

Every nonsquare integer not equal to -1 is a primitive root modulo a positive lower density of primes

Manjul Bhargava

12 October 2026

Abstract

For every integer a that is neither a square nor -1 , we prove that a positive lower density of primes have a as a primitive root. More precisely, a zero-free half-plane $\Re s > 1 - 1/N$ for all Dedekind zeta functions gives a lower proportion of at least $c_a/(N \log N)$, with $c_a > 0$ independent of $N \geq 2$. The theorem of Cureton and Thorner supplies $N = 6000$, so the positive-proportion conclusion is unconditional. The proof uses the marked Type II estimates of OpenAI to count primes p such that $p - 1$ is a small cofactor times one large prime. Allowing the cofactor to vary supplies an additional factor of $\log x$ in the count. We give the counting and sieve deductions in detail and explain the dependence on the zero-free width. The argument gives a lower bound rather than the exact Artin density.

1 Introduction

The purpose of this article is to establish the following theorem:

Theorem 1. *For any nonsquare integer a not equal to -1 , the set of primes p such that a is a primitive root modulo p has positive lower density in the primes.*

For a prime $p \nmid a$, write $\text{ord}_p(a)$ for the multiplicative order of a modulo p . Thus a is a primitive root modulo p if $\text{ord}_p(a) = p - 1$. Put

$$P_a(X) = \#\{p \leq X : p \nmid a, \text{ord}_p(a) = p - 1\}, \quad N_a(x, 2x) = P_a(2x) - P_a(x).$$

Then, in fact, we prove that for some $\eta_a > 0$, we have

$$N_a(x, 2x) \geq \eta_a \frac{x}{\log x} \quad \text{for all sufficiently large } x, \quad \liminf_{X \rightarrow \infty} \frac{P_a(X)}{\pi(X)} \geq \eta_a > 0.$$

An integer a will be called *admissible* if it is neither a square nor -1 . For such an admissible a , **Artin's conjecture** predicts

$$P_a(X) \sim A(a) \text{Li}(X), \quad A(a) = \sum_{n \geq 1} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]} > 0.$$

The degrees in this formula include the familiar corrections arising from intersections of the fields. Under the generalized Riemann hypothesis, Hooley [4] proved the predicted asymptotic.

However, we show that a fixed zero-free half-plane for Dedekind zeta functions suffices for a positive-proportion result. Cureton and Thorner [1, Theorem 1.1] recently proved that, for every number field K , the Dedekind zeta function $\zeta_K(s)$ does not vanish in

$$\Re s > 1 - \frac{1}{6000}.$$

Their theorem, along with the marked Type II estimates of OpenAI, enables us to prove Theorem 1.

The infinitude of primes modulo which an admissible a is a primitive root was established in OpenAI's [2], where it was shown that the number of such primes less than x is $\gg_a \frac{x}{\log^2 x}$. The content of Theorem 1 is to show that the latter quantity can be improved to $\gg_a \frac{x}{\log x}$, thus yielding a positive lower density in the primes.

We keep the width of the zero-free half-plane as a parameter in order to make its effect on this density explicit. Write $\text{QRH}(N)$ for the assertion that every nontrivial zero of every Dedekind zeta function has real part at most $1 - 1/N$. Thus $\text{QRH}(6000)$ is the theorem of Cureton and Thorner. Throughout, $N \geq 2$ is fixed before x tends to infinity.

The main analytic tool is a *marked replacement principle*. The underlying Type II estimate originates in OpenAI's "The Poisson–Dirichlet law for prime predecessors" [3, Theorem 3.1]. The form needed here is developed in [2, Section 10, especially Lemma 10.2 and Proposition 10.3]. The "marks" are auxiliary prime divisors of the predecessor that are required to lie in prescribed intervals. In the resulting weighted bilinear sums, the estimates permit a restriction on the prime factors of one variable to be replaced by its expected density while retaining the required structure of the predecessor. Section 3 states this consequence precisely and proves the deduction from the cited estimates, including the uniformity needed for our enlarged family of cofactors. This is a separate analytic input to the construction of candidate primes; the zero-free strip is used later to remove failures of the primitive-root condition.

The quantitative form of the argument is as follows.

Theorem 2 (Dependence on the zero-free width). *Fix an admissible integer a . There exists $c_a > 0$, independent of N , with the following property. For every fixed $N \geq 2$, if $\text{QRH}(N)$ holds, then*

$$N_a(x, 2x) \geq \frac{c_a}{N \log N} \frac{x}{\log x}$$

for all sufficiently large x , with the threshold allowed to depend on a, N . After decreasing c_a if necessary, it follows that

$$\liminf_{X \rightarrow \infty} \frac{P_a(X)}{\pi(X)} \geq \frac{c_a}{N \log N}.$$

Only the zeta functions of $\mathbb{Q}(\zeta_q, a^{1/q})$, for odd primes q , are needed from $\text{QRH}(N)$.

We now describe the proof. This also indicates the purpose of each of the parameters introduced below.

1. *Reduce the problem to prime divisors of an index.* The integer

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

equals one precisely when a is a primitive root. We choose one fixed progression of primes for which a is a quadratic nonresidue. The index is then odd. For an odd prime q , the condition $q \mid i_p(a)$ is equivalent, away from ramification, to complete splitting of p in $\mathbb{Q}(\zeta_q, a^{1/q})$. These elementary reductions are explained in Section 2.

2. *Restrict the factorization of $p-1$.* The zero-free strip controls index divisors bounded by a sufficiently small power of p . We also allow one very large prime factor, for which a different argument is available. More precisely, for $x < p \leq 2x$, we seek primes of the form

$$p-1 = crQ, \quad c \in \{2, 4\}, \quad r \leq x^\epsilon, \quad Q > x^{0.9} \text{ prime},$$

where every odd prime divisor of r exceeds a fixed cutoff Y . The *cofactor* $cr = (p-1)/Q$ is simply the small remaining factor after removing Q ; once the power of two c is fixed, we also refer to its

variable part r as the cofactor. Since $r \leq x^\epsilon$, the prime Q is at least a constant multiple of $x^{1-\epsilon}$. Thus intermediate-sized prime factors are absent.

If a fails to be a primitive root at such a prime, some odd prime divisor of its index either divides r or equals Q . The first possibility involves only primes $q \leq x^\epsilon$, which the zero-free strip can handle. In the second, $\text{ord}_p(a)$ divides $cr \leq 4x^\epsilon$, so p divides one of the integers $a^j - 1$ with $j \leq 4x^\epsilon$. The product of their absolute values has too small a logarithm to have many distinct prime divisors exceeding x . This gives a negligible exceptional set without applying the zero-free estimate at Q .

3. *Let the cofactor vary.* We allow many possible values of the small remaining factor r . In the averaged sieve count, the normalization for a given r is on the scale $x/(r \log^2 x)$. Thus the relevant size of the family is its weighted reciprocal sum, rather than just its cardinality. Using only a very thin family would give too few candidate primes. We enlarge the cofactor to $r = sr_0$. The factor s is supported on the auxiliary prime intervals required by marked replacement. The factor r_0 is squarefree, has all its prime divisors between Y and $x^{\epsilon/8}$, and satisfies

$$r_0 \leq x^{\epsilon/2}, \quad \sum_{q|r_0} \frac{1}{q} \leq \tau.$$

The reciprocal sum of these cofactors is

$$\sum_{r_0} \frac{1}{r_0} \asymp \frac{\epsilon \log x}{\log Y}.$$

With the marked parameters fixed, this supplies the desired extra factor of $\log x$ in the total weighted reciprocal mass. It offsets one of the two logarithms in the prime-pair normalization and gives a count on the scale $x/\log x$, sufficient for a positive proportion of primes. The lower bound is proved for the whole family together; no prime-pair lower bound for each fixed r is required. The restriction involving τ ensures that the enlarged cofactors change the local sieve products by only a factor $1 + O(\tau)$. Sections 4 and 6 prove these assertions by Euler products and elementary inequalities.

4. *Count the candidate primes.* We first count all integers $d = crQ + 1$ with the required structure: Q is already prime, but d need not be. Bombieri–Vinogradov gives enough distribution in progressions to sieve out small prime factors of d . For a surviving composite, write $d = mn$, where n is its least prime factor. Marked replacement permits us to estimate the roughness condition on m , meaning the absence of small prime divisors, while preserving the prescribed factorization of $mn - 1$. We can then subtract according to n , with the terms governed by Buchstab’s elementary differential-delay equation. The composites still left have two prime factors near $\sqrt{x}$; a separate two-variable upper sieve bounds their contribution. It is the marked Type II input that makes this subtraction possible; distribution in progressions alone would not justify the prime-pair lower bound. Sections 5–9 yield

$$\#\mathcal{C}(x; Y) \geq A_a \frac{\epsilon}{\log Y} \frac{x}{\log x},$$

where $A_a > 0$ is independent of ϵ, Y, N .

5. *Remove the failures of the primitive-root condition.* The splitting bound proved from the smoothed explicit formula in Section 10 gives

$$\sum_{Y < q \leq x^\epsilon} \#\{x < p \leq 2x : q \mid i_p(a)\} \leq \frac{C_a}{Y \log Y} \frac{x}{\log x} + O_a\left(\frac{x^{1-1/N+\epsilon}}{\log x}\right).$$

The constant C_a is independent of N . The failures coming from $q = Q$ number $O_a(x^{2\epsilon}/\log x)$. Both error terms are negligible once $\epsilon < 1/N$ and $2\epsilon < 1$.

6. *Choose the parameters.* The sieve parameters and the number of auxiliary prime intervals can all be fixed in terms of a , before ϵ and N enter. The final lower bound is therefore

$$N_a(x, 2x) \geq \left(\frac{A_a \epsilon - C_a/Y}{\log Y} + o(1) \right) \frac{x}{\log x}.$$

Take $\epsilon = \theta_a/N$, with $\theta_a > 0$ sufficiently small, and then $Y \asymp_a N$. This proves Theorem 2, and $N = 6000$ gives Theorem 1. Section 12 explains why optimizing this final expression gives the order $1/(N \log N)$, while leaving open the best bound obtainable from a given zero-free width.

The elementary parts of the proof are given in full. We use Bombieri–Vinogradov, a standard block form of Brun’s sieve, and the smoothed Dedekind explicit formula, together with the marked replacement proposition deduced from the cited analytic estimates. In particular, the paper does not claim an elementary proof of the analytic replacement principle. The accompanying Lean development verifies the positive-proportion argument from explicit statements of these cited and classical inputs; its scope is described at the end of Section 12.

Notation. All letters described as primes range over positive rational primes. A dyadic interval is an interval of the form $[T, 2T)$. We write $L = \log x$, use natural logarithms, and put $P^-(1) = \infty$. The notation $U \ll_a V$ means $U \leq C_a V$ for a constant depending only on a ; $U \asymp_a V$ means both inequalities. Unless stated otherwise, the parameters are fixed before $x \rightarrow \infty$; constants in an $o(1)$ or in a threshold for x may depend on these fixed parameters.

2 The index and a fixed progression

We begin with the two elementary facts that explain the shape of the construction. Since $\mathbb{F}_p^\times$ is cyclic, for a prime $q \mid p-1$ one has

$$q \mid i_p(a) \iff a^{(p-1)/q} \equiv 1 \pmod{p}.$$

If $(a/p) = -1$, Euler’s criterion shows that $2 \nmid i_p(a)$. For odd q , the two conditions $p \equiv 1 \pmod{q}$ and $a^{(p-1)/q} \equiv 1 \pmod{p}$ say that $X^q - a$ has all its roots in $\mathbb{F}_p$. For $p \nmid aq$, this is equivalent to complete splitting in

$$K_q = \mathbb{Q}(\zeta_q, a^{1/q}).$$

This is the splitting criterion in [2, Lemma 2.3]. We will use it only at the final step.

We next choose a progression on which a is a quadratic nonresidue, meaning that its reduction is not a square modulo the prime. The predecessor will have a fixed power of two.

Choose M, c, u , depending only on a , such that

$$8 \mid M, \quad c \in \{2, 4\}, \quad (u, M) = 1, \quad c \mid u-1, \quad \left(\frac{u-1}{c}, \frac{M}{c} \right) = 1, \quad (1)$$

and every prime $p \equiv u \pmod{M}$ has $(a/p) = -1$. For completeness, take $M = 8 \prod_{\ell \mid a, \ell \text{ odd}} \ell$, and write $a = d_0 t^2$ with $d_0 \neq 1$ signed squarefree. Require $u \not\equiv 0, 1 \pmod{\ell}$ at odd $\ell \mid M$, and $u \bmod 8 \in \{3, 5, 7\}$. If an odd $j \geq 5$ divides d_0 , both quadratic signs occur among the nonzero residues other than 1 modulo j ; reciprocity allows that sign to be chosen last. If there is no such j , the following choices work, taking $u \equiv 2 \pmod{3}$ whenever $3 \mid M$:

d_0	-1	2	-2	3	-3	6	-6
$u \bmod 8$	3	3	7	5	5	3	7.

Use the Chinese remainder theorem, choosing the representative $0 \leq u < M$. Take $c = 2$ for $u \equiv 3, 7 \pmod{8}$, and $c = 4$ for $u \equiv 5 \pmod{8}$. This proves (1) and the required quadratic sign, as in [2, Lemma 2.4].

Throughout the argument M stays fixed. The later cutoff Y is kept separate from M , so all estimates involving this progression have a fixed modulus. Put $M_0 = M/c$, and fix $0 \leq \Psi \leq 1$, smooth and compactly supported in $(1, 2)$, with $\int \Psi > 0$.

3 The marked replacement principle

The following input is the only part of the argument specific to the marked construction. We state it in the form needed here. Its role is to let us sieve one factor of a product without losing the condition imposed on the predecessor of that product.

Set

$$L = \log x, \quad W = \exp(L^{0.24}), \quad V(y) = \prod_{\ell \leq y} (1 - 1/\ell).$$

Choose a fixed positive integer K , and fixed numbers $0.1 < a_1 < \dots < a_K < 0.2$. Let

$$\mathcal{P}_i = \{\ell \text{ prime} : e^{L^{a_i}} \leq \ell \leq e^{2L^{a_i}}\}, \quad V_i = \sum_{\ell \in \mathcal{P}_i} \frac{1}{\ell}.$$

We call these the marked prime groups. They are disjoint for large x , and $V_i = \log 2 + o(1)$. For a positive integer h , put $h_{\mathcal{P}} = \prod_{\ell \in \cup_i \mathcal{P}_i} \ell^{v_\ell(h)}$, the part of h supported on the marked primes, and define

$$\omega_i(h) = \#\{\ell \in \mathcal{P}_i : \ell \mid h\}, \quad \mathcal{W}(h) = \prod_{i=1}^K \frac{\omega_i(h) 2^{1-\omega_i(h)}}{V_i}. \quad (2)$$

The factor $\omega_i(h)$ counts the choices of a marked prime in the group, while $2^{1-\omega_i(h)}$ limits the weight of integers with many such prime divisors. A factor with $\omega_i = 0$ is zero. For large x ,

$$0 \leq \mathcal{W}(h) \leq B_K \quad (3)$$

with a constant depending only on K : for an integer $j \geq 1$, the factor $j2^{1-j}$ is at most one, and the V_i are bounded away from zero.

A positive integer is called z -rough if it has no prime factor at most z . The density of rough integers is described by Buchstab's function ω_B : $\omega_B(u) = 1/u$ for $1 \leq u \leq 2$, and $(u\omega_B(u))' = \omega_B(u-1)$ for $u > 2$. For $s > \gamma > 0$, write

$$D_\gamma(s) = \gamma^{-1} \omega_B(s/\gamma), \quad R_\gamma(m) = \mathbf{1}_{P^-(m) > x^\gamma}, \quad B_\gamma(m) = \frac{D_\gamma(\log m/L)}{LV(W)} \mathbf{1}_{P^-(m) > W}. \quad (4)$$

This is the same density as that defined by the prime-product integrals in [2, (10.11)]. Indeed, writing those terms as $D_{\gamma,j}$, one has

$$D_{\gamma,1}(s) = \frac{1}{s}, \quad D_{\gamma,j}(s) = \frac{1}{j!} \int_{\substack{t_i \geq \gamma \ (1 \leq i < j) \\ \sum_{i < j} t_i \leq s - \gamma}} \frac{1}{s - \sum_{i < j} t_i} \prod_{i < j} \frac{dt_i}{t_i} \quad (j \geq 2).$$

The sum over j is locally finite. By symmetry among the j prime factors, multiplication by s cancels one denominator and gives

$$sD_{\gamma,j}(s) = \frac{1}{(j-1)!} \int_{\substack{t_i \geq \gamma \ (1 \leq i < j) \\ \sum_{i < j} t_i \leq s - \gamma}} \prod_{i < j} \frac{dt_i}{t_i}.$$

Differentiating and summing gives $(sD_\gamma(s))' = D_\gamma(s - \gamma)$ for $s > 2\gamma$, with $sD_\gamma(s) = 1$ for $\gamma < s \leq 2\gamma$. Rescaling Buchstab's defining equation therefore identifies the two densities, interval by interval. This also gives their joint continuity on compact subsets of $s > \gamma > 0$.

Proposition 3 (Uniform marked replacement, MR). *Fix a modulus M , a reduced residue u , a smooth function Ψ compactly supported in $(1, 2)$, and fixed numbers*

$$\beta > 0, \quad 0 < \gamma < s_- < s_+ < 1.$$

For K sufficiently large in terms of these data and the comparison constants below, the following holds. If $H_m, H_n \geq x^\beta$, $H_m H_n \asymp x$ with fixed comparison constants, and the full m -dyad has logarithmic exponents in $[s_-, s_+]$, then

$$\sum_{\substack{m \in I \\ H_n \leq n < 2H_n}} (R_\gamma(m) - B_\gamma(m)) b_n \mathbf{1}_{mn \equiv u \pmod{M}} \Psi(mn/x) F_x(mn-1) \mathcal{W}(mn-1) \ll x L^{-6}. \quad (5)$$

Here $I \subseteq [H_m, 2H_m)$ is any interval, $|b_n| \leq 1$ is supported on W -rough integers, and

$$|F_x(h)| \leq 1, \quad F_x(\ell h) = F_x(h) \quad (h \geq 1, \ell \in \bigcup_i \mathcal{P}_i). \quad (6)$$

The estimate has one implied constant and one threshold for x , simultaneously for all permitted dyads, functions F_x , intervals, and coefficients in the fixed exponent window. Thus it also applies to a family of dyads growing with x . The required lower bound on K is independent of F_x and of the particular a_i . Constants and thresholds may depend on the fixed band exponents.

Deduction from the cited estimates. We use [2, Lemma 10.2 and Proposition 10.3], with damping parameter $1/2$. These results allow every bounded invariant selector F_x , uniformly over its choice. Proposition 10.3 supplies the rough-factor discrepancy $R_\gamma - B_\gamma$, including real power twists m^{iv} . We explain how to add the progression and the smooth weight, following the proof of [2, Lemma 12.1].

Since $(u, M) = 1$, character orthogonality gives

$$\mathbf{1}_{mn \equiv u \pmod{M}} = \frac{1}{\varphi(M)} \sum_{\lambda \bmod M} \overline{\lambda(u)} \lambda(m) \lambda(n).$$

Here a Dirichlet character is extended by zero on integers not coprime to its modulus. To separate the smooth weight, put

$$\widehat{\psi}(v) = \frac{1}{2\pi} \int_{\mathbb{R}} \Psi(e^t) e^{-ivt} dt.$$

Fourier inversion yields

$$\Psi(mn/x) = \int_{\mathbb{R}} \widehat{\psi}(v) x^{-iv} m^{iv} n^{iv} dv.$$

The function $\widehat{\psi}$ decreases faster than every negative power of $1 + |v|$.

For each character λ and $|v| \leq L$, apply the coefficient criterion of [2, Lemma 10.2], with $C = 2$ and $D_* = 6$, to

$$\alpha_m = \mathbf{1}_I(m) m^{iv} \lambda(m) (R_\gamma(m) - B_\gamma(m)), \quad \beta_n = b_n n^{iv} \lambda(n).$$

Both sequences are supported on W -rough integers and have absolute value at most L^2 for large x . The character-transform estimates required by that criterion are verified in the proof of [2, Proposition 10.3], for every fixed logarithmic modulus range, frequency range, and desired saving. Multiplication by the fixed character λ preserves them: a character χ of modulus $k \leq L^A$ becomes $\lambda\chi$, of

modulus $\text{lcm}(M, k) \leq L^{A+1}$ for large x . The factor m^{iv} , with $|v| \leq L$, shifts a tested frequency by at most L ; increasing its fixed logarithmic range by one absorbs this shift. The criterion therefore bounds the inner marked sum by $O(xL^{-6})$, uniformly in λ, v and F_x .

Integrating over $|v| \leq L$ preserves this bound because $\int |\hat{\psi}(v)| dv$ is finite. On the remaining tail the coefficient bounds and (3) give the sufficient crude bound $O_K(xL^2)$; rapid decay makes its integral $O_{K,\Psi,A}(xL^{-A})$ for every fixed A . Summing over the finitely many characters proves (5).

Finally, the source estimate is uniform over all permitted F_x . In the proof of its Lemma 10.2, invariance removes the selected marked primes from the argument of F_x , and Cauchy–Schwarz then removes the remaining bounded factor containing F_x . Thus the number of groups and the analytic constants do not depend on the particular selector. Independence of the required K from the band exponents is also part of the cited estimate.

The same uniformity holds over the dyads in the fixed exponent window. Proposition 10.3 supplies one character-transform constant and one threshold throughout this window, for each fixed range and saving. In the proof of Lemma 10.2, the auxiliary accuracies and then K are chosen before these transform bounds are invoked. The resulting error constant and threshold therefore apply simultaneously to every active dyad. This common threshold is essential when the number of dyads grows with x . $\square$

The selector in Section 5 satisfies (6), including when $\ell \mid h$. The uniformity just proved therefore applies to our enlarged cofactor family and allows the same K to work for every fixed N .

For intuition, R_γ is an exact roughness condition. The weight B_γ imposes only the much weaker condition of being W -rough, and multiplies it by the ratio of the two expected densities. Proposition 3 says that this replacement is valid inside the displayed marked sum. Its proof uses the cited marked Type II estimates and does not use QRH(N).

4 A cofactor with a large reciprocal sum

The sieve normalization for a cofactor r is on the scale $x/(rL^2)$. We therefore seek a family for which $\sum 1/r$ has size L ; the prime-pair lower bound will be proved only after summing over this family. The next lemma constructs such a family while keeping its sieve factors close to those of a fixed cofactor.

The constants $\epsilon, \tau > 0$ will be small, with $\epsilon < 0.01$; $Y \geq 3$ will be large. All are fixed before x tends to infinity. Put

$$R = x^{\epsilon/2}, \quad Z = x^{\epsilon/8} = R^{1/4}.$$

Let $\mathcal{R}_x$ consist of squarefree positive integers r_0 with

$$r_0 \leq R, \quad q \mid r_0 \implies Y < q \leq Z, \quad q \notin \bigcup_i \mathcal{P}_i, \quad \sum_{q \mid r_0} \frac{1}{q} \leq \tau. \quad (7)$$

The integer 1 is permitted. Define

$$H_0 = \sum_{r_0 \in \mathcal{R}_x} \frac{1}{r_0}.$$

Lemma 4. *For Y sufficiently large in terms of τ , and then x sufficiently large,*

$$H_0 \asymp_K \frac{\epsilon L}{\log Y}. \quad (8)$$

The comparison constants can be chosen independently of Y, ϵ, τ , within the stated restrictions; the threshold for x can depend on all of them. If s ranges over integers supported on the marked prime groups, then

$$J_{\mathcal{P}} := \sum_s \frac{\mathcal{W}(s)}{s} \asymp_K 1, \quad J_{\mathcal{P}} \geq 1, \quad \sum_{s > x^t} \frac{\mathcal{W}(s)}{s} \ll_K e^{-tL^{1-a_K}} \quad (t > 0 \text{ fixed}). \quad (9)$$

In particular, for the unique decomposition $r = sr_0$ with these disjoint prime supports,

$$J := \sum_{\substack{s \text{ supported on the groups} \\ r_0 \in \mathcal{R}_x}} \frac{\mathcal{W}(s)}{sr_0} = J_{\mathcal{P}} H_0 \gg_K \frac{\epsilon L}{\log Y}, \quad (10)$$

and

$$\sum_{sr_0 > x^\epsilon} \frac{\mathcal{W}(s)}{sr_0} \ll_K H_0 e^{-(\epsilon/2)L^{1-a_K}}. \quad (11)$$

Proof. First omit the bounds on the size of r_0 and on the sum of reciprocals of its prime divisors. The harmonic mass is

$$H = \prod_{\substack{Y < q \leq Z \\ q \notin \cup_i \mathcal{P}_i}} (1 + 1/q) \asymp_K \frac{\log Z}{\log Y}.$$

Mertens' product estimate gives constants independent of $Y \geq 3$; deleting the K groups costs only a factor depending on K . Under the probability measure assigning a squarefree product mass $1/(Hr_0)$, the events $q \mid r_0$ are independent, with probabilities $1/(q+1)$. Therefore

$$\mathbb{E} \log r_0 \leq (1 + o(1)) \log Z, \quad \mathbb{E} \sum_{q \mid r_0} \frac{1}{q} \leq \sum_{n > Y} \frac{1}{n(n+1)} \leq \frac{1}{[Y]}.$$

Markov's inequality removes at most $1/4 + o(1)$ for $r_0 > R$, and at most $1/(\tau \lfloor Y \rfloor)$ for the other restriction. With $Y > 10/\tau$, a fixed positive fraction of H remains. This proves (8).

For the marked mass, define $E_i(t) = \prod_{\ell \in \mathcal{P}_i} (1 + t/(\ell - 1))$. Summing over all positive exponents of each prime gives

$$J_{\mathcal{P}} = \prod_{i=1}^K \frac{E'_i(1/2)}{V_i}.$$

Products consisting of exactly one prime to exponent one from each group contribute 1. The upper bound follows from this Euler product. For the tail, put $v = L^{-a_K}$. Since $\ell^v \leq e^2$ at each group prime, $\sum_s \mathcal{W}(s)/s^{1-v} \ll_K 1$, using (3) and the geometric series at each prime. Rankin's inequality proves (9). Finally $r_0 \leq x^{\epsilon/2}$, so $sr_0 > x^\epsilon$ implies $s > x^{\epsilon/2}$. This proves (10)–(11). $\square$

5 Counting the integers before sieving

We now encode the desired predecessor factorization in a weight on integers d . At this stage d need not be prime. It is the large factor Q of $d - 1$ that is prime, so distribution in progressions follows from the usual theorems about rational primes.

A selector is simply a function taking the values zero and one. Define, for every $h \geq 1$,

$$F_x(h) = \mathbf{1}_{\{h/h_{\mathcal{P}} = cr_0 Q \text{ for some } r_0 \in \mathcal{R}_x, Q > x^{0.9} \text{ prime}\}}, \quad (12)$$

and

$$w(d) = \mathbf{1}_{d \equiv u \pmod{M}} \Psi(d/x) F_x(d-1) \mathcal{W}(d-1), \quad X_0 = \sum_{d \geq 2} w(d). \quad (13)$$

For every group prime ℓ , $(\ell h)_{\mathcal{P}} = \ell h_{\mathcal{P}}$, even if $\ell \mid h$. Hence $F_x(\ell h) = F_x(h)$, exactly as MR requires.

On the support of w , write $d = csr_0 Q + 1 = crQ + 1$. The representation is unique: $s = (d-1)_{\mathcal{P}}$; a prime $Q > x^{0.9}$ cannot divide r_0 , and two such primes cannot divide $(d-1)/c < 2x$. All prime divisors of r_0 are at most $Z < x^{0.9}$. Thus

$$r \leq x^{0.11}, \quad \mathcal{W}(d-1) = \mathcal{W}(s), \quad 0 \leq w(d) \leq B_K \quad (14)$$

for large x . We always take Y larger than the prime divisors of M , so $(r, M) = 1$.

Let $t_r = \mathcal{W}(s)$ when $r = sr_0$ is permitted, and zero otherwise. Define

$$A_r = \sum_{\substack{Q > x^{0.9} \text{ prime} \\ crQ+1 \equiv u \pmod{M}}} \Psi((crQ+1)/x).$$

Then $X_0 = \sum_r t_r A_r$ and $\sum_r t_r/r = J$. The contribution from $r > x^\epsilon$ is, by $A_r \ll x/r$,

$$O_K \left(x H_0 e^{-(\epsilon/2)L^{1-a_K}} \right). \quad (15)$$

It is negligible relative to xJL^{-A} , for every fixed A .

We shall also need a lower bound relative to the *full* harmonic mass J . Since $J = J_{\mathcal{P}} H_0 \geq H_0$, (11) implies

$$J_{\leq x^\epsilon} := \sum_{r \leq x^\epsilon} \frac{t_r}{r} = J - O_K \left(H_0 e^{-(\epsilon/2)L^{1-a_K}} \right) \geq \frac{J}{2} \quad (16)$$

for all sufficiently large x . The factor $1/2$ is independent of K , although the threshold may depend on it. The restriction $r \leq x^\epsilon$ is imposed only when estimating this tail; it is not inserted into F_x , since doing so would destroy marked-prime invariance.

Lemma 5. *Suppose $0 < \epsilon < \kappa < 0.01$, and put $D = x^{1/2-\kappa/2}$. For an odd squarefree ℓ , let $A_r(\ell)$ include the additional condition $\ell \mid crQ + 1$, and put*

$$g_r(\ell) = \frac{\mathbf{1}_{(\ell, Mr)=1}}{\varphi(\ell)}, \quad E_r(\ell) = A_r(\ell) - g_r(\ell) A_r.$$

For every fixed $A > 0$,

$$\sum_{r \leq x^\epsilon} t_r \sum_{\substack{\ell \leq D \\ \ell \text{ odd, squarefree}}} |E_r(\ell)| \ll_{A, M, \Psi, \epsilon, \kappa} xJL^{-A}. \quad (17)$$

Moreover

$$X_0 \asymp_{M, \Psi} \frac{xJ}{L}, \quad (18)$$

with comparison constants independent of $K, Y, \tau, \epsilon, \kappa$.

Proof. For $r \leq x^\epsilon$ the lower cutoff on Q is automatic. The progression is the reduced class

$$Q \equiv ((u-1)/c) r^{-1} \pmod{M_0}.$$

If $(\ell, Mr) > 1$, both $A_r(\ell)$ and $g_r(\ell)$ vanish. Otherwise the condition on ℓ combines with it into a reduced class modulo $M_0\ell$. The prime variable has scale $T \asymp x/(cr)$. Take $\eta = (\kappa - \epsilon)/4$. Then

$$(1 - \epsilon)(1/2 - \eta) - (1/2 - \kappa/2) = (\kappa - \epsilon)(1 + \epsilon)/4 > 0.$$

Consequently $M_0\ell \leq T^{1/2-\eta}$ throughout the required range, for large x . The Bombieri–Vinogradov theorem, with its maximum over reduced residue classes, and partial summation give

$$\sum_{\ell \leq D} \left| A_r(\ell) - \frac{g_r(\ell)}{\varphi(M_0)} I_r \right| \ll (x/r) L^{-A'}, \quad I_r = \frac{x}{cr} \int_1^2 \frac{\Psi(y)}{\log((xy-1)/(cr))} dy.$$

The smoothing has bounded total variation independently of r . The term $\ell = 1$ evaluates A_r ; replacing $I_r/\varphi(M_0)$ by A_r in the other terms costs at most a factor $O(L)$, since $\sum_{\ell \leq D} 1/\varphi(\ell) \ll L$. Increase A' , multiply by t_r , and sum to obtain (17). Finally $I_r \asymp_{\Psi} x/(rL)$, uniformly for $\epsilon < 0.01$. The fixed-modulus prime number theorem, with partial summation, gives

$$A_r = \frac{I_r}{\varphi(M_0)} + o_{M,\Psi} \left(\frac{x}{rL} \right) \asymp_{M,\Psi} \frac{x}{rL} \quad (r \leq x^\epsilon),$$

simultaneously throughout this range. Indeed the prime scale is at least $x^{0.99}/c$, which tends to infinity uniformly in r , and the finitely many reduced classes modulo M_0 have a common error bound. Multiplying by t_r , summing, and using (16) gives comparison with xJ/L , with constants independent of $K, Y, \tau, \epsilon, \kappa$. The tail (15) is $o(xJ/L)$, proving (18). $\square$

Only the two-sided comparison (18) is needed. Since r can be a fixed power of x , we retain $\log(x/r)$ in the integral I_r ; it is comparable to L , but its ratio to L need not tend to one.

6 The effect of the cofactor on the sieve

For a fixed r , sieving $crQ + 1$ by an odd prime $\ell \nmid Mr$ removes a proportion $1/(\ell - 1)$ of the reduced residue classes of Q . If $\ell \mid r$, it removes nothing. Thus enlarging r increases the surviving local product. The reciprocal-sum restriction makes this increase uniformly small.

Write

$$V_M(y) = \prod_{\substack{2 < \ell \leq y \\ \ell \nmid M}} \left(1 - \frac{1}{\ell - 1} \right), \quad S_M = \lim_{y \rightarrow \infty} \frac{V_M(y)}{V(y)} > 0. \quad (19)$$

For $s \leq x^{0.11}$ supported on the marked primes,

$$\sum_{\ell \mid s} \frac{1}{\ell} \leq 0.11 L^{0.9} e^{-L^{0.1}} = o(1).$$

Together with (7), this gives $\sum_{\ell \mid r} 1/\ell \leq \tau + o(1) \leq 2\tau$ for every fixed $\tau > 0$ and all sufficiently large x . Hence, uniformly for contributing $r \leq x^{0.11}$ and all y ,

$$V_M(y) \leq \prod_{2 < \ell \leq y} (1 - g_r(\ell)) \leq e^{20\tau} V_M(y). \quad (20)$$

Indeed deleting the factor at a prime dividing r multiplies the product by $(1 - 1/(\ell - 1))^{-1}$, whose logarithm is at most $10/\ell$ for odd ℓ . Set $E_\tau = e^{20\tau}$. This slightly looser fixed factor absorbs the marked-prime contribution and is the bound used in the formalization. We retain it in the upper bounds and choose τ small enough at the end of the sieve subtraction.

7 Subtracting according to the least prime factor

The argument in this section is an inclusion-exclusion calculation in two stages. We first count integers having no small prime factor. We then subtract those whose least prime factor lies below $x^{1/2-\kappa}$. Marked replacement makes the second count accessible.

The elementary sieve input. We use the classical block form of Brun's sieve. If the intersections of bad conditions at squarefree ℓ have mass $X'g(\ell) + E(\ell)$, with g multiplicative, $0 \leq g(p) \leq 1 - \eta_0$, and $\sum_{v < p \leq v^2} g(p) \leq C_0$, then an even depth H , sufficiently large in terms of η_0, C_0 , gives

$$S = X' \prod_{p \leq z} (1 - g(p))(1 + O(e^{-H})) + O\left(\sum_{\ell \leq z^{4H+2}} |E(\ell)|\right). \quad (21)$$

Only products of sieving primes occur in the remainder. For $H = 2$, the corresponding upper bound has an implied constant depending only on η_0, C_0 and remainder range $\ell \leq z^{10}$. These two parameters can be fixed absolutely in our applications. We use the bounded-coefficient form recorded in [2, Lemma 11.1]. Its constants are uniform when H grows. Standard Mertens and Buchstab estimates also give

$$\int_b^{1/2} D_t(1-t) \frac{dt}{t} = D_b(1) - 1, \quad D_b(1) \leq \frac{e^{-\gamma_E}}{b} (1 + C_d e^{-c_d/b}) \quad (22)$$

for sufficiently small fixed $b > 0$. The identity has a direct proof. Substitute $u = 1/t$ on its left. The result is

$$\int_2^{1/b} \omega_B(u-1) du = [u\omega_B(u)]_2^{1/b} = D_b(1) - 1,$$

by the defining differential equation and $2\omega_B(2) = 1$. The inequality is the standard rapid convergence of Buchstab's function to $e^{-\gamma_E}$. Thus the large rough-number terms cancel, leaving the one-prime contribution 1.

The initial lower sieve. Assume henceforth $\epsilon < b < 0.01$. Apply (21) at each $r \leq x^\epsilon$, with $z = x^b$, $g = g_r$, and $H = 2\lfloor 1/(40b) \rfloor$. For small b , $z^{4H+2} \leq x^{0.2+2b} < D$, so (17) controls all errors. Use the lower inequality in (20), and absorb (15). There are absolute $C_s, c_s > 0$ such that

$$S_b := \sum_{P^-(d) > x^b} w(d) \geq \frac{S_M X_0}{L} \left\{ \frac{e^{-\gamma_E}}{b} (1 - C_s e^{-c_s/b}) + o(1) \right\}. \quad (23)$$

After enlarging C_s , one may take $c_s = 1/20$, since $H \geq 1/(20b) - 2$. The constant C_s and an upper bound $b_0 > 0$ on the permitted values of b are fixed before ϵ, Y, τ and the marked groups. The vanishing error and the threshold for x may depend on these later choices. This allows us to choose b before the zero-free width enters the argument.

A prime divisor in a prescribed interval. Next fix $b \leq \gamma < \gamma' \leq 1/2 - \kappa$. At $r \leq x^\epsilon$, any prime $x^\gamma < n \leq x^{\gamma'}$ is coprime to Mr . Conditioning on $n \mid d$, the local main mass is $A_r/(n-1)$. Sieve the remaining prime factors of d up to W , with $H = 2\lceil (\log L)^2 \rceil$. The remainder moduli are

$$n\ell \leq x^{1/2-\kappa} W^{4H+2} = x^{1/2-\kappa+o(1)} < D.$$

The map $(n, \ell) \mapsto n\ell$ is injective, since n is its only prime divisor exceeding W . Thus the summed error uses (17) once, without multiplicity weights. From (20) and Mertens' theorem,

$$\sum_{\substack{x^\gamma < n \leq x^{\gamma'} \\ n \text{ prime}}} \sum_{\substack{n|d \\ P^-(d) > W}} w(d) \leq E_\tau S_M X_0 V(W) \{\log(\gamma'/\gamma) + o(1)\}. \quad (24)$$

The tail $r > x^\epsilon$ remains negligible: for $x \geq 2$, each $d < 2x$ has at most $2/b$ distinct prime divisors greater than x^b . Its contribution is therefore at most $2/b$ times (15), which is $o(X_0 V(W))$. Thus the number of conditioning primes introduces no growing multiplicity into the tail estimate.

The subtraction. Put $U_\kappa = \sum_{P^-(d) > x^{1/2-\kappa}} w(d)$. For a fixed bin $(\gamma, \gamma'] \subseteq (b, 1/2 - \kappa]$, any d whose least prime factor lies in that bin is counted by

$$T_{\gamma, \gamma'} = \sum_{\substack{x^\gamma < n \leq x^{\gamma'} \\ n \text{ prime}}} \sum_{P^-(m) > x^\gamma} w(mn).$$

Use the half-open dyadic partition, so that each pair (m, n) belongs to exactly one box. There are $O(L)$ relevant boxes; both factors have scale at least $x^{b/2}$, and the full m -dyads have exponents in $[1/2 + \kappa/2, 1 - b/2]$. Proposition 3, with $\beta = b/2$, replaces $R_\gamma(m)$ by $B_\gamma(m)$, at total cost $O(xL^{-5}) = o(X_0/L)$. The disjoint boxes let us combine the replaced main terms before applying (24); the factor $O(L)$ is paid only in the replacement errors. On the product support, $\log m/L = 1 - \log n/L + O(1/L)$. By continuity of D , and then (24),

$$T_{\gamma, \gamma'} \leq \frac{E_\tau S_M X_0}{L} \left\{ \sup_{\gamma \leq t \leq \gamma'} D_\gamma(1-t) \log(\gamma'/\gamma) + o(1) \right\}. \quad (25)$$

Choose a sufficiently fine fixed partition of $[b, 1/2 - \kappa]$. The sum of the expressions in braces, without $o(1)$, is at most $D_b(1) - 1 + 1/20$, by (22) and uniform continuity. Subtraction gives

$$\frac{LU_\kappa}{S_M X_0} \geq \frac{e^{-\gamma_E}}{b} (1 - C_s e^{-c_s/b}) - E_\tau (D_b(1) - 1 + 1/20) + o(1). \quad (26)$$

Choose b so small that

$$\frac{e^{-\gamma_E}}{b} (C_s e^{-c_s/b} + C_d e^{-c_d/b}) < 1/10, \quad (27)$$

and then $\tau \leq 0.01$ so small that

$$(E_\tau - 1)(D_b(1) + 1) < 1/10. \quad (28)$$

It follows that

$$U_\kappa \geq (3/4 + o(1)) S_M X_0 / L. \quad (29)$$

The choices of b and τ involve no zero-free width. The loss from the enlarged cofactor is $O(\tau/b)$, which is made small by choosing τ after b .

8 Removing the remaining semiprimes

After the preceding subtraction, every surviving composite has its prime factors near the square root of x . We show that their total contribution tends to zero with κ . The constant in this estimate

must be independent of the number K of marks; this permits κ to be chosen before K . A composite contributing to U_κ , for $\kappa < 0.01$, has exactly two prime factors counted with multiplicity. Each lies between $x^{1/2-\kappa}$ and $2x^{1/2+\kappa}$. Their ordered pairs are covered by at most $C_{\text{dyad}}(\kappa L + 1)$ dyadic boxes $\mathcal{B} = [M_1, 2M_1) \times [M_2, 2M_2)$, with

$$x/4 \leq M_1 M_2 \leq 2x, \quad [M_i, 2M_i) \subseteq [x^{0.46}, x^{0.54}] \quad (30)$$

for large x .

Lemma 6. *For any such box,*

$$\sum_{\substack{(m,n) \in \mathcal{B} \\ P^-(m) > W, P^-(n) > W}} w(mn) \leq C_1 X_0 V(W)^2, \quad (31)$$

where C_1 depends at most on M, Ψ , uniformly for $\tau \leq 0.01$, and is independent of $K, Y, \epsilon, b, \kappa$.

Proof. Fix $r \leq x^{0.11}$, and write $k = cr$. A contributing pair satisfies $mn \equiv 1 \pmod{k}$, and $(mn - 1)/k = Q > x^{0.9}$ is prime. At each odd prime $j \leq z' = x^{0.002}$, $j \nmid cr$, forbid $mn \equiv 1 \pmod{j}$; if $j \leq W$, also forbid $mn \equiv 0 \pmod{j}$. There are respectively $j - 1$ and $2j - 1$ such pairs modulo j , and the conditions are disjoint. For a squarefree product ℓ of these primes, put

$$\rho(\ell) = \prod_{j|\ell} (j - 1 + (2j - 1)\mathbf{1}_{j \leq W}), \quad g(\ell) = \rho(\ell)/\ell^2.$$

Since the sieving primes are coprime to $k = cr$, the Chinese remainder theorem applies. There are $\varphi(k)$ pairs of residues modulo k satisfying $mn \equiv 1 \pmod{k}$. Counting the pairs in each residue class of the box gives main mass $X'g(\ell)$, where $X' = M_1 M_2 \varphi(k)/k^2$, and error

$$|E(\ell)| \ll \varphi(k)\rho(\ell) \left(\frac{M_1 + M_2}{k\ell} + 1 \right) \ll d(\ell)^2 (M_1 + M_2 + r\ell).$$

Here $d(\ell)$ is the divisor function. Since $\sum_{\ell \leq T} d(\ell)^2 \ll T \log^3(2T)$, summing to $(z')^{10} = x^{0.02}$ gives

$$\sum_{\ell \leq x^{0.02}} |E(\ell)| \ll (x^{0.56} + rx^{0.04})L^3 = o((x/r)L^{-10})$$

uniformly for $r \leq x^{0.11}$. The local densities satisfy $g(j) \leq 7/9$, $g(j) \leq 3/j$. For $j \leq W$ the remaining factor is

$$1 - (3j - 2)/j^2 = (1 - 1/j)^3 (1 - 1/(j - 1)^2);$$

for $W < j \leq z'$ it is

$$1 - (j - 1)/j^2 = (1 - 1/j)(1 + 1/(j(j - 1))).$$

The correction products are bounded. Omitting primes dividing r costs at most $\exp(C\tau + o(1))$, by the same reciprocal-sum bound as in (20). The $H = 2$ upper sieve therefore bounds the pairs at this r by

$$O((x/r)V(W)^2V(z')).$$

We may discard the progression and bound Ψ by 1 for this upper bound. Multiply by t_r , sum, and use $V(z') \asymp L^{-1}$ and (18). This gives (31), without introducing the pointwise bound B_K . $\square$

In the range (30), $R_{0.4}(m)$ is exactly the prime indicator and $D_{0.4}(s) = 1/s$. Use marked replacement first in the m -variable and then in the n -variable, with $\beta = b/2$, $s_- = 0.46$, $s_+ = 0.54$, interchanging m, n for the second application, to replace both prime indicators by $\mathbf{1}_{P^-(m) > W}/(V(W) \log m)$ and its n -analogue. The companion coefficients are bounded by 1 for large x , and are W -rough. By (31), the resulting mass in one box is at most $(0.46)^{-2} C_1 X_0/L^2$. Thus for a constant C_2 depending only on M, Ψ ,

$$\sum_{\substack{d \text{ composite} \\ P^-(d) > x^{1/2-\kappa}}} w(d) \leq C_2(\kappa + L^{-1}) X_0/L + o(X_0/L). \quad (32)$$

All replacements together cost $O(xL^{-5})$. Prime squares are included; counting other semiprimes twice is harmless.

9 Fixing the sieve parameters and counting candidates

The order of choices is important both for the proof and for its dependence on N . We first make all choices that can be made using a alone.

1. Fix M, c, u, Ψ , hence S_M , and take the constant C_2 in (32) uniformly for $0 < \tau \leq 0.01$.
2. Choose $0 < \kappa < 0.01$ so that $C_2 \kappa < S_M/8$.
3. Choose $0 < b < \min(b_0, 0.01)$ small enough for (27), using the constants fixed before ϵ . Then choose $0 < \tau \leq 0.01$ satisfying (28), and fix the finite partition used in (26).
4. Choose K large enough for the finitely many applications of marked replacement, and fix the band exponents, for example $a_i = 0.1 + 0.1i/(K+1)$.

These choices are independent of ϵ, Y, N . Indeed, the first set of replacement parameters consists of

$$\beta = b/2, \quad \gamma \in [b, 1/2 - \kappa], \quad [s_-, s_+] = [1/2 + \kappa/2, 1 - b/2],$$

with only the finitely many selected values of γ . The second set has $\gamma = 0.4$, $[s_-, s_+] = [0.46, 0.54]$, and the same β . Neither set involves ϵ . The selector does involve ϵ, Y , but Proposition 3 is uniform over that selector.

Put $\epsilon_a = \min(\kappa, b)/10$, and now allow any fixed $0 < \epsilon < \epsilon_a$. Choose $Y \geq Y_a$, where the fixed constant Y_a exceeds $10/\tau$, the prime divisors of M , and the Kummer cutoff $Q_0(a)$ and exceptional primes identified in the next section. Equations (29) and (32) give

$$\sum_{d \text{ prime}} w(d) \geq \frac{1}{2} S_M X_0/L$$

for all sufficiently large x . Remove the negligible contribution with $r > x^\epsilon$, and use $w(d) \leq B_K$. Equations (10) and (18) now show that

$$\#\mathcal{C}(x; Y) \geq A_a \frac{\epsilon}{\log Y} \frac{x}{L}, \quad (33)$$

where $A_a > 0$ is independent of ϵ, Y, N . The threshold for x may depend on ϵ, Y .

Every candidate has

$$p \equiv u \pmod{M}, \quad p-1 = crQ, \quad r \leq x^\epsilon, \quad Q > x^{0.9} \text{ prime}, \quad (34)$$

and every odd prime divisor of r exceeds Y . The marked primes exceed any fixed Y once x is sufficiently large. The factor ϵ in (33), previously absorbed into the constant, is the dependence we shall need.

10 The consequence of the zero-free strip

We now use a zero-free half-plane for the first time. The theorem of Cureton and Thorner [1, Theorem 1.1] supplies the width $\delta = 1/6000$ for every number field. We retain a general δ below: the following bound is uniform in the number field and in the width of the strip. That second uniformity is what keeps the final constant independent of N .

Lemma 7. *Let $0 < \delta \leq 1/2$. Suppose $K/\mathbb{Q}$ is Galois, of degree n and discriminant D_K , and its nontrivial zeta zeros have real part at most $1 - \delta$. Then*

$$\#\{x < p \leq 2x : p \text{ splits completely in } K\} \ll \frac{x}{nL} + \frac{x^{1-\delta}}{L} \left(\frac{\log |D_K|}{n} + 1 \right). \quad (35)$$

The implied constant is absolute; in particular it is independent of both K and δ .

Proof. Choose a fixed nonnegative smooth function f , supported in $(1/2, 3)$, with $f \geq 1$ on $[1, 2]$, and write

$$\hat{f}(s) = \int_0^\infty f(t)t^{s-1} dt.$$

For an integral ideal $\mathfrak{a}$, let $\Lambda_K(\mathfrak{a}) = \log N\mathfrak{p}$ if $\mathfrak{a}$ is a positive power of a prime ideal $\mathfrak{p}$, and let it be zero otherwise. The smoothed Dedekind explicit formula gives

$$\sum_{\mathfrak{a}} \Lambda_K(\mathfrak{a}) f(N\mathfrak{a}/x) = x\hat{f}(1) - \sum_{\rho} x^{\rho} \hat{f}(\rho) + O_f(n \log(2x)).$$

The last term is harmless for our upper bound. The uniform zero count

$$N_K(T) \ll (T+1)(\log |D_K| + n \log(T+3))$$

and the rapid decay of $\hat{f}(\sigma + it)$, uniformly for $0 \leq \sigma \leq 1$, imply $\sum_{\rho} |\hat{f}(\rho)| \ll_f \log |D_K| + n$. The zero sum is therefore $O_f(x^{1-\delta}(\log |D_K| + n))$. Since $1 - \delta \geq 1/2$, the remainder is absorbed with a constant independent of δ . Each completely split prime $x < p \leq 2x$ contributes at least $n \log x$, and all other coefficients on the left are nonnegative. Division proves (35). Zeros on the boundary $\Re s = 1 - \delta$ are allowed throughout. $\square$

The Kummer fields. Let h_a be the greatest common divisor of the prime valuations of $|a|$. For odd $q \nmid h_a$, $X^q - a$ is irreducible, the pure field has degree q , and this is coprime to $[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = q-1$. Thus

$$[K_q : \mathbb{Q}] = q(q-1).$$

The discriminant of the pure field divides the polynomial discriminant, whose absolute value is $q^q |a|^{q-1}$; the cyclotomic discriminant has absolute value q^{q-2} . The compositum discriminant inequality therefore gives

$$|D_{K_q}| \leq (q^q |a|^{q-1})^{q-1} (q^{q-2})^q.$$

Taking logarithms and dividing by the degree gives

$$\begin{aligned} \frac{\log |D_{K_q}|}{q(q-1)} &\leq \left(2 - \frac{1}{q-1}\right) \log q + \left(1 - \frac{1}{q}\right) \log |a| \\ &\leq 2 \log q + \log |a|. \end{aligned} \quad (36)$$

The degree and discriminant bounds are also recorded in [2, Lemma 9.1, (9.1)] for all sufficiently large prime q . Write $Q_0(a)$ for the fixed cutoff in that cited statement. To retain precisely its

quantifiers, as in the formalization, include $Q_0(a)$ and the prime divisors of h_a in the choice of Y_a , and take $Y \geq Y_a$. This choice depends only on a , not on δ . Lemma 7 now gives, uniformly for $q > Y$, that

$$B_q(x) := \#\{x < p \leq 2x : p \text{ splits completely in } K_q\} \ll_a \frac{x}{q(q-1)L} + \frac{x^{1-\delta} \log(2q)}{L}. \quad (37)$$

Since $\sum_{q \leq T} \log q \ll T$ and $\sum_{q > Y} 1/(q(q-1)) \ll 1/(Y \log Y)$, summing (37) yields

$$\sum_{Y < q \leq x^\epsilon} B_q(x) \leq \frac{C_a}{Y \log Y} \frac{x}{L} + O_a(x^{1-\delta+\epsilon}/L). \quad (38)$$

All sums here are over primes. The constant C_a and the implied constant are independent of δ . For each fixed $\epsilon < \delta$, the error is $o(x/L)$.

11 Completing the proof and choosing the zero-free width

Let p be a candidate prime. Its index $i_p(a)$ is odd, by the chosen progression. If it exceeds one, choose an odd prime $q \mid i_p(a)$. Since $p-1 = crQ$, there are just two cases.

If $q \mid r$, then $Y < q \leq x^\epsilon$. Here $p > q$ and $p \nmid a$, so the ramification exclusions in the splitting criterion hold. The index criterion from Section 2 identifies p as a completely split prime of K_q . Equation (38) bounds all candidates lost in this case.

If $q = Q$, then $\text{ord}_p(a) \mid cr \leq 4x^\epsilon$. Therefore p divides the nonzero integer

$$\prod_{1 \leq j \leq 4x^\epsilon} |a^j - 1|.$$

The logarithm of this product is $O_a(x^{2\epsilon})$, because $\log |a^j - 1| \ll_a j$. Every distinct prime divisor exceeding x contributes at least $\log x$ to this logarithm. There are consequently at most $O_a(x^{2\epsilon}/L)$ such primes. This is $o(x/L)$ if $2\epsilon < 1$.

Combining the candidate lower bound with these two subtractions gives

$$N_a(x, 2x) \geq \left(\frac{A_a \epsilon - C_a/Y}{\log Y} + o(1) \right) \frac{x}{L} \quad (\epsilon < \delta, 2\epsilon < 1). \quad (39)$$

Here A_a, C_a are positive constants independent of ϵ, Y, δ , once the sieve parameters have been fixed as in Section 9.

Choose a positive θ_a so small that $\theta_a < \min(\kappa, b, 1)/10$, and put

$$\delta = \frac{1}{N}, \quad \epsilon = \frac{\theta_a}{N}, \quad Y = \max \left(Y_a, \frac{4C_a}{A_a \epsilon} \right).$$

Then $\epsilon < \delta$, $2\epsilon < 1$, and $C_a/Y \leq A_a \epsilon/4$. Moreover $Y \asymp_a N$ for $N \geq 2$, and hence $\log Y \asymp_a \log N$. For sufficiently large x , (39) yields

$$N_a(x, 2x) \geq \frac{A_a \epsilon}{2 \log Y} \frac{x}{L} \gg_a \frac{x}{N \log N \log x}.$$

This proves the dyadic assertion of Theorem 2. Applying it to $(X/2, X]$ and using the prime number theorem gives the stated positive lower relative density, after adjusting the constant. Finally, [1, Theorem 1.1] permits $N = 6000$, which proves Theorem 1.

Notice the order of quantifiers: the same constant depending on a works for every fixed N , but x must then exceed a threshold depending on a, N . We claim no uniform bound for that threshold when N grows with x .

12 The density bound and its limits

There are three distinct questions: the lower bound furnished by this construction, the optimal consequence of a prescribed zero-free strip, and the exact Artin density.

For the present construction, fix the sieve parameters and examine the coefficient

$$f_\epsilon(Y) = \frac{A_a\epsilon - C_a/Y}{\log Y}.$$

To make it positive, one needs $Y > C_a/(A_a\epsilon)$. Thus, as $\epsilon \rightarrow 0$, its positive values are at most a constant multiple of $\epsilon/\log(1/\epsilon)$. Conversely, taking Y to be a sufficiently large constant multiple of $1/\epsilon$ gives that order. Differentiating shows that the optimizing value satisfies

$$Y = \frac{C_a}{A_a\epsilon}(\log Y + 1).$$

It has size $\epsilon^{-1}\log(1/\epsilon)$; this improves the constant in the guaranteed bound, but does not change its order. When using the zero-free width $1/N$, the splitting error requires $\epsilon < 1/N$, and the order obtained from this final balance is $1/(N \log N)$.

This is an optimization of the displayed lower bound, with the other sieve parameters fixed. It is not an upper bound on what could follow from QRH(N), and it does not show that a different argument cannot do better. The constant c_a is not evaluated numerically here: in particular, the marked replacement input does not specify here a numerical choice of K .

With Proposition 3 supplied by the cited marked Type II estimates, the theorem takes the form

$$\text{QRH}(N) \implies \liminf_{X \rightarrow \infty} \frac{P_a(X)}{\pi(X)} \gg_a \frac{1}{N \log N}.$$

The theorem of Cureton and Thorner [1, Theorem 1.1] establishes the premise for $N = 6000$, giving the unconditional positive-proportion result. The implication for a general N records how the lower bound changes with any available zero-free width; it does not assert that every stronger zero-free region is known.

There is no substantive difference between writing $\log N$ and $\log(2N)$ in this lower bound. For $N \geq 2$,

$$\log N \leq \log(2N) \leq 2 \log N.$$

Thus either formulation implies the other after changing the constant by at most a factor of two. In particular, that constant can still be chosen independently of N .

For comparison, $N = 2$ is a special case: the functional equation reflects every nontrivial zero across $\Re s = 1/2$, so QRH(2) is the generalized Riemann hypothesis. Hooley's theorem then gives the full density $A(a)$, without using marked replacement.

For substantially wider strips, classical arguments also give a positive proportion without using marked replacement. Hooley's refinement, discussed by Murty [6], applies when the zero-free width is greater than $1/(2e)$. In particular it covers integer $N = 3, 4, 5$. This historical result gives positive proportion, rather than the full Artin density; it should be distinguished from the small-width quantitative argument developed here.

Finally, finite inclusion-exclusion and Chebotarev give the unconditional upper bound

$$\limsup_{X \rightarrow \infty} \frac{P_a(X)}{\pi(X)} \leq A(a).$$

Here extend the notation to $K_2 = \mathbb{Q}(\sqrt{a})$. For any fixed y , apart from the finitely many ramified primes, every primitive-root prime avoids complete splitting in all K_q with $q \leq y$, including $q = 2$. The density of primes avoiding this finite list is

$$\sum_{n \mid \prod_{q \leq y} q} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, a^{1/n}) : \mathbb{Q}]}.$$

Letting $y \rightarrow \infty$ gives the assertion by absolute convergence. Our argument supplies a positive lower bound using a restricted family of predecessors. It does not show that all remaining primes contribute the amount needed to reach this upper bound.

Formal verification. The accompanying Lean development verifies the positive-proportion argument from explicitly stated versions of the cited results and the classical analytic inputs. In particular, the candidate-prime estimate, the cofactor tails and full-mass comparison, the Buchstab subtraction, the semiprime bound, the Kummer splitting estimate, and the final parameter choice are proved within the development. None of these intermediate estimates is left as an additional input to the final theorem. That theorem gives $c_a/(N \log N)$, with $c_a > 0$ chosen before N , and its specialization at $N = 6000$.

The accepted source theorems themselves remain explicit hypotheses of the formal theorem; their proofs have not been formalized here. Thus Lean checks the deduction from those statements. Matching the formal hypotheses to the cited mathematical results is a separate source check. The development records these hypotheses and their references, and its completed build has no proof placeholders or added global axioms.

Acknowledgments

I thank Peter Sarnak for helpful conversations. GPT-6 was used to help write and formalize the arguments. The author was supported by the National Science Foundation (Grant DMS-1001828).

References

- [1] D. Cureton and J. Thorner, A quasi-Riemann hypothesis for Dedekind zeta functions, Hexagon preprint 2610.00200v1, 12 October 2026. See Theorem 1.1. [hexagon:2610.00200v1](#).
- [2] OpenAI, Primitive roots for every admissible integer base, preprint, 4 October 2026. The marked replacement proposition follows from Lemma 10.2 and Proposition 10.3, with the fixed-progression and smooth-weight separation in the proof of Lemma 12.1. The block sieve and rough-number estimates appear in Sections 11–12. [Manuscript](#).
- [3] OpenAI, The Poisson–Dirichlet law for prime predecessors, preprint, 24 September 2026. See Theorem 3.1 for the one-sided marked Type II estimate, and Sections 3–5 for its proof. [Manuscript](#).
- [4] C. Hooley, On Artin’s conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
- [5] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I: Classical Theory*, Cambridge Studies in Advanced Mathematics **97**, Cambridge University Press, 2007. Standard background on primes in progressions and sieve estimates.
- [6] M. Ram Murty, Artin’s conjecture and elliptic analogues, in *Sieve Methods, Exponential Sums, and their Applications in Number Theory*, G. R. H. Greaves, G. Harman, and M. N. Huxley (eds.), Cambridge University Press, 1997, 325–344. See Section 1 for Hooley’s weaker zero-free hypothesis. [doi:10.1017/CBO9780511526091.022](#).