

PRODUCTS OF PRIMES IN ARITHMETIC PROGRESSIONS

KAISA MATOMÄKI AND JONI TERÄVÄINEN

ABSTRACT. A conjecture of Erdős states that, for any large prime q , every reduced residue class $(\bmod q)$ can be represented as a product $p_1 p_2$ of two primes $p_1, p_2 \leq q$. We establish a ternary version of this conjecture, showing that, for any sufficiently large cube-free integer q , every reduced residue class $(\bmod q)$ can be written as $p_1 p_2 p_3$ with $p_1, p_2, p_3 \leq q$ primes. We also show that, for any $\varepsilon > 0$ and any sufficiently large integer q , at least $(2/3 - \varepsilon)\varphi(q)$ reduced residue classes $(\bmod q)$ can be represented as a product $p_1 p_2$ of two primes $p_1, p_2 \leq q$.

The problems naturally reduce to studying character sums. The main innovation in the paper is the establishment of a multiplicative dense model theorem for character sums over primes in the spirit of the transference principle. In order to deal with possible local obstructions we establish bounds for the logarithmic density of primes in certain unions of cosets of subgroups of $\mathbb{Z}_q^\times$ of small index and study in detail the exceptional case that there exists a quadratic character $\psi(\bmod q)$ such that $\psi(p) = -1$ for very many primes $p \leq q$.

1 INTRODUCTION

For integers $k, q \geq 1$ and a real number $N \geq 1$, write

$$E_k(N) = \{a \in \mathbb{Z}_q^\times : a \equiv p_1 \cdots p_k \pmod{q} \text{ for some primes } p_1, \dots, p_k \leq N\},$$

where $\mathbb{Z}_q^\times$ is the set of reduced residue classes $(\bmod q)$. We study the size of $E_k(N)$ for $k \in \{2, 3\}$.

Let us first note that when $k = 1$, Linnik's problem can be formulated as asking for the smallest L such that $E_1(Cq^L) = \mathbb{Z}_q^\times$ for some constant C and all large enough q . Linnik [13, 14] first proved the existence of such constant L and the best known exponent today is $L = 5$ by a result of Xylouris [27] (which is a slight improvement of an earlier result of Heath-Brown [9]).

Concerning the case $k = 2$, Erdős conjectured (see [4]) that $E_2(q) = \mathbb{Z}_q^\times$ for all large enough primes q . This remains open even under the generalized Riemann hypothesis. In this paper we establish a ternary variant of Erdős' conjecture:

Theorem 1.1. *(i) Let $q \in \mathbb{N}$ be cube-free and sufficiently large. Then*

$$E_3(q) = \mathbb{Z}_q^\times.$$

(ii) Let $\varepsilon > 0$ and let $q \in \mathbb{N}$ be sufficiently large in terms of ε . Then

$$E_3(q^{1+\varepsilon}) = \mathbb{Z}_q^\times.$$

Previously, Walker had shown in [26] that $E_{48}(q) = \mathbb{Z}_q^\times$ and later in [25] that $E_{20}(q) = \mathbb{Z}_q^\times$. This was improved independently by Szabó [23] and Zhao [28] to $E_6(q) = \mathbb{Z}_q^\times$ (Szabó [23] needed to assume that q is prime), so we get significantly closer to the conjecture of Erdős.

On the other hand, several authors have considered the least N for which $E_3(N) = \mathbb{Z}_q^\times$. The best results in the literature are that $N = 650q^3$ works for all $q \geq 2$ due to Ramaré, Srivastav and Serra [21], and that $N = q^{6/5+\varepsilon}$ works for all sufficiently large q due to Szabó [23] (improving on [1]). Theorem 1.1 shows that $N = q$ works for every sufficiently large cube-free q , and that $N = q^{1+\varepsilon}$ works for every q that is sufficiently large in terms of ε . Actually our techniques would allow one to establish that, for some quite small $\alpha > 0$, one has $E_3(q^{1-\alpha}) = \mathbb{Z}_q^\times$ for all sufficiently large cube-free q .

We also note that Klurman, Mangerel and the second author [11] proved that, once $\varepsilon > 0$ is sufficiently small, we have $E_3(q) = \mathbb{Z}_q^\times$ for all large enough q^ε -smooth numbers q , and also $E_3(q) = \mathbb{Z}_q^\times$ for all but $O(1)$ primes $q \in [Q^{1/2}, Q]$ for any $Q \geq 1$. The method in [11] depends on the quality of the zero-free regions available for Dirichlet L -functions (mod q), and hence it does not work for arbitrary q . In case when q is smooth, one has better character sum estimates, and due to this our methods would allow one to prove $E_3(q^{1-\alpha}) = \mathbb{Z}_q^\times$ for somewhat larger α than in the cube-free case.

Remark 1.2. In Theorem 1.1(i), the assumption that $q \in \mathbb{N}$ is cube-free and sufficiently large could be weakened for instance to the assumption that, for some $\varepsilon > 0$, the cube-full part of q is $\leq q^{1/9-\varepsilon}$ and q is sufficiently large in terms of ε . Let us briefly sketch why this is the case; we leave the details to the interested reader. In the proof of Theorem 1.1(ii), we look at $E_3(q^{1+100\varepsilon})$ instead of $E_3(q)$ just because we need Proposition 6.2 to be applicable with $\theta = 2/3 + 10\varepsilon$. But, as noted in Remark 5.1, the only property of θ needed for Proposition 6.2 is that

$$(1.1) \quad \max_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \max_{N^{1-\theta} \leq y \leq N} \frac{1}{y} \left| \sum_{n \leq y} \chi(n) \right| \ll N^{-\varepsilon_0}$$

for some $\varepsilon_0 > 0$. By a direct consequence of the Burgess bound (see [10, (12.56)]), we do have (1.1) with $N = q$ and $\theta = 2/3 + 10\varepsilon$ under the assumption that the cube-full part of q is $\leq q^{1/9-100\varepsilon}$. Now the claim follows by adjusting ε .

We also consider another approximation toward the conjecture of Erdős, namely the problem of lower-bounding the density of $E_2(q)$ inside $\mathbb{Z}_q^\times$, and prove the following.

Theorem 1.3. *Let $\varepsilon > 0$ and let $q \in \mathbb{N}$ be sufficiently large in terms of ε .*

(i) *We have*

$$|E_2(q)| \geq \left(\frac{2}{3} - \varepsilon \right) \varphi(q).$$

(ii) *Assume that q is cube-free. Then*

$$|E_2(q)| \geq \left(\frac{11}{16} - \varepsilon \right) \varphi(q).$$

Here $2/3 \approx 0.666\dots$ and $11/16 = 0.6875$ whereas the previous record was due to Szabó [23] with $3/8 = 0.375$ in place of $11/16$ in the case that q is cube-free (for general q , Szabó's method gives proportion $1/3 - \varepsilon$). Note that Theorem 1.3(i) immediately implies (taking $\varepsilon < 1/6$) the previously unknown result that $E_4(q) = \mathbb{Z}_q^\times$ for all large q .

In addition to studying $E_k(N)$ as in Theorems 1.1 and 1.3, there is still another approximation toward the conjecture of Erdős — one can ask what is the least integer k such that every $a \in \mathbb{Z}_q^\times$ can be written as $a = pn$ with $p, n \leq q$ and n having at most

k prime factors. Our methods are not applicable to this binary problem that is in the literature approached through sieving the variable n . The best result on this problem is due to Zhao [28] with $k = 5$. Zhao [28] also obtained that every $a \in \mathbb{Z}_q^\times$ can be written as $a = p_1 p_2 n$ with $p_1, p_2, n \leq q$ and n having at most two prime factors. Of course our Theorem 1.1 improves this last result to n being prime in case q is cube-free.

We shall give outlines of proofs in the following subsection, but let us here very briefly mention the main components of the proofs. The main innovation is the establishment of a multiplicative dense model theorem for character sums over primes in the spirit of the transference principle. The dense model theorem transfers our problems to additive combinatorial problems concerning product sets of positive density subsets of $\mathbb{Z}_q^\times$. To consider these latter problems, we use Kneser's theorem after which we need to deal with the case that the primes are concentrated in a union of cosets of a small index subgroup of $\mathbb{Z}_q^\times$. To deal with this case, we use some sieve theory to obtain lower bounds for the number of primes in unions of cosets of small index. In particular we need to take special care of the case when there exists an exceptional quadratic character $\psi \pmod{q}$ for which $\psi(p) = -1$ for very many primes $p \leq q$.

The multiplicative transference principle established here is likely to have other applications as well. In a forthcoming work joint with Merikoski, we shall consider Linnik's problem using sieve ideas and some of the techniques used in this work.

1.1 Proof outline

The starting point of the proof of Theorem 1.1(i) is (essentially) the orthogonality identity

$$(1.2) \quad \sum_{\substack{p_1, p_2, p_3 \leq q \\ p_1 p_2 p_3 \equiv a \pmod{q}}} \log p_1 \log p_2 \log p_3 = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left(\sum_{p \leq q} \bar{\chi}(p) \log p \right)^3 \chi(a).$$

Separating the contribution of the principal character $\chi_0 \pmod{q}$ and applying the prime number theorem, this becomes

$$(1 + o(1)) \frac{q^3}{\varphi(q)} + \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \left(\sum_{p \leq q} \bar{\chi}(p) \log p \right)^3 \chi(a).$$

If we knew that we have

$$(1.3) \quad \max_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \left| \sum_{p \leq q} \bar{\chi}(p) \log p \right| \ll \frac{q}{(\log q)^{10}},$$

say, the claim would follow quickly by applying to (1.2) this bound together with the standard mean value theorem for character sums (see Lemma 3.6 below). However, unfortunately, there are no chances to unconditionally establish (1.3) — note that the sum is only up to $p \leq q$ with q the conductor of the character.

We overcome this obstacle by establishing a dense model theorem for character sums over primes. This is motivated by the transference approach to additive problems, introduced by Green [6] in the case of counting arithmetic progressions and generalized in [12], [22], [17], [16] to deal with the ternary Goldbach equation.

In particular Shao [22] considered the ternary Goldbach problem for positive density subsets of the primes. More precisely, he proved that if a set $A \subseteq \mathbb{P}$ has lower relative density greater than $5/8$, then each sufficiently large odd integer N can be represented as a sum of three primes from A . Taking $W = \prod_{p \leq w} p$ with w growing to infinity and splitting into arithmetic progressions $(\bmod W)$, this problem reduces to studying a sumset problem in $\mathbb{Z}_W$ and to studying, for b_i coprime to W ,

$$(1.4) \quad \sum_{\substack{n_1, n_2, n_3 \leq N/W \\ (Wn_1+b_1)+(Wn_2+b_2)+(Wn_3+b_3)=N \\ Wn_1+b_1, Wn_2+b_2, Wn_3+b_3 \in A}} \log n_1 \log n_2 \log n_3 \\ = \int_0^1 \left(\prod_{i=1}^3 \sum_{n \leq N/W} \frac{W}{\varphi(W)} f_{b_i}(n) e(\alpha(Wn+b_i)) \right) e(-\alpha N) d\alpha,$$

where $f_{b_i}: [1, N/W] \cap \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$ are defined by $f_{b_i}(n) = \frac{\varphi(W)}{W} (\log n) \mathbf{1}_{Wn+b_i \in A}$.

Now, for each b with $(b, W) = 1$, one can find a dense model $g_b: [1, N/W] \cap \mathbb{N} \rightarrow [0, 1]$ such that $\widehat{g_b}$ is close to $\widehat{f_b}$ in sup norm. Then one can replace f_{b_i} by g_{b_i} in (1.4) (since one has also an L^r bound for $\widehat{f_b}$ and $\widehat{g_b}$ for some $r \in (2, 3)$) and reduce the problem to studying sumsets of positive density subsets of the integers. The corresponding sumset problems can in principle be solved unless there are some "local" obstructions, such as A being concentrated in an arithmetic progression or a Bohr set.

We argue similarly. In particular we essentially let $f: [1, q] \cap \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$ be defined through $f(n) = 1_{n \in \mathbb{P}} \log n$ and prove a multiplicative analogue of a dense model theorem, showing, using the Burgess bound for cube-free q and a linear sieve majorant, that there exists $g: \mathbb{Z}_q^\times \rightarrow [0, \frac{8}{3} + \varepsilon]$ such that

$$\max_{\chi \pmod{q}} \left| \sum_{n \leq q} f(n) \overline{\chi}(n) - \frac{q}{\varphi(q)} \sum_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right| = o(\varphi(q)).$$

Moreover, by a Halász–Montgomery type inequality and the mean value theorem (again in the form of Lemma 3.6) we can show that $\widehat{f}$ and $\widehat{g}$ satisfy suitable L^r bounds with $r \in (2, 3)$ (which we will formulate as large value estimates rather than L^r bounds, see Remark 3.9 below). Combining these facts with (1.2), we can show that

$$\begin{aligned} \sum_{\substack{p_1, p_2, p_3 \leq q \\ p_1 p_2 p_3 \equiv a \pmod{q}}} \log p_1 \log p_2 \log p_3 &= \sum_{\substack{n_1, n_2, n_3 \leq q \\ n_1 n_2 n_3 \equiv a \pmod{q}}} f(n_1) f(n_2) f(n_3) \\ &= \frac{q^3}{\varphi(q)^3} \sum_{\substack{a_1, a_2, a_3 \in \mathbb{Z}_q^\times \\ a_1 a_2 a_3 = a}} g(a_1) g(a_2) g(a_3) + o\left(\frac{q^3}{\varphi(q)}\right). \end{aligned}$$

Writing

$$A = \{a \in \mathbb{Z}_q^\times : |g(a)| \geq \varepsilon/10\},$$

we obtain that $a \in E_3(q)$ if $(\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_A)(a) \gg \varphi(q)^2$. Furthermore, it follows from the construction of g that

$$|A| \geq \left(\frac{3}{8} - \varepsilon\right) \varphi(q).$$

Using a popular sums version of Kneser's theorem (Lemma 6.1), we have $(\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_A)(a) \gg \varphi(q)^2$ for all $a \in \mathbb{Z}_q^\times$ (and hence $E_3(q) = \mathbb{Z}_q^\times$) unless A is essentially (up to a set of cardinality $o(\varphi(q))$) stuck in $k + 1$ cosets of a subgroup $H \leq \mathbb{Z}_q^\times$ of index $3k + 2$, for some $k \in \{0, 1, 2\}$, and $A \cdot A$ is essentially the union of $2k + 1$ cosets of H . The dense model g is defined in such a way that this means that also the primes $p \leq q$ are essentially stuck in these cosets.

We are now left with three problematic scenarios:

- (i) Almost all primes up to q are contained in 3 cosets of an index 8 subgroup of $\mathbb{Z}_q^\times$.
- (ii) Almost all primes up to q are contained in 2 cosets of an index 5 subgroup of $\mathbb{Z}_q^\times$.
- (iii) Almost all primes up to q are contained in a coset of an index 2 subgroup of $\mathbb{Z}_q^\times$.

None of these scenarios should happen in reality, but the existing bounds for least primes in cosets (for example [1, Theorem 2.4]) do not seem to rule them out, and scenario (iii) could in fact happen if there were Siegel zeros.

Using a lemma of Heath-Brown on character sums over primes, we will be able to show that, for at least one of the remaining $2k + 1$ cosets not occupied by A , say a_0H , one has

$$(1.5) \quad \sum_{\substack{p \in (q^{\alpha-\varepsilon}, q^\alpha] \\ p \in a_0H}} \frac{1}{p} \gg 1 \quad \text{for some } \alpha \in [2\varepsilon, 1],$$

except in the case when $k = 0$ and A is essentially contained in the coset $a_1H \neq H$. This last case, corresponding to (iii) above, requires some special care as we will explain below. Also the bound (1.5) is not quite sufficient to refute the scenarios (i) or (ii), since above we would need a positive natural density of primes $p \leq q$ in the coset a_0H . However, in case (1.5) holds we study the logarithmically weighted count

$$\sum_{\substack{p_1 p_2 p_3 \equiv a \pmod{q} \\ p_2, p_3 \leq q \\ q^{\alpha-\varepsilon} < p_1 \leq q^\alpha}} \frac{\log p_2 \log p_3}{p_1} = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left(\sum_{p \leq q} \bar{\chi}(p) \log p \right)^2 \left(\sum_{q^{\alpha-\varepsilon} < p_1 \leq q^\alpha} \frac{\bar{\chi}(p_1)}{p_1} \right) \chi(a).$$

In this case we use the dense model only for the primes p_2, p_3 . Using again large value results for character sums (also for an appropriate moment of the character sum of p_1), we can show that

$$\begin{aligned} \sum_{\substack{p_1 p_2 p_3 \equiv a \pmod{q} \\ p_2, p_3 \leq q \\ q^{\alpha-\varepsilon} < p_1 \leq q^\alpha}} \frac{\log p_2 \log p_3}{p_1} &= \left(\frac{q}{\varphi(q)} \right)^2 \sum_{\substack{p_1 a_2 a_3 = a \\ q^{\alpha-\varepsilon} < p_1 \leq q^\alpha \\ a_2, a_3 \in \mathbb{Z}_q^\times}} \frac{g(a_2)g(a_3)}{p_1} + o\left(\frac{q^2}{\varphi(q)} \right) \\ &\geq \varepsilon^2 \left(\frac{q}{\varphi(q)} \right)^2 \sum_{\substack{p_1 a_2 a_3 = a \\ q^{\alpha-\varepsilon} < p_1 \leq q^\alpha \\ a_2, a_3 \in A}} \frac{1}{p_1} + o\left(\frac{q^2}{\varphi(q)} \right), \end{aligned}$$

with A as above. Since $A \cdot A$ is now essentially a union of $2k + 1$ cosets, this together with (1.5) will allow us to finish the proof.

On the other hand, in case that $k = 0$ and A is essentially contained in the coset $a_1H \neq H$ (so that we are in scenario (iii)), we can use sieve-theoretic arguments to show

(see Lemma 8.1) that either (1.5) holds with $a_0 \in H$ or there exists $y \in [q^{5/7}, q]$ such that

$$(1.6) \quad \sum_{\substack{p \leq y \\ \psi(p)=1}} 1 \gg y L(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p < q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right),$$

where ψ is the quadratic character (mod q) for which $\psi(h) = 1$ for every $h \in H$. The lower bound in (1.6) can be a lot smaller than $y/\log y$ if $L(1, \psi)$ is small (and hence we cannot rule out scenario (iii)), but we can use a sieve to construct a pseudorandom majorant for the primes $p \leq q$ with $\psi(p) = 1$ that takes into account this smaller density of primes with $\psi(p) = 1$, and this allows us to prove a lossless Halász–Montgomery type large value theorem for primes $p \leq y$ with $\psi(p) = 1$ (see Lemma 9.5). This in turn will allow us to make an appropriate transference and finish the proof.

In case q is not cube-free, taking into account the version of Burgess for arbitrary moduli the previous argument would only give us

$$(1.7) \quad |A| \geq \left(\frac{1}{3} - \varepsilon\right) \varphi(q).$$

This is not sufficient for a successful application of Kneser’s theorem since we might have that $|A \cdot A \cdot A| \leq (1 - 3\varepsilon)\varphi(q)$ even if A is not stuck in a union of arithmetic progressions. But once we study $E_3(q^{1+100\varepsilon})$ we can replace $1/3 - \varepsilon$ by $1/3 + \varepsilon$ in (1.7) and the previous method works, since we can also show that A occupies at least proportion $3/8 - \varepsilon$ of cosets of any subgroup of $\mathbb{Z}_q^\times$ with fixed index.

In the proof of Theorem 1.3, we argue similarly to the first part of the proof of Theorem 1.1 to obtain that either the claim holds or we have a similar local obstruction as in the ternary case. In this case, we are able to prove lower bounds for the number of products of two primes in the cosets not occupied by $A \cdot A$ through studying multiplicative energy.

2 NOTATION

2.1 General notation

Throughout the paper, we assume that $\varepsilon > 0$ is sufficiently small. We write $x \sim y$ as a shorthand for $y < x \leq 2y$. By φ, Λ , and τ_k we denote the Euler totient function, the von Mangoldt function, and the k -fold divisor function (with $\tau = \tau_2$), as usual. For $z \geq 1$, we write $P(z) = \prod_{p < z} p$. We write (a, b) for the greatest common divisor of integers a and b . We write

$$(2.1) \quad [N]_q = \{n \leq N : (n, q) = 1\}.$$

By (3.2) below we have that

$$(2.2) \quad |[N]_q| = \frac{\varphi(q)}{q} N + O(\tau(q)).$$

For a finite, nonempty set A and a function $f : A \rightarrow \mathbb{C}$, we use the notation

$$\mathbb{E}_{n \in A} f(n) = \frac{1}{|A|} \sum_{n \in A} f(n).$$

2.2 Group theory

For a finite abelian group G written in multiplicative notation and subsets $A, B \subseteq G$, define the product set $A \cdot B = \{ab : a \in A, b \in B\}$, and for $c \in G$ define the dilation $cA = c \cdot A = \{ca : a \in G\}$. For a subset $A \subseteq G$, the stabilizer of A is the subgroup $\{g \in G : g \cdot A = A\}$.

The convolution of two functions $f, g : G \rightarrow \mathbb{C}$ is defined as

$$(f * g)(a) = \sum_{\substack{b, c \in G \\ bc = a}} f(b)g(c).$$

By $\chi_0 \pmod{q}$ we denote the principal Dirichlet character $\pmod{q}$. For a subgroup $H \leq \mathbb{Z}_q^\times$ and an element $b \in \mathbb{Z}_q^\times$, we abuse the notation by writing, for $n \in \mathbb{Z}$, $n \in bH$ if $n \pmod{q} \in bH$.

We will frequently use that the orthogonality of characters implies that, for any $a \in \mathbb{Z}_q^\times$ and $n \in \mathbb{N}$ or $n \in \mathbb{Z}_q^\times$,

$$\mathbf{1}_{n=a \pmod{q}} = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \bar{\chi}(n) \chi(a)$$

and, for any $H \leq \mathbb{Z}_q^\times$ and $b \in \mathbb{Z}_q^\times$,

$$(2.3) \quad \mathbf{1}_{n \in bH} = \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi(h)=1 \text{ for all } h \in H}} \bar{\chi}(n) \chi(b).$$

Note that the number of characters in the last sum equals the index of H in $\mathbb{Z}_q^\times$.

3 AUXILIARY RESULTS

3.1 Sieves, Burgess' bound, and products of primes in cosets

We shall use the linear sieve, see e.g. [5, Section 12].

Lemma 3.1. *Let $z \geq 2$ and let $D = z^s$ with $s \geq 1$. There exist coefficients $\lambda_d^\pm$ such that the following hold.*

- (i) $|\lambda_d^\pm| \leq 1$ for every $d \in \mathbb{N}$ and $\lambda_d^\pm$ are supported on $\{d \leq D : d \mid P(z)\}$.
- (ii) For every $n \in \mathbb{N}$,

$$\sum_{d|n} \lambda_d^- \leq \mathbf{1}_{(n, P(z))=1} \leq \sum_{d|n} \lambda_d^+.$$

- (iii) If $h : \mathbb{N} \rightarrow [0, 1]$ is a multiplicative function such that

$$\prod_{w_1 \leq p < z_1} (1 - h(p))^{-1} \leq \frac{\log z_1}{\log w_1} \left(1 + O\left(\frac{1}{\log w_1}\right) \right)$$

for any $z_1 \geq w_1 \geq 2$, then

$$\begin{aligned} \sum_{d|P(z)} \lambda_d^+ h(d) &\leq (F_0(s) + o(1)) \prod_{p < z} (1 - h(p)), \\ \sum_{d|P(z)} \lambda_d^- h(d) &\geq (f_0(s) + o(1)) \prod_{p < z} (1 - h(p)), \end{aligned}$$

where F_0 and f_0 are the upper and lower bound linear sieve functions (see e.g. [5, (12.1)–(12.2)]), so that in particular

$$(3.1) \quad \begin{aligned} F_0(s) &= 2e^\gamma/s \text{ for } s \in [1, 3], \\ f_0(s) &= 2e^\gamma \log(s-1)/s \text{ for } s \in [2, 4]. \end{aligned}$$

Applying the sieve in our set-up often leads us to sums over integers coprime to the modulus $q \in \mathbb{N}$. For these we note that by Möbius inversion we have, for any $y \geq 1$,

$$(3.2) \quad \sum_{\substack{m \leq y \\ (m, q) = 1}} 1 = \sum_{e|q} \mu(e) \sum_{m \leq y/e} 1 = y \sum_{e|q} \frac{\mu(e)}{e} + O(\tau(q)) = y \frac{\varphi(q)}{q} + O(\tau(q)).$$

For character sums we use the Burgess bound.

Lemma 3.2. *Let $q \in \mathbb{N}$, let χ be a primitive character (mod q) and let $M, N \geq 1$. Then, for any $\varepsilon > 0$*

$$\left| \sum_{M < n \leq M+N} \chi(n) \right| \ll_\varepsilon N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2} + \varepsilon}$$

for $r \in \{1, 2, 3\}$. If q is cube-free or χ has bounded order, then this holds for any $r \in \mathbb{N}$.

In particular, for any $\varepsilon > 0$, there exists $\delta = \delta(\varepsilon) > 0$ such that for any $q \in \mathbb{N}$ and any $N \geq q^{1/3+\varepsilon}$ we have

$$\left| \sum_{n \leq N} \chi(n) \right| \ll_\varepsilon N^{1-\delta}.$$

When q is cube-free or χ has bounded order, this holds for $N \geq q^{1/4+\varepsilon}$.

Proof. The case $r = 1$ of the first part follows from the Pólya–Vinogradov inequality (see e.g. [10, Theorem 12.4]). The case $r \geq 2$ of the first part is the Burgess bound, see e.g. [10, Theorem 12.5] for the general and cube-free case and [9, Lemma 2.4] for the bounded order case.

The second part follows from the first by taking $r = 3$ in the case of arbitrary q and r large in case q is cube-free or χ has bounded order. $\square$

Let us prove the following quick consequence of the linear sieve and the Burgess bound.

Lemma 3.3 (The number of products of at most two primes in cosets). *Let $\varepsilon > 0$ be fixed. Let $q \in \mathbb{N}$, $N \geq q^{3/4+\varepsilon}$, and let $\theta_0 = 1 - \varepsilon - \frac{\log q}{4 \log N}$. Let $H \leq \mathbb{Z}_q^\times$ be a subgroup of fixed index Y and let $b \in \mathbb{Z}_q^\times$. Then*

$$(1 + o(1)) \frac{2 \log(3\theta_0 - 1)}{\theta_0} \cdot \frac{N}{Y \log N} \leq \sum_{\substack{n \leq N \\ n \in bH \\ p|n \Rightarrow p \geq N^{1/3}}} 1 \leq (1 + o(1)) \frac{2}{\theta_0} \cdot \frac{N}{Y \log N}$$

Proof. Let us first prove the lower bound. Let λ_d^- be as in Lemma 3.1 with $D = N^{\theta_0}$ and $s = 3\theta_0$ (so that $z = N^{1/3}$). By Lemma 3.1(ii),

$$(3.3) \quad \sum_{\substack{n \leq N \\ n \in bH \\ p|n \Rightarrow p \geq N^{1/3}}} 1 \geq \sum_{d \leq D} \lambda_d^- \sum_{\substack{m \leq N/d \\ dm \in bH}} 1.$$

Now we detect the condition $dm \in b \cdot H$ using (2.3). Let $\chi_0, \chi_1, \dots, \chi_{Y-1}$ be the characters (mod q) for which $\chi_j(h) = 1$ for every $h \in H$. Then

$$\sum_{\substack{m \leq N/d \\ dm \in bH}} 1 = \sum_{m \leq N/d} \frac{1}{Y} \sum_{j=0}^{Y-1} \overline{\chi_j}(dm) \chi_j(b) = \frac{\mathbf{1}_{(d,q)=1}}{Y} \sum_{\substack{m \leq N/d \\ (m,q)=1}} 1 + \frac{1}{Y} \sum_{j=1}^{Y-1} \overline{\chi_j}(d) \chi_j(b) \sum_{m \leq N/d} \overline{\chi_j}(m).$$

By (3.2) and the Burgess bound (Lemma 3.2, where we note that each χ_j has bounded order $\leq Y$) we obtain, for some $\delta = \delta(\varepsilon) > 0$,

$$(3.4) \quad \sum_{\substack{m \leq N/d \\ dm \in bH}} 1 = \mathbf{1}_{(d,q)=1} \frac{1}{Y} \frac{N}{d} \frac{\varphi(q)}{q} + O(\tau(q)) + O((N/d)^{1-\delta}).$$

Plugging this into (3.3), we obtain

$$\sum_{\substack{n \leq N \\ n \in bH \\ p|n \Rightarrow p > N^{1/3}}} 1 \geq \frac{N}{Y} \cdot \frac{\varphi(q)}{q} \sum_{(d,q)=1} \frac{\lambda_d^-}{d} + O(D\tau(q) + N^{1-\delta} D^\delta).$$

By Lemma 3.1(iii) and Mertens' theorem, we have

$$\sum_{(d,q)=1} \frac{\lambda_d^-}{d} \geq (f_0(s) + o(1)) \prod_{p < N^{1/3}} \left(1 - \frac{\mathbf{1}_{p|q}}{p}\right) = (e^{-\gamma} f_0(s) + o(1)) \frac{q}{\varphi(q) \log N^{1/3}}$$

The lower bound part of the claim now follows from (3.1), since $s = 3\theta_0 \leq 4$ and either $3\theta_0 \geq 2$ or the claim is trivial. The upper bound follows completely similarly but using the upper bound linear sieve instead. $\square$

3.2 Lower bounds on product sets

Next we collect some results concerning convolutions of characteristic functions and product sets (or equivalently sumsets in additive notation). The following simple lemma gives a lower bound for convolutions on a product set.

Lemma 3.4. *Let G be a finite abelian group.*

(i) *Let $A, B \subseteq G$ be nonempty subsets of G . Then we have*

$$\mathbf{1}_A * \mathbf{1}_B(c) \geq |A| + |B| - |G|$$

for all $c \in G$.

(ii) *Let $H \leq G$, let $a, b \in G$, and let $A \subseteq aH$ and $B \subseteq bH$. Then, for any $c \in abH$, we have*

$$\mathbf{1}_A * \mathbf{1}_B(c) \geq |A| + |B| - |H|.$$

Proof. Part (i) follows since

$$\begin{aligned} \mathbf{1}_A * \mathbf{1}_B(c) &= |cA^{-1} \cap B| = |G| - |(cA^{-1})^c \cup B^c| \\ &\geq |G| - (|G| - |A|) - (|G| - |B|) = |A| + |B| - |G|. \end{aligned}$$

Part (ii) follows from applying part (i) to the group H and sets $a^{-1}A, b^{-1}B \subseteq H$. $\square$

Kneser's theorem (see e.g. [24, Theorem 5.5]) is a standard tool for studying product sets inside abelian groups.

Lemma 3.5 (Kneser's theorem). *Let G be a finite abelian group and let $A, B \subseteq G$. Let H be the stabilizer of $A \cdot B$. Then*

$$|A \cdot B| \geq |A \cdot H| + |B \cdot H| - |H| \geq |A| + |B| - |H|.$$

3.3 Mean values of character sums

The following lemma is the basic mean value theorem (or large sieve) for characters sums.

Lemma 3.6 (Mean value theorem). *Let $q \in \mathbb{N}$ and $N \geq 2$. Then, for any complex coefficients a_n ,*

$$\sum_{\chi \pmod{q}} \left| \sum_{n \leq N} a_n \chi(n) \right|^2 \leq (N + \varphi(q)) \sum_{\substack{n \leq N \\ (n, q) = 1}} |a_n|^2.$$

Proof. Squaring out, using the orthogonality of characters and the inequality $|a_m a_n| \leq (|a_m|^2 + |a_n|^2)/2$, we obtain

$$\begin{aligned} \sum_{\chi \pmod{q}} \left| \sum_{n \leq N} a_n \chi(n) \right|^2 &\leq \varphi(q) \sum_{\substack{m, n \leq N \\ m \equiv n \pmod{q} \\ (mn, q) = 1}} |a_m a_n| \leq \varphi(q) \sum_{\substack{n \leq N \\ (n, q) = 1}} |a_n|^2 \sum_{\substack{m \leq N \\ m \equiv n \pmod{q}}} 1 \\ &\leq \varphi(q) \left(\frac{N}{q} + 1 \right) \sum_{\substack{n \leq N \\ (n, q) = 1}} |a_n|^2. \end{aligned}$$

□

We shall also use the following large value theorem due to Huxley (see e.g. [10, Theorem 9.15 with $s_r(\chi) = 0$ for every r]).

Lemma 3.7. *Let $q \in \mathbb{N}$ and $N \geq 2$, and let $\chi_1, \dots, \chi_R$ be distinct Dirichlet characters of modulus q . Then, for any complex coefficients a_n ,*

$$\sum_{j=1}^R \left| \sum_{n \leq N} a_n \chi_j(n) \right|^2 \ll (N + R^{2/3} N^{1/3} q^{1/3}) (\log(qN))^6 \sum_{n \leq N} |a_n|^2.$$

The following lemma gives variants of Halász–Montgomery type mean value theorems that are tailored for character sums supported on numbers without small prime factors (for the usual Halász–Montgomery type mean value theorem, see e.g. [10, Theorem 9.14]). Using different r in Burgess' bound one would obtain different results. A similar result can also be found from [20, Theorem 3].

Lemma 3.8. *Let $q \in \mathbb{N}$ and let $\chi_1, \dots, \chi_R$ be distinct Dirichlet characters of modulus q . Let $\varepsilon > 0$ and $C \geq 1$ be fixed. Then the following hold.*

(i) *Let $N \in [q^\varepsilon, q^C]$. Then, for any complex coefficients a_n ,*

$$\sum_{j=1}^R \left| \sum_{\substack{n \leq N \\ (n, P(q^\varepsilon)) = 1}} a_n \chi_j(n) \right|^2 \ll \left(\frac{N}{\log q} + q^{\frac{1}{2} + 2\varepsilon} R \right) \sum_{\substack{n \leq N \\ (n, P(q^\varepsilon)) = 1}} |a_n|^2.$$

(ii) Let $q^C \geq N_2 \geq N_1 \geq q^{2\varepsilon}$. Then, for any complex coefficients a_n ,

$$\sum_{j=1}^R \left| \sum_{\substack{N_1 < n \leq N_2 \\ (n, P(q^\varepsilon))=1}} \frac{a_n}{n} \chi_j(n) \right|^2 \ll \left(1 + \frac{q^{1/9+3\varepsilon}}{N_1^{1/3}} R \right) \sum_{\substack{N_1 < n \leq N_2 \\ (n, P(q^\varepsilon))=1}} \frac{|a_n|^2}{n}.$$

Proof. We only prove the second claim, the first claim follows similarly (using non-logarithmic averages and taking $r = 1$ instead of $r = 3$ in Burgess' bound). By the duality principle (see e.g. [10, Section 7.1]), it suffices to show that, for any complex coefficients c_j ,

$$(3.5) \quad \sum_{\substack{N_1 < n \leq N_2 \\ (n, P(q^\varepsilon))=1}} \frac{1}{n} \left| \sum_{j=1}^R c_j \chi_j(n) \right|^2 \ll \left(1 + \frac{q^{1/9+2\varepsilon}}{N_1^{1/3}} R \right) \sum_{j=1}^R |c_j|^2.$$

Let λ_d^+ be as in Lemma 3.1 with sifting parameter $D = q^\varepsilon$ and $s = 1$ (so that $z = D$). Then the left-hand side of (3.5) is by Lemma 3.1(ii)

$$\leq \sum_{N_1 < n \leq N_2} \frac{1}{n} \sum_{d|n} \lambda_d^+ \left| \sum_{j=1}^R c_j \chi_j(n) \right|^2 = \sum_{j,k=1}^R c_j \overline{c_k} \sum_{d \leq q^\varepsilon} \frac{\lambda_d^+}{d} \chi_j(d) \overline{\chi_k(d)} \sum_{N_1/d < n \leq N_2/d} \frac{\chi_j(n) \overline{\chi_k(n)}}{n}.$$

The diagonal terms with $j = k$ contribute by (3.2), partial summation, and Lemma 3.1(iii)

$$\begin{aligned} \sum_{j=1}^R |c_j|^2 \sum_{\substack{d \leq q^\varepsilon \\ (d, q)=1}} \frac{\lambda_d^+}{d} \sum_{\substack{N_1/d < n \leq N_2/d \\ (n, q)=1}} \frac{1}{n} &= \sum_{j=1}^R |c_j|^2 \sum_{\substack{d \leq q^\varepsilon \\ (d, q)=1}} \frac{\lambda_d^+}{d} \left(\frac{\varphi(q)}{q} \log \frac{N_2}{N_1} + O\left(\frac{\tau(q)d}{N_1}\right) \right) \\ &\ll \sum_{j=1}^R |c_j|^2. \end{aligned}$$

On the other hand, the non-diagonal terms with $j \neq k$ contribute

$$\ll \sum_{\substack{j,k=1 \\ j \neq k}}^R |c_j c_k| \sum_{d \leq q^\varepsilon} \frac{1}{d} \left| \sum_{N_1/d < n \leq N_2/d} \frac{\chi_j(n) \overline{\chi_k(n)}}{n} \right|.$$

By partial summation and the Burgess bound (Lemma 3.2) with $r = 3$, this is

$$\ll R \sum_{j=1}^R |c_j|^2 \sum_{d \leq q^\varepsilon} \frac{1}{d} \frac{q^{1/9+\varepsilon}}{(N_1/d)^{1/3}},$$

and the claim follows. $\square$

Lemma 9.5 below will provide another Halász–Montgomery type mean value theorem.

Remark 3.9. It would be possible to combine the previous three lemmas to obtain bounds for r th moments of character sums over primes with real $r > 2$ in the spirit of what is often done in the transference principle. However we obtain quantitatively stronger results by applying these lemmas directly in the proof of Proposition 5.2 below.

4 A MULTIPLICATIVE TRANSFERENCE PRINCIPLE

4.1 A dense model theorem

Recall the notation

$$[N]_q = \{n \in \mathbb{N} : n \leq N \text{ and } (n, q) = 1\}.$$

The following proposition is a dense model theorem which gives, for an unbounded function $f : [N]_q \rightarrow \mathbb{R}_{\geq 0}$ which is majorized by a pseudorandom measure, a model function $g : \mathbb{Z}_q^\times \rightarrow \mathbb{R}_{\geq 0}$ that is bounded and such that character sums of f and g behave similarly.

Such results originate from the work of Green [6]. The following proposition should be compared with e.g. [7, Proposition 5.1], [19, Theorem 2.1] or [17, Theorem 2.3].

Proposition 4.1 (A multiplicative dense model theorem). *Let $q \in \mathbb{N}$ and $N \geq 2$. Let $r > 1$ be fixed. Let $\eta, \varepsilon \in (0, 1)$, $C \geq 1$, and let*

$$(4.1) \quad \delta \in \left(\left(\frac{10Cr \log \log q}{\varepsilon \log q} \right)^{1/r}, \frac{1}{10} \right).$$

Let $f : [N]_q \rightarrow \mathbb{R}_{\geq 0}$ satisfy:

(A1) *There exists a majorant function $\nu : [N]_q \rightarrow \mathbb{R}_{\geq 0}$ such that $f(n) \leq \nu(n)$ for every $n \in [N]_q$,*

$$|\mathbb{E}_{n \in [N]_q} \nu(n) - 1| \leq \eta, \quad \text{and} \quad \max_{\chi \neq \chi_0} |\mathbb{E}_{n \in [N]_q} \nu(n) \overline{\chi}(n)| \ll q^{-\varepsilon}.$$

(A2) *There are at most $C\delta^{-r}$ characters $\chi \pmod{q}$ such that*

$$|\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n)| \geq \delta.$$

Then there exists a function $g : \mathbb{Z}_q^\times \rightarrow \mathbb{R}_{\geq 0}$ with the following properties.

(i) *For every $a \in \mathbb{Z}_q^\times$, we have*

$$0 \leq g(a) \leq 1 + \eta + O(q^{-\varepsilon/2}).$$

(ii) *We have, for any $\chi \pmod{q}$,*

$$\left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right| \leq \delta.$$

(iii) *We have, for any $\chi \pmod{q}$,*

$$\left| \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right| \leq |\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n)|$$

and

$$\left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right| \leq |\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n)|.$$

(iv) *We have $\mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) = \mathbb{E}_{n \in [N]_q} f(n)$.*

(v) *Let $H \leq \mathbb{Z}_q^\times$ be a subgroup of index $Y < 1/(2\delta)$. Then, for any $b \in \mathbb{Z}_q^\times$, we have*

$$\mathbb{E}_{n \in [N]_q} f(n) \mathbf{1}_{n \in bH} = \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \mathbf{1}_{a \in bH} + O(\delta).$$

Proof. Let

$$T := \{ \chi \pmod{q} : |\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n)| \geq \delta \}$$

be the large spectrum of f , and define the multiplicative Bohr set

$$B := \{ b \in \mathbb{Z}_q^\times : |\chi(b) - 1| \leq \delta/5 \text{ for all } \chi \in T \}.$$

By (A2) we have $|T| \leq C\delta^{-r}$. Let us bound $|B|$ from below similarly to [24, Proof of Lemma 4.20]. Write $T = \{\chi_1, \dots, \chi_k\}$, where χ_j are distinct and $k \leq C\delta^{-r}$. By the pigeonhole principle, there exists a k -tuple $(\xi_1, \dots, \xi_k) \in \mathbb{C}^k$ with $|\xi_i| = 1$ for every i such that, writing

$$A = \{a \in \mathbb{Z}_q^\times : |\chi_j(a) - \xi_j| \leq \delta/10 \text{ for every } j = 1, \dots, k\},$$

we have

$$|A| \geq (100/\delta + 1)^{-k} \varphi(q).$$

But now if $x, y \in A$, then $x/y \in B$. Hence, using (4.1),

$$(4.2) \quad |B| \geq |A| \geq \varphi(q) \exp(-C\delta^{-r} \log(100/\delta + 1)) \geq q^{1-\varepsilon/2}.$$

We define $g: \mathbb{Z}_q^\times \rightarrow \mathbb{R}$ by

$$g(a) := \varphi(q) \mathbb{E}_{b_1, b_2 \in B} \mathbb{E}_{n \in [N]_q} f(n) \mathbf{1}_{n \equiv ab_1 b_2^{-1} \pmod{q}}.$$

Let us now verify the claims (i)–(v).

Claim (i): The lower bound $g(a) \geq 0$ is immediate from the definition of g . By the definition of g , assumption (A1) and orthogonality of characters,

$$\begin{aligned} g(a) &\leq \varphi(q) \mathbb{E}_{b_1, b_2 \in B} \mathbb{E}_{n \in [N]_q} \nu(n) \mathbf{1}_{n \equiv ab_1 b_2^{-1} \pmod{q}} \\ &= \sum_{\chi \pmod{q}} \mathbb{E}_{n \in [N]_q} \nu(n) \overline{\chi}(n) \chi(a) |\mathbb{E}_{b \in B} \chi(b)|^2. \end{aligned}$$

Separating the contribution of the principal character, we obtain

$$g(a) \leq \mathbb{E}_{n \in [N]_q} \nu(n) + O \left(\max_{\chi \neq \chi_0} |\mathbb{E}_{n \in [N]_q} \nu(n) \overline{\chi}(n)| \sum_{\chi \pmod{q}} |\mathbb{E}_{b \in B} \chi(b)|^2 \right).$$

By the assumption (A1), Lemma 3.6, and (4.2), we obtain

$$g(a) \leq 1 + \eta + O \left(\frac{q^{1-\varepsilon}}{|B|} \right) \leq 1 + \eta + O(q^{-\varepsilon/2}).$$

Claim (ii): Changing the order of summation and using the orthogonality of characters, we see that

$$\begin{aligned} \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) &= \mathbb{E}_{b_1, b_2 \in B} \mathbb{E}_{a \in \mathbb{Z}_q^\times} \overline{\chi}(a) \varphi(q) \mathbb{E}_{n \in [N]_q} f(n) \mathbf{1}_{n \equiv ab_1 b_2^{-1} \pmod{q}} \\ (4.3) \quad &= \mathbb{E}_{b_1, b_2 \in B} \chi(b_1) \overline{\chi}(b_2) \mathbb{E}_{a \in \mathbb{Z}_q^\times} \overline{\chi}(a) \chi(a) \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \\ &= |\mathbb{E}_{b \in B} \chi(b)|^2 \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n). \end{aligned}$$

Hence

$$(4.4) \quad \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) = \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \left(1 - |\mathbb{E}_{b \in B} \chi(b)|^2 \right).$$

If now $\chi \notin T$, then by (4.4) and the definition of T , we have

$$\left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right| \leq \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \leq \delta.$$

On the other hand, if $\chi \in T$, then for every $b \in B$ we have $|\chi(b) - 1| \leq \delta/5$ and thus by (4.4) and (A1) we obtain

$$\begin{aligned} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right| &\leq \mathbb{E}_{n \in [N]_q} \nu(n) \left| 1 - |\mathbb{E}_{b \in B} \chi(b)|^2 \right| \\ &\leq (1 + \eta) \left(\left(1 + \frac{\delta}{5} \right)^2 - 1 \right). \end{aligned}$$

Since by assumptions of the proposition $\eta < 1$ and $\delta < 1/10$, the last expression is $\leq \delta$ and claim (ii) follows.

Claim (iii): This is immediate from (4.3) and (4.4).

Claim (iv): This follows from (4.3) with $\chi = \chi_0$.

Claim (v): Let

$$D = \{ \chi \pmod{q} : \chi(n) = 1 \text{ for every } n \in H \}.$$

By (2.3)

$$(4.5) \quad \mathbb{E}_{n \in [N]_q} f(n) \mathbf{1}_{n \in bH} - \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \mathbf{1}_{a \in bH} = \frac{1}{Y} \sum_{\chi \in D} \chi(b) \left(\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right)$$

If now $\chi \notin T$, then by (iii) and the definition of T we have

$$\left| \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) \right| \leq \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \leq \delta.$$

On the other hand if $\chi \in T$, then (since $\delta < 1/(2Y)$ and χ takes values in Y th roots of unity) by the definition of B we have $\chi(b) = 1$ for every $b \in B$ and so by (4.3) we have

$$\mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) = \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n).$$

Consequently, in any case

$$\mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) \overline{\chi}(a) = \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) + O(\delta)$$

and the claim (v) follows from inserting this into (4.5). $\square$

5 APPLYING THE TRANSFERENCE PRINCIPLE

Let $\varepsilon > 0$, $N \geq q^{1/2}$, and define

$$(5.1) \quad \theta = \theta(N, q) := \begin{cases} 1 - \varepsilon - \frac{\log q}{4 \log N} & \text{if } q \text{ is cube-free;} \\ 1 - \varepsilon - \frac{\log q}{3 \log N} & \text{otherwise,} \end{cases}$$

and

$$(5.2) \quad \theta_0 = \theta_0(N, q) := 1 - \varepsilon - \frac{\log q}{4 \log N}.$$

Remark 5.1. The only property of $\theta(N, q)$ needed in what follows is that

$$(5.3) \quad \max_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \max_{N^{1-\theta} \leq y \leq N} \frac{1}{y} \left| \sum_{n \leq y} \chi(n) \right| \ll N^{-\varepsilon_0}$$

for some $\varepsilon_0 > 0$. Similarly, $\theta_0(N, q)$ is any exponent such that (5.3) holds with θ_0 in place of θ when the maximum is taken over characters $\chi \pmod{q}$ of bounded order.

The following proposition transfers the problem of studying $E_3(N)$ into a dense setup. We only need a qualitative result for $N \geq q$, but prove a more quantitative result in a larger range which might be helpful for further applications, or for working out a value of α for which $E_3(q^{1-\alpha}) = \mathbb{Z}_q^\times$ for every sufficiently large cube-free $q \in \mathbb{N}$.

Proposition 5.2 (Conclusion of transference). *Let $q \in \mathbb{N}$ be sufficiently large. Let $\kappa > 0$ and $C \geq 1$ be fixed and let $N \in [q^{2/3+\kappa}, q^C]$. Let $\varepsilon > 0$ be sufficiently small but fixed. Then there exists a set $A \subseteq \mathbb{Z}_q^\times$ such that the following hold.*

(i) *We have*

$$|A| \geq \left(\frac{\theta}{2} - \varepsilon\right) \varphi(q).$$

(ii) *For all but $O(\varphi(q)(\log q)^{-\varepsilon/5})$ values of $a \in \mathbb{Z}_q^\times$ we have*

$$(5.4) \quad (\mathbf{1}_A * \mathbf{1}_A)(a) \gg \frac{\varphi(q)}{(\log q)^{1/2-\varepsilon}} \implies a \in E_2(N).$$

(iii) *If $N \geq q^{4/5+\kappa}$, then*

$$(5.5) \quad (\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_A)(a) \gg \frac{\varphi(q)^2}{(\log q)^{1/2-\varepsilon}} \implies a \in E_3(N).$$

(iv) *Assume that $N \geq q$ and let $\alpha_1 \in (2\varepsilon, 1]$. Write $L = \lfloor 1/\alpha_1 \rfloor$. Then*

$$\sum_{\substack{a=pa_1a_2 \\ q^{\alpha_1-\varepsilon} < p \leq q^{\alpha_1} \\ a_1, a_2 \in A}} \frac{1}{p} \gg \frac{\varphi(q)}{(\log q)^{\frac{1}{2L}-\varepsilon}} \implies a \in E_3(N).$$

(v) *For any subgroup $H \leq \mathbb{Z}_q^\times$ of index $Y < \varepsilon^{-1/2}$, A contains $> \varepsilon\varphi(q)$ elements from at least*

$$\left\lceil \left(\frac{\theta_0}{2} - 3\varepsilon^{1/2} \frac{\theta_0}{\theta} \right) Y \right\rceil$$

distinct cosets of H .

(vi) *For any subgroup $H \leq \mathbb{Z}_q^\times$ of index $Y < \varepsilon^{-1/2}$ and any $b \in \mathbb{Z}_q^\times$, we have*

$$(5.6) \quad |A \cap bH| \geq \left(\frac{\theta}{2} \cdot \frac{|E_1(N) \cap bH|}{N/\log N} - \frac{\varepsilon}{5Y} \right) \varphi(q).$$

Proposition 9.6 below adds one more conclusion to this proposition.

Remark 5.3. In the case where q is cube-free and $N = q$, we obtain the bound $|A| \geq (3/8 - 3\varepsilon/2)\varphi(q)$ which is rather good. However, when q is not cube-free, we only obtain that $|A| \geq (1/3 - 3\varepsilon/2)\varphi(q)$ which is problematic — for instance A could be stuck in a single coset of a subgroup of index 3 and we could not deduce Theorem 1.3(i). However, we can actually rule out this scenario by utilizing part (v) of the proposition.

Proof of Proposition 5.2. We let $D = N^\theta$ and $z = N^{\theta/3}$. We shall apply Proposition 4.1 with $r = 2$,

$$(5.7) \quad \delta = \frac{1}{(\log q)^{1/2-\varepsilon/2}},$$

and with $f, \nu: [N]_q \rightarrow \mathbb{R}_{\geq 0}$ defined by

$$(5.8) \quad f(n) := \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \log N \cdot \mathbf{1}_{n \in \mathbb{P}} \mathbf{1}_{n \geq z}$$

and

$$(5.9) \quad \nu(n) := \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \log N \cdot \sum_{\substack{d|n \\ d \leq D}} \lambda_d^+,$$

where λ_d^+ are the upper bound linear sieve weights from Lemma 3.1 with D and z as above (and $s = 3$), so that $f(n) \leq \nu(n)$ for every $n \in [N]_q$.

Now f satisfies Proposition 4.1(A2) for some $C = O(1)$ by Lemma 3.8(i). Let us confirm that ν satisfies Proposition 4.1(A1) for some $\eta = o(1)$. For any character $\chi \pmod{q}$, we have

$$(5.10) \quad \begin{aligned} \mathbb{E}_{n \in [N]_q} \nu(n) \bar{\chi}(n) &= \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \log N \cdot \mathbb{E}_{n \in [N]_q} \bar{\chi}(n) \sum_{\substack{d|n \\ d \leq D}} \lambda_d^+ \\ &= \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \log N \sum_{d \leq D} \lambda_d^+ \bar{\chi}(d) \frac{1}{|[N]_q|} \sum_{m \leq N/d} \bar{\chi}(m). \end{aligned}$$

By the choice of θ , here $N/d \geq q^{1/4+\varepsilon/4}$ when q is cube-free and $N/d \geq q^{1/3+\varepsilon/4}$ otherwise. Hence when $\chi \neq \chi_0$, the Burgess bound (Lemma 3.2) gives that the innermost sum is $O(q^{-2\varepsilon_0} N/d)$ for some $\varepsilon_0 = \varepsilon_0(\varepsilon) > 0$ and thus we have that, for any $\chi \neq \chi_0$,

$$|\widehat{\nu}(\chi)| \ll q^{1-\varepsilon_0}.$$

On the other hand, by (5.10) and (3.2),

$$(5.11) \quad \begin{aligned} \mathbb{E}_{n \in [N]_q} \nu(n) &= \mathbb{E}_{n \in [N]_q} \nu(n) \overline{\chi_0}(n) = \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \cdot \log N \sum_{\substack{d \leq D \\ (d,q)=1}} \lambda_d^+ \frac{1}{|[N]_q|} \sum_{\substack{n \leq N/d \\ (n,q)=1}} 1 \\ &= \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \cdot \log N \frac{1}{N^{\frac{\varphi(q)}{q}} + O(\tau(q))} \sum_{\substack{d \leq D \\ (d,q)=1}} \lambda_d^+ \left(\frac{\varphi(q)N}{qd} + O(\tau(q)) \right) \\ &= \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \log N \sum_{\substack{d \leq D \\ (d,q)=1}} \frac{\lambda_d^+}{d} + O\left(\frac{Dq^\varepsilon \log N}{N} \right). \end{aligned}$$

By Lemma 3.1(iii) and Mertens' theorem,

$$(5.12) \quad \sum_{\substack{d \leq D \\ (d,q)=1}} \frac{\lambda_d^+}{d} = (2e^\gamma + o(1)) \frac{\log z}{\log D} \prod_{\substack{p < z \\ p \nmid q}} \left(1 - \frac{1}{p} \right) = (1 + o(1)) \frac{2}{\theta \log N} \cdot \frac{q}{\varphi(q)}$$

and thus

$$\mathbb{E}_{n \in [N]_q} \nu(n) = 1 + o(1)$$

and Proposition 4.1(A1) holds for some $\eta = o(1)$.

Having established the assumptions, we may now apply Proposition 4.1 with $r = 2$ and δ, f and ν as in (5.7), (5.8) and (5.9). Hence we can find a function $g: \mathbb{Z}_q^\times \rightarrow [0, 1 + o(1)]$ obeying Proposition 4.1(i)–(v). By Proposition 4.1(iv) and the prime number theorem,

$$(5.13) \quad \mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) = \mathbb{E}_{n \in [N]_q} f(n) = \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \log N \cdot \mathbb{E}_{n \in [N]_q} \mathbf{1}_{n \in \mathbb{P}} \mathbf{1}_{n \geq z} = \frac{\theta}{2} + O((\log q)^{-1}).$$

We will constantly use the fact that, by the definition of f , the prime number theorem, and (2.2),

$$(5.14) \quad \frac{1}{|[N]_q|^2} \sum_{n \in [N]_q} f(n)^2 \ll \frac{1}{|[N]_q|^2} \left(\frac{\varphi(q)}{q} \right)^2 N \log N \ll \frac{\log N}{N}.$$

Write

$$(5.15) \quad A := \{a \in \mathbb{Z}_q^\times : |g(a)| \geq \varepsilon/10\}.$$

Now we are ready to establish the claims (i)–(v) of Proposition 5.2.

Claim (i): By Proposition 4.1(i),

$$\mathbb{E}_{a \in \mathbb{Z}_q^\times} g(a) = \frac{1}{\varphi(q)} \left(\sum_{a \in \mathbb{Z}_q^\times \setminus A} g(a) + \sum_{a \in A} g(a) \right) \leq \frac{\varepsilon}{10} + \frac{|A|}{\varphi(q)} (1 + o(1)).$$

Combining this with (5.13) we obtain

$$(5.16) \quad |A| \geq \left(\frac{\theta}{2} - \varepsilon \right) \varphi(q).$$

Claim (iii): Note that definitely $a \in E_3(N)$ if $(f * f * f)(n) > 0$ for some $n \equiv a \pmod{q}$. Now, by orthogonality of characters and Proposition 4.1(iii) we obtain that

$$(5.17) \quad \begin{aligned} & \frac{1}{|[N]_q|^3} \sum_{n \equiv a \pmod{q}} (f * f * f)(n) - \frac{1}{\varphi(q)^3} (g * g * g)(a) \\ &= \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} (\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n))^3 \chi(a) - \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left(\mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right)^3 \chi(a) \\ &= O \left(\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right| \right). \end{aligned}$$

To bound the right-hand side, we split the characters into three sets

$$(5.18) \quad \mathcal{X}_1 = \left\{ \chi \pmod{q} : \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \leq \frac{1}{N^{1/4}} \right\},$$

$$(5.19) \quad \mathcal{X}_2 = \left\{ \chi \pmod{q} : \frac{1}{N^{1/4}} < \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \leq \frac{q^{1/4+\kappa}}{N^{1/2}} \right\},$$

and

$$(5.20) \quad \mathcal{X}_3 = \left\{ \chi \pmod{q} : \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| > \frac{q^{1/4+\kappa}}{N^{1/2}} \right\}.$$

By the definition of $\mathcal{X}_1$, Proposition 4.1(iii), Lemma 3.6 and (5.14), we see that

$$\begin{aligned}
 (5.21) \quad & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_1} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \bar{\chi}(b) \right| \\
 & \leq \frac{1}{\varphi(q)} \frac{1}{N^{1/4}} \sum_{\chi \pmod{q}} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \\
 & \ll \frac{1}{\varphi(q)} \frac{1}{N^{1/4}} (N + \varphi(q)) \frac{\log N}{N} \ll \frac{q^\kappa}{N^{1/4}q} + \frac{q^\kappa}{N^{5/4}}.
 \end{aligned}$$

This is $O(1/q^{1+\kappa/4})$ when $N \geq q^{4/5+\kappa}$.

On the other hand, by the definition of $\mathcal{X}_3$, Lemma 3.8(i) with $\varepsilon = \kappa/2$ and (5.14),

$$\left(\frac{q^{1/4+\kappa}}{N^{1/2}} \right)^2 |\mathcal{X}_3| \leq \sum_{\chi \in \mathcal{X}_3} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \ll \left(\frac{N}{\log q} + q^{1/2+\kappa} |\mathcal{X}_3| \right) \frac{\log N}{N}.$$

Now the second term cannot dominate and so

$$(5.22) \quad \sum_{\chi \in \mathcal{X}_3} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \ll 1.$$

Combining this with Proposition 4.1(ii), we obtain

$$(5.23) \quad \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_3} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \bar{\chi}(b) \right| \ll \frac{\delta}{\varphi(q)}.$$

To deal with $\mathcal{X}_2$, we write, for $\delta_0 \in [N^{-1/4}, q^{1/4+\kappa}/N^{1/2}]$,

$$(5.24) \quad \mathcal{X}_{2,\delta_0} := \{ \chi \pmod{q} : \delta_0 < |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)| \leq 2\delta_0 \}.$$

If we can show that, for any $\delta_0 \in [N^{-1/4}, q^{1/4+\kappa}/N^{1/2}]$, we have

$$(5.25) \quad |\mathcal{X}_{2,\delta_0}| \ll \frac{\delta_0^{-3}}{(\log q)^{10}},$$

then we obtain using also Proposition 4.1(iii) that

$$\begin{aligned}
 (5.26) \quad & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_2} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \bar{\chi}(b) \right| \\
 & \ll \frac{1}{\varphi(q)} (\log q) \max_{\delta_0 \in [N^{-1/4}, q^{1/4+\kappa}/N^{1/2}]} \sum_{\chi \in \mathcal{X}_{2,\delta_0}} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^3 \ll \frac{1}{\varphi(q) (\log q)^9}.
 \end{aligned}$$

Now (5.25) follows for $\delta_0 \in [N^{-1/4}, q^{1/4+\kappa}/N^{1/2}]$ and $N \geq q^{4/5+\kappa}$ since Lemma 3.7 implies that

$$(5.27) \quad |\mathcal{X}_{2,\delta_0}| \ll \delta_0^{-2} (\log q)^7 + \delta_0^{-6} q N^{-2} (\log q)^{21}.$$

Using (5.21), (5.23), and (5.26) on the right-hand side of (5.17), we obtain

$$(5.28) \quad \frac{1}{|[N]_q|^3} \sum_{n \equiv a \pmod{q}} (f * f * f)(n) = \frac{1}{\varphi(q)^3} (g * g * g)(a) + O\left(\frac{\delta}{\varphi(q)}\right).$$

By the definitions of f and δ and (5.28) we obtain that $a \in E_3(N)$ if

$$(g * g * g)(a) \gg \frac{\varphi(q)^2}{(\log q)^{1/2-\varepsilon}}.$$

But this obviously holds if $(\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_A)(a) \gg \varphi(q)^2 (\log q)^{-1/2+\varepsilon}$.

Claim (ii): Now definitely $a \in E_2(N)$ if $(f * f)(n) > 0$ for some $n \equiv a \pmod{q}$. By the orthogonality of characters

$$(5.29) \quad \begin{aligned} & \frac{1}{|[N]_q|^2} \sum_{n \equiv a \pmod{q}} (f * f)(n) - \frac{1}{\varphi(q)^2} (g * g)(a) \\ &= \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left(\left(\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right)^2 - \left(\mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right)^2 \right) \chi(a). \end{aligned}$$

By orthogonality of characters and Proposition 4.1(iii),

$$(5.30) \quad \begin{aligned} & \sum_{a \in \mathbb{Z}_q^\times} \left| \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left(\left(\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right)^2 - \left(\mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right)^2 \right) \chi(a) \right|^2 \\ &= \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \left(\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right)^2 - \left(\mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right)^2 \right|^2 \\ &\ll \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right|^2. \end{aligned}$$

We split the characters into three sets $\mathcal{X}_1 \cup \mathcal{X}_2 \cup \mathcal{X}_3$ as in (5.18), (5.19), and (5.20). By the definition of $\mathcal{X}_1$, Proposition 4.1(iii), Lemma 3.6, and (5.14) we see that

$$(5.31) \quad \begin{aligned} & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_1} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right|^2 \\ &\leq \left(\frac{1}{N^{1/4}} \right)^2 \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \\ &\ll \frac{1}{N^{1/2} \varphi(q)} (N + \varphi(q)) \frac{\log N}{N} \ll \frac{\log N}{N^{1/2} \varphi(q)} + \frac{\log N}{N^{3/2}}. \end{aligned}$$

This is $O(1/q^{1+\kappa/2})$ when $N \geq q^{2/3+\kappa}$. On the other hand, recall that by (5.22)

$$\sum_{\chi \in \mathcal{X}_3} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \ll 1.$$

Combining this with Proposition 4.1(ii), we obtain

$$(5.32) \quad \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_3} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right|^2 \ll \frac{\delta^2}{\varphi(q)}.$$

To deal with $\mathcal{X}_2$, we recall the definition of $\mathcal{X}_{2,\delta_0}$ from (5.24). If we can show that, for any $\delta_0 \in [N^{-1/4}, q^{1/4+\kappa}/N^{1/2}]$, we have

$$(5.33) \quad |\mathcal{X}_{2,\delta_0}| \ll \frac{\delta_0^{-4}}{(\log q)^{10}},$$

then we obtain using also Proposition 4.1(iii) that

$$(5.34) \quad \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_2} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right|^2 \ll \frac{1}{\varphi(q)(\log q)^9}.$$

Now (5.33) follows for $\delta_0 \in [N^{-1/4}, q^{1/4+\kappa}/N^{1/2}]$ and $N \geq q^{2/3+\kappa}$ from (5.27).

Combining (5.31), (5.32), and (5.34), we obtain

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right|^2 \ll \frac{\delta^2}{\varphi(q)}.$$

This together with (5.29) and (5.30) implies

$$(5.35) \quad \frac{1}{|[N]_q|^2} \sum_{n \equiv a \pmod{q}} (f * f)(n) = \frac{1}{\varphi(q)^2} (g * g)(a) + O\left(\frac{\delta^{1-\varepsilon/2}}{\varphi(q)}\right)$$

for all but $O(\delta^{\varepsilon/2} \varphi(q))$ elements $a \in \mathbb{Z}_q^\times$. Now

$$\frac{1}{\varphi(q)^2} (g * g)(a) + O\left(\frac{\delta^{1-\varepsilon/2}}{\varphi(q)}\right) \geq \frac{\varepsilon^2}{\varphi(q)^2} (\mathbf{1}_A * \mathbf{1}_A)(a) + O\left(\frac{\delta^{1-\varepsilon/2}}{\varphi(q)}\right)$$

and claim (ii) follows recalling the definition of δ .

Claim (iv): Let $f_0: [N]_q \rightarrow \mathbb{R}_{\geq 0}$ be defined through

$$f_0(n) = \frac{\mathbf{1}_{n \in \mathbb{P} \cap (q^{\alpha_1 - \varepsilon}, q^{\alpha_1}]}}{n}.$$

Note that definitely $a \in E_3(N)$ if $(f * f * f_0)(n) > 0$ for some $n \equiv a \pmod{q}$. Now by orthogonality of characters and Proposition 4.1(iii) (abusing the notation to consider f_0 as a function from $\mathbb{Z}_q^\times$ when convolved with g),

$$(5.36) \quad \begin{aligned} & \frac{1}{|[N]_q|^2} \sum_{n \equiv a \pmod{q}} (f * f * f_0)(n) - \frac{1}{\varphi(q)^2} (g * g * f_0)(a) \\ &= \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left(\left(\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right)^2 - \left(\mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right)^2 \right) \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \chi(a) \\ &= O\left(\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right| \right. \\ & \quad \left. \cdot \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right| \right). \end{aligned}$$

When considering the right-hand side, we split the characters into two sets

$$\mathcal{X}_1 = \left\{ \chi \pmod{q} : \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right| < (\log q)^{-10} \right\}$$

and

$$\mathcal{X}_2 = \left\{ \chi \pmod{q} : \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right| \geq (\log q)^{-10} \right\}.$$

By the definition of $\mathcal{X}_1$, Proposition 4.1(iii), Lemma 3.6, and (5.14), we see that

(5.37)

$$\begin{aligned} & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_1} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right| \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right| \\ & \ll (\log q)^{-10} \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \\ & \ll (\log q)^{-10} \frac{1}{\varphi(q)} (N + \varphi(q)) \frac{\log N}{N} \ll \frac{1}{\varphi(q) (\log q)^9}. \end{aligned}$$

Recall that $L = \lfloor 1/\alpha_1 \rfloor$. By Proposition 4.1(ii,iii) and Hölder's inequality, we obtain

(5.38)

$$\begin{aligned} & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_2} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right| \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right| \\ & \ll \delta^{1/L} \frac{1}{\varphi(q)} \left(\sum_{\chi \in \mathcal{X}_2} \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right|^{2L} \right)^{\frac{1}{2L}} \left(\sum_{\chi \in \mathcal{X}_2} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right|^2 \right)^{1 - \frac{1}{2L}}. \end{aligned}$$

Recall we assume that ε is sufficiently small. Then $[L(\alpha_1 - \varepsilon), L\alpha_1] \subseteq [3/8, 1]$. We obtain by the definition of $\mathcal{X}_2$, Lemma 3.8(ii), and Mertens' theorem that

$$\begin{aligned} ((\log q)^{-10})^{2L} |\mathcal{X}_2| & \leq \sum_{\chi \in \mathcal{X}_2} \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right|^{2L} \\ & = \sum_{\chi \in \mathcal{X}_2} \left| \sum_{q^{L(\alpha_1 - \varepsilon)} < n \leq q^{L\alpha_1}} \left(\sum_{\substack{n=p_1 \cdots p_L \\ q^{\alpha_1 - \varepsilon} < p_1, \dots, p_L \leq q^{\alpha_1}}} 1 \right) \frac{\overline{\chi}(n)}{n} \right|^2 \\ & \leq \left(1 + q^{1/9 + 3\varepsilon - 1/8} |\mathcal{X}_2| \right) \sum_{\substack{n \leq q \\ (n, P(q^{\alpha_1 - \varepsilon})) = 1}} \frac{\tau_L(n)^2}{n} \\ & \ll (1 + q^{-1/100} |\mathcal{X}_2|) \prod_{q^{\alpha_1 - \varepsilon} \leq p \leq q} \left(1 + \frac{L^2}{p} \right) \ll 1 + q^{-1/100} |\mathcal{X}_2|. \end{aligned}$$

Now the second term cannot dominate, and so $|\mathcal{X}_2| \ll (\log q)^{20L}$ and

$$\sum_{\chi \in \mathcal{X}_2} \left| \sum_{n \in [N]_q} f_0(n) \overline{\chi}(n) \right|^{2L} \ll 1.$$

Applying also Lemma 3.8(i), we see that (5.38) is $\ll \delta^{\frac{1}{L}}/\varphi(q)$. Combining this with (5.37) we obtain from (5.36) that

$$(5.39) \quad \frac{1}{|[N]_q|^2} \sum_{n \equiv a \pmod{q}} (f * f * f_0)(n) = \frac{1}{\varphi(q)^2} (g * g * f_0)(a) + O\left(\frac{\delta^{\frac{1}{L}}}{\varphi(q)}\right),$$

where we still have abused the notation by considering on the right-hand side f_0 as a function from $\mathbb{Z}_q^\times$.

By the definitions of f and f_0 and (5.39) we obtain that $a \in E_3(N)$ if

$$(g * g * f_0)(a) \gg \varphi(q) \delta^{1/L - \varepsilon/4},$$

and the claim follows by the definitions of A and δ .

Remark 5.4. The reason we needed to use logarithmic averaging in Proposition 5.2(iv) is that when $\alpha_1 < 1/3 + \varepsilon$, we cannot apply Halász–Montgomery type results without losses without logarithmic averaging. In this range, in order to make the Burgess bound applicable, we need to take higher than second moment of the character sum, and we cannot use a sieve to find a correct order of magnitude sieve majorant for example for the characteristic function of integers of the form $n = p_1 p_2$ with $p_j \sim q^{\alpha_1}$.

Claim (v): Let $H \leq \mathbb{Z}_q^\times$ be a subgroup of index $Y < \varepsilon^{-1/2}$, and let $b_1 H, \dots, b_K H$ be all the distinct cosets of H from which A contains at least $\varepsilon \varphi(q)$ elements, and let $c_1 H, \dots, c_{Y-K} H$ be the remaining distinct cosets. Thanks to Proposition 4.1(v), the definition of f , and Lemma 3.3, we have, for any $j \in \{1, \dots, K\}$

$$(5.40) \quad \begin{aligned} \frac{1}{\varphi(q)} \sum_{a \in b_j H} g(a) &= \mathbb{E}_{n \in [N]_q} \mathbf{1}_{n \in b_j H} f(n) + O(\delta) \\ &= \frac{\theta}{2} \cdot \frac{\varphi(q)}{q} \log N \frac{1}{|[N]_q|} \sum_{\substack{z \leq p \leq N \\ p \in b_j H}} 1 + O(\delta) \leq (1 + o(1)) \frac{\theta}{Y \theta_0}, \end{aligned}$$

recalling that $\delta = o(1)$. On the other hand, for any $j \in \{1, \dots, Y - K\}$ we have by Proposition 4.1(i) and (5.15) (using also $\varepsilon \leq \varepsilon^{1/2}/Y$)

$$\begin{aligned} \frac{1}{\varphi(q)} \sum_{a \in c_j H} g(a) &= \frac{1}{\varphi(q)} \sum_{a \in A \cap c_j H} g(a) + \frac{1}{\varphi(q)} \sum_{a \in A^c \cap c_j H} g(a) \\ &\leq \frac{1}{\varphi(q)} \cdot \varepsilon \varphi(q) \cdot \left(1 + \frac{\varepsilon}{10}\right) + \frac{1}{\varphi(q)} \cdot \frac{\varphi(q)}{Y} \cdot \frac{\varepsilon}{10} \leq \frac{2\varepsilon^{1/2}}{Y}. \end{aligned}$$

Combining these with (5.13), we obtain that

$$\frac{\theta}{2} \leq (1 + o(1)) K \frac{\theta}{Y \theta_0} + 2\varepsilon^{1/2} \varphi(q) + o(1),$$

and the claim follows.

Claim (vi): The definition of f , Proposition 4.1(v, i), and the definition of A imply that

$$\begin{aligned} \frac{\theta}{2} \frac{|E_1(N) \cap bH|}{N/\log N} &= \frac{1}{\varphi(q)} \sum_{a \in bH} g(a) + o(1) = \frac{1}{\varphi(q)} \sum_{a \in A \cap bH} g(a) + \frac{1}{\varphi(q)} \sum_{a \in A^c \cap bH} g(a) + o(1) \\ &\leq \left(1 + \frac{\varepsilon}{20}\right) \frac{|A \cap bH|}{\varphi(q)} + \frac{\varepsilon}{10Y} + o(1) \leq \frac{|A \cap bH|}{\varphi(q)} + \frac{\varepsilon}{5Y}, \end{aligned}$$

and (5.6) follows. $\square$

6 PRODUCTS SETS

6.1 Reduction from popular products to product sets

In the notation of Proposition 5.2, we have reduced the study of $E_3(q)$ to getting a lower bound of the form $(\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_A)(a) \gg \varphi(q)^2$ for all $a \in \mathbb{Z}_q^\times$. If instead it sufficed just to show that $a \in A \cdot A \cdot A$, we could apply Kneser's theorem (Lemma 3.5). However, we need that a has many representations as a product of three elements of A . Fortunately, the following lemma which is a quick consequence of work of Gryniewicz [8] allows us to essentially reduce to studying $A \cdot A \cdot A$.

Lemma 6.1. *Let $t \geq u \geq 1$ be integers. Let A, B be finite subsets of a finite abelian group G with $|A|, |B| \geq t$. Then at least one of the following holds.*

(a) *We have*

$$(\mathbf{1}_A * \mathbf{1}_B)(a) \geq u$$

for at least

$$|A| + |B| - 2t - \frac{u|G|}{t}$$

values of $a \in G$.

(b) *There exist subsets $A' \subseteq A, B' \subseteq B$ with*

$$|A \setminus A'| + |B \setminus B'| \leq t - 1$$

such that

$$(\mathbf{1}_A * \mathbf{1}_B)(a) \geq t$$

for every $a \in A' \cdot B'$.

Proof. Let $N_i(A, B)$ denote the set of $c \in G$ such that c has at least i representations as ab with $a \in A, b \in B$. Then by [8, Theorem 1.1] either (b) holds, or we have

$$(6.1) \quad \sum_{i=1}^t |N_i(A, B)| \geq t(|A| + |B| - 2t) + 1.$$

If (6.1) holds, then we trivially also have

$$\sum_{i=u}^t |N_i(A, B)| \geq t(|A| + |B| - 2t) - u|G|.$$

Since $|N_u(A, B)| \geq |N_t(A, B)|$ for $t \geq u$, we conclude that

$$|N_u(A, B)| \geq \frac{1}{t} \sum_{i=u}^t |N_i(A, B)| \geq |A| + |B| - 2t - \frac{u|G|}{t}.$$

The claim (a) follows, since for each $a \in N_u(A, B)$ we have $(\mathbf{1}_A * \mathbf{1}_B)(a) \geq u$. $\square$

Next we combine the previous lemma with Proposition 5.2 to obtain criteria about when $a \in E_j(N)$.

Proposition 6.2 (Criteria on sizes of $E_2(N)$ and $E_3(N)$). *Let $\kappa, \varepsilon > 0$ and $C \geq 1$ be fixed. Let $q \in \mathbb{N}$ be large in terms of κ, ε , and let $N \in [q^{2/3+\kappa}, q^C]$. Let θ and θ_0 be as in (5.1) and (5.2). Then at least one of the following holds:*

(a) *We have $|E_2(N)| \geq (\theta - 2\varepsilon)\varphi(q)$. If $\theta > 2/3 + 3\varepsilon$, then we also have $E_3(N) = \mathbb{Z}_q^\times$.*

(b) *There exist sets $A', B' \subseteq \mathbb{Z}_q^\times$ such that the following hold.*

(b.i)

$$|A'|, |B'| \geq (\theta/2 - 3\varepsilon/2)\varphi(q).$$

(b.ii)

$$|(A' \cdot B') \cap E_2(N)| \geq |A' \cdot B'| - \varepsilon\varphi(q),$$

(b.iii) *If $N \geq q^{4/5+\kappa}$, then*

$$(\mathbf{1}_{A' \cdot B'} * \mathbf{1}_{A'})(a) \gg \varphi(q) \implies a \in E_3(N).$$

(b.iv) *Assume that $N \geq q$ and let $\alpha_1 \in (2\varepsilon, 1]$. Write $L = \lfloor 1/\alpha_1 \rfloor$. Then*

$$\sum_{\substack{cp \equiv a \pmod{q} \\ q^{\alpha_1 - \varepsilon} < p \leq q^{\alpha_1} \\ c \in A' \cdot B'}} \frac{1}{p} \gg 1 \implies a \in E_3(N).$$

(b.v) *For any subgroup $H \leq \mathbb{Z}_q^\times$ of index $Y \leq \varepsilon^{-1/2}$, $A' \cap B'$ contains at least $\frac{\varepsilon}{2}\varphi(q)$ elements from at least $\lceil (\theta_0/2 - 3\varepsilon^{1/2}\theta_0/\theta)Y \rceil$ cosets of H .*

(b.vi) *For any $b \in \mathbb{Z}_q^\times$, we have*

$$|A' \cap B' \cap bH| \geq \left(\frac{\theta}{2} \cdot \frac{|E_1(N) \cap bH|}{N/\log N} - \frac{\varepsilon}{3} \right) \varphi(q).$$

Proposition 8.3 below adds one more conclusion to part (b) of this proposition.

Proof of Proposition 6.2. We may assume that $\varepsilon > 0$ is small enough. Let A be as in Proposition 5.2. Note that $|A| \geq (\theta/2 - \varepsilon)\varphi(q)$. We apply Lemma 6.1 with $t = \lceil \varepsilon\varphi(q)/10 \rceil$ and $u = \lfloor \varepsilon^2\varphi(q)/1000 \rfloor$, and with A and B in the lemma both equalling the set A .

If Lemma 6.1(a) holds, then the first part of Proposition 6.2(a) holds by Proposition 5.2(ii) and the second part of Proposition 6.2(a) holds by Proposition 5.2(iii) and Lemma 3.4(i) applied with $\{a \in \mathbb{Z}_q^\times : (\mathbf{1}_A * \mathbf{1}_A)(a) \geq u\}$ in place of A and A in place of B .

Let us now show that if Lemma 6.1(b) holds then (b.i)–(b.vi) hold. Now (b.i) follows immediately and (b.ii) holds by Proposition 5.2(ii) since $A', B' \subseteq A$ and

$$(6.2) \quad c \in A' \cdot B' \implies \mathbf{1}_A * \mathbf{1}_A(c) \geq \varepsilon\varphi(q)/10.$$

Moreover, we have (b.iii) by Proposition 5.2(iii) and the estimate

$$\begin{aligned} (\mathbf{1}_{A' \cdot B'} * \mathbf{1}_{A'})(a) &= \sum_{c \in A' \cdot B'} \mathbf{1}_{A' \cdot B'}(c) \mathbf{1}_{A'}(ac^{-1}) \ll \frac{1}{\varphi(q)} \sum_{c \in A' \cdot B'} (\mathbf{1}_A * \mathbf{1}_A)(c) \mathbf{1}_{A'}(ac^{-1}) \\ &\leq \frac{\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_A(a)}{\varphi(q)}. \end{aligned}$$

Claim (b.iv) follows similarly from Proposition 5.2(iv).

Since

$$(6.3) \quad |A \setminus A'| + |A \setminus B'| \leq \frac{\varepsilon}{10} \varphi(q),$$

Claim (b.v) follows from Proposition 5.2(v) and (b.vi) follows from Proposition 5.2(vi). $\square$

6.2 Structure of sets with small doubling

In this subsection we provide a consequence of Kneser's theorem which tells us about the structure of A and B in case $A \cdot B$ is small. The following lemma is quite similar to parts of [1, Section 4] and [23, Lemma 3].

Lemma 6.3. *Let $\alpha, \alpha', \beta \in (0, 1]$ be such that $\beta < 2\alpha \leq 2\alpha'$, and let $A, B \subseteq \mathbb{Z}_q^\times$ with $|A|, |B| \geq \alpha\varphi(q)$. Assume that A and B each meet at least proportion α' of cosets of any subgroup $H_0 \leq \mathbb{Z}_q^\times$ of order $< 1/(2\alpha - \beta)$. Then at least one of the following holds.*

(a) *We have*

$$|A \cdot B| \geq \beta\varphi(q).$$

(b) *Write $H \leq \mathbb{Z}_q^\times$ for the stabilizer of $A \cdot B$ and write Y for its index. Then the following hold.*

(b.i) *We have*

$$1 < Y < \frac{1}{2\alpha' - \beta}.$$

(b.ii) *If $\alpha' > 1/3$ and $\beta \leq 2/3$, then $Y = 3k + 2$ for some integer k with*

$$(6.4) \quad \frac{k+1}{3k+2} \geq \alpha',$$

and each of A and B intersects exactly $k+1$ cosets of H , and $A \cdot B$ is the union of $2k+1$ cosets (mod H).

(b.iii) *If, for some small enough $\varepsilon > 0$, we have $\alpha' \geq \frac{3}{8} - \varepsilon$ and $\beta < \frac{11}{16} - 2\varepsilon$, then $Y = 3k+2$ for some integer $k \in \{0, 1, 2\}$, and each of A and B intersects exactly $k+1$ cosets of H , and $A \cdot B$ is the union of $2k+1$ cosets (mod H).*

Proof. If $Y = 1$, then $A \cdot B = \mathbb{Z}_q^\times$ and (a) holds. Assume henceforth that $Y > 1$. By Kneser's theorem (Lemma 3.5)

$$|A \cdot B| \geq |A \cdot H| + |B \cdot H| - |H| \geq |A| + |B| - |H| \geq \left(2\alpha - \frac{1}{Y}\right) \varphi(q).$$

We see that either (a) holds or

$$1 < Y < \frac{1}{2\alpha - \beta}.$$

By assumption, this implies that each of A and B meets at least proportion α' of cosets of H . Hence actually

$$(6.5) \quad |A \cdot B| \geq |A \cdot H| + |B \cdot H| - |H| \geq (2 \lceil \alpha' Y \rceil - 1) |H| \geq \left(2\alpha' - \frac{1}{Y}\right) \varphi(q)$$

and so either (a) holds or (b.i) holds.

We may suppose from now on that (b.i) holds. Then using the second inequality in (6.5), we obtain in this case

$$(6.6) \quad |A \cdot B| \geq (2 \lceil \alpha' Y \rceil - 1) |H| = \frac{2 \lceil \alpha' Y \rceil - 1}{Y} \varphi(q).$$

If $\alpha' > 1/3$ and $\beta \leq 2/3$, then if Y is not $2 \pmod{3}$, we have

$$\lceil \alpha' Y \rceil = \left\lceil \frac{Y}{3} + \left(\alpha' - \frac{1}{3} \right) Y \right\rceil \geq \frac{Y}{3} + \frac{2}{3},$$

so we obtain by (6.6)

$$|A \cdot B| \geq \left(\frac{2Y}{3} + \frac{4}{3} - 1 \right) \frac{\varphi(q)}{Y} > \frac{2}{3} \varphi(q) \geq \beta \varphi(q),$$

so (a) holds.

If instead $\alpha' \geq 3/8 - \varepsilon$ and $\beta < 11/16 - 2\varepsilon$ with $\varepsilon > 0$ small, then (b.i) gives $Y < 16$. Moreover, by a case check we see that

$$\frac{2\lceil \alpha' Y \rceil - 1}{Y} \geq \frac{11}{16}$$

for all $Y \in \{1, \dots, 15\}$ that are not of the form $Y = 3k + 2$ with $k \in \{0, 1, 2\}$. Hence, if Y is not of this form, then (6.6) implies that (a) holds.

We may henceforth assume that $Y = 3k + 2$ for some $k \in \mathbb{N}$ if $\alpha' > 1/3$ and $\beta \leq 2/3$, and that $Y = 3k + 2$ with $k \in \{0, 1, 2\}$ if $\alpha' \geq 3/8 - \varepsilon$ and $\beta < 11/16 - 2\varepsilon$. Now A and B must each intersect at least

$$\lceil \alpha' Y \rceil \geq \left\lceil \frac{1}{3}(3k + 2) \right\rceil \geq k + 1$$

cosets of H . If A intersects $\geq k + 2$ cosets of H , then $|A \cdot H| \geq (k + 2)|H|$, so by the first inequality of (6.5) we have

$$|A \cdot B| \geq (k + 2 + k + 1 - 1) |H| = (2k + 2) \frac{\varphi(q)}{3k + 2},$$

and now (a) holds since $(2k + 2)/(3k + 2) > 2/3$ for all $k \in \mathbb{N}$ and $(2k + 2)/(3k + 2) > 11/16$ for $k \in \{0, 1, 2\}$. Using symmetry, we may assume that each of A and B intersects exactly $k + 1$ cosets.

Now since

$$|A \cdot B| \geq |A \cdot H| + |B \cdot H| - |H| = (2k + 1)|H|,$$

we see that $A \cdot B$ must intersect (and hence consist of) at least $2k + 1$ cosets of H . If $A \cdot B$ is the union of at least $2k + 2$ cosets of H , then we have

$$|A \cdot B| \geq (2k + 2)|H| \geq 2|A| \geq 2\alpha\varphi(q) > \beta\varphi(q)$$

and (a) holds.

Hence if (a) does not hold, then A and B must each be contained in $k + 1$ cosets of H and $A \cdot B$ must be the union of $2k + 1$ cosets of H . Finally, we have (6.4) by the assumption that A meets at least proportion α' of cosets of an index Y subgroup. $\square$

We shall also use the following which is [23, Lemma 4].

Lemma 6.4. *Let G be an abelian group of order $3k + 2$ for some integer $k \geq 0$. Let $B \subseteq G$ with $|B| = k + 1$. Assume that $B \cdot B = G \setminus B$ and that the stabilizer of $B \cdot B$ is the identity. Then G is cyclic and for some $g \in G$ which generates G we have $B = \{g^{k+1}, \dots, g^{2k+1}\}$.*

7 PRIMES IN COSETS OF INDICES 5 AND 8

In order to deal with the case that Lemma 6.3(b) holds, we need to have information on the distribution of primes in cosets of $\mathbb{Z}_q^\times$ of index $3k + 2$ for small k ($k \in \{0, 1, 2\}$ suffices for us). We can obtain lower bounds for the logarithmic density of primes in certain collections of such cosets.

Lemma 7.1 (Positive logarithmic density of primes in some unions of cosets). *Let $q \in \mathbb{N}$ be large, let $k \in \{1, 2\}$ and let H be a subgroup of index $3k + 2$ such that $\mathbb{Z}_q^\times/H$ is cyclic and generated by gH with $g \in \mathbb{Z}_q^\times$. Then*

$$(7.1) \quad \sum_{\substack{p \leq q \\ p \notin \bigcup_{j=1}^{k+1} g^{k+j}H}} \frac{\log p}{p} \geq \frac{1}{1000} \log q.$$

In the proof of this lemma we use the following lemma which is [23, Proposition 6] and is based on [9, Lemmas 5.2–5.3]. Also Szabó [23] used it in a similar context.

Lemma 7.2. *Let $q \in \mathbb{N}$ and $\alpha \in \mathbb{R}_{>0}$. Let $f: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ be defined as*

$$f(t) = \begin{cases} \alpha - t & \text{if } 0 \leq t \leq \alpha; \\ 0 & \text{if } t > \alpha. \end{cases}$$

(i) *If χ is a non-principal character (mod q) of bounded order, then*

$$\operatorname{Re} \sum_p \frac{\chi(p) \log p}{p} f\left(\frac{\log p}{\log q}\right) \leq \left(\frac{\alpha}{8} + o(1)\right) \log q.$$

(ii) *We have*

$$\sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right) = \left(\frac{\alpha^2}{2} + o(1)\right) \log q.$$

Proof of Lemma 7.1. Let $J = 2$ if $k = 1$ and $J = 4$ if $k = 2$. Let $\alpha = 1$ in Lemma 7.2. For $j = 0, \dots, J$, we define

$$\beta_j := \frac{\sum_{p \in g^j H \cup g^{-j} H} \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right)}{\sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right)}.$$

Trivially

$$(7.2) \quad \beta_j \in [0, 1] \text{ for each } j = 0, \dots, J \text{ and } \sum_{j=0}^J \beta_j = 1.$$

Let us first consider the case $k = 1$, so that $J = 2$. If (7.1) does not hold, then

$$\sum_{\substack{p \leq q \\ p \notin g^2 H \cup g^3 H}} \frac{\log p}{p} < \frac{1}{1000} \log q.$$

Hence by definition of β_j and Lemma 7.2(ii) we have $\beta_0 + \beta_1 \leq (2 + o(1)) \cdot \frac{1}{1000}$, and consequently (7.2) implies that $\beta_2 \geq \frac{499}{500} - o(1)$. Let χ be the character (mod q) for which

$\chi(g) = e(2/5)$ and $\chi(h) = 1$ for every $h \in H$. Then, since $\cos(0) > \cos(2\pi/5) > 0 > \cos(4\pi/5)$, we have

$$\begin{aligned} & \operatorname{Re} \sum_p \frac{\chi(p) \log p}{p} f\left(\frac{\log p}{\log q}\right) \\ &= \left(\beta_0 + \beta_1 \cos\left(\frac{4\pi}{5}\right) + \beta_2 \cos\left(\frac{2\pi}{5}\right) \right) \sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right) \\ &\geq \left(\frac{1}{500} \cos\left(\frac{4\pi}{5}\right) + \frac{499}{500} \cos\left(\frac{2\pi}{5}\right) - o(1) \right) \sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right). \end{aligned}$$

Applying Lemma 7.2(i) to the left-hand side and Lemma 7.2(ii) to the right-hand side, we obtain

$$\frac{1}{8} \geq \left(\frac{499}{500} \cos\left(\frac{2\pi}{5}\right) + \frac{1}{500} \cos\left(\frac{4\pi}{5}\right) \right) \frac{1}{2} - o(1) = 0.153\dots + o(1).$$

But this is not true, and we have obtained a contradiction.

Let us now turn to the case $k = 2$. If (7.1) does not hold, then

$$\sum_{\substack{p \leq q \\ p \notin g^3 H \cup g^4 H \cup g^5 H}} \frac{\log p}{p} < \frac{1}{1000} \log q.$$

Hence, by definition of β_j and Lemma 7.2(ii),

$$(7.3) \quad \beta_0 + \beta_1 + \beta_2 \leq 2 \cdot \frac{1}{1000} + o(1).$$

Let now χ be the character (mod q) for which $\chi(g) = e(1/8)$ and $\chi(h) = 1$ for every $h \in H$. By the definitions of β_j and Lemma 7.2(ii) we obtain

$$\begin{aligned} & \operatorname{Re} \sum_p \frac{\chi(p)^2 \log p}{p} f\left(\frac{\log p}{\log q}\right) = (\beta_0 + \beta_4 - \beta_2) \sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right) \\ &\geq \left(\beta_4 - \frac{1}{500} + o(1) \right) \sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right) = \left(\frac{\beta_4}{2} - \frac{1}{1000} + o(1) \right) \log q. \end{aligned}$$

Applying Lemma 7.2(i) to the left-hand side, we obtain $\beta_4 \leq \frac{1}{4} + \frac{1}{500} + o(1)$, and consequently by (7.2) and (7.3) we must have $\beta_3 \geq \frac{3}{4} - \frac{1}{250} + o(1)$.

On the other hand, using the definition of β_j and our bounds for β_j , we obtain

$$\begin{aligned} & \operatorname{Re} \sum_p \frac{\chi(p)^3 \log p}{p} f\left(\frac{\log p}{\log q}\right) = \left(\beta_0 - \beta_1 \frac{1}{\sqrt{2}} + \beta_3 \frac{1}{\sqrt{2}} - \beta_4 \right) \sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right) \\ &\geq \left(-\frac{1}{500} \frac{1}{\sqrt{2}} + \left(\frac{3}{4} - \frac{1}{250} + o(1) \right) \frac{1}{\sqrt{2}} - \frac{1}{4} - \frac{1}{500} \right) \sum_p \frac{\chi_0(p) \log p}{p} f\left(\frac{\log p}{\log q}\right). \end{aligned}$$

Applying Lemma 7.2(i) to the left-hand side and Lemma 7.2(ii) to the right-hand side, we obtain

$$\frac{1}{8} \geq \frac{93}{250\sqrt{2}} - \frac{1}{8} - \frac{1}{1000} + o(1) = 0.137\dots + o(1),$$

which is a contradiction. $\square$

Remark 7.3. We have not tried to optimize the lower bound in Lemma 7.1. In our cases $k \in \{1, 2\}$, it would be quite easy to do such an optimization by hand. For larger k one could use linear programming (which has been previously used in a somewhat similar context in [15, Proof of Theorem 2]) to take full advantage of the information provided by Lemma 7.2. Even this is not sufficient to prove a similar result in case $k = 3$, but as it turns out we will only need the cases $k \in \{1, 2\}$ in the proofs of our theorems.

8 SIZE OF $E_3(N)$

Proof of Theorem 1.1. Let $\varepsilon > 0$ be small. Let $N = q$ if q is cube-free and $N = q^{1+100\varepsilon}$ otherwise. Adjusting ε , it suffices to prove that $E_3(N) = \mathbb{Z}_q^\times$. Recall the definitions of θ and θ_0 from (5.1) and (5.2). We have

$$\theta \geq 1 - \varepsilon - \frac{\log q}{3 \log N} \geq \frac{2}{3} + 10\varepsilon$$

and

$$\theta_0 = 1 - \varepsilon - \frac{\log q}{4 \log N} \geq \frac{3}{4} - \varepsilon.$$

Let us apply Proposition 6.2. If Proposition 6.2(a) holds, then we immediately get $E_3(N) = \mathbb{Z}_q^\times$.

Hence we can assume that Proposition 6.2(b) holds. Let A' and B' be as there, in particular

$$(8.1) \quad |A'|, |B'| \geq \left(\frac{\theta}{2} - \frac{3}{2}\varepsilon \right) \varphi(q) \geq \left(\frac{1}{3} + 3\varepsilon \right) \varphi(q).$$

Write H for the stabilizer of $A' \cdot B'$. We apply Lemma 6.3 with $A = A', B = B', \alpha = 1/3 + 3\varepsilon, \alpha' = 3/8 - 10\varepsilon^{1/2}, \beta = 2/3 - 5\varepsilon/2$ (which is an admissible choice of parameters by (8.1) and Proposition 6.2(b.v)). In case Lemma 6.3(a) holds, we have $E_3(N) = \mathbb{Z}_q^\times$ by Proposition 6.2(b.iii), (8.1), and Lemma 3.4(i).

Hence we can assume that Lemma 6.3(b) holds. Then by Lemma 6.3(b.i)–(b.ii) A' and B' are contained in $k + 1$ cosets of a subgroup H of index $Y = 3k + 2$ with

$$1 < Y < \frac{1}{3/4 - 2/3 - 30\varepsilon^{1/2}} < 13,$$

so that $k \in \{0, 1, 2, 3\}$. Furthermore $A' \cdot B'$ is the union of $2k + 1$ cosets of H . If $k = 3$ (so that $Y = 11$) then (6.4) fails, so this case cannot actually occur.

Hence we can assume that $k \in \{0, 1, 2\}$. By Proposition 6.2(b.v) we know that A' and B' are contained in the same $k + 1$ cosets of H . Let now $a_1, \dots, a_{k+1}, b_1, \dots, b_{2k+1}$ be such that

$$A', B' \subseteq \bigcup_{j=1}^{k+1} a_j H$$

and

$$(8.2) \quad A' \cdot B' = \bigcup_{j=1}^{2k+1} b_j H = \left(\bigcup_{j=1}^{k+1} a_j H \right)^2.$$

By Proposition 6.2(b.v) the set A' contains at least $\frac{\varepsilon}{2}\varphi(q)$ elements from each a_jH with $j \in \{1, \dots, k+1\}$. Combining this and (8.2) with Proposition 6.2(b.iii) and Lemma 3.4(ii), we see that

$$(8.3) \quad \left(\bigcup_{j=1}^{k+1} a_jH \right) \cdot \left(\bigcup_{j=1}^{2k+1} b_jH \right) \subseteq E_3(N).$$

The left-hand side does not yet necessarily cover all of $\mathbb{Z}_q^\times$. To proceed, we split into two cases.

8.1 Case 1: $k \in \{1, 2\}$ or $k = 0$ and $a_1 \in H$

We shall in a moment show that in this case there exists $\alpha_1 \in (2\varepsilon, 1]$ such that

$$(8.4) \quad \sum_{\substack{q^{\alpha_1 - \varepsilon} < p \leq q^{\alpha_1} \\ p \notin \bigcup_{j=1}^{k+1} a_jH}} \frac{\log p}{p} \gg \log q.$$

Let us first show how (8.4) implies the claim that $E_3(N) = \mathbb{Z}_q^\times$. By (8.4) there exists $a_0 \in \mathbb{Z}_q^\times$ such that $a_0H \not\subseteq \{a_1H, \dots, a_{k+1}H\}$ and

$$\sum_{\substack{q^{\alpha_1 - \varepsilon} < p \leq q^{\alpha_1} \\ p \in a_0H}} \frac{\log p}{p} \gg \log q.$$

Then, for each $a \in a_0H \cdot \bigcup_{j=1}^{2k+1} b_jH$ we have by (8.2)

$$\sum_{\substack{cp \equiv a \pmod{q} \\ q^{\alpha_1 - \varepsilon} < p \leq q^{\alpha_1} \\ c \in A' \cdot \bar{B}'}} \frac{1}{p} \geq \sum_{\substack{q^{\alpha_1 - \varepsilon} < p \leq q^{\alpha_1} \\ p \in a_0H}} \frac{1}{p} \gg 1.$$

Hence by Proposition 6.2(b.iv) we obtain that

$$a_0H \cdot \bigcup_{j=1}^{2k+1} b_jH \subseteq E_3(N).$$

Combining this with (8.3) and Lemma 3.4(i) we see that $E_3(N) = \mathbb{Z}_q^\times$.

Hence the remaining task is to prove (8.4). Consider first the case that $\bigcup_{j=1}^{k+1} a_jH$ and $\bigcup_{j=1}^{2k+1} b_jH$ are not complements of each other. In this case there exists $b_0 \in \mathbb{Z}_q^\times$ such that b_0H intersects neither of these unions. By Lemma 3.3 we know that $b_0H \cap [1, q]$ contains $\gg q/\log q$ integers who have at most two prime factors and whose prime factors are $\geq q^{1/3}$. Since $b_0 \notin \bigcup_{j=1}^{k+1} a_jH$ by Proposition 6.2(b.vi), there must be $\gg q/\log q$ products of exactly two primes $\geq q^{1/3}$ in $b_0H \cap [1, q]$. But since

$$b_0 \notin \bigcup_{j=1}^{2k+1} b_jH = \left(\bigcup_{j=1}^{k+1} a_jH \right)^2,$$

we see that both prime factors cannot be from $\cup_{j=1}^{k+1} a_j H$. Consequently

$$\frac{q}{\log q} \ll \sum_{\substack{q^{1/3} \leq p \leq q^{2/3} \\ p \notin \cup_{j=1}^{k+1} a_j H}} \sum_{q^{1/3} \leq p' \leq q/p} 1 \ll \sum_{\substack{q^{1/3} \leq p \leq q^{2/3} \\ p \notin \cup_{j=1}^{k+1} a_j H}} \frac{q}{p \log q/p}$$

and (8.4) follows.

Note that if $k = 0$ and $a_1 \in H$, then definitely $a_1 H = H$ and $b_1 H = a_1^2 H = H$ are not complements of each other, and so in the rest of the proof of case 1 we can assume that $k \in \{1, 2\}$ and $\cup_{j=1}^{k+1} a_j H$ and $\cup_{j=1}^{2k+1} b_j H$ are complements of each other. But then (8.4) follows from Lemmas 6.4 and 7.1.

8.2 Case 2: $k = 0$ and $a_1 \notin H$

This is the most difficult case; due to the possible existence of exceptional characters, there may exist a quadratic character ψ such that $\psi(p) = -1$ for almost all primes, and thus we might indeed have $p \notin H$ for almost all primes p . We need two auxiliary results before we can finish the proof of Theorem 1.1 in this case. In this subsection we state these results and finish the proof of Theorem 1.1 assuming them. We postpone the proofs of the auxiliary results to Section 9.

First, while we cannot show that the primes with $\psi(p) = 1$ have positive logarithmic density, we can show the following.

Lemma 8.1 (Lower-bounding the number of primes with $\psi(p) = 1$). *Let $q \in \mathbb{N}$ be sufficiently large and let $\psi \pmod{q}$ be a real character. Then there exists a positive constant c_0 such that either*

$$(8.5) \quad \sum_{\substack{q^{1/4} < p \leq q^{5/7} \\ \psi(p)=1}} \frac{1}{p} \geq \frac{1}{10}$$

or there exists $y \in [q^{5/7}, q]$ such that

$$(8.6) \quad \sum_{\substack{p \leq y \\ \psi(p)=1}} 1 \geq c_0 y L(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right).$$

This lemma has some similarities with the work of Dunn, Kerr, Shparlinski and Zaharescu [3, Theorem 1.1] (see also work of Benli [2, Theorem 4], but there is an inaccuracy¹ in the proof: In the proof of [2, Lemma 9] the k -dimensional fundamental lemma of the sieve is currently applied with level z^s larger than the upper bound for e in [2, Proposition 7] — however the methods in [2] definitely do yield a result like [2, Theorem 4], possibly with a slightly different lower bound).

Remark 8.2. The bound (8.5) is clearly optimal up to a constant factor, and similarly the lower bound in (8.6) is optimal up to a constant factor (see Lemma 9.4 below).

The second important auxiliary result is the following addition to Proposition 6.2.

Proposition 8.3. *In the set-up of Proposition 6.2, in case Proposition 6.2(b) holds, the sets A', B' satisfy in addition to (b.i)–(b.vi) also the following:*

¹The author of [2] is in the process of correcting this.

Assume that $N \geq q$ and $M \in [q^{2/3+3\varepsilon}, q]$. Then

$$\sum_{\substack{cp \equiv a \pmod{q} \\ p \sim M, \psi(p)=1 \\ c \in A' \cdot B'}} 1 \gg ML(1, \psi) \frac{\varphi(q)}{q} \prod_{2 < p \leq q} \left(1 - \frac{2}{p}\right) \implies a \in E_3(N).$$

Now we finish the proof of Theorem 1.1 in the remaining case $k = 0$ and $a_1 \notin H$, assuming Lemma 8.1 and Proposition 8.3. In this case $A', B' \subseteq a_1 H$ and $A' \cdot B' = a_1^2 H = H$.

By (8.3) it suffices to show that $a \in E_3(N)$ for every $a \in H$. Since $A' \cdot B' = H$, by Proposition 8.3 this follows if, for some $M \in [q^{2/3+3\varepsilon}, q]$, we have

$$\sum_{\substack{p \sim M \\ \psi(p)=1}} 1 \gg ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p < q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right).$$

But this either follows from Lemma 8.1 or (8.5) holds. But if (8.5) holds, then (8.4) holds and the argument in case 1 goes through. $\square$

9 PROOFS OF LEMMA 8.1 AND PROPOSITION 8.3

In the proofs of Lemma 8.1 and Proposition 8.3 we will apply a sieve to the sequence $(1 * \psi)(n)$. In the course of doing this, we shall need the fundamental lemma of the sieve (see e.g. [5, Lemma 6.8]):

Lemma 9.1 (Fundamental lemma of the sieve). *Let $\kappa \geq 1$ be fixed. Let $z \geq 2$ and let $D = z^s$ with $s \geq 9\kappa + 1$. There exist coefficients $\lambda_d^\pm$ such that the following hold.*

- (i) $|\lambda_d^\pm| \leq 1$ for every $d \in \mathbb{N}$ and $\lambda_d^\pm$ are supported on $\{d \leq D : d \mid P(z)\}$.
- (ii) For every $n \in \mathbb{N}$,

$$\sum_{d \mid n} \lambda_d^- \leq \mathbf{1}_{(n, P(z))=1} \leq \sum_{d \mid n} \lambda_d^+.$$

- (iii) If $h: \mathbb{N} \rightarrow [0, 1)$ is a multiplicative function such that, for some $K \geq 1$, one has

$$\prod_{w_1 \leq p < z_1} (1 - h(p))^{-1} \leq K \left(\frac{\log z_1}{\log w_1} \right)^\kappa$$

for any $z_1 \geq w_1 \geq 2$, then

$$\begin{aligned} \sum_{d \mid P(z)} \lambda_d^+ h(d) &\leq (1 + e^{9\kappa-s} K^{10}) \prod_{p < z} (1 - h(p)), \\ \sum_{d \mid P(z)} \lambda_d^- h(d) &\geq (1 - e^{9\kappa-s} K^{10}) \prod_{p < z} (1 - h(p)). \end{aligned}$$

Before moving on, let us collect some arithmetic information concerning $(1 * \psi)(n)$.

Lemma 9.2. *Let $q \in \mathbb{N}$ and let ψ be a quadratic character $\pmod{q}$. For each $\varepsilon > 0$, there exists a constant $\eta = \eta(\varepsilon)$ such that, for any $x \geq q^{1/4+\varepsilon}$,*

$$\sum_{n \leq x} (1 * \psi)(n) = L(1, \psi)x + O_\varepsilon(x^{1-\eta}).$$

Proof. This follows easily from the Dirichlet hyperbola method and the Burgess bound, see [18, Proposition 3.1]. $\square$

Lemma 9.3. *Let $q \in \mathbb{N}$ and let ψ be a quadratic character (mod q). For each $\varepsilon > 0$, there exists a constant $\eta = \eta(\varepsilon)$ such that whenever $d \in \mathbb{N}$ and $x/d \geq q^{1/4+\varepsilon}$, we have*

$$(9.1) \quad \sum_{\substack{n \leq x \\ d|n}} (1 * \psi)(n) = h(d)L(1, \psi)x + O_\varepsilon(\tau_3(d)\tau(d)(x/d)^{1-\eta}),$$

where h is a multiplicative function such that, for every $p \in \mathbb{P}$,

$$(9.2) \quad h(p) = \frac{1 + \psi(p)}{p} - \frac{\psi(p)}{p^2} \quad \text{and} \quad |h(p^k)| \leq \frac{2k}{p^k} \quad \text{for any } k \in \mathbb{N}.$$

Proof. This follows easily from Lemma 9.2 (and is essentially a special case of [2, Proposition 7]). Let

$$S_d := \sum_{\substack{n \leq x \\ d|n}} (1 * \psi)(n) = \sum_{\substack{m_1 m_2 \leq x \\ d|m_1 m_2}} \psi(m_2).$$

Writing $d = d_1 d_2$ with $d_1 = (d, m_1)$, we see that

$$S_d = \sum_{d=d_1 d_2} \sum_{\substack{m_1 \\ d_1|m_1 \\ (d_2, m_1/d_1)=1}} \sum_{\substack{m_2 \leq x/m_1 \\ d_2|m_2}} \psi(m_2).$$

We remove the condition $(d_2, m_1/d_1) = 1$ by Möbius inversion, obtaining

$$S_d = \sum_{d=d_1 d_2} \sum_{d_2=f g} \mu(f) \sum_{\substack{m_1 \\ d_1|m_1 \\ f|m_1/d_1}} \sum_{\substack{m_2 \leq x/m_1 \\ d_2|m_2}} \psi(m_2).$$

Making the change of variables $m_1 \rightarrow d_1 f m_1$ and $m_2 \rightarrow m_2 d_2 = m_2 f g$, we obtain

$$S_d = \sum_{d=d_1 f g} \mu(f) \psi(f g) \sum_{m_1 m_2 \leq x/(d_1 f^2 g)} \psi(m_2) = \sum_{d=d_1 f g} \mu(f) \psi(f g) \sum_{m \leq \frac{x}{df}} (1 * \psi)(m).$$

Now $f \geq (x/d)^{\varepsilon/2}$ contribute

$$\ll \tau_3(d) \sum_{\substack{f|d \\ f \geq (x/d)^{\varepsilon/2}}} \frac{x}{df} \log \frac{x}{d} \ll \tau_3(d) \tau(d) \left(\frac{x}{d}\right)^{1-\varepsilon/2} \log \frac{x}{d},$$

whereas by Lemma 9.2 the contribution of $f < (x/d)^{\varepsilon/2}$ is, for some $\eta > 0$,

$$\begin{aligned} & \sum_{\substack{d=d_1 f g \\ f < (x/d)^{\varepsilon/2}}} \mu(f) \psi(f g) \left(L(1, \psi) \frac{x}{df} + O\left(\left(\frac{x}{df}\right)^{1-\eta}\right) \right) \\ &= x L(1, \psi) \sum_{d=d_1 f g} \frac{\mu(f) \psi(f g)}{d_1 f^2 g} + O\left(\tau_3(d) \left(\frac{x}{d}\right)^{1-\eta/2}\right). \end{aligned}$$

Writing out the Euler product we obtain (9.1) with h being the multiplicative function such that, for any $p \in \mathbb{P}$ and $k \in \mathbb{N}$,

$$\begin{aligned} h(p^k) &= \sum_{p^k=d_1g} \frac{\psi(g)}{d_1g} - \sum_{p^k=d_1pg} \frac{\psi(pg)}{d_1p^2g} = \sum_{j=0}^k \frac{\psi(p^j)}{p^k} - \sum_{j=0}^{k-1} \frac{\psi(p^{j+1})}{p^{k+1}} \\ &= \frac{\psi(p^k)}{p^k} + \frac{1}{p^k} \sum_{j=0}^{k-1} \psi(p^j) \left(1 - \frac{\psi(p)}{p}\right) \end{aligned}$$

which clearly satisfies (9.2). $\square$

Before turning to the proof of Lemma 8.1, let us quickly combine Lemmas 9.1 and 9.3 to obtain an upper bound corresponding to (8.6).

Lemma 9.4 (Upper-bounding the number of primes with $\psi(p) = 1$). *Let $\varepsilon > 0$ be fixed, let $q \in \mathbb{N}$ be sufficiently large and let $\psi \pmod{q}$ be a real character. Then there exists a positive constant C_ε such that, for any $y \in [q^{1/4+\varepsilon}, q]$ we have*

$$\sum_{\substack{p \leq y \\ \psi(p)=1}} 1 \leq C_\varepsilon y L(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right).$$

Proof. We can clearly assume that ε is small. Let λ_d^+ be as in Lemma 9.1 with $\kappa = 2$, sifting parameter $z = q^{\varepsilon^2}$, and level $D = q^{\varepsilon/2}$ (so that $s = 1/(2\varepsilon)$).

Now by Lemma 9.1(ii) and Lemma 9.3, we have, for some $\eta > 0$,

$$\begin{aligned} \sum_{\substack{p \leq y \\ \psi(p)=1}} 1 &\leq \sum_{p \leq y} (1 * \psi)(p) \leq \sum_{n \leq y} (1 * \psi)(n) \sum_{e|n} \lambda_e^+ \leq \sum_{e|P(q^{\varepsilon^2})} \lambda_e^+ \sum_{\substack{n \leq y \\ e|n}} (1 * \psi)(n) \\ &= y L(1, \psi) \sum_{e|P(q^{\varepsilon^2})} \lambda_e^+ h(e) + O(y^{1-\eta}), \end{aligned}$$

where h is as in Lemma 9.3. Now the claim follows from the fact that $L(1, \psi) \gg_\delta q^{-\delta}$ by Siegel's theorem and Lemma 9.1(iii) since

$$(9.3) \quad \prod_{p < q^{\varepsilon^2}} (1 - h(p)) \asymp \prod_{p \leq q} (1 - h(p)) \asymp \prod_{p|q} \left(1 - \frac{1}{p}\right) \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) = \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right).$$

$\square$

Proof of Lemma 8.1. Let $w = q^{\varepsilon^4}$, where $\varepsilon > 0$ is small but fixed. Let $a_n = (1 * \psi)(n) \mathbf{1}_{(n, P(w))=1}$. Note that $a_n \geq 0$ for all n . Let $\lambda_d^\pm$ be as in Lemma 9.1 with $\kappa = 2$, sifting parameter $z = w$, and level $D = q^{\varepsilon^2}$ (so that $s = \varepsilon^{-2}$).

We use Chebychev's method like Dunn, Kerr, Shparlinski and Zaharescu do in the proof of [3, Theorem 1.1]. Now by Lemma 9.1(ii), Lemma 9.3, and partial summation, we have,

for some $\eta > 0$,

$$\begin{aligned}
 \sum_{d \leq q} \Lambda(d) \sum_{\substack{n \leq q \\ d|n}} a_n &= \sum_{n \leq q} a_n \sum_{d|n} \Lambda(d) = \sum_{n \leq q} a_n \log n \geq \sum_{e|P(w)} \lambda_e^- \sum_{\substack{n \leq q \\ e|n}} (1 * \psi)(n) (\log n) \\
 (9.4) \qquad &= q(\log q) L(1, \psi) \sum_{e|P(w)} \lambda_e^- h(e) + O(q^{1-\eta}).
 \end{aligned}$$

By Lemma 9.1(ii) and Lemma 9.3, we have, for some $\eta > 0$,

$$\begin{aligned}
 \sum_{\substack{d \leq q^{5/7} \\ (d, P(w))=1}} \Lambda(d) \sum_{\substack{n \leq q \\ d|n}} a_n &\leq \sum_{\substack{d \leq q^{5/7} \\ (d, P(w))=1}} \Lambda(d) \sum_{e|P(w)} \lambda_e^+ \sum_{\substack{n \leq q \\ de|n}} (1 * \psi)(n) \\
 (9.5) \qquad &= L(1, \psi) q \sum_{e|P(w)} \lambda_e^+ h(e) \cdot \sum_{\substack{d \leq q^{5/7} \\ (d, P(w))=1}} \Lambda(d) h(d) + O(q^{1-\eta}).
 \end{aligned}$$

By (9.2) and Mertens' theorem,

$$\sum_{\substack{d \leq q^{1/4} \\ (d, P(w))=1}} \Lambda(d) h(d) \leq \sum_{w \leq p \leq q^{1/4}} \frac{2 \log p}{p} + \sum_{\substack{p^k \leq q^{1/4} \\ p \geq w, k \geq 2}} \frac{2k}{p^k} \log p \leq \frac{1}{2} \log q.$$

Furthermore, if (8.5) does not hold, then since $|h(p)| > 1/p^2$ for $p \nmid q$ implies $\psi(p) = 1$, we have

$$\sum_{\substack{q^{1/4} \leq d \leq q^{5/7} \\ (d, P(w))=1}} \Lambda(d) h(d) < 2 \cdot \frac{1}{10} \log q^{5/7} + O(q^{-1/10}) = \frac{1}{7} \log q + O(q^{-1/10}).$$

Inserting (9.6) and (9.7) into (9.5) and noting that $L(1, \psi) \sum_{e|P(w)} \lambda_e^+ h(e) > 0$, we see that, for some $\eta > 0$,

$$\sum_{\substack{d \leq q^{5/7} \\ (d, P(w))=1}} \Lambda(d) \sum_{\substack{n \leq q \\ d|n}} a_n \leq \frac{9}{14} q L(1, \psi) (\log q) \sum_{e|P(w)} \lambda_e^+ h(e) + O(q^{1-\eta}).$$

Once ε is sufficiently small, this together with (9.4) and Lemma 9.1(iii) implies that, for some $\eta > 0$,

$$\sum_{\substack{q^{5/7} < d \leq q \\ d|n}} \Lambda(d) \sum_{\substack{n \leq q \\ d|n}} a_n \geq \frac{1}{3} q (\log q) L(1, \psi) \prod_{p < w} (1 - h(p)) + O(q^{1-\eta}).$$

By Siegel's bound, the right-hand side is $\gg_\delta q^{1-\delta}$ for any $\delta > 0$. Note that higher prime powers give a negligible contribution to the left-hand side, a_n are supported on numbers whose all prime factors p satisfy $\psi(p) \in \{0, 1\}$ and $p \geq w$. Furthermore $a_n = O_\varepsilon(1)$. Hence (9.8) implies

$$q(\log q) L(1, \psi) \prod_{p < w} (1 - h(p)) \ll \sum_{\substack{q^{5/7} < p \leq q \\ \psi(p) \in \{0, 1\}}} \log p \frac{q}{p \log w} + \sum_{\substack{p \leq q \\ \psi(p) \in \{0, 1\}}} \log p$$

Now the primes with $\psi(p) = 0$ make a negligible contribution and we obtain

$$q(\log q)L(1, \psi) \prod_{p < w} (1 - h(p)) \ll \sum_{\substack{q^{5/7}/2 \leq y < q/2 \\ y=2^\ell}} \frac{1}{y} \sum_{\substack{p \sim y \\ q^{5/7} < p \leq q \\ \psi(p) \in \{0,1\}}} 1 + (\log q) \sum_{\substack{p \leq q \\ \psi(p)=1}} 1.$$

and the claim follows. $\square$

We will need the following variant of the Halász–Montgomery type mean value theorem (Lemma 3.8) which takes into account the possible sparsity of the set of primes p with $\psi(p) = 1$.

Lemma 9.5 (Sharp Halász–Montgomery with weight $1 * \psi$). *Let $\varepsilon > 0$ and $C \geq 1$ be fixed, $q \in \mathbb{N}$, and let $N \in [q^{2/3+3\varepsilon}, q^C]$. Let $\chi_1, \dots, \chi_R$ be distinct Dirichlet characters of modulus q and let ψ be a quadratic character of modulus q . Then there exists $\eta = \eta(\varepsilon) > 0$ such that, for any complex coefficients a_n ,*

$$\begin{aligned} & \sum_{j=1}^R \left| \sum_{\substack{n \leq N \\ (n, P(q^\varepsilon))=1}} (1 * \psi)(n) a_n \chi_j(n) \right|^2 \\ & \ll_\varepsilon \left(NL(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p} \right) + Nq^{-\eta} R \right) \sum_{\substack{n \leq N \\ (n, P(q^\varepsilon))=1}} (1 * \psi)(n) |a_n|^2. \end{aligned}$$

Proof. The proof is somewhat similar to the proof of Lemma 3.8 although there are some additional complications. By the duality principle (see e.g. [10, Section 7.1]), it suffices to show that, for any complex coefficients c_j ,

$$(9.9) \quad \sum_{\substack{n \leq N \\ (n, P(q^\varepsilon))=1}} (1 * \psi)(n) \left| \sum_{j=1}^R c_j \chi_j(n) \right|^2 \ll \left(NL(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p} \right) + Nq^{-\eta} R \right) \sum_{j=1}^R |c_j|^2.$$

Let λ_d^+ be as in Lemma 9.1 with $\kappa = 2$, sifting parameter $z = q^{\varepsilon^2}$ and level $D = q^\varepsilon$ (so that $s = \varepsilon^{-1}$). Then the left-hand side of (9.9) is by Lemma 9.1(ii)

$$(9.10) \quad \leq \sum_{d \leq D} \lambda_d^+ \sum_{\substack{n \leq N \\ d|n}} (1 * \psi)(n) \left| \sum_{j=1}^R c_j \chi_j(n) \right|^2 = \sum_{j,k=1}^R c_j \overline{c_k} \sum_{d \leq D} \lambda_d^+ \sum_{\substack{n \leq N \\ d|n}} \chi_j(n) \overline{\chi_k(n)} (1 * \psi)(n).$$

Note that for a character $\chi \pmod{q}$ with $\chi \notin \{\chi_0, \psi\}$, by the hyperbola method and the Burgess bound (Lemma 3.2) we have

$$\sum_{\substack{n \leq N \\ d|n}} \chi(n) (1 * \psi)(n) = \sum_{e \leq N^{1/2}} \psi(e) \sum_{\substack{n \leq N \\ d|n, e|n}} \chi(n) + \sum_{e \leq N^{1/2}} \overline{\psi}(e) \sum_{\substack{eN^{1/2} < n \leq N \\ d|n, e|n}} \chi(n) \psi(n) \ll \frac{N}{d} q^{-2\eta}$$

for some $\eta = \eta(\varepsilon) > 0$, provided that $N^{1/2}/d \geq q^{1/3+\varepsilon/10}$. Using this and the assumption $N \geq q^{2/3+3\varepsilon}$, we see that (9.10) for $\chi_j \overline{\chi_k} \notin \{\chi_0, \psi\}$ is

$$\ll R \sum_{j=1}^R |c_j|^2 N q^{-\eta}.$$

For the remaining pairs we note that

$$(1 * \psi)(n) \psi(n) = (1 * \psi)(n) \chi_0(n) = (1 * \psi)(n) \mathbf{1}_{(n,q)=1}$$

and thus they contribute to (9.10) at most

$$(9.11) \quad \left| \sum_{\substack{j,k=1 \\ \chi_j \overline{\chi_k} \in \{\chi_0, \psi\}}}^R c_j \overline{c_k} \sum_{d \leq D} \lambda_d^+ \sum_{\substack{n \leq N \\ d|n \\ (n,q)=1}} (1 * \psi)(n) \right| \leq 2 \sum_{j=1}^R |c_j|^2 \left| \sum_{\substack{d \leq D \\ (d,q)=1}} \lambda_d^+ \sum_{\substack{n \leq N \\ d|n \\ (n,q)=1}} (1 * \psi)(n) \right|.$$

By Möbius inversion, Lemma 9.3 and (9.2), we have, for any $d \leq D$ with $(d, q) = 1$ and some $\eta' > 0$,

$$\begin{aligned} \sum_{\substack{n \leq N \\ d|n \\ (n,q)=1}} (1 * \psi)(n) &= \sum_{e|q} \mu(e) \sum_{\substack{n \leq N \\ de|n}} (1 * \psi)(n) \\ &= \sum_{\substack{e|q \\ de \leq N/q^{1/4+\varepsilon}}} \mu(e) \sum_{\substack{n \leq N \\ de|n}} (1 * \psi)(n) + O \left(\sum_{\substack{e|q \\ de > N/q^{1/4+\varepsilon}}} \sum_{\substack{n \leq N \\ de|n}} \tau(n) \right) \\ &= \sum_{\substack{e|q \\ de \leq N/q^{1/4+\varepsilon}}} \mu(e) \left(L(1, \psi) h(de) N + O \left((de)^{\eta'/10} \left(\frac{N}{de} \right)^{1-\eta'} \right) \right) + O \left(q^{1/3} \right) \\ &= h(d) N L(1, \psi) \prod_{p|q} (1 - h(p)) + O \left(\left(\frac{N}{d} \right)^{1-\eta'/2} \right). \end{aligned}$$

Thus, using Lemma 9.1(iii) and a variant of (9.3) we can bound the right-hand side of (9.11) as

$$\begin{aligned}
&= 2 \sum_{j=1}^R |c_j|^2 NL(1, \psi) \prod_{p|q} (1 - h(p)) \sum_{\substack{d \leq D \\ (d, q)=1}} h(d) \lambda_d^+ + O \left(\sum_{j=1}^R |c_j|^2 \sum_{\substack{d \leq D \\ (d, q)=1}} \left(\frac{N}{d} \right)^{1-\eta'/2} \right) \\
&\leq 4 \sum_{j=1}^R |c_j|^2 NL(1, \psi) \prod_{p|q} (1 - h(p)) \cdot \prod_{\substack{p < z \\ (p, q)=1}} (1 - h(p)) + O \left(\sum_{j=1}^R |c_j|^2 N^{1-\eta'/4} \right) \\
&\ll \sum_{j=1}^R |c_j|^2 NL(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p} \right)
\end{aligned}$$

by Siegel's bound $L(1, \psi) \gg_\delta q^{-\delta}$. Now the claim follows. $\square$

This allows us to add one more conclusion to Proposition 5.2:

Proposition 9.6. *In the set-up of Proposition 5.2, the set A satisfies in addition to (i)–(vi) also the following:*

Assume that $N \geq q$ and $M \in [q^{2/3+3\varepsilon}, q]$. Then

$$\sum_{\substack{pa_1a_2 \equiv a \pmod{q} \\ p \sim M, \psi(p)=1 \\ a_1, a_2 \in A}} 1 \gg \frac{\varphi(q)}{(\log q)^{1/2-\varepsilon}} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p} \right) \implies a \in E_3(N).$$

Proof. We proceed similarly to the proof of Proposition 5.2(iv) but with different choice of f_0 . We let $f: [N]_q \rightarrow \mathbb{R}_{\geq 0}$ be as in (5.8) and let $f_0: [N]_q \rightarrow \mathbb{R}_{\geq 0}$ be defined through

$$f_0(n) = \mathbf{1}_{n \in \mathbb{P} \cap (M, 2M]} \mathbf{1}_{(n, q)=1} (1 * \psi)(n).$$

Note that f_0 is supported on primes with $\psi(p) = 1$ and definitely $a \in E_3(N)$ if $(f * f * f_0)(n) > 0$ for some $n \equiv a \pmod{q}$. Recall that f satisfies the assumptions in Proposition 4.1 with $\delta = (\log q)^{-1/2+\varepsilon/2}$ and $\eta = o(1)$. Let g then be as in Proposition 4.1.

Now by orthogonality of characters and Proposition 4.1(iii) (abusing the notation to consider f_0 as a function from $\mathbb{Z}_q^\times$ when necessary)

$$\begin{aligned}
&\frac{1}{|[N]_q|^2} \sum_{n \equiv a \pmod{q}} (f * f * f_0)(n) - \frac{1}{\varphi(q)^2} (g * g * f_0)(a) \\
&= \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left(\left(\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right)^2 - \left(\mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right)^2 \right) \sum_{n \sim M} f_0(n) \overline{\chi}(n) \chi(a) \\
(9.12) \quad &= O \left(\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) \right| \left| \sum_{n \sim M} f_0(n) \overline{\chi}(n) \right| \right. \\
&\quad \left. \cdot \left| \mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b) \right| \right).
\end{aligned}$$

Let us first consider the right-hand side. Let the multiplicative function h be as in Lemma 9.3. We split the characters into two sets

$$\mathcal{X}_1 = \left\{ \chi \pmod{q} : \left| \sum_{n \sim M} f_0(n) \overline{\chi}(n) \right| < (\log q)^{-10} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) \right\}$$

and

$$\mathcal{X}_2 = \{ \chi \pmod{q} : \chi \notin \mathcal{X}_1 \}.$$

By the definition of $\mathcal{X}_1$, Proposition 4.1(iii) and Lemma 3.6, we see that

$$\begin{aligned} & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_1} |\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n)| \left| \sum_{n \sim M} f_0(n) \overline{\chi}(n) \right| |\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \overline{\chi}(b)| \\ & \ll (\log q)^{-10} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} |\mathbb{E}_{n \in [N]_q} f(n) \overline{\chi}(n)|^2 \\ (9.13) \quad & \ll (\log q)^{-10} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) \frac{1}{\varphi(q)} (N + \varphi(q)) \frac{\log N}{N} \\ & \ll \frac{1}{\varphi(q)(\log q)^9} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right). \end{aligned}$$

On the other hand, by the definition of $\mathcal{X}_2$, Lemma 9.5, and Lemma 9.4, we obtain

$$\begin{aligned} & \left((\log q)^{-10} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) \right)^2 |\mathcal{X}_2| \leq \sum_{\chi \in \mathcal{X}_2} \left| \sum_{n \sim M} f_0(n) \overline{\chi}(n) \right|^2 \\ & \ll \left(ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) + Mq^{-\eta} |\mathcal{X}_2| \right) \sum_{\substack{p \sim M \\ (p, q)=1}} (1 * \psi)(p) \\ & \ll \left(ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) + Mq^{-\eta} |\mathcal{X}_2| \right) ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right). \end{aligned}$$

By Siegel's bound $L(1, \psi) \gg q^{-\eta/10}$, so the second term cannot dominate and so $|\mathcal{X}_2| \ll (\log q)^{20}$ and moreover

$$\sum_{\chi \in \mathcal{X}_2} \left| \sum_{n \sim M} f_0(n) \overline{\chi}(n) \right|^2 \ll \left(ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p}\right) \right)^2.$$

Furthermore using the bound $|\mathcal{X}_2| \ll (\log q)^{20}$ and Lemma 3.8(i), we obtain similarly to (5.22) that

$$\sum_{\chi \in \mathcal{X}_2} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \ll 1.$$

Combining these with Proposition 4.1(ii) and Cauchy–Schwarz, we obtain

$$\begin{aligned} & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_2} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)| \left| \sum_{n \sim M} f_0(n) \bar{\chi}(n) \right| \left| \mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n) - \mathbb{E}_{b \in \mathbb{Z}_q^\times} g(b) \bar{\chi}(b) \right| \\ & \ll \delta \frac{1}{\varphi(q)} \left(\sum_{\chi \in \mathcal{X}_2} \left| \sum_{n \sim M} f_0(n) \bar{\chi}(n) \right|^2 \right)^{\frac{1}{2}} \left(\sum_{\chi \in \mathcal{X}_2} |\mathbb{E}_{n \in [N]_q} f(n) \bar{\chi}(n)|^2 \right)^{1/2} \\ & \ll \frac{\delta}{\varphi(q)} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p} \right). \end{aligned}$$

Combining with (9.12) and (9.13), we obtain

$$\frac{1}{|[N]_q|^2} \sum_{n \equiv a \pmod{q}} (f * f * f_0)(n) = \frac{1}{\varphi(q)^2} (g * g * f_0)(a) + O \left(\frac{\delta}{\varphi(q)} ML(1, \psi) \frac{\varphi(q)}{q} \prod_{\substack{2 < p \leq q \\ \psi(p)=1}} \left(1 - \frac{2}{p} \right) \right).$$

Recall $A = \{a \in \mathbb{Z}_q^\times : |g(a)| \geq \varepsilon/10\}$ in Proposition 5.2, so the main term on the right-hand side is

$$\geq \frac{1}{\varphi(q)^2} \sum_{\substack{pa_1 a_2 \equiv a \pmod{q} \\ p \sim M, \psi(p)=1}} g(a_1) g(a_2) \geq \frac{\varepsilon^2}{\varphi(q)^2} \sum_{\substack{pa_1 a_2 \equiv a \pmod{q} \\ p \sim M, \psi(p)=1 \\ a_1, a_2 \in A}} 1,$$

and the claim follows. $\square$

Now Proposition 8.3 finally follows from Proposition 9.6 since (6.2) implies that

$$\sum_{\substack{pa_1 a_2 \equiv a \pmod{q} \\ p \sim M, \psi(p)=1 \\ a_1, a_2 \in A}} 1 \geq \sum_{\substack{cp \equiv a \pmod{q} \\ p \sim M, \psi(p)=1 \\ c \in A' \cdot B'}} (\mathbf{1}_A * \mathbf{1}_A)(c) \geq \frac{\varepsilon \varphi(q)}{10} \sum_{\substack{cp \equiv a \pmod{q} \\ p \sim M, \psi(p)=1 \\ c \in A' \cdot B'}} 1.$$

10 SIZE OF $E_2(q)$

Proof of Theorem 1.3. Let $\varepsilon > 0$ be small. Recall the definitions of θ and θ_0 from (5.1) and (5.2). Note that $\theta \geq 3/4 - \varepsilon$ if q is cube-free and $\theta \geq 2/3 - \varepsilon$ if q is not cube-free. Let us apply Proposition 6.2. If Proposition 6.2(a) holds, then the claim follows immediately (adjusting ε). Hence we can assume that Proposition 6.2(b) holds. Let A' and B' be as there. We apply Lemma 6.3 for these sets, taking $\alpha = \alpha' = 3/8 - 2\varepsilon$, and $\beta = 11/16 - 5\varepsilon$ if q is cube-free and $\alpha = 1/3 - 2\varepsilon$, $\alpha' = 3/8 - 10\varepsilon^{1/2}$ and $\beta = 2/3 - 7\varepsilon$ if q is not cube-free. If Lemma 6.3(a) holds, the claim follows immediately (adjusting ε) from Proposition 6.2(b.ii)

We may then assume that Lemma 6.3(b) holds. In particular, then the stabilizer H of $A' \cdot B'$ has index $Y = 3k + 2$ with $k \in \{0, 1, 2\}$ (in case q is cube-free, this follows from Lemma 6.3(b.iii) and in case q is not cube-free first Lemma 6.3(b.i) implies that $Y \leq 12$ so that $k \in \{0, 1, 2, 3\}$ and then (6.4) implies $k \neq 3$). Moreover, by Lemma 6.3(b.ii) there

exist cosets $a_1H, \dots, a_{k+1}H$ and $b_1H, \dots, b_{2k+1}H$ such that A' and B' are contained in $\cup_{j=1}^{k+1} a_jH$ (by Proposition 6.2(b.v) A' and B' are contained in the same $k+1$ cosets) and

$$\left(\bigcup_{j=1}^{k+1} a_jH \right) \cdot \left(\bigcup_{j=1}^{k+1} a_jH \right) = \bigcup_{j=1}^{2k+1} b_jH = A' \cdot B'.$$

Furthermore by Proposition 6.2(b.ii) and (b.vi)

$$(10.1) \quad \left| E_2(q) \cap \left(\bigcup_{j=1}^{2k+1} b_jH \right) \right| \geq \left(\frac{2k+1}{Y} - \varepsilon \right) \varphi(q)$$

and

$$(10.2) \quad \sum_{\substack{p \leq q \\ p \notin \cup_{j=1}^{k+1} a_jH}} 1 \leq (2k+1) \cdot 2\varepsilon \frac{q}{\log q}.$$

Let us next observe that there exists $y \in [q^\varepsilon, q]$ and a_0 such that $a_0 \notin \cup_{j=1}^{k+1} a_jH$ and

$$(10.3) \quad \sum_{\substack{p \sim y \\ p \in a_0H}} 1 \gg \frac{y}{q^{\eta'}}$$

for any $\eta' > 0$; in case $k = 0$ and $a_1 \notin H$ this follows from Lemma 8.1 and otherwise it follows as (8.4).

By Kneser's theorem (Lemma 3.5),

$$\left| \left(\bigcup_{j=0}^{k+1} a_jH \right) \cdot \left(\bigcup_{j=1}^{k+1} a_jH \right) \right| \geq (k+2)|H| + (k+1)|H| - |H| = (2k+2)|H| > \left| \bigcup_{j=1}^{2k+1} b_jH \right|.$$

Hence there exists $j_0 \in \{1, \dots, k+1\}$ such that

$$(10.4) \quad a_0 a_{j_0}H \notin \bigcup_{j=1}^{2k+1} b_jH.$$

Let

$$\mathcal{P}_1 = \{p \sim y : p \in a_0H\}$$

and

$$\mathcal{P}_2 = \{p \leq q : p \in a_{j_0}H\}.$$

Now by the prime number theorem, Lemma 3.3 and (10.2),

$$(10.5) \quad \begin{aligned} |\mathcal{P}_2| &= \sum_{p \leq q} 1 - \sum_{\substack{j=1 \\ j \neq j_0}}^{k+1} \sum_{\substack{p \leq q \\ p \in a_jH}} 1 - \sum_{\substack{p \leq q \\ p \notin \cup_{j=1}^{k+1} a_jH}} 1 \geq \left(1 - \frac{k}{3k+2} \cdot \frac{2}{\theta_0} - 2\varepsilon(2k+1) + o(1) \right) \frac{q}{\log q} \\ &\geq \begin{cases} (1 - 20\varepsilon) \frac{q}{\log q} & \text{if } k = 0; \\ \left(\frac{7}{15} - 20\varepsilon \right) \frac{q}{\log q} & \text{if } k = 1; \\ \left(\frac{1}{3} - 20\varepsilon \right) \frac{q}{\log q} & \text{if } k = 2. \end{cases} \end{aligned}$$

Note that, for any $a \in \mathbb{Z}_q^\times$, we have

$$(10.6) \quad \sum_{\substack{a=p_1 p_2 \\ p_1 \in \mathcal{P}_1 \\ p_2 \in \mathcal{P}_2}} 1 > 0 \implies a \in E_2(q) \cap a_0 a_{j_0} H.$$

By the Cauchy–Schwarz inequality,

$$(10.7) \quad (|\mathcal{P}_1||\mathcal{P}_2|)^2 = \left(\sum_{a \in \mathbb{Z}_q^\times} \sum_{\substack{a=p_1 p_2 \\ p_1 \in \mathcal{P}_1 \\ p_2 \in \mathcal{P}_2}} 1 \right)^2 \leq |E_2(q) \cap a_0 a_{j_0} H| \sum_{a \in \mathbb{Z}_q^\times} \left(\sum_{\substack{a=p_1 p_2 \\ p_1 \in \mathcal{P}_1 \\ p_2 \in \mathcal{P}_2}} 1 \right)^2.$$

This is a multiplicative variant of [24, second inequality in (2.8)] — on the right-hand side we have the multiplicative energy $E_q^\times(\mathcal{P}_1, \mathcal{P}_2)$, where $E_q^\times(B, C)$ is defined between two finite sets $B, C \subseteq \{n \in \mathbb{Z} : (n, q) = 1\}$ by

$$E_q^\times(B, C) = \sum_{\substack{b_1, b_2 \in B, c_1, c_2 \in C \\ b_1 c_1 \equiv b_2 c_2 \pmod{q}}} 1.$$

Then by (10.7)

$$(10.8) \quad |E_2(q) \cap a_0 a_{j_0} H| \geq \frac{(|\mathcal{P}_1||\mathcal{P}_2|)^2}{E_q^\times(\mathcal{P}_1, \mathcal{P}_2)}.$$

Now we show an upper bound for $E_q^\times(\mathcal{P}_1, \mathcal{P}_2)$. Let λ_d^+ be as in Lemma 3.1 with level $D = q^\theta$ and $s = 1$ (so that $z = D$).

Then by Lemma 3.1(ii)

$$E_q^\times(\mathcal{P}_1, \mathcal{P}_2) \leq \sum_{p_1, q_1 \in \mathcal{P}_1, p_2 \in \mathcal{P}_2, n_2 \leq q} \sum_{d|n_2} \lambda_d^+ 1_{p_1 p_2 \equiv q_1 n_2 \pmod{q}}.$$

Thus by the orthogonality of characters

$$(10.9) \quad E_q^\times(\mathcal{P}_1, \mathcal{P}_2) \leq \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{p \in \mathcal{P}_1} \chi(p) \right|^2 \sum_{p \in \mathcal{P}_2} \chi(p) \sum_{n \leq q} \overline{\chi(n)} \sum_{d|n} \lambda_d^+.$$

We first consider the contribution of $\chi = \chi_0$ to (10.9). This is by (3.2), Lemma 3.1(iii) and (10.5)

$$(10.10) \quad \begin{aligned} & \leq \frac{1}{\varphi(q)} |\mathcal{P}_1|^2 |\mathcal{P}_2| \left| \sum_{\substack{d \leq D \\ (d, q) = 1}} \lambda_d^+ \left(\frac{\varphi(q)}{d} + O(\tau(q)) \right) \right| \leq \frac{1}{\varphi(q)} (2 + o(1)) |\mathcal{P}_1|^2 |\mathcal{P}_2| \frac{q}{\log z} \\ & \leq \frac{2 + o(1)}{\theta} |\mathcal{P}_1|^2 |\mathcal{P}_2| \frac{q}{\varphi(q) \log q} \\ & \leq \begin{cases} \frac{1}{\varphi(q)} (3 + 100\varepsilon) |\mathcal{P}_1|^2 |\mathcal{P}_2|^2 & \text{when } k = 0; \\ \frac{1}{\varphi(q)} \left(\frac{45}{7} + 100\varepsilon \right) |\mathcal{P}_1|^2 |\mathcal{P}_2|^2 & \text{when } k = 1; \\ \frac{1}{\varphi(q)} (9 + 100\varepsilon) |\mathcal{P}_1|^2 |\mathcal{P}_2|^2 & \text{when } k = 2. \end{cases} \end{aligned}$$

We shall show that

$$(10.11) \quad \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \left| \sum_{p \in \mathcal{P}_1} \chi(p) \right|^2 \left| \sum_{p \in \mathcal{P}_2} \chi(p) \right| \left| \sum_{n \leq q} \chi(n) \sum_{d|n} \lambda_d^+ \right| \ll \frac{|\mathcal{P}_1|^2 |\mathcal{P}_2|^2}{(\log q)^{20} \varphi(q)}.$$

Before proving (10.11), let us show how it implies Theorem 1.3(i)–(ii). Combining (10.11) with (10.9) and the evaluation of the contribution of the principal character in (10.10), we obtain

$$E_q^\times(\mathcal{P}_1, \mathcal{P}_2) \leq \begin{cases} \frac{1}{\varphi(q)} (3 + 101\varepsilon) |\mathcal{P}_1|^2 |\mathcal{P}_2|^2 & \text{when } k = 0; \\ \frac{1}{\varphi(q)} \left(\frac{45}{7} + 101\varepsilon \right) |\mathcal{P}_1|^2 |\mathcal{P}_2|^2 & \text{when } k = 1; \\ \frac{1}{\varphi(q)} (9 + 101\varepsilon) |\mathcal{P}_1|^2 |\mathcal{P}_2|^2 & \text{when } k = 2. \end{cases}$$

This together with (10.8), (10.4), and (10.1) implies

$$|E_2(q)| \geq \begin{cases} \left(\frac{1}{2} - \varepsilon \right) \varphi(q) + \left(\frac{1}{3} - 200\varepsilon \right) \varphi(q) & \text{if } k = 0; \\ \left(\frac{3}{5} - \varepsilon \right) \varphi(q) + \left(\frac{7}{45} - 200\varepsilon \right) \varphi(q) & \text{if } k = 1; \\ \left(\frac{5}{8} - \varepsilon \right) \varphi(q) + \left(\frac{1}{9} - 200\varepsilon \right) \varphi(q) & \text{if } k = 2. \end{cases}$$

In each case the claim follows on taking $\varepsilon > 0$ small enough (since $1/2 + 1/3, 3/5 + 7/45, 5/8 + 1/9 > 11/16$).

Let us now turn to proving the remaining claim (10.11). We argue somewhat similarly as in the proof of Proposition 5.2(iv). We write

$$\mathcal{X}_1 = \left\{ \chi \pmod{q} : \left| \sum_{p \in \mathcal{P}_1} \chi(p) \right| \leq \frac{|\mathcal{P}_1|}{(\log q)^{20}} \right\}$$

and

$$\mathcal{X}_2 = \left\{ \chi \pmod{q} : \chi \neq \chi_0 \text{ and } \left| \sum_{p \in \mathcal{P}_1} \chi(p) \right| > \frac{|\mathcal{P}_1|}{(\log q)^{20}} \right\}.$$

By the definition of $\mathcal{X}_1$, the Cauchy–Schwarz inequality, the mean value theorem (Lemma 3.6) and (10.5), we have

$$\begin{aligned} & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_1} \left| \sum_{p \in \mathcal{P}_1} \chi(p) \right|^2 \left| \sum_{p \in \mathcal{P}_2} \chi(p) \right| \left| \sum_{n \leq q} \chi(n) \sum_{d|n} \lambda_d^+ \right| \\ & \ll \frac{1}{\varphi(q)} \frac{|\mathcal{P}_1|^2}{(\log q)^{40}} \left(\sum_{\chi \pmod{q}} \left| \sum_{p \in \mathcal{P}_2} \chi(p) \right|^2 \right)^{1/2} \left(\sum_{\chi \pmod{q}} \left| \sum_{n \leq q} \chi(n) \sum_{d|n} \lambda_d^+ \right|^2 \right)^{1/2} \\ & \ll \frac{1}{\varphi(q)} \frac{|\mathcal{P}_1|^2}{(\log q)^{40}} (q |\mathcal{P}_2|)^{1/2} (q \cdot q \log q)^{1/2} \ll \frac{|\mathcal{P}_1|^2 |\mathcal{P}_2|^2}{(\log q)^{20} \varphi(q)}. \end{aligned}$$

For $\chi \in \mathcal{X}_2$, we note that by the Burgess bound (Lemma 3.2), for some $\eta > 0$,

$$\left| \sum_{n \leq q} \chi(n) \sum_{d|n} \lambda_d^+ \right| = \left| \sum_{d \leq q^\theta} \lambda_d^+ \chi(d) \sum_{n \leq q/d} \chi(n) \right| \ll q^{1-\eta}.$$

Hence, choosing $L = \lceil \frac{\log q}{\log y} \rceil$ and applying Hölder's inequality, we obtain

$$\begin{aligned} & \frac{1}{\varphi(q)} \sum_{\chi \in \mathcal{X}_2} \left| \sum_{p \in \mathcal{P}_1} \chi(p) \right|^2 \left| \sum_{p \in \mathcal{P}_2} \chi(p) \right| \left| \sum_{n \leq q} \chi(n) \sum_{d|n} \lambda_d^+ \right| \\ & \ll \frac{(q^{1-\eta})^{2/L}}{\varphi(q)} \left(\sum_{\chi \in \mathcal{X}_2} \left| \sum_{p \in \mathcal{P}_1} \chi(p) \right|^{2L} \right)^{\frac{1}{L}} \left(\sum_{\chi \in \mathcal{X}_2} \left| \sum_{p \in \mathcal{P}_2} \chi(p) \right|^2 \right)^{1/2} \left(\sum_{\chi \in \mathcal{X}_2} \left| \sum_{n \leq q} \chi(n) \sum_{d|n} \lambda_d^+ \right|^2 \right)^{\frac{1}{2} - \frac{1}{L}}. \end{aligned}$$

Applying Lemma 3.6 to each mean square and using (10.3) with $\eta' = \eta/(10L)$, we see that the above expression is

$$\ll \frac{(q^{1-\eta})^{2/L}}{\varphi(q)} (y^{2L} (\log q)^{L-1})^{\frac{1}{L}} (q|\mathcal{P}_2|)^{1/2} (q \cdot q \log q)^{\frac{1}{2} - \frac{1}{L}} \ll \frac{|\mathcal{P}_1|^2 |\mathcal{P}_2|^2}{q^{\eta/L} \varphi(q)}.$$

This completes the proof of (10.11). $\square$

ACKNOWLEDGMENTS

KM was supported by Academy of Finland grant no. 285894. JT was supported by Academy of Finland grant no. 340098, a von Neumann Fellowship (NSF grant no. DMS-1926686), and funding from the European Union's Horizon Europe research and innovation programme under Marie Skłodowska-Curie grant agreement no. 101058904. The authors would like to thank Igor Shparlinski for useful discussions and for pointing out the paper [28]. The authors are also grateful to the anonymous referee for helpful comments and corrections.

REFERENCES

- [1] R. Balasubramanian, O. Ramaré, and P. Srivastav. Product of three primes in large arithmetic progressions. *Int. J. Number Theory*, 19(4):843–857, 2023.
- [2] K. Benli. Small prime k th power residues. *Proc. Amer. Math. Soc.*, 148(9):3801–3809, 2020.
- [3] A. Dunn, B. Kerr, I. E. Shparlinski, and A. Zaharescu. Bilinear forms in Weyl sums for modular square roots and applications. *Adv. Math.*, 375:107369, 58, 2020.
- [4] P. Erdős, A. M. Odlyzko, and A. Sárközy. On the residues of products of prime numbers. *Period. Math. Hungar.*, 18(3):229–239, 1987.
- [5] J. Friedlander and H. Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.
- [6] B. Green. Roth's theorem in the primes. *Ann. of Math. (2)*, 161(3):1609–1636, 2005.
- [7] B. Green and T. Tao. Restriction theory of the Selberg sieve, with applications. *J. Théor. Nombres Bordeaux*, 18(1):147–182, 2006.
- [8] D. J. Grynkiewicz. On extending Pollard's theorem for t -representable sums. *Israel J. Math.*, 177:413–439, 2010.
- [9] D. R. Heath-Brown. Zero-free regions for Dirichlet L -functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc. (3)*, 1992.
- [10] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.
- [11] O. Klurman, A. P. Mangerel, and J. Teräväinen. Multiplicative functions in short arithmetic progressions. *Proc. Lond. Math. Soc. (3)*, 127(2):366–446, 2023.
- [12] H. Li and H. Pan. A density version of Vinogradov's three primes theorem. *Forum Math.*, 22(4):699–714, 2010.
- [13] U. V. Linnik. On the least prime in an arithmetic progression. I. The basic theorem. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):139–178, 1944.

- [14] U. V. Linnik. On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):347–368, 1944.
- [15] K. Matomäki. On signs of Fourier coefficients of cusp forms. *Math. Proc. Cambridge Philos. Soc.*, 152(2):207–222, 2012.
- [16] K. Matomäki, J. Maynard, and X. Shao. Vinogradov’s theorem with almost equal summands. *Proc. Lond. Math. Soc. (3)*, 115(2):323–347, 2017.
- [17] K. Matomäki and X. Shao. Vinogradov’s three primes theorem with almost twin primes. *Compos. Math.*, 153(6):1220–1256, 2017.
- [18] P. Pollack. Bounds for the first several prime character nonresidues. *Proc. Amer. Math. Soc.*, 145(7):2815–2826, 2017.
- [19] S. Prendiville. Four variants of the Fourier-analytic transference principle. *Online J. Anal. Comb.*, (12):Paper No. 5, 25, 2017.
- [20] J.-C. Puchta. Primes in short arithmetic progressions. *Acta Arith.*, 106(2):143–149, 2003.
- [21] O. Ramaré, P. Srivastav, and O. Serra. Product of primes in arithmetic progressions. *Int. J. Number Theory*, 16(4):747–766, 2020.
- [22] X. Shao. A density version of the Vinogradov three primes theorem. *Duke Math. J.*, 163(3):489–512, 2014.
- [23] B. Szabó. On the existence of products of primes in arithmetic progressions. *arXiv e-prints*, page arXiv:2208.05762, August 2022.
- [24] T. Tao and V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.
- [25] A. Walker. Topics in analytic and combinatorial number theory. PhD thesis. University of Oxford, 2018.
- [26] A. Walker. A multiplicative analogue of Schnirelmann’s theorem. *Bull. Lond. Math. Soc.*, 48(6):1018–1028, 2016.
- [27] T. Xylouris. *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, volume 404 of *Bonner Mathematische Schriften [Bonn Mathematical Publications]*. Universität Bonn, Mathematisches Institut, Bonn, 2011. Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.
- [28] L. Zhao. On products of primes and almost primes in arithmetic progressions. *Acta Arith.*, 204(3):253–267, 2022.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF TURKU, 20014 TURKU, FINLAND
 Email address: ksmato@utu.fi

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF TURKU, 20014 TURKU, FINLAND
 Email address: joni.p.teravainen@gmail.com