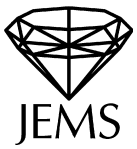
J. Eur. Math. Soc. 11, 627–703



Enrico Bombieri · Jean Bourgain

On Kahane's ultraflat polynomials

Received September 3, 2008

Abstract. This paper is devoted to the construction of polynomials of almost constant modulus on the unit circle, with coefficients of constant absolute value. In particular, one obtains a much improved estimate for the error term. A major part of this paper deals also with the long-standing problem of the effective construction of ultraflat polynomials.

Keywords. Trigonometric polynomials, probabilistic methods, exponential sums

1. Introduction

In 1957 Erdős put forward several problems on polynomials which have since then attracted much attention. One of them asked what is the smallest maximum modulus of an exponential polynomial $P(\theta) = \sum a_m e^{2\pi i m\theta}$ of degree n with coefficients $|a_m| = 1$ of modulus 1. Such polynomials are called *unimodular*. Erdős thought that the maximum of an exponential unimodular polynomial of degree n was at least $(1+c)\sqrt{n}$ for some fixed positive constant c.

In 1966 Littlewood [17] constructed exponential unimodular polynomials with

$$|P(\theta)| = (1 + o(1))\sqrt{n} \tag{1.1}$$

on the unit circle, except in a rather small neighbourhood of $\theta = 0$ where a bound $O(\sqrt{n})$ would hold. In view of this result, he was led to conjecture that there were exponential unimodular polynomials of degree n with maximum modulus $(1 + o(1))\sqrt{n}$ on the unit circle, which would disprove Erdős's conjecture.

Further results in this circle of ideas were obtained by Newman [18], Beller and Newman [2], and Byrnes [6].[1] The next important progress was done by Körner [16] who introduced ideas from probability theory to show how to achieve unimodularity starting from polynomials with coefficients only bounded by 1.

E. Bombieri, J. Bourgain: School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA; e-mail: eb@ias.edu, bourgain@ias.edu

Mathematics Subject Classification (2000): Primary 42A05; Secondary 42A61

[1] Note that Theorem 2 of [6] is incorrect (as pointed out to the authors by Bahman Saffari, see [19]) and the use of Byrnes's claim invalidates the proofs of Theorems 6 and 7 of [16]. However, the important Lemma 2 of [16], which is a basic tool for achieving unimodularity, does not depend on [6] and remains valid.

Finally, the solution of Erdős's problem was provided by Kahane [14] with the construction of the so-called "ultraflat" polynomials, namely exponential unimodular polynomials $P(\theta)$ of degree n such that (1.1) held uniformly in θ. The $o(1)$ term was made precise in the same paper [14] as $O(n^{-1/17}\sqrt{\log n})$. Other important results on exponential unimodular polynomials, in particular the behaviour of derivatives, the consideration of other norms, and a thorough discussion of the literature, can be found in Queffélec and Saffari [19].

In this paper we prove the following four results. We write $e(\theta) = e^{2\pi i\theta}$, $\| \ \|_\infty$ for the maximum norm on the the unit circle, and $\|\widehat{P}\|_{\ell^1}$ for the ℓ^1-norm of the vector $\widehat{P}$ of Fourier coefficients of the polynomial P.

Definition 1.

$$\mu(n) = \sup \frac{\|\widehat{P}\|_{\ell^1}}{\|P\|_\infty}$$

where the supremum is over all non-zero exponential polynomials of degree n.

It is known (H. Shapiro, S. Neuwirth and E. Ricard) that

$$\mu(n) \le \sqrt{n}. \tag{1.2}$$

A short proof, communicated to us by H. Queffélec, goes as follows. We write $P(\theta) = \sum \widehat{P}(m)(m\theta)$. Then

$$\frac{1}{n}\sum_{m=0}^{n} |P(\theta + m/n)|^2 = |\widehat{P}(0) + \widehat{P}(n)e(n\theta)|^2 + \sum_{m=1}^{n-1} |\widehat{P}(m)|^2.$$

Optimizing with respect to θ we get

$$(|\widehat{P}(0)| + |\widehat{P}(n)|)^2 + \sum_{m=1}^{n-1} |\widehat{P}(m)|^2 \le \|P\|_\infty^2.$$

Also,

$$\|P\|_{\ell^1}^2 \le n\Big((|\widehat{P}(0)| + |\widehat{P}(n)|)^2 + \sum_{m=1}^{n} |\widehat{P}(m)|^2\Big)$$

by the Cauchy–Schwarz inequality, and (1.2) follows.

Theorem 2. *Let $\varepsilon > 0$. Then*

$$\mu(n) \ge \sqrt{n} - O((\log n)^{3/2+\varepsilon}).$$

More precisely, let

$$\alpha := n^{-1/2}(\log n)^{3/2+\varepsilon}$$

and $A \ge 0$. Then there is a polynomial in $e(\theta)$ given by

$$P(\theta) = \sum \widehat{P}(m)e(m\theta)$$

with $\operatorname{supp}(\widehat{P}) = [0, n]$, *with* $|\widehat{P}(m)| = 1$ *for* $2\alpha n < m < (1 - 2\alpha)n$, *and* $|\widehat{P}(m)| \leq 1$ *otherwise, such that*

$$|P(\theta)| = \sqrt{n} + O(n^{-A}) \qquad \text{if } |\theta| \leq 1/2 - 2\alpha,$$
$$|P(\theta)| \leq \sqrt{n} + O(n^{-A}) \qquad \text{if } 1/2 - 2\alpha < |\theta| \leq 1/2.$$

Theorem 3. *Let* $\varepsilon > 0$ *and* $\alpha = n^{-1/2}(\log n)^{3/2+\varepsilon}$. *Then there is*

$$P(\theta) = \sum \widehat{P}(m) e(m\theta)$$

with $\operatorname{supp}(\widehat{P}) = [0, n]$ *and* $|\widehat{P}(m)| = 1$ *there, such that*

$$|P(\theta)| = \sqrt{n} + O(n^{1/4}(\log n)^{3/4+\varepsilon}) \qquad \text{if } |\theta| \leq 1/2 - 2\alpha,$$
$$|P(\theta)| \leq \sqrt{n} + O(n^{1/4}(\log n)^{3/4+\varepsilon}) \qquad \text{if } 1/2 - 2\alpha < |\theta| \leq 1/2.$$

Theorem 4. *Let* $\varepsilon > 0$. *For every* $n \geq 1$ *there is*

$$P(\theta) = \sum \widehat{P}(m) e(m\theta)$$

with $\operatorname{supp}(\widehat{P}) \subset [0, n]$ *and* $|\widehat{P}(m)| = 1$ *there, such that*

$$|P(\theta)| = \sqrt{n} + O(n^{1/2-1/9+\varepsilon})$$

for every θ.

Remark 5. The proof can be refined so as to replace n^{ε} by a power of $\log n$.

These theorems improve the corresponding results of Kahane in [14] and represent the limit of our methods.

Remark 6. As such, the proofs of Theorems 3 and 4 are not constructive because they use a randomizing construction (twice for Theorem 4). An effective construction of a polynomial such as in Theorem 3 with the slightly worse error term $O(n^{1/4}(\log n)^{9/4+\varepsilon})$ is possible, as will be indicated in Section 13.

The last part of the paper from Section 14 onwards is dedicated to an effective construction of a polynomial satisfying Theorem 4, a problem which has been around for some time. We state

Theorem 7. *Let* $\varepsilon > 0$. *For every* $n \geq 1$ *there is an effectively constructible polynomial satisfying the hypotheses and conclusion of Theorem* 4.

Remark 8. The proof can be refined so as to replace n^{ε} by $\exp(c \log n / \log\log n)$ for some $c > 0$.

Here by effective we mean that all coefficients are given explicitly in terms of elementary functions and sequences of signs ± 1 determined in terms of Legendre or Jacobi symbols associated to moduli which are primes or squarefree numbers in prescribed intervals.

The content of this paper is as follows.

Sections 2 and 3 prove Theorem 2 and 3, using a Gaussian phase for the coefficients and a smoothing of the amplitudes at the beginning and end of the polynomials, together with precise asymptotic expansions. Here we follow the methods of [4].

Section 4 constructs a smooth partition of unity on the unit circle and deforms it slightly to obtain polynomials, supported in $[-M, N+M]$, close to 1 in absolute value everywhere on the unit circle.

Section 5 chooses phase steps and coefficients. Section 6 decomposes the polynomial P_0 in five pieces $P_1, \dots, P_5$ which have to be treated separately. Section 7 studies the coefficients of P_1 using Poisson summation. Section 8 introduces the basic Körner correction. Section 9 obtains by randomization a good bound for the coefficients of P_2. The short Sections 10 and 11 bound the coefficients of the remaining components of P_0. Section 12 contains elementary estimates of Weyl sums and the proof of Theorem 3 using the Körner correction.

Derandomization starts in Section 13 with the proof of the statement in Remark 6, which is easy.

Section 14 contains some remarks about the problem and chooses a key parameter δ.

Section 15 gives a derandomized version of the polynomials P_2 and P_4 appearing in the decomposition of P_0 done in Section 6. This is achieved by introducing an explicit sequence of signs determined by the expansion of a number in base p, where p is a prime number dividing a certain squarefree number t, and studying associated mixed exponential sums. Because of the definition chosen for the sequence of signs ± 1, this requires the study of carries in the sum $x+1$ in base p in order to deals with correlations.

Section 16 deal with the coefficients of P_3 and P_5, again by Poisson summation.

Section 17 starts the derandomization of the Körner correction, beginning with the polynomial $P^{(1)}$ defined in Section 12. Denoting by $\xi(z)$ a certain function, the problem becomes to find explicit coefficients ω_k such that

$$\sum_{-M<k<N+M} \omega_k \xi(\widehat{P^{(1)}}(k)) e(k\theta)$$

is essentially as small as what can be obtained by probabilistic methods. The main difficulty is that the function $\xi(z)$ which controls the Körner correction has the same argument as z and has absolute value $(1/(N+2M) - |z|^2)^{1/2}$. If z is small, a good approximation to it may be given by multiplying the argument by a short Taylor series approximation to the square root, but if $|z|^2$ is close to $1/(N+2M)$ then one needs many terms of the Taylor expansion. Moreover, one also needs to control $z/|z|$ and a new difficulty arises, namely that after doing the Taylor series approximation one ends up with terms of type $z \times |z|^{\text{odd}}$. Since the expression for z is a complicated sum, in order to control $|z|^{\text{odd}}$ one needs to express z as a sum of a simple dominating term and a smaller explicit error term, and then proceed with a further Taylor expansion for $|z|^{\text{odd}}$ with center the dominating

term. The nature of the two Taylor expansions changes according to various ranges for $k \in (-M, M+N)$, requiring different considerations. Lemmas 29 and 30 show how to modify $P^{(1)}$ to a new polynomial $P^{(3)}$ with a good explicit Körner correction in the range $k \notin [2\tau N, N - 2\tau N]$.

Section 18 deals with the explicit Körner correction in the range $k \in [2M, N - 2M]$. This reduces the problem to the evaluation of certain exponential sums for which we want to obtain square root cancellation, and in order to achieve this, certain arithmetic conditions are imposed on N, M, and on the parameter ε in Lemmas 31 and 32.

Sections 19 to 23 deal with the most difficult range $k \in [N - 2M, N - 2\tau N]$, the range $[2\tau N, 2M]$ being entirely similar. The first two sections perform a reduction to two different mixed exponential sums, but only on a certain localization assumption (C16) defined in the middle of Section 20. A serious difficulty is that in this range all five polynomials $P_1, \ldots, P_5$ in the decomposition of P_0 play a role in the Fourier coefficients of $P^{(3)}$. Now the Taylor series technique reduces the problem to the study of these two mixed exponential sums, in several variables over $\mathbb{Z}/t\mathbb{Z}$, for a certain parameter t which must be localized in a narrow range. (The many variables arise because the Taylor series involve expansions of high powers of exponential sums in one variable, which become correlated *via* the factors ω_k.)

Section 21 reduces the first sum to a new mixed exponential sum in an arbitrarily large number of variables, which is dealt with by appealing to Deligne's Riemann Hypothesis for L-functions of varieties over finite fields. Here we have bypassed the problem of showing directly the vanishing of the higher l-adic cohomology groups associated to the mixed exponential sum by means of an intricate elementary argument involving repeated use of Cauchy's inequality, followed, at each stage, by a simplification of the mixed exponential sums. The easy Section 22 deals with the second sum. Section 23 checks that indeed all cases are covered for the proof of Theorem 7, under various conditions on parameters made during our arguments; these conditions are listed at the beginning of the section.

Section 24 concludes the proof of Theorem 7 by showing that the key condition (C16) can be satisfied using a standard result of the sieve about large gaps between almost primes and appealing to a theorem of Roth [20] about large gaps between squarefree numbers to end the proof.

The final comments in this section indicate an alternative way of finishing the proof. Then some parts of our arguments, namely the carries considerations in Section 15 and the use of a sieve in Section 24, may be eliminated by appealing to a modified version of a theorem of Filaseta and Trifonov [9] about intervals $[n, n + n^{\theta+o(1)}]$ free of squarefree numbers. Their result $\theta \leq 1/5$ is the current world record for the exponent and, curiously enough, it is precisely $1/5$ that suffices for us. A larger exponent would have given a gain smaller than $1/9$ in the exponent in our Theorem 7. Even so, an improvement on the Filaseta–Trifonov result would have no effect on lowering the exponent $1/2 - 1/9$, since there are other reasons that block the calculations at that level. We believe that further improvements on the problem will require substantially new constructions and ideas.

2. First steps for Theorems 2 and 3

We follow the same pattern of proof as in our previous paper [4]. Here A will denote an arbitrary large but fixed constant, so the dependence on A in the estimates will not be considered.

We start with the polynomial P with $\operatorname{supp}(\widehat{P}) \subset [0, n]$ defined by

$$P(\theta, \alpha) = \sum_{m=-\infty}^{\infty} \chi_\alpha\left(\frac{m}{n}\right) e\left(n\Phi\left(\frac{m}{n}\right)\right) e(m\theta)$$

where Φ is a smooth phase function to be chosen in a moment and $\chi_\alpha(x)$ is a smooth function on $\mathbb{R}$ such that $\chi_\alpha(x) = 0$ for $x < 0$ or $x > 1$ and $\chi_\alpha(x) = 1$ for $2\alpha < x < 1 - 2\alpha$. Here $\alpha \le 1/4$ a small parameter to be chosen later.

By Poisson's summation formula, we have

$$P(\theta, \alpha) = \sum_{h=-\infty}^{\infty} \int_{\mathbb{R}} \chi_\alpha\left(\frac{x}{n}\right) e\left(n\Phi\left(\frac{x}{n}\right) + (\theta - h)x\right) dx. \tag{2.1}$$

As in Littlewood [17], we choose $\Phi(x)$ to be

$$\Phi(x) = \frac{x^2 - x}{2}.$$

With this choice of $\Phi(x)$ the Poisson summation formula (2.1) becomes, after the change of variable $ny \leftarrow x$,

$$P(\theta, \alpha) = \sum_{h=-\infty}^{\infty} n \int_{\mathbb{R}} \chi_\alpha(y) e\left(n\left\{\frac{y^2}{2} + \left(\theta - h - \frac{1}{2}\right)y\right\}\right) dy.$$

We choose χ_α as follows. Let $\psi(x)$ be a positive even smooth function with compact support in $[-1, 1]$ and with $\int_{\mathbb{R}} \psi(x)\, dx = 1$. We introduce two new functions:

$$\varphi_\alpha(x) = \begin{cases} 1 & \text{if } \alpha < x < 1 - \alpha, \\ 0 & \text{otherwise,} \end{cases} \qquad \psi_\alpha(x) = \frac{1}{\alpha}\psi\left(\frac{x}{\alpha}\right),$$

hence ψ_α is supported in $[-\alpha, \alpha]$ and $\int_{\mathbb{R}} \psi_\alpha(x)\, dx = 1$. Then we define

$$\chi_\alpha(x) = (\varphi_\alpha * \psi_\alpha)(x).$$

By construction,

$$\chi_\alpha(x) = \begin{cases} 0 & \text{if } x < 0, \\ 1 & \text{if } 2\alpha < x < 1 - 2\alpha, \\ 0 & \text{if } x > 1, \end{cases} \qquad \chi_\alpha(x) = \chi_\alpha(1 - x).$$

Moreover, for $\nu \ge 1$ the derivative $\chi_\alpha^{(\nu)}$ is supported in $[0, 2\alpha] \cup [1 - 2\alpha, 1]$ and is $\ll \alpha^{-\nu}$ there (not uniformly in ν).

Lemma 9. *For $1/n \le \alpha \le 1/4$, $H \ge 1$, and $\theta \in \mathbb{T} = [-1/2, 1/2]$,*

$$P(\theta,\alpha) = \sum_{|h|\le H} n \int_{\mathbb{R}} \chi_\alpha(y) e\left(n\left\{\frac{y^2}{2} + \left(\theta - h - \frac{1}{2}\right)y\right\}\right) dy + O(H^{-1}).$$

Proof. We integrate by parts twice with respect to the exponential factor, getting for $|h| \ge 1$ the bound

$$\begin{aligned}\int_{\mathbb{R}} \chi_\alpha(y) e\left(n\left\{\frac{y^2}{2} + \left(\theta - h - \frac{1}{2}\right)y\right\}\right) dy \\ \ll n^{-2} \max_{y\in[0,1]} \left\{ \frac{|\chi_\alpha(y)|}{|y+\theta-h-1/2|^4} + \frac{|\chi'_\alpha(y)|}{|y+\theta-h-1/2|^3} + \frac{|\chi''_\alpha(y)|}{|y+\theta-h-1/2|^2} \right\} \\ \ll n^{-1}|h|^{-2}.\end{aligned}$$

To see this, note that:

- χ'_α and χ''_α are supported in $[0, 2\alpha] \cup [1-2\alpha, 1]$;
- $\chi_\alpha^{(\nu)} \ll \alpha^{-\nu}$ for $\nu \ge 1$;
- $|y+\theta-h-1/2| \ge |h| - 1$ on the support $[0, 1]$ of χ_α.

If we multiply by n and sum over $|h| > H$ we obtain the lemma. □

Lemma 10. *Let*

$$I(\lambda) = \int_{\mathbb{R}} \left\{ e\left(-\frac{y^2}{2\alpha^2 n}\right) - 1 \right\} \widehat{\psi}(y) \frac{\sin(2\pi\lambda y)}{2\pi y}\, dy.$$

Then for $0 < \varepsilon \le 1/4$, $A \ge 0$, $n^{-1/2+\varepsilon} \le \alpha \le 1/4$, $\theta \in \mathbb{T}$ and

$$\lambda = \frac{1/2 - |\theta| - \alpha}{\alpha}$$

we have

$$P(\theta,\alpha) = e\left(-\frac{n}{2}\left(\frac{1}{2} - \theta\right)^2 + \frac{1}{8}\right)\sqrt{n}\left\{1 - \int_\lambda^\infty \psi(x)\, dx + I(\lambda)\right\} + O(|\lambda| n^{-A}).$$

Proof. We abbreviate

$$\xi_h = h + \frac{1}{2} - \theta.$$

We have

$$\int_{\mathbb{R}} \chi_\alpha(y) e\left(n\left\{\frac{y^2}{2} - \xi_h y\right\}\right) dy = e\left(-\frac{n}{2}\xi_h^2\right) \int_{\mathbb{R}} \chi_\alpha(y) e\left(\frac{n}{2}(\xi_h - y)^2\right) dy.$$

The last integral is a convolution integral and we evaluate it using the inverse Fourier transform. The Fourier transform is

$$f \mapsto \widehat{f}(x) = \int_{\mathbb{R}} e(-xy) f(y)\, dy,$$

hence $\widehat{\widehat{f}}\,(x) = f(-x)$. The Fourier transform of $e(nx^2/2)$ is

$$e\left(n\frac{x^2}{2}\right)^{\widehat{}} = \frac{e(1/8)}{\sqrt{n}} e\left(-\frac{x^2}{2n}\right).$$

Therefore,

$$\begin{aligned}\int_{\mathbb{R}} \chi_\alpha(y) e\left(\frac{n}{2}(\xi_h - y)^2\right) dy &= \frac{e(1/8)}{\sqrt{n}} \int_{\mathbb{R}} \widehat{\chi}_\alpha(y) e\left(-\frac{y^2}{2n} + \xi_h y\right) dy \\ &= \frac{e(1/8)}{\sqrt{n}} \chi_\alpha(\xi_h) + \frac{e(1/8)}{\sqrt{n}} \int_{\mathbb{R}} \widehat{\chi}_\alpha(y) e(\xi_h y) \left\{ e\left(-\frac{y^2}{2n}\right) - 1 \right\} dy. \end{aligned} \tag{2.2}$$

Recall that $\chi_\alpha(x) = (\varphi_\alpha * \psi_\alpha)(x)$ and

$$\widehat{\varphi}_\alpha(x) = \frac{e(-\alpha x) - e(-(1-\alpha)x)}{2\pi i x}, \qquad \widehat{\psi}_\alpha(x) = \widehat{\psi}(\alpha x),$$

hence

$$\widehat{\chi}_\alpha(x) = \widehat{\psi}(\alpha x) \frac{e(-\alpha x) - e(-(1-\alpha)x)}{2\pi i x}.$$

We substitute into (2.2) and make a change of variable $y \leftarrow z/\alpha$ in the last integral. Since $\widehat{\psi}$ is even, only the even part of the integrand matters here and we obtain

$$\begin{aligned}\int_{\mathbb{R}} \chi_\alpha(y) e\left(\frac{n}{2}(\xi_h - y)^2\right) dy &= \frac{e(1/8)}{\sqrt{n}} \chi_\alpha(\xi_h) \\ &\quad + I\left(\frac{\xi_h - \alpha}{\alpha}\right) - I\left(\frac{\xi_h - 1 + \alpha}{\alpha}\right). \end{aligned} \tag{2.3}$$

Next, we prove that for every fixed $A \geq 0$, $0 < \varepsilon \leq 1/2$, and

$$n^{-1/2+\varepsilon} \leq \alpha \leq 1/4$$

we have

$$I(\lambda) \ll |\lambda| n^{-A} \quad \text{if } \lambda \notin [-1, 1]. \tag{2.4}$$

We proceed as in [4, Sections 5 and 6]. We recall the well-known inequality (see [4, Lemma 7.1])[2]

$$\left| e^z - \sum_{j=0}^{J-1} \frac{z^j}{j!} \right| \leq \frac{|z|^J}{J!} \quad \text{for } \Re(z) \leq 0 \tag{2.5}$$

and the easy calculation (note that $\psi(x)$ is even)

$$\int_{\mathbb{R}} \widehat{\psi}(y) \frac{\sin(2\pi\lambda y)}{2\pi y} y^{2j}\, dy = (2\pi i)^{-2j} \psi^{(2j-1)}(\lambda).$$

[2] By $\Re(z)$ and $\Im(z)$ we denote the real and imaginary part of the complex number z.

Since $|\sin(x)| \le |x|$, the last equation and the definition of $I(\lambda)$ yield

$$\left| I(\lambda) - \sum_{j=1}^{J-1} \frac{\psi^{(2j-1)}(\lambda)}{j!(-4\pi i\alpha^2 n)^j} \right| \le (4\pi\alpha^2 n)^{-J} \frac{|\lambda|}{J!} \int_{\mathbb{R}} |\widehat{\psi}(y)| y^{2J}\, dy.$$

The function $\widehat{\psi}$ is rapidly decreasing at infinity, thus (not uniformly in J) $\int_{\mathbb{R}} |\widehat{\psi}(y)| y^{2J}\, dy \ll 1$. Therefore, the estimate (not uniform in J)

$$I(\lambda) \ll |\lambda|(\alpha^2 n)^{-J} \ll |\lambda| n^{-2\varepsilon J}$$

holds if $|\lambda| \ge 1$. The estimate (2.4) follows by taking $J > A/(2\varepsilon)$.

By the last displayed inequality, if $|h| \ge 1$ we have

$$I\left(\frac{\xi_h - \alpha}{\alpha}\right) \ll |h|\alpha^{-1} n^{-A}, \qquad I\left(\frac{\xi_h - 1 + \alpha}{\alpha}\right) \ll |h|\alpha^{-1} n^{-A}.$$

If instead $h = 0$, noting that $I(\lambda)$ is odd we find

$$I\left(\frac{\xi_h - \alpha}{\alpha}\right) - I\left(\frac{\xi_h - 1 + \alpha}{\alpha}\right) = I\left(\frac{1/2 - |\theta| - \alpha}{\alpha}\right) + O(\alpha^{-1} n^{-A}).$$

Hence Lemma 9 yields Lemma 10 with the error term $O(H^2\alpha^{-1}n^{-A}) + O(H^{-1})$. We conclude the proof by taking $H = n^{A/3}$ and replacing A by $3A + 1$, which we may because A can be taken arbitrarily large. □

3. Proofs of Theorems 2 and 3

We choose ψ as in [4], namely

$$\psi(x) = c(a) \exp\left(-\frac{1}{(1-x)^a} - \frac{1}{(1+x)^a} \right)$$

if $-1 < x < 1$ and 0 otherwise, with $c(a)$ such that $\int_{\mathbb{R}} \psi(x)\, dx = 1$.

Lemma 11. *Let $\kappa > 1$, $a \ge 2$, and $A \ge 0$, be fixed and suppose that*

$$n^{-1/2} (\log n)^{(3/2+1/a)\kappa} \le \alpha \le 1/4.$$

If $|\theta| \le 1/2 - 2\alpha$ then

$$P(\theta, \alpha) = e\left(-\frac{n}{2}\left(\frac{1}{2} - \theta\right)^2 + \frac{1}{8} \right) \sqrt{n} + O(n^{-A}),$$

while if $1/2 - 2\alpha < |\theta| \le 1/2$ then

$$|P(\theta, \alpha)| \le \sqrt{n} + O(n^{-A}).$$

Proof. This follows from [4, Lemma 7.7] upon taking[3] $M = \lfloor \log n \rfloor$, $t = n$. □

Proof of Theorem 2. Combine Lemma 11 and [4, Lemmas 7.7 and 7.8]. □

Proof of Theorem 3. Theorem 2 and the Körner correction as in Lemma 15 in this paper or as in Lemma 2 in [14] immediately imply the weaker result with the error term $O(n^{1/4}(\log n)^{5/4+\varepsilon})$. The improvement in the exponent of the logarithm comes from the refinement by Queffélec and Saffari in [19, Lemma 8]. □

4. First steps for Theorem 4

The strategy in the preceding part of this paper was to use a Gaussian phase and coefficients of constant modulus, smoothing them down to 0 at the beginning and end of the polynomial. A careful choice of the smoothing then yielded control of the absolute value of the polynomial.

However, the polynomial $P(\theta)$ constructed for Theorem 2 falls short of providing the desired example for two reasons. The first is that the polynomial has absolute value smaller than $\sqrt{n} + o(\sqrt{n})$ when $|\theta|$ gets very close to $1/2$. The second is that the Fourier coefficients of $P(\theta)$ are smaller than $1 + o(1)$ at the beginning and end of the polynomial, due to the smoothing factor introduced to handle Poisson summation. This second obstacle was removed in Theorem 3 by a direct application of the Körner correction, but removing the first obstacle is the crux of the matter here and one has to follow a more circuitous route.

In Kahane's paper [14] this was achieved by randomizing the phase near $|\theta| = 1/2$ and using smoothed truncated approximations to eliminate the high frequency Fourier coefficients of the modified function $P(\theta)$, to ensure that $P(\theta)$ remained a polynomial of length near to n. The Fourier coefficients smaller than 1 introduced by the random procedure and by the smoothed truncation were dealt with by another application of the Körner correction. Our approach is somewhat different from Kahane's and we shall work directly with polynomials. This has several advantages, namely the direct construction of a large class of polynomials of nearly constant absolute value on $\mathbb{T}$ and also avoiding the smoothed truncation used in [14], which is fairly costly for the final result.

Our starting point is a partition of unity $P(\theta)$ by translates $\gamma(\theta - \theta_s)$ of a short polynomial γ, with $\widehat{\gamma}$ supported in $[-M, M]$; here M is not too large, to be chosen later. From this partition of unity we construct a new polynomial of length about N, by patching together $\gamma(\theta - \theta_s)e(N_s\theta)e(-N_s\theta_s)z_s$ where the steps N_s vary slowly between 0 and N. The coefficients z_s are near to 1 in absolute value and chosen so that $e(-N_s\theta_s)z_s$ changes slowly with s. By doing so, we end up with the construction of a rather general polynomial $P_0(\theta)$ that remains everywhere close to 1 in absolute value, with $\widehat{P_0}$ supported in the interval $[-M, N + M]$. The details are as follows.

Let N and M be large positive integers with $N^{1/2} \ll M \ll N$, where M will be specified at the end as being of order $N^{1-\eta}$ for a certain $\eta > 0$. The exponential polynomial

[3] The error term $O(t^{-1000})$ in [4] can be taken as $O(t^{-A})$ for arbitrary A.

$\gamma(\theta)$ will have $\operatorname{supp}(\widehat{\gamma}) \subset (-M, M)$, hence

$$\gamma(\theta) := \sum_{|m|<M} \widehat{\gamma}(m) e(m\theta).$$

We also write

$$\theta_s := -\frac{1}{2} + \frac{s}{M} \quad \text{for } 0 \le s < M.$$

During the various phases of the construction we shall impose various conditions, labeled (C0), (C1), ... to separate them from the numbering of equations. Here A will denote a fixed arbitrarily large constant and the dependence on A in the estimates will not be considered. We assume that

$$N = 2RM \tag{C0}$$

so N is an even multiple of M. This condition will not affect the final result.

Lemma 12. *Let $0 < \varepsilon \le 1/2$ and $A \ge 0$ be given. There is an exponential polynomial*

$$\gamma(\theta) = \sum_{|m|<M} \widehat{\gamma}(m) e(m\theta),$$

real and positive everywhere, such that for $\theta \in \mathbb{T}$:

$$\sum_{0\le s<M} \gamma(\theta - \theta_s) = 1; \tag{4.1}$$

$$0 \le \widehat{\gamma}(m) \le \widehat{\gamma}(0) = 1/M; \tag{4.2}$$

$\widehat{\gamma}(m) = \psi(m)$ where $\psi \in C_0^\infty([-M, M])$ satisfies

$$\psi^{(\nu)}(x) \ll M^{-1-\nu} \quad \textit{for every fixed } \nu, \tag{4.3}$$

and

$$\gamma(\theta) \ll N^{-A} \quad \textit{for } M^{-1+\varepsilon} \le |\theta| \le 1/2. \tag{4.4}$$

Proof. A simple construction runs as follows. Let $\chi \in C_0^\infty([-1/2, 1/2])$ be real and even and define

$$\gamma(\theta) = c\left|\sum_{m\in\mathbb{Z}} \chi\left(\frac{m}{M}\right) e(m\theta)\right|^2 \quad \text{where} \quad c = \frac{1}{M}\left(\sum_{m\in\mathbb{Z}} \chi\left(\frac{m}{M}\right)^2\right)^{-1}.$$

Clearly, $\gamma(\theta)$ is a positive exponential polynomial with $\operatorname{supp}(\widehat{\gamma}) \subset (-M, M)$ and (4.2) holds. Moreover, (4.3) holds with

$$\psi(x) = c \sum_{m=-\infty}^{\infty} \chi\left(\frac{m+x}{M}\right)\chi\left(\frac{m}{M}\right)$$

because c is of order M^{-2}.

Next, we compute

$$\sum_{0\le s<M}\gamma(\theta-\theta_s)=\sum_{0\le s<M}\sum_{|m|<M}\widehat{\gamma}(m)e(m\theta-m\theta_s)$$
$$=\sum_{|m|<M}\sum_{0\le s<M}\widehat{\gamma}(m)e\left(m\left(\theta+\frac{1}{2}\right)\right)e\left(-\frac{ms}{M}\right)=M\widehat{\gamma}(0)$$

as one verifies by summing first over s. Hence (4.1) follows from (4.2).

Poisson's summation formula and integration by parts J times show that

$$\sum_{m\in\mathbb{Z}}\chi\left(\frac{m}{M}\right)e(m\theta)=\sum_{h\in\mathbb{Z}}\int_{\mathbb{R}}\chi\left(\frac{x}{M}\right)e((\theta-h)x)\,dx$$
$$=M\sum_{h\in\mathbb{Z}}\int_{\mathbb{R}}\chi(x)e((M(\theta-h)x)\,dx$$
$$\ll M\sum_{h\in\mathbb{Z}}(1+M|\theta-h|)^{-J}\ll M^{1-\varepsilon J}$$

provided $M^{-1+\varepsilon}\le|\theta|\le 1/2$ and $J\ge 2$. Now inequality (4.4) is immediate by taking J sufficiently large. □

In the next step, we put together the translates $\gamma(\theta-\theta_s)$ in a new exponential polynomial by setting

$$P_0(\theta):=\sum_{0\le s<M}\gamma(\theta-\theta_s)e(N_s(\theta-\theta_s))z_s \tag{4.5}$$

where the integers N_s and the coefficients z_s satisfy for $0\le s<M$ the following conditions:

$$0\le N_s\le N, \tag{C1}$$
$$|N_s-N_{s+1}|<\delta M, \tag{C2}$$
$$|z_s|=1+O(\delta^2), \tag{C3}$$
$$|z_{s+1}-e(N_s(\theta_{s+1}-\theta_s))z_s|<\delta, \tag{C4}$$

where we define $N_M=N_0$, $z_M=z_0$, and where δ is a small parameter, to be chosen later as a small negative power of N. Clearly,

$$\operatorname{supp}(\widehat{P_0})\subset[-M,N+M].$$

The next lemma shows that the polynomial P_0 continues to be close to 1 in absolute value.

Lemma 13. *Let $\gamma(\theta)$ be as in Lemma* 12 *and let P_0 be defined by* (4.5) *with the conditions* (C1) *to* (C4) *satisfied. Then*

$$|P_0(\theta)|=1+O(\delta^2M^{2\varepsilon})+O(M^{-A+1}).$$

Proof. By (4.4), we have $\gamma(\theta-\theta_s) = O(N^{-A})$ unless s belongs to the interval

$$I := [(1/2+\theta)M - M^{\varepsilon}, (1/2+\theta)M + M^{\varepsilon}]$$

with the proviso that if $s < 0$ or $s \geq M$ we replace θ_s by $\theta_{s\pm M}$ as needed.

Let us fix θ. We compute (uniformly in θ), for $s \in I$,

$$\begin{aligned}
&|e((\theta-\theta_{s+1})N_{s+1})z_{s+1} - e((\theta-\theta_s)N_s)z_s| \\
&\quad = |z_{s+1} - e(-(\theta-\theta_{s+1})(N_{s+1}-N_s))e((\theta_{s+1}-\theta_s)N_s)z_s| \\
&\quad \leq |z_{s+1} - e((\theta_{s+1}-\theta_s)N_s)z_s| + |1 - e(-(\theta-\theta_{s+1})(N_{s+1}-N_s))| \cdot |z_s| \ll \delta M^{\varepsilon}
\end{aligned}$$

because of (C4), (C2), (C3), and $|\theta-\theta_s|(N_{s+1}-N_s) \leq 2\delta M^{\varepsilon}$.

Since $|z_s| = 1 + O(\delta^2)$, this implies that the points

$$v_s := e((\theta-\theta_s)N_s)z_s$$

have absolute value

$$|v_s| = |z_s| = 1 + O(\delta^2).$$

Those with $s \in I$ have argument in some arc on $|z| = 1$ of length at most $O(M^{2\varepsilon}\delta)$, because we have seen that moving from one point to the next the argument cannot change by more than $O(M^{\varepsilon}\delta)$, while there are at most $|I| + 1 = O(M^{\varepsilon})$ possibilities for $s \in I$. In particular, the convex closure of the points v_s with $s \in I$ is contained in an annulus

$$1 - CM^{2\varepsilon}\delta^2 \leq |z| \leq 1 + CM^{2\varepsilon}\delta^2$$

for some constant C.

By (4.4) we have

$$\sum_{s\in I}\gamma(\theta-\theta_s) = \sum_{0\leq s<M}\gamma(\theta-\theta_s) - \sum_{s\notin I}\gamma(\theta-\theta_s) = 1 - \sum_{s\notin I}\gamma(\theta-\theta_s) = 1 + O(M^{-A+1})$$

and also $\gamma(\theta-\theta_s) \geq 0$ for any s. Therefore, since

$$\Big(\sum_{s\in I}\gamma(\theta-\theta_s)\Big)^{-1}\sum_{s\in I}\gamma(\theta-\theta_s)v_s$$

lies in the convex closure of the points v_s with $s \in I$, we conclude that

$$\Big|\sum_{s\in I}\gamma(\theta-\theta_s)v_s\Big| = 1 + O(M^{2\varepsilon}\delta^2) + O(M^{-A+1}). \tag{4.6}$$

We have also seen that $\gamma(\theta-\theta_s) = O(M^{-A})$ for $s \notin I$, hence

$$\sum_{s\notin I}\gamma(\theta-\theta_s)v_s = O(M^{-A+1}). \tag{4.7}$$

Putting together (4.6) and (4.7) we get the lemma. □

5. Choosing coefficients and parameters

We begin by choosing the phase jumps $N_{s+1} - N_s$ so that $P_0(\theta)$ is close (up to a constant factor) to the polynomial $P(\theta)$, yielding Theorem 2, except for $|\theta|$ near $1/2$. The details are as follows.

Let

$$\tau := N^{-1/2+\varepsilon}, \qquad s_1 := \lfloor \tau M \rfloor.$$

Let $\beta \in C_0^\infty([0, 1]$ be a positive function, symmetric about $x = 1/2$, hence

$$\beta(x) = \beta(1 - x),$$

such that for $0 \le x \le 1/2$,

$$\beta(x) = 1 \qquad \text{if } 2\tau < x \le 1/2, \tag{C5}$$

$$0 \le \beta(x) \le 1 \qquad \text{if } \tau \le x \le 2\tau, \tag{C6}$$

$$\beta(x) = 0 \qquad \text{if } 0 \le x \le \tau. \tag{C7}$$

We will need natural derivative estimates for $\beta^{(\nu)}(x)$ for $0 \le x \le 1/2$ and $\nu \ge 1$; the range $1/2 \le x \le 1$ is dealt with using the symmetry condition $\beta(x) = \beta(1 - x)$. For an appropriate choice of $\beta(x)$ and any fixed $0 < \eta \le 1$ we have (not uniformly in ν)

$$\beta^{(\nu)}(x) \ll \tau^{-\nu} \min(\beta(x), 1 - \beta(x))^{1-\eta} \qquad \text{if } \tau \le x \le 2\tau, \tag{5.1}$$

$$\beta^{(\nu)}(x) = 0 \qquad \text{otherwise.}$$

We set

$$z_s := e\left(\frac{1}{M}\sum_{t=0}^{s-1} N_t\right)\zeta_s$$

(hence $z_0 = \zeta_0$) and impose the condition

$$e\left(\frac{1}{M}\sum_{t=0}^{M-1} N_t\right) = 1. \tag{5.2}$$

Then the key condition (C4) simply becomes

$$|\zeta_{s+1} - \zeta_s| < \delta \tag{C4$'$}$$

(condition (5.2) is used to deal with $s = M - 1$). Also, (C3) is the same as

$$|\zeta_s| = 1 + O(\delta^2). \tag{C3$'$}$$

Let us abbreviate

$$L := \lfloor R\tau^{-1} \rfloor - 2R.$$

Then (recall that $N = 2RM$) we choose the phase steps N_s as follows:

$$\begin{aligned} N_s &= RM + Ls && \text{if } 0 \le s < s_1, \\ N_s &= 2RM - 2Rs && \text{if } s_1 \le s \le M - s_1, \\ N_s &= RM - L(M - s) && \text{if } M - s_1 < s < M. \end{aligned} \tag{5.3}$$

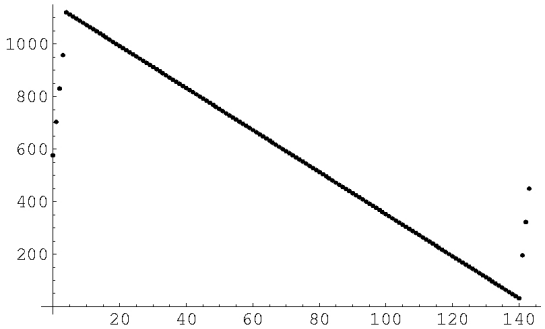
With this choice we have $\sum_{t=0}^{M-1} N_t = M^2 R$ and (5.2) is satisfied, hence we may replace condition (C4) by (C4′). The important condition (C2) now becomes $L < \delta M$ if $0 \le s < s_1 - 1$ or $M - s_1 + 1 \le s < M - 1$, $2R < \delta M$ if $s_1 \le s < M - s_1 - 1$, and also

$$-2R + RM - \lfloor R\tau^{-1} \rfloor (s_1 - 1) < \delta M$$

if $s = s_1 - 1$ or $s = M - s_1$. It is an easy matter to verify that for large N this follows from the simpler condition

$$N^{3/2} M^{-2} < \delta, \tag{C2′}$$

which we shall suppose henceforth.



The steps N_s. $N = 1152$, $M = 144$, $R = 4$.

The choice of ζ_s is limited for the time being to

$$\zeta_s = 1 \quad \text{if } 2s_1 \le s \le M - 2s_1. \tag{5.4}$$

6. The decomposition $P_0 = P_1 + P_2 + P_3 + P_4 + P_5$

Since $\gamma(\theta - \theta_s)$ is concentrated, as s varies, near $\theta_s \sim \theta$ and since $\sum_s \gamma(\theta - \theta_s) = 1$, our choice of ζ_s implies that $P_0(\theta)$ behaves like Littlewood's polynomial (up to multiplication by a normalizing factor) for θ away from $\pm 1/2$. Thus its Fourier coefficients $\widehat{P_0}(k)$ are close to $N^{-1/2}$ in absolute value, provided k stays sufficiently away from the end points of the support of P_0.

In order to make this explicit, we decompose P_0 into five pieces

$$P_0 = P_1 + P_2 + P_3 + P_4 + P_5$$

determined by the choice of the phase steps N_s, by the smoothing function $\beta(x)$, and the choice (5.4) for ζ_s:

$$P_1(\theta) := \sum_{s_1 \le s \le M - s_1} \gamma(\theta - \theta_s) e(N_s(\theta - \theta_s)) e\Big(\frac{1}{M}\sum_{t=0}^{s-1} N_t\Big)\beta\Big(\frac{s}{M}\Big),$$

$$P_2(\theta) := \sum_{s_1 \le s < 2s_1} \gamma(\theta - \theta_s) e(N_s(\theta - \theta_s)) e\Big(\frac{1}{M}\sum_{t=0}^{s-1} N_t\Big)\Big\{\zeta_s - \beta\Big(\frac{s}{M}\Big)\Big\},$$

$$P_3(\theta) := \sum_{0 \le s < s_1} \gamma(\theta - \theta_s) e(N_s(\theta - \theta_s)) e\Big(\frac{1}{M}\sum_{t=0}^{s-1} N_t\Big)\zeta_s,$$

$$P_4(\theta) := \sum_{M - 2s_1 < s \le M - s_1} \gamma(\theta - \theta_s) e(N_s(\theta - \theta_s)) e\Big(\frac{1}{M}\sum_{t=0}^{s-1} N_t\Big)\Big\{\zeta_s - \beta\Big(\frac{s}{M}\Big)\Big\},$$

$$P_5(\theta) := \sum_{M - s_1 < s < M} \gamma(\theta - \theta_s) e(N_s(\theta - \theta_s)) e\Big(\frac{1}{M}\sum_{t=0}^{s-1} N_t\Big)\zeta_s,$$

with $\beta(x)$ as defined in the preceding section.

7. The Fourier coefficients of P_1

Lemma 14. *The Fourier coefficients of $P_1(\theta)$ have support* $\operatorname{supp}(\widehat{P_1}) \subset [-M, N + M]$. *Let*

$$\Omega := (L + 2R)\frac{s_1^2 - s_1}{2M}, \qquad \varepsilon > 0, \qquad J > 1/\varepsilon.$$

Then:

(i) *For $k \in [2\tau N, N - 2\tau N]$,*

$$\widehat{P_1}(k) = e\Big(\Omega - \frac{1}{8} + \frac{k^2}{2N} - \frac{k}{2}\Big)N^{-1/2}(1 + \kappa_1) + O(N^{-A})$$

where

$$\kappa_1 := M\sum_{j=1}^{J} \frac{N^j}{j!(4\pi i)^j}\psi^{(2j)}(0) = O(M^{-2}N) \tag{7.1}$$

and $A = 2\varepsilon J - 1$.

(ii) *For $k \notin [2\tau N, N - 2\tau N]$,*

$$\widehat{P_1}(k) = e\Big(\Omega - \frac{1}{8} + \frac{k^2}{2N} - \frac{k}{2}\Big)N^{-1/2}c(k) + O(M^{-2}N^{1/2}) \tag{7.2}$$

where

$$\Big|c(k) - \beta\Big(1 - \frac{k}{N}\Big)\Big| \le \frac{1}{10}\Big\{1 - \beta\Big(1 - \frac{k}{N}\Big)\Big\}.$$

(iii) *Moreover, with a suitable choice of $\beta(x)$ both $\Re(c(k))$ and $\Im(c(k))$ can be expressed as sums of a bounded number of bounded monotonic functions of k, with bounds independent of M, N.*

Proof. A straightforward calculation yields, recalling that $\widehat{\gamma}(m) = \psi(m)$,

$$\begin{aligned}\widehat{P}_1(k) &= e(\Omega) \sum_{m+N_s=k} \psi(k-N_s)\beta\left(\frac{s}{M}\right) e\left(-k\theta_s + 2Rs - \frac{N}{2}\left(\frac{s}{M}\right)^2\right) \\ &= (-1)^k e(\Omega) \sum_{0\le s<M} \varphi_k\left(\frac{s}{M}\right) e\left((N-k)\frac{s}{M} - \frac{N}{2}\left(\frac{s}{M}\right)^2\right)\end{aligned}$$

where

$$\varphi_k(x) := \psi(k - N + Nx)\beta(x).$$

We transform the sum using Poisson summation obtaining

$$\begin{aligned}\widehat{P}_1(k) &= (-1)^k e(\Omega) \sum_{h\in\mathbb{Z}} \int_{\mathbb{R}} \varphi_k\left(\frac{x}{M}\right) e\left((N-k)\frac{x}{M} - \frac{N}{2}\left(\frac{x}{M}\right)^2\right) e(-hx)\,dx \\ &= (-1)^k e(\Omega) M \sum_{h\in\mathbb{Z}} e\left(\frac{N}{2}\xi_{k,h}^2\right) \int_{\mathbb{R}} \varphi_k(x) e\left(-\frac{N}{2}(\xi_{k,h}-x)^2\right) dx \qquad (7.3)\end{aligned}$$

where we have abbreviated

$$\xi_{k,h} := 1 - \frac{k}{N} - \frac{Mh}{N}$$

for the stationary phase point of the integral. The precise evaluation of the last sum goes as follows.

We need to estimate the integral in the right-hand side of (7.3), first for large h to obtain control of the tail of the sum, then for smaller values of h with an asymptotic expansion. The first part goes as in Lemma 9. We integrate by parts twice with respect to the exponential, getting

$$\begin{aligned}&\int_{\mathbb{R}} \varphi_k(x) e\left(-\frac{N}{2}(\xi_{k,h}-x)^2\right) dx \\ &\qquad \ll N^{-2} \max_{x\in[0,1]} \left\{ \frac{|\varphi_k(x)|}{|x-\xi_{k,h}|^4} + \frac{|\varphi_k'(x)|}{|x-\xi_{k,h}|^3} + \frac{|\varphi_k''(x)|}{|x-\xi_{k,h}|^2} \right\}. \qquad (7.4)\end{aligned}$$

We estimate the derivatives of $\varphi_k(x)$ using Lemma 12. By Leibniz's rule and (5.1), (4.3),

$$\begin{aligned}\varphi_k^{(\nu)}(x) &= \sum_{\mu=0}^{\nu} \binom{\nu}{\mu} N^\mu \psi^{(\mu)}(k-N+Nx)\beta^{(\nu-\mu)}(x) \qquad (7.5) \\ &\ll \sum_{\mu=0}^{\nu} N^\mu M^{-1-\mu} \tau^{\mu-\nu} \ll M^{-1}\tau^{-\nu} \qquad (7.6)\end{aligned}$$

provided

$$M \geq N\tau,$$

which we may suppose. Also

$$|x - \xi_{k,h}| \geq \frac{M}{2N}|h|$$

if $x \in [0, 1]$, $k \in [-M, N + M]$, and $|h| \geq 2 + 2N/M$. We conclude that the integral in (7.4) is $O(NM^{-3}|h|^{-2})$ as soon as $M \geq \tau N$ and $|h| \geq H \geq 2 + 2N/M$; the total contribution to the sum over h in this range is therefore $O(1/H)$.

For smaller values of h we need to be more careful because stationary phase may contribute to the integrals. As in the proof of Lemma 10, we have

$$\begin{aligned}\int_{\mathbb{R}} \varphi_k(x) e\left(-\frac{N}{2}(\xi_{k,h} - x)^2\right) dx \\ = \frac{e(-1/8)}{\sqrt{N}}\varphi_k(\xi_{k,h}) + \frac{e(-1/8)}{\sqrt{N}} \int_{\mathbb{R}} \widehat{\varphi}_k(y) e(\xi_{k,h} y)\left\{e\left(\frac{y^2}{2N}\right) - 1\right\} dy. \qquad (7.7)\end{aligned}$$

We use again the approximation of the exponential in (2.5) to obtain from (7.7) an asymptotic series

$$\begin{aligned}\int_{\mathbb{R}} \varphi_k(x) e\left(-\frac{N}{2}(x - \xi_{k,h})^2\right) dx = \frac{e(-1/8)}{\sqrt{N}}\varphi_k(\xi_{k,h}) \\ + \sum_{j=1}^{J-1} \frac{e(-1/8)}{\sqrt{N}} \frac{1}{j!(4\pi i N)^j} \varphi_k^{(2j)}(\xi_{k,h}) + \frac{\Gamma(k, h, J)}{\sqrt{N}\, J!(4\pi N)^J} \int_{\mathbb{R}} |\widehat{\varphi}_k(y)| y^{2J}\, dy \qquad (7.8)\end{aligned}$$

for some complex number $\Gamma(k, h, J)$ satisfying the bound

$$|\Gamma(k, h, J)| \leq 1.$$

In particular, this estimate is uniform with respect to h.

We estimate the error term in this asymptotic expansion. By Cauchy's inequality and Plancherel's formula

$$\begin{aligned}\int_{\mathbb{R}} |\widehat{\varphi}_k(y)| y^{2J}\, dy \leq \left\{\int_{\mathbb{R}} \frac{dy}{1 + y^2}\right\}^{1/2} \left\{\int_{\mathbb{R}} |\widehat{\varphi}_k(y)|^2 (y^{4J} + y^{4J+2})\, dy\right\}^{1/2} \\ = \sqrt{\pi}\left\{\int_{\mathbb{R}} ((2\pi)^{-4J} |\varphi^{(2J)}(y)|^2 + (2\pi)^{-4J-2} |\varphi^{(2J+1)}(y)|^2)\, dy\right\}^{1/2}. \qquad (7.9)\end{aligned}$$

and it remains to estimate the derivatives $\varphi_k^{(\nu)}$. We recall (7.6), namely $\varphi_k^{(\nu)}(x) \ll M^{-1}\tau^{-\nu}$. Noting that φ_k has support in [0, 1], we infer that (not uniformly in ν)

$$\int_{\mathbb{R}} |\varphi_k^{(\nu)}(x)|^2\, dx \ll M^{-2} N^{\nu(1-2\varepsilon)}.$$

By (7.9), we deduce

$$\int_{\mathbb{R}} |\widehat{\varphi_k}(y)| y^{2J}\, dy \ll N^{(1-2\varepsilon)J}. \tag{7.10}$$

Hence the error term is $O(N^{1-2\varepsilon J})$.

We have shown that with such a choice for J we have

$$\int_{\mathbb{R}} \varphi_k(x) e\left(-\frac{N}{2}(x-\xi_{k,h})^2\right) dx = \frac{e(-1/8)}{\sqrt{N}} \sum_{j=0}^{J-1} \frac{1}{j!(4\pi i N)^j} \varphi_k^{(2j)}(\xi_{k,h}) + O(N^{1-2\varepsilon J}).$$

Stationary phase occurs only at $x = \xi_{k,h}$, but Leibniz's formula (7.5) for $h \neq 0$ yields

$$\varphi_k^{(\nu)}(\xi_{k,h}) = \sum_{\mu=0}^{\nu} \binom{\nu}{\mu} N^{\mu} \psi^{(\mu)}(k - N + N\xi_{k,h}) \beta^{(\nu-\mu)}(\xi_{k,h}) = 0$$

because $\psi \in C_0^{\infty}([-M, M])$ and $k - N + N\xi_{k,h} = -hM \notin (-M, M)$. Thus the asymptotic series vanishes identically for $h \neq 0$ and the contribution to Poisson summation of terms with $1 \leq |h| < H$ is $O(HMN^{-A})$. Taking H to be a large power of N and A even larger we see that the contribution of these terms is, for example, $O(N^{-1000})$ and it can be ignored in what follows.

If $h = 0$ then $\xi_{k,0} = 1 - k/N$ and also $k - N + N\xi_{k,0} = 0$. By Leibniz's formula again, we get

$$\varphi_k^{(2j)}(\xi_{k,0}) = \sum_{\mu=0}^{2j} \binom{2j}{\mu} N^{\mu} \psi^{(\mu)}(0) \beta^{(2j-\mu)}\left(1 - \frac{k}{N}\right).$$

We note that $\psi'(0) = 0$ because $\psi(x)$ is an even function. Hence

$$\begin{aligned} \varphi_k^{(2j)}(\xi_{k,0}) &= \frac{1}{M} \beta^{(2j)}\left(1 - \frac{k}{N}\right) + \sum_{\mu=2}^{2j} \binom{2j}{\mu} N^{\mu} \psi^{(\mu)}(0) \beta^{(2j-\mu)}\left(1 - \frac{k}{N}\right) \\ &= \frac{1}{M} \beta^{(2j)}\left(1 - \frac{k}{N}\right) + O(\tau^{-2j} M^{-1} (\tau N/M)^2). \end{aligned} \tag{7.11}$$

It then follows from (7.8) and the last equation in (7.11) that

$$\begin{aligned} &\int_{\mathbb{R}} \varphi_k(x) e\left(-\frac{N}{2}(x-\xi_{k,0})^2\right) dx \\ &\qquad = \frac{1}{M} \frac{e(-1/8)}{\sqrt{N}} \sum_{j=0}^{J-1} \frac{1}{j!(4\pi i N)^j} \beta^{(2j)}\left(1 - \frac{k}{N}\right) + O(M^{-3} N^{1/2}). \end{aligned} \tag{7.12}$$

In the range where $\beta(x) = 1$ the derivatives of β vanish, hence statement (i) of the lemma follows from the first equation in (7.11) and from (7.12).

If $\beta(x) < 1$ we use the bound (5.1) to obtain, for $j \geq 1$ and a suitable constant $c(j,\eta)$ independent of k and N, the estimate

$$\begin{aligned} N^{-j}\left|\beta^{(2j)}\left(1-\frac{k}{N}\right)\right| &\leq N^{-j}c(j,\eta)\left(1-\beta\left(1-\frac{k}{N}\right)\right)^{1-\eta}\tau^{-2j} \\ &= c(j,\eta)N^{-2\varepsilon j}\left(1-\beta\left(1-\frac{k}{N}\right)\right)^{1-\eta} \\ &\leq 1-\beta\left(1-\frac{k}{N}\right) \end{aligned} \tag{7.13}$$

provided

$$1-\beta\left(1-\frac{k}{N}\right) > c(j,\eta)^{1/\eta}N^{-2\varepsilon j/\eta}.$$

If instead this condition is not satisfied, we have

$$N^{-j}\left|\beta^{(2j)}\left(1-\frac{k}{N}\right)\right| \leq c(j,\eta)N^{-2\varepsilon j}\left(1-\beta\left(1-\frac{k}{N}\right)\right)^{1-\eta} \leq c(j,\eta)^{1/\eta}N^{-2\varepsilon j/\eta}.$$

We conclude that in any case we have (not uniformly in j or η)

$$N^{-j}\left|\beta^{(2j)}\left(1-\frac{k}{N}\right)\right| \leq 1-\beta\left(1-\frac{k}{N}\right)+O(N^{-2\varepsilon j/\eta}).$$

Therefore (not uniformly in J or η)

$$\begin{aligned} \left|\sum_{j=1}^{J-1}\frac{1}{j!(4\pi i N)^j}\beta^{(2j)}\left(1-\frac{k}{N}\right)\right| &\leq \left(\sum_{j=1}^{J-1}\frac{1}{j!(4\pi)^j}\right)\left(1-\beta\left(1-\frac{k}{N}\right)\right)+O(N^{-2\varepsilon/\eta}) \\ &\leq (e^{1/(4\pi)}-1)\left(1-\beta\left(1-\frac{k}{N}\right)\right)+O(N^{-2\varepsilon/\eta}) \\ &< \frac{1}{10}\left(1-\beta\left(1-\frac{k}{N}\right)\right)+O(N^{-2\varepsilon/\eta}). \end{aligned} \tag{7.14}$$

The proof of the lemma is completed by splitting the sum in the Poisson summation formula (7.3) in two pieces, one for $|h| < H$, the other for the tail $|h| > H$ with H satisfying $H \geq 2 + 2N/M$, for example $H = N^{A+1}$ with $A \geq 1$.

By (7.4) and this choice of H, the tail is estimated as $O(N^{-A-1})$.

By (7.8) and (7.10), the sum over h with $1 \leq |h| < N^{A+1}$ is estimated as $O(N^{A+1-2\varepsilon J})$, which is small if J is large.

Therefore, by (7.14) with a sufficiently small η, the contribution for $h = 0$ yields the main term of the two estimates of the lemma. It remains to prove the last statement of the lemma. This will follow from (7.12) if each derivative $\beta^{(2j)}(x)$ for $j < J$ has finitely many maxima and minima, which is indeed not a serious restriction on $\beta(x)$. □

8. The Körner correction

Suppose we have an exponential polynomial

$$P(\theta) := \sum_{n=p+1}^{q} a_n e(n\theta)$$

with coefficients $|a_n| \le 1$. We want to find a new exponential polynomial

$$P^*(\theta) := \sum_{n=p+1}^{q} a_n^* e(n\theta)$$

with coefficients $|a_n^*| = 1$ such that the maximum norm $\|P^* - P\|_\infty$ is small.

The *Körner construction* is as follows. Let a_n, $p < n \le q$, be complex numbers with $a \le |a_n| \le b$ and choose a_n^* to be

$$a_n^* := \begin{cases} a_n \pm i e^{i \arg(a_n)} \sqrt{b^2 - |a_n|^2} & \text{if } a_n \ne 0, \\ \pm b & \text{if } a_n = 0, \end{cases}$$

where the sign $\pm$ is chosen at random with probability $1/2$. Thus a_n is the mid-point of the chord of the circle $|z| = b$ perpendicular to the radius through the point a_n, with end points at the two choices for a_n^*.

Lemma 15 (Körner's correction)**.** *Let*

$$Q(\theta) := \sum_{n=p+1}^{q} a_n e(n\theta)$$

be an exponential polynomial with coefficients $0 \le a \le |a_n| \le b$ for every n. Then there is a choice of signs $\pm$ such that the new polynomial $Q^*(\theta) := \sum a_n^* e(n\theta)$ obtained by Körner's construction satisfies

$$\|Q^* - Q\|_\infty \ll \sqrt{b^2 - a^2}\sqrt{(q-p)\log(q-p+1)}.$$

Remark 16. A more precise result is in Queffélec and Saffari [19, Lemma 8], with the elimination of the $\sqrt{\log(q-p+1)}$ factor.

Proof. We give here the short proof. We begin with the remark that for any exponential polynomial

$$Q(\theta) = \sum_{n=0}^{L} a_n e(n\theta)$$

of degree L we have

$$\max_\theta |Q(\theta)| \le 2 \max_{1 \le j \le 7L} |Q(j/(7L))|. \tag{8.1}$$

In fact, let θ_0 be such that $|Q(\theta_0)| = \max|Q(\theta)|$ and let $\theta_1 = j/(CL) \pmod 1$ be such that $|\theta_1 - \theta_0| \le 1/(2CL)$; here CL is an integer to be chosen later. Then

$$|Q(\theta_1) - Q(\theta_0)| \le \left| \int_{\theta_0}^{\theta_1} Q'(\phi)\, d\phi \right| \le \frac{1}{2CL} \max_{\phi} |Q'(\phi)|$$
$$\le \frac{1}{2CL} 2\pi L \max_{\theta} |Q(\theta)| = \frac{\pi}{C} |Q(\theta_0)|$$

as one sees applying S. Bernstein's well-known inequality for the maximum of the derivative of an exponential polynomial. If we take $C = 7$, hence $\pi/7 < 1/2$, the result follows.

Now the standard probability argument proceeds by noting that if $Z_1, \dots, Z_N$ are random variables then by convexity, for $t \ge 1$,

$$\mathbb{E}(\max_j |Z_j|) \le \mathbb{E}(\max |Z_j|^t)^{1/t} \le \mathbb{E}\Big(\sum_{j=1}^{N} |Z_j|^t \Big)^{1/t} \le N^{1/t} \max_j \mathbb{E}(|Z_j|^t)^{1/t}.$$

We apply this bound with

$$Z_j := \sum_{n=p+1}^{q} (a_n^* - a_n) e(n y_j) = \sum_{n=p+1}^{q} \omega_n i e(n y_j + \arg a_n) \sqrt{b^2 - |a_n|^2}$$

with a Bernoulli sequence (ω_n) of signs $\omega_n = \pm 1$. The expectation of Z_j is $\mathbb{E}(Z_j) = 0$.

By Khinchin's inequality

$$\mathbb{E}(|Z_j|^t) \le t^{t/2} \Big(\sum_{n=p+1}^{q} |a_n^* - a_n|^2 \Big)^{t/2}$$

and we conclude that

$$\mathbb{E}(\max_j |Z_j|) \le \sqrt{t}\, N^{1/t} \| (a_n^* - a_n)_{n=p+1,\dots,q} \|_{\ell^2}.$$

We take $y_j := j/(7(q-p))$ with $j = 1, \dots, 7(q-p)$, hence $N = 7(q-p)$, optimize with $t = 2 \log N$, and estimate the ℓ^2-norm with the ℓ^∞-norm noting that $|a_n^* - a_n| \le \sqrt{b^2 - a^2}$ for every n. Then (8.1) yields the result. □

9. The Fourier coefficients of P_2

Our goal here is to show that we can choose the coefficients ζ_s in such a way that the Fourier coefficients of $P_2(\theta)$ are very small. We will achieve this by a random construction of the points ζ_s somewhat similar to Körner's construction, but the fulfilment of the condition (C4′) on the points ζ_s will create substantial additional difficulties.

Lemma 17. *The coefficients ζ_s can be chosen so that conditions* (C3′) *and* (C4′) *are satisfied and*

$$\widehat{P_2}(k) = 0 \qquad \text{if } k \notin [N - M - \tau N, N + M],$$
$$\widehat{P_2}(k) \ll \delta^{-1/2} N^{-1/4+\varepsilon} M^{-1/2} + \delta^{-1} M^{-1} \qquad \text{if } k \in [N - M - \tau N, N + M].$$

Proof. As at the beginning of the proof of Lemma 14, we get the equation

$$\widehat{P_2}(k) = (-1)^k e(\Omega) \sum_{s_1 \le s < 2s_1} \left(\zeta_s - \beta\left(\frac{s}{M}\right)\right) \psi(k - N + 2Rs) e\left((N-k)\frac{s}{M} - \frac{N}{2}\left(\frac{s}{M}\right)^2\right).$$

Since $\psi \ll M^{-1}$, the trivial estimate for $\widehat{P_2}(k)$ is of order $\tau = N^{-1/2+\varepsilon}$, so we need gain only a factor $N^{-\eta}$, for any small $\eta > 0$, to achieve a non-trivial result.

The function ψ has support in $[-M, M]$, therefore $\widehat{P_2}(k) = 0$ unless $k - N + 2Rs \in [-M, M]$. Since $s \in [s_1, 2s_1]$, this implies that k is restricted to the narrow interval

$$N - M - \tau N < k < N + M. \tag{9.1}$$

Therefore, disregarding the phase factor $(-1)^k e(\Omega)$, we need to obtain a non-trivial bound for

$$S(k) := \sum_{s_1 \le s < 2s_1} \left(\zeta_s - \beta\left(\frac{s}{M}\right)\right) \psi(k - N + 2Rs) e\left((N-k)\frac{s}{M} - \frac{N}{2}\left(\frac{s}{M}\right)^2\right)$$

for $-M < N - k < M - \tau N$, by means of an appropriate choice of the coefficients ζ_s. We also need to verify the constraints (C3′) and (C4′), which we repeat here for the reader's convenience:

$$|\zeta_s| = 1 + O(\delta^2), \tag{C3′}$$
$$|\zeta_{M-1} - \zeta_0| < \delta, \quad |\zeta_s - \zeta_{s+1}| < \delta \quad \text{for } s_1 \le s < 2s_1. \tag{C4′}$$

We cannot apply directly the Körner correction with ζ_s independent random variables, because of the constraint conditions. On the other hand, these conditions imply no *a priori* dependence between ζ_s and $\zeta_{s'}$ if $s' - s$ is somewhat larger than $1/\delta$, and this suggests proceeding in the following way.

At a later stage, it will be important to choose s_1 rather precisely in a range by allowing the parameter τ to vary in an interval $[\tau_0/4, \tau_0]$. So we introduce a fixed parameter ε_0 and correspondingly $\tau_0 = N^{-1/2+\varepsilon_0}$ and vary the parameter ε in the interval

$$\varepsilon \in [\varepsilon_0 - \log 4/\log N, \varepsilon_0].$$

We begin by subdividing the interval $[s_1, 2s_1 - 1]$ into Q subintervals

$$[\Delta_q, \Delta_{q+1}], \quad q = 1, \dots, Q,$$

with the first $Q-1$ intervals of length Δ and a last interval $[\Delta_Q, \Delta_{Q+1}]$ of length at most Δ. Thus $\Delta_q = s_1 + (q-1)\Delta$ for $q \le Q$ and $\Delta_{Q+1} = 2s_1$. We will choose Δ later on, proportional to $1/\delta$. Obviously, since $s_1 = \tau M$, we have

$$Q \asymp \tau M \Delta^{-1}.$$

We let $Q_0 := \lceil \tau_0 M \rceil$ so that in any case

$$Q_0/4 \le Q \le Q_0.$$

Let $X = (\omega_q)$, $q = 1, \dots, Q$, be a Bernoulli sequence of signs $\omega_q = \pm 1$. Then take $u_s \in [0, 1/4]$ such that

$$\cos(2\pi u_s) = \beta(s/M)$$

and set

$$\zeta_s(X) = e(\lambda_s \omega_q u_{\Delta_q} + \lambda'_s \omega_{q+1} u_{\Delta_q}) \quad \text{for } \Delta_q \le s < \Delta_{q+1}. \tag{9.2}$$

Here $(\lambda_s, \lambda'_s) \in [0,1]^2$ will be specified later but we will impose the condition

$$(\lambda_{\Delta_q}, \lambda'_{\Delta_q}) = (1,0), \qquad (\lambda_{\Delta_{q+1}-1}, \lambda'_{\Delta_{q+1}-1}) = (0,1) \tag{C8}$$

to ensure compatibility of ζ_s at the beginning and end of the intervals $[\Delta_q, \Delta_{q+1} - 1]$ when going from one interval to the next.

The choice of λ_s and λ'_s must be such that the expectation $\mathbb{E}(\zeta_s(X))$ is close to $\beta(s/M)$. Since

$$\mathbb{E}(e(a\omega_q + b\omega_{q+1})) = \mathbb{E}(e(a\omega_q))\mathbb{E}(e(b\omega_{q+1})) = \cos(2\pi a)\cos(2\pi b)$$

we impose the further condition

$$\cos(2\pi\lambda_s u_{\Delta_q})\cos(2\pi\lambda'_s u_{\Delta_q}) = \beta(\Delta_q/M), \tag{C9}$$

which, given $\lambda_s \in [0,1]$, determines λ'_s uniquely (note that as λ_s decreases, λ'_s increases). This will ensure that

$$\mathbb{E}(\zeta_s(X)) = \beta(\Delta_q/M).$$

Moreover, we want to evolve from $(\lambda_{\Delta_q}, \lambda'_{\Delta_q}) = (1,0)$ to $(\lambda_{\Delta_{q+1}-1}, \lambda'_{\Delta_{q+1}-1}) = (0,1)$ (thus verifying (C8)) in small steps so as to satisfy (C3′) and (C4′). Therefore, we will avoid backtracking and impose the further condition that λ_s is decreasing, and λ'_s is increasing, in s.

Using the inequality $|e(x) - 1| \le 2\pi|x|$, we verify that the constraints will be satisfied if

$$(|\lambda_s - \lambda_{s+1}| + |\lambda'_{s+1} - \lambda'_s|) u_{\Delta_q} \le \delta/(2\pi). \tag{9.3}$$

Note also that

$$\sum_{s=\Delta_q}^{\Delta_{q+1}-2} (|\lambda_s - \lambda_{s+1}| + |\lambda'_{s+1} - \lambda'_s|) = 2$$

because of the monotonicity condition on λ_s and λ'_s, yielding the telescoping of the sum.

Suppose now that (λ_s, λ'_s) has been determined and for $\Delta_q \le s \le \Delta_{q+1} - 2$ define λ_{s+1} to be the smallest positive for which

$$\lambda_s - \lambda_{s+1} + \lambda'_{s+1} - \lambda'_s \le \frac{\delta}{2\pi u_{\Delta_q}}.$$

This means that we must have the equality sign unless we cannot decrease λ_{s+1} any further, namely stopping at $\lambda_{s+1} = 0$. Therefore, if

$$\Delta_{q+1} - \Delta_q > 4\pi u_{\Delta_q} \delta^{-1} + 1 \tag{C10}$$

we must reach the pair $(\lambda_{\Delta_{q+1}}, \lambda'_{\Delta_{q+1}}) = (0, 1)$ at the end, evolving from $(1, 0)$ to $(0, 1)$ and satisfying the key conditions (C3′) and (C4′) all the way, because otherwise we would contradict the average (9.2). Since $u_s \le 1/4$, we see that (C10) is satisfied for $q = 1, \dots, Q-1$ if

$$\Delta > \pi\delta^{-1} + 1.$$

This proves the existence of a choice of (λ_s, λ'_s) with all the required properties, namely the initial condition at the beginning and end of the interval, monotonicity, and (9.3), provided $\Delta > \pi\delta^{-1} + 1$.

Passing from one interval to the next we have

$$\zeta_{\Delta_{q+1}-1}(X) = e(\omega_{q+1} u_{\Delta_q}), \qquad \zeta_{\Delta_{q+1}}(X) = e(\omega_{q+1} u_{\Delta_{q+1}}),$$

hence

$$|\zeta_{\Delta_{q+1}-1}(X) - \zeta_{\Delta_{q+1}}(X)| \le 2\pi |u_{\Delta_{q+1}} - u_{\Delta_q}|. \tag{9.4}$$

For $0 < x < y \le \pi/2$ and some point ξ between x and y we have

$$\cos(x) - \cos(y) = (x - y)(1 - \cos^2(\xi))^{1/2}.$$

From this and the derivatives estimate (5.1) we infer that for any fixed $\eta > 0$,

$$\begin{aligned} 2\pi |u_{\Delta_q} - u_{\Delta_{q+1}}| &\ll \{\beta(\Delta_{q+1}/M) - \beta(\Delta_q/M)\}\{1 - \beta(\Delta_{q+1}/M)\}^{-1/2} \\ &\ll \frac{\Delta}{\tau M}\{1 - \beta(\Delta_q/M)\}^{1/2-\eta}. \end{aligned} \tag{9.5}$$

By (9.4) and (9.5) it follows that (C4′) is certainly implied by

$$\pi\delta^{-1} + 1 < \Delta \le c_1 \tau M \delta \{1 - \beta(\Delta_q/M)\}^{-1/2+\eta}$$

for a sufficiently small positive constant c_1 depending on η. Since $\tau = N^{-1/2+\varepsilon}$, it suffices to take

$$\Delta = \lceil \pi\delta^{-1} \rceil + 2, \quad \delta > N^{1/4} M^{-1/2}. \tag{C11}$$

For the last interval $[\Delta_Q, \Delta_{Q+1}]$ we simply set

$$\zeta_s = \beta(s/M).$$

The constraint condition (C3′) is $\beta(s/M) = 1 + O(\delta^2)$. Since $\beta(2s_1/M) = 1$ by construction, we deduce from (5.1) that

$$1 - \beta(\Delta_Q/M) \ll \frac{\Delta}{M}\tau^{-1}\{1 - \beta(\Delta_Q/M)\}^{1-\eta}$$

giving

$$1 - \beta(\Delta_Q/M) \ll (\Delta/\tau M)^{1/\eta}.$$

If η is sufficiently small, this is much smaller than δ^2 because of (C11).

We have

$$\begin{aligned}\zeta_s(X) - \beta(\Delta_q/M) &= i\cos(2\pi\lambda_s' u_{\Delta_q})\sin(2\pi\lambda_s u_{\Delta_q})\omega_q \\ &\quad + i\cos(2\pi\lambda_s u_{\Delta_q})\sin(2\pi\lambda_s' u_{\Delta_q})\omega_{q+1} \\ &\quad - \sin(2\pi\lambda_s u_{\Delta_q})\sin(2\pi\lambda_s' u_{\Delta_q})\omega_q\omega_{q+1},\end{aligned}$$

hence, abbreviating

$$r(k,s) := \psi(N-k+2Rs)e\left((N-k)\frac{s}{M} - \frac{N}{2}\left(\frac{s}{M}\right)^2\right) \tag{9.6}$$

we find

$$\begin{aligned}(-1)^k e(-\Omega)\widehat{P}_2(k) &= \sum_{q=1}^{Q-1}\sum_{\Delta_q \le s < \Delta_{q+1}} \{\zeta_s(X) - \beta(\Delta_q/M)\}r(k,s) \\ &\quad + \sum_{q=1}^{Q-1}\sum_{\Delta_q \le s < \Delta_{q+1}} \{\beta(\Delta_q/M) - \beta(s/M)\}r(k,s) \\ &= iZ(k) + iZ'(k) - Z''(k) - Z'''(k) \\ &\quad + \sum_{q=1}^{Q-1}\sum_{\Delta_q \le s < \Delta_{q+1}} (\beta(\Delta_q/M) - \beta(s/M))r(k,s)\end{aligned} \tag{9.7}$$

where

$$\begin{aligned}Z(k) &:= \sum_{q=1}^{Q-1} A_q(k)\omega_q, & Z'(k) &:= \sum_{q=1}^{Q-1} B_q(k)\omega_{q+1}, \\ Z''(k) &:= \sum_{\substack{q=1\\ q\ \text{even}}}^{Q-1} C_q(k)\omega_q\omega_{q+1}, & Z'''(k) &:= \sum_{\substack{q=1\\ q\ \text{odd}}}^{Q-1} C_q(k)\omega_q\omega_{q+1}\end{aligned} \tag{9.8}$$

with

$$A_q(k) := \sum_{\Delta_q \le s < \Delta_{q+1}} r(k,s)\cos(2\pi\lambda_s' u_{\Delta_q})\sin(2\pi\lambda_s u_{\Delta_q}) \ll \frac{\Delta}{M},$$

$$B_q(k) := \sum_{\Delta_q \le s < \Delta_{q+1}} r(k,s)\sin(2\pi\lambda'_s u_{\Delta_q})\cos(2\pi\lambda_s u_{\Delta_q}) \ll \frac{\Delta}{M},$$

$$C_q(k) := \sum_{\Delta_q \le s < \Delta_{q+1}} r(k,s)\sin(2\pi\lambda'_s u_{\Delta_q})\sin(2\pi\lambda_s u_{\Delta_q}) \ll \frac{\Delta}{M}.$$

The sum in (9.7) is majorized by

$$\ll Q\Delta\frac{\Delta}{M}\tau^{-1}M^{-1} \ll \frac{\Delta}{M}$$

and it remains to estimate $Z(k)$, $Z'(k)$, $Z''(k)$, $Z'''(k)$.

We do this using Khinchin's inequality as in Section 8, noting that $Z(k)$, $Z'(k)$, $Z''(k)$, and $Z'''(k)$ are sums of $Q-1$ independent random variables with coefficients bounded by $O(\Delta/M)$. Therefore, we see that there is a choice of the Bernoulli sequence ω such that

$$\max_k \max(|Z(k)|, |Z'(k)|, |Z''(k)|, |Z'''(k)|) \ll \frac{\Delta}{M}\sqrt{Q\log N} \ll \delta^{-1/2}M^{-1/2}N^{-1/4+\varepsilon} \tag{9.9}$$

for all k.

We conclude the proof by recalling that $\widehat{P}_2(k) = 0$ if k does not satisfy (9.1). □

10. The Fourier coefficients of P_3

We have

Lemma 18. *The coefficients ζ_s can be chosen so that conditions* (C3′) *and* (C4′) *are satisfied, $\zeta_0 = 1$, and*

$$\widehat{P}_3(k) \ll MN^{-3/2+\varepsilon}.$$

Proof. We have

$$\widehat{P}_3(k) = (-1)^k \sum_{0 \le s < s_1} \psi(k - N_s)e\left(-k\frac{s}{M}\right)e\left(\frac{1}{M}\sum_{t=0}^{s-1} N_t\right)\zeta_s.$$

Since ψ is supported in $[-M, M]$, recalling the definition (5.3) of N_s for $s \in [0, s_1 - 1]$ we may also restrict s to

$$|k - RM - Ls| < M$$

with $L = \lfloor R\tau^{-1}\rfloor - 2R$. Therefore, s runs through not more than

$$2ML^{-1} + 1 \ll M^2N^{-3/2+\varepsilon}$$

values. We conclude that $\widehat{P}_3(k) \ll MN^{-3/2+\varepsilon}$ for every k, no matter how we choose the coefficients ζ_s with $|\zeta_s| = 1$, thus satisfying the constraint (C3′). We still must satisfy the constraint (C4′). This we can do starting from $s = s_1 - 1$ with $\zeta_{s_1-1} = \zeta_{s_1}$ and ending with $\zeta_0 = 1$, provided s_1 is somewhat larger than $1/\delta$, say $\delta M > N^{1/2}$. However, this last condition is superseded by condition (C2′). □

11. The Fourier coefficients of P_4 and P_5

The estimate of the Fourier coefficients of P_4 and P_5 is essentially identical, the only difference being the ranges of k involved. We find

Lemma 19.

$$\widehat{P}_4(k) = 0 \qquad \text{if } k \notin [-M, M + \tau N],$$
$$\widehat{P}_4(k) \ll \delta^{-1/2} M^{-1/2} N^{-1/4+\varepsilon} + \delta^{-1} M^{-1} \qquad \text{if } k \in [-M, M + \tau N],$$

and

$$\widehat{P}_5(k) \ll M N^{-3/2+\varepsilon} \quad \text{for every } k.$$

Proof. The same as for Lemma 17, *mutatis mutandis*. □

12. Conclusion of proof

We recall an estimate of quadratic Weyl sums.

Lemma 20. *Let N be a positive integer, and let α be a real number with a rational approximation a/q such that $(a, q) = 1$ and $|\alpha - a/q| < B/q^2$, where $B \geq 1$. Then*

$$\sum_{k=1}^{N} e(\alpha k^2 + \theta k) \ll \sqrt{q} + BN/\sqrt{q} \quad \text{uniformly in } \theta.$$

Remark 21. The estimate with an extra logarithmic factor is well known from the theory of Weyl sums and it could be used for our purposes here, with the same conclusions up to the unimportant logarithmic factor. We state the finer result here only for completeness.

Proof. This is an easy consequence of the analysis of incomplete Gauss sums by Hardy and Littlewood [11] in 1921; for $B = 1$, $q \leq 4N$ it is explicit in Fiedler, Jurkat, and Körner [8, Th. 6]. Another (very non-elementary) short proof for $B = 1$, but immediately adaptable to $B \geq 1$, is in [3, p. 5]. □

Corollary 22. *Let $c(k)$ be a positive monotonic function and assume the same hypotheses as in the lemma. Then*

$$\sum_{k=1}^{N} c(k) e(\alpha k^2 + \theta k) \ll \{\max_k c(k)\}(\sqrt{q} + BN/\sqrt{q}) \quad \text{uniformly in } \theta.$$

Proof. Apply the preceding lemma and partial summation. □

First of all, we need to bring all Fourier coefficients below $(N + 2M)^{-1/2}$ if we want to be able to apply the Körner construction. Since

$$N^{-1/2} - (N + 2M)^{-1/2} = O(MN^{-3/2})$$

we do this first step in the range $k \in [2M, N-2M]$ by replacing $\widehat{P_1}(k)$ by the slightly smaller quantity $(1 - MN^{-1+2\varepsilon})\widehat{P_1}(k)$. In fact, in this range we have $\widehat{P_2}(k) = 0$ and $\widehat{P_4}(k) = 0$, while $\widehat{P_3}(k) = O(MN^{-3/2+\varepsilon})$ and $\widehat{P_5}(k) = O(MN^{-3/2+\varepsilon})$. Therefore, we have for $k \in [2M, N-2M]$ the inequality

$$(1 - MN^{-1+2\varepsilon})\widehat{P_1}(k)| + \sum_{i=2}^{5} |\widehat{P_i}(k)| \le (1 - MN^{-1+2\varepsilon})N^{-1/2} + O(MN^{-3/2+\varepsilon}) < (N+2M)^{-1/2}.$$

By Lemma 14 and Corollary 22 applied to the intervals of monotonicity of the real and imaginary part of κ_1 (take $\alpha = 1/(2N)$ and use the last clause of Lemma 14) we have

$$\sum_{k\in I} \widehat{P_1}(k)e(k\theta) = O(1)$$

uniformly in θ and every subinterval $I \subset [-M, N+M]$.

Thus it follows by Lemma 13 that this correction changes the absolute value of $P_0(\theta)$ by not more than $O(MN^{-1+\varepsilon})$.

In the range $[2\tau N, 2M]$ and $[N-2M, N-\tau N]$ we have to be more careful because of the presence of non-zero Fourier coefficients $\widehat{P_2}(k)$ or $\widehat{P_4}(k)$, which are bounded only by $O(\delta^{-1/2}M^{-1/2}N^{-1/4+\varepsilon})$. By the same argument as before, multiplying by $1-\delta^2N^{4\varepsilon}$ the Fourier coefficients $\widehat{P_1}(k)$ in this range introduces the still admissible error of $O(\delta^2N^{4\varepsilon})$ in the evaluation of the corresponding modified exponential polynomial. Now

$$(1 - \delta^2N^{4\varepsilon})|\widehat{P_1}(k)| + \sum_{i=2}^{5} |\widehat{P_i}(k)| \le (N+2M)^{-1/2}$$

provided we choose

$$\delta \asymp M^{-1/5}N^{1/10} \tag{12.1}$$

and

$$M < N^{6/7}, \tag{12.2}$$

which we shall suppose henceforth.

We have shown that the modified exponential polynomial

$$P^{(1)}(\theta) := P_0(\theta) - MN^{-1+2\varepsilon} \sum_{k\in[2M,N-2M]} \widehat{P_1}(k)e(k\theta) - \delta^2N^{4\varepsilon} \sum_{k\notin[2M,N-2M]} \widehat{P_1}(k)e(k\theta) \tag{12.3}$$

satisfies, with δ as in (12.1), the conditions

$$\begin{aligned} &|\widehat{P^{(1)}}(k)| \le (N+2M)^{-1/2} \quad \text{if } k \in [2M, N-2M],\\ &|\widehat{P^{(1)}}(k)| \le (N+2M)^{-1/2} \quad \text{otherwise},\\ &|P^{(1)}(\theta)| = 1 + O(\delta^2N^{4\varepsilon}) + O(MN^{-1+2\varepsilon}). \end{aligned} \tag{12.4}$$

We recall the various conditions that the parameters N, M and δ must still satisfy:

$$\tau N < M < N,$$
$$N = 2RM, \tag{C0}$$
$$M^{-2}N^{3/2} < \delta, \tag{C2$'$}$$
$$N^{1/4}M^{-1/2} < \delta, \tag{C11}$$

all other conditions having being verified in the course of our arguments.

The compatibility condition (C2$'$) is equivalent to

$$M > N^{7/9-\varepsilon}, \tag{C12}$$

which we shall suppose henceforth.

The error $O(MN^{-1+2\varepsilon})$ in the estimate of $P^{(1)}(\theta)$ is absorbed in the error term $O(\delta^2 N^{4\varepsilon})$, provided $M < N^{6/7}$. Thus if

$$N^{7/9-\varepsilon} < M < N^{6/7} \tag{C12$'$}$$

we can eliminate the error term $O(MN^{-1+2\varepsilon})$ in (12.4) with M, N restricted only by (C12$'$).

In order to increase the absolute value of the coefficients exactly to $(N+2M)^{-1/2}$, we apply Lemma 15 (the Körner correction) to the three exponential polynomials with Fourier coefficients $\widehat{P^{(1)}}(k)$ in the three intervals $k \in [-M, 2M]$, $k \in [2M, N-2M]$, $k \in [N-2M, N+M]$ respectively. The corresponding deviations from the uncorrected exponential polynomials are

$$O(N^{-1/2}\sqrt{M\log M}), \qquad O(N^{-1/2}(MN^{-1+2\varepsilon})^{1/2}\sqrt{N\log N}), \qquad O(N^{-1/2}\sqrt{M\log M}).$$

This yields an exponential polynomial $P^*(\theta)$ with $\widehat{P^*}$ supported in $[-M, N+M]$ and

$$|\widehat{P^*}(k)| = (N+2M)^{-1/2},$$
$$|P^*(\theta)| = 1 + O(M^{-2/5}N^{1/5+4\varepsilon}) + O(M^{1/2}N^{-1/2+\varepsilon}(\log N)^{1/2}).$$

Taking M of order $N^{7/9}$, which satisfies the key condition (C12$'$), yields

$$|P(\theta)| = 1 + O(N^{-1/9+4\varepsilon}).$$

Because of condition (C0), this proves Theorem 4 (after a change of phase and rescaling) whenever n is an integer with a factorization $n = 2mr$ with for example

$$10^{-1}n^{2/9} < r < 10n^{2/9}.$$

However, this is not a real restriction because, given n, the integer $n' = \lfloor n/2r \rfloor 2r$ with $r = \lfloor n^{2/9} \rfloor$ is of the required type and $n - 2r < n' \le n$. Completing the unimodular polynomial of degree n' to a unimodular polynomial $P(\theta)$ of degree n with a Gaussian phase k^2/r introduces an error of at most $O(\sqrt{r})$, which does not alter the conclusion of the theorem. □

Remark 23. The argument given here is optimal in the following sense. The choice $M \asymp N^{7/9}$, hence $\delta \asymp N^{-1/18}$, yields equality (up to powers $N^{o(1)}$) for the three terms δ^2, $\delta^{-1/2}N^{-1/4}M^{-1/2}$, $M^{1/2}N^{-1/2}$, as well as equality in the constraint (C2′). The major stumbling block for improving our arguments seems to lie in the constraint (C2′).

13. Explicit constructions, I

The Körner correction argument can be made constructive in the proof of Theorem 3 by noting that it is applied to polynomials with increasing or decreasing coefficients. In this case, the following simple remarks will show how to choose the sequence of signs (ω_m) explicitly without recurring to Khinchin's inequality. By "constructive" and "explicit" we mean that we can choose ω_m as a function of m of polynomial complexity, i.e. computable in $O((\log n)^C)$ steps for some constant C.

Proof of the statement in Remark 6 of Section 1. We start by recalling a well-known property of the Golay–Shapiro sequence (see [1] for a survey and additional references).

Let $\Omega_k^{\pm} = (\omega_m^{\pm})_{m=0,\dots,2^k-1}$ be two sequences defined inductively by

$$\Omega_0^{\pm} := 1, \quad \Omega_{k+1}^{\pm} := (\omega_m^{+})_{m=0,\dots,2^k-1} \cup (\pm\omega_{m-2^k}^{-})_{m=2^k,\dots,2^{k+1}-1}$$

so that Ω_∞^+ is the Golay–Shapiro sequence. An alternative definition is *via* $\omega_m^+ = (-1)^{u(m)}$ where $u(m)$ counts the occurrences of pairs 11 in the dyadic expansion of m. The associated Rudin–Shapiro exponential polynomials

$$P_k^{\pm}(\theta) = \sum_{m=0}^{2^k-1} \omega_m^{\pm} e(m\theta)$$

satisfy

$$|P_k^{+}(\theta)|^2 + |P_k^{-}(\theta)|^2 = 2^{k+1} \tag{13.1}$$

for every $\theta \in \mathbb{T}$, as one readily sees by induction on k. It is also true that for $\theta \in \mathbb{T}$ and $n \geq 1$ and an absolute constant C we have

$$\Big| \sum_{a \leq m < b} \omega_m^{+} e(m\theta) \Big| \leq C\sqrt{b-a}. \tag{13.2}$$

This is proved by recalling (13.1) and noting that for positive integers m and k we have

$$\Omega_\infty^{+}|_{[2^k m, 2^k(m+1))} = \pm\Omega_k^{\pm}$$

for suitable choices of signs $\pm$. Then applying a greedy algorithm, dividing the interval $[a, b)$ into pieces of length a power of 2, yields the result; see [21] for a refined treatment of this argument giving a good value for C. Now partial summation shows that if $c(m)$ is positive and increasing (or decreasing) in $[a, b]$ then

$$\Big| \sum_{a \leq m < b} \omega_m^{+} c(m) e(m\theta) \Big| \leq C\{\max_m c(m)\}\sqrt{b-a} \tag{13.3}$$

continues to hold.

In the proof of Theorem 3, we apply the Körner construction with

$$a_m = (-1)^m e\left(\frac{m^2}{2n}\right)\chi_\alpha\left(\frac{m}{n}\right)$$

to the ranges

$$0 \le m < n^{1/2}(\log n)^{3/2+\varepsilon}, \qquad 0 \le n - m < n^{1/2}(\log n)^{3/2+\varepsilon}.$$

Consider for example the range

$$I = [0, \lfloor n^{1/2}(\log n)^{3/2+\varepsilon}\rfloor],$$

the analysis for the other range being identical. We have

$$\arg(a_m) = -\pi m + \pi m^2/n \pmod{2\pi}.$$

We subdivide the interval I into $O((\log n)^{3+2\varepsilon})$ subintervals

$$I_h := I \cap [(hn)^{1/2}, ((h+1)n)^{1/2}];$$

then, with a little extra care in the choice of χ_α, we can ensure that both the real and imaginary parts of ia_m have constant sign and are monotonic on each subinterval I_h. Indeed, this is verified for our choice of χ_α in Section 3 provided n is large enough. Now we simply choose $\omega_m = (-1)^m\omega_m^+$. By (13.3) with $\theta + 1/2$ in place of θ, each subinterval will contribute an error term bounded by $O(h^{-1/4}n^{1/4})$. There are at most $O((\log n)^{3+2\varepsilon})$ subintervals to consider. Altogether, taking into account the fact that ε is arbitrarily small, this will give an explicit construction with the error term $O(n^{1/4}(\log n)^{9/4+\varepsilon})$. □

14. Explicit constructions, II

The problem of obtaining an ultraflat Kahane polynomial with an explicit construction is interesting and has been around for some time.

The first randomization discussed in Section 11 already requires a sequence (ω_m) such that cancellation occurs not only for the sequence (ω_m), but also for the sequence $(\omega_m\omega_{m+1})$. This is not automatic. For example, (13.2) does not hold for the sequence $(\omega_m^+\omega_{m+1}^+)$, because

$$\sum_{0\le m<2^k} \omega_m^+\omega_{m+1}^+ i^{m-1} = 2^{k-1}.$$

To see this, note that

$$\omega_{2m}^+\omega_{2m+1}^+ = (-1)^m, \qquad \omega_{2m+1}^+\omega_{2m+2}^+ = (-1)^m\omega_m^+\omega_{m+1}^+$$

for every m.

However, the cancellation in the sums $Z(k), \dots, Z'''(k)$ in (9.8) can still be obtained with other explicit sequences (ω_q), because the coefficients vary quite slowly with q (up to factors of type $e(q\theta)$). The next sections will deal with this task.

For the rest of this paper, δ is chosen so that (12.1) holds, namely

$$\delta \asymp M^{-1/5}N^{1/10}. \tag{12.1}$$

15. Explicit constructions, II: The coefficients $\widehat{P}_2(k)$ and $\widehat{P}_4(k)$

Our basic choice for derandomizing a Bernoulli sequence is a modification of the classical Jacobi symbol. We use the notation $p^\mu \parallel n$ to indicate that p^μ is the highest power of p dividing the integer n. We begin by setting, for p a prime,

$$\left[\frac{u}{p}\right] := \begin{cases} \left(\frac{u}{p}\right) & \text{if } (u,\, p) = 1, \\ 1 & \text{if } (u,\, p) = p, \end{cases}$$

and in general, for squarefree n, we set

$$\left[\frac{u}{n}\right] := \prod_{p|n} \left[\frac{u}{p}\right].$$

The symbol $\left[\frac{u}{n}\right]$ is periodic with period n.

Definition 24. *Let K be a positive integer. We say that an integer n is a K-*strong almost prime *if*

$$n \text{ has no prime factors } \le n^{1/(K+1)}. \tag{C(K)}$$

It is clear that the total number $\Omega(n)$ of prime factors of n, counted with their multiplicity, is at most K. Hence a sieve up to N which removes all prime divisors up to $N^{1/(K+1)}$ produces only K-strong almost primes.

Lemma 25. *Let $0 < \varepsilon < 1$ and a positive integer K be given. Let $\widehat{P}_2(k)$ be obtained by the same construction as in Section 9 but taking now*

$$\omega_q := \prod_{p^\mu \| t} \prod_{\lambda=0}^{\mu-1} \left[\frac{q_0(p) + \cdots + q_\lambda(p)}{p}\right] \tag{15.1}$$

where $q = \sum q_\lambda(p) p^\lambda$ is the expansion of q in base p, t is a K-strong almost prime, and $7Q_0 < t < 14Q_0$ (recall that $Q_0 = \lceil \tau_0 M\delta \rceil \sim N^{-1/2+\varepsilon_0} M\delta$). Then

$$\widehat{P}_2(k) \ll \delta^{-1/2} N^{-1/4+2\varepsilon} M^{-1/2}.$$

The same bound and construction also hold for $\widehat{P}_4(k)$.

We first need an auxiliary estimate.

Lemma 26. *Let ω_q be as in Lemma 25, let there be given $0 < \varepsilon < 1$ and a positive integer K, and suppose that t is a K-strong almost prime. Then*

$$\max_{1 \le Q_1 \le Q} \max_{\theta} \left| \sum_{1 \le q \le Q_1} \omega_q e(q\theta) \right| \ll Q^{1/2+2\varepsilon},$$

$$\max_{1 \le Q_1 \le Q} \max_{\theta} \left| \sum_{1 \le q \le Q_1} \omega_q \omega_{q+1} e(q\theta) \right| \ll Q^{1/2+2\varepsilon}.$$

Proof. By the same argument used at the beginning of the proof of Lemma 15, we see that it suffices to prove the lemma for the special values $\theta = a/t$. By a well-known method which goes back to Mordell, the estimate for an incomplete sum in the range $1 \le q \le Q_1$ is the same as for all (i.e. for all $\theta = a/t$) complete (i.e. over $1 \le q \le t$) sums, up to a factor $t^{o(1)}$ (which we may make explicit as a divisor function).

Consider first the sum

$$\sum_{q=1}^{t} \omega_q e\left(\frac{aq}{t}\right). \tag{15.2}$$

Let $t = \prod p^{\mu}$ and a be given. Then we can write uniquely

$$\frac{aq}{t} \equiv \sum_{p^{\mu} \| t} \sum_{h=1}^{\mu} p^{-\lambda} L_{h,p}(q_0(p), \dots, q_{\mu-1}(p)) \pmod 1$$

for certain linear forms $L_{\lambda,p} \pmod p$ determined by a, t, and p. Therefore, the sum in (15.2) splits as a product

$$\prod_{p^{\mu} \| t} \left\{ \sum_{q_0=0}^{p-1} \cdots \sum_{q_{\mu-1}=0}^{p-1} \prod_{\lambda=0}^{\mu-1} \left[\frac{q_0 + \cdots + q_{\lambda}}{p}\right] e\Big(\sum_{h=1}^{\mu} p^{-h} L_{h,p}(q_0, \dots, q_{\mu-1})\Big)\right\}. \tag{15.3}$$

We make a change of variables $(\bmod p)$ by setting $u_{\lambda} = q_0 + \cdots + q_{\lambda}$ in (15.3). This changes the linear forms $L_{h,p}$ into new linear forms $(\bmod p)$, in the variables u_{λ}, and we can further split (15.3) as

$$\prod_{p^{\mu} \| t} \prod_{\lambda=0}^{\mu-1} \left\{ \sum_{u_{\lambda}=0}^{p-1} \left[\frac{u_{\lambda}}{p}\right] e\Big(\sum_{h=1}^{\mu} p^{-h} A_{\lambda,h}(p) u_{\lambda}\Big)\right\}$$

for certain coefficients $A_{\lambda,h}(p) \pmod p$.

The sum for $h \ge 2$ in the exponential is bounded by 2 and does not oscillate, hence we can remove it at a cost of $O(\log p)$ for each factor. It follows that

$$\sum_{q=1}^{t} \omega_q e\left(\frac{aq}{t}\right) \ll t^{o(1)} \prod_{p^{\mu} \| t} \left\{ (C \log p)^{\mu} \prod_{\lambda=0}^{\mu-1} \left| \sum_{u_{\lambda}=0}^{p-1} \left[\frac{u_{\lambda}}{p}\right] e\left(\frac{a_{\lambda}(p) u_{\lambda}}{p}\right)\right|\right\}$$

for an absolute constant C and certain integers $a_{\lambda}(p)$.

The inner sum is 1 plus a Gauss sum, hence it is majorized by $1 + \sqrt{p}$. This gives the bound

$$\sum_{q=1}^{t} \omega_q e\left(\frac{aq}{t}\right) \ll t^{1/2+o(1)} \prod_{p^{\mu} \| t} (2C \log p)^{\mu}. \tag{15.4}$$

If t has no small prime factors, the product in (15.4) is negligible. More precisely, if t is a K-strong almost prime the product does not exceed $O((\log t)^K)$. This proves the desired bound for the first sum.

The proof of the similar result for the second sum follows the same lines and it is here that the actual choice of ω_q (rather than the simpler $\left[\frac{q}{t}\right]$) plays a role. We indicate the main changes to be made.

The factor $\omega_q\omega_{q+1}$ creates a complication because ω_{q+1} depends on the expansion of $q+1$ in base p and its relation to the corresponding expansion of q depends on the number, and location, of carries in the addition $q+1$. Let $q_0, q_1, \dots$ be the digits of $q = q_0 + q_1 p + \cdots$, and $v_0, v_1, \dots$ be the corresponding digits for $q+1$. Let *carry* denote the number of carries in the sum $q+1$ done in base p. Then

$$\begin{aligned} &q_0 = \cdots = q_{carry-1} = p-1, \qquad q_{carry} < p-1,\\ &v_0 = \cdots = v_{carry-1} = 0,\\ &v_{carry} = q_{carry} + 1,\\ &v_i = q_i \quad \text{if } i > carry. \end{aligned}$$

In this way, the digits $v_i(q)$ of $q+1$ are given explicitly as functions of the digits of q.

The same transformations as before lead us to estimate

$$\prod_{p^\mu \| t}\Bigg(\sum_{q_0=0}^{p-1}\cdots\sum_{q_{\mu-1}=0}^{p-1} \times \prod_{\lambda=0}^{\mu-1}\left[\frac{q_0+\cdots+q_\lambda}{p}\right]\left[\frac{v_0(q)+\cdots+v_\lambda(q)}{p}\right] e\Bigg(\sum_{h=1}^{\mu}\frac{L_{h,p}(q_0,\dots,q_{\mu-1})}{p^h}\Bigg)\Bigg). \tag{15.5}$$

Consider now the factor in (15.5) determined by the prime p. We make the change of variables $u_\lambda = q_0 + \cdots + q_\lambda$, $\lambda = 0, \dots, \mu-1$, and proceed as before. Then we have

$$v_0(q) + \cdots + v_\lambda(q) = \begin{cases} 0 \pmod p & \text{if } \lambda < carry,\\ u_\lambda + carry + 1 \pmod p & \text{if } \lambda \geq carry. \end{cases}$$

This decomposes the factor at p into a sum

$$\sum_{carry=0}^{\mu-1}\zeta_{carry}\prod_{\lambda=carry}^{\mu-1}\Bigg\{\sum_{u_\lambda=0}^{p-1}{}'\left[\frac{u_\lambda}{p}\right]\left[\frac{u_\lambda+carry+1}{p}\right]e\Bigg(\sum_{h=1}^{\mu}p^{-h}A_{\lambda,h}u_\lambda\Bigg)\Bigg\}$$

where the coefficients ζ_{carry} are roots of unity and $\sum'$ means that the variable u_{carry} omits the value $p - carry - 1 \pmod p$.

Again, we can remove the terms with $h \geq 2$ in the exponential at a cost of not more than $(C\log p)^\mu$. It remains to estimate a typical sum over u_i, namely

$$\sum_{u=0}^{p-1}\left[\frac{u}{p}\right]\left[\frac{u+carry+1}{p}\right]e\left(\frac{au}{p}\right)$$

(possibly with the term $u = p-1$ omitted) and our goal is to obtain a bound $O(\sqrt{p})$ for this sum.

If $carry + 1$ is not divisible by p the sum reduces to a Kloosterman sum or Jacobsthal sum, with a total bound $3 + 2\sqrt{p}$ using Weil's classical estimate. Thus taking the product over p we obtain the desired bound $O(t^{1/2}(\log n)^K)$.

If instead p divides $carry + 1$, if $a = 0$ we cannot do better than the trivial estimate $p^{\mu-p+1}$. However, this problem is avoided if $\mu < p$. Since we already imposed the condition than all prime factors of p are larger than $n^{1/(K+1)}$, we must have $\mu \le K$. This condition for μ is automatically satisfied if $p > K + 1$, hence for $n > (K+1)^{K+1}$. □

Proof of Lemma 25. Consider now the sums $Z(k)$, $Z'(k)$, $Z''(k) + Z'''(k)$. We write a typical sum Z as

$$Z = \sum_{q=1}^{Q-1} \phi_q \sum_{\Delta_q \le s < \Delta_{q+1}} r(k,s) f(s,q) = \sum_{j=0}^{\Delta-1} \sum_{q=1}^{Q-1} \phi_q r(k, \Delta_q + j) f(\Delta_q + j, q) \quad (15.6)$$

where, for every $q = 1, \dots, Q-1$, we have $\phi_q = \omega_q$, ω_{q+1}, or $\omega_q \omega_{q+1}$, and where $f(s,q)$ is one of the three functions

$$\begin{aligned} &\cos(2\pi\lambda'_s u_{\Delta_q}) \sin(2\pi\lambda_s u_{\Delta_q}), \qquad \sin(2\pi\lambda'_s u_{\Delta_q}) \cos(2\pi\lambda_s u_{\Delta_q}), \\ &\sin(2\pi\lambda'_s u_{\Delta_q}) \sin(2\pi\lambda_s u_{\Delta_q}), \end{aligned} \quad (15.7)$$

and estimate separately the contribution of the sums with a fixed j.

Clearly,

$$Z \ll \Delta \max_j \Big| \sum_{q=1}^{Q-1} \phi_q r(k, \Delta_q + j) f(\Delta_q + j, q) \Big|. \quad (15.8)$$

We have

$$r(k, \Delta_q + j) = e\left(q(N-k)\frac{\Delta}{M}\right) e\left((N-k)\frac{s_1 - \Delta + j}{M}\right) t(k, \Delta_q + j)$$

where we have written

$$t(k,s) = e\left(-\frac{N}{2}\left(\frac{s}{M}\right)^2\right) \psi(N - k + 2Rs);$$

note that

$$t(k,s) \ll 1/M. \quad (15.9)$$

For the rest of the argument we fix j so that the sum in (15.8) has maximum absolute value and write

$$x(q) := 2\pi\lambda_{\Delta_q + j} u_{\Delta_q}, \qquad y(q) := 2\pi\lambda'_{\Delta_q + j} u_{\Delta_q}, \qquad g(q) := f(\Delta_q + j, q).$$

Then

$$Z \ll \Delta \max_\theta \Big| \sum_{q=1}^{Q-1} \phi_q e(q\theta) t(k, \Delta_q + j) g(q) \Big|.$$

Let us write for simplicity

$$v(k,q) := t(k, \Delta_q + j)g(q).$$

Then by partial summation and Lemma 26 we find

$$Z \ll \Delta Q^{1/2+\varepsilon+o(1)}\Big\{|v(k, Q-1)| + \sum_{q=1}^{Q-2} |v(k,q) - v(k,q+1)|\Big\}.$$

We claim that

$$|v(k, Q-1)| + \sum_{q=1}^{Q-2} |v(k,q) - v(k,q+1)| \ll M^{-1}N^{2\varepsilon}. \tag{15.10}$$

Since $Q \ll \tau M/\Delta$ and Δ is of order $1/\delta$, this will show that

$$Z \ll \delta^{-1/2}M^{-1/2}N^{-1/4+5\varepsilon/2+o(1)},$$

which, up to an irrelevant extra factor $N^{3\varepsilon/2+o(1)}$, is the same as what was obtained in (9.9) by the randomization argument.

The term $|v(k, Q-1)|$ is $O(1/M)$ because of (15.9).

Also

$$|\psi(N-k+R(\Delta_q+j)) - \psi(N-k)| \ll R\Delta Q \max|\psi'| \ll \Delta Q M^{-3}N$$

and $\psi(x) \ll 1/M$. Thus we may replace $\psi(N-k+R(\Delta_q+j))$ by $\psi(N-k)$, which is independent of q, introducing an error term of order at most $\Delta Q^2 M^{-3}N \ll \Delta^{-1}M^{-1}N^{2\varepsilon}$.

In a similar way, we have

$$\left|e\left(-\frac{N}{2}\left(\frac{s+\Delta}{M}\right)^2\right) - e\left(-\frac{N}{2}\left(\frac{s}{M}\right)^2\right)\right| \ll NM^{-2}\Delta^2 Q$$

and this introduces an error term $O(M^{-1}N^{2\varepsilon})$.

We conclude that

$$\sum_{q=1}^{Q-2} |v(k,q) - v(k,q+1)| \ll M^{-1}N^{2\varepsilon} + \frac{1}{M}\sum_{q=1}^{Q-2} |g(q) - g(q+1)|. \tag{15.11}$$

Our next step consists in computing the pairs (λ_s, λ'_s) explicitly. Recall that for $\Delta_q \le s < \Delta_{q+1}$ the pairs (λ_s, λ'_s) were defined inductively by

$$\begin{aligned}
&(\lambda_{\Delta_q}, \lambda'_{\Delta_q}) = (1,0), \quad (\lambda_{\Delta_{q+1}-1}, \lambda'_{\Delta_{q+1}-1}) = (0,1),\\
&\cos(2\pi\lambda_s u_{\Delta_q})\cos(2\pi\lambda'_s u_{\Delta_q}) = \beta(\Delta_q/M),\\
&\lambda_s \ge \lambda_{s+1} \ge 0, \quad \lambda'_s \le \lambda'_{s+1} \le 1,
\end{aligned}$$

and λ_{s+1} being smallest with the above properties and

$$|\lambda_s - \lambda_{s+1}| + |\lambda'_{s+1} - \lambda'_s| \le \frac{\delta}{2\pi u_{\Delta_q}}.$$

Since λ_{s+1} was taken as small as possible, we must have

$$\lambda_{s+1} - \lambda'_{s+1} = \lambda_s - \lambda'_s - \frac{\delta}{2\pi u_{\Delta_q}}$$

unless we reach first $\lambda_{s+1} = 0$, which occurs precisely when

$$-1 > \lambda_s - \lambda'_s - \frac{\delta}{2\pi u_{\Delta_q}}.$$

Thus by induction we see that setting

$$j_q = \left\lceil \frac{4\pi u_{\Delta_q}}{\delta} \right\rceil = 4u_{\Delta_q}\Delta + O(1) \tag{15.12}$$

we have, after multiplication by $2\pi u_{\Delta_q}$,

$$x(q) - y(q) = \arccos(\beta(\Delta_q/M)) - \delta j \quad \text{if } j < j_q, \tag{15.13}$$

$$\cos(x(q))\cos(y(q)) = \beta(\Delta_q/M),$$

$$x(q) = 0 \quad \text{if } j_q \le j. \tag{15.14}$$

Since $\beta(x)$ is in our range an increasing function of x and since $\cos(2\pi u_{\Delta_q}) = \beta(\Delta_q/M)$ we see that u_{Δ_q} is a decreasing function of q, hence j_q is also a decreasing function of q. Moreover, we have verified in (9.5) that $|u_{\Delta_q} - u_{\Delta_{q+1}}| \ll \Delta/(\tau M)$ and it follows that

$$j_q - j_{q+1} \ll 1 + \Delta^2(\tau M)^{-1} \ll 1$$

by using condition (C11) in the last step. By the preceding formula, (15.13), (15.12), (15.14), and (15.11), we conclude that in order to prove our claim it suffices to prove the bound

$$\sum_{\substack{1\le q<Q-1\\ j<j_q}} |g(q) - g(q+1)| \ll N^{2\varepsilon}.$$

To prove this we show that $g(q)$ is a piecewise monotonic function of q, with the number of pieces bounded by an absolute constant. The result (with the more precise bound $O(1)$) then follows by telescoping the sums over the monotonicity intervals.

For simplicity, in the following argument we abbreviate x, y, β for $x(q)$, $y(q)$, and $\beta(\Delta_q/M)$, where $\Delta_q = s_1 + (q-1)\Delta$, considering them as continuous differentiable functions of q.

By our preceding discussion, we have either $g(q) = 0$ or $g(q) = \sqrt{1-\beta^2}$ in the interval $q_0 \le q \le Q_1$ where $j_q \le j$, and we have monotonicity there.

In the interval $q < q_0$ we eliminate y from (15.13) using $\cos(x)\cos(y) = \beta$, obtaining

$$x - \arccos\left(\frac{\beta}{\cos(x)}\right) - \arccos(\beta) = -\delta j.$$

We differentiate with respect to q, thus eliminating the constant term δj, obtaining an identity $Ax' + B\beta' = 0$ where A and B are algebraic functions in the arguments $\cos(x)$ and β alone.

Next, we eliminate y from $g(q)$ using the equation $\cos(x)\cos(y) = \beta$, differentiate with respect to q, and equate the result to 0 in order to obtain an equation for the end points of the intervals of monotonicity of $g(q)$ (except the beginning and end of the range of q). This equation is of type $Cx' + D\beta' = 0$ with C, D algebraic functions in the arguments $\cos(x)$ and β alone. Therefore, we have $AD - BC = 0$ with $AD - BC = F(\cos(x), \beta)$ with $F(X, Y)$ an algebraic function of X and Y with constant coefficients. Note also that $AD - BC$ is not identically 0. To see this point, we remark that $Ax' + B\beta' = 0$ identically in q. If $AD - BC$ were identically 0 then C, D would be proportional to A, B, and $g'(q) = Cx' + D\beta'$ would be identically 0, hence $g(q)$ would be constant, which certainly is not the case.

Let $\mathbb{C}(X, Y)$ be the field of rational functions in X, Y, with complex coefficients. Then $F := F(X, Y)$ satisfies a unique irreducible monic equation over $\mathbb{C}(X, Y)$, namely

$$F^d + a_1(X, Y)F^{d-1} + \cdots + a_d(X, Y) = 0$$

for certain rational functions $a_i \in \mathbb{C}(X, Y)$. Let $U(x, y)$ be a numerator for the rational function $a_d(X, Y)$. Then $U(X, Y)$ is not identically 0, and $U(\cos(x), \beta)$ vanishes whenever $AD - BC$ vanishes. Thus we have obtained a polynomial equation $U(\cos(x), \beta) = 0$, independent of δj, satisfied by $x(q)$ whenever $g'(q) = 0$.

On the other hand, the equation $x - y = \arccos(\beta) - \delta j$ yields

$$\begin{aligned}\cos(x) &= \cos(y + \arccos(\beta) - \delta j)\\ &= \cos(y)\left\{\beta\cos(\delta j) + \frac{1}{\sqrt{1-\beta^2}}\sin(\delta j)\right\}\\ &\quad - \sin(y)\left\{\frac{1}{\sqrt{1-\beta^2}}\cos(\delta j) - \beta\sin(\delta j)\right\}.\end{aligned}$$

Using once again the equation $\cos(x)\cos(y) = \beta$ to eliminate y, and proceeding in the same way as before, we obtain another polynomial equation

$$V(\cos(x), \beta, \cos(\delta j)) = 0$$

satisfied identically in q. Clearly, we may assume that $V(X, Y, \cos(\delta j))$ is irreducible as a polynomial in X, Y. Therefore, taking the resultant of $U(X, Y)$ and $V(X, Y, \cos(\delta j))$ with respect to X (this resultant certainly is not identically 0, because $U(X, Y)$ and $V(X, Y, \cos(\delta j))$ are both irreducible, hence $U(X, Y)$ cannot divide $V(X, Y, \cos(\delta j))$ without having $U(X, Y)$ proportional to $V(X, Y, \cos(\delta j))$, which is not the case) we obtain a non-trivial equation $W(\beta, \cos(\delta j)) = 0$ satisfied by $\beta = \beta(\Delta_q/M)$. In particular, β can take at most $\deg_\beta(W)$ values. Since β is monotonic in q, we have at most $\deg_\beta(W)$ values of q for which $g'(q) = 0$. □

16. Explicit constructions, II: The coefficients $\widehat{P}_3(k)$ and $\widehat{P}_5(k)$

We need a more precise analysis of the Fourier coefficients of the exponential polynomials $P_3(\theta)$ and $P_5(\theta)$.

Lemma 27. *Suppose the support of the auxiliary function χ in the proof of Lemma* 12 *is* $\mathrm{supp}(\chi) \subset [-1/4, 1/4]$. *Then there are μ, ν, independent of k, such that*

$$\widehat{P}_3(k) + \widehat{P}_5(k) = \frac{1}{\sqrt{LM}} e\left(-\frac{k^2}{2LM} + \mu k + \nu\right) U_1(k) + \frac{1}{M}\left\{e\left(-\frac{s_1}{M}k\right)U_2(k) + e\left(\frac{s_1}{M}k\right)U_3(k)\right\} \tag{16.1}$$

where

$$U_i(k) \ll 1 \quad \text{for } i = 1, 2, 3, \tag{16.2}$$

$$U_1'(k) \ll (LM)^{-1/2}, \quad U_i'(k) \ll M^{-1} \quad \text{for } i = 2, 3. \tag{16.3}$$

Moreover, if $2M \le k \le N - 2M$ then $U_1(k)$ is independent of k and also, for any fixed A,

$$U_i'(k) \ll N^{-A} \quad \text{for } i = 1, 2, 3.$$

Proof. We start with $\widehat{P}_3(k)$. Recall that

$$\widehat{P}_3(k) = (-1)^k \sum_{0 \le s < s_1} \psi(k - N_s) e\left(-k\frac{s}{M}\right) e\left(\frac{1}{M}\sum_{t=0}^{s-1} N_t\right)\zeta_s$$

with $N_s = RM + Ls$ and $L = \lfloor R\tau^{-1} \rfloor - 2R$. The coefficients ζ_s are subject to the conditions

$$\zeta_0 = 1, \quad |\zeta_s| = 1, \quad |\zeta_s - \zeta_{s+1}| < \delta \tag{C4$'$}$$

for $0 \le s < s_1$. By our choice of ω_q in Lemma 25, we have $\omega_1 = 1$. Also $(\lambda_{s_1}, \lambda'_{s_1}) = (1, 0)$, $\beta(s_1/M) = 0$, and it follows that $\zeta_{s_1} = i$.

Therefore, we choose

$$\zeta_s := e\left(\frac{s}{4s_1}\right) \quad \text{for } 0 \le s < s_1.$$

The Fourier coefficient $\widehat{P}_5(k)$ is obtained in the same way, upon replacing s by $M - s$ throughout (excluding $s = 0$). Hence

$$\widehat{P}_3(k) + \widehat{P}_5(k) = (-1)^k \sum_{-s_1 < s < s_1} \psi(k - RM - Ls) e\left(\frac{L}{M}\frac{s^2}{2} + \phi s\right)$$

where

$$\phi := \frac{1}{4s_1} - \frac{k}{M} + R - \frac{L}{2M}.$$

As usual, we transform the sum by Poisson summation and evaluate the resulting sum by stationary phase. Note, however, that the restriction of $\psi(k - RM - Lx)$ to the open interval $-s_1 < x < s_1$ need not have compact support, so some extra care is needed here.

We abbreviate

$$\Psi(x) := \psi(k - RM - Lx), \qquad \mathcal{L}(x) := \frac{L}{M}x + \phi.$$

Then Poisson summation yields

$$(-1)^k\{\widehat{P_3}(k) + \widehat{P_5}(k)\} = \lim_{H\to\infty} \sum_{|h|<H} \int_{-s_1}^{s_1} \Psi(x) e\left(\frac{L}{M}\frac{x^2}{2} + (\phi - h)x\right) dx$$
$$+ \frac{1}{2}\Psi(-s_1)e\left(\frac{L}{M}\frac{s_1^2}{2} - \phi s_1\right) - \frac{1}{2}\Psi(s_1)e\left(\frac{L}{M}\frac{s_1^2}{2} + \phi s_1\right). \qquad (16.4)$$

Since ψ now has support in $[-M/2, M/2]$, for fixed k the integral is restricted to the interval $I_k \cap [-s_1, s_1]$ where

$$I_k := \left[\frac{k - RM - M/2}{L}, \frac{k - RM + M/2}{L}\right].$$

Stationary phase may occur at the points $x = \xi_h$ with

$$\frac{L}{M}\xi_h + \phi - h = 0$$

and then

$$\psi(k - RM - L\xi_h) = \psi\left(\frac{M}{4s_1} - \frac{L}{2} - Mh\right).$$

If $h \neq -1, 0, 1$ the point

$$\frac{M}{4s_1} - \frac{L}{2} - Mh$$

is well away from the support of ψ, and thus there is no stationary phase. In this case it is convenient to integrate by parts repeatedly, taking the exponential as integrating factor. This yields the equation

$$\int_{-s_1}^{s_1} \Psi(x) e\left(\frac{L}{M}\frac{x^2}{2} + (\phi - h)x\right) dx$$
$$= \sum_{j=0}^{J} \frac{(-1)^j D_h^j \Psi(x)}{(2\pi i)^j(\mathcal{L}(x) - h)} e\left(\frac{L}{M}\frac{x^2}{2} + (\phi - h)x\right)\Big|_{-s_1}^{s_1}$$
$$+ \frac{(-1)^J}{(2\pi i)^J(\mathcal{L}(x) - h)} \int_{-s_1}^{s_1} (D_h^J \Psi(x)) e\left(\frac{L}{M}\frac{x^2}{2} + (\phi - h)x\right) dx \qquad (16.5)$$

where D_h is the differential operator

$$D_h F(x) = \frac{d}{dx}\{(\mathcal{L}(x) - h)^{-1} F(x)\}$$

and $D_0 F(x) = F(x)$. Now $D_h^j \Psi(x)$ is a linear combination

$$D_h^j \Psi(x) = \sum_{l=0}^{j} c_{j,l} (\mathcal{L}(x) - h)^{-j-l-1} L^j M^{-j-l} \psi^{(l)}(k - RM - Lx). \tag{16.6}$$

For $x \in I_k$ we have

$$\frac{L}{M} x \in \frac{k}{M} - R + \left[-\frac{1}{2}, \frac{1}{2}\right] \tag{16.7}$$

and, since $L/M = o(1)$, we also have from (16.7) the bound

$$|\mathcal{L}(x)| < 3/4, \quad |\mathcal{L}(x) - h| > |h|/5 \quad \text{for } |h| \geq 1.$$

Therefore, from (16.6) we obtain, for $|h| \geq 1$,

$$D_h^j \Psi(x) \ll |h|^{-j-1} L^j M^{-1-j}. \tag{16.8}$$

For $j = 0$ we need a more refined estimate obtained by grouping together terms with h and $-h$, namely

$$(\mathcal{L}(x) - h)^{-1} \Psi(x) + (\mathcal{L}(x) + h)^{-1} \Psi(x) = \frac{2\mathcal{L}(x)}{\mathcal{L}(x)^2 - h^2} \Psi(x) \ll |h|^{-2} M^{-1}. \tag{16.9}$$

Now using (16.5), (16.8), (16.9), we can evaluate the contribution to the Poisson summation formula in (16.4) due to the terms with $|h| \geq 1$ to be

$$\sum_{\pm} \lim_{H \to \infty} \sum_{h=1}^{H} \sum_{j=0}^{J} \frac{(-1)^j}{(2\pi i)^j} e\left(\frac{L}{M} \frac{s_1^2}{2} \pm \phi s_1\right) (D_h^j + D_{-h}^j) \Psi(\pm s_1) + O(N^{-A}) \tag{16.10}$$

because $e(hs_1) = 1$ and because the resulting series in h is absolutely convergent. A rather similar calculation holds for the derivative with respect to k of the coefficients of the exponentials $e(\pm k s_1/M)$.

This proves that the contribution to $(-1)^k\{\widehat{P^{(3)}}(k) + \widehat{P^{(5)}}(k)\}$ originating from the terms with $|h| \geq 1$ in the Poisson summation formula is indeed given by the second and third terms in formula (16.1), and that $U_2(k)$ and $U_3(k)$ satisfy (16.2) and (16.3).

If $h = 0$ the point

$$\xi_0 = -\frac{M}{L}\phi$$

is the point of stationary phase of the integrand. After making the change of variables $y + \xi_0 \leftarrow x$, the integral becomes

$$e\Big(-\frac{L}{2M}\xi_0^2\Big)\int_{-s_1-\xi_0}^{s_1-\xi_0}\psi\Big(\frac{M}{4s_1}-\frac{L}{2}-Ly\Big)e\Big(\frac{L}{2M}y^2\Big)\,dy = e\Big(-\frac{L}{2M}\xi_0^2\Big)(LM)^{-1/2}U_1(k). \qquad (16.11)$$

By a standard estimate the integral in (16.11) is $\ll (LM)^{-1/2}$, because $\psi \ll M^{-1}$ and $\psi' \ll M^{-2}$. Since

$$e\Big(-\frac{L}{2M}\xi_0^2\Big) = e\Big(-\frac{k^2}{2LM}+\mu k+\nu\Big)$$

with μ, ν independent of k, this proves that $U_1(k)$ satisfies (16.2).

We write for simplicity

$$U_1(k) := (LM)^{1/2}\int_{-s_1-\xi_0}^{s_1-\xi_0} G(y)\,dy$$

and note that by (16.11) the integrand $G(y)$ is independent of k. Thus differentiating with respect to k we see

$$U_1'(k) = -(LM)^{1/2}\{G(s_1-\xi_0)-G(-s_1-\xi_0)\}\frac{\partial\xi_0}{\partial k} \ll (LM)^{-1/2}.$$

This proves that $U_1'(k)$ satisfies (16.3).

Finally, if $2M \le k \le N-2M$ the interval I_k is contained in $[-s_1, s_1]$, hence the sum of boundary terms in the expression (16.10) vanishes identically, hence the contribution of (16.10) to Poisson summation is $O(N^{-A})$. By the same token, in this range we have

$$\int_{-s_1-\xi_0}^{s_1-\xi_0}\psi\Big(\frac{M}{4s_1}-\frac{L}{2}-Ly\Big)e\Big(\frac{L}{2M}y^2\Big)\,dy = \int_{\mathbb{R}}\psi\Big(\frac{M}{4s_1}-\frac{L}{2}-Ly\Big)e\Big(\frac{L}{2M}y^2\Big)\,dy,$$

which is independent of k. This proves the last clause of the lemma. □

17. Explicit constructions, II: The Körner correction, preliminary steps

We want a constructive version of the Körner correction of the Fourier coefficients of the exponential polynomial $P^{(1)}(\theta)$, as defined in Section 12, namely

$$P^{(1)}(\theta) := P_0(\theta) - MN^{-1+2\varepsilon}\sum_{k\in[2M,N-2M]}\widehat{P_1}(k)e(k\theta) - \delta^2 N^{4\varepsilon}\sum_{k\notin[2M,N-2M]}\widehat{P_1}(k)e(k\theta). \qquad (12.3)$$

The Körner costruction for a complex number z with $|z| < (N+2M)^{-1/2}$ consists in replacing z by

$$z^* := z + i\omega_k\frac{z}{|z|}\sqrt{\frac{1}{N+2M}-|z|^2}.$$

Writing for simplicity

$$\xi(z) := \frac{z}{|z|}\sqrt{\frac{1}{N+2M} - |z|^2}$$

our task consists in finding an explicit sequence (ω_k) such that the correction

$$\sum_{-M<k<N+M} \omega_k \xi(\widehat{P^{(1)}}(k)) e(k\theta)$$

introduced by the Körner construction is essentially as small as what can be obtained choosing ω_k by probabilistic methods.

The main difficulty in doing this lies in the structure of the function $\xi(z)$. If $|z|$ is small compared with $1/(N+2M)$ we can expand the square root in power series, leaving us to deal with complicated sums of type

$$\sum_k \omega_k \widehat{P^{(1)}}(k) |\widehat{P^{(1)}}(k)|^{2j-1} e(k\theta),$$

but if $|z|$ is close to $1/(N+2M)$ the situation is more delicate.

Thus our first task is to simplify as much as possible the Fourier coefficients of $P^{(1)}(\theta)$.

There are seven different ranges for k to consider, namely the intervals

$$[-M, \tau N], \quad [\tau N, 2\tau N], \quad [2\tau N, 2M], \quad [2M, N-2M],$$
$$[N-2M, N-2\tau N], \quad [N-2\tau N, N-\tau N], \quad [N-\tau N, N+M].$$

Lemma 28. *Define*

$$P^{(2)}(\theta) = P^{(1)}(\theta) - \sum_{\tau N \le k < 2\tau N} \{\widehat{P}_4(k) + \widehat{P}_3(k) + \widehat{P}_5(k)\} e(k\theta)$$
$$- \sum_{N-2\tau N < k \le N-\tau N} \{\widehat{P}_2(k) + \widehat{P}_3(k) + \widehat{P}_5(k)\} e(k\theta).$$

Then

$$|P^{(2)}(\theta)| = 1 + O(M^{-2/5} N^{1/5+5\varepsilon}) + O(MN^{-1+2\varepsilon}), \tag{17.1}$$

$$\widehat{P^{(2)}}(k) = (1-\delta^2 N^{4\varepsilon})\widehat{P}_1(k) \quad \text{if } k \in [\tau N, 2\tau N) \cup (N-2\tau N, N-\tau N], \tag{17.2}$$

$$\widehat{P^{(2)}}(k) = \widehat{P^{(1)}}(k) \quad \text{otherwise}. \tag{17.3}$$

Proof. Equations (17.2) and (17.3) are obvious from the definition.

For $k \in [\tau N, 2\tau N]$ the Fourier coefficients of $P^{(1)}(\theta)$ are given by

$$\widehat{P^{(1)}}(k) = (1-\delta^2 N^{4\varepsilon})\widehat{P}_1(k) + \widehat{P}_4(k) + \widehat{P}_3(k) + \widehat{P}_5(k).$$

For $k \in [N - 2\tau N, N - \tau N]$ the same formula holds with $\widehat{P_4}(k)$ replaced by $\widehat{P_2}(k)$. We have

$$\sum_{\tau N<k<2\tau N} \{\widehat{P_3}(k) + \widehat{P_5}(k)\} e(k\theta) \ll MN^{-3/2+\varepsilon}\tau N \ll MN^{-1+2\varepsilon},$$

hence we can remove these terms from $P^{(1)}(\theta)$ without affecting its absolute value in a significant way. The same occurs with

$$\sum_{\tau N<k<2\tau N} \widehat{P_4}(k) e(k\theta) \ll M^{-2/5}N^{1/5+2\varepsilon} = \delta^2 N^{2\varepsilon}.$$

This proves (17.1). □

Lemma 29. *Let*

$$\omega_k = \left[\frac{k}{p_1}\right]$$

where p_1 is a prime number, $2\tau N < p_1 < 4\tau N$. Then the Körner correction of $P^{(2)}(\theta)$ in the ranges $k \in [\tau N, 2\tau N]$ and $k \in [N - 2\tau N, N - \tau N]$ is

$$\Big(\sum_{\tau N\le k<2\tau N} + \sum_{N-2\tau N\le k<N-\tau N}\Big)\omega_k \xi(\widehat{P^{(2)}}(k)) e(k\theta) \ll N^{-1/4+2\varepsilon}.$$

Proof. By symmetry, it suffices to prove the lemma only in the range $[\tau N, 2\tau N]$. By Lemma 14 (7.2), and (7.13), we have

$$\widehat{P_1}(k) = e\left(\Omega - \frac{1}{8} + \frac{k^2}{2N} - \frac{k}{2}\right) N^{-1/2} c(k) + O(M^{-2}N^{1/2}),$$
$$c(k) = \sum_{j=0}^{J-1} \frac{1}{j!(4\pi i N))^j} \beta^{(2j)}\left(1 - \frac{k}{N}\right), \tag{17.4}$$

with β a smooth function subject only to the natural conditions stated at the beginning of Section 5. The error term $O(M^{-2}N^{1/2})$ is negligible, because $M^{-2}N^{1/2} \ll N^{-1}$. Moreover, the exponential $e(k^2/(2N))$ is slowly oscillating over intervals of length $O(\sqrt{N})$, and we can cover the interval $[\tau N, 2\tau N]$ with not more than $O(N^{\varepsilon})$ such subintervals. Now

$$\xi(\widehat{P^{(2)}}(k)) := i\frac{\widehat{P_1}(k)}{|\widehat{P_1}(k)|}\sqrt{\frac{1}{N+2M} - (1-\delta^2 N^{4\varepsilon})^2 |\widehat{P_1}(k)|^2}$$
$$= ie\left(\Omega - \frac{1}{8} + \frac{k^2}{2N} - \frac{k}{2} + \arg(c(k))\right)\sqrt{\frac{1}{N+2M} - \frac{1}{N}(1-\delta^2 N^{4\varepsilon})^2 |c(k)|^2} + O(N^{-1})$$

and $c(k)$ is a nice function given by (17.4). By a careful choice of the function β, it follows that

$$\xi(\widehat{P^{(2)}}(k)) = \frac{1}{\sqrt{N}} e\left(-\frac{k}{2}\right) u(k) + O(N^{-1})$$

where $u(k)$ is bounded, with real and imaginary parts expressible as sums of a bounded number of functions of k, monotonic over $O(N^{\varepsilon})$ subintervals covering $[\tau N, 2\tau N]$. Thus the error introduced by the Körner correction is

$$\ll N^{\varepsilon-1/2} \max_I \max_\theta \left| \sum_{k\in I} \left(\frac{k}{p_1}\right) e(k\theta) \right|$$

where I ranges over all subintervals of $[\tau N, 2\tau N]$. This is $O(N^{\varepsilon-1/2}\sqrt{\tau N}\log N)$, hence $O(N^{-1/4+2\varepsilon})$, which amply suffices for our purposes. □

In the ranges $k \in [-M, \tau N]$ and $k \in [N - \tau N, N + M]$ the amplitude of the Fourier coefficients of $P^{(1)}(\theta)$ is not well controlled and in order to compute the effect of the Körner correction we need to modify first these Fourier coefficients, by adding a term with a larger amplitude and controlled phase.

Lemma 30. *Let p_1 be a prime with $2M < p_1 < 4M$, and define*

$$\begin{aligned}
\omega_k &:= \left[\frac{k}{p_1}\right], \\
P_6(\theta) &:= \frac{N^{-\varepsilon}}{\sqrt{N+2M}} \sum_{-M<m<\tau N} e\left(\frac{m^2}{p_1}\right) e(m\theta), \\
P_7(\theta) &:= \frac{N^{-\varepsilon}}{\sqrt{N+2M}} \sum_{N-\tau N<m<N+M} e\left(\frac{m^2}{p_1}\right) e(m\theta), \\
P^{(3)}(\theta) &:= P^{(2)}(\theta) + P_6(\theta) + P_7(\theta).
\end{aligned}$$

Then

$$\begin{aligned}
|P^{(3)}(\theta)| &= 1 + O(N^{1/5+4\varepsilon}M^{-2/5}) + O(N^{-1/2}M^{1/2}), \\
\widehat{P^{(3)}}(k) &= \widehat{P^{(2)}}(k) \quad for\ \ k \in [\tau N, N - \tau N].
\end{aligned}$$

The Körner correction of $P^{(3)}(\theta)$ in the range $k \notin [\tau N, N - \tau N]$ is

$$\sum_{k\notin[\tau N, N-\tau N]} \omega_k \xi(\widehat{P^{(3)}}(k)) e(k\theta) \ll M^{1/2}N^{-1/2+C\varepsilon}$$

where C is an absolute constant.

Proof. Again by symmetry it suffices to consider the range $k \in [-M, \tau N]$. By Lemma 20 with $\alpha = 1/p_1$ we have

$$|P_6(\theta)| + |P_7(\theta)| \ll M^{1/2}N^{-1/2}.$$

In the range $[-M, \tau N]$ we have $\widehat{P_1}(k) = 0$, hence

$$\widehat{P^{(3)}}(k) = \widehat{P_6}(k) + \widehat{P_4}(k) + \widehat{P_3}(k) + \widehat{P_5}(k).$$

We abbreviate

$$Q(k) := \widehat{P}_6(k)^{-1}(\widehat{P}_4(k) + \widehat{P}_3(k) + \widehat{P}_5(k)).$$

Using $\widehat{P}_6(k) = N^{-\varepsilon}/\sqrt{N+2M}$, Lemma 25 for estimating $\widehat{P}_4(k)$, and Lemma 27 for estimating $\widehat{P}_3(k) + \widehat{P}_5(k)$, we verify that $Q(k) \ll N^{-\eta}$ for some fixed $\eta > 0$ (with our final choice for M, we get $\eta = 1/9$).

A quick calculation by expanding the square root shows that the Körner correction is

$$\begin{aligned}\xi(\widehat{P^{(3)}}(k)) &:= ie\left(\frac{k^2}{p_1}\right)\frac{1+Q(k)}{|1+Q(k)|}\sqrt{\frac{1}{N+2M} - \frac{N^{-2\varepsilon}}{N+2M}|1+Q(k)|^2} \\ &= i\,\frac{e(k^2/p_1)}{\sqrt{N+2M}}\sum_{j=0}^{\infty}(-1)^j\binom{\frac{1}{2}}{j}N^{-2j\varepsilon}(1+Q(k))^{j+1/2}(1+\overline{Q(k)})^{j-1/2}\end{aligned}$$

and we need to show that

$$\sum_{-M<k<\tau N}\omega_k\xi(k)e(k\theta)$$

is small. Clearly, by expanding $(1+Q(k))^{j\pm1/2}$ in power series we see that it suffices to bound

$$\frac{1}{\sqrt{N}}\sum_{-M<k<\tau N}\omega_k e\left(\frac{k^2}{p_1}\right)Q(k)^h\overline{Q(k)}^l e(k\theta) \tag{17.5}$$

for all non-negative integers h and l up to a sufficiently large bound, for example $2/\eta$.

By expanding $Q(k)^j$ and $\overline{Q(k)}^l$, this is the same as estimating the sums

$$\frac{N^{(h+l)(1/2+\varepsilon)}}{\sqrt{N}}\sum_{-M<k<\tau N}\omega_k e\left((l-h+1)\frac{k^2}{p_1}\right)U(k)^a V(k)^{h-a}\overline{U(k)}^b\overline{V(k)}^{l-b}e(k\theta),$$

where we have written for simplicity

$$U(k) := \widehat{P}_4(k), \quad V(k) := \widehat{P}_3(k) + \widehat{P}_5(k),$$

for $0 \le a \le h$, $0 \le b \le l$. Now recall that

$$U(k) = \sum_{M-2s_1<s\le M-s_1}\psi(k-N_s)e(-k\theta_s)\left(\zeta_s - \beta\left(\frac{s}{M}\right)\right)e\left(\frac{1}{M}\sum_{t=0}^{s-1}N_t\right)$$

and similarly

$$V(k) = \Big\{\sum_{0\le s<s_1} + \sum_{M-s_1<s<M}\Big\}\psi(k-N_s)e(-k\theta_s)\zeta_s e\left(\frac{1}{M}\sum_{t=0}^{s-1}N_t\right).$$

It follows that a typical sum in (17.5) is the sum of not more than s_1^{h+l} sums of type

$$\frac{N^{(h+l)(1/2+\varepsilon)}}{\sqrt{N}}g(t_1,\dots,t_{h+l})\sum_{-M<k\le\tau N}\Big\{\prod_{j=1}^{h+l}\psi(k-N_{t_j})\Big\}\omega_k e\left((l-h+1)\frac{k^2}{p_1}+k\theta'\right)$$

with $g(t_1, \dots, t_{h+l}) = O(2^{h+l})$ independent of k and θ' a suitable translation of the θ in (17.5).

By the Weil estimate for (now incomplete) mixed exponential sums in one variable (note that τN is small with respect to M, and M has the same order as p_1), we get

$$\sum_{-M<k\le\tau N} \Big\{\prod_{j=1}^{h+l} \psi(k - N_{t_j})\Big\}\Big(\frac{k}{p_1}\Big) e\Big((l-h+1)\frac{k^2}{p_1} + k\theta'\Big) \ll M^{-h-l+1/2} \log N.$$

(Here θ' was arbitrary, but the same argument used to prove (8.1) shows that it suffices to deal with $\theta' = a/p_1$.)

Therefore, a typical sum in (17.5) is bounded (not uniformly in h, l) by

$$O(s_1^{h+l} N^{(h+l)(1/2+\varepsilon)-1/2} M^{-h-l+1/2} \log N) = O(M^{1/2} N^{-1/2+2(h+l)\varepsilon} \log N),$$

because $s_1 = \tau M \le M N^{-1/2+\varepsilon}$. Since $h + l$ is bounded independently of ε, we get once more an estimate $O(M^{1/2} N^{-1/2+C\varepsilon})$, for some absolute constant C, for the Körner correction in the range $k \in [-M, \tau N]$ and, by the same proof, in the range $k \in [N - \tau N, N + M]$. □

18. Explicit constructions, II: The Körner correction in the range $[2M, N - 2M]$

In this section we obtain a good bound for the Körner correction of $P^{(3)}(\theta)$. We will prove

Lemma 31. *Let K be a positive integer. Suppose that*

$$N = 2m^2 r^2, \quad n := mr, \quad M = m^2, \quad R = r^2, \tag{C13}$$

$$n \text{ is squarefree.} \tag{C14}$$

Write uniquely, for $k \in [2M, N - 2M]$, $k = 2nu + v$ with $0 \le v < 2n$ and set

$$\omega_k := \Big[\frac{v}{n}\Big]. \tag{18.1}$$

Then the Körner correction of $P^{(3)}(\theta)$ in the range $2M < k < N - 2M$ is

$$\sum_{2M<k<N-2M} \omega_k \xi(\widehat{P^{(3)}}(k)) e(k\theta) \ll M^{1/2} N^{-1/2+4\varepsilon}.$$

Proof. If $k \in [2M, N - 2M]$ we have

$$\widehat{P^{(3)}}(k) = \widehat{P^{(1)}}(k) = (1 - MN^{-1+2\varepsilon})\widehat{P}_1(k) + \widehat{P}_3(k) + \widehat{P}_5(k).$$

By Lemmas 14 and 27, in the given range of k we have

$$\widehat{P^{(1)}}(k) = \frac{K_1}{\sqrt{N}} e\Big(\frac{k^2}{2N} + \mu' k + \nu'\Big) + \frac{K_2}{\sqrt{LM}} e\Big(-\frac{k^2}{2LM} + \mu k + \nu\Big) + O(N^{-A})$$

where

$$K_1 := (1 - MN^{-1+2\varepsilon})(1+\kappa_1), \qquad K_2 := (1 - MN^{-1+2\varepsilon})\kappa_2,$$

A is arbitrarily large, κ_1 and κ_2 are independent of k, and

$$\kappa_1 \ll M^{-2}N, \qquad \kappa_2 \ll 1.$$

In view of the above, writing for simplicity

$$K_3 := K_2 K_1^{-1}\sqrt{\frac{N}{LM}}, \qquad u(k) := \frac{1}{2N}k^2 + \mu' k + \nu', \qquad v(k) := -\frac{1}{2LM}k^2 + \mu k + \nu$$

for suitable $\mu, \mu' \nu, \nu'$, independent of k, and noting that $K_3 \ll \sqrt{N/(LM)} \ll N^{-1/4+\varepsilon/2}$, we infer that

$$\begin{aligned}\frac{\widehat{P^{(3)}}(k)}{|\widehat{P^{(3)}}(k)|} &= e(u(k))\frac{1 + K_3 e(v(k) - u(k))}{|1 + K_3 e(v(k) - u(k))|} + O(N^{-A+1/2}) \\ &= e(u(k)) \sum_{j=-J}^{J} c_j e(ju(k) - jv(k)) + O(N^{-A+1/2}) \qquad (18.2)\end{aligned}$$

for certain numerical coefficients c_j, independent of k, such that

$$c_j \ll N^{-(1/4-\varepsilon/2)|j|}$$

provided we take J sufficiently large as a function of A.

A similar calculation yields

$$\begin{aligned}\sqrt{\frac{1}{N+2M} - |\widehat{P^{(3)}}(k)|^2} &= \sqrt{\frac{1}{N+2M} - \frac{|K_1|^2}{N}|1 + K_3 e(v(k) - u(k))|^2} \\ &= M^{1/2}N^{-1+\varepsilon} \sum_{j=-J}^{J} d_j e(ju(k) - jv(k)) + O(N^{-A+1/2}) \qquad (18.3)\end{aligned}$$

for certain coefficients d_j, independent of k, such that

$$d_j \ll (M^{-1}N^{3/4-3\varepsilon/2})^{|j|}$$

provided we take J sufficiently large as a function of A.

Multiplying together (18.2) and (18.3) we find that the Körner correction has an asymptotic expansion

$$M^{1/2}N^{-1+\varepsilon} \sum_{j=-2J}^{2J} f_j e((j+1)u(k) - jv(k)) + O(N^{-A})$$

where the coefficients f_j are independent of k and

$$f_j \ll (M^{-1}N^{3/4-3\varepsilon/2})^{|j|}. \qquad (18.4)$$

We need to show that with the hypotheses of the lemma the sums

$$M^{1/2}N^{-1+\varepsilon}(M^{-1}N^{3/4-3\varepsilon/2})^{|j|}\sum_{2M<k<N-2M}\omega_k e((j+1)u(k)-jv(k))e(k\theta)$$

are small for $|j|\le 2J$, uniformly in θ. Since we may absorb the linear part of $(j+1)u(k)-jv(k)$ into the factor $e(k\theta)$, we need good bounds for

$$S_j:=\sum_{2M<k<N-2M}\omega_k e\bigg(\bigg(\frac{j+1}{2N}+\frac{j}{2LM}\bigg)k^2\bigg)e(k\theta) \tag{18.5}$$

for $|j|\le 2J$.

We write uniquely $k=2nu+v$, $0\le v<2n$, hence the range for u and v is given by

$$0\le v<2n,\qquad u\in I_v:=\bigg[\frac{2M-v}{2n},n-\frac{2M+v}{2n}\bigg].$$

Note that since $v<2n$ we can partition the interval for v into not more than four subintervals, in each of which I_v is independent of v.

We recall that our choice of ω_k is

$$\omega_k=\bigg[\frac{v}{n}\bigg]. \tag{18.1}$$

By (18.5), our problem becomes that of estimating

$$S_j:=\sum_{u\in I_1}\sum_{v\in I_2}\bigg[\frac{v}{n}\bigg]e\bigg(\frac{j+1}{n}uv+\frac{2jr^2}{L}u^2+g(u,v)\bigg)e(u\theta_1+v\theta_2) \tag{18.6}$$

where we have abbreviated

$$g(u,v):=\frac{j+1}{4n^2}v^2+\frac{2jn}{LM}uv+\frac{j}{2LM}v^2 \tag{18.7}$$

and where I_1 and I_2 are certain subintervals of $[0,n]$, $[0,2n]$.

Now $g(u,v)$ is a slowly oscillating function of u, v, because $L\asymp r^2n^{1-2\varepsilon}$. Also replacing θ_1 and θ_2 with close rational approximations h/n and l/n introduces only slowly oscillating corrections. Therefore, dividing the interval for v into $O(n^{2\varepsilon})$ subintervals of length not more than $cn^{1-2\varepsilon}$, with c a small constant, and using a double partial summation argument in the variables u, v, we infer that

$$S_j\ll n^{2\varepsilon}\max_{h,l,\mathcal{R}}\bigg|\sum_{(u,v)\in\mathcal{R}}\prod_{p|n}\bigg[\frac{v}{p}\bigg]e\bigg(\frac{j+1}{n}uv+\frac{2jr^2}{L}u^2+\frac{h}{n}u+\frac{l}{n}v\bigg)\bigg|$$

with $\mathcal{R}$ ranging over subrectangles of $[0,n]\times[0,n]$ with sides parallel to the (u,v) axes.

Now, by choosing L carefully in an appropriate range, we prove the key estimate

$$S_j\ll n^{1+5\varepsilon}.$$

Then, by applying this bound to (18.7) and to the expression in (18.4), we infer that the error introduced by this explicit Körner correction is bounded as

$$\ll M^{1/2}N^{-1+\varepsilon}n^{1+5\varepsilon} \ll N^{3\varepsilon}\sqrt{M/N}.$$

A difficulty in estimating the sum S_j is due to the fact that the sum has a natural period n associated with the exponential $e((j+1)uv/n)$, while the exponential $e(2jr^2u^2/L)$ has a period L which *a priori* may not be in resonance with n. Thus it turns out that it is necessary to adjust L so that r^2/L is in resonance with the frequency $1/n$.

We have a simple lemma.

Lemma 32. *Suppose that $r > n^\rho$ for a fixed ρ with $0 < \rho < 1$ and let ε_0 be a fixed positive number with $0 < \varepsilon_0 < \rho/3$. Then there are ε with*

$$\varepsilon_0 - \frac{\log 2}{\log n} \le \varepsilon \le \varepsilon_0$$

and a positive integer a with $(a,n) = 1$, $a \sim n^{2\varepsilon_0}$, such that $2r^2/L$ admits a rational approximation

$$\left|\frac{2r^2}{L} - \frac{a}{n}\right| < \frac{1}{n^2}.$$

Proof. Note that since $L = \lfloor R/\tau \rfloor - 2R$ we have

$$L = \lfloor 2^{1/2-\varepsilon} r^2 n^{1-2\varepsilon} \rfloor - 2r^2.$$

If we keep r, m, and $n = rm$ fixed and ε in $[\varepsilon_0 - \log 2/\log n, \varepsilon_0]$, the quantity L will run over a set of integers covering the interval $[L_0, 4L_0]$, where

$$L_0 = \lfloor 2^{1/2-\varepsilon_0} r^2 n^{1-2\varepsilon_0} \rfloor - 2r^2 \sim 2^{1/2-\varepsilon_0} r^2 n^{1-2\varepsilon_0}.$$

By clearing denominators, it suffices to find L and a, with $L \in [L_0, 4L_0]$ and $(a,n) = 1$, such that

$$|2r^2 n - aL| < L_0 n^{-1}.$$

Fix a number a coprime with n such that $a \sim 2^{-1} n^{2\varepsilon_0}$. Then the interval

$$[2r^2 n - L_0 n^{-1} + a, 2r^2 n + L_0 n^{-1} - a]$$

contains a number aL divisible by a, because for large n,

$$2L_0 n^{-1} \sim 2^{3/2-\varepsilon_0} r^2 n^{-2\varepsilon_0} > 2n^{2\rho-2\varepsilon_0} > n^{4\varepsilon_0} > 4a.$$

By the choice of a, we have $L \sim 2r^2 n^{1-2\varepsilon_0}$ hence there is ε, within $\log 2/\log n$ of ε_0, yielding the number L with the desired property. □

For the rest of this section, we assume that ε is chosen so that the conclusion of Lemma 32 holds. By the preceding lemma, the exponential $e((r^2/L - a/n)u^2)$ is slowly oscillating. By dividing the interval for u into $O(n^{2\varepsilon})$ shorter intervals of length not more than $cn^{1-2\varepsilon}$,

with c a small constant, we can remove this factor in the exponential sum S_j, at a cost of an extra factor $n^{2\varepsilon}$. This gives

$$S_j \ll n^{4\varepsilon} \max_{h,l,\mathcal{R}} \left| \sum_{(u,v)\in\mathcal{R}} \left[\frac{v}{n}\right] e\left(\frac{j+1}{n}uv + \frac{2ja}{n}u^2 + \frac{h}{n}u + \frac{l}{n}v\right)\right|.$$

As in the proof of Lemma 26, we complete the sum to a sum mod n, at a cost of $O((\log n)^2)$. Since n is squarefree, the complete sum splits into a product over $p|n$ of factors (up to a multiplier ± 1) of type (we denote by $\overline{x}$ the multiplicative inverse of $x \pmod p$)

$$\sum_{u=0}^{p-1}\sum_{v=0}^{p-1}\left[\frac{v}{p}\right] e\left(\frac{j+1}{p}uv + \frac{2ja\,\overline{n/p}}{p}u^2 + \frac{h}{p}u + \frac{l}{p}v\right). \tag{18.8}$$

Our task is to estimate the sum in (18.8) obtaining a square root cancellation.

If $p = 2$ the sum does not exceed 4. Now suppose p is odd.

We perform first the summation over v. If $j \neq -1$ and $(j+1)u + l \neq 0$, we have a Gauss sum except for an additional contribution of 1 due to the term with $v = 0$. Thus the summation over v yields

$$\left(1 + \left(\frac{(j+1)u+l}{p}\right)\eta\sqrt{p}\right) e\left(\frac{2ja\,\overline{n/p}}{p}u^2 + \frac{h}{p}u\right)$$

with $\eta = 1$ or $\eta = i$ according as $p \equiv 1$ or $3 \pmod 4$. If $j \neq -1$ and $(j+1)u+l = 0$, then u is uniquely determined and we have a contribution of p in absolute value. Therefore, summing over u we get in the case $j \neq -1$ the bound

$$\left|\sum_{u=0}^{p-1} e\left(\frac{2ja\,\overline{n/p}}{p}u^2 + \frac{h}{p}u\right)\right| + \sqrt{p}\left|\sum_{u=0}^{p-1}\left(\frac{(j+1)u+l}{p}\right) e\left(\frac{2ja\,\overline{n/p}}{p}u^2 + \frac{h}{p}u\right)\right| \le 4p$$

by the standard Weil estimate for mixed exponential sums in one variable.

If $j = -1$ and $l \neq 0$, the sum over v is is again a Gauss sum, independent of u, except for an additional contribution of 1 due to the term with $v = 0$. Then summation over u yields the bound

$$(1 + \sqrt{p})(2\sqrt{p}) < 4p.$$

If instead $j = -1$ and $l = 0$, summing over v yields the bound 1 and summation over u gives the bound $2\sqrt{p}$.

We have shown that the sum in (18.8) does not exceed $4p$ in absolute value. Hence

$$|S_j| \ll n^{4\varepsilon}(\log n)^2 \prod_{p|n}(4p) \ll n^{1+5\varepsilon},$$

concluding the proof. □

19. Explicit constructions, II: The correction in the ranges $k \in [2\tau N, 2M]$ and $k \in [N - 2M, N - 2\tau N]$. First step

This is the most delicate range and we will need to break up the analysis of the associated sum into this and the next four sections. The main difficulty is due to the fact that this time all polynomials $P_2, \dots, P_5$ enter the picture and we can only reduce everything to a sum mod t.

We deal with the range $[N - 2M, N - 2\tau N]$, the proof in the complementary range being the same by symmetry.

If $k \in [N - 2M, N - 2\tau N]$ we have

$$\begin{aligned}\widehat{P^{(3)}}(k) &= (1 - \delta^2 N^{4\varepsilon})\widehat{P}_1(k) + \widehat{P}_2(k) + \widehat{P}_3(k) + \widehat{P}_5(k)\\ &= (1 - \delta^2 N^{4\varepsilon})(1 + \kappa_1)\widehat{P}_1(k)(1 + S)\end{aligned} \tag{19.1}$$

with

$$S = (1 - \delta^2 N^{4\varepsilon})^{-1}(1 + \kappa_1)^{-1}\widehat{P}_1(k)^{-1}\{\widehat{P}_2(k) + \widehat{P}_3(k) + \widehat{P}_5(k)\}. \tag{19.2}$$

By Lemma 14 the main component of $\widehat{P^{(3)}}(k)$ is

$$(1 - \delta^2 N^{4\varepsilon})\widehat{P}_1(k) = e\left(\Omega - \frac{1}{8} + \frac{k^2}{2N} - \frac{k}{2}\right)N^{-1/2}(1 - \delta^2 N^{4\varepsilon})(1 + \kappa_1) + O(N^{-A})$$

with $A = 2\varepsilon J - 1$ and

$$\kappa_1 = M\sum_{j=1}^{J}\frac{N^j}{j!(4\pi i)^j}\psi^{(2j)}(0) = O(M^{-2}N)$$

independent of k; the other components are of lower order because by (12.1), (12.2), and Lemmas 18 and 19,

$$\begin{aligned}\widehat{P}_2(k) &\ll \delta^{-1/2}M^{-1/2}N^{-1/4+\varepsilon} \ll \delta^2 N^{-1/2+2\varepsilon},\\ \widehat{P}_3(k) &\ll MN^{-3/2+\varepsilon} \ll \delta^2 N^{-1/2+\varepsilon},\\ \widehat{P}_5(k) &\ll MN^{-3/2+\varepsilon} \ll \delta^2 N^{-1/2+\varepsilon},\end{aligned}$$

hence

$$S \ll \delta^2 N^{2\varepsilon}. \tag{19.3}$$

From (19.1), Lemma 14, and (7.1), we infer that in the Körner construction

$$\begin{aligned}&\xi(\widehat{P^{(3)}}(k))\\ &\quad= i\frac{\widehat{P}_1(k)}{|\widehat{P}_1(k)|}\left(\frac{1+S}{1+\overline{S}}\right)^{1/2}\left\{\frac{1}{N+2M} - \left|\frac{1-\delta^2N^{4\varepsilon}}{\sqrt{N}}(1+\kappa_1)\right|^2(1+S)(1+\overline{S})\right\}^{1/2}\\ &\quad= iK_4\delta\frac{e(k^2/(2N)+\mu k+\nu)}{\sqrt{N}}\left(\frac{1+S}{1+\overline{S}}\right)^{1/2}\{1 - K_5\delta^{-2}N^{-4\varepsilon}(S+\overline{S}+S\overline{S})\}^{1/2}\\ &\qquad+ O(M^{-2}N^{1/2})\end{aligned}$$

where μ, ν are independent of k and also

$$K_4 = O(N^{2\varepsilon}), \qquad K_5 = O(1)$$

are independent of k. Note that because of the bound (19.3) we have

$$1 - K_5\delta^{-2}N^{-4\varepsilon}(S + \overline{S} + S\overline{S}) = 1 + O(N^{-2\varepsilon}), \tag{19.4}$$

hence we can develop the square root of the left-hand side of (19.4) in a MacLaurin series stopping with an error $O(N^{-A})$, provided we take the first $J + 1$ terms of the expansion with $J \geq A/(2\varepsilon)$. Therefore, the Körner correction, up to the negligible error term $O(M^{-1}N^{1/2})$, is majorized by

$$\ll \delta N^{-1/2+2\varepsilon}(\delta^{-2}N^{-4\varepsilon})^{a+b} \max_{\theta} \left| \sum_{k\in[2\tau N, 2M]} \omega_k e\left(\frac{k^2}{2N}\right) S^a \overline{S}^b e(k\theta) \right|$$

for some positive integers a, b, bounded by $O(1/\varepsilon)$.

We expand the powers of S and $\overline{S}$ using (19.2). If $\widehat{P}_3(k) + \widehat{P}_5(k)$ or its conjugate is not involved in the expansion, we are dealing with

$$\begin{aligned} &\ll \delta N^{-1/2+2\varepsilon}(\delta^{-2}N^{1/2-4\varepsilon})^{a+b} \\ &\quad \times \sum_{k\in[N-2M, N-2\tau N]} \omega_k e\left((1-a+b)\frac{k^2}{2N}\right) \widehat{P}_2(k)^a \overline{\widehat{P}_2(k)}^b e(k\theta). \end{aligned} \tag{19.5}$$

If instead $\widehat{P}_3(k) + \widehat{P}_5(k)$ or its conjugate is involved in the expansion, using Lemma 27 we see that we are dealing with

$$\begin{aligned} &\ll \delta N^{-1/2+2\varepsilon}(\delta^{-2}N^{1/2-4\varepsilon})^{a+b}(LM)^{-1/2(a+b-h-l)} \\ &\quad \times \sum_{k\in[N-2M, N-2\tau N]} U(k)\omega_k e\left(\left(\frac{j_1}{2N} + \frac{j_2}{2LM}\right)k^2\right) \widehat{P}_2(k)^h \overline{\widehat{P}_2(k)}^l e(k\theta) \end{aligned}$$

where

$$j_1 := 1-a+b, \qquad j_2 := -a+b+h-l, \qquad h+l < a+b, \qquad h \leq a, \qquad l \leq b, \tag{19.6}$$

and $U(k)$ is a differentiable function of k satisfying

$$U(k) \ll 1, \qquad U'(k) \ll (LM)^{-1/2}. \tag{19.7}$$

Because of (19.7) the factor $U(k)$ is slowly oscillating over intervals of length $\sqrt{LM}$, hence we can remove it at a cost of a factor $M/\sqrt{LM}$ and summing over some interval $I \subset [N - 2M, N - 2\tau N]$. Therefore, we need to deal with

$$\begin{aligned} &\ll \delta N^{-1/2+2\varepsilon}(\delta^{-2}N^{1/2-4\varepsilon})^{a+b} M(LM)^{-(1+a+b-h-l)/2} \\ &\quad \times \sum_{k\in I} \omega_k e\left(\left(\frac{j_1}{2N} + \frac{j_2}{2LM}\right)k^2\right) \widehat{P}_2(k)^h \overline{\widehat{P}_2(k)}^l e(k\theta) \end{aligned} \tag{19.8}$$

with j_1, j_2, h, l as in (19.6). Now we compute, using the fact that $a+b > h+l$ if $j_2 \neq 0$:

$$\begin{aligned}(\delta^{-2}N^{1/2-4\varepsilon})^{a+b-h-l} M(LM)^{-(1+a+b-h-l)/2} &= \left(\frac{\delta^{-4}N^{1-8\varepsilon}}{LM}\right)^{(a+b-h-l)/2} M(LM)^{-1/2} \\ &\ll \delta^{-2}N^{1/2-4\varepsilon}L^{-1} \\ &\asymp \delta^{-2}MN^{-1-3\varepsilon} \\ &\asymp M^{7/5}N^{-6/5-3\varepsilon} \ll 1\end{aligned} \tag{19.9}$$

because we assumed $M \ll N^{6/7}$.

Putting together (19.5) for the case $j_2 = 0$ and (19.8) and (19.9) for the case $j_2 \neq 0$, we infer that it suffices to give an estimate for

$$D\sum_{k\in I}\omega_k e\left(\left(\frac{j_1}{2N}+\frac{j_2}{2LM}\right)k^2\right)\widehat{P}_2(k)^a\overline{\widehat{P}_2(k)}^b e(k\theta)$$

where

$$D = \begin{cases}\delta N^{-1/2+2\varepsilon}(\delta^{-2}N^{1/2-4\varepsilon})^{a+b} & \text{if } j_2 = 0, \\ \delta^{-1}MN^{-3/2-\varepsilon}(\delta^{-2}N^{1/2-4\varepsilon})^{a+b} & \text{if } j_2 \neq 0,\end{cases} \tag{19.10}$$

for every $\theta \in \mathbb{T}$ and all subintervals $I \subset [N-2M, N-2\tau N]$, with j_1, j_2, a, and b bounded by $O(1/\varepsilon)$.

20. Explicit constructions, II: The correction in the ranges $k \in [2\tau N, 2M]$ and $k \in [N-2M, N-2\tau N]$. Second step

Recall that

$$N = 2n^2 = 2m^2r^2, \quad M = m^2, \quad R = r^2. \tag{C13}$$

We write

$$N-k = 2nu+v, \quad \left\lfloor\frac{2\tau N - v}{2n}\right\rfloor \leq u \leq \left\lfloor\frac{2M-v}{2n}\right\rfloor, \quad 0 \leq v < 2n, \tag{20.1}$$

and take

$$\omega_k = \omega_u^{(1)}\omega_v^{(2)}$$

with $\omega_u^{(1)}$ and $\omega_v^{(2)}$ to be defined later.

Note that since $0 \leq v < 2n$ the interval for u is one of not more than four possible intervals, and each possibility is a subinterval of $0 \leq v < 2n$.

By (20.1) we have

$$\begin{aligned}\left(\frac{j_1}{2N}+\frac{j_2}{LM}\right)(N-k)^2 &= j_1u^2 + \frac{j_1}{n}uv + \frac{j_1v^2}{4n^2} + \frac{4j_2r^2}{L}u^2 + \frac{4j_2}{mL}ruv + \frac{j_2}{m^2L}v^2 \\ &\equiv \frac{j_1}{n}uv + \frac{4j_2r^2}{L}u^2 + F(u,v) \pmod 1\end{aligned}$$

where $F(u, v)$ is bounded and slowly oscillating for u, v in the given domain. Also, k^2 equals $(N-k)^2$, plus a linear function in u and v, plus a constant. Therefore, we need a bound for the simplified expression

$$D \sum_{2\tau M<2nu+v<2M} \omega_u^{(1)}\omega_v^{(2)} e\left(\frac{j_1}{n}uv + \frac{4j_2r^2}{L}u^2\right)\widehat{P}_2(k)^h\overline{\widehat{P}_2(k)}^l e(u\theta_1)e(v\theta_2)$$

for $(\theta_1, \theta_2) \in \mathbb{T}^2$ and all subintervals $I_1 \subset [0, m/r]$, $I_2 \subset [0, 2n)$, and where $N-k = 2nu+v$.

Recall that $(-1)^k\widehat{P}_2(k)$ is a linear combination with bounded constant coefficients of three sums of type

$$\sum_{j=0}^{\Delta-1}\sum_{q=1}^{Q-1}(*)_q r(k, \Delta_q + j) f(\Delta_q + j, q) \tag{15.6}$$

where $\Delta_q = s_1 + (q-1)\Delta$ with $\Delta \asymp \delta^{-1}$, where

$$(*)_q = \omega_q \quad \text{or} \quad \omega_{q+1} \quad \text{or} \quad \omega_q\omega_{q+1} \tag{20.2}$$

with ω_q given by (15.1), where

$$7Q_0 < t < 14Q_0, \qquad \delta \asymp M^{-1/5}N^{1/10}, \qquad Q \le s_1/\Delta,$$

where

$$r(k, s) := \psi(N-k+2Rs)e\left((N-k)\frac{s}{M} - \frac{N}{2}\left(\frac{s}{M}\right)^2\right), \tag{9.6}$$

and where $f(s, q)$ is one of the functions

$$\begin{aligned}&\cos(2\pi\lambda'_s u_{\Delta_q})\sin(2\pi\lambda_s u_{\Delta_q}),\ \sin(2\pi\lambda'_s u_{\Delta_q})\cos(2\pi\lambda_s u_{\Delta_q}),\\ &\sin(2\pi\lambda'_s u_{\Delta_q})\sin(2\pi\lambda_s u_{\Delta_q}),\end{aligned} \tag{15.7}$$

for $q = 1, \dots, Q-1$.

By expanding $\widehat{P}_2(k)^h\overline{\widehat{P}_2(k)}^l$ it follows that $\widehat{P}_2(k)^h\overline{\widehat{P}_2(k)}^l$ is a linear combination, with bounded coefficients and certain choices of the signs $\pm$, of $\ll \Delta^{h+l}$ sums of type

$$\begin{aligned}\sum_{2\tau M<2nu+v<2M}\ \sum_{\mathbf{q}\in[1,Q-1]^{h+l}}\ \prod_{\nu=1}^{h+l}&\psi(2nu+v+2R(\Delta_{q_\nu}+i_\nu))f(\Delta_{q_\nu}+i_\nu, q_\nu)(*)_{q_\nu}\omega_u^{(1)}\omega_v^{(2)}\\ &\times e\left(\mathcal{L} + \frac{j_1}{n}uv + \frac{4j_2r^2}{L}u^2 + \frac{\Delta}{M}\sum_{\nu=1}^{h+l}\pm q_\nu(2nu+v) - \frac{N\Delta^2}{2M^2}\sum_{\nu=1}^{h+l}\pm q_\nu^2\right)\end{aligned} \tag{20.3}$$

where $\mathcal{L}$ stands for a linear form in all variables.

As in the proof of Lemma 25 with the estimate (15.10), the functions $\psi(2nu+v+2R(\Delta_{q_\nu}+i_\nu))f(\Delta_{q_\nu}+i_\nu, q_\nu)$ and the exponential $e\big(\pm\frac{\Delta}{M}q_\nu v \mp \frac{N\Delta^2}{2M^2}q_\nu^2\big)$ do not oscillate in subintervals for q_ν of length $\ll QN^{-2\varepsilon}$. Hence we can remove the corresponding factors

and exponentials in (20.3) at a cost of a factor $N^{2\varepsilon(h+l)}$, but gaining M^{-h-l} from the size of $\psi(x)$.

Putting everything together, we see that the Körner correction relative to the interval $[N-2M, N-2\tau N]$ is bounded by some expression

$$\ll D(\Delta M^{-1}N^{2\varepsilon})^{h+l}\sum_{u\in I_1}\sum_{v\in I_2}\sum_{\mathbf{q}\in\mathcal{Q}}\prod_{\nu=1}^{h+l}(*)_{q_\nu}\omega_u^{(1)}\omega_v^{(2)} \times e\left(\mathcal{L}+\frac{j_1}{n}uv+\frac{2j_2r^2}{L}u^2+\frac{2r\Delta}{m}u\sum_{\nu=1}^{h+l}\pm q_\nu\right)$$

with I_1, I_2 subintervals of $[0, m/r]$, $[0, n)$, with $\mathcal{Q}$ a parallelepiped $\subset [1, Q-1]^{h+l}$ with sides parallel to the q_ν-axes, and with $\mathcal{L}$ a linear form in u, v, $\mathbf{q}$.

The next simplification is done by writing $u = tx + y$, so that

$$\left\lfloor\frac{-y}{t}\right\rfloor \le x \le \left\lfloor\frac{m/r-y}{t}\right\rfloor, \quad 0\le y<t,$$

and decomposing $\omega_u^{(1)}$ as $\omega_x^{(3)}\omega_y^{(4)}$. The exponential becomes

$$e\left(\mathcal{L}+\frac{j_1}{n}yv+\frac{2r\Delta}{m}y\sum_{\nu=1}^{h+l}\pm q_\nu+\frac{j_1}{n}txv+\frac{2r\Delta}{m}tx\sum_{\nu=1}^{h+l}\pm q_\nu+\frac{4j_2r^2}{L}(tx+y)^2\right) \tag{20.4}$$

where now $\mathcal{L}$ is a linear form in x, y. We note that

$$\frac{2j_2r^2}{L}y^2 \ll \tau t^2 \asymp \tau(\tau M\delta)^2 \asymp N^{-3/2+3\varepsilon}M^{2-2/5}N^{1/5} \asymp M^{8/5}N^{-13/10+3\varepsilon} = o(1)$$

provided

$$M < N^{13/16-2\varepsilon}, \tag{C15}$$

which we shall suppose (note that this condition is compatible with condition (C12′)). Therefore, we can remove the exponential $e\left(\frac{4j_2r^2}{L}y^2\right)$ from (20.4), at no extra cost. In a similar way, a calculation shows that the term $e\left(\frac{8j_2r^2}{L}txy\right)$ does not oscillate (up to linear terms) if $x \asymp m/(rt)$ and also y varies in intervals of order $N^{-\varepsilon}M^{-9/5}N^{7/5}$, therefore we can remove this term at a cost of a factor $M^{9/5}N^{-7/5+\varepsilon}$.

Moreover, writing $2r\Delta t = Am + X$ for some integer A, we find

$$\frac{2r\Delta t}{m}x\sum_{\nu=1}^{h+l}\pm q_\nu \equiv \frac{X}{m}x\sum_{\nu=1}^{h+l}\pm q_\nu \pmod 1 \ll X\Delta^{-2} \pmod 1,$$

hence we can remove this term from (20.4), at a cost of $X\Delta^{-2}$. Thus choosing $X = \Delta^3N^\varepsilon$, which we can if

$$|2r\Delta t - Am| \ll \Delta^3N^\varepsilon, \tag{C16}$$

our cost in eliminating this term is ΔN^ε.

A similar calculation shows that since

$$\frac{2r\Delta}{m}y\sum_{\nu=1}^{h+l}\pm q_\nu=\frac{A}{t}y\sum_{\nu=1}^{h+l}\pm q_\nu+\left(\frac{2r\Delta}{m}-\frac{A}{t}\right)y\sum_{\nu=1}^{h+l}\pm q_\nu=\frac{A}{t}y\sum_{\nu=1}^{h+l}\pm q_\nu+O(N^\varepsilon)$$

we can replace the fraction $2r\Delta/m$ by A/t, at a cost of N^ε.

Thus assuming (C16) we need a bound for

$$D(\Delta M^{-1}N^{2\varepsilon})^{h+l}\Delta M^{9/5}N^{-7/5+3\varepsilon}\sum_{x\in I_3}\sum_{y\in I_4}\sum_{v\in I_2}\sum_{\mathbf{q}\in\mathcal{Q}}\prod_{\nu=1}^{h+l}(*)_{q_\nu}$$
$$\times\,\omega_x^{(3)}\omega_y^{(4)}\omega_v^{(2)}e\left(\mathcal{L}+\frac{j_1}{n}yv+\frac{j_1}{n}txv+\frac{2j_2r^2}{L}t^2x^2+\frac{A}{t}y\sum_{\nu=1}^{h+l}\pm q_\nu\right)$$

where $I_3\subset[0,m/(rt)]$, $I_4\subset[0,t)$, $I_2\subset[0,n)$, and $\mathcal{L}$ is a linear form in x, y, v, $\mathbf{q}$.

Our next step consists in shortening the sum over v and decreasing the denominator n to t. We begin by replacing t/n by A/n_1 where

$$n_1:=\left\lfloor\frac{An}{t}\right\rfloor.$$

Since $t\asymp Q\asymp\tau M\delta$, we have

$$n_1\asymp N^{-\varepsilon}A\delta^{-1}r^2. \tag{20.5}$$

Clearly,

$$\left|\frac{t}{n}-\frac{A}{n_1}\right|<\frac{A}{n_1^2}, \tag{20.6}$$

hence

$$j_1\frac{t}{n}xv=\frac{j_1}{n_1}Axv+\left(\frac{t}{n}-\frac{A}{n_1}\right)j_1xv=\frac{j_1}{n_1}Axv+O(A^{-1}N^\varepsilon M^{9/5}N^{-7/5}),$$

taking into account (20.5), (20.6), and (12.1), namely $\delta\asymp M^{-1/5}N^{1/10}$.

The error term is $O(AN^\varepsilon)$ if we choose

$$M\asymp N^{7/9}, \tag{C17}$$

which is compatible with (C12′). With this choice and $\Delta=\delta^{-1}$, the parameters of the sum become

$$n\asymp\Delta^9,\quad m\asymp\Delta^7,\quad r\asymp\Delta^2,\quad t\asymp N^\varepsilon\Delta^4,\quad n_1\asymp\Delta^5. \tag{20.7}$$

With this choice the exponential of the error term is slowly oscillating in intervals of length $N^{-\varepsilon}|I_3|$ and $N^{-\varepsilon}|I_2|$ for x and v, hence we can eliminate it at a cost of a factor $N^{2\varepsilon}$. Moreover,

$$A\asymp r\Delta t/m\asymp N^\varepsilon.$$

We write

$$v = n_1 s + w, \qquad \omega_v^{(2)} = \omega_s^{(5)} \omega_w^{(6)}$$

where now

$$s \in I_5 \subset [0, CN^{\varepsilon}\Delta^4], \qquad w \in I_6 = [0, n_1 - 1] \ll \Delta^5,$$

for some constant C. We have

$$\frac{j_1}{n_1} xv \equiv \frac{j_1}{n_1} xw \pmod 1,$$

hence we can replace $j_1 Atxv/n$ by $j_1 Axw/n_1$. Next, note that

$$\begin{aligned} \frac{j_1}{n} yv &= \frac{j_1 A}{t} \frac{t}{An} yv = \frac{j_1 A}{tn_1} yv + O(N^{2\varepsilon}\Delta^{-1}) \\ &= \frac{j_1 A}{t} ys + \frac{j_1 A}{tn_1} yw + O(N^{2\varepsilon}\Delta^{-1}) = \frac{j_1 A}{t} ys + O(N^{\varepsilon}). \end{aligned} \tag{20.8}$$

The error term $O(N^{\varepsilon})$ term is slowly oscillating, hence we can replace the term $j_1 yv/n$ by $j_1 Ays/t$ in the exponential sum at a cost of a factor N^{ε}.

Thus assuming (C16) we need a bound for

$$\begin{aligned} &D(\Delta M^{-1} N^{2\varepsilon})^{h+l} \Delta M^{9/5} N^{-7/5+4\varepsilon} \\ &\qquad \times \sum_{x \in I_3} \sum_{y \in I_4} \sum_{s \in I_5} \sum_{w \in I_6} \sum_{\mathbf{q} \in \mathcal{Q}} \prod_{v=1}^{h+l} (*)_{q_v} \omega_x^{(3)} \omega_y^{(4)} \omega_s^{(5)} \omega_w^{(6)} \\ &\qquad \times e\left(\mathcal{L} + \frac{j_1 A}{n_1} xw + \frac{2j_2 r^2}{L} t^2 x^2 + \frac{A}{t} j_1 ys + \frac{A}{t} y \sum_{v=1}^{h+l} \pm q_v \right) \end{aligned} \tag{20.9}$$

where $I_3 \subset [0, m/(rt)]$, $I_4, I_5 \subset [0, t)$, $I_6 \subset [0, n_1)$, and $\mathcal{L}$ is a linear form in x, y, s, w, $\mathbf{q}$.

The variables y, s, and $\mathbf{q}$ in (20.9) are decoupled from the variables x, w, therefore the multiple sum in (20.9) is a product $S^{(1)} S^{(2)}$ where

$$\begin{aligned} S^{(1)} &:= \sum_{y \in I_4} \sum_{s \in I_5} \sum_{\mathbf{q} \in \mathcal{Q}} \omega_y^{(4)} \omega_s^{(5)} \prod_{v=1}^{h+l} (*)_{q_v} e\left(\mathcal{L} + \frac{A}{t} j_1 ys + \frac{A}{t} y \sum_{v=1}^{h+l} \pm q_v \right), \\ S^{(2)} &:= \sum_{x \in I_3} \sum_{w \in I_6} \omega_x^{(3)} \omega_w^{(6)} e\left(\mathcal{L} + \frac{j_1}{n_1} Axw + \frac{4j_2 r^2}{L} t^2 x^2 \right) \end{aligned} \tag{20.10}$$

with $\mathcal{L}$ a linear function in all variables appearing in the sum.

21. Explicit constructions, II: The correction in the ranges $k \in [2\tau N, 2M]$ and $k \in [N - 2M, N - 2\tau N]$. The sum $S^{(1)}$

In this section we prove the bound

$$S^{(1)} \ll t^{(h+l+2)/2}(B \log N)^{(\Omega(t)+1)(h+l+2)} \tag{21.1}$$

where B is a suitable positive quantity depending only on $h + l$ and where $\Omega(t)$ denotes the number of prime factors of t, counted with multiplicity. We shall apply this bound only with $\Omega(t)$ bounded by a function of the parameter ε, hence the logarithmic term in (21.1) is $O(N^{o(1)})$ and only the exponent of t in this bound is what will matter here.

We start by completing the sum $S^{(1)}$ to a sum mod t over the full range $(y, s, \mathbf{q}) \in (\mathbb{Z}/t\mathbb{Z})^{2+h+l}$ and with $\mathcal{L} \in (\mathbb{Z}/t\mathbb{Z})[y, \mathbf{q}]$, at a cost of $O((\log t)^{h+l+2}) = O(N^{o(1)})$.

By the Chinese Remainder Theorem we have, for any integer x,

$$x \equiv \sum_{p^\mu \| t} t_p \bar{t}_p (x \pmod{p^\mu}) \pmod{t}$$

where $t_p = t/p^\mu$ and $\bar{t}_p$ is a multiplicative inverse of $t_p \pmod{p^\mu}$.

We assume now that

the integers t and A are coprime. (C18)

We set

$$\omega_y^{(4)} := \prod_{p^\mu \| t} \prod_{\lambda=0}^{\mu-1} \left[\frac{(A\bar{t}_p y)_\lambda}{p}\right] \left[\frac{(A\bar{t}_p y)_\lambda + 1}{p}\right]$$

with $(A\bar{t}_p y)_\lambda$ the digits of $A\bar{t}_p y$ in base p. We also choose ω_s in the same way as for the variables q_ν, namely

$$\omega_s^{(5)} := \prod_{p^\mu \| t} \prod_{\lambda=0}^{\mu-1} \left[\frac{s_0(p) + \cdots + s_\lambda(p)}{p}\right]$$

with s_λ the digits of s in base p.

Since by condition (C18) the integer A is invertible mod t, we can make the change of variable $y \leftarrow Ay$, ending up with

$$S^{(1)} \ll N^{o(1)} \Bigg| \sum_{(y,s,\mathbf{q})} \prod_{p^\mu \| t} \prod_{\lambda=0}^{\mu-1} \left[\frac{(\bar{t}_p y)_\lambda}{p}\right] \left[\frac{(\bar{t}_p y)_\lambda + 1}{p}\right] \omega_s^{(5)} \times \prod_{\nu=1}^{h+l} (*)_{q_\nu} e\left(\frac{1}{t}\mathcal{L} + \frac{1}{t} y\left(j_1 s + \sum_{\nu=1}^{h+l} \pm q_\nu\right)\right)\Bigg| \tag{21.2}$$

where $(y, s, \mathbf{q}) \in (\mathbb{Z}/t\mathbb{Z})^{2+h+l}$.

Then the sum in (21.2) factors into a product of similar sums mod p^μ, namely (after the change of variable mod p^μ given by $y \leftarrow \bar{t}_p y$):

$$\sum_{(y,s,\mathbf{q})\in(\mathbb{Z}/p^\mu\mathbb{Z})^{2+h+l}} \prod_{\lambda=0}^{\mu-1}\left[\frac{y_\lambda}{p}\right]\left[\frac{y_\lambda+1}{p}\right]\prod_{\lambda=0}^{\mu-1}\left[\frac{s_0+\cdots+s_\lambda}{p}\right] \times \prod_{\nu=1}^{h+l}(*)_{q_\nu}(p)e\left(\frac{1}{p^\mu}\mathcal{L}+\frac{1}{p^\mu}y\left(j_1 s+\sum_{\nu=1}^{h+l}\pm q_\nu\right)\right) \tag{21.3}$$

where $(*)_q(p)$ is the part mod p in the definition of (20.2) of $(*)_q$ using (15.1) and where $\mathcal{L}$ denotes a linear form in the variables $y, q_1, \ldots, q_{h+l}$ with integer coefficients.

In the same way as in the proof of Lemma 25, we write $y = \sum y_\lambda p^\lambda$, $q_\nu = \sum q_{\nu\lambda} p^\lambda$, $s = \sum s_\lambda p^\lambda$. Then we have

$$y\left(j_1 s+\sum_{\nu=1}^{h+l}\pm q_\nu\right) \equiv \sum_{\lambda+\lambda'<\mu} p^{\lambda+\lambda'} y_\lambda\left(j_1 s_{\lambda'}+\sum_{\nu=1}^{h+l}\pm q_{\nu\lambda'}\right) \pmod{p^\mu}.$$

We substitute this in (21.3) and remove the terms with $\lambda+\lambda' \le \mu-2$ at a cost of a factor bounded by $O((C\log p)^{(h+l+2)\mu})$, because the exponential of their contribution does not oscillate. In the same way, we can replace the term $p^{-\mu}\mathcal{L}$ by $p^{-1}\mathcal{L}$ where now $\mathcal{L}$ is a linear form, with integer coefficients, in the new variables y_λ, s_λ, and $q_{\nu\lambda'}$.

Hence

$$\begin{aligned}|(21.3)| \ll{}& (C\log p)^{(h+l+2)\mu} \\ &\times \Bigg| \sum_{\mathbf{y}\in[0,p-1]^\mu}\sum_{\mathbf{s}\in[0,p-1]^\mu}\sum_{q_{10}=0}^{p-1}\cdots\sum_{q_{\nu\lambda}=0}^{p-1}\cdots\sum_{q_{h+l,\mu-1}=0}^{p-1}\prod_{\lambda=0}^{\mu-1}\left[\frac{y_\lambda}{p}\right]\left[\frac{y_\lambda+1}{p}\right] \\ &\times \prod_{\lambda=0}^{\mu-1}\left[\frac{s_0+\cdots+s_\lambda}{p}\right]\prod_{\nu=1}^{h+l}(*)_{q_\nu}(p)e\left(\frac{1}{p}\mathcal{L}+\frac{1}{p}\sum_{\nu=1}^{h+l}\sum_{\lambda=0}^{\mu-1}y_\lambda(s_{\mu-1-\lambda}\pm q_{\nu,\mu-1-\lambda})\right)\Bigg|.\end{aligned} \tag{21.4}$$

Note that by the definition (15.1) the coefficients $(*)_{q_\nu}(p)$ are defined in terms of the digits of q_ν and $q_\nu+1$ (hence of the digits of q_ν alone on subsets where the number of carries in the addition $q_\nu+1$ remains fixed). Therefore, this replaces the original sum by a new sum in which all variables run independently over all residue classes mod p.

Now we make the change of variables

$$q_{\nu 0}+\cdots+q_{\nu\lambda} = u_{\nu\lambda},$$

and a similar one for s,

$$s_0+\cdots+s_\lambda = u_{0\lambda},$$

thus decoupling the variables in $q_{\nu\lambda}$ and s_λ. As in Section 15, we need to be careful with the carries in the addition $q+1$ in base p.

This yields, in the general case, a product of modified Legendre symbols

$$(*)_{q_\nu}(p) = \prod_{\lambda=0}^{\mu-1}\left[\frac{f_{\nu\lambda}(u_{\nu\lambda})}{p}\right]$$

with $f_{\nu\lambda}(x)$ any one of $x, x+1, x(x+1)$.

Special cases occur when $q_\nu + 1$ is involved in $(*)_{q_\nu}(p)$ and we have to make a number of carries in the addition $q_\nu + 1$ in base p. If we deal with $\omega_{q_\nu} + 1$ or $\omega_{q_\nu}\omega_{q_\nu+1}$ and the number of carries in the sum $q_\nu + 1$ is *carry*, we must omit the sums over $u_{\nu\lambda}$ for $\lambda < carry$. Then $f_{\nu\lambda}(x) = x + carry + 1$ or $x(x + carry + 1)$ and we have to omit the value $u_{\nu,carry} = p - carry - 1 \pmod p$.

We conclude that the sum in (21.4) can be expressed as a finite sum of μ products of sums of type

$$\sum_{(y,\mathbf{u})\in\mathbb{F}_p^{1+d}}\left[\frac{y}{p}\right]\left[\frac{y+1}{p}\right]e\left(\frac{a_0}{p}y\right)\prod_{\nu=1}^{d}\left(\frac{f_\nu(u_\nu)}{p}\right)e\left(\frac{b_\nu}{p}yu_\nu + \frac{a_\nu}{p}u_\nu\right) \tag{21.5}$$

where $f_\nu(x)$ is a polynomial of degree 1 or 2 with simple roots, and $d \le h + l + 1$.

Our goal is to obtain square root cancellation in the sum (21.5).

We note first that if $b_\nu = 0$ the variable u_ν becomes uncoupled from y and we can sum over u_ν yielding a factor of size $O(\sqrt{p})$ by Weil's estimate, with the desired square root cancellation. Therefore, we may suppose that all b_ν are non-zero, in which case the change of variables $u_\nu \leftarrow b_\nu u_\nu$ shows that there is no loss of generality in considering only the case where $b_\nu = 1$ always. This step, although not necessary, will simplify notation considerably in what follows.

It will be important to generalize the sum in (21.5) to a sum T_ν with the variables running over the finite field $\mathbb{F}_{p^\nu}$ and consider as well the conjugate sums, obtained by the action on T_ν of the Galois group of $\mathbb{Q}(\sqrt[p]{1})$. The multiplicative and additive characters are extended to $\mathbb{F}_{p^\nu}$ in the usual way, by writing χ (resp. ψ)[4] for the multiplicative (resp. additive) character; and also we simplify notation by writing $\mathbf{x} = (x_1, \dots, x_d)$. Moreover, we replace the symbol $\left[\frac{*}{p}\right]$ by the character $\chi(*)$, since the sum over the points where the character vanishes is again a sum of the same type, but over a smaller number of variables.

The characters χ and ψ are given explicitly by

$$\begin{aligned}
&\chi(x) := \left(\frac{\mathrm{Norm}_{\mathbb{F}_{p^\nu}/\mathbb{F}_p}(x)}{p}\right) = \left(\frac{x^{1+p+\cdots+p^{\nu-1}}}{p}\right) \quad \text{if } x \neq 0,\\
&\chi(0) := 0,\\
&\psi(x) := e_p(\mathrm{Trace}_{\mathbb{F}_{p^\nu}/\mathbb{F}_p}(x)) = e_p(x + x^p + \cdots + x^{p^{\nu-1}}).
\end{aligned}$$

Since χ is a real character, Galois conjugation is trivial on χ. A full set of Galois conjugates of $\psi(x)$ consists of the additive characters $\psi(ux)$ with $u \in \mathbb{F}_p^*$.

[4] No confusion should arise here with the function ψ with compact support used earlier in this paper.

The extension of our sum to the finite field $\mathbb{F}_{p^\nu}$ is now

$$T_\nu := \sum_{(y,\mathbf{x})\in\mathbb{F}_{p^\nu}^{1+d}} \chi(g(y))\psi(a_0 y)\prod_{i=1}^{d}\chi(f_i(x_i))\psi(yx_i + a_i x_i)$$

where $g(y)$ is a non-constant polynomial in y with simple roots and each $f_i(x)$ is a polynomial of degree 1 or 2, also with simple roots. It is immediate that

$$|T_\nu| \le 2^d (p^\nu)^{1+d/2}, \tag{21.6}$$

because for each fixed y the sum is a product of Gauss, Jacobsthal, or Kloosterman sums, hence the result follows from Weil's estimate and summing over y.

Lemma 33. *If $g(y)$ has simple roots, degree at least 2, and p is sufficiently large, then for every $u \in \mathbb{F}_p^*$ and $\nu \ge 1$,*

$$T_\nu(u) \ll (p^\nu)^{(1+d)/2}. \tag{21.7}$$

The constant implicit in $\ll$ depends only on d and the degree of $g(y)$.

Proof. Katz [15] has obtained a more general result that, in our case, provides the required estimate under the condition that $g(y)$ has at least $d+1$ simple roots. Since in our case $d \le h + l \ll 1/\varepsilon$, if we take for g a polynomial of degree $\lfloor C/\varepsilon \rfloor$ with no square factors, with C a sufficiently large numerical constant, this result already suffices for our purposes. Katz's argument requires Deligne's celebrated results on exponential sums, the l-adic Fourier transform of Laumon, as well as delicate monodromy calculations.

We give here another more elementary proof (but still fairly complicated), since it illustrates how elementary considerations can be used with success, in conjunction with Deligne's deep theorems, to obtain sharp bounds for exponential sums.

For a good and comprehensive overview of sums over finite fields, including an account of the cohomological tools needed for dealing with them, we refer to the monograph [13] of Iwaniec and Kowalski, Ch. 11.

By the general theory (see [13, Theorem 11.34, Exercise 3, Corollary 11.36]), for l a prime distinct from p we have

$$T_\nu(u) = \sum_{i=0}^{2d+2}(-1)^i \mathrm{Trace}(F^\nu | H_c^i(\overline{U}, \mathcal{L})) \tag{21.8}$$

where F is the geometric Frobenius, $\overline{U}$ is the open subset of affine space of dimension $n+1$ where $\chi(g)\prod\chi(f_i) \ne 0$ (viewed as a smooth scheme over an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$), and $\mathcal{L}$ is a certain lisse sheaf on $\overline{U}$. Therefore, by expressing the traces as the sum of the ν-th powers of the eigenvalues of F on $H_c^i(\overline{U}, \mathcal{L})$ and simplifying (note that *a priori* it could happen that F may have the same eigenvalue on different cohomology groups $H_c^i(\overline{U}, \mathcal{L})$ and $H_c^{i'}(\overline{U}, \mathcal{L})$, so cancellation of eigenvalues could occur in (21.8)), we can write

$$T_\nu(u) = \sum_{i=1}^{r} m_i \alpha_i(u)^\nu \tag{21.9}$$

where the "roots" $\alpha_i(u)$ are distinct algebraic integers, independent of v, conjugate under Galois conjugation for $u \in \mathbb{F}_p^*$, and where the coefficients m_i are suitable non-zero integers. We also have the important information that the total number $\sum |m_i|$ of "roots" (thus counted with their multiplicity) is bounded only in terms of d and the degrees of the polynomials g and f_i (see [13, Theorem 11.39]).

By Deligne's fundamental theorem [7, Corollaire (3.3.4), p. 206], we infer that

for each i, there is a non-negative integer m such that every $\alpha_i(u)$, $u \in \mathbb{F}_p^*$, is an algebraic integer of absolute value $p^{m/2}$. (21.10)

The idea of the proof is to exploit the behaviour of "roots" under Galois conjugation (see Hooley [12]).

Let z_i, $i = 1, \dots, s$, be distinct complex numbers with $|z_i| = 1$ and let c_i, $i = 1, \dots, s$, be arbitrary complex numbers. Then

$$\sum_{v=1+v_0}^{K+v_0} \Big| \sum_{i=1}^{s} c_i z_i^v \Big|^2 = K \sum_{i=1}^{s} |c_i|^2 + O\Big(\sum_{i \neq j} |c_i c_j| \Big| \sum_{v=1}^{K} (z_i/z_j)^v \Big| \Big)$$
$$= K \sum_{i=1}^{s} |c_i|^2 + O\Big(\sum_{i \neq j} \frac{|c_i c_j|}{|1 - z_i/z_j|} \Big) \tag{21.11}$$

where the constant implied in the $O(\ )$ symbol is absolute (and in fact does not exceed 2). Now a standard application of (21.11) to (21.9), combined with the estimate (21.6), immediately yields

$$|\alpha_i(u)| \leq p^{1+d/2}.$$

By Deligne's result (21.10), we may now assume that

$$|\alpha_i(u)| = p^{1+d/2} \qquad \text{for } i = 1, \dots, s, \tag{21.12}$$
$$|\alpha_i(u)| \leq p^{(1+d)/2} \qquad \text{for } s < i \leq r. \tag{21.13}$$

Our goal is to prove that $s = 0$, i.e. that there are no "roots" of absolute value $p^{1+d/2}$, provided p is sufficiently large. By (21.12) and (21.13), we have

$$T_v(u) = \sum_{i=1}^{s} m_i \alpha_i(u)^v + O(p^{(1+d)v/2}) \tag{21.14}$$

where $\alpha_i(u) \neq \alpha_j(u)$ for $i \neq j$ and $|\alpha_i(u)| = p^{1+d/2}$. Morever, $\sum |m_i|$ in (21.9) is bounded independently of p, hence so is the constant implicit in the $O(\ )$ symbol in (21.14). By (21.11) and (21.14), we infer

$$\sum_{v=2}^{K+1} p^{-(2+d)v} \Big(\sum_{u \in \mathbb{F}_p^*} |T_v(u)|^2 \Big) = (p-1)K \sum_{i=1}^{s} |m_i|^2$$
$$+ O\Big(p \max_{u,\, i \neq j} \frac{1}{|\arg(\alpha_i(u)) - \arg(\alpha_j(u))|} \Big). \tag{21.15}$$

We shall prove, by a direct calculation, that

$$p^{-(2+d)\nu} \sum_{u \in \mathbb{F}_p^*} |T_\nu(u)|^2 \ll p^{1-2^{-d}}. \tag{21.16}$$

Then comparison with (21.15) shows that

$$\sum_{i=1}^{s} |m_i|^2 \ll p^{-2^{-d}} + K^{-1} \max_{u,\, i \neq j} \frac{1}{|\arg(\alpha_i(u)) - \arg(\alpha_j(u))|},$$

hence, letting $K \to \infty$, we infer that $s = 0$ provided p is sufficiently large. By (21.14), this will conclude the alternative proof of the key estimate (21.7).

It remains to prove (21.16). To this end, it will prove convenient to use the following notation. We write vectors in boldface characters, as $\mathbf{x}_i = (x_{i1}, \dots, x_{id})$ and $\mathbf{a} = (a_1, \dots, a_d)$. $\mathbf{I}$ is the identity vector. We denote by $|_k$ the truncation operator, on vectors of length d, given by

$$(x_1, \dots, x_d)|_k = (x_{k+1}, \dots, x_d).$$

Throughout the argument, we will encounter sums over variables

$$y, y' \in \mathbb{F}_{p^\nu}, \qquad u, v_1, v_2, \dots \in \mathbb{F}_p \subset \mathbb{F}_{p^\nu}$$

which will be constrained by the requirement that the point $(y, y', u, v_1, v_2, \dots)$ should not be a zero or a pole (or a point of indetermination) of certain rational functions of these variables. Variables over $\mathbb{F}_p$ will be called *short* and over $\mathbb{F}_{p^\nu}$ will be called *long*. We indicate by $\sum^*$ the fact that the sum in question is restricted in this way.

We also abbreviate

$$F(\mathbf{x}_0, \mathbf{x}_1, \dots) = \prod_{i=0}^{\infty} \prod_{j=1}^{d} \chi(f_j(x_{ij})).$$

We begin by computing

$$\begin{aligned} \sum_u^* |T_\nu(u)|^2 = \sum_u \sum_{y,y'} \chi(g(y)g(y'))\psi(a_0 u(y - y')) \sum_{\mathbf{x}_0, \mathbf{x}_1} F(\mathbf{x}_0, \mathbf{x}_1) \\ \times \psi(uy\mathbf{I} \cdot \mathbf{x}_0 - uy'\mathbf{I} \cdot \mathbf{x}_1 + u\mathbf{a} \cdot (\mathbf{x}_0 - \mathbf{x}_1)). \end{aligned}$$

We make a change of variables replacing y by $yu^{-1} - a_1$ and y' by $y'u^{-1} - a_1$ (here $u \neq 0$). In this way the variables x_{01} and x_{11} become uncoupled with u and we get

$$\begin{aligned} \sum_u^* |T_\nu(u)|^2 \leq \sum_{y,y'} \Big| \sum_{x_{01}} \chi(f_1(x_{01}))\psi(yx_{01}) \Big|^2 \\ \times \Big| \sum_u^* \chi(g(yu^{-1} - a_1)g(y'u^{-1} - a_1)) \sum_{\mathbf{x}_0|_1, \mathbf{x}_1|_1} F(\mathbf{x}_0|_1, \mathbf{x}_1|_1) \\ \times \psi(\mathbf{I}|_1 \cdot (y\mathbf{x}_0 - y'\mathbf{x}_1)|_1 + u(\mathbf{a} - a_1\mathbf{I})|_1 \cdot (\mathbf{x}_0 - \mathbf{x}_1)|_1) \Big|. \end{aligned}$$

By Weil's estimate (note that $\chi(f_1(x))$ is not constant because $f_1(x)$ has distinct roots), this simplifies to

$$\sum_u^* |T_\nu(u)|^2 \le 4p^\nu \sum_{y,y'} \Big| \sum_{\mathbf{x}_0|_1,\mathbf{x}_1|_1} \sum_u^* \chi(G_1(y,y';u))F(\mathbf{x}_0|_1,\mathbf{x}_1|_1) \times \psi(\mathbf{I}|_1\cdot(y\mathbf{x}_0 - y'\mathbf{x}_1)|_1 + u(\mathbf{a}-a_1\mathbf{I})|_1\cdot(\mathbf{x}_0-\mathbf{x}_1)|_1)\Big| \qquad (21.17)$$

where we have abbreviated

$$G_1(y,y';u) := g(yu^{-1}-a_1)g(y'u^{-1}-a_1).$$

We apply Cauchy's inequality to this equation, getting

$$\Big(\sum_u^* |T_\nu(u)|^2\Big)^2 \le 16p^{4\nu} \sum_{y,y'} \Big| \sum_u^* \sum_{\mathbf{x}_0|_1,\mathbf{x}_1|_1} \Big|^2.$$

We expand the square, so that we have to deal with the sum

$$\sum_{y,y'} \sum_{u,v}^* \sum_{\mathbf{x}_0|_1,\dots,\mathbf{x}_3|_1} \chi(G_1(y,y';u)G_1(y,y';v))F(\mathbf{x}_0|_1,\dots,\mathbf{x}_3|_1) \times \psi(\mathbf{I}|_1\cdot(y\mathbf{x}_0|_1-\cdots+y'\mathbf{x}_3)|_1) \times \psi(u(\mathbf{a}-a_1\mathbf{I})|_1\cdot(\mathbf{x}_0-\mathbf{x}_1)|_1 - v(\mathbf{a}-a_1\mathbf{I})|_1\cdot(\mathbf{x}_2-\mathbf{x}_3)|_1).$$

We want to make the terms involving x_{i1}, $i=0,\dots,3$, independent of u. To this end, we perform a change of variable with the following replacements:

$$y \to y-(a_2-a_1)u, \qquad y' \to y'-(a_2-a_1)u, \qquad v \to u+v_1,$$

where v_1 is a new short variable and where now $u+v_1 \ne 0$. In this way, the argument in $\psi(\ )$ becomes

$$yx_{02} - y'x_{12} - yx_{22} + y'x_{32} - v_1(a_2-a_1)(x_{22}-x_{32}) + (y\mathbf{x}_0 - y'\mathbf{x}_1 - y\mathbf{x}_2 + y'\mathbf{x}_3)|_2 + u(\mathbf{a}-a_2\mathbf{I})|_2\cdot(\mathbf{x}_0-\mathbf{x}_1-\mathbf{x}_2+\mathbf{x}_3)|_2 - v_1(\mathbf{a}-a_1\mathbf{I})|_2\cdot(\mathbf{x}_2-\mathbf{x}_3)|_2.$$

Since the terms involving $x_{02},\dots,x_{32}$ are independent of u, we can estimate the sum over these variables using again Weil's bound, getting

$$\sum_{y,y'} \Big| \sum_u^* \sum_{\mathbf{x}_0|_1,\mathbf{x}_1|_1} \Big|^2 \le 2^4 p^{2\nu} \sum_{y,y'} \sum_{v_1} \Big| \sum_u^* \sum_{\mathbf{x}_0|_2,\dots\mathbf{x}_3|_2} \chi(G_2(y,y';u,v_1))F(\mathbf{x}_0|_2,\dots,\mathbf{x}_3|_2)\psi(-v_1(\mathbf{a}-a_1\mathbf{I})|_2\cdot(\mathbf{x}_2-\mathbf{x}_3)|_2) \times \psi(\mathbf{I}|_2\cdot(y\mathbf{x}_0-\cdots+y'\mathbf{x}_3)|_2 + u(\mathbf{a}-a_2\mathbf{I})|_2\cdot(\mathbf{x}_0-\cdots+\mathbf{x}_3)|_2)\Big|$$

where

$$G_2(y, y'; u, v_1) := G_1(y - (a_2 - a_1)u, y' - (a_2 - a_1)u; u) \times G_1(y - (a_2 - a_1)u, y' - (a_2 - a_1)u; u + v_1). \tag{21.18}$$

The right-hand side of (21.18) has the same structure as in (21.17), with the difference that the number of vectors $\mathbf{x}_i$ has doubled and a new outside short variable $v_1 \in \mathbb{F}_p$ has been introduced. The actual expression of the term $\psi(-v_1(\mathbf{a} - a_1\mathbf{I})|_2 \cdot (\mathbf{x}_2 - \mathbf{x}_3)|_2)$ is unimportant here, except for the fact that it is independent of y, y', u and is linear in the variables $\mathbf{x}_i$. The main point is that the length of the vectors has decreased. Therefore, we may proceed by induction, applying Cauchy's inequality and doubling the number of vector variables at each step, making the change of variables

$$y \to y - (a_k - a_{k-1})u, \quad y' \to y' - (a_k - a_{k-1})u, \quad v \to u + v_{k-1}$$

where v_{k-1} is a new short variable, to extract a factor in the sum that can be estimated by Weil's bound and reducing at the same time the dimension of the $\mathbf{x}$ vectors by 1.

Performing the induction yields

$$\Big(\sum_u{}^* |T_\nu(u)|^2\Big)^{2^k} \le 2^{k2^{k+1}} (p^\nu)^{(k+2)2^k-2} p^{2^k-(k+1)} \sum_{y,y'} \sum_{v_1,\dots,v_{k-1}} \Big| \sum_u{}^* \sum_{\mathbf{x}_0|_k,\dots,\mathbf{x}_{2^k-1}|_k} \chi(G_k(y, y'; u, v_1, \dots, v_{k-1})) F(\mathbf{x}_0|_k, \dots, \mathbf{x}_{2^k-1}|_k) \psi(L_k(\mathbf{x}_0|_k, \dots, \mathbf{x}_{2^k-1}|_k)) \times \psi(\mathbf{I}|_k \cdot (y\mathbf{x}_0 - \cdots + y'\mathbf{x}_{2^k-1})|_k + u(\mathbf{a} - a_k\mathbf{I})|_k \cdot (\mathbf{x}_0 - \cdots + \mathbf{x}_{2^k-1})|_k)\Big|^2 \tag{21.19}$$

where

$$G_k(y, y'; u, v_1, \dots, v_{k-1}) = \prod_{I \subset \{1,\dots,k-1\}} G_1\Big(y - (a_k - a_1)u, y' - (a_k - a_1)u; u + \sum_{i \in I} v_i\Big) = \prod_{I \subset \{1,\dots,k-1\}} g\bigg(\frac{y - a_k u - a_1 \sum_{i \in I} v_i}{u + \sum_{i \in I} v_i}\bigg) g\bigg(\frac{y' - a_k u - a_1 \sum_{i \in I} v_i}{u + \sum_{i \in I} v_i}\bigg),$$

where L_k is a linear function in the variables $\mathbf{x}_i|_k$ with coefficients depending on $v_1, \dots, v_{k-1}$ and $\mathbf{a}$, but independent of u, y, y'; here the sequence of signs $\pm$ in (21.19) is the well-known Thue–Morse sequence. The sum over u is restricted, for given $v_1, \dots, v_{k-1}$, to $u + \sum_{i \in I} v_i \ne 0$ for all $I \subset \{1, \dots, k-1\}$.

If we complete the induction to $k = d$ the vectors $\mathbf{x}|_d$ are empty and everything simplifies to

$$\Big(\sum_u{}^* |T_\nu(u)|^2\Big)^{2^d} \le 2^{d2^{d+1}} (p^\nu)^{(d+2)2^d-2} p^{2^d-(d+1)} \times \sum_{y,y'} \sum_{v_1,\dots,v_{d-1}} \Big| \sum_u{}^* \chi(G_d(y, y'; u, v_1, \dots, v_{d-1}))\Big|^2 \tag{21.20}$$

Again, we expand the square, getting

$$\sum_{y,y'} \sum_{v_1,\dots,v_{d-1}} \Big| \sum_u^* \Big|^2$$
$$\le \sum_{y'} \sum_{v_1,\dots,v_{d-1}} \sum_{u,u'}^* \Big| \sum_y^* \chi(G_d(y,y';u,v_1,\dots,v_{d-1}))G_d(y,y';u',v_1,\dots,v_{d-1}))\Big|.$$

Let us fix y' and $v_1,\dots,u,u'$. The polynomial in y given by

$$\Gamma_d(y) := G_d(y,y';u,v_1,\dots,v_{d-1})G_d(y,y';u',v_1,\dots,v_{d-1})$$

is well defined if $u+\sum_{i\in I} v_i \neq 0$ and $u'+\sum_{i\in I} v_i \neq 0$ for all $I \subset \{1,\dots,d-1\}$. It is either of degree $2^d \deg(g)$ or identically 0, the latter case occurring if $(y' - a_d u - a_1 \sum_{i\in I} v_i)/(u+\sum_{i\in I} v_i)$, or the same quantity with u' in place of u, is a zero of $g(y)$ for some subset $I \in \{1,\dots,d-1\}$. Since $\chi(0)=0$, we can ignore this latter case that does not contribute to the sum over y.

The sum over y is a pure character sum over the long variable y and we obtain the desired square root cancellation if the polynomial $\Gamma_d(y)$ is either identically 0 or has at least one simple root. This is a gain over the trivial estimate obtained by applying the Weil bound to the sums over the variables $\mathbf{x}_i$ alone and will suffice for what we want. It remains to analyze the situation where $\Gamma_d(y)$ has only multiple roots. We will now show that in this case there must be a linear relation among $v_1,\dots,v_{d-1},u,u'$ within a certain finite set of relations, thus saving a short variable in the count, and this again will suffice for concluding the proof.

The roots of $\Gamma_d(y)$ are located at the $2^d \deg(g)$ points

$$(\beta+a_1)\sum_{i\in I} v_i + (\beta+a_d)u, \qquad (\beta+a_1)\sum_{i\in I} v_i + (\beta+a_d)u',$$

for the 2^{d-1} subsets $I \subset \{1,\dots,d-1\}$, where β runs over the $\deg(g)$ distinct roots of $g(y)$.

If all roots of $\Gamma_d(y)$ are multiple, we obtain at least one non-trivial linear relation among the variables $u,u',\dots,v_{d-1}$ unless $\deg(g)=1$, which was excluded by hypothesis. The number of possible relations obtained in this way is at most $2^{2d-1}\deg(g)^2 - 2^{d-1}\deg(g)$. In this case, we use the trivial estimate p^ν for the sum over y.

If instead $\Gamma_d(y)$ has at least one simple root then, by Weil's estimate on character sums in one variable,

$$\Big| \sum_{y\in\mathbb{F}_{p^\nu}} \chi(\Gamma_d(y))\Big| < 2^d \deg(g)(p^\nu)^{1/2}.$$

We conclude that

$$\sum_{y,y'} \sum_{v_1,\dots,v_{d-1}} \Big| \sum_u^* \Big|^2 \le 2^d \deg(g)(p^\nu)^{3/2} p^{d+1} + (2^{2d}\deg(g)^2 - 2^d \deg(g))p^{2\nu}p^d.$$

If $\nu \geq 2$, this gives the bound $2^{2d} \deg(g)^2 p^{2\nu} p^d$, which, substituted in (21.20), yields

$$\Big(\sum_u{}^* |T_\nu(u)|^2 \Big)^{2^d} \leq 2^{d2^{d+1}+2d} \deg(g)^2 (p^\nu)^{(d+2)2^d} p^{2^d-1} \tag{21.21}$$

for $\nu \geq 2$. This proves (21.16) and the lemma. □

Remark 34. From (21.21) we see that $p > 2^{d2^{d+1}+2d} \deg(g)^2$ suffices for the conclusion of Lemma 33.

22. Explicit constructions, II: The correction in the ranges $k \in [2\tau N, 2M]$ and $k \in [N - 2M, N - 2\tau N]$. The sum $S^{(2)}$

In this section we estimate the sum $S^{(2)}$. Recall that

$$S^{(2)} := \sum_{x \in I_3} \sum_{w \in I_6} \omega_x^{(3)} \omega_w^{(6)} e\Big(\mathcal{L} + \frac{j_1}{n_1} Axw + \frac{4 j_2 r^2}{L} t^2 x^2 \Big) \tag{20.10}$$

where $\mathcal{L}$ is a linear form in x, v, $I_3 \subset [0, m/(rt)]$, and $I_6 \subset [0, n_1 - 1]$. The number t was subject to conditions (C(K)), (C16), (C18), and $7Q_0 < t < 14Q_0$ in Lemma 25; only the last condition matters here. Since $m/(rt) \asymp N^{-\varepsilon}\Delta$, we have $|I_3| = o(\Delta)$ for large N.

In the next step we reduce the range for w using a by now familiar argument. We write

$$w = n_2 y + z, \qquad \omega_w^{(6)} = \omega_y^{(7)} \omega_z^{(8)}$$

where now $\Delta^4 \leq n_2 \leq 2\Delta^4$, hence $y \leq n_1/n_2 \asymp \Delta$ and $z < n_2 \asymp \Delta^4$.

This time we need to choose n_2 a little more carefully, making sure that

$$p_7 := \lfloor n_1/n_2 \rfloor \asymp \Delta \tag{22.1}$$

is a prime number; this we can do without any trouble, because

$$\frac{n_1}{h} - \frac{n_1}{h+1} \ll \Delta^{-3} = o(1)$$

if $\Delta^4 \leq h \leq 2\Delta^4$, so that $\lfloor n_1/h \rfloor$ spans all integers in $[n_1/(2\Delta^4), n_1/\Delta^4]$ as h varies.

By the same argument used in Section 20 to split off the variable w, the variable z becomes decoupled from the other variables. We choose for $\omega_z^{(8)}$ an appropriate Legendre symbol. Then the contribution to $S^{(2)}$ coming from the sum over z is a factor not exceeding $\Delta^2 \log N$. We set

$$\omega_x^{(3)} = \omega_y^{(7)} = \Big[\frac{x}{p_7} \Big], \tag{22.2}$$

and complete the sum. (Note that $I_3 \subset [0, p_7)$.) We conclude that

$$S^{(2)} \ll N^{5\varepsilon}(\log N)^3\Delta^2 \times \max_{a_1,a_2}\left|\sum_{x=1}^{p_7}\sum_{y=1}^{p_7}\left(\frac{x}{p_7}\right)\left(\frac{y}{p_7}\right)e\left(\frac{a_1}{p_7}x+\frac{a_2}{p_7}y+\frac{j_1}{p_7}Axy+\frac{4j_2r^2}{L}t^2x^2\right)\right| + N^{5\varepsilon}(\log N)^3\Delta^3. \tag{22.3}$$

(The extra term here arises by replacing the symbol $[p/q]$ by the Legendre symbol.) For the final evaluation, we distinguish cases.

Case I: $j_2 \neq 0$. In this case we use the trivial estimate using $p_7 \asymp \Delta$ (better bounds are easy to prove, but they are not needed here)

$$S^{(2)} \ll N^{5\varepsilon}(\log N)^3\Delta^4. \tag{22.4}$$

Case II: $j_2 = 0$. If $(j_1x + a_2, p_7) = 1$ the sum over y is

$$\left(\frac{j_1Ax+a_2}{p_7}\right)\sqrt{p_7} \quad \text{or} \quad \left(\frac{j_1Ax+a_2}{p_7}\right)i\sqrt{p_7}$$

according as $p \equiv 1$ or $3 \pmod 4$. Then the sum over x is a Kloosterman sum or Jacobsthal sum, bounded in any case by $2\sqrt{p_7}$. Hence in this case we have by (22.1) and (22.3) the bound

$$S^{(2)} \ll N^{5\varepsilon}(\log N)^3\Delta^3. \tag{22.5}$$

23. Explicit constructions, II: Conclusion

Here we put together all the estimates obtained. The polynomial to consider is $P^{(3)}(\theta)$ after performing the Körner correction. We recall the conditions we have imposed so far:

- $N = 2RM$, (C0)
- $\delta = \Delta^{-1} \asymp M^{-1/5}N^{1/10}$, (12.1)
- $M = m^2$, $R = r^2$, $n := mr$, (C13)
- n is squarefree, (C14)
- t satisfies condition (C(K)) for some integer $K \geq 1$, (C(K))
- $7Q_0 < t < 14Q_0 \quad (Q_0 \asymp \tau\delta M)$,
- Lemma 32 holds,
- $|2r\Delta t - Am| \ll \Delta^3N^{\varepsilon}$ for some integer A, (C16)
- $M \asymp N^{7/9}$, (C17)
- the integers t and A are coprime, (C18)

all other conditions either having been verified or being a consequence of the above conditions.

By (12.1), (C17), and (20.7) we have already noted that

$$n \asymp \Delta^9, \quad m \asymp \Delta^7,\ r \asymp \Delta^2, \quad 7Q_0 < t < 14Q_0, \quad Q_0 \asymp N^{\varepsilon}\Delta^4. \tag{20.7}$$

Lemma 35. *Suppose that the parameters M, N, and $\tau = N^{-1/2+\varepsilon}$ of the polynomial $P^{(3)}(\theta)$ satisfy all the above conditions. Let $P(\theta)$ be obtained from $P^{(3)}(\theta)$ by performing the Körner correction. Then*

$$|P(\theta)| = 1 + O(N^{-1/9+C\varepsilon})$$

for an absolute constant C.

Proof. By Lemma 30 with $M \asymp N^{7/9}$ we have

$$|P^{(3)}(\theta)| = 1 + O(N^{-1/9+4\varepsilon}).$$

The Körner corrections are:

$$\begin{aligned}
&O(N^{-1/4+2\varepsilon}) && \text{in } [\tau N, 2\tau N] \cup [N - 2\tau N, N - \tau N] && \text{(by Lemma 29),}\\
&O(N^{-1/9+C\varepsilon}) && \text{in } [-M, \tau N] \cup [N - \tau N, N + M] && \text{(by Lemma 30),}\\
&O(N^{-1/9+3\varepsilon}) && \text{in } k \notin [2M, N - 2M] && \text{(by Lemma 31).}
\end{aligned}$$

We put together the results of Sections 19 to 22 and compute the correction in the range $[N - 2M, N - 2\tau N]$, the proof for $[2\tau N, 2M]$ being the same. We have already shown (by (20.9) and the comments at the end of that section) that the Körner correction is bounded by

$$D(\Delta M^{-1} N^{2\varepsilon})^{h+l} \Delta M^{9/5} N^{-7/5+3\varepsilon} \times |S^{(1)}| \times |S^{(2)}|$$

with $h + l$, j_1, j_2 bounded by C/ε for some absolute constant C. Here

$$D = \begin{cases} \delta N^{-1/2+2\varepsilon} (\delta^{-2} N^{1/2-4\varepsilon})^{h+l} & \text{if } j_2 = 0,\\ \delta^{-1} M N^{-3/2-\varepsilon} (\delta^{-2} N^{1/2-4\varepsilon})^{h+l} & \text{if } j_2 \neq 0. \end{cases} \tag{19.10}$$

Moreover, taking $g(y) = y(y + 1)$, by Lemma 33, (22.4), and (22.5), we have

$$\begin{aligned}
S^{(1)} &\ll t^{(2+h+l)/2} (\log N)^{(\Omega(t)+1)(h+l+2)}, \qquad (23.1)\\
S^{(2)} &\ll N^{5\varepsilon} (\log N)^3 \Delta^4 \quad \text{if } j_2 \neq 0,\\
S^{(2)} &\ll N^{5\varepsilon} (\log N)^3 \Delta^3 \quad \text{if } j_2 = 0,
\end{aligned}$$

where the implied constants depend at most on $h+l$. The estimate for D if $j_2 \neq 0$ is better than the corresponding estimate when $j_2 = 0$ by a factor $MN^{-1-3\varepsilon}\delta^{-2} \asymp N^{-3\varepsilon}\Delta^{-2}$, which amply suffices for the loss of Δ in the bound for $S^{(2)}$ if $j_2 \neq 0$, compared with the bound obtained when $j_2 = 0$. Hence the worst situation occurs for $j_2 = 0$. Therefore, we compute for the case $j_2 = 0$:

$$\begin{aligned}
&D(\Delta M^{-1} N^{2\varepsilon})^{h+l} \Delta M^{9/5} N^{-7/5+3\varepsilon} \times |S^{(1)}| \times |S^{(2)}|\\
&\quad \ll \Delta^{-1} \Delta^{-9} N^{2\varepsilon} (\Delta^{11} N^{-4\varepsilon})^{h+l} (\Delta^{-13} N^{2\varepsilon})^{h+l}\\
&\qquad \times \Delta N^{3\varepsilon} (\Delta^4 N^{\varepsilon})^{(2+h+l)/2+o(1)} (\log N)^{h+l} \Delta^3 N^{5\varepsilon} (\log N)^3\\
&\quad \ll \Delta^{-2} N^{21\varepsilon/2+o(1)} (N^{-3\varepsilon/2})^{h+l} \ll N^{-1/9+11\varepsilon}. \qquad \square
\end{aligned}$$

24. Explicit constructions, II: Proof of Theorem 7

First proof. It is clear that if we have an ultraflat polynomial of degree N with error term $O(N^{-1/9+o(1)})$ then after padding the length of the polynomial with appropriate Gaussian coefficients we also have ultraflat polynomials of degree N_0 with the same error term, provided

$$|N - N_0| < N_0^{7/9+o(1)}.$$

Hence if every interval $[N_0, N_0 + N_0^{7/9+o(1)}]$ contains such a number N then every degree will be admissible for our explicit construction.

By Lemma 21 and the preceding observation we can take N to be any integer satisfying all conditions stated at the beginning of the preceding Section 23.

Hence let us fix N_0, let Δ be a positive integer, m be a squarefree number, and r be squarefree and coprime with m, satisfying

$$2^{-1}\Delta^7 < m < \Delta^7, \quad \Delta^2 < r < 2\Delta^2, \quad (m, r) = 1,$$

and let us verify that $N = 2m^2r^2$ is admissible.

The verification of Lemma 32 simply means changing an initial choice $\varepsilon = \varepsilon_0$ to some unspecified new value $\varepsilon \in [\varepsilon_0 - \log 2/\log n, \varepsilon_0]$, which does not alter our conclusions.

Since now Δ, M, R, and ε_0 are determined, so is Q_0 of order $N^{\varepsilon}\Delta^4$.

It remains to verify that we can find A and t such that

- t satisfies condition (C(K)) for some integer $K \geq 1$, (C(K))
- $7Q_0 < t < 14Q_0$,
- $|2r\Delta t - Am| \ll \Delta^3 N^{\varepsilon}$ for some integer A, (C16)
- the integers t and A are coprime. (C18)

Since t is of order Q_0, A is of order $r\Delta Q_0/m$. So we fix

$$A_0 = \left\lceil \frac{14r\Delta Q_0}{m} \right\rceil, \quad t_0 = \left\lceil \frac{A_0 m}{2r\Delta} \right\rceil$$

so that

$$0 \leq 2r\Delta t_0 - A_0 m < 2r\Delta \ll \Delta^3, \quad \frac{A_0 m}{2r\Delta} \leq t_0 < \frac{A_0 m}{2r\Delta} + 1,$$

hence for large Δ,

$$7Q_0 < t_0 < \frac{A_0 m}{2r\Delta} + 1 < 7Q_0 + O(\Delta^4) < 8Q_0.$$

If we change t_0 to $t = t_0 + x$, condition (C16) remains satisfied provided $x = O(N^{\varepsilon})$. This is quite a short interval and we do not know whether it always contains prime numbers, or even squarefree numbers, and this led to the complications in Section 15, with all its ripple effects in the following sections, in order to allow a much more general class of integers for choosing t.

We now show that if K is large enough we can find t satisfying all the required conditions and in particular $\Omega(t) \leq K$, hence the $\log N$ term in (23.1) will contribute only

$N^{o(1)}$ and becomes irrelevant for our estimates. (Note that since $\Omega(t)$ could be sometimes of order $\log t/\log\log t$ some control on the factorization of t was needed.)

This is done by applying the lower bound linear sieve to the interval $[t_0, t_0 + n^\varepsilon]$. This is a sequence of about n^ε integers of size $\asymp \Delta^{4+18\varepsilon}$, well-distributed up to level $n^{\varepsilon - o(1)}$, and we have to sieve out all primes up to size about $\Delta^{(4+18\varepsilon)/(K+1)}$. By the lower bound linear sieve, the number of K-strong almost primes in the sequence is $\gg n^\varepsilon/\log\Delta$, provided

$$2\frac{4+18\varepsilon}{K+1} < 9\varepsilon,$$

i.e. $K > 3 + 8/(9\varepsilon)$ (see for example Halberstam and Richert [10, Theorem 8.4]).

We have shown that any number $N = 2m^2r^2$ with m, r coprime squarefree numbers in the intervals $[2^{-1}\Delta^7, \Delta^7]$ and $[\Delta^2, 2\Delta^2]$ is the degree of an ultraflat polynomial with error term $O(N^{1/2-1/9+C\varepsilon})$. It remains to show that any interval $[N_0, N_0 + N_0^{7/9}]$ contains such a number N, if N_0 is sufficiently large.

Given N_0, let $\Delta = \lfloor (N_0/2)^{1/18} \rfloor$ and let r be the smallest prime in the interval $[\Delta^2, 2\Delta^2]$. Let $Q(x)$ denote the number of squarefree integers up to x. We recall the following simple argument due to Estermann and Roth (see Roth [20, p. 263]). Let $x^{1/3} < y < x^{1/2}$. Then for some $\eta \in [-1, 1]$ we have

$$\begin{aligned} Q(x+y) - Q(x) &= \sum_{x < n \le x+y} |\mu(n)| = \sum_{x < l^2 m \le x+y} \mu(l) \\ &= \sum_{1 \le l \le x^{1/3}} \mu(l) \left\{ \left\lfloor \frac{x+y}{l^2} \right\rfloor - \left\lfloor \frac{x}{l^2} \right\rfloor \right\} + \eta \sum_{\substack{x < l^2 m \le x+y \\ l > x^{1/3}}} 1 \\ &= \frac{6}{\pi^2} y + O(x^{1/3}) \end{aligned}$$

because if $l > x^{1/3}$ we have $m < 2x^{1/3}$, while for fixed m there are

$$\lfloor \sqrt{(x+y)/m} \rfloor - \lfloor \sqrt{x/m} \rfloor < 1 + y/(2\sqrt{xm}) < 3/2$$

numbers $l^2 m$ with $x < l^2 m \le x + y$.

Therefore, a positive proportion of integers in $[\sqrt{N_0/(2r^2)} + 1, \sqrt{N_0/(2r^2)} + C\Delta^{7/3}]$ are squarefree numbers and most of them are not divisible by r. If m_0 is such a squarefree number, the number $N = 2m_0^2 r^2$ is admissible. Since $m_0 r^2 \asymp \Delta^{11}$ and $11 + 7/3 < 14$, we have $N \in [N_0, N_0 + N_0^{7/9}]$ for large N_0. □

Second proof. There is an alternative construction of N that avoids the use of condition (C(K)) for t, replacing it by the new condition that t is squarefree and coprime with Ar. This time we exploit the fact that there is some freedom in choosing Δ. We will take $\Delta \asymp M^{2/5} N^{-1/10+o(1)}$ rather than the sharper $\Delta \asymp M^{2/5} N^{-1/10}$ which was used before. The new condition on t has the advantage of simplifying somewhat the analysis of Section 15, since Lemma 26 will be needed only for t squarefree, thus eliminating the need of controlling the effect of carries in the sum $q + 1$. Another consequence is that

the analysis at the beginning of Section 21 also simplifies, since now $\mu = 1$ and $\lambda = 0$ always. This has the advantage that in the estimate (23.1) of the sum $S^{(1)}$ the power $\log N$ can be replaced by the corresponding power of a constant, hence it is $O(N^{o(1)})$, thus avoiding the additional (minor) irritation of providing a control of $\Omega(t)$. In what follows we give a short account on how this is done.

Given N_0, we take a prime $r \asymp N_0^{1/9}$ and consider the interval

$$I = [x, x + y]$$

with

$$x = \frac{\sqrt{N_0}}{\sqrt{2}r^2}, \qquad y = N_0^{1/18}(\log N_0)^{13/2}. \tag{24.1}$$

Since $\sqrt{N_0}/(\sqrt{2}r^2) \asymp N_0^{5/18}$ we may apply the theorem of Filaseta and Trifonov [9] to find squarefree integers in I. However, we need additional information about the factorization of these numbers and in order to do this we allow numbers with a square factor d^2 of small size.

Lemma 36. *Let y be given by* (24.1)*. Then the interval I contains an integer $k = k_0k_1t$ such that*

(i) $k_0 < (\log N_0)^{15/4}$.
(ii) $k_1 \asymp N_0^{1/18}$ *is a prime.*
(iii) t *is squarefree and* $(t, k_0k_1) = 1$.

Proof. We begin by setting $d \le D$ with

$$D = (\log x)^\beta, \qquad 1 \le \beta < 5/3.$$

Let Q_D be the set of numbers in I with no square factor $d^2 > D^2$ and denote by $M_d(I)$ the set of multiples of d^2 in I. Clearly, $M_d(I) = 0$ if $d > 2\sqrt{x}$. Then

$$\begin{aligned} |I \setminus Q_D| &\le \sum_{\substack{D<d<2\sqrt{x} \\ p|d \Rightarrow p \le D}} M_d(I) + \sum_{D<p\le y/D} M_p(I) + \sum_{y/D<p<2\sqrt{x}} M_p(I) \\ &= \Sigma_1 + \Sigma_2 + \Sigma_3. \end{aligned} \tag{24.2}$$

Noting that $M_d \le y/d^2 + 1$ and recalling that $1 \le \beta < 5/3$, we see that the first sum in (24.2) is[5]

$$\Sigma_1 \le y \sum_{d>D} \frac{1}{d^2} + \Psi(2\sqrt{x}, D) \ll \frac{y}{D} \tag{24.3}$$

by the well-known elementary estimate of de Bruijn [5]

$$\Psi(z, (\log z)^\beta) \ll z^{1-1/\beta+o(1)},$$

valid for fixed $\beta \ge 1$.

[5] The function $\Psi(x, y)$ is the number of integers up to x whose prime factors do not exceed y.

The second sum is majorized trivially by

$$\Sigma_2 \le \sum_{D<p\le y/D} \left(\frac{y}{p^2}+1\right) \ll \frac{y}{D}. \tag{24.4}$$

For the third sum, we use the following bound proved in [9, last formula]. Let $z = cx^{1/5}\log x$ where $1 \le c < (\log x)^A$ for a constant[6] A. Then

$$\sum_{z(\log x)^{1/2}<p<2\sqrt{x}} M_p([x, x+z]) \ll c^{2/3}x^{1/5}\log x. \tag{24.5}$$

We split the interval I into $O(y/z)$ subintervals of length z, to which we apply (24.5). This yields

$$\Sigma_3 \ll yz^{-1}c^{2/3}x^{1/5}\log x \ll y/D \tag{24.6}$$

provided

$$c \gg D^3.$$

If we take $c = D^3$, $\beta = 5/4$, then $z(\log x)^{1/2} \asymp y/D$ and we deduce from (24.3), (24.4), and (24.6) that

$$|Q_D| = y + O(y(\log x)^{-5/4}). \tag{24.7}$$

In order to conclude the proof of the lemma we proceed as follows. Let $\mathcal{P}$ be the set of primes $p \in [N_0^{1/18}, 2N_0^{1/18}]$ and define

$$I_p := I \cap p\mathbb{Z}.$$

Then $|I_p| \sim yp^{-1}$ and any integer in I belongs to I_p for at most five values of p, because $x \asymp N_0^{5/18}$ and $p \asymp N_0^{1/18}$. Therefore

$$\Big|\bigcup_{p\in\mathcal{P}} I_p\Big| \ge \frac{1}{5}\sum_{p\in\mathcal{P}} |I_p| \sim \frac{1}{5}y\sum_{p\in\mathcal{P}}\frac{1}{p} \sim \frac{\log 2}{5}\frac{y}{\log(N_0^{1/18})}.$$

By (24.7), Q_D and I_p must have a non-empty intersection for at least 13% of $p \in \mathcal{P}$ and we take k_1 to be one of these primes. The bound $k_0 < D^3$ follows by noting that p^3 is the highest power of a prime $p < D$ that would not be detected from square factors d^2 with $d > D$. □

We apply Lemma 36 and set $\Delta = k_0k_1$. Then

$$\left|\Delta t - \frac{\sqrt{N_0}}{\sqrt{8}\,r^2}\right| \ll N_0^{1/18}(\log N_0)^{13/2}.$$

Now we specify $m \in [2r\Delta t, 2r\Delta t + N_0^{3/18}]$, requiring that m is squarefree and $(m, r) = 1$. Since $2r\Delta t \asymp N_0^{7/18}$, this provides us with $\asymp N_0^{7/18}$ squarefree numbers. Since r is prime,

[6] The authors assume c to be an arbitrarily large constant, but the uniformity in c extends to this range.

those violating $(m, r) = 1$ contribute not more than $O(N_0^{3/18}/r) + 1 = O(N_0^{1/18})$ and we can find m with the required properties.

By construction, the key condition (C16) $|m - 2r\Delta t| \ll \Delta^3$ is satisfied and $n = mr$ is squarefree. Setting $N = 2m^2r^2$ we have in succession

$$\left|m - \frac{\sqrt{N_0}}{\sqrt{2}\,r}\right| \ll N_0^{3/18}(\log N_0)^{13/2},$$
$$|\sqrt{2}\,mr - \sqrt{N_0}| \ll N_0^{5/18}(\log N_0)^{13/2},$$
$$|N - N_0| = |2m^2r^2 - N_0| \ll N_0^{7/9}(\log N_0)^{13/2}.$$

This finishes our sketch for ending the proof along these lines. □

References

[1] Allouche, J.-P., Liardet, P.: Generalized Rudin–Shapiro sequences. Acta Arith. **50**, 1–27 (1991) Zbl 0763.11010 MR 1129977

[2] Beller, E., Newman, D. J.: An ℓ_1 extremal problem for polynomials. Proc. Amer. Math. Soc. **29**, 474–481 (1971) Zbl 0224.30001 MR 0280688

[3] Bombieri, E.: On Vinogradov's mean value theorem and Weyl sums. In: Automorphic Forms and Analytic Number Theory (Montreal, PQ, 1989), Univ. Montréal, Montreal, QC, 7–24 (1990) Zbl 0734.11043 MR 1111007

[4] Bombieri, E., Bourgain, J.: A remark on Bohr's inequality. Int. Math. Res. Notices **2004**, no. 80, 4307–4330 Zbl 1069.30001 MR 2126627

[5] de Bruijn, N. G.: On the number of positive integers $\leq x$ and free of prime factors $> y$, II. Indag. Math. **28**, 239–247 (1966) Zbl 0139.27203 MR 0205945

[6] Byrnes, J. S.: On polynomials with coefficients of modulus one. Bull. London Math. Soc. **9**, 171–176 (1977) Zbl 0364.30004 MR 0486435

[7] Deligne, P.: La conjecture de Weil II. Publ. Math. IHES **52**, 138–252 (1980) Zbl 0456.14014 MR 0601520

[8] Fiedler, H., Jurkat, W., Körner, O.: Asymptotic expansions of finite theta series. Acta Arith. **32**, 129–146 (1977) Zbl 0308.10021 MR 0563894

[9] Filaseta, M., Trifonov, O.: On the gaps between squarefree numbers II. J. London Math. Soc. **45**, 215–221 (1992) Zbl 0799.11032 MR 1171549

[10] Halberstam, H., Richert, H. E.: Sieve Methods. London Math. Soc. Monogr. 4. Academic Press, London (1974) Zbl 0298.10026 MR 0424730

[11] Hardy, G. H., Littlewood, J. E.: Some problems of "Partitio numerorum": II. Proof that every large number is the sum of at most 21 biquadrates. Math. Z. **9**, 14–27 (1921) JFM 48.0142.01 MR 1544448

[12] Hooley, C.: On exponential sums and certain of their applications. In: Journées arithmétiques 1980, J. V. Armitage (ed.), Cambridge Univ. Press, 92–122 (1982) Zbl 0488.10041 MR 0697259

[13] Iwaniec, H., Kowalski, E.: Analytic Number Theory. Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc. (2004) Zbl 1059.11001 MR 2061214

[14] Kahane, J.-P.: Sur les polynômes à coefficients unimodulaires. Bull. London Math. Soc. **12**, 321–342 (1980) Zbl 0443.30005 MR 0587702

[15] Katz, N. M.: On a question of Bombieri and Bourgain. www.math.princeton.edu/~nmk, 8 pp.

[16] Körner, T. W.: On a polynomial of J. S. Byrnes. Bull. London Math. Soc. **12**, 219–224 (1980) Zbl 0435.30004 MR 0572106

[17] Littlewood, J. E.: On the mean values of certain trigonometric polynomials. J. London Math. Soc. **36**, 307–334 (1961) Zbl 0108.05801 MR 0141934

[18] Newman, D. J.: An L^1 extremal problem for polynomials. Proc. Amer. Math. Soc. **16**, 1287–1290 (1965) Zbl 0151.08103 MR 0185119

[19] Queffélec, H., Saffari, B.: On Bernstein's inequality and Kahane's ultraflat polynomials. J. Fourier Anal. Appl. **2**, 519–582 (1996) Zbl 0874.42001 MR 1423528

[20] Roth, K. F.: On the gaps between squarefree numbers. J. London Math. Soc. **16**, 263–268 (1951) Zbl 0043.04802 MR 0043119

[21] Saffari, B.: Une fonction extrémale liée à la suite de Rudin–Shapiro. C. R. Acad. Sci. Paris **303**, 97–100 (1986) Zbl 0608.10051 MR 0853595

[22] Weil, A.: On some exponential sums. Proc. Nat. Acad. Sci. U.S.A. **34**, 204–207 (1948) Zbl 0032.26102 MR 0027006