hexagon:2611.00341v1

AN UNCONDITIONAL ARTIN–MATTHEWS THEOREM FOR SIMULTANEOUS PRIMITIVE ROOTS

VLADO VOJDANOVSKI

Abstract. Let S be a finite set of integers different from 0 and ± 1. We prove that the primes for which every member of S is a primitive root have positive lower relative density precisely when neither of Matthews' two obstructions occurs. The proof uses the marked estimates for prime predecessors and uniform splitting estimates of OpenAI. Its principal step is a refinement of the large-prime-factor law for prime predecessors by a fixed cubic Frobenius condition. We obtain this refinement from a shifted bilinear estimate for cubic theta series, a divisor-weighted positive sieve estimate, and a prime-extraction argument that retains the natural Hecke coefficients. The resulting lower bound holds in every sufficiently large dyadic interval.

1. Introduction

For a nonempty finite set

$$S = \{a_1, \dots, a_r\} \subset \mathbb{Z} \setminus \{0, 1, -1\},$$

write $\mathcal{P}_S$ for the primes $p \nmid a_1 \cdots a_r$ such that

$$\operatorname{ord}_p(a_i) = p - 1 \qquad (1 \le i \le r).$$

There are two elementary obstructions to the infinitude of this set:

(A) The product of some odd-cardinality subset of S belongs to $\mathbb{Q}^{\times 2}$.

(B) The product of some even-cardinality subset of S belongs to $-3\mathbb{Q}^{\times 2}$, and, for every prime $\ell \equiv 1 \pmod 3$, at least one element of S is a cube modulo ℓ.

Here a cube modulo a prime includes zero. The subsets in these conditions consist of distinct elements of S.

Theorem 1.1. *If neither* (A) *nor* (B) *holds, there are constants $c_S > 0$ and x_S such that*

$$\#\{x < p \le 2x : p \in \mathcal{P}_S\} \ge c_S \frac{x}{\log x} \qquad (x \ge x_S). \tag{1.1}$$

Consequently,

$$\liminf_{x \to \infty} \frac{\#(\mathcal{P}_S \cap [1, x])}{\pi(x)} > 0.$$

If either (A) *or* (B) *holds, $\mathcal{P}_S$ is finite.*

Matthews established this obstruction classification under the generalized Riemann hypothesis [4]. Anwar and Pappalardi proved its infinitude direction under Schinzel's Hypothesis H and gave an elementary treatment of the finite obstructions [2]. For one integer, Bhargava has proved positive lower relative density by combining marked Type II estimates with a uniform zero-free half-plane [3]. The conclusion here is likewise a lower-density statement; the exact conjectural density is not needed.

2020 *Mathematics Subject Classification.* Primary 11N64; Secondary 11F30, 11N36, 11R45.

Key words and phrases. Simultaneous primitive roots, cubic characters, shifted convolution, sieve methods, prime predecessors.

The simultaneous problem has an additional cubic feature. Requiring every a_i to be a quadratic nonresidue can force $p \equiv 1 \pmod 3$. One must then ensure that none of the a_i is a cube modulo p. This condition is encoded by Frobenius in

$$K = \mathbb{Q}(\zeta_3, a_1^{1/3}, \dots, a_r^{1/3}),$$

and generally cannot be specified by rational congruences alone. We prove a large-prime-factor law with this fixed Frobenius condition. Once it is available, the remaining index obstructions are removed by uniform splitting estimates and an elementary product argument.

1.1. **The analytic statement.** Fix $0 < \varepsilon < 1/4$ and a nonzero function $\Phi \in C_c^\infty((1,2))$ with $0 \le \Phi \le 1$. Put

$$I_x = (x^{1-\varepsilon}, x^{1-\varepsilon/2}], \qquad f_x(u) = \sum_{\substack{\ell \in I_x \\ \ell \text{ prime}}} \mathbf{1}_{\ell \mid u}, \qquad C_x = \sum_{\substack{\ell \in I_x \\ \ell \text{ prime}}} \frac{1}{\ell}. \tag{1.2}$$

On the support of $\Phi(u/x)$, the function f_x takes only the values zero and one for sufficiently large x. Mertens' theorem gives

$$C_x \longrightarrow c_\varepsilon := \log \frac{1-\varepsilon/2}{1-\varepsilon} > 0. \tag{1.3}$$

Let $F = \mathbb{Q}(\zeta_3)$ and $H = \mathrm{Gal}(K/F)$. Complex conjugation acts by inversion on H. Thus an inversion-stable subset $\mathcal{C} \subset H$ defines an unambiguous Frobenius condition at unramified rational primes that split in F.

Theorem 1.2. *Let $K = F(b_1^{1/3}, \dots, b_s^{1/3})$ for fixed nonzero rational numbers b_i, and let $\mathcal{C} \subset H$ be inversion-stable. Let $3 \mid M$, and let $U \subset (\mathbb{Z}/M\mathbb{Z})^\times$ consist of classes congruent to 1 modulo 3. Then*

$$\begin{aligned} \sum_{\substack{p \text{ prime} \\ p \text{ unramified in } K}} & \Phi\Big(\frac{p-1}{x}\Big) \mathbf{1}_{p \bmod M \in U} \mathbf{1}_{\mathrm{Frob}_p \in \mathcal{C}} f_x(p-1) \\ &= \Big(\frac{|U|}{\varphi(M)} \frac{|\mathcal{C}|}{|H|} c_\varepsilon \int_0^\infty \Phi(t)\, dt + o(1) \Big) \frac{x}{\log x}. \end{aligned} \tag{1.4}$$

Without a Frobenius condition, the same assertion holds for every fixed M and every $U \subset (\mathbb{Z}/M\mathbb{Z})^\times$, with $|\mathcal{C}|/|H|$ omitted.

The proof has three analytic parts. First we extend the interior prime-predecessor law to fixed arithmetic progressions. Next we prove that the nontrivial cubic trace terms have zero mean in the statistic (1.2). This uses a weight-one extension of the shifted bilinear estimate of Assing, Blomer, and Li [1], followed by a positive sieve bound with the divisor function as a majorant. Finally, finite character expansion gives Theorem 1.2.

1.2. **External inputs and notation.** We use the marked Type II coefficient criterion of [6, Lemma 10.2], the correlation and prime-extraction framework of [7, Sections 3–7], and the block sieve of [8, Lemma 2.9]. The precise forms used below are stated where they enter the argument. The Hecke zero-free input is [9, Theorem 1.1 and Lemma 4.8]: finite-order Hecke L-functions over F have no zeros in $\Re s > 7/8$, with conductor-uniform polynomial growth in a fixed strip. The splitting estimate used at the end is [6, Lemmas 9.1–9.2 and proof of Proposition 2.2].

We write $e(t) = \exp(2\pi i t)$, $L = \log x$, and $\tau(n)$ for the divisor function. The functions $\omega(n)$ and $\Omega(n)$ count prime factors without and with multiplicity, respectively, and $P^-(n)$ denotes the least prime factor, with $P^-(1) = \infty$. All implied constants may depend on the fixed field, characters, and smooth functions under discussion. Each modulus and each finite family of auxiliary intervals is fixed before x tends to infinity. The order of the later auxiliary limits will be specified explicitly.

2. Divisor weights and the marked bilinear estimate

We use finite collections of small prime divisors to insert weights into bilinear sums. We give the definitions and the precise external estimate needed below. All numbers of bands and all band exponents in this section are fixed before x tends to infinity.

Put

$$L = \log x, \qquad w_x = \exp(L^{0.24}), \qquad V(y) = \prod_{p \le y} \left(1 - \frac{1}{p}\right).$$

We write $P^-(n)$ for the least prime divisor of $n > 1$, and put $P^-(1) = \infty$. A positive integer n is y-rough if $P^-(n) > y$. Dirichlet characters, including principal characters, are extended by zero on integers not coprime to their modulus.

2.1. The divisor weights.

Fix $K \ge 1$ and $0.1 < \alpha_1 < \cdots < \alpha_K < 0.2$. Set

$$\mathcal{P}_i = \{p \text{ prime} : \exp(L^{\alpha_i}) \le p \le \exp(2L^{\alpha_i})\}, \qquad V_i = \sum_{p \in \mathcal{P}_i} \frac{1}{p}, \qquad \omega_i(u) = \sum_{p \in \mathcal{P}_i} \mathbf{1}_{p|u}.$$

The bands $\mathcal{P}_i$ are disjoint for large x, and $V_i = \log 2 + o(1)$. With $\rho = 1/2$, define

$$W(u) = \prod_{i=1}^{K} \frac{\omega_i(u)\rho^{\omega_i(u)-1}}{V_i}. \tag{2.1}$$

The factor is zero when $\omega_i(u) = 0$. We call the collection of bands, together with this weight, an *array*. The weight is nonnegative, supported on integers having a prime divisor in every band, and bounded by a constant depending only on K for large x. Equivalently, with $\omega_{\mathrm{band}}(u) = \sum_i \omega_i(u)$,

$$W(u) = \rho^{\omega_{\mathrm{band}}(u)-K} \sum_{\substack{p_i \in \mathcal{P}_i \ (1 \le i \le K) \\ p_1 \cdots p_K | u}} \prod_{i=1}^{K} V_i^{-1}.$$

This identity specifies the normalization when one prime divisor is selected from each band. In particular, the sum over selected divisors is a counting sum; the reciprocal factors $1/p_i$ enter its mean.

The *independent divisor model* replaces the indicators $\mathbf{1}_{p|u}$, for all primes in the arrays under consideration, by independent Bernoulli variables of means $1/p$. Denote its expectation by $\mathbb{E}_x$, and put

$$m_W = \mathbb{E}_x W. \tag{2.2}$$

For example, independence between bands gives the exact formula

$$m_W = \prod_{i=1}^{K} \left\{ \prod_{p \in \mathcal{P}_i} \left(1 - \frac{1-\rho}{p}\right) \frac{1}{V_i} \sum_{p \in \mathcal{P}_i} \frac{1}{p - (1-\rho)} \right\}.$$

Consequently, for constants depending on K but not on the fixed band exponents,

$$0 < c_K \le m_W \le C_K, \qquad \mathbb{E}_x(W^2) \le C_K \tag{2.3}$$

for all sufficiently large x. The upper bounds also follow directly from boundedness of W. For the lower bound, the event of exactly one divisor in each band has probability bounded below, since $V_i \longrightarrow \log 2$ and $\sum_{p \in \mathcal{P}_i} p^{-2} \longrightarrow 0$.

Let

$$u_{\mathcal{P}} = \prod_{p \in \bigcup_i \mathcal{P}_i} p^{v_p(u)}.$$

A function $F : \mathbb{N} \to \mathbb{C}$ is *invariant under the band primes* if

$$F(pu) = F(u) \quad (u \geq 1,\ p \in \bigcup_i \mathcal{P}_i). \tag{2.4}$$

Equivalently, $F(u)$ depends only on $u/u_{\mathcal{P}}$. This condition removes the whole band-prime part, including repeated prime factors. The centered large-prime statistic $f_x - C_x$ is invariant in this sense for sufficiently large x.

2.2. **The coefficient criterion.** The following is the coefficient criterion of [6, Lemma 10.2]. Its important uniformity is that the required number K of bands is independent of their particular fixed exponents.

Proposition 2.1 (Marked bilinear estimate)**.** *Fix $\delta, C, D > 0$. Suppose that $H_m, H_n \geq x^\delta$ and $X = H_m H_n \asymp x$, with fixed comparison constants. Let F satisfy $|F| \leq 1$ and (2.4). Let α_m, β_n be supported on w_x-rough integers in $[H_m, 2H_m]$ and $[H_n, 2H_n]$, respectively, with $|\alpha_m|, |\beta_n| \leq L^C$. The support of α may be restricted to any interval $I \subseteq [H_m, 2H_m]$. Assume that, for every fixed $A_0, B, A > 0$, every Dirichlet character ϑ modulo $k \leq L^{A_0}$, and every $|t| \leq 2XL^B$,*

$$\frac{1}{H_m}\left|\sum_m \alpha_m \vartheta(m) m^{it}\right| \ll_A L^{-A}, \tag{2.5}$$

uniformly in the interval, character, and frequency. Constants in this hypothesis may depend on all fixed parameters defining the coefficient. Then, for sufficiently large fixed K,

$$\left|\sum_{m,n} \alpha_m \beta_n F(mn-1) W(mn-1)\right| \ll XL^{-D}. \tag{2.6}$$

The required lower bound on K is independent of the band exponents α_i. The implicit constant and the threshold for x may depend on those exponents and on all other fixed data.

The version with prime-minus-rough coefficients is [7, Theorem 3.1]. In particular, the sequence

$$\alpha_m = m^{iv}\left(\mathbf{1}_{m \text{ prime}} - \frac{\mathbf{1}_{P^-(m) > w_x}}{V(w_x)\log m}\right), \qquad |v| \leq L^C, \tag{2.7}$$

restricted to a permitted interval, satisfies (2.5) by [7, Lemma 5.2]. Multiplying this coefficient by a fixed Dirichlet character preserves the criterion: the product with a test character has modulus at most $ML^{A_0} \leq L^{A_0+1}$ for all sufficiently large x, where M is fixed. This observation will be used for fixed arithmetic progressions.

2.3. **Removing the divisor weights at primes.** We also record the positive estimate that will remove these weights. Choose b arrays $W_1, \dots, W_b$, each with K bands, so that all their band exponents are distinct. Write $m_j = \mathbb{E}_x W_j$ and

$$Z_b(u) = \left(\frac{1}{b}\sum_{j=1}^{b} \frac{W_j(u)}{m_j} - 1\right)^2.$$

Disjoint arrays are independent in the divisor model. Thus

$$\mathbb{E}_x Z_b = \frac{1}{b^2}\sum_{j=1}^{b} \mathrm{Var}_x(W_j/m_j) \leq \frac{C_K}{b}. \tag{2.8}$$

For every fixed nonnegative smooth compactly supported Φ on $(0, \infty)$, the prime version is

$$\limsup_{x\to\infty} \frac{L}{x} \sum_{p \text{ prime}} \Phi((p-1)/x) Z_b(p-1) \ll_\Phi \frac{C_K}{b}. \tag{2.9}$$

The constant is independent of b and of the fixed band exponents. Here and below b is fixed while taking the limit in x.

For completeness, this estimate uses only the progression calculation and the positive sieve in [7, §7]. The summed progression estimate of [7, Lemma 7.2], with the large-prime statistic omitted, applies to Z_b: its expansion contains constants, single arrays, and products of two arrays, including repeated arrays. Apply the upper bound in the block sieve of [7, Lemma 2.6] at depth 2, with $z = x^{c_0/20}$ for a fixed permitted progression exponent $c_0 > 0$. Its divisor level is $z^{10} = x^{c_0/2}$, inside that progression range. Every prime p in the support exceeds z, so its contribution is bounded by the sifted nonnegative weight. The main term is $O_\Phi(x\mathbb{E}_x Z_b/\log z)$, and the summed remainder is $o(x/L)$. Equation (2.8) proves (2.9).

In particular, if $|a_p| \le C$ at primes, Cauchy's inequality and the prime number theorem give

$$\limsup_{x\to\infty} \frac{L}{x}\left|\sum_p \Phi((p-1)/x)a_p\left(\frac{1}{b}\sum_{j=1}^{b}\frac{W_j(p-1)}{m_j}-1\right)\right| \ll_{\Phi,C} \sqrt{\frac{C_K}{b}}. \tag{2.10}$$

This estimate concerns bounded prime coefficients; it requires no bound for their extension to composite integers.

3. A giant prime factor in a fixed progression

The distribution of a large prime factor of $p-1$ will be needed with p restricted to a fixed residue class. We prove this extension here. The modulus remains fixed throughout the argument.

Proposition 3.1. *Let $M \ge 1$, let $U \subset (\mathbb{Z}/M\mathbb{Z})^\times$, and put*

$$B_U(n) = \mathbf{1}_{n \bmod M \in U}, \qquad d_U = \frac{|U|}{\varphi(M)}.$$

For the giant-factor statistic f_x and reciprocal sum C_x defined above, and any fixed smooth function Φ of compact support in $(0,\infty)$, one has

$$\sum_{p \text{ prime}} \Phi\left(\frac{p-1}{x}\right) B_U(p)(f_x(p-1) - C_x) = o\left(\frac{x}{\log x}\right). \tag{3.1}$$

Consequently,

$$\sum_{p \text{ prime}} \Phi\left(\frac{p-1}{x}\right) B_U(p) f_x(p-1) = \left(d_U c_\varepsilon \int_0^\infty \Phi(t)\,dt + o(1)\right)\frac{x}{\log x}. \tag{3.2}$$

All constants may depend on M, U, ε, and Φ.

The proof extends the prime extraction in [7, Section 7]. There are three points to check: the one-sided replacement of a prime factor, the two-sided correlation after the small prime factors have been removed, and the positive sieve used to remove the auxiliary weights. We give these checks explicitly.

3.1. Character twists in the replacement estimates.

Retain the roughness threshold w_x and the sieve product V from Section 2. For a fixed Dirichlet character χ modulo M, the replacement coefficient is

$$\alpha_\chi(m) = \chi(m)m^{iv}\left(\mathbf{1}_{m \text{ prime}} - \frac{\mathbf{1}_{P^-(m)>w_x}}{V(w_x)\log m}\right), \tag{3.3}$$

restricted to the interval occurring in the replacement. Dirichlet characters are extended by zero on nonunits.

The marked coefficient estimate [6, Lemma 10.2] applies to (3.3). Indeed, testing this coefficient against a character θ of modulus at most L^A gives the original prime-minus-rough coefficient tested

against $\chi\theta$. The latter has a modulus at most ML^A, and hence at most L^{A+1} for sufficiently large x. The long-coefficient estimate [7, Lemma 5.2], with this larger fixed exponent, supplies every required logarithmic saving, uniformly in the interval and the prescribed frequency range. This also applies to the conjugate coefficient. Rough support and size bounds are unchanged. In particular, the second coefficient may be multiplied by $\chi(n)$ as well. The number of marking bands can be chosen independently of their particular admissible exponents.

The corresponding two-sided assertion requires a separate argument: a character of an integer need not be unchanged when an active prime factor is removed. We recall the notation needed for that argument. Let $\mathcal{P}_g$ be the disjoint active prime groups in [7, Section 6], let

$$V_g = \sum_{q\in\mathcal{P}_g} \frac{1}{q}, \qquad \omega_g(n) = \sum_{q\in\mathcal{P}_g} \mathbf{1}_{q|n}, \qquad \omega_{\mathcal{P}}(n) = \sum_g \omega_g(n),$$

and let n_* be obtained from n by removing all powers of primes in $\mathcal{P} = \bigcup_g \mathcal{P}_g$. There are $O(\log L)$ groups, each with reciprocal mass bounded above and below by fixed positive constants; the small groups lie between $\exp(L^{0.27})$ and $\exp(L^{0.36})$, and the large groups between $\exp(L^{0.39})$ and $\exp(L^{0.46})$. For their fixed damping parameter $0 < q_0 < 1$, put

$$A_{\mathbf{t}}(n) = q_0^{\omega_{\mathcal{P}}(n)-\sum_g t_g} \prod_g \frac{(\omega_g(n))_{t_g}}{V_g^{t_g}}, \qquad A_1 = A_{(1,\dots,1)},$$

where $(u)_t = u(u-1)\cdots(u-t+1)$, and the weight is zero if some $\omega_g(n) < t_g$. Bounded tests on the represented prime lists are allowed in these weights. For bounded t_g they have size $L^{O(1)}$. The fixed marking array W uses smaller primes and is disjoint from these groups. Define

$$F_x(w) = W(w)\big(f_x(w) - C_x\big).$$

Both W and f_x are invariant under multiplication by any active prime, including its higher powers. The same is therefore true of F_x.

Lemma 3.2. *Let $G(n) = G(n_*)$ and suppose $|G(n)| \le L^C \tau(n_*)^C$ for a fixed C. For every fixed smooth compactly supported Ψ and every $A > 0$,*

$$\sum_{w\ge 1} \frac{\Psi(w/x)}{w} F_x(w)\chi(w+1)G(w+1)A_1(w)A_1(w+1) \ll L^{-A}. \tag{3.4}$$

Proof. We modify the graph proof of [7, Theorem 6.1]. In its physical coordinates an edge joins n to $n' = n + D$, where $D = D_R D_C$ is the product of its prime labels. The factor D_R consists of labels shared by the two endpoints; D_C consists of the remaining labels. For large x, every label is prime to M.

Use $\chi(n')G(n')$ at the second endpoint and multiply the edge by $\overline{\chi(D)}$. This modification is allowed by the graph transference estimate [7, Proposition 6.2]. To see this, write $e(t) = \exp(2\pi i t)$ and expand

$$\overline{\chi(D)} = \sum_{r \bmod M} c_r e(rD/M), \qquad c_r = \frac{1}{M} \sum_{a \bmod M} \overline{\chi(a)} e(-ra/M).$$

Parseval and Cauchy's inequality give $\sum_r |c_r| \le \sqrt{M}$. Since

$$e(rD/M) = e(rn'/M)e(-rn/M),$$

each summand is the original graph pairing with both endpoint vectors multiplied by $e(rn/M)$, using conjugation at the first endpoint in the inner product. These phases preserve all norms, supports, and independence from the sampled prime labels. The factor $\chi(n')$ can only decrease absolute values. Thus the same transference bound and the same finite family of comparison patterns [7, Proposition 6.3] apply. Separating the smooth factor by Mellin inversion commutes with this finite Fourier expansion.

Recombine the Fourier sum before removing the shared labels. On writing $n = D_R w$ and $n' = D_R(w + D_C)$, the character factors become

$$\overline{\chi(D_R D_C)}\chi(D_R(w + D_C)) = \overline{\chi(D_C)}\chi(w + D_C). \tag{3.5}$$

This identity includes nonunits $w + D_C$, when both sides vanish. The invariant cores can now be stripped exactly as in the original proof. Their reciprocal prime factors and damping weights are unchanged; all collision errors have the original positive bounds. The pattern with $D_C = 1$ is precisely (3.4).

For a comparison pattern, $D_C = D_A D_B$, with the two free prime products sampled independently. Its separated expression has the form

$$\mathbb{E}\, b_1(D_A) b_2(D_B) \sum_w \mathcal{U}(w)\mathcal{V}(w + D_A D_B), \qquad |b_1|, |b_2| \le 1.$$

Here $\mathcal{U}$ and $\mathcal{V}$ are the first and second endpoint sequences, including their smooth cutoffs and marked weights; the expectation uses the reciprocal-prime measures of the two free lists. Equation (3.5) replaces these three factors by

$$b_1(D_A)\overline{\chi(D_A)}, \qquad b_2(D_B)\overline{\chi(D_B)}, \qquad \chi(y)\mathcal{V}(y),$$

respectively, and leaves $\mathcal{U}$ unchanged. The comparison estimates in [7, Section 6] allow arbitrary bounded free-list tests. They use the second endpoint only through its global square norm and coefficient mean-square bounds, which are preserved here. Their local Fourier-energy and divisor-model cancellation estimates act on the unchanged first endpoint. Hence each comparison retains its arbitrary logarithmic saving. Subtracting the comparison terms from the graph estimate proves the lemma. □

3.2. **The positive sieve in residue classes.** We may assume $\Phi \ge 0$, by decomposing a general smooth function into finitely many such functions with scalar coefficients. Let H be a fixed marking-array weight, a product of two such weights, or a fixed linear combination of these, and write $\mathbb{E}_x(H)$ for its independent-divisor-model mean. Choose $0 < c_0 < \varepsilon/4$. The progression estimate [7, Lemma 7.2] has the following version:

$$\sum_{r \le x^{c_0}} \Bigg| \sum_{\substack{u \ge 1 \\ r \mid u+1}} \Phi(u/x) B_U(u+1) f_x(u) H(u) - \frac{|U|}{M} \frac{\mathbf{1}_{(r,M)=1}}{r}\, x C_x \mathbb{E}_x(H) \int_0^\infty \Phi(t)\, dt \Bigg| \ll_A x L^{-A}. \tag{3.6}$$

The same formula holds with f_x and C_x replaced by 1.

Here is the modification of its proof. Expand H by the represented-divisor expansion used in that lemma, keeping its positive Bonferroni remainder. Each retained divisor d' is composed of marking primes and has size $x^{o(1)}$; its total coefficient mass is $x^{o(1)}$. For a giant prime ℓ write $u = \ell y$. Both ℓ and d' are prime to the fixed M for large x. If $(r, M) > 1$, no term is possible. If $(r, M) = 1$, the congruences for a given $a \in U$ are

$$\ell y \equiv -1 \pmod r, \qquad \ell y \equiv a - 1 \pmod M, \qquad d' \mid y.$$

When $(d', r) = 1$, smooth counting in the resulting progression gives

$$\frac{x}{M r \ell d'} \int_0^\infty \Phi(t)\, dt + O_\Phi(1);$$

otherwise there is no solution. There is no need for $a - 1$ to be a unit modulo M. The total rounding error is $x^{1-\varepsilon/2+c_0+o(1)}$, and the positive remainder and the exclusion of marking primes dividing r have the bounds of [7, Lemma 7.2]. This proves (3.6) with the same model mean.

The local density of the condition $q \mid u+1$ in this calculation is

$$g(q) = \begin{cases} 0, & q \mid M, \\ 1/q, & q \nmid M. \end{cases}$$

For z larger than the prime divisors of M,

$$\prod_{q \le z} (1 - g(q)) = \frac{M}{\varphi(M)} V(z). \tag{3.7}$$

The initial density $|U|/M$ therefore becomes d_U at prime scale. Apply the positive block sieve [7, Lemma 2.6], equivalently the block construction of [8, Lemma 2.9], with fixed even h and

$$\gamma = \frac{c_0}{4h+3}, \qquad z = x^{\gamma}.$$

Its divisor level is at most $z^{4h+2} < x^{c_0}$, as required by (3.6). Subtracting C_x times the formula without f_x cancels the main terms. For a fixed nonnegative array W, of mean m_W, this gives

$$\limsup_{x \to \infty} \frac{L}{x m_W} \left| \sum_{\substack{n \ge 1 \\ P^-(n) > x^{\gamma}}} \Phi\left(\frac{n-1}{x}\right) B_U(n) W(n-1) \big(f_x(n-1) - C_x\big) \right| \ll \frac{e^{-h}}{\gamma}. \tag{3.8}$$

The surviving constant may depend on the fixed progression and cutoff, but not on the number or positions of the fixed marking bands. The factor m_W occurs in both sieve main terms. Errors depending on the particular array disappear in the x-limit.

3.3. **Prime extraction and removal of the arrays.** Expand the residue-class indicator as

$$B_U(v) = \sum_{\chi \bmod M} b_\chi \chi(v), \qquad b_\chi = \frac{1}{\varphi(M)} \sum_{a \in U} \overline{\chi(a)}. \tag{3.9}$$

The identity holds on nonunits as well. In the composite removal of [7, Section 7], a rough $v \asymp x$ is written as a product of a bounded number of prime factors, the bound depending on γ. Telescope each character term using (3.3). The other factors carry the corresponding multiplicative character values. All one-sided replacement errors have arbitrary logarithmic saving, while the predecessor core remains $f_x(v-1) - C_x$, clipped outside the required range if necessary. This clipping preserves its invariance under marking primes.

In the subsequent allocation of active prime factors, retain $\chi(v)$ as a factor of the whole integer v. It is the same for every allocation of a fixed factorization. Thus the exact allocation counts and damping identities are unchanged. The errors in replacing thresholds and logarithms by their stripped versions are bounded by the same positive expressions as before, since $|\chi(v)| \le 1$; the positive estimates controlling unsuccessful allocations are likewise unchanged. The remaining invariant core $G(v_*)$ is therefore the original one. Every final two-sided correlation is (3.4). Lemma 3.2 bounds these correlations with enough logarithmic saving to absorb the polynomial in L cost of the finite expansions. Each composite contribution is $o(x/L)$. Consequently (3.8) also holds with its rough sum replaced by the sum over primes.

For completeness, the last removal of the fixed arrays uses a positive estimate. Choose b disjoint arrays $W_1, \dots, W_b$, each with the sufficient fixed number K of bands, and let m_j be their model means. Put

$$Z_b(u) = \left| \frac{1}{b} \sum_{j=1}^{b} \frac{W_j(u)}{m_j} - 1 \right|^2 .$$

Apply (3.6) without the giant factor to the expansion of this nonnegative square, followed by the upper sieve. The independent model for disjoint arrays, as in the deweighting step of [7, Section 7], gives

$$\limsup_{x\to\infty}\frac{L}{x}\sum_{p\ \text{prime}}\Phi\left(\frac{p-1}{x}\right)B_U(p)Z_b(p-1)\ll\frac{C_K}{b}.$$

Cauchy's inequality, the boundedness of f_x-C_x on the support, and the prime-count upper bound now give

$$\limsup_{x\to\infty}\frac{L}{x}\left|\sum_{p\ \text{prime}}\Phi\left(\frac{p-1}{x}\right)B_U(p)(f_x(p-1)-C_x)\right|\ll\frac{e^{-h}}{\gamma}+\sqrt{\frac{C_K}{b}}.$$

First fix h,γ,K,b and the arrays, and take $x\to\infty$. Next let $b\to\infty$ with h,K fixed. Finally let the even integer $h\to\infty$, choosing a sufficient K each time. Since $\gamma^{-1}=(4h+3)/c_0$, both errors vanish. This proves (3.1). The prime number theorem in the fixed residue classes, together with $C_x\to c_\varepsilon$, proves (3.2) and completes the proof of Proposition 3.1.

4. Cubic Hecke characters and the prime coefficient estimate

Let η be a nontrivial cubic Hecke character of $F=\mathbb{Q}(\zeta_3)$ satisfying $\eta^\sigma=\eta^{-1}$, where σ is complex conjugation. Extend η by zero on ideals not coprime to its conductor, and define

$$L_F(s,\eta)=\sum_{n\ge1}\frac{\lambda_\eta(n)}{n^s},\qquad\lambda_\eta(n)=\sum_{\mathrm{N}\,\mathfrak{a}=n}\eta(\mathfrak{a}).\tag{4.1}$$

The classical theta-series construction [5, §4.8] associates to this series a holomorphic cuspidal newform of weight one. Its nebentypus is $\psi=\chi_{-3}$. Indeed, the restriction of η to rational ideles is both invariant under conjugation and equal to its inverse, and has order dividing three; it is therefore trivial. Cuspidality follows from $\eta\neq\eta^\sigma$. The induced representation is self-dual, so its coefficients are real, including at ramified primes.

The ideal formula, or the degree-two Euler factors, gives

$$|\lambda_\eta(n)|\le\tau(n),\qquad\lambda_\eta(mn)=\lambda_\eta(m)\lambda_\eta(n)\quad((m,n)=1).\tag{4.2}$$

At an unramified prime set

$$t_\eta(p)=\begin{cases}\eta(\mathfrak{p})+\eta(\overline{\mathfrak{p}}), & p=\mathfrak{p}\overline{\mathfrak{p}}\ \text{in } F,\\ 0, & p\ \text{inert in } F.\end{cases}$$

At the finitely many ramified primes put $t_\eta(p)=\lambda_\eta(p)$. Thus $\lambda_\eta(p)=t_\eta(p)$ and $|t_\eta(p)|\le2$ at every prime. At an inert prime the Euler factor is $(1-p^{-2s})^{-1}$. At a split prime with trace 2, the coefficients at p^j are $j+1$; with trace -1 they are $1,-1,0,1,-1,0,\dots$. These formulas will allow us to keep the prime-power coefficients until their contribution has been estimated.

Lemma 4.1. *Fix $A_0,B,A,\delta,C>0$. Uniformly for Dirichlet characters θ of modulus $k\le L^{A_0}$, intervals $J\subset[H,2H]$ with $x^\delta\le H\le x^C$, and $|t|\le x^B$, one has*

$$\frac{1}{H}\left|\sum_{p\in J}t_\eta(p)\theta(p)p^{it}\right|\ll_{\eta,A_0,B,A,\delta,C}L^{-A}.\tag{4.3}$$

The same holds after inserting any fixed Dirichlet character.

Proof. Put $\xi=\eta(\theta\circ\mathrm{N}_{F/\mathbb{Q}})$. The norm pullback is invariant under σ. If ξ were principal, η would be invariant as well, contrary to $\eta^\sigma=\eta^{-1}\neq\eta$. The primitive character inducing ξ is thus nonprincipal and has conductor norm $Q_\xi\ll_\eta k^2$.

The zero-free and strip-growth theorems in [9] imply

$$\left|\frac{L_F'}{L_F}(15/16+iT,\xi)\right| \ll_\eta \log(Q_\xi(3+|T|)). \tag{4.4}$$

Here is the uniformity argument. The disk centered at $2+iT$ with radius $35/32$ lies in $\Re s > 7/8$. Choose an analytic logarithm of $L_F(s,\xi)$ on the disk, normalized by the Euler series at its center. The strip-growth bound controls the real part of this logarithm by $O(\log(Q_\xi(3+|T|)))$, while the value at the center is bounded. The Borel–Carathéodory theorem, followed by Cauchy's estimate on two slightly smaller disks, gives (4.4), since the point $15/16+iT$ is at distance $34/32$ from the center. The omitted Euler factors of an imprimitive character contribute $O(\log(2k))$ there.

For a smooth function g supported in a fixed positive dyadic interval, Mellin inversion of $-L_F'/L_F$, with the oscillation carried in its height variable, gives

$$\begin{aligned}\sum_{\mathfrak{p}}\sum_{j\ge1}\xi(\mathfrak{p})^j \log \mathrm{N}\,\mathfrak{p}\, g\left(\frac{(\mathrm{N}\,\mathfrak{p})^j}{H}\right)(\mathrm{N}\,\mathfrak{p})^{ijt}\\ \ll_g H^{15/16}\log(Q_\xi(3+|t|)).\end{aligned} \tag{4.5}$$

We shifted the line of integration to $15/16$; nonprincipality and zero-freeness ensure that no pole is crossed. The terms with residue degree or exponent at least two contribute $O(H^{1/2}(\log H)^2)$. The remaining terms are precisely the rational prime sum with coefficient $t_\eta(p)\theta(p)\log p$, apart from finitely many ramified primes.

To pass to an arbitrary interval J, smooth its endpoints in intervals of length HL^{-D}. The derivative and Mellin norms increase by fixed powers of L, and the boundary error is at most $O(HL^{-D}\log H+\log H)$ by counting integers. Choose D after A. Since $H\ge x^\delta$, the factor $H^{-1/16}$ absorbs every such logarithmic loss. Partial summation removes $\log p$ and proves the claim. A fixed extra character only changes the conductor by a fixed factor and hence is covered by increasing A_0. □

Combining Lemma 4.1 with Proposition 2.1 applies the marked Type II estimate to the prime-supported coefficient

$$\alpha_m = \mathbf{1}_{m \text{ prime}}\lambda_\eta(m)\chi(m)m^{iv}, \qquad |v|\le L^C,$$

with zero comparison term. In particular, for every prescribed logarithmic saving and sufficiently many fixed marking intervals,

$$\sum_{m,n}\alpha_m\beta_n G(mn-1)W(mn-1) \ll xL^{-A} \tag{4.6}$$

in the ranges of that proposition. The second coefficient may be any allowed rough sequence of logarithmic size. The function G is invariant under multiplication by marking primes; the trace is placed in α, where Lemma 4.1 supplies its cancellation.

5. A shifted bilinear estimate at weight one

Let $\varphi=\theta_\eta$ be the weight-one theta series attached to the cubic character η over $F=\mathbb{Q}(\zeta_3)$. Its level N is fixed, its nebentypus is the quadratic character $\psi=\chi_{-3}$, and its Fourier expansion is

$$\varphi(z)=\sum_{n\ge1}\lambda_\eta(n)e(nz), \qquad e(t)=\exp(2\pi it).$$

The coefficients are real and satisfy $|\lambda_\eta(n)|\le\tau(n)$. This section proves the estimate needed when a large prime factor is separated from its small cofactor.

Proposition 5.1. *Let $\Phi \in C_c^\infty((0,\infty))$ be fixed, let $X \geq 2$, and let $1 \leq M_1 \leq M_2$. Suppose that $|\alpha_m|, |\beta_n| \leq 1$ and that α_m is supported on squarefree positive integers. For every $\nu > 0$,*

$$\left| \sum_{M_1 \leq m \leq M_2} \sum_{n \geq 1} \alpha_m \beta_n \Phi(mn/X) \lambda_\eta(mn+1) \right| \ll_{\eta,\Phi,\nu} X^\nu \left(X M_1^{-1/2} + X^{7/8} M_2^{3/8} \right). \tag{5.1}$$

There is no coprimality restriction on m and no further restriction on β_n.

We adapt the argument of Assing–Blomer–Li [1, Theorem 2.4 and Sections 8.2–8.3]. Their Voronoi formula is stated for trivial nebentypus. We first establish the formula for φ and calculate the character factors in its two applications.

5.1. **Voronoi summation and coefficient norms.** Suppose that $N \mid q$ and $(a,q) = 1$. Choose integers b, d with $ad - bq = 1$. Applying the modular transformation $\left(\begin{smallmatrix} a & b \\ q & d \end{smallmatrix}\right)$ to $-d/q + i/(q^2 y)$ gives

$$\varphi(a/q + iy) = \psi(d) \frac{i}{qy} \varphi(-d/q + i/(q^2 y)). \tag{5.2}$$

Here $\psi(d) = \psi(a)$ because ψ is quadratic. Mellin inversion of (5.2) yields, for $H \in C_c^\infty((0,\infty))$,

$$\sum_{n \geq 1} \lambda_\eta(n) e(an/q) H(n) = \frac{\psi(d)}{q} \sum_{n \geq 1} \lambda_\eta(n) e(-dn/q) \mathcal{H}(n/q^2), \tag{5.3}$$

$$\mathcal{H}(y) = 2\pi i \int_0^\infty H(x) J_0(4\pi\sqrt{xy})\, dx.$$

Cuspidality justifies the Mellin integrals at both endpoints. The formula has a single holomorphic Bessel transform. The estimates for this transform follow by the integration-by-parts argument in [1, Lemma 7.5], with $J_{k-1} = J_0$.

We also need a coefficient estimate uniform in an additive frequency. The function $(\operatorname{Im} z)^{1/2} |\varphi(z)|$ is invariant under $\Gamma_0(N)$ and bounded on a fundamental domain: it is bounded on the compact part and tends to zero at each cusp. Thus

$$\sup_{z \in \mathbb{H}} (\operatorname{Im} z)^{1/2} |\varphi(z)| < \infty.$$

For $T \geq 2$, put $y = 1/T$ in the Fourier expansion and convolve over one period with

$$D_T(t) = \sum_{1 \leq j \leq T} \exp(2\pi j/T) e(jt).$$

Partial summation of the Dirichlet kernel gives $\|D_T\|_1 \ll \log(2T)$. The convolution cancels the factors $\exp(-2\pi n/T)$ for $n \leq T$, and consequently

$$\sup_{\theta \in \mathbb{R}} \left| \sum_{n \leq T} \lambda_\eta(n) e(n\theta) \right| \ll_\eta T^{1/2} \log(2T). \tag{5.4}$$

A smooth dyadic cutoff and a factor n^{-it} may be inserted by partial summation, at the cost of $O(1 + |t|)$ and the cutoff seminorms. The elementary bound by τ also gives

$$\sum_{n \leq T} |\lambda_\eta(n)|^2 \ll_\nu T^{1+\nu}. \tag{5.5}$$

For later use, fix coprime m_3, m_4, a positive integer D, and smooth cutoffs w_j supported on $k_j \asymp K_j$. Define

$$A_\rho = \sum_{\substack{m_4 k_2 - m_3 k_1 = \rho \\ m_3^2 k_1 \equiv m_4^2 k_2 \pmod D}} \lambda_\eta(k_1) \lambda_\eta(k_2) k_1^{-it_1} k_2^{-it_2} w_1(k_1) w_2(k_2).$$

Expand the congruence as a normalized average of D additive characters. For each character, A_ρ is the coefficient sequence of a product of two trigonometric polynomials, with frequencies $-m_3k_1$ and m_4k_2. Parseval, the supremum bound (5.4) on one factor, and (5.5) on the other imply

$$\|A\|_2 \ll_{\eta,\nu,w_1,w_2} (K_1K_2)^{(1+\nu)/2}(1+|t_1|+|t_2|)^2. \tag{5.6}$$

The triangle inequality for the normalized character average introduces no factor of D.

5.2. **The double Voronoi transformation.** We first restrict the small variables to be coprime to N. Let $m_1, m_2 \asymp M$ be distinct squarefree integers, with $(m_1m_2, N) = 1$, and write

$$d = (m_1, m_2), \qquad m_1 = dm_3, \quad m_2 = dm_4, \qquad D = (m_1 - m_2, d^\infty), \quad F_0 = ND^2.$$

The notation (v, d^∞) means the largest divisor of $|v|$ all of whose prime divisors divide d. Squarefreeness gives

$$(m_3, m_4) = 1, \qquad (D, m_3m_4) = 1, \qquad d \mid D, \qquad (F_0, m_3m_4) = 1.$$

For a smooth function g supported on $[T, 2T]$, consider

$$\mathcal{T}(m_1, m_2) = \sum_n \lambda_\eta(m_1n+1)\lambda_\eta(m_2n+1)g(n).$$

Writing $k_i = m_in + 1$ transforms the relation between the two arguments into

$$m_4(k_1 - 1) = m_3(k_2 - 1), \qquad k_1 \equiv 1 \pmod d. \tag{5.7}$$

Use the circle moduli

$$q \asymp Q, \qquad F_0 \mid q, \qquad (q, m_3m_4) = 1,$$

where Q is a sufficiently large fixed power of the parameters. Their total totient weight is $Q^{2+o(1)}/F_0$, as in the circle construction of [1, Section 8.2]. In particular, both q and q/d are divisible by N.

After detecting (5.7), the two additive numerators in the Voronoi transformations are

$$a_1 = m_4a(1 + jq/d), \qquad a_2 = -m_3a, \qquad (a, q) = 1, \quad j \pmod d.$$

Both are units modulo q. Indeed, d is squarefree and $d^2 \mid q$, so every prime divisor of q also divides q/d. Hence $1 + jq/d$ is a unit modulo q. The additional factor from the two applications of (5.3) is

$$\psi(a_1)\psi(a_2) = \psi(-m_3m_4)\psi(a)^2\psi(1 + jq/d) = \psi(-m_3m_4). \tag{5.8}$$

This scalar is independent of a and j. In particular, the sign $\psi(-1) = -1$ is retained by the formula.

Write

$$S(b, c; q) = \sideset{}{^*}\sum_{a \pmod q} e((ba + c\bar{a})/q)$$

for the ordinary Kloosterman sum. Summing over a and j now gives, apart from the scalar in (5.8), precisely

$$S(m_3 - m_4, \overline{m_3m_4}(m_4k_2 - m_3k_1); q)\mathbf{1}_{m_3^2k_1 \equiv m_4^2k_2 \pmod D}. \tag{5.9}$$

The factors q^{-2}, the normalized circle weight, and the d-congruence average are unchanged. The terms with $m_4k_2 = m_3k_1$ have the Ramanujan sum $S(m_3 - m_4, 0; q)$. Since $m_3 \neq m_4$, their total is $O(Q^{-1})$ times a fixed polynomial in the other parameters, by the same divisor estimate as in [1, Section 8.2]; the choice of Q makes this negligible.

For the remaining terms put $\rho = m_4k_2 - m_3k_1$ and divide the ρ-range into dyadic intervals $|\rho| \asymp R$. The coefficient norm is (5.6). We may therefore apply [1, Theorem 2.4] to (5.9), with its parameters

$$(r, s, n, m, M, C, Z) = (m_3m_4, F_0, |m_3 - m_4|, \rho, R, Q/F_0, Z_1).$$

Here Z_1 is the smoothness parameter furnished by the Bessel transforms. The coprimality condition $(r,s)=1$ follows from the identities above. The dual-length truncations and the condition on the Bessel scale are those in [1, Section 8.2], because (5.3) has its holomorphic transform with $k=1$. The Kloosterman estimate includes the exceptional spectrum. All dependence on the original level N is absorbed into the fixed-form constant.

In particular, if $g^{(j)} \ll_j T^{-j}$, the resulting correlation bound, specialized to the shift 1, is

$$|\mathcal{T}(m_1,m_2)| \ll_{\eta,\nu,g} (MT)^{\nu}\left\{(MT+1)^{1/2}M^{1/2}\frac{D}{d^{1/2}} + (MT+1)^{3/4}\frac{D^{1/4}}{M^{1/4}}\right\}. \tag{5.10}$$

The two terms are the two contributions with nonnegative powers of Q in the calculation on the last page of [1, Section 8.2]. The arithmetic factor involving the shift is $(1, Dm_3m_4)^{1/4}=1$. Thus the character computation (5.8) and the norm estimate (5.6) supply the required changes at weight one.

5.3. **Bilinear summation.** We complete the proof of Proposition 5.1. First suppose $m \asymp M$, $n \asymp T$, $(m,N)=1$, and $MT \asymp X$. Cauchy's inequality in n reduces the square of the bilinear sum to

$$T\sum_{m_1,m_2}\alpha_{m_1}\overline{\alpha_{m_2}}\sum_{n} g(n)\lambda_\eta(m_1n+1)\lambda_\eta(m_2n+1),$$

with a smooth majorant g on a fixed enlargement of the n-interval. The diagonal contributes $\ll_\nu X^\nu TX$. To see this without losing a factor M, sum first over $k=mn+1$. Each k has at most $\tau(k-1)$ representations in the two intervals, and the bound $|\lambda_\eta(k)| \le \tau(k)$ gives the assertion.

For the off-diagonal terms, fix d, D as above. The relation

$$m_3 \equiv m_4 \pmod{D/d}, \qquad m_3 \neq m_4,$$

implies that the number of pairs is $\ll M^2/(dD)$; if D/d exceeds a fixed multiple of M/d, there are no such pairs. Substituting this count into the first term of (5.10) gives

$$\ll_\nu X^\nu TX^{1/2}M^{5/2},$$

since $\sum_{d\le 2M} d^{-3/2}$ is bounded and the number of admissible D for a fixed squarefree d is absorbed by X^ν. Explicitly, for any $v>0$, Rankin's bound gives

$$\#\{D \le 4M : \mathrm{rad}(D) \mid d\} \le (4M)^v \prod_{p\mid d}(1-p^{-v})^{-1} \ll_v M^v d^v;$$

one chooses v smaller than the prescribed ν. For the second term, the same count gives

$$\ll_\nu X^\nu TX^{3/4}M^{7/4},$$

using $D \ge d$ and the convergent sum of $d^{-7/4}$. These are the arithmetic sums in [1, Proposition 8.1]. We have therefore obtained

$$|B|^2 \ll_{\eta,\nu} X^\nu\left(TX + TX^{1/2}M^{5/2} + TX^{3/4}M^{7/4}\right). \tag{5.11}$$

When $M \le X^{1/3}$ the middle term is bounded by the last. Taking square roots and using $T \asymp X/M$ yields

$$|B| \ll_{\eta,\nu} X^\nu\left(XM^{-1/2} + X^{7/8}M^{3/8}\right).$$

For $M > X^{1/3}$ the same conclusion follows from the trivial bound $|B| \ll_\nu X^{1+\nu}$.

A Mellin inversion of $\Phi(mn/X)$ separates the two variables. On the integration line $\mathrm{Re}\, s = 0$, the resulting factors m^{-s} and n^{-s} have modulus one; the Mellin transform has rapid decay. Dividing $[M_1, M_2]$ into dyadic intervals and summing the two geometric series proves (5.1) under $(m,N)=1$.

Finally, for a squarefree m put

$$d_0 = (m, \mathrm{rad}(N)), \qquad m = d_0 m_0, \qquad n_0 = d_0 n.$$

Then $(m_0, N) = 1$ and $mn + 1 = m_0 n_0 + 1$. For each of the finitely many $d_0 \mid \mathrm{rad}(N)$ use the separate coefficients

$$\alpha'_{m_0} = \alpha_{d_0 m_0}, \qquad \beta'_{n_0} = \mathbf{1}_{d_0 \mid n_0} \beta_{n_0/d_0},$$

retaining the original interval restrictions in α'. The coprime case applies, and its factors depending on d_0 are absorbed into the constant. If a lower endpoint becomes less than one, the corresponding bounded interval is covered by the trivial bound. Summing over d_0 proves the proposition.

Remark 5.2. An additional bounded function of $m \pmod r$ and $n \pmod r$ can be inserted in (5.1) at a cost of at most r^2, by dividing both coefficient sequences into residue classes. In particular, a fixed Dirichlet character $\chi(mn + 1)$ costs only a fixed constant. A restriction on n alone is absorbed directly into β_n.

6. Sampling the Hecke coefficients in progressions

We next combine the shifted bilinear estimate with elementary lattice counting. The marking primes are smaller than every fixed positive power of x, whereas the primes in I_x are larger than $x^{1-\varepsilon}$. Consequently every marking weight H satisfies

$$H(\ell k) = H(k) \qquad (\ell \in I_x). \tag{6.1}$$

In this section H may be one array, a product of two arrays, a constant, or a fixed linear combination of these. In particular H is bounded, with a bound depending on the fixed arrays.

Proposition 6.1. *Let $c = \varepsilon/64$ and $R = x^c$. For every fixed Dirichlet character χ and every $A > 0$,*

$$\sum_{r \le R} \left| \sum_{\substack{u \ge 1 \\ r \mid u+1}} \Phi(u/x) H(u) (f_x(u) - C_x) \lambda_\eta(u+1) \chi(u+1) \right| \ll_A x L^{-A}. \tag{6.2}$$

6.1. **The contribution with a large prime factor.** Expand f_x and write $u = \ell k$. The support of Φ gives $x^{\varepsilon/2} \ll k \ll x^\varepsilon$. Divide this range into dyadic intervals $k \asymp T$, and write uniquely

$$k = d^2 a, \qquad a \text{ squarefree}.$$

Put $D = x^{\varepsilon/32}$. For $d \le D$, set $n = d^2 \ell$. By (6.1) the summand becomes

$$H(d^2 a) \mathbf{1}_{d^2 \mid n} \mathbf{1}_{n/d^2 \in I_x \text{ prime}} \Phi(an/x) \lambda_\eta(an+1) \chi(an+1), \qquad a \asymp T/d^2.$$

The congruence $r \mid an + 1$ implies $(a, r) = 1$ and is the disjoint union of the conditions

$$a \equiv b \pmod r, \qquad n \equiv -b^{-1} \pmod r, \qquad b \in (\mathbb{Z}/r\mathbb{Z})^\times.$$

There are at most r such pairs. The fixed factor $\chi(an + 1)$ is handled by partitioning a, n into residue classes modulo its fixed conductor. All restrictions now separate into a bounded coefficient in a and a bounded coefficient in n. No factorization of $\lambda_\eta(an + 1)$ is involved.

Apply Proposition 5.1 to each pair, and sum over $d \le D$ and $r \le R$. On a single T-interval this gives

$$\ll_\nu x^\nu R^2 \left(x T^{-1/2} D^2 + x^{7/8} T^{3/8} D^{1/4} \right). \tag{6.3}$$

The factors in D follow from $\sum_{d \le D} d \ll D^2$ and $\sum_{d \le D} d^{-3/4} \ll D^{1/4}$. The smallest first-variable scale is $x^{7\varepsilon/16}$ up to a constant, so this application remains in a positive-power range.

For $d > D$, an absolute bound suffices. Dropping the primality condition on ℓ, the number of pairs on one T-interval is at most

$$\frac{x}{T}\sum_{d>D}\frac{T}{d^2} \ll \frac{x}{D}.$$

For each pair, the number of $r \le R$ dividing $\ell k+1$ is at most $\tau(\ell k+1)$. Thus (4.2) and the elementary divisor bound imply

$$\sum_{r\le R} |\text{contribution with } d > D| \ll_{\nu,H} x^{1+2\nu}/D. \tag{6.4}$$

In particular this step costs a divisor factor, rather than R. The three exponents in (6.3) and (6.4), before logarithmic losses, are at most

$$1-\frac{\varepsilon}{4}+\frac{\varepsilon}{16}+\frac{\varepsilon}{32}+\nu, \quad \frac{7}{8}+\frac{3\varepsilon}{8}+\frac{\varepsilon}{128}+\frac{\varepsilon}{32}+\nu, \quad 1-\frac{\varepsilon}{32}+2\nu.$$

Choosing $\nu < \varepsilon/512$ and allowing for the $O(L)$ dyadic intervals gives a total $O(x^{1-\varepsilon/128})$.

6.2. **Cancellation in norm classes.** The term multiplied by C_x is estimated by lattice counting. The ring $\mathcal{O}_F$ has class number one and six units. There is a fixed integer M_η such that the function $\vartheta(z) = \eta((z))$, extended by zero at the conductor, is periodic modulo $M_\eta\mathcal{O}_F$. Hence

$$\lambda_\eta(n) = \frac{1}{6}\sum_{\substack{z\in\mathcal{O}_F\\ \mathrm{N}\,z=n}} \vartheta(z). \tag{6.5}$$

The Dirichlet character $\chi(\mathrm{N}\,z)$ is periodic as well.

For every modulus q and every $b \bmod q$, the complete sum of $\vartheta(z)\chi(\mathrm{N}\,z)$ subject to $\mathrm{N}\,z \equiv b \pmod q$ is zero, when taken modulo a common multiple of all the fixed moduli and q. To see this, lift a unit z_0 on which ϑ is nontrivial to the larger finite ring. Such a lift exists by surjectivity of reduction on the unit groups of these quotient rings. Then

$$v = z_0/\overline{z_0}, \qquad \mathrm{N}\,v = 1, \qquad \vartheta(v) = \vartheta(z_0)^2 \ne 1.$$

Multiplication by v preserves every norm condition and every conductor exclusion, and multiplies the sum by $\vartheta(v)$. This argument also applies when b is not a unit modulo q.

Tile the Eisenstein lattice by complete residue cells of side $O(q)$. The radial smooth function in (6.5) is supported in a disk of radius $O(\sqrt{x})$ and changes by $O(q/\sqrt{x})$ across a cell. Subtracting its value at one point of each complete cell, and bounding the boundary cells directly, gives

$$\left|\sum_{n\equiv b\,(q)} \lambda_\eta(n)\chi(n)\Phi((n-1)/x)\right| \ll_{\eta,\chi,\Phi} q\sqrt{x}+q^2. \tag{6.6}$$

6.3. **A square-mean truncation of the marking weights.** We record the truncation estimate that also enters the positive sieve.

Lemma 6.2. *Let H be as above, and let $h_0 = \lfloor L^{1/100}\rfloor$. There is a divisor polynomial*

$$H_0(u) = \sum_d c_d \mathbf{1}_{d\mid u}, \qquad \max_{c_d\ne 0} d = x^{o(1)}, \qquad \sum_d |c_d| = x^{o(1)},$$

with squarefree support, and a nonnegative function E_H such that $|H - H_0| \le E_H$ and

$$\sum_{u\asymp x} E_H(u)^2 \ll_H x h_0^{O_H(1)}\frac{C_H^{h_0}}{h_0!} + x^{o(1)}. \tag{6.7}$$

Proof. Expand each array by choosing its represented prime in each interval and then expanding the remaining damping factors in the divisibility indicators. If several arrays occur, group equal chosen primes first; the resulting monomials are indexed by the union of their prime labels. Truncate the expansion of the unrepresented factors at degree h_0. The Bonferroni inequalities bound the absolute error by a fixed power of $1+\Omega_0$, times a constant multiple of $\binom{\Omega_0}{h_0}$; here Ω_0 counts the distinct prime hits in the union of the fixed marking intervals. This is the represented-label expansion used in [7, proof of Lemma 7.2].

For completeness, its square has the required small mean. Let V_0 be the bounded sum of reciprocal primes in those intervals. In the independent divisor model, group the two h_0-element label sets by the size j of their intersection. Their total expectation is at most

$$\sum_{j=0}^{h_0} \frac{V_0^{2h_0-j}}{j!(h_0-j)!^2} \le \frac{[2\max(V_0,V_0^2)]^{h_0}}{h_0!}.$$

The fixed powers coming from represented labels introduce only $h_0^{O_H(1)}$ and a fixed exponential factor. Every union of labels in this calculation has degree at most $2h_0+O_H(1)$ and hence product $x^{o(1)}$. Counting its divisibility condition by $O(x/d)+O(1)$ proves (6.7). The total number and coefficient mass of the retained terms and of these error terms are $x^{o(1)}$, which also bounds the sum of rounding errors. □

Apply this lemma to the contribution in Proposition 6.1 without f_x. Its summed truncation error is at most a constant times

$$\sum_{u\asymp x} \tau(u+1)|\lambda_\eta(u+1)|E_H(u).$$

Cauchy's inequality, (4.2), and $\sum_{n\asymp x}\tau(n)^4 \ll xL^{15}$ show that this is $O_A(xL^{-A})$ for every A. For a retained d, the conditions $d \mid u$ and $r \mid u+1$ either are inconsistent or specify one residue class for $n = u+1$ modulo rd. Equation (6.6) and the coefficient-mass bound therefore give

$$x^{1/2+2c+o(1)} + x^{3c+o(1)}$$

after summing $r \le R$. This is a power saving. Combining it with the large-prime-factor estimate proves Proposition 6.1.

7. A divisor-weighted sieve estimate

The coefficients $\lambda_\eta(n)$ are bounded by $\tau(n)$, but need not be bounded independently of n. We therefore estimate the error of the upper sieve with the divisor weight still present. The normalization by m_W will allow us subsequently to remove the marking array.

7.1. **The sieve polynomials.** Put $z = x^\gamma$, where $\gamma > 0$ is fixed, and let h be an even positive integer. Partition the primes at most z into the nonempty blocks

$$\mathcal{B}_j = \{p : z^{2^{-j-1}} < p \le z^{2^{-j}}\}, \qquad j \ge 0, \qquad h_j = (j+1)h.$$

For a finite set A of primes, write $p_A = \prod_{p\in A} p$. Define polynomials in the divisibility indicators by

$$U_j(n) = \sum_{a=0}^{h_j}(-1)^a \sum_{\substack{A\subseteq\mathcal{B}_j\\|A|=a}} \mathbf{1}_{p_A\mid n}, \qquad E_j(n) = \sum_{\substack{A\subseteq\mathcal{B}_j\\|A|=h_j+1}} \mathbf{1}_{p_A\mid n},$$

and set

$$U_h = \prod_j U_j, \qquad E_h = \sum_j E_j \prod_{k\ne j} U_k, \qquad V_h = U_h - E_h. \tag{7.1}$$

These are the block polynomials of [8, Lemma 2.9]. Their pointwise properties follow directly from the binomial identity

$$\sum_{a=0}^{h_j}(-1)^a\binom{t}{a}=\begin{cases}1, & t=0,\\ \binom{t-1}{h_j}, & t\ge 1.\end{cases}$$

In fact, if $I_j(n)$ is the indicator that no prime of $\mathcal{B}_j$ divides n, then $U_j\ge I_j\ge 0$ and $U_j-I_j\le E_j$. Telescoping the product gives

$$0\le U_h(n)-\mathbf{1}_{P^-(n)>z}\le E_h(n),\qquad E_h(n)\ge 0. \tag{7.2}$$

Here $P^-(n)$ denotes the least prime factor of n, with $P^-(1)=\infty$.

Every polynomial in (7.1) is a sum of squarefree divisor indicators with coefficients of absolute value at most one. Indeed, the correction indexed by j has degree exactly h_j+1 in block j and degree at most h_k in every other block. Thus the correction supports are pairwise disjoint and are disjoint from the support of U_h. Since

$$\sum_{j\ge 0}h_j2^{-j}=4h,$$

all the divisors that occur are at most z^{4h+2}. In particular, writing

$$E_h(n)=\sum_{r\mid n}e_r,\qquad |e_r|\le 1,\qquad e_r=0\quad\text{unless } r \text{ is squarefree and } r\le z^{4h+2}, \tag{7.3}$$

we have $E_h(n)\le\tau(n)$.

Proposition 7.1 (Divisor-weighted upper-sieve error)**.** *Let $\Phi\ge 0$ be smooth with compact support in $(0,\infty)$, and let W be a fixed marking array with independent-model mean m_W. Fix $c<1/4$, and suppose that $\gamma(4h+2)\le c$. For all sufficiently large even h,*

$$\limsup_{x\to\infty}\frac{\log x}{xm_W}\sum_n\Phi\Big(\frac{n-1}{x}\Big)W(n-1)\tau(n)E_h(n)\ll_\Phi\frac{e^{-h}}{\gamma^2}. \tag{7.4}$$

The implied constant is independent of the number and locations of the fixed marking bands. Error terms tending to zero with x may depend on these bands, on h, and on γ.

Proof. We first bound the expectation of E_h for the local densities imposed by the divisor function. For s near 1, let

$$g_s(p)=2p^{-s}-p^{-2s},\qquad \mathcal{M}_h(s)=\sum_r e_rg_s(r),\qquad P_2(z)=\prod_{p\le z}(1-p^{-1})^2,$$

where g_s is extended multiplicatively to squarefree integers. For block j, let

$$A_j(s)=\prod_{p\in\mathcal{B}_j}(1-g_s(p)),$$

and let $u_j(s)$ and $e_j(s)$ be the elementary-symmetric expressions obtained from U_j and E_j by replacing $\mathbf{1}_{p\mid n}$ by $g_s(p)$. The exact identity (7.1) becomes

$$\mathcal{M}_h(s)=\sum_j e_j(s)\prod_{k\ne j}u_k(s). \tag{7.5}$$

Choose a sufficiently small absolute $b>0$. Uniformly on $|s-1|\le b/\log z$, we have

$$|g_s(p)|\ll p^{-1},\qquad |g_s(p)-g_1(p)|\ll\frac{b\log p}{p\log z}.$$

The reciprocal prime mass of each block is bounded by an absolute constant. Also $1-g_1(p)=(1-p^{-1})^2\ge 1/4$. Taking logarithms therefore shows that

$$\left|\frac{A_j(s)}{A_j(1)}\right|,\left|\frac{A_j(1)}{A_j(s)}\right|\le \exp(Cb2^{-j}).$$

Each $|A_j(s)|$ is bounded below by a positive absolute constant, and $\prod_j |A_j(s)|\ll P_2(z)$. On the other hand,

$$|e_j(s)|\le \frac{C^{h_j+1}}{(h_j+1)!},\qquad |u_j(s)-A_j(s)|\le \sum_{a>h_j}\frac{C^a}{a!}.$$

The factorial tails, summed over $h_j=(j+1)h$, are $O(e^{-h})$ once h exceeds an absolute constant. Substitution into (7.5), followed by Cauchy's estimate on a smaller disk, yields

$$|\mathcal{M}_h(1)|\ll e^{-h}P_2(z),\qquad |\mathcal{M}_h'(1)|\ll (\log z)e^{-h}P_2(z). \tag{7.6}$$

The same argument gives $\sup_{|s-1|\le b/\log z}|\mathcal{M}_h(s)|\ll e^{-h}P_2(z)$. It applies to complex s because it uses the polynomial identity and absolute elementary-symmetric bounds.

Next fix squarefree integers d,r with $(d,r)=1$. Orthogonality of Dirichlet characters gives, initially for $\Re s>1$,

$$\begin{aligned}&\sum_{\substack{n\ge 1\\ r\mid n\\ n\equiv 1 \pmod d}}\frac{\tau(n)}{n^s}\\ &\qquad=\frac{r^{-s}}{\varphi(d)}\sum_{\vartheta \bmod d}\vartheta(r)L(s,\vartheta)^2\prod_{p\mid r}(2-\vartheta(p)p^{-s}).\end{aligned} \tag{7.7}$$

To check the factor at $p\mid r$, use $\sum_{a\ge 0}\tau(p^{a+1})t^a=(2-t)/(1-t)^2$. If $(d,r)>1$, the original divisibility conditions are incompatible. The principal-character term of (7.7) is exactly

$$\zeta(s)^2 g_s(r)h_s(d),\qquad h_s(d)=\prod_{p\mid d}\frac{(1-p^{-s})^2}{p-1}. \tag{7.8}$$

In particular,

$$h_1(p)=\frac{1}{p}-\frac{1}{p^2}. \tag{7.9}$$

Write $\Phi_x(t)=\Phi(t-x^{-1})$, so that $\Phi_x(n/x)=\Phi((n-1)/x)$. Its smooth seminorms are bounded uniformly for large x. Put $\widehat{\Phi}_x(s)=\int_0^\infty \Phi_x(t)t^{s-1}\,dt$. Mellin inversion in (7.7), followed by a shift to $\Re s=3/4$, crosses only the double pole of the principal term at 1. The standard polynomial bounds for Dirichlet L-functions on this fixed strip and the rapid decay of $\widehat{\Phi}_x$ bound the remaining integral by

$$O_\Phi\Big(x^{3/4}d^C 3^{\omega(r)}r^{-3/4}\Big) \tag{7.10}$$

for an absolute fixed C.

Apply Lemma 6.2 to write

$$W_0(u)=\sum_d c_d\mathbf{1}_{d\mid u},\qquad |W(u)-W_0(u)|\le E_{\mathrm{arr}}(u),\qquad \max d=x^{o(1)},\quad \sum_d |c_d|=x^{o(1)}.$$

All these d are squarefree. With $h_0=\lfloor(\log x)^{0.01}\rfloor$, the second-moment bound in that lemma is

$$\sum_{u\asymp x}E_{\mathrm{arr}}(u)^2\ll x h_0^{O_W(1)}\frac{C_W^{h_0}}{h_0!}+x^{o(1)}.$$

Since $0 \le E_h(n) \le \tau(n)$, Cauchy's inequality and $\sum_{n \asymp x} \tau(n)^4 \ll x(\log x)^{15}$ show that replacing W by W_0 in the sum of the proposition costs

$$\ll_\Phi \sum_{n \asymp x} \tau(n)^2 E_{\mathrm{arr}}(n-1) \ll_{A,W} x(\log x)^{-A} \tag{7.11}$$

for every fixed $A > 0$. This estimate treats the whole polynomial E_h at once.

The contour errors (7.10), summed over $r \le x^c$ and the retained d, are $O(x^{3/4+c/4+o(1)})$. It remains to compute the sum of the pole contributions. Their holomorphic factor is

$$\mathcal{J}_h(s) = \sum_r e_r g_s(r) \sum_{\substack{d \\ (d,r)=1}} c_d h_s(d). \tag{7.12}$$

We claim that, uniformly for $|s-1| \le b/\log z$,

$$\mathcal{J}_h(s) = m_W \mathcal{M}_h(s) + O_{A,W,h,\gamma}((\log x)^{-A}) \tag{7.13}$$

for every fixed A.

Indeed, at a marking prime p, $h_s(p) = p^{-1} + O(p^{-2})$ on this disk. The polynomial expectation of the fixed array at these parameters consequently differs from its independent-model mean by $O_W(\sum_{p \text{ marking}} p^{-2})$. This follows either by changing one local factor at a time in its absolutely convergent divisor expansion, or by the corresponding finite polynomial identity for the truncated array. Excluding a marking prime that divides r changes the expectation by at most

$$O_W\left(\sum_{\substack{p \mid r \\ p \text{ marking}}} \frac{1}{p} \right) \ll_W (\log x) \exp\bigl(-(\log x)^{0.1}\bigr).$$

Both errors decrease faster than every negative power of $\log x$. The model truncation has the same factorial tail as the physical truncation. Finally,

$$\sum_r |e_r g_s(r)| \le \prod_{p \le z} (1 + |g_s(p)|) \ll (\log z)^C.$$

Multiplying the preceding errors by this bound proves (7.13). The argument is valid for complex local parameters by the same absolute polynomial estimates. Cauchy's estimate gives its differentiated version at $s = 1$, losing only a factor $\log z$.

The required residue is now that of $x^s \widehat{\Phi}_x(s) \zeta(s)^2 \mathcal{J}_h(s)$ at $s = 1$. Writing γ_E for Euler's constant, it equals

$$\begin{aligned} x m_W \{ &[(\log x)\widehat{\Phi}_x(1) + \widehat{\Phi}_x'(1) + 2\gamma_E \widehat{\Phi}_x(1)] \mathcal{M}_h(1) \\ &+ \widehat{\Phi}_x(1) \mathcal{M}_h'(1) \} + O_{A,W,h,\gamma}(x(\log x)^{-A}). \end{aligned} \tag{7.14}$$

Mertens' estimate gives $P_2(z) \ll (\log z)^{-2}$. Using (7.6), $\log z = \gamma \log x$, the contour error, and (7.11), we conclude that

$$\sum_n \Phi\left(\frac{n-1}{x}\right) W(n-1)\tau(n) E_h(n) \ll_\Phi \frac{x m_W e^{-h}}{\gamma^2 \log x} + o_{W,h,\gamma}(x/\log x).$$

Here $\gamma < 1/4$, so the derivative term, which costs $1/\gamma$ after normalization, is covered by $1/\gamma^2$. For fixed W, its mean is bounded away from zero; dividing and taking the limit proves the proposition, with the stated uniformity. □

Corollary 7.2 (The marked rough sum)**.** *Fix the giant-factor interval and ε as above, and put $c = \varepsilon/64$. For each sufficiently large even h, set $\gamma = c/(4h+3)$. For every fixed marking array W,*

$$\limsup_{x\to\infty} \frac{\log x}{x m_W} \left| \sum_{P^-(n)>x^\gamma} \Phi\Big(\frac{n-1}{x}\Big) W(n-1)(f_x(n-1) - C_x)\lambda_\eta(n)\chi(n) \right| \ll_{\Phi,\varepsilon} \frac{e^{-h}}{\gamma^2}. \tag{7.15}$$

The surviving constant is independent of the marking bands.

Proof. The upper polynomial $U_h(n)$ has divisor coefficients of absolute value at most one and level $z^{4h+2} \le x^c$. Proposition 6.1 therefore gives

$$\sum_n \Phi\Big(\frac{n-1}{x}\Big) W(n-1)(f_x(n-1) - C_x)\lambda_\eta(n)\chi(n)U_h(n) = o(x/\log x).$$

On the support of Φ, the centered statistic $f_x - C_x$ is bounded by a constant depending only on ε. The absolute error in replacing U_h by $\mathbf{1}_{P^-(n)>z}$ is bounded by that constant times the sum in Proposition 7.1, because $|\lambda_\eta(n)\chi(n)| \le \tau(n)$ and (7.2) holds. This proves (7.15). □

8. Extraction of the prime trace

We next remove composites from the rough sum. The prime coefficient has zero mean in every Dirichlet test by Lemma 4.1. Consequently the marked bilinear estimate removes the composite terms directly.

Proposition 8.1 (Prime extraction)**.** *Let $0 < \gamma < 1/2$ be fixed, and put $a(n) = \lambda_\eta(n)\chi(n)$. Let G_x be bounded uniformly on the support of $\Phi(u/x)$ and invariant under multiplication by every marking prime. For a marking array W with sufficiently many bands,*

$$\begin{aligned} &\sum_{p \text{ prime}} \Phi\Big(\frac{p-1}{x}\Big) W(p-1)G_x(p-1)a(p) \\ &\quad = \sum_{P^-(n)>x^\gamma} \Phi\Big(\frac{n-1}{x}\Big) W(n-1)G_x(n-1)a(n) + o(x/\log x). \end{aligned} \tag{8.1}$$

The required number of bands is independent of their fixed exponents. In particular this holds for $G_x = f_x - C_x$.

Proof. Write $z = x^\gamma$ and $J = \lceil 2/\gamma \rceil$. For all sufficiently large x, a z-rough integer on the support has at most J prime factors counted with multiplicity. Hence $|a(n)| \le \tau(n) \le 2^J$ there. The number of such integers divisible by the square of a prime greater than z is at most

$$Cx \sum_{q>z} q^{-2} \ll x/z.$$

The array and G_x are bounded for fixed parameters, so these integers contribute $O_{\gamma,W}(x^{1-\gamma}) = o(x/\log x)$.

A remaining composite can be written as a product of j distinct primes, $n = p_1 \cdots p_j$, with $2 \le j \le J$. Summation over ordered factorizations, with weight $1/j!$, counts it once. Coprime multiplicativity gives $a(n) = \prod_{i=1}^j a(p_i)$. Isolate $m = p_1$ and write $v = p_2 \cdots p_j$. The coefficient of v is

$$\beta_j(v) = \sum_{\substack{p_2\cdots p_j = v \\ p_i > z}} \prod_{i=2}^{j} a(p_i), \qquad |\beta_j(v)| \le 2^{j-1}(j-1)!.$$

We may temporarily allow repeated primes in this expression: their contribution is bounded by the preceding square-divisibility estimate, since both the original weights and the ordered-product

weights are bounded in terms of γ. The coefficient β_j is supported on z-rough integers and is bounded independently of x.

Decompose m and v into dyadic intervals. Both variables are at least x^γ, their product is comparable with x, and there are $O((\log x)^2)$ relevant boxes. Replacing $\Phi((mv-1)/x)$ by $\Phi(mv/x)$ costs only a fixed power of $\log x$: the pointwise change is $O_\Phi(x^{-1})$ and the relevant divisor moments have size x times a fixed logarithmic power. Mellin inversion then separates the product cutoff. Its rapidly decaying transform permits restriction to $|t| \le (\log x)^B$, with arbitrarily small logarithmic error after choosing B.

The first coefficient in a separated box is $\mathbf{1}_{m \text{ prime}} a(m) m^{it}$. Lemma 4.1 verifies all its Dirichlet tests, including the extra logarithmic frequency t. Proposition 2.1 therefore applies with second coefficient $\beta_j(v)v^{it}$ and core $G_x(mv-1)$. A bounded clipping and rescaling of G_x, if necessary, make it globally bounded without changing it on the support. This preserves its marking-prime invariance. For $G_x = f_x - C_x$, that invariance is exact because no marking prime belongs to the giant interval.

Every such box is $O_A(x(\log x)^{-A})$ for an arbitrarily prescribed fixed A, once sufficiently many bands have been chosen. Choose A to absorb the dyadic decomposition and Mellin truncation. Summing over j proves that the composite contribution is $o(x/\log x)$. All primes on the support exceed z for large x, so their contribution to the rough sum is precisely the left side of (8.1). □

Theorem 8.2 (Cubic traces and a large prime factor)**.** *Let η be a fixed nontrivial cubic Hecke character of $F = \mathbb{Q}(\zeta_3)$ satisfying $\eta^\sigma = \eta^{-1}$, and let χ be any fixed Dirichlet character. For the giant-factor statistic f_x,*

$$\sum_{p \text{ prime}} \Phi\Big(\frac{p-1}{x}\Big)\chi(p)t_\eta(p)(f_x(p-1)-C_x) = o(x/\log x). \tag{8.2}$$

Consequently,

$$\sum_{p \text{ prime}} \Phi\Big(\frac{p-1}{x}\Big)\chi(p)t_\eta(p)f_x(p-1) = o(x/\log x). \tag{8.3}$$

Proof. We prove the assertion for nonnegative Φ; decomposition into a fixed linear combination of such test functions gives the general smooth version if required. Fix a sufficiently large even h, set $c = \varepsilon/64$ and $\gamma = c/(4h+3)$, and choose a sufficient number K of bands for Proposition 8.1. Corollary 7.2 and that proposition imply, for every fixed array of this size,

$$\limsup_{x\to\infty} \frac{\log x}{x m_W}\left|\sum_p \Phi\Big(\frac{p-1}{x}\Big) W(p-1)(f_x(p-1)-C_x)a(p)\right| \ll_{\Phi,\varepsilon} \frac{e^{-h}}{\gamma^2}.$$

For an arbitrary fixed positive integer B, choose B disjoint arrays $W_1,\dots,W_B$ of size K, with means $m_1,\dots,m_B$, and write

$$A_B(u) = \frac{1}{B}\sum_{b=1}^{B}\frac{W_b(u)}{m_b}, \qquad Z_B(u) = |A_B(u)-1|^2.$$

The positive prime variance estimate (2.9), proved in [7, Section 7], gives

$$\limsup_{x\to\infty}\frac{\log x}{x}\sum_p \Phi\Big(\frac{p-1}{x}\Big) Z_B(p-1) \ll_\Phi \frac{C_K}{B}.$$

At primes $|a(p)| \le 2$ and $f_x(p-1) - C_x$ is uniformly bounded on the support. Cauchy's inequality and the usual upper bound for the number of primes thus give

$$\begin{aligned}&\left|\sum_p \Phi\Big(\frac{p-1}{x}\Big)\,(A_B(p-1)-1)(f_x(p-1)-C_x)a(p)\right| \\ &\qquad \ll_{\Phi,\varepsilon} \left(\sum_p \Phi\Big(\frac{p-1}{x}\Big)\,Z_B(p-1)\right)^{1/2}\left(\sum_p \Phi\Big(\frac{p-1}{x}\Big)\right)^{1/2}.\end{aligned}$$

Average the marked bounds over b and take $x \to \infty$ with all these choices fixed. The result is

$$\limsup_{x\to\infty} \frac{\log x}{x}\left|\sum_p \Phi\Big(\frac{p-1}{x}\Big)\,(f_x(p-1)-C_x)a(p)\right| \ll_{\Phi,\varepsilon} \frac{e^{-h}}{\gamma^2} + O_{\Phi,\varepsilon}\left(\sqrt{\frac{C_K}{B}}\right).$$

First let B become arbitrarily large with h and K fixed. Then let h tend to infinity. Since $\gamma^{-2} = (4h+3)^2/c^2$, the remaining bound tends to zero. At each stage only finitely many arrays are used before taking the limit in x. This proves (8.2), since $a(p) = \chi(p)t_\eta(p)$ away from finitely many primes.

Finally Lemma 4.1, with the fixed smooth cutoff, gives $\sum_p \Phi((p-1)/x)\chi(p)t_\eta(p) = o(x/\log x)$. As C_x is bounded, subtracting this term from (8.2) proves (8.3). □

9. Cubic Frobenius conditions

We deduce Theorem 1.2 from the arithmetic progression law and the cubic trace estimate. Let $K = F(b_1^{1/3}, \dots, b_s^{1/3})$ and $H = \mathrm{Gal}(K/F)$ as in that theorem. Kummer theory identifies H with an elementary abelian 3-group. Complex conjugation fixes the real cube roots and inverts ζ_3; therefore

$$\mathrm{Gal}(K/\mathbb{Q}) = H \rtimes \langle\sigma\rangle, \qquad \sigma h \sigma^{-1} = h^{-1}.$$

The commutators with σ generate H, since $h^{-2} = h$ in a group of exponent three. If $H \neq 1$, the maximal abelian subextension of $K/\mathbb{Q}$ is consequently F. In particular,

$$K \cap \mathbb{Q}(\zeta_M) = F \qquad (3 \mid M). \tag{9.1}$$

For $H = 1$ this is immediate as well.

Every nontrivial character $\eta \in \widehat{H}$ is, by class field theory, a cubic Hecke character of F with $\eta^\sigma = \eta^{-1}$. Let $\mathcal{R}$ contain one character from each pair $\{\eta, \eta^{-1}\}$ of nontrivial characters. Finite Fourier inversion on H gives, for an inversion-stable $\mathcal{C}$,

$$\mathbf{1}_{\mathcal{C}}(h) = \frac{|\mathcal{C}|}{|H|} + \sum_{\eta\in\mathcal{R}} c_\eta(\eta(h) + \eta(h)^{-1}), \qquad c_\eta = \frac{1}{|H|}\sum_{g\in\mathcal{C}} \overline{\eta(g)}. \tag{9.2}$$

The coefficients c_η are real because $\mathcal{C}$ is inversion-stable. At an unramified split rational prime the paired character value is exactly $t_\eta(p)$.

Expand the fixed residue-class indicator as

$$\mathbf{1}_{p \bmod M \in U} = \sum_{\chi \bmod M} b_\chi \chi(p), \qquad b_\chi = \frac{1}{\varphi(M)}\sum_{u\in U} \overline{\chi(u)}. \tag{9.3}$$

This identity retains the zero extension on nonunits. Inserting (9.2) and (9.3), Theorem 8.2 makes every nonconstant term $o(x/L)$. Proposition 3.1, the prime number theorem in fixed progressions, and (1.3) evaluate the constant term as

$$\left(\frac{|U|}{\varphi(M)}\frac{|\mathcal{C}|}{|H|}c_\varepsilon \int \Phi + o(1)\right)\frac{x}{L}.$$

This proves Theorem 1.2. Relation (9.1) also shows directly why no further compatibility factor occurs between the rational congruence and the cubic condition.

10. The finite obstructions and the final sieve

10.1. **Choosing the quadratic progression.** We give the elementary choice of progression explicitly; it is the quadratic reciprocity argument of [2, Lemma 1]. Let V be the $\mathbb{F}_2$-subspace of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by the classes of the a_i. Failure of (A) is equivalent to the existence of a linear functional $\ell : V \to \mathbb{F}_2$ such that

$$\ell([a_i]) = 1 \qquad (1 \le i \le r).$$

Indeed, the only obstruction to specifying these values is a relation among an odd number of the $[a_i]$.

Enlarge V by adjoining $[-1], [2], [3]$ and the classes of the primes dividing $a_1 \cdots a_r$, and extend ℓ to this space. If possible, choose such an extension with $\ell([-3]) = 1$. If this is impossible, $[-3]$ belongs to V and every admissible functional takes the value zero on it. Expressing $[-3]$ as a sum of classes $[a_i]$ shows that it is the product of an even number of the a_i modulo squares.

Let $\mathcal{T}$ consist of 3 and the odd prime divisors of the bases, and put

$$M_0 = 8 \prod_{q \in \mathcal{T}} q.$$

Choose a unit class modulo 8 with the prescribed Legendre values for -1 and 2. For each $q \in \mathcal{T}$, quadratic reciprocity prescribes one of the two possible Legendre values of $u \bmod q$ in order to have $(q/p) = (-1)^{\ell([q])}$. When $q > 3$, either choice has $(q-1)/2 \ge 2$ representatives, so we may also require $u \not\equiv 1$ modulo q. At $q = 3$ there is a unique choice for the prescribed sign. The Chinese remainder theorem gives $u_0 \in (\mathbb{Z}/M_0\mathbb{Z})^\times$ such that every prime $p \equiv u_0 \pmod{M_0}$ satisfies

$$\left(\frac{a_i}{p}\right) = -1 \quad (1 \le i \le r), \qquad p \not\equiv 1 \pmod q \quad (q \in \mathcal{T},\ q > 3). \tag{10.1}$$

Moreover $p \equiv 2 \pmod 3$ if $\ell([-3]) = 1$, and $p \equiv 1 \pmod 3$ otherwise, because $(-3/p)$ is the quadratic character modulo 3.

In the first case no cubic condition is needed. In the second case, failure of (B) supplies a prime $\ell_0 \equiv 1 \pmod 3$ for which none of the a_i is a cube. This prime divides none of the bases, since zero is a cube. Its Frobenius in

$$K = F(a_1^{1/3}, \dots, a_r^{1/3})$$

shows that the set

$$\mathcal{C} = \{h \in \mathrm{Gal}(K/F) : h(a_i^{1/3}) \ne a_i^{1/3} \text{ for all } i\} \tag{10.2}$$

is nonempty. It is inversion-stable. At a split unramified prime its Frobenius condition says that every a_i is a noncube. In this case put $d_{\mathcal{C}} = |\mathcal{C}|/|H| > 0$; in the case with no cubic condition put $d_{\mathcal{C}} = 1$.

10.2. **The uniform splitting estimate.** For $p \nmid a$ write

$$i_p(a) = \frac{p-1}{\mathrm{ord}_p(a)}.$$

For a prime q and $p \nmid aq$, the condition $q \mid i_p(a)$ is equivalent to complete splitting in $\mathbb{Q}(\zeta_q, a^{1/q})$. The field-degree and smooth prime-ideal estimates in [6, Lemmas 9.1–9.2], as combined before the restricted-range specialization in the proof of its Proposition 2.2, give the following form. There is

a common $\delta_0 = 10^{-6}$ such that, for every fixed $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ and every sufficiently large prime q (depending only on a),

$$\#\{x < p \le 2x : q \mid i_p(a)\} \ll_a \frac{x}{q(q-1)\log x} + \frac{x^{1-\delta_0}\log(2q)}{\log x}. \tag{10.3}$$

The implied constant is independent of q. A fixed smooth majorant for the interval gives the same upper bound for sharp endpoints.

Choose $0 < \varepsilon < \min(\delta_0/4, 1/4)$ in (1.2). Let Y exceed the fixed exceptional primes for each of the finitely many bases and every prime dividing M_0. Enlarge the progression by putting

$$M_Y = M_0 \prod_{\substack{3<q\le Y \\ q\nmid M_0}} q,$$

where here and below q in such products is prime. Let U_Y be all classes modulo M_Y that equal u_0 modulo M_0 and avoid 0 and 1 modulo every new q. Their relative density among primes is

$$d_Y = \frac{|U_Y|}{\varphi(M_Y)} = \frac{1}{\varphi(M_0)} \prod_{\substack{3<q\le Y \\ q\nmid M_0}} \frac{q-2}{q-1} \asymp_S \frac{1}{\log Y}. \tag{10.4}$$

For the last assertion use Mertens' theorem and

$$\frac{q-2}{q-1} = \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{(q-1)^2}\right).$$

The second product converges to a positive limit.

Summing (10.3) over the bases and over $Y < q \le 2x^{\varepsilon}$ yields

$$\#\{x < p \le 2x : \text{some } q \in (Y, 2x^{\varepsilon}] \text{ divides some } i_p(a_i)\} \le C_S \frac{x}{Y\log x} + O_S(x^{1-\delta_0+\varepsilon}). \tag{10.5}$$

Here C_S is independent of Y. Fix Y large enough that

$$C_S/Y < \tfrac{1}{4} d_Y d_{\mathcal{C}} c_{\varepsilon} \int \Phi.$$

Such a choice is possible by (10.4). From now on Y, M_Y, and U_Y remain fixed.

10.3. **Proof of Theorem 1.1.** Theorem 1.2, with the cubic condition (10.2) when necessary, gives

$$\left(d_Y d_{\mathcal{C}} c_{\varepsilon} \int \Phi + o(1)\right) \frac{x}{\log x} \tag{10.6}$$

as the weighted count of suitable primes with $p - 1 = kQ$, $Q \in I_x$ prime, and $k < 2x^{\varepsilon}$. Compact support inside $(1, 2)$ ensures that these primes lie in $(x, 2x]$ for all sufficiently large x. The weights are at most one.

No prime $q \le Y$ divides any $i_p(a_i)$: the prime 2 is excluded by (10.1); the prime 3 either does not divide $p - 1$ or is excluded by the noncube condition; every larger such q is excluded by $p \not\equiv 1 \pmod q$. Equation (10.5) removes all remaining index primes at most $2x^{\varepsilon}$, at a cost smaller than one quarter of the main term in (10.6), up to $o(x/\log x)$.

If an index prime remains, it must be Q, since it divides kQ and is larger than k. The condition $Q \mid i_p(a_i)$ implies $a_i^k \equiv 1 \pmod p$. Every such p is therefore a divisor of the nonzero integer

$$\mathcal{N}_x = \prod_{i=1}^{r} \prod_{1 \le j \le \lfloor 2x^{\varepsilon} \rfloor} |a_i^j - 1|.$$

Since $|a_i| \geq 2$,

$$\log \mathcal{N}_x \ll_S \sum_{j \leq 2x^{\varepsilon}} j \ll_S x^{2\varepsilon}.$$

It follows that at most $O_S(x^{2\varepsilon}/\log x) = o(x/\log x)$ primes larger than x divide $\mathcal{N}_x$. Subtracting these losses from (10.6) proves (1.1), for example with c_S equal to one quarter of its positive leading constant. Applying the dyadic bound to $(x/2, x]$ and using the prime number theorem gives the positive lower relative density.

Finally suppose (A) holds. At an odd prime where all the bases are primitive roots, all their Legendre symbols equal -1. Their product over the indicated odd subset is then -1, contradicting the square relation. If (B) holds, the even product instead forces $(-3/p) = 1$, hence $p \equiv 1 \pmod 3$. The second part of (B) makes at least one base a cube at p, so that its order divides $(p-1)/3$. The finitely many primes dividing the relations or the bases can be discarded. Thus $\mathcal{P}_S$ is finite in either case, completing the proof. □

Example 10.1. For $S = \{2, -6\}$ the relation $2(-6) = -3 \cdot 2^2$ forces the split case, but both bases are primitive roots modulo 13. The classes of 2 and -6 are independent in $F^{\times}/F^{\times 3}$: their valuations at the primes above 2 and 3 show this successively. Hence $H \simeq (\mathbb{Z}/3\mathbb{Z})^2$, and $\mathcal{C}$ has four elements. If η_1, η_2 are the two coordinate characters, then

$$\mathbf{1}_{\mathcal{C}} = \frac{4 - 2t_{\eta_1} - 2t_{\eta_2} + t_{\eta_1\eta_2} + t_{\eta_1\eta_2^{-1}}}{9}$$

at split primes. This displays explicitly the four nonconstant trace terms handled by Theorem 8.2.

References

[1] E. Assing, V. Blomer, and J. Li, *Uniform Titchmarsh divisor problems*, Adv. Math. **393** (2021), Article 108076. doi:10.1016/j.aim.2021.108076. The section and theorem numbers cited here refer to arXiv:2005.13915v1.

[2] M. Anwar and F. Pappalardi, *On simultaneous primitive roots*, Acta Arith. **180** (2017), no. 1, 35–43. doi:10.4064/aa8566-3-2017.

[3] M. Bhargava, *Every nonsquare integer not equal to -1 is a primitive root modulo a positive lower density of primes*, Hexagon preprint 2610.00228v1, 14 October 2026. Public manuscript.

[4] K. R. Matthews, *A generalisation of Artin's conjecture for primitive roots*, Acta Arith. **29** (1976), no. 2, 113–146. doi:10.4064/aa-29-2-113-146.

[5] T. Miyake, *Modular Forms*, Springer Monographs in Mathematics, Springer, Berlin, 2006. doi:10.1007/3-540-29593-3.

[6] OpenAI, *Primitive roots for every admissible integer base*, preprint, 4 October 2026. Public manuscript.

[7] OpenAI, *The Poisson–Dirichlet law for prime predecessors*, preprint, 24 September 2026. Public manuscript.

[8] OpenAI, *Weighted dilation graphs, smooth shifted primes and totient fibers*, preprint, 24 September 2026. Public manuscript.

[9] OpenAI, *The Quasi-Riemann Hypothesis: A Zero-Free Half-Plane $\Re s > 7/8$*, preprint, 30 September 2026. Public manuscript.