 \prod_{\substack{p \leq K \\ p \equiv 3[4]}} \left(1 - \frac{1}{p} \right)^{-2} \sum_{\substack{3 \leq n \leq N \\ n \equiv 1[2] \\ (n, P_{4;3}(K))=1}} \frac{1}{\log n}, \\ &\ll \delta(K)^{-\ell} \frac{(\delta(K)N)^{\ell-2}}{(\log N)^{\frac{\ell-2}{2}}} \delta(K) \frac{N}{\log N} \end{aligned}$$

where $\delta(K) = \prod_{\substack{p \leq K \\ p \equiv 3[4]}} (1 - 1/p)$. The lemma follows readily. \square

10. THE TRIGONOMETRIC POLYNOMIAL IN THE LARGE

Here are Lemma 3 and a modification of Lemma 2 of [57] by R. Vaughan.

Lemma 10.1. *Assume that $|q\alpha - a| \leq 1/q$ for some a prime to q . Then we have*

$$\sum_{u \leq U} \max_{Z \leq UV/u} \left| \sum_{v \leq Z} a_u e(uv\alpha) \right| \leq \|a\|_\infty \left(\frac{UV}{q} + U + q \right) \log(UVq).$$

Lemma 10.2. *Assume that $|q\alpha - a| \leq 1/q$ for some a prime to q . Then we have*

$$\sum_{u \leq U} \max_{Z \leq Y} \left| \sum_{v \leq Z} a_u b_v e(uv\alpha) \right| \leq \|a\|_2 \|b\|_2 \log(UYq)^{5/2} \sqrt{UYq^{-1} + U + V + q}.$$

It is convenient to extend these two lemmas in the form given in Lemma 4 in [27] by G. Harman. The proof of which lies in fact between Eq. (15) and (16) of [57]. We are slightly more precise than G. Harman in the dependence in the coefficients.

Lemma 10.3. *Assume that $|q\alpha - a| \leq 1/q$ for some a prime to q . Then for $R \geq 1/2$, $U' \leq 2U$, $V' \leq 2V$ and $X' \leq 2X$ we have*

$$\begin{aligned} & \sum_{R < r \leq 2R} \left| \sum_{\substack{U < u \leq U' \\ V < v \leq V' \\ X < uv \leq X'}} a_u b_v e(ruv\alpha) \right| \\ & \leq \|a\|_{2,2} \|b\|_2 R \sqrt{X} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RX}} + \frac{1}{\sqrt{V}} + \frac{1}{\sqrt{RU}} \right) \log(RXq)^3 \end{aligned}$$

where the norm $\|a\|_{2,2}$ is defined by $\|a\|_{2,2}^2 = \sum_u d(u)|a_u|^2$, the function $d(u)$ being the number of divisors of u .

We state this inequality with a symmetric left-hand side: U and V may thus be interchanged to decrease the right-hand side. The size conditions $u \in (U, U']$ and $v \in (V, V']$ can easily be carried by altering the sequences (a_u) and (b_v) . It is better to use the above when $U \leq X^{1/2}$ and to reverse the roles of U and V otherwise.

Proof. Let us denote by S the sum to be studied. We write

$$\begin{aligned} S &= \sum_{R < r \leq 2R} \sum_{U < u \leq 2U} a_u \sum_{rX < ruv \leq rX'} c_r b_v \mathbf{1}_{V < v \leq V'} e(ruv\alpha) \\ &\leq 2 \sum_{UR < w \leq 4UR} A_w \max_{Z \leq 2RX} \left| \sum_{v \leq Z/w} b_v^* e(wv\alpha) \right| \end{aligned}$$

with an obvious notation.

Now we can apply Lemma 10.2. We first notice that

$$\begin{aligned} \|A\|_2^2 &\leq \sum_w \left(\sum_{ur=w} |a_u| \right)^2 \leq \sum_u |a_u|^2 \sum_{u|w} d(w) \\ &\ll RU \log(RU) \sum_u \frac{d(u)|a_u|^2}{u} \ll R \sum_u d(u)|a_u|^2 \log(RU). \end{aligned}$$

The lemma follows readily. \square

The aim of this section is the following crucial lemma.

Lemma 10.4. *Let $|q\alpha - a| \leq 1/q$ with $q \leq N$ and $(a, q) = 1$. We have*

$$\frac{S(\alpha; N)}{N/\sqrt{\log N}} \ll \left(\frac{1}{\sqrt{q}} + \frac{1}{N^{1/6}} + \sqrt{\frac{q}{N}} \right) (\log N)^7.$$

As the same method would work for the primes with the same result, it is interesting to compare with [57, Theorem 1] of R. Vaughan. If we forget the log-powers, our result has the worse $N^{-1/6}$ compared with $N^{-1/5}$ there.

Proof. We start by localizing the variable n and set $S^*(\alpha, N) = \sum_{N/2 < n \leq N} b(n)e(n\alpha)$. Theorem 1.4 with $Z = \sqrt{N}$ proposes a decomposition of S^* into two types of sum that we study one after the other. We select $M = M_0$ and set $\alpha = \frac{a}{q} + \frac{\beta}{q^2}$.

Study of the linear part. Lemma 10.1 gives us directly

$$(26) \quad \sum_{\substack{d \mid P_{4,3}(z) \\ d \leq M}} \mu(d) \sum_{\substack{n \equiv 0[d] \\ n \equiv 1[4] \\ N/2 < n \leq N}} e(n\alpha) \ll \left(\frac{N}{q} + M + q \right) \log(Nq).$$

Study of the bilinear part.

We localize the variable ℓ in a dyadic interval $[L, L'] \subset [M, Mz]$ with $L' \leq 2L$. Let a_ℓ^* denotes either \tilde{a}_ℓ or $a_\ell(t)$ for some t , and $b_k^* = b_k(t)$ for some t . Lemma 10.3 applies with $R = 1/2$ and yields the upper bound

$$(27) \quad N(\log qN)^{9/2} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{N}} + \frac{1}{\sqrt{\min(L, N/L)}} \right).$$

Gathering the estimates. On gathering (26) and (27) together with the error term given by Theorem 1.4, we reach

$$\begin{aligned} S^*(\alpha, N)/N &\ll \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{N}} + \frac{1}{\sqrt{z}} + \frac{1}{\sqrt{M}} + \frac{\sqrt{Mz}}{\sqrt{N}} \right) (\log N)^{11/2} \log T \\ &\quad + \frac{M \log N}{N} + \frac{\log N}{q} + \frac{z(\log N)^3}{T}. \end{aligned}$$

We select $M = z = N^{1/3}$ and $T = N$, getting

$$S^*(\alpha, N) \ll \left(\frac{N}{\sqrt{q}} + N^{5/6} + \sqrt{Nq} \right) (\log N)^{13/2}.$$

We sum diadically over N to get the claimed final estimate. \square

11. THE TRIGONOMETRIC POLYNOMIAL AT RATIONALS WITH SMALL DENOMINATOR

In Section 8, we analysed $S(\alpha; N)$ when α is close to a rational a/q with q being small by using Dirichlet series. The two consequences are the lack of effectivity when $q > (\log N)^2$ and the lesser generality of the proof. The main result of this section is Lemma 11.3 which restores effectivity. A closer look discloses that we would be able to accommodate a general sieve setting. We refrain to do so because we want the reader to see clearly where we fail, in this specific example, to get $\sqrt{q}/\varphi(q)$ as the main of our bound.

As in Lemma 7.1, we shall understand the analytic factor $e(n\alpha)$ in $S(\frac{a}{q} + \beta; N)$ as a control of the behaviour in small intervals. Hence, to handle it, it is enough to understand the behaviour of $b(n)e(na/q)$ in small intervals. This is the topic of this section. We start with a sieve lemma.

Lemma 11.1. *Assume $2 \leq z^2 \leq L$, $m \geq 1$ and $\log(2m) \leq \sqrt{\log z}$. Then we have*

$$\sum_{\substack{m=m_1-m_2 \\ (m_1 m_2, P_{4;3}(z))=1 \\ M < m_1 \leq M+L}} 1 \ll \frac{m}{\varphi(m)} \frac{L}{\log z}.$$

Proof. This is for instance a simple instance of Montgomery's sieve. Let us denote by Σ the quantity to be bounded above. We give some details. Notice that $(m_1, P_{4;3}(z)) = 1$. The mentioned sieve provides us with the bound $\Sigma \leq (L + z^2)/G(z)$ where $G(z) = \sum_{d|P_{4;3}(z)=1} \mu^2(d) \prod_{p|d} g_m(p)$ and

$$g_m(p) = \begin{cases} \frac{2}{p-2} & \text{if } (m, p) = 1 \text{ and } p|P_{4;3}(z), \\ \frac{1}{p-1} & \text{if } p|m \text{ and } p|P_{4;3}(z), \\ 0 & \text{when } p \nmid P_{4;3}(z). \end{cases}$$

We appeal for instance to the book [17, Chapter 2, Theorem 2] of G. Greaves to evaluate the function G . Notice that

$$\sum_{p \leq t} g_m(p) \log p = \log t + \mathcal{O}(\log \log(3m)).$$

We thus infer that

$$G(z) \gg \prod_{\substack{p \leq z \\ p|P_{4,;3}(z)}} (1 + g_m(p)) \gg \prod_{\substack{p|m \\ p|P_{4,;3}(z)}} \frac{p-2}{p-1} (\log z).$$

We finally notice that

$$\prod_{\substack{p|m \\ p|P_{4,;3}(z)}} \frac{p-1}{p-2} \leq \prod_{\substack{p|m \\ p|P_{4,;3}(z)}} \frac{p-1}{p-2} \frac{p-1}{p} \prod_{\substack{p|m \\ p|P_{4,;3}(z)}} \frac{p}{p-1} \ll m/\varphi(m).$$

The lemma follows readily. \square

Lemma 11.2. *Let $A, B \geq 1$. Let $N/(\log N)^B \leq U \leq N$, $q \leq (\log N)^B$ and $(a, q) = 1$. For any $A \geq 1$, we have*

$$\frac{S(\frac{a}{q}; N) - S(\frac{a}{q}; N-U)}{U/\sqrt{\log N}} \ll_{A,B} \frac{\sqrt{q \log \log N} \log \log \log N}{\varphi(q)} + \frac{1}{(\log N)^A}.$$

The implied constant can be effectively computed.

This can be compared with [62, Theorem 2a, Chapter IX] in the book of I. M. Vinogradov, where, in the case of primes, the author gets $(\log N)^\varepsilon$ (for any positive ε) rather than our $\sqrt{\log \log N} \log \log \log N$.

Proof of Lemma 11.2. We may assume that N is so large that $N^{1/2}q\sqrt{\log N} \leq N^{3/4} \leq U$, for the bound we claim is otherwise trivial to obtain. We use Theorem 1.3 with $D = N^{1/4}$.

Estimation of the linear part. As in the proof of (26), we readily get

$$(28) \quad \sum_{\substack{d|P_{4,;3}(z) \\ d \leq D \\ q \nmid 4d}} \mu(d) \sum_{\substack{N-U < n \leq N \\ n \equiv 0[d] \\ n \equiv 1[4]}} e(na/q) \ll \sum_{1 \leq b \leq q} \frac{D}{q} \frac{q}{b} \ll N^{1/4} \log 4q.$$

When $q|4d$, we need to refine (28). We write $q = q_2 q_*$ with $q_2|4$ and $(q_*, 2) = 1$ and proceed as follows. A reasoning similar to the one used in Lemma 9.2 leads to

$$(29) \quad \sum_{\substack{d|P_{4,;3}(z) \\ d \leq D \\ q \nmid 4d}} \mu(d) \sum_{\substack{n \equiv 0[d] \\ n \equiv 1[4] \\ N-U < n \leq N}} e(na/q) = \sum_{\substack{d|P_{4,;3}(z) \\ d \leq D \\ q_*|d}} \frac{e(aq_*/q_2)\mu(d)U}{4d} + \mathcal{O}(D/q).$$

On using Lemma 3.2, we complete the sum and find that

$$(30) \quad \begin{aligned} \sum_{\substack{d|P_{4,;3}(z) \\ d \leq D \\ q_* \nmid d}} \frac{\mu(d)}{d} &= \frac{\mu(q_*)}{q_*} \prod_{p < z, p \equiv 3[4]} \left(1 - \frac{1}{p}\right) \prod_{p|q_*} \left(1 - \frac{1}{p}\right)^{-1} \\ &\quad + \mathcal{O}\left(\sqrt{\log z} \exp\left(\frac{-\log D}{\log z} \log \frac{\log D}{2 \log z}\right)\right) \\ &\ll \frac{1}{\varphi(q)\sqrt{\log z}} + \sqrt{\log z} \exp\left(\frac{-\log D}{\log z} \log \frac{\log D}{2 \log z}\right), \end{aligned}$$

uniformly in $q \leq N$ and provided that $\log z \geq \sqrt{\log N}$ say.

Bilinear part – Preliminary treatment. Let us now turn towards the treatment of the bilinear part. We localize the variable p in a dyadic interval $[P, P'] \subset [z, \sqrt{N}]$ with $P' \leq 2P$. It turns out that this would be enough when $U = N$ but does not

suffice in general. So we subdivide the diadic interval $[P, P']$ in subintervals of size at most W : say $[P^*, P^* + W]$, meaning that we study

$$\Sigma_P(W, P^*) = \sum_{\substack{N-U < mp \leq N \\ (m, P_{4;3}(z))=1 \\ P^* \leq p \leq P^* + W \\ p \equiv 3[4]}} \rho(m)e(mp/q).$$

In this sum, we replace the condition $mp \in (N - U, N]$ by $mp^* \in (N - U, N]$, getting a new sum we denote by $\Sigma_P^0(W, P^*)$. For each p , we find that

$$\frac{N-U}{P^*} - \frac{N-U}{p} + \frac{N}{P^*} - \frac{N}{p} \leq \frac{(N-U)W}{P^{*2}} + \frac{NW}{P^{*2}} \leq \frac{2NW}{P^2}.$$

Since we have about $\frac{1}{2}P/\log P$ primes p , and as this upper bound is ≥ 1 , this amounts to a total number of couples (p, m) that is at most $\mathcal{O}(NW/[P \log P])$. We directly select $W = \sqrt{P}$ and use $\Sigma_P^0(\sqrt{P}, P^*) = \Sigma_P^0(P^*)$.

Bilinear part – Applying Cauchy. Let us resume the study of Σ by employing Cauchy's inequality but we keep part of the information that ℓ is prime by using an enveloping sieve up to P^η . This means that we majorize the characteristic function of the primes between P^* and $P^* + W$ by an upper bound sieve. We do so by using the Selberg sieve and add a little twist: we do not sieve out the prime factors of q . The readers may find the details for instance in the paper [37] by van J. E. Lint & H.-E. Richert. Here is what we get:

$$\begin{aligned} |\Sigma_P^0(P^*)|^2 &\ll \frac{W}{\log P} \sum_{P^* \leq \ell \leq P^* + W} \left(\sum_{\substack{d|\ell \\ (d,q)=1}} \lambda_d \right)^2 \left| \sum_{\substack{N-U < mP^* \leq N \\ (m, P_{4;3}(z))=1}} \rho(m)e(m\ell a/q) \right|^2 \\ &\ll \frac{W}{\log P} \sum_{\substack{\frac{N-U}{P^*} < m_1, m_2 \leq \frac{N}{P^*} \\ (m_1 m_2, P_{4;3}(z))=1}} \rho(m_1)\rho(m_2) \sum_{\ell \in I(m_1, m_2)} \left(\sum_{\substack{d|\ell \\ (d,q)=1}} \lambda_d \right)^2 e\left(\frac{(m_1 - m_2)\ell a}{q}\right) \end{aligned}$$

where $I(m_1, m_2)$ is an interval of length at most W . Notice that $m_1 - m_2 = m$ has at most $\frac{m}{\varphi(m)} \frac{U}{P \log z}$ solutions when $m \neq 0$ by Lemma 11.1.

Bilinear part – Diagonal contribution. Since m lies in an interval of length $\mathcal{O}(U/P)$, the diagonal contribution C , i.e. when $m \equiv 0[q]$, satisfies

$$C \ll \frac{W}{\log P} \left(\underset{[\mathbf{m}=0]}{\frac{U}{P\sqrt{\log z}}} + \sum_{q|m \ll U/P} \frac{m}{\varphi(m)} \frac{U}{P \log z} \right) \frac{W}{\frac{\varphi(q)}{q} \log P}.$$

We write $m = qt$ and notice that $\frac{m}{\varphi(m)} \leq \frac{q}{\varphi(q)} \frac{t}{\varphi(t)}$ so that

$$\begin{aligned} C &\ll \left(\frac{U}{P\sqrt{\log z}} + \frac{U^2}{\varphi(q)P^2 \log z} \right) \frac{qW^2}{\varphi(q)(\log P)^2} \\ &\ll \left(\frac{qP\sqrt{\log z}}{U} + 1 \right) \frac{qU^2W^2}{(\varphi(q)P \log P)^2 \log z} \ll \frac{qU^2W^2}{(\varphi(q)P \log P)^2 \log z}. \end{aligned}$$

since $P \leq N^{1/2}$ and $N^{1/2}q\sqrt{\log N} \leq U$.

Bilinear part – Off-diagonal contribution. By off-diagonal, we mean $m \not\equiv 0[q]$. First notice that

$$\begin{aligned} \sum_{\ell \in I(m_1, m_2)} \left(\sum_{\substack{d|\ell \\ (d,q)=1}} \lambda_d \right)^2 e\left(\frac{m\ell a}{q}\right) &= \sum_{\substack{d_1, d_2 \leq P^{2\eta} \\ (d_1 d_2, q)=1}} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{\ell \in I(m_1, m_2) \\ [d_1, d_2]|\ell}} e\left(\frac{m\ell a}{q}\right) \\ &\ll qP^{4\eta}. \end{aligned}$$

The contribution of the m -sum is

$$\ll \sum_{m \ll U/P} \frac{m}{\varphi(m)} \frac{U}{P \log z} \ll \frac{U^2}{P^2 \log z}.$$

Bilinear part – Resuming the proof. We gather both estimates and reach

$$\begin{aligned} |\Sigma_P^0(P^*)|^2 &\ll \frac{qU^2W^2}{(\varphi(q)P \log P)^2 \log z} + qP^{4\eta} \frac{WU^2}{P^2(\log P) \log z} \\ &\ll \frac{qU^2W^2}{(\varphi(q)P \log P)^2 \log z} \left(1 + \frac{\varphi(q)^2 \log P}{W} P^{4\eta}\right). \end{aligned}$$

We select $\eta = 1/9$ and assume that $q \leq z^{1/8}$, so that

$$|\Sigma_P^0(P^*)|^2 \ll \frac{qU^2W^2}{(\varphi(q)P \log P)^2 \log z} \quad (q \leq z^{1/8}).$$

We sum over P^* , recall that $W = \sqrt{P}$. This leads to

$$\sum_{P^*} |\Sigma_P^0(P^*)| \ll \frac{\sqrt{q}U}{\varphi(q)(\log z)^{1/2} \log P}.$$

We add the error term $\mathcal{O}(NP^{1/2}/[P \log P])$ and then sum over P , add (28), (29) and (30) together with the error term coming from Theorem 1.3, and, on calling $S^\sharp(a/q)$ the trigonometric sum to be studied, we find that

$$\begin{aligned} S^\sharp(a/q) &\ll \frac{\sqrt{q}U \log \frac{\log N}{\log z}}{(\log z)^{1/2} \varphi(q)} + [\text{P to } P^*] \frac{\sqrt{N}}{\sqrt{z \log z}} \\ &\quad + [(\text{29}), (\text{30})] \frac{U}{\varphi(q)\sqrt{\log z}} + [(\text{28})] N^{1/4} \log 4q \\ &\quad + [\text{E' from Thm 1.3}] \frac{U}{z} + N \exp\left(-\frac{\log N}{4 \log z} \log \frac{\log N}{8 \log z}\right) \sqrt{\log z}. \end{aligned}$$

Some explanation may be required for the second summand of the first line. In order to sum $1/\log P$ over our dyadic intervals delimited by $P = z2^k$, where $k \in \{0, \dots, K\}$ with $K = [(\log \frac{\sqrt{N}}{z})/\log 2]$, we first notice that (with $T = [(\log z)/\log 2]$)

$$\begin{aligned} \sum_{0 \leq k \leq K} \frac{1}{\log z + k \log 2} &\leq \frac{1}{\log 2} \sum_{0 \leq k \leq K} \frac{1}{k+T} \\ &\ll \sum_{k \leq K+T} \frac{1}{k} - \sum_{k < T} \frac{1}{k} \ll \log \frac{\log N}{\log z} + \frac{1}{\log z} \\ &\ll \log \frac{\log N}{\log z}. \end{aligned}$$

Since $q \leq \sqrt{N}$, we easily simplify the above in

$$S^\sharp(\alpha) \ll \frac{U \sqrt{q} \log \frac{\log N}{\log z}}{\varphi(q)\sqrt{\log z}} + N^{1/2} + \frac{U}{z} + N \exp\left(-\frac{\log N}{4 \log z} \log \frac{\log N}{8 \log z}\right) \sqrt{\log z}.$$

We select $\log z = \frac{\log N}{(4A+5) \log \log N}$ and reach

$$\begin{aligned} S^\sharp(\alpha) &\ll \frac{U \sqrt{q} \log \log N \log \log \log N}{\varphi(q)\sqrt{\log N}} + N \exp(-(A+1)(\log \log N) \log \log \log N) \\ &\ll \frac{U \sqrt{q} \log \log N \log \log \log N}{\varphi(q)\sqrt{\log N}} + \frac{N}{(\log N)^{(A+1) \log \log \log N}}. \end{aligned}$$

This estimate would allow $q \ll (\log N)^C \log \log \log N$ for a positive constant C and similarly $U \geq N(\log N)^{-C \log \log \log N}$. We prefer to simplify the statement. The proof of this lemma is ended. \square

Let us convert the behaviour in small intervals in analytic variations

Lemma 11.3. *Let $A, B \geq 1$. Let $q \leq (\log N)^B$, $(a, q) = 1$ and $|\alpha - \frac{a}{q}| \leq (\log N)^B/N$. We have*

$$\frac{S(\alpha; N)}{N/\sqrt{\log N}} \ll_{A,B} \frac{\sqrt{q \log \log N} \log \log \log N}{\varphi(q)} + \frac{1}{(\log N)^A}.$$

The implied constant can be effectively computed.

Proof. Let us write $\alpha = \frac{a}{q} + \beta$. We write

$$S(\alpha; N) = \sum_{1 \leq k \leq \frac{N}{U}} (S(\alpha; N - (k-1)U) - S(\alpha; N - kU)) + \mathcal{O}\left(\frac{U}{\sqrt{\log U}}\right)$$

for a parameter U that we shall choose later. Given k and on setting $M = N - (k-1)U$, we have

$$\begin{aligned} S(\alpha; M) - S(\alpha; M - U) &= e(M\beta) \sum_{M-U < n \leq M} b(n)e(na/q) - 2\pi i \beta \int_{M-U}^M \sum_{M-U < n \leq t} b(n)e(na/q)e(t\beta) dt \\ &\ll (1 + |\beta|U) \left(\frac{U\sqrt{q}(\log \log M)^{1/2} \log \log \log M}{(\log M)^{1/2} \varphi(q)} \right) \end{aligned}$$

by Lemma 11.2. On summing over k , we get

$$S(\alpha; N) \ll (1 + |\beta|U) \left(\frac{\sqrt{q}N(\log \log N)^{1/2} \log \log \log N}{\varphi(q)\sqrt{\log N}} + \frac{N}{(\log N)^A} \right).$$

We select $U = N/(\log N)^B$ and conclude easily. \square

12. A GLOBAL BOUND FOR THE TRIGONOMETRIC POLYNOMIAL, PROOF OF THEOREM 1.5

Proof of Theorem 1.5. Let us start with the generic non effective part. Lemma 10.4 applies when q is larger than $(\log N)^{14+2A}$, while Lemma 8.1 is enough to take care of the case when $q \leq (\log N)^{14+2A}$.

Let us now examine how to modify the previous sketch to recover effectivity when $A < 1/2$. Lemma 10.4 applies when $q \geq (\log N)^{14+2A}$, Lemma 11.3 applies when $\log N \leq q \leq (\log N)^{14+2A}$ and Lemma 8.1 is enough to take care of the case $q \leq \log N$. \square

13. AN ADDITIVE APPLICATION, PROOF OF THEOREM 1.6

Lemma 13.1. *For any $\ell > 2$ and any subset \mathcal{B}' of the Gaussian integers, we have*

$$\int_0^1 \left| \sum_{\substack{b \leq N \\ b \in \mathcal{B}'}} e(b\alpha) \right|^\ell d\alpha \ll \frac{N^{\ell-1}}{(\log N)^{\ell/2}}.$$

Proof. This is a trivial consequence of the method developed in [19, Theorem 1.1] by B. Green and T. Tao, or in a simplified form in [48]. \square

Here is the main lemma of this section.

Lemma 13.2. *Let $N \equiv 3[4]$ be an integer, $K \in [2, \log \log N]$ be a parameter, and \mathcal{B}_1 and \mathcal{B}_2 be two sets of odd primitive Gaussian integers. We have*

$$\sum_{\substack{n+b_1+b_2=N \\ b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2}} b(n) = \frac{4CP_{4;3}(K)}{\varphi(P_{4;3}(K))} \sum_{\substack{b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2 \\ N-(b_1+b_2) \geq 3 \\ (N-(b_1+b_2), P_{4;3}(K))=1}} \frac{1}{\sqrt{\log(N-(b_1+b_2))}} + \mathcal{O}\left(\frac{N^2}{\sqrt{K}(\log N)^{3/2}}\right).$$

Proof. We consider the Dirichlet dissection of the torus \mathbb{R}/\mathbb{Z} :

$$\mathfrak{M}(a/q) = \{\alpha / |\alpha - a/q| \leq 1/(qQ)\}$$

for $Q = N/(\log N)^B$, where $B = 2A + 14$ for some $A > 0$. We call each interval $\mathfrak{M}(a/q)$ as a major arc and we denote their union as

$$(31) \quad \mathfrak{M} = \bigcup_{q_2 \in \{1, 2, 4\}} \bigcup_{\substack{q_* \leq N/Q q_2 \\ q_* | P_{4;3}(K)}} \bigcup_{a \bmod^{*} q_2 q_*} \mathfrak{M}\left(\frac{a}{q_2 q_*}\right).$$

We set

$$\mathfrak{m} = (\mathbb{R}/\mathbb{Z}) \setminus \mathfrak{M}.$$

We further define

$$(32) \quad S_1(\alpha) = \sum_{\substack{b_1 \leq N \\ b_1 \in \mathcal{B}_1}} e(b_1 \alpha), \quad S_2(\alpha) = \sum_{\substack{b_2 \leq N \\ b_2 \in \mathcal{B}_2}} e(b_2 \alpha),$$

while $S_K^b(\alpha; N)$ is defined in (25). We employ the circle method:

$$(33) \quad \begin{cases} r(N) = \int_0^1 S(\alpha) S_1(\alpha) S_2(\alpha) e(-N\alpha) d\alpha, \\ r^b(N) = \int_0^1 S_K^b(\alpha, N) S_1(\alpha) S_2(\alpha) e(-N\alpha) d\alpha, \end{cases}$$

and write

$$(34) \quad r(N) = r_0(N) + r'(N), \quad r'(N) = \int_{\mathfrak{m}} S(\alpha) S_1(\alpha) S_2(\alpha) e(-N\alpha) d\alpha$$

and, correspondingly,

$$(35) \quad r^b(N) = r_0^b(N) + r^{b'}(N), \quad r^{b'}(N) = \int_{\mathfrak{m}} S_K^b(\alpha, N) S_1(\alpha) S_2(\alpha) e(-N\alpha) d\alpha.$$

Let $\ell \in (2, 3)$. We notice that

$$(36) \quad \frac{1}{\ell} + \frac{1}{\ell} + \frac{\ell-2}{\ell} = 1, \quad \frac{\ell}{\ell-2} = \ell + \frac{3-\ell}{\ell-2} \ell$$

and use Hölder inequality to infer that

$$|r'(N)| \leq \left(\int_{\mathfrak{m}} |S_1(\alpha)|^\ell d\alpha \right)^{1/\ell} \left(\int_{\mathfrak{m}} |S_2(\alpha)|^\ell d\alpha \right)^{1/\ell} \left(\int_{\mathfrak{m}} |S(\alpha)|^\ell |S(\alpha)|^{\frac{\ell(3-\ell)}{\ell-2}} d\alpha \right)^{\frac{\ell-2}{\ell}}.$$

We extract $\max_{\alpha \in \mathfrak{m}} |S(\alpha)|^{\frac{\ell(3-\ell)}{\ell-2}}$ from the last term and then extend all three integrals to the full circle. When $\alpha \in \mathfrak{m}$, we have three cases: (i) $q \geq \log^B(N)$ (ii) $q \leq \log^B(N)$, $q_2 \nmid 4$ (iii) $q \leq \log^B(N)$, $q_2 \mid 4$, $q_* \nmid P_{4;3}(K)$. We majorize the maximum in case (i) via Theorem 1.5 and via Lemma 8.1 in the other cases where we further notice that $\log q \ll \log \log N$. In the case (iii), there exists at least one prime $p > K$ that divide q^* and thus $1/\varphi(q^*) \ll 1/K$. This argument implies that

$$\max_{\alpha \in \mathfrak{m}} |S(\alpha)| \ll \max\left(\frac{N}{(\log N)^A}, \frac{N \log \log N}{(\log N)^{3/2}}, \frac{1}{K \sqrt{\log N}}\right) \ll \frac{N}{K \sqrt{\log N}}.$$

Hence we get that

$$|r'(N)| \ll \left(\frac{N^{\ell-1}}{\log^{\ell/2}(N)} \right) \left(\frac{N}{K\sqrt{\log N}} \right)^{3-\ell} \ll \frac{N^2}{K^{3-\ell}(\log N)^{3/2}}.$$

We choose $\ell = 5/2$.

The same proof applies for $r^{\flat}(N)$, though the estimates for $S_K^{\flat}(\alpha)$ are different; furthermore Lemma 9.4 replaces Lemma 13.1. We obtain:

$$r^{\flat}(N) \ll \left(e^K \frac{N}{(\log N)^B} \right)^{3-\ell} \left(\frac{N^{\ell-1}}{(\log N)^{\ell/2}} \right)^{\frac{\ell-2}{\ell} + \frac{2}{\ell}} \left(\sqrt{\log K} \right)^{\frac{\ell-2}{\ell}}$$

as $q \leq N/(\log N)^B$. This gets reduced to

$$r^{\flat}(N) \ll \frac{N^2(\log N)^{3-\ell}\sqrt{\log \log N}}{(\log N)^{B(3-\ell)+\frac{\ell}{2}}} \ll \frac{N^2}{(\log N)^{B-1}}.$$

On the major arcs, $S(\alpha; N)$ and $S_K^{\flat}(\alpha; N)$ are similar by Lemma 8.1 and 9.3, hence the result. \square

Proof of Theorem 1.6. We start with Lemma 13.2 with the aim of replacing the $1/\sqrt{\log(N - b_1 - b_2)}$ by the simpler $1/\sqrt{\log N}$. Let $\varepsilon = 1/(\log N)^2$. We first notice that, with $m = b_1 + b_2$,

$$\frac{1}{\sqrt{\log(N - m)}} - \frac{1}{\sqrt{\log N}} = \frac{\log \frac{N}{N-m}}{\sqrt{\log(N - m)\log N}(\sqrt{\log N} + \sqrt{\log(N - m)})}.$$

Hence

$$\begin{aligned} \sum_{\substack{b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2 \\ N - (b_1 + b_2) \geq \varepsilon N \\ (N - (b_1 + b_2), P_{4,3}(K)) = 1}} \frac{1}{\sqrt{\log(N - b_1 - b_2)}} &= \sum_{\substack{b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2 \\ N - (b_1 + b_2) \geq \varepsilon N \\ (N - (b_1 + b_2), P_{4,3}(K)) = 1}} \frac{1}{\sqrt{\log N}} \\ &\quad + \mathcal{O}\left(\frac{|\mathcal{B}_1 \cap [1, N]| |\mathcal{B}_2 \cap [1, N]| \log(1/\varepsilon)}{\sqrt{\log(\varepsilon N)} \log N}\right). \end{aligned}$$

This remainder term is readily seen to be $\ll N^2(\log \log N)/(\log N)^{5/2}$. Next, there for each integer m in $[(1 - \varepsilon)N, N]$, the sieve tells us that number of decomposition $m = b_1 + b_2$ is at most $N(\log \log N)/\log N$. This gives us finally that

$$\begin{aligned} \sum_{\substack{b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2 \\ N - (b_1 + b_2) \geq 3 \\ (N - (b_1 + b_2), P_{4,3}(K)) = 1}} \frac{1}{\sqrt{\log(N - (b_1 + b_2))}} &= \sum_{\substack{b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2 \\ N - (b_1 + b_2) \geq 3 \\ (N - (b_1 + b_2), P_{4,3}(K)) = 1}} \frac{1}{\sqrt{\log N}} \\ &\quad + \mathcal{O}\left(\frac{N^2 \log \log N}{(\log N)^{5/2}}\right). \end{aligned}$$

Theorem 1.6 follows readily for this estimate. \square

14. A CHALLENGE. PROOF OF THEOREM 1.7

The following is useful for the proof of Theorem 1.7.

Lemma 14.1. *For any integer k , we define $N_k = \frac{(1+\sqrt{2})^k - (1-\sqrt{2})^k}{2\sqrt{2}}$. Then the quantity N_k is an integer, N_k and N_{k+1} are coprime, and we have $|\sqrt{2} - \frac{N_{k+1}-N_k}{N_k}| \leq \frac{1}{2N_k^2}$. When y is large enough, each interval $[y, 3y]$ contains a N_k .*

Proof. We readily check that $N_1 = 1$, $N_2 = 2$ and that $N_{k+2} - 2N_{k+1} - N_k = 0$, from which the reader will easily deduce that the N_k 's are integers and that N_k and N_{k+1} are coprime. Let us set $\alpha = 1 + \sqrt{2}$ so that $1/\alpha = -(1 - \sqrt{2})$ and $\alpha^2 = 2\alpha + 1$. We compute that

$$8N_k^2 \left(\sqrt{2} - \frac{N_{k+1} - N_k}{N_k} \right) = 8\alpha N_k^2 - 8N_k N_{k+1} = 2(\alpha - 1)(\alpha^{-2k} - (-1)^k)$$

and this last quantity is swiftly shown to be, in absolute value, at most 4. The last assertion comes from the fact that $1 + \sqrt{2} < 3$. \square

Proof of Theorem 1.7. This proof is a direct consequence of two points: Lemma 10.4 and the fact that $\sqrt{2}$ has convergent denominators in each interval $[y, 3y]$, as shown in Lemma 14.1. \square

15. BOUNDS ON MULTIPLES. PROOF OF THEOREM 1.8

Proof of Theorem 1.8. Let us assume that N is not the square of an integer. We start with Theorem 1.4 which we use with $Z = \sqrt{N}$, $u_n = e(r\alpha b)$, $M = M_0$ and the parameters M_0 and z to be chosen.

Bilinear part – Vinogradov part. We are to study

$$\Delta_1 = \sum_{\substack{z \leq p \leq \sqrt{N} \\ p \equiv 3[4]}} \sum_{R/2 < r \leq R} \left| \sum_{N/2 < pm \leq N} \rho(m) e(pmra) \right|.$$

Let us localize the variable p in $(P', P]$, so the variable m is localized in $(N/(2P), N/P']$. We use Lemma 10.3 to infer that this is bounded above in absolute value, and up to a multiplicative constant, by

$$\frac{NR}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{\sqrt{P}}{\sqrt{N}} + \frac{1}{\sqrt{RP}} \right) (\log N)^4.$$

On summing diadically over P' , we infer that

$$(37) \quad \Delta_1 \ll \frac{NR}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{1}{N^{1/4}} + \frac{1}{\sqrt{Rz}} \right) (\log N)^5.$$

Linear part. We are to study

$$\Delta_0 = \sum_{R/2 < r \leq R} c_r \sum_{\substack{d \leq M_0 \\ d | P_{4;3}(z)}} \mu(d) \sum_{\substack{n \leq N \\ n \equiv 0[d]}} e(nra).$$

Let us glue r and d in a single variable u and use Lemma 10.1 with $U = RM_0$ and $UV = N$, getting, for any positive ε ,

$$(38) \quad \Delta_0 \ll_\varepsilon \left(\frac{N}{q} + RM_0 + q \right) N^\varepsilon.$$

Bilinear part – Simple sieve part. We are finally to study, for any $t \in [0, 1]$ the quantity

$$\Delta_3 = \sum_{R/2 < r \leq R} \left| \sum_{M_0 \leq \ell \leq M_0 z} \alpha_\ell(t) \sum_{N/2 < k\ell \leq N} \beta_k(t) e(k\ell ra) \right|.$$

Let us localize the variable ℓ in an interval $(L', L]$, so that k is localized on $(N/(2L), N/L']$. We may thus employ Lemma 10.3 and reach the bound, for each of any such piece and up to a multiplicative constant,

$$\frac{RN}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{1}{\sqrt{N/L}} + \frac{1}{\sqrt{RL}} \right) (\log N)^5.$$

We sum diadically on L to reach

$$(39) \quad \Delta_3 \ll \frac{RN}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{\sqrt{M_0 z}}{\sqrt{N}} + \frac{1}{\sqrt{RM_0}} \right) (\log N)^6.$$

Gathering the estimates. It is best to choose M_0 as small as possible though larger than z , so we select $M_0 = z$, getting the upper bound

$$\frac{NR}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{1}{N^{1/4}} + \frac{1}{\sqrt{Rz}} + \frac{z}{\sqrt{N}} + \frac{1}{Rq} + \frac{z}{N} + \frac{q}{RN} + \frac{1}{z} \right) N^\varepsilon.$$

We readily simplify that into

$$\frac{NR}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{1}{N^{1/4}} + \frac{1}{\sqrt{Rz}} + \frac{z}{\sqrt{N}} + \frac{1}{z} \right) N^\varepsilon.$$

We assume that $R \leq N$ and select $z = (N/R)^{1/3}$.

$$\frac{NR}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{1}{N^{1/4}} + \frac{1}{R^{1/3}N^{1/6}} + \frac{R^{1/3}}{N^{1/3}} \right) N^\varepsilon.$$

We readily check that $R^{-1/3}N^{-1/6} + R^{1/3}N^{-1/3} \geq N^{-1/4}$, so we may discard this summand. This concludes the proof of our lemma. \square

16. DIOPHANTINE APPROXIMATION AND PROOF OF THEOREM 1.9

We recall a classical lemma of trigonometric approximation in the precise form given in [27, Lemma 1] by G. Harman which is based on [40], see also [56, Theorem 19] by J. Vaaler.

Lemma 16.1. *Let (a_n) be a sequence of non-negative reals for $N/2 < n \leq N$. Then for $\delta > 0$, α and β be arbitrary real numbers and $R \geq 1$ be some given parameter, We have*

$$\sum_{\|n\alpha - \beta\| \leq \delta} a_n = 2\delta \sum_n a_n + \mathcal{O}\left(\delta \sum_{r \leq R} \left| \sum_n a_n e(rn\alpha) \right| \right) + \mathcal{O}\left(\frac{1}{R} \sum_n a_n \right).$$

Proof of Theorem 1.9. We employ Lemma 16.1 together with Theorem 1.8. With an obvious notation, this leads to

$$\begin{aligned} \sum_{\|n\alpha - \beta\| \leq \delta} b(n) &= (2\delta + \mathcal{O}(1/R))B(N) + \delta \sum_{r \leq R} |S(r\alpha; N)| \\ &= (2\delta + \mathcal{O}(1/R))B(N) \\ &\quad + \mathcal{O}_\varepsilon \left(\frac{\delta RN}{\sqrt{\log N}} \left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{\sqrt{RN}} + \frac{1}{R^{1/3}N^{1/6}} + \frac{R^{1/3}}{N^{1/3}} \right) N^\varepsilon \right). \end{aligned}$$

Since α is quadratic irrational, there exists a constant C such that we may find approximations a/q of α with $q \in [\sqrt{RN}, C\sqrt{RN}]$ and $|q\alpha - a| \leq 1/q$ for any N , see Lemma 14.1 for the case $\alpha = \sqrt{2}$. With such a choice, we get

$$\left| \sum_{\|n\alpha - \beta\| \leq \delta} \frac{b(n)}{B(N)} - 2\delta \right| \ll_\varepsilon \frac{1}{R} + \delta \left(\frac{\sqrt{R}}{\sqrt{N}} + \frac{R^{3/4}}{N^{1/4}} + \frac{R^{2/3}}{N^{1/6}} + \frac{R^{4/3}}{N^{1/3}} \right) N^\varepsilon.$$

We select $R = N^{1/4-2\theta}$ and $\delta^{-1} = N^{1/4-\theta}$ for $\theta > 0$ and small enough. This proves our theorem. \square

17. APPENDIX: SOME ESTIMATES WITH PRIMES CONGRUENT TO 3 MODULO 4

We shall freely use the Mertens Theorems for primes congruent to 3 modulo 4, namely

$$(40) \quad \sum_{\substack{n \leq N \\ n \equiv 3[4]}} \frac{\Lambda(n)}{n} = \frac{1}{2} \log N + \mathcal{O}(1) \quad \text{and} \quad \prod_{\substack{p \leq z \\ p \equiv 3[4]}} \left(1 - \frac{1}{p}\right) \asymp 1/\sqrt{\log z}.$$

An explicit version of the first estimate may be found in [45, Corollaire 1], but we waive this aspect most of the times. However, in the case of Theorem 1.3, it is better to rely on the next explicit estimate that is rather straightforward to get.

Lemma 17.1. *When $z \geq 1$, we have $\sum_{\substack{p < z \\ p \equiv 3[4]}} \frac{\log p}{p+1} \leq \frac{1}{2} \log z - \frac{1}{4} \log 3$.*

Proof. The inequality has been checked by GP/Pari up to 10^8 with a minimal value reached for $z = 3$. Let us proceed for the proof. We first check that

$$\sum_{\substack{p < z \\ p \equiv 3[4]}} \frac{\log p}{p+1} \leq \sum_{\substack{n < z \\ n \equiv 3[4]}} \frac{\Lambda(n)}{n}.$$

We treat this last sum with Dirichlet characters and write

$$2 \sum_{\substack{n < z \\ n \equiv 3[4]}} \frac{\Lambda(n)}{n} = \sum_{\substack{n < z \\ n \equiv 1[2]}} \frac{\Lambda(n)}{n} - \sum_{\substack{n < z \\ n \equiv 3[4]}} \frac{\Lambda(n)\chi_4(n)}{n}$$

where χ_4 is the only non-principal character modulo 4. By using the Prime Number Theorem in Arithmetic Progression, we conclude that

$$2 \sum_{\substack{n < z \\ n \equiv 3[4]}} \frac{\Lambda(n)}{n} = \log z - \log 2 - \gamma + \frac{L'(1, \chi_4)}{L(1, \chi_4)} + o(1),$$

see also [45, Corollaire 1]. We have $L(1, \chi_4) = \pi/4$ (see for instance [2, Théorème 3, Part 2, Chapter V] by Z. I. Borevitch and I. R. Chafarevitch) and $L'(1, \chi_4)$ may be computed approximately with the series expansion:

$$\begin{aligned} -L'(1, \chi_4) &= \sum_{k \geq 0} \left(\frac{\log(4k+1)}{4k+1} - \frac{\log(4k+3)}{4k+3} \right) \\ &= \sum_{k \geq 0} \frac{2\log(4k+1) - (4k+1)\log(1 + \frac{2}{4k+1})}{(4k+1)(4k+3)} \\ &= -\frac{\log 3}{3} + \sum_{k \geq 1} \frac{2\log(4k+1) - (4k+1)\log(1 + \frac{2}{4k+1})}{(4k+1)(4k+3)}. \end{aligned}$$

The good part of the last series is that it is a sum of non-negative terms and can thus be computed with acceleration of convergence process. We get in this manner

$$(41) \quad L'(1, \chi_4) = 0.192901 \dots, \quad \frac{1}{2} \left(\frac{L'(1, \chi_4)}{L(1, \chi_4)} - \gamma - \log 2 \right) = -0.512376 \dots$$

By [45, Corollaire 4], we have, when $z \geq 182$

$$(42) \quad \sum_{\substack{n < z \\ n \equiv 3[4]}} \frac{\Lambda(n)}{n} = \frac{1}{2} \log z + \frac{1}{2} \left(\frac{L'(1, \chi_4)}{L(1, \chi_4)} - \gamma - \log 2 \right) + \mathcal{O}^*(2/9).$$

On collecting our estimates, the lemma follows readily. \square

REFERENCES

- [1] C. Bauer. “An L -function free proof of Hua’s theorem on sums of five prime squares”. In: *Studia Sci. Math. Hungar.* 57.1 (2020), pp. 1–39 (cit. on p. 5).
- [2] Z. I. Borevitch and I. R. Chafarevitch. *Théorie des nombres*. Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Translated from the Russian by Myriam Verley and Jean-Luc Verley, Reprint of the 1967 French translation. Éditions Jacques Gabay, Sceaux, 1993, pp. iv+246. ISBN: 2-87647-149-3 (cit. on p. 34).
- [3] J. Bourgain, P. Sarnak, and T. Ziegler. “Disjointness of Moebius from horocycle flows”. In: *From Fourier analysis and number theory to Radon transforms and geometry*. Vol. 28. Dev. Math. Springer, New York, 2013, pp. 67–83. DOI: [10.1007/978-1-4614-4075-8\5](https://doi.org/10.1007/978-1-4614-4075-8_5) (cit. on p. 2).
- [4] V. Brun. “La série $\frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{29} + \frac{1}{31} + \frac{1}{41} + \frac{1}{43} + \frac{1}{59} + \frac{1}{61} + \dots$ où les dénominateurs sont ”nombres premiers jumeaux” est convergente ou finie.” In: *Darboux Bull.* 43.2 (1919), pp. 100–104, 124–128 (cit. on p. 2).
- [5] M. Caggerata, A. Perelli, and A. Zaccagnini. “An extension of the Bourgain-Sarnak-Ziegler Theorem with modular applications”. In: *Quart. J. Math. Oxford* (2020), pp. 359–377. DOI: [10.1093/qmathj/haz048](https://doi.org/10.1093/qmathj/haz048) (cit. on p. 2).
- [6] Z. Cui and J. Wu. “The Selberg-Delange method in short intervals with an application”. In: *Acta Arith.* 163.3 (2014), pp. 247–260 (cit. on pp. 14, 15).
- [7] H. Daboussi. “Effective estimates of exponential sums over primes”. In: *Analytic number theory. Vol. 1. Proceedings of a conference in honor of Heini Halberstam, May 16–20, 1995, Urbana, IL, USA. Boston, MA: Birkhaeuser. Prog. Math.* 138 (1996), pp. 231–244 (cit. on p. 6).
- [8] H. Daboussi and J. Rivat. “Explicit upper bounds for exponential sums over primes”. In: *Math. Comp.* 70.233 (2001), pp. 431–447 (cit. on p. 9).
- [9] H. Diamond, H. Halberstam, and H.-E. Richert. “Combinatorial sieves of dimension exceeding one”. In: *J. Number Theory* 28.3 (1988), pp. 306–346 (cit. on p. 10).
- [10] L. Dickson. *Theory of numbers*. Chelsea Publishing Company, 1971 (cit. on p. 5).
- [11] P. D. T. A. Elliott. *Probabilistic number theory. I*. Vol. 239. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science]. Mean-value theorems. Springer-Verlag, New York-Berlin, 1979, xxii+359+xxxiii pp. (2 plates). ISBN: 0-387-90437-9 (cit. on p. 9).
- [12] K. Ford and H. Halberstam. “The Brun-Hooley sieve”. In: *J. Number Theory* 81.2 (2000), pp. 335–350 (cit. on pp. 10, 11).
- [13] E. Fouvry, C. Levesque, and M. Waldschmidt. “Representation of integers by cyclotomic binary forms”. In: *Acta Arith.* 184.1 (2018), pp. 67–86 (cit. on p. 3).
- [14] J. Friedlander and H. Iwaniec. *Opera de cribro*. Vol. 57. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 2010, pp. xx+527. ISBN: 978-0-8218-4970-5 (cit. on pp. 2, 5, 15).
- [15] P. Gallagher. “Bombieri’s mean value theorem”. In: *Mathematika* 15 (1968), pp. 1–6 (cit. on p. 2).
- [16] G. Greaves. “On the representation of a number in the form $x^2 + y^2 + p^2 + q^2$ where p, q are odd primes”. In: *Acta Arith.* 29 (1976), pp. 251–256. DOI: [10.4064/aa-29-3-251-256](https://doi.org/10.4064/aa-29-3-251-256) (cit. on p. 5).
- [17] G. Greaves. *Sieves in number theory*. Vol. 43. Ergebnisse der Mathematik und ihrer Grenzgebiete. xii+304 pp. Springer-Verlag, Berlin, 2001 (cit. on p. 25).

- [18] B. Green and T. Tao. “Linear equations in primes”. In: *Ann. of Math.* (2) 171.3 (2010), pp. 1753–1850. DOI: [10.4007/annals.2010.171.1753](https://doi.org/10.4007/annals.2010.171.1753) (cit. on p. 5).
- [19] B. Green and T. Tao. “Restriction theory of the Selberg sieve, with applications”. In: *J. Théor. Nombres Bordx* 18.1 (2006). Available at <http://fr.arxiv.org/pdf/math.NT/0405581>, pp. 147–182 (cit. on pp. 5, 6, 29).
- [20] B. Green and T. Tao. “The primes contain arbitrarily long arithmetic progressions”. In: *Ann. of Math.* (2008) (cit. on p. 5).
- [21] B. Green. “Roth’s theorem in the primes”. In: *Ann. of Math.* (2) 161.3 (2005), pp. 1609–1636 (cit. on p. 5).
- [22] B. Green and T. Tao. “An inverse theorem for the Gowers $U^3(G)$ norm”. In: *Proc. Edinb. Math. Soc.* (2) 51.1 (2008), pp. 73–153 (cit. on p. 2).
- [23] B. Green. “Roth’s theorem in the primes”. In: *Ann. of Math.* 3.161 (2005), pp. 1609–1636 (cit. on p. 6).
- [24] H. Halberstam and H.-E. Richert. *Sieve methods*. London Mathematical Society Monographs, No. 4. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974, xiv+364 pp. (loose errata) (cit. on pp. 10, 11).
- [25] G. H. Hardy and S. Ramanujan. “Une formule asymptotique pour le nombre des partitions de n .” In: *C. R. Acad. Sci., Paris* () (cit. on p. 1).
- [26] G. Hardy and J. Littlewood. “Some problems of “Partitio Numerorum” III. On the expression of a number as a sum of primes”. In: *Acta Math.* 44 (1923), pp. 1–70 (cit. on p. 1).
- [27] G. Harman. “On the distribution of αp modulo one”. In: *J. London Math. Soc.* (2) 27.1 (1983), pp. 9–18. DOI: [10.1112/jlms/s2-27.1.9](https://doi.org/10.1112/jlms/s2-27.1.9) (cit. on pp. 7, 13, 23, 33).
- [28] G. Harman. “On the distribution of αp modulo one. II”. In: *Proc. London Math. Soc.* (3) 72.2 (1996), pp. 241–260. DOI: [10.1112/plms/s3-72.2.241](https://doi.org/10.1112/plms/s3-72.2.241) (cit. on pp. 7, 13).
- [29] G. Harman. *Prime-Detecting Sieves*. Vol. 33. London Mathematical Society Monographs Series. Princeton University Press, Princeton, NJ, 2007, pp. xvi+362. ISBN: 978-0-691-12437-7 (cit. on pp. 7, 12).
- [30] D. R. Heath-Brown and C. Jia. “The distribution of αp modulo one”. In: *Proc. London Math. Soc.* (3) 84.1 (2002), pp. 79–104 (cit. on p. 7).
- [31] K. Indlekofer. “Scharfe Abschätzung für die Anzahlfunction der B -Zwillinge”. In: *Acta Arith.* 26 (1974/75), pp. 207–212 (cit. on p. 5).
- [32] H. Iwaniec. “The half dimensional sieve”. In: *Acta Arith.* 29 (1976), pp. 69–95 (cit. on pp. 5, 15).
- [33] H. Iwaniec and E. Kowalski. *Analytic number theory*. American Mathematical Society Colloquium Publications. xii+615 pp. American Mathematical Society, Providence, RI, 2004 (cit. on p. 3).
- [34] C. H. Jia. “On the distribution of αp modulo one”. In: *J. Number Theory* 45.3 (1993), pp. 241–253 (cit. on p. 7).
- [35] C. Jia. “On the distribution of αp modulo one. II”. In: *Sci. China Ser. A* 43.7 (2000), pp. 703–721 (cit. on p. 7).
- [36] E. Landau. “Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate.” German. In: *Arch. der Math. u. Phys.* (3) 13 (1908), pp. 305–312 (cit. on p. 5).
- [37] J. van Lint and H. Richert. “On primes in arithmetic progressions”. In: *Acta Arith.* 11 (1965), pp. 209–216 (cit. on p. 27).

- [38] K. Matomäki. “The distribution of αp modulo one”. In: *Math. Proc. Cambridge Philos. Soc.* 147.2 (2009), pp. 267–283 (cit. on p. 7).
- [39] K. Matomäki and X. Shao. “Vinogradov’s three primes theorem with almost twin primes”. In: *Compos. Math.* 153.6 (2017), pp. 1220–1256 (cit. on p. 5).
- [40] H. Montgomery. “The analytic principle of the large sieve”. In: *Bull. Amer. Math. Soc.* 84.4 (1978), pp. 547–567 (cit. on p. 33).
- [41] K. Prachar. “Über Zahlen der Form $a^2 + b^2$ in einer arithmetischen Progression”. In: *Math. Nachr.* 10 (1953), pp. 51–54 (cit. on p. 15).
- [42] O. Ramaré. “A note on additive properties of dense subsets of sifted sequences”. In: *Bull. Lond. Math. Soc.* 45.4 (2013), pp. 677–682 (cit. on p. 5).
- [43] O. Ramaré. “On Bombieri’s asymptotic sieve”. In: *J. Number Theory* 130.5 (2010), pp. 1155–1189 (cit. on pp. 2, 6).
- [44] O. Ramaré. “Prime numbers: emergence and victories of bilinear forms decomposition”. In: *Newsletter of the EMS* 90 (2013), pp. 18–27 (cit. on p. 2).
- [45] O. Ramaré. “Sur un théorème de Mertens”. In: *Manuscripta Math.* 108 (2002), pp. 483–494 (cit. on p. 34).
- [46] O. Ramaré and I. Ruzsa. “Additive properties of dense subsets of sifted sequences”. In: *J. Théorie N. Bordeaux* 13 (2001), pp. 559–581 (cit. on pp. 5, 6).
- [47] O. Ramaré. *Excursions in Multiplicative Number Theory*. Birkhäuser Advanced Texts: Basler Lehrbücher. [Birkhäuser Advanced Texts: Basel Textbooks]. With the collaboration of P. Moree and A. Sedunova. Birkhäuser/Springer, Cham (cit. on p. 8).
- [48] O. Ramaré. “Notes on restriction theory in the primes”. In: *Israel J. Math.* 261.2 (2024), pp. 717–738 (cit. on p. 29).
- [49] O. Ramaré and G. K. Viswanadham. “Modular ternary additive problems with irregular or prime numbers”. In: *Tr. Mat. Inst. Steklova* 314. Analiticheskaya i Kombinatornaya Teoriya Chisel (2021). English version published in *Proc. Steklov Inst. Math.* 314 (2021), no. 1, 203–237, pp. 211–247 (cit. on p. 6).
- [50] G. J. Rieger. “Über die Anzahl der als Summe von zwei Quadrate darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke. II”. In: *J. Reine Angew. Math.* 217 (1965), pp. 200–216 (cit. on pp. 15–17).
- [51] J.-P. Serre. “Divisibilité de certaines fonctions arithmétiques”. In: *Enseign. Math. (2)* 22.3-4 (1976), pp. 227–260 (cit. on pp. 15, 17).
- [52] X. Shao. “A density version of the Vinogradov three primes theorem”. In: *Duke Math. J.* 163.3 (2014), pp. 489–512 (cit. on p. 5).
- [53] X. Shao. “An L -function-free proof of Vinogradov’s three primes theorem”. In: *Forum Math. Sigma* 2 (2014), Paper No. e27, 26. DOI: [10.1017/fms.2014.27](https://doi.org/10.1017/fms.2014.27) (cit. on pp. 5, 6).
- [54] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*. Second. Vol. 1. Cours Spécialisés. Paris: Société Mathématique de France, 1995, pp. xv+457. ISBN: 2-85629-032-9 (cit. on p. 15).
- [55] J. Teräväinen. “The Goldbach problem for primes that are sums of two squares plus one”. In: *Mathematika* 64.1 (2018), pp. 20–70 (cit. on p. 5).
- [56] J. Vaaler. “Some Extremal Functions in Fourier Analysis”. In: *Bull. A. M. S.* 12 (1985), pp. 183–216 (cit. on p. 33).
- [57] R. C. Vaughan. “On the distribution of αp modulo 1”. In: *Mathematika* 24.2 (1977), pp. 135–141 (cit. on pp. 7, 23, 24).
- [58] R. Vaughan. “An elementary method in prime number theory”. In: *Acta Arith.* 37 (1980), pp. 111–115 (cit. on p. 12).

- [59] R. Vaughan. “Mean value theorems in prime number theory”. In: *J. London Math Soc.* (2) 10 (1975), pp. 153–162 (cit. on p. 2).
- [60] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers*. Russian. Tr. Mat. Inst. Steklova 23, 3-109 (1947). 1947 (cit. on p. 2).
- [61] I. Vinogradov. “Representation of an odd number as a sum of three primes”. In: *Dokl. Akad. Nauk SSSR* 15 (1937), pp. 291–294 (cit. on p. 2).
- [62] I. Vinogradov. *The method of trigonometrical sums in the theory of numbers*. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation. Mineola, NY: Dover Publications Inc., 2004, pp. x+180. ISBN: 0-486-43878-3 (cit. on pp. 7, 26).
- [63] I. M. Vinogradow. “New estimations of trigonometrical sums containing primes.” In: *C. R. (Dokl.) Acad. Sci. URSS, n. Ser.* () (cit. on p. 2).

(O. Ramaré) CNRS/ INSTITUT DE MATHÉMATIQUES DE MARSEILLE, AIX MARSEILLE UNIVERSITÉ, U.M.R. 7373, SITE SUD, CAMPUS DE LUMINY, CASE 907, 13288 MARSEILLE CEDEX 9, FRANCE.

Email address: olivier.ramare@univ-amu.fr

(G. K. Viswanadham) IISER BERHAMPUR, BERHAMPUR, ODISHA, 760 010, INDIA.

Email address: viswanadh@iiserbpr.ac.in