MATHEMATICS OF COMPUTATION
Volume 65, Number 216
October 1996, Pages 1717–1735

EXPLICIT BOUNDS FOR PRIMES IN RESIDUE CLASSES

ERIC BACH AND JONATHAN SORENSON

Abstract. Let E/K be an abelian extension of number fields, with $E \neq \mathbb{Q}$. Let Δ and n denote the absolute discriminant and degree of E. Let σ denote an element of the Galois group of E/K. We prove the following theorems, assuming the Extended Riemann Hypothesis:

(1) There is a degree-1 prime $\mathfrak{p}$ of K such that $\left(\frac{\mathfrak{p}}{E/K}\right) = \sigma$, satisfying $N\mathfrak{p} \leq (1 + o(1))(\log \Delta + 2n)^2$.

(2) There is a degree-1 prime $\mathfrak{p}$ of K such that $\left(\frac{\mathfrak{p}}{E/K}\right)$ generates the same group as σ, satisfying $N\mathfrak{p} \leq (1 + o(1))(\log \Delta)^2$.

(3) For $K = \mathbb{Q}$, there is a prime p such that $\left(\frac{p}{E/\mathbb{Q}}\right) = \sigma$, satisfying $p \leq (1 + o(1))(\log \Delta)^2$.

In (1) and (2) we can in fact take $\mathfrak{p}$ to be unramified in $K/\mathbb{Q}$. A special case of this result is the following.

(4) If $\gcd(m, q) = 1$, the least prime $p \equiv m \pmod q$ satisfies $p \leq (1 + o(1))(\varphi(q) \log q)^2$.

It follows from our proof that (1)–(3) also hold for arbitrary Galois extensions, provided we replace σ by its conjugacy class $\langle\sigma\rangle$. Our theorems lead to explicit versions of (1)–(4), including the following: the least prime $p \equiv m \pmod q$ is less than $2(q \log q)^2$.

1. Introduction

In this paper, we present explicit versions of several useful theorems from analytic number theory. All of our results will rely on the Extended Riemann Hypothesis (ERH). This has been used by many authors as a heuristic assumption, in attempts to explain the observed behavior of number-theoretic algorithms. Thus, our results can be used to obtain explicit bounds on the running times of these algorithms.

The problems we will address involve the distribution of primes in residue classes, and more generally, the distribution of prime ideals in cosets of generalized class groups. This subject has a long history, going back to Euler's statement that every arithmetic progression beginning with 1 contains an infinite number of primes. The generalization to arbitrary progressions was proved by Dirichlet [13, 14], in work

Received by the editor October 4, 1994 and, in revised form, September 5, 1995.

1991 *Mathematics Subject Classification.* Primary 11N13, 11M26; Secondary 11R44, 11Y35.

This research was supported in part by NSF grants CCR-9208639 and CCR-9204414, a grant from the Wisconsin Alumni Research Foundation, and a Butler University Fellowship.

An extended abstract appeared in the *Proceedings of Symposia in Applied Mathematics: Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics*, Mathematics of Computation 50th Anniversary Symposium, August 9–13, 1993, Vancouver, British Columbia, as part of the *Lehmer Minisymposium* on computational number theory, Walter Gautschi, Editor, *PSAPM* volume 48, published by the American Mathematical Society, pp. 535–539.

that many consider to be the start of rigorous analytic number theory. We will not review all of the history here, but only mention how the ERH has come into play.

Various authors have observed that if $\gcd(m,q) = 1$, then the least prime p congruent to m mod q is not very large. Thus, a search for p through the sequence $m, m+q, m+2q, \dots$ should terminate quickly. Linnik [21] proved that $p \le q^{O(1)}$; the sharpest known estimate of the exponent is due to Heath-Brown [17]: $p = O(q^{11/2})$. (No explicit version of Linnik's theorem seems to be known.) However, the available data on primes in progressions [36] suggest this exponent is too large. In an attempt to obtain realistic estimates, several authors have invoked the ERH. From work of Chowla [10], Titchmarsh [34], Turán [35], and Wang, Hsieh, and Yu [37], we have the bound $p = q^{2+o(1)}$, assuming the ERH.

In algebraic number theory, Dirichlet's theorem generalizes to the theorem of Chebotarev [33], which states that there are infinitely many prime ideals with each possible Artin symbol, and estimates their density. It then becomes a problem to estimate the least such prime ideal. This was done (assuming ERH) by Lagarias and Odlyzko [23], and Lagarias, Montgomery, and Odlyzko [22]. Oesterlé [29] has stated an explicit version of this theorem: if E/K is a Galois extension of number fields, then the least prime ideal of K with a given Artin symbol must have norm no larger than $70(\log|\Delta|)^2$, if Δ is the discriminant of E. (Oesterlé apparently never published his proof.) We improve this result in two ways: our constant factor is smaller, and we show that the least prime ideal can be taken to have degree 1, a property that is important for applications.

In the design of algorithms, one frequently uses a prime with a given Artin symbol not for its own sake, but because it has some group-theoretic property. For example, to construct an irreducible polynomial of degree 3 over a finite field of p elements, we can use a cubic nonresidue q mod p. Although there are two possibilities for the power character of q, they are both equivalent as far as the algorithmic problem is concerned. With this and similar applications in mind, we will say that two elements of a group are *equivalent* if they generate the same subgroup. As we will see, slightly sharper results can be obtained for the relaxed problem of finding a prime with Artin symbol equivalent to a given one.

It is an interesting problem to give efficient constructions for numbers with given group-theoretic properties modulo n. We will not go more deeply into this here, except to note some cases in which our bounds do not lead to efficient constructions. If G is a proper subgroup of the multiplicative group modulo p, the least prime outside G is $O(\log p)^2$ [4] assuming ERH. Under the same assumption, the least primitive root mod p is $O(\log p)^6$ [32]. In both cases, using the theorems of this paper would lead to bounds of $O(p \log p)^2$.

It is also of interest to ask if the growth rates in our estimates are best possible. We believe they are not, although proving this seems out of reach even with the ERH. For one thing, a key step in our proof is to estimate an oscillatory sum by taking the absolute value of each term; one would naturally expect lots of cancellation, which we ignore. Also, simple probabilistic models suggest that the least $p \equiv m$ mod q is $O(\varphi(q)(\log q)^2)$ [8, 18, 36]. In this case, replacing an *ad hoc* model with a "name brand" heuristic like the ERH essentially squares the bound. All of this suggests an interesting arena for more computational experiments.

The ERH is supported by computational evidence and probabilistic arguments. For the first, we refer the reader to the references in [5] and the recent work of Rumely [31]. An example of the second, based on ideas of Cramér, appears in [6].

As possible applications of our results, we mention the following. Brent and Kung's construction of n-bit multipliers with low area-time complexity [9] uses a prime congruent to 1 mod n. Bach and Shallit's generalization of the "$p \pm 1$" factoring method [7] requires a prime in a certain residue class, with prescribed splitting behavior. A similar device was used by Adleman and Lenstra [2] to construct irreducible polynomials over finite fields. Finally, our results allow one to estimate the least prime p for which $(\frac{p}{n})$ takes a prescribed value; such primes are useful in primality testing [25] and other contexts.

We now give a rough sketch indicating our argument, using the notation of [5]. Suppose for simplicity that $(\mathbb{Z}/(n))^*/G$ is cyclic of prime order, and we want a prime belonging to a coset C that generates this group. Suppose there are no such primes below x. Then the following sum, taken over all characters χ of $(\mathbb{Z}/(n))^*/G$, must vanish for every $a > 0$:

$$\sum_{\chi} \sum_{n<x} \bar{\chi}(C)\Lambda(n)\chi(n)(n/x)^a \log(x/n) = 0.$$

If we evaluate this by residues and observe that $\prod_{\chi} L(s,\chi) = \zeta_K$, we obtain an estimate

$$\frac{x}{(1+a)^2} \leq \frac{\sqrt{x}}{2a+1}[\log\Delta + O(1)] + \cdots,$$

where Δ is the discriminant of the nth cyclotomic field, and $\cdots$ indicates error terms that asymptotically are small. Taking a arbitrarily close to 0 leads to the estimate

$$x \leq (1+o(1))(\log\Delta)^2.$$

After covering some notation and background in §2, we state and prove our asymptotic results in §3, with the technical details deferred to §4. We conclude with explicit bounds in §5.

2. Notation and background

This is a companion piece to [5], so we refer the reader to that paper (especially §3) for undefined notation and terminology.

The complexity of a number field is measured by two invariants: its *degree* n and its *discriminant* Δ. For convenience we will suppress the sign of the discriminant, so that $\Delta > 0$ henceforth. Recall that $n = r_1 + 2r_2$, where r_1 is the number of real embeddings and $2r_2$ is the number of complex embeddings. We will use subscripts such as K or E/K to signal that an invariant depends on a field or an extension. (Note that the discriminant of an extension is an ideal.)

The discriminant of a field is a multiple of the discriminant of any subfield. More precisely, if E/K is an extension of number fields, we have

$$\Delta_E = \Delta_K^{n_{E/K}} N\Delta_{E/K}. \tag{2.1}$$

(See [20, §15].)

If K is an algebraic number field, we will say "prime of K" rather than "nonzero prime ideal of the ring of algebraic integers of K." Also, if E/K is an abelian extension, and χ is a character of the Galois group of E/K, the Artin symbol induces a function on the integral ideals of K; for simplicity, we will use the symbol χ for both. We also write $\hat{\chi}$ for the primitive character induced by χ.

Suppose E/K is an abelian extension, with Galois group G. For each character χ of G, there is an associated intermediate field E_χ (so that $K \subset E_\chi \subset E$). A theorem due to Hecke (see [19]) states that $\zeta_E(s)$, the Dedekind zeta function of E, is a product of Hecke L-functions:

$$\zeta_E(s) = \prod_{\chi} L(s, \hat{\chi}). \tag{2.2}$$

This, together with representations of ζ'/ζ and L'/L (i.e., (3.11) and (3.12) of [5]), leads to the *conductor-discriminant formula*

$$\Delta_{E/K} = \prod_{\chi} \mathfrak{f}_{\chi}, \tag{2.3}$$

in which $\mathfrak{f}_{\chi}$ denotes the conductor of E_{χ}/K.

As in [5], we will use the digamma function $\psi(s) = \Gamma'(s)/\Gamma(s)$. We recall the following identities:

$$2\psi(2s) = \psi(s) + \psi(s+1/2) + 2\log 2 \quad (\textit{duplication formula}), \tag{2.4}$$

$$\psi(1+s) = \psi(s) + \frac{1}{s} \quad (\textit{recurrence relation}). \tag{2.5}$$

Differentiating these, we get

$$4\psi'(2s) = \psi'(s) + \psi'(s+1/2) \tag{2.6}$$

and

$$\psi'(1+s) = \psi'(s) - \frac{1}{s^2}. \tag{2.7}$$

For further properties of the digamma function and its derivative, see Abramowitz and Stegun [1].

Finally, we recall a representation given in [5]. With the convention that zeros in sums are restricted to the critical strip, we have

$$\begin{aligned} \frac{L'}{L}(s,\hat{\chi}) \quad &= \quad \sum_{L(\rho,\hat{\chi})=0} \left(\frac{1}{s-\rho} - \frac{1}{2-\rho} \right) - [\psi_{\hat{\chi}}(s) - \psi_{\hat{\chi}}(2)] \\ &\quad - E_{\hat{\chi}} \left[\frac{1}{s} - \frac{1}{s-1} + \frac{3}{2} \right] + \frac{L'}{L}(2,\hat{\chi}), \end{aligned} \tag{2.8}$$

where $E_{\hat{\chi}}$ is 1 if $\hat{\chi}$ is principal, 0 otherwise, and

$$\psi_{\hat{\chi}}(s) = \frac{r_2 + \alpha(\hat{\chi})}{2} \psi\left(\frac{s}{2}\right) + \frac{r_2 + \beta(\hat{\chi})}{2} \psi\left(\frac{s+1}{2}\right) - \frac{n \log \pi}{2}. \tag{2.9}$$

In this formula, $\alpha(\hat{\chi})$ and $\beta(\hat{\chi})$ are nonnegative integers summing to r_1. We will not need their definitions here, except to note that for the principal character, $\alpha = r_1$ and $\beta = 0$. (We also write ψ_{ζ_K} in this case.)

By combining (2.2) and (2.9), one can show

$$\psi_{\zeta_E}(s) = \sum_{\chi} \psi_{\hat{\chi}}(s). \tag{2.10}$$

The remainder of the paper assumes that the zeta functions of E and $\mathbb{Q}$ are zero-free in $\Re(s) > 1/2$. To make our results useful in other contexts, however, we will explicitly indicate which lemmas and theorems make these assumptions. The others hold unconditionally.

In the sequel, let a be a real number with $0 < a < 1$. We require the inequality

$$z^a \log(1/z) \leq \frac{1}{ea} \tag{2.11}$$

which is valid for $0 < z \leq 1$.

3. Asymptotic bounds

In this section, we give asymptotic versions of our estimates. Our proofs will rely upon analytic lemmas that are given in §4. Roughly speaking, we obtain our bounds by taking linear combinations of the "explicit formulas" from [5].

Theorem 3.1 (ERH)**.** *Let E/K be an abelian extension of number fields, with $E \neq \mathbb{Q}$. Let Δ denote the absolute value of E's discriminant* (*we assume $\Delta \to \infty$*)*. Let n denote the degree of E. Let $\sigma \in G$, the Galois group of E/K.*

1. *There is a prime ideal $\mathfrak{p}$ of K with $\left(\frac{\mathfrak{p}}{E/K}\right) = \sigma$, of residue degree* 1*, satisfying $N\mathfrak{p} \leq (1 + o(1))(\log\Delta + 2n)^2$.*
2. *There is a degree-*1 *prime ideal $\mathfrak{p}$ of K such that $\left(\frac{\mathfrak{p}}{E/K}\right)$ is equivalent to σ, satisfying $N\mathfrak{p} \leq (1 + o(1))(\log\Delta)^2$.*
3. *For $K = \mathbb{Q}$, there is a prime p with $\left(\frac{p}{E/\mathbb{Q}}\right) = \sigma$, satisfying $p \leq (1+o(1))\cdot(\log\Delta)^2$.*

In cases (1) *and* (2) *we can take $\mathfrak{p}$ to be unramified in $K/\mathbb{Q}$.*

(Recall that σ and σ' are equivalent if they generate the same subgroup of G.)

Before giving the proof, we note two facts.

Theorem 3.2. *If Theorem 3.1 holds for cyclic extensions, then it holds for arbitrary abelian extensions.*

Proof. This uses a trick from [12] (see also [26]). Let L be the subfield of E fixed by σ. Then E/L is cyclic. Let $\mathfrak{P}$ be a prime of L satisfying the conditions of the theorem for E/L. Then $\mathfrak{P}$ lies above some prime $\mathfrak{p}$ of K, and we have $N\mathfrak{p} = N\mathfrak{P}$ (this is in fact a rational prime p). Then for any prime $\wp$ of E dividing $\mathfrak{P}$, we have (for all integral x)

$$x^\sigma \equiv x^{N\mathfrak{P}} = x^{N\mathfrak{p}} \bmod \wp.$$

If we replace $\wp$ by another prime divisor of $\mathfrak{p}$, then the same relation holds (in general, the relation holds for some conjugate of σ, but E/K is abelian, so this conjugate must equal σ). This shows that $\left(\frac{\mathfrak{p}}{E/K}\right) = \sigma$, as desired. Clearly, any upper bound on $N\mathfrak{P}$ is also an upper bound on $N\mathfrak{p}$. □

If E/K is Galois, then the Artin symbol is no longer an element but a conjugacy class. The above argument is still valid with this modification, so we have the following result.

Corollary 3.3 (ERH)**.** *Theorem 3.1 holds for Galois extensions E/K, provided we replace σ by its conjugacy class $\langle\sigma\rangle$.*

Proof of Theorem 3.1. We give a proof of (1). A proof for (2) is obtained by substituting zero for $p(x)$, and a proof for (3) is obtained by substituting zero for $d(x)$ and $r(x)$.

By Theorem 3.2, we may assume that E/K has a cyclic Galois group G. As in [5], we consider

$$S(x,\chi) = \sum_{N\mathfrak{a}<x} \Lambda(\mathfrak{a})\chi(\mathfrak{a}) \left(\frac{N\mathfrak{a}}{x}\right)^a \log\left(\frac{x}{N\mathfrak{a}}\right). \tag{3.1}$$

If $\mu = \sigma^{-1}$, we may sum this over all characters χ of G to obtain

$$\sum_{\chi} \chi(\mu) S(x,\chi) = |G| \sum_{\substack{N\mathfrak{a}<x \\ \chi(\mathfrak{a})=\chi(\sigma)}} \Lambda(\mathfrak{a}) \left(\frac{N\mathfrak{a}}{x}\right)^a \log\left(\frac{x}{N\mathfrak{a}}\right). \tag{3.2}$$

Denote the contribution of proper prime powers, ramified primes, and powers of primes of degree greater than 1 to the right-hand side above by $p(x)$, $r(x)$, and $d(x)$, respectively. If no primes $< x$ meet the conditions of the theorem, then

$$\sum_{\chi} \chi(\mu) S(x,\chi) \leq p(x) + r(x) + d(x).$$

Let $i(x)$ be the additional error incurred by using primitive characters in the left-hand sum, so that

$$\sum_{\chi} \chi(\mu) S(x,\hat{\chi}) \leq i(x) + p(x) + r(x) + d(x). \tag{3.3}$$

Let $a = 1/\log\log\Delta$; for sufficiently large Δ we will have $0 < a < 1$.

By a residue computation we have

$$\sum_{\chi} \chi(\mu) S(x,\hat{\chi}) = x(1+o(1)) - (1+o(1))\sqrt{x}(\log\Delta - 2n)$$
$$- O(n(\log\log\Delta)^2) - \log x(\log\Delta + n\log\log\Delta).$$

(See §4.2.) We also have the following bounds:

$$\begin{aligned} i(x) &= O(\log x \log\Delta \log\log n \log\log\Delta), \\ r(x) &= O(\log x \log\Delta \log\log\Delta), \\ d(x) &\leq 2n\sqrt{x}(1+o(1)), \\ p(x) &\leq 2n\sqrt{x}(1+o(1)). \end{aligned}$$

By Minkowski's Theorem, $n \leq O(\log\Delta)$.

Thus,

$$x(1+o(1)) \leq \sqrt{x}(\log\Delta + 2n) + \log x(\log\Delta)^{1+o(1)}.$$

Dividing by $\sqrt{x}$, noting that we may assume $x \geq (\log\Delta)^2$, and then squaring both sides completes the proof. □

We give two applications of this result.

Corollary 3.4 (ERH)**.** *Let m and q be integers, with* $\gcd(m,q) = 1$*. There is a prime $p \equiv m \pmod q$ satisfying $p \leq (1+o(1))(\varphi(q)\log q)^2$.*

Proof. Let K be $\mathbb{Q}$ and E be $\mathbb{Q}(\omega)$, where ω is a primitive qth root of unity. Then the corollary follows immediately from the proof of Theorem 3.1 (note that $d(x) = r(x) = 0$ since $n_K = 1$). □

Corollary 3.5 (ERH)**.** *Let K be a quadratic field, with discriminant D and class number h. Each ideal class of K contains an unramified degree-*1 *prime $\mathfrak{p}$ satisfying $N\mathfrak{p} \leq (1+o(1))(h\log|D|)^2$.*

Proof. Take E to be the Hilbert class field of K. Then E/K is unramified, so $\Delta_E = |D|^h$. □

We do not know if the $2n$ term in Theorem 3.1 can be eliminated. Our proof does show that the coefficient 2 can be replaced by any number larger than $\psi(1) - \log 2\pi - 4 = 1.584907...$. In some cases, though, the $2n$ term is superfluous. This is so if $E/\mathbb{Q}$ is abelian, for then $n/\log \Delta = o(1)$. Ankeny [3] improved this and showed that if the Galois group of E is solvable in r steps, then $n/\log \Delta = O(1/\log \log \cdots \log n)$, where the log is iterated r times. To be able to disregard the $2n$ term, some condition on E seems necessary, because Golod and Shafarevich's examples of infinite class field towers [15] imply that $n/\log \Delta \neq o(1)$ (see Hasse [16, p. 46]). Alternatively, we can bound n in terms of $\log \Delta$; for this purpose, the discriminant bounds surveyed by Odlyzko [28] are useful.

4. Technical estimates

In this section we fill in the missing details from the proof of Theorem 3.1 by giving estimates for $p(x)$, $r(x)$, $d(x)$, $i(x)$, and by evaluating $\sum_\chi S(x, \hat{\chi})\chi(\mu)$ by residues.

4.1. **Handling imprimitive characters.** In this subsection we bound the error incurred by including imprimitive characters in the sum. First, we require two lemmas.

Lemma 4.1. *If $n \geq 2$, then*

$$\sum_{\substack{d|n \\ d>1}} \varphi(n/d) \leq \varphi(n)(e^\gamma \log \log n + 2).$$

Proof. Since $n = \sum_{d|n} \varphi(n/d)$, the sum is $n - \varphi(n) = \varphi(n)[n/\varphi(n) - 1]$. From (3.41) of [30] we conclude that $n/\varphi(n) \leq e^\gamma \log \log n + 3$ for $n \geq 2$, which completes the proof. □

Lemma 4.2. *Let E/K be a cyclic extension of degree n, with (primitive) character χ and conductor $\mathfrak{f}$. Let Δ be the absolute value of E's discriminant. Then $(N\mathfrak{f})^{\varphi(n)} \leq \Delta$.*

Proof. We first show that if χ and χ' generate the same subgroup of the character group, they must have the same conductor. (Here it is essential to interpret the conductor as a "cycle" or "ray modulus." See, e.g., [24].) By the definition of conductors, if $\mathfrak{p} \equiv 1 \bmod \mathfrak{f}$, then $\chi(\mathfrak{p}) = 1$; because χ' is a power of χ, we have $\chi'(\mathfrak{p}) = 1$. Therefore $\mathfrak{f}'$, the conductor of χ', is a multiple of $\mathfrak{f}$. By the same argument, $\mathfrak{f}$ is a multiple of $\mathfrak{f}'$, so they are equal.

Thus, there are $\varphi(n)$ characters with the same conductor; from the conductor-discriminant formula (2.3) we conclude

$$(N\mathfrak{f})^{\varphi(n)} \leq \prod_\chi N\mathfrak{f}_\chi \leq \Delta. \quad \square$$

Now, we can estimate the contribution of imprimitive characters. Let

$$i(x) = \sum_\chi \chi(\mu) S(x, \hat{\chi}) - \sum_\chi \chi(\mu) S(x, \chi). \tag{4.1}$$

The next lemma gives a bound for this.

Lemma 4.3. *Assume the hypotheses of the previous lemma. If E/K is unramified (in particular if $E = K$), then $i(x) = 0$. Otherwise,*

$$|i(x)| \leq \frac{e^{\gamma} \log\log n_{E/K} + 2}{ea \log 2} \log x \log \Delta_E,$$

which is $O((\log x \log \Delta \log\log n)/a)$.

Proof. By our hypothesis on E/K, the only possible imprimitive characters are the χ^d with $\gcd(d, n) > 1$. (Note that there are $\varphi(n/d)$ for each d.) Thus the total contribution of these will be at most

$$\begin{aligned}|i(x)| &\leq \sum_{\substack{d|n\\ d>1}} \varphi(\frac{n}{d}) \sum_{\substack{N\mathfrak{p}^k<x\\ \mathfrak{p}|\mathfrak{f}}} \Lambda(\mathfrak{p}^k) \left(\frac{N\mathfrak{p}^k}{x}\right)^a \log\left(\frac{x}{N\mathfrak{p}^k}\right)\\ &\leq \frac{1}{ea}\left(\sum_{\substack{d|n\\ d>1}} \varphi(n/d)\right) \sum_{\substack{N\mathfrak{p}^k<x\\ \mathfrak{p}|\mathfrak{f}}} \Lambda(\mathfrak{p}^k)\\ &\leq \frac{1}{ea}\left(\varphi(n)(e^{\gamma}\log\log n + 2)\right)\omega(\mathfrak{f})\log x,\end{aligned}$$

where $\omega(\mathfrak{f})$ is the number of distinct primes dividing $\mathfrak{f}$. (Here we have observed that $k \leq \frac{\log x}{\log N\mathfrak{p}}$ and used Lemma 4.1 and (2.11).) This is at most

$$\frac{e^{\gamma}\log\log n + 2}{ea \log 2} \log x(\varphi(n)\log N\mathfrak{f}).$$

Applying Lemma 4.2 gives the result. □

4.2. **Residue computations.** In this subsection we express the sum in (4.1) as a contour integral and evaluate it by residues. Formally, we have

$$\begin{aligned}\sum_{\chi} S(x, \hat{\chi})\chi(\mu) &= -\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2} \sum_{\chi} \chi(\mu)\frac{L'}{L}(s, \hat{\chi}) ds\\ &= I_1 + I_{1/2} + I_{\leq 0} + I_{-a},\end{aligned}$$

where I_x is the contribution of poles with real part x (and integral, in the case of $I_{\leq 0}$). This is justified as in [5].

4.2.1. *Residue at $s = 1$.*

Lemma 4.4. *We have*

$$I_1 = \frac{x}{(1+a)^2}.$$

Proof. Observe that only the principal character can contribute a pole at 1. □

4.2.2. *Residues at $\Re(s) = 1/2$.* First, we require two lemmas.

Lemma 4.5. *If $s > 1$, then*

$$\psi_{\zeta_E}(s) \leq \frac{n_E}{2}\left(\psi(s) - \log 2\pi\right).$$

Proof. By (2.9), we have

$$\begin{aligned}\psi_{\zeta_E}(s) &= \frac{r_1+r_2}{2}\psi\left(\frac{s}{2}\right)+\frac{r_1}{2}\psi\left(\frac{s+1}{2}\right)-\frac{n_E\log\pi}{2}\\ &= \frac{n_E}{2}\left[\frac{r_1}{n_E}\psi\left(\frac{s}{2}\right)+\frac{2r_2}{n_E}\frac{\psi(\frac{s}{2})+\psi(\frac{s+1}{2})}{2}\right]-\frac{n_E\log\pi}{2},\end{aligned}$$

where $n_E = r_1+2r_2$. Since ψ is increasing,

$$\psi\left(\frac{s}{2}\right) < \frac{\psi(\frac{s}{2})+\psi(\frac{s+1}{2})}{2}.$$

We use this inequality to bound the convex combination inside the brackets, and apply the duplication formula. □

Lemma 4.6 (ERH). *If $0<a<1$, then*

$$\sum_{\zeta_E(\rho)=0}\frac{1}{|\rho+a|^2}\le\frac{1}{2a+1}\left(\log\Delta_E+n_E(\psi(1+a)-\log 2\pi)+\frac{2}{a+1}+\frac{2}{a}\right),$$

where the sum is over zeros ρ of ζ_E with $0<\Re(\rho)<1$.

Proof. We have the identity

$$\frac{1}{|\rho+a|^2}=\frac{1}{2a+1}\left(\frac{1}{1+a-\rho}+\frac{1}{1+a-\overline{\rho}}\right).$$

Using (5.11) of [23], we have

$$\sum_{\zeta_E(\rho)=0}\left(\frac{1}{1+a-\rho}+\frac{1}{1+a-\overline{\rho}}\right)=\log\Delta_E+\frac{2}{1+a}+\frac{2}{a}+2\psi_{\zeta_E}(1+a)+2\frac{\zeta_E'}{\zeta_E}(1+a).$$

Using Lemma 4.5 and noting that $\zeta_E'/\zeta_E(1+a)\le 0$ completes the proof. □

Lemma 4.7 (ERH). *We have*

$$|I_{1/2}|\le\frac{\sqrt{x}}{2a+1}\left[\log\Delta_E+n_E(\psi(1+a)-\log 2\pi)+\frac{2}{1+a}+\frac{2}{a}\right].$$

Proof. Assuming the ERH, we get

$$\begin{aligned}|I_{1/2}| &\le \sqrt{x}\sum_{\chi}\sum_{L(\rho,\hat{\chi})=0}\frac{1}{|\rho+a|^2}\\ &= \sqrt{x}\sum_{\zeta_E(\rho)=0}\frac{1}{|\rho+a|^2}.\end{aligned}$$

Now use Lemma 4.6. □

4.2.3. *Residues at $s=0,-1,-2,\ldots$.*

Lemma 4.8. *We have*

$$|I_{\le 0}|\le n_E\left(\frac{1}{a^2}+\frac{1}{x(1-a)^2}+\frac{3}{x^2}\right)=O_a(n_E).$$

Proof. For $k = 0, 1, 2, \ldots$ we have a term

$$-\frac{x^{-k}}{(a-k)^2} \sum_{\chi} \hat{\chi}(\mu) \operatorname{Res}_{-k} \frac{L'}{L}(s, \hat{\chi}).$$

All of the residues are nonnegative because they come from zeros of L-functions in the left half-plane. (Recall L is always analytic there, even for the principal character.) Therefore, the absolute value of this is at most

$$\begin{aligned} \frac{x^{-k}}{(a-k)^2} \sum_{\chi} \operatorname{Res}_{-k} \frac{L'}{L}(s, \hat{\chi}) &= \frac{x^{-k}}{(a-k)^2} \operatorname{Res}_{-k} \frac{\zeta_E'}{\zeta_E}(s) \\ &\le \frac{n_E x^{-k}}{(a-k)^2}. \end{aligned}$$

(Here we used the fact that $\operatorname{Res}_{-k} \zeta_E'/\zeta_E(s) \le n_E$; see [5, §2].) Summing over all values of $k \ge 0$ and noting that $x \ge 1$, we obtain the bound. □

4.2.4. *Residue at $s = -a$.* Since there is a double pole at $s = -a$, we have

$$\begin{aligned} I_{-a} &= -\sum_{\chi} \chi(\mu) \frac{d}{ds} \left(x^s \frac{L'}{L}(s, \hat{\chi}) \right)_{s=-a} \\ &= -(\log x) x^{-a} \sum_{\chi} \chi(\mu) \frac{L'}{L}(-a, \hat{\chi}) - x^{-a} \sum_{\chi} \chi(\mu) \left(\frac{L'}{L} \right)' (-a, \hat{\chi}). \end{aligned}$$

We write A_1 for the first term and A_2 for the second, so that $I_{-a} = A_1 + A_2$.

Lemma 4.9. *The absolute value of A_1 is at most*

$$\frac{\log x}{x^a} \left(\sum_{\zeta_E(\rho)=0} \frac{2+a}{|\rho + a|^2} + \frac{n_E}{2} \left(\psi\left(\frac{-a}{2}\right) - \psi\left(\frac{1-a}{2}\right) + 4 - 2\log 2 \right) + \frac{1}{a} \right).$$

Proof. Using (2.9), we get a representation for $\sum_{\chi} \chi(\mu) \frac{L'}{L}(-a, \hat{\chi})$. We now estimate each term of this. First, since the ρ are closer to $-a$ than 2,

$$\left| \sum_{\chi} \chi(\mu) \sum_{L(\rho, \hat{\chi})=0} \left(\frac{1}{-a-\rho} - \frac{1}{2-\rho} \right) \right| \le \sum_{\zeta_E(\rho)=0} \left| \frac{1}{\rho + a} + \frac{1}{2-\rho} \right| \le \sum_{\zeta_E(\rho)=0} \frac{2+a}{|\rho+a|^2}.$$

Second, (2.9) implies

$$\begin{aligned} \sum_{\chi} \chi(\mu)(\psi_{\hat{\chi}}(-a) - \psi_{\hat{\chi}}(2)) = \sum_{\chi} \chi(\mu) \Bigg(&\frac{r_2 + \alpha(\hat{\chi})}{2} \left(\psi\left(\frac{-a}{2}\right) - \psi(1) \right) \\ &+ \frac{r_2 + \beta(\hat{\chi})}{2} \left(\psi\left(\frac{1-a}{2}\right) - \psi\left(\frac{3}{2}\right) \right) \Bigg). \end{aligned}$$

Since $0 < a < 1$, we have $\psi(-a/2) - \psi(1) > 0$ and $\psi((1-a)/2) - \psi(3/2) < 0$, so the absolute value of this sum is bounded by

$$\begin{aligned} &\sum_{\chi} \left(\frac{n_K}{2} \left(\psi\left(\frac{-a}{2}\right) - \psi(1) \right) - \frac{n_K}{2} \left(\psi\left(\frac{1-a}{2}\right) - \psi\left(\frac{3}{2}\right) \right) \right) \\ &\qquad \le \frac{n_E}{2} \left(\psi\left(\frac{-a}{2}\right) - \psi(1) - \psi\left(\frac{1-a}{2}\right) + \psi\left(\frac{3}{2}\right) \right). \end{aligned}$$

Third, we have

$$-\sum_{\chi}\chi(\mu)E_{\hat{\chi}}\left[\frac{1}{-a}-\frac{1}{-a-1}+\frac{3}{2}\right]=\frac{1}{a}-\frac{1}{a+1}-\frac{3}{2},$$

which is at most $1/a$ in absolute value. Finally,

$$\left|\sum_{\chi}\chi(\mu)\frac{L'}{L}(2,\hat{\chi})\right|\le\sum_{\chi}\sum_{\mathfrak{a}}\frac{\Lambda(\mathfrak{a})}{N\mathfrak{a}^2}\le -n_{E/K}\frac{\zeta_K'}{\zeta_K}(2)\le -n_E\frac{\zeta'}{\zeta}(2)<n_E.$$

(Here we have used the special value $\frac{\zeta'}{\zeta}(2)=-0.569960\ldots$.) Combining these four estimates and observing that $\psi(3/2)-\psi(1)+2=4-2\log 2$, we get the result. □

Recall that we can use Lemma 4.6 to bound $\sum_{\zeta_E(\rho)=0}\frac{1}{|\rho+a|^2}$.

Lemma 4.10. *We have*

$$|A_2|\le\frac{1}{x^a}\left(\sum_{\zeta_E(\rho)=0}\frac{1}{|\rho+a|^2}+n_E\left(\psi'(2-a)+\frac{1}{(1-a)^2}+\frac{1}{a^2}\right)+\frac{1}{a^2}+\frac{1}{(1+a)^2}\right).$$

Proof. Differentiating (2.9) with respect to s, we get a representation for $\sum_{\chi}\chi(\mu)(\frac{L'}{L})'(-a,\hat{\chi})$. This is straightforward to estimate, once we observe that

$$\left|\sum_{\chi}\chi(\mu)\psi_{\hat{\chi}}'(-a)\right|\le\sum_{\chi}\psi_{\hat{\chi}}'(-a)=\psi_{\zeta_E}'(-a)=\frac{n_E}{4}\left(\psi'\left(\frac{-a}{2}\right)+\psi'\left(\frac{1-a}{2}\right)\right).$$

(Note that ψ' is always positive.) We apply (2.6) and (2.7) (twice) to get the result. □

In the next two subsections, we let $\Psi(x)=\sum_{n<x}\Lambda(n)$. (This is usually denoted by $\psi(x)$, but we use Ψ to avoid confusion with the digamma function.)

4.3. **Prime powers.** Next we derive a bound on $p(x)$, the contribution of prime powers to the sum (3.2). Thus,

$$p(x)\le|G|\sum_{\substack{N\mathfrak{p}^k<x\\k>1}}\Lambda(\mathfrak{p}^k)\left(\frac{N\mathfrak{p}^k}{x}\right)^a\log\left(\frac{x}{N\mathfrak{p}^k}\right).$$

Lemma 4.11. *We have*

$$p(x)\le 2n_E(\sqrt{x}+O(x^{1/3})).$$

Proof. Since $(N\mathfrak{p}^k/x)^a\le 1$, we have

$$p(x)\le n_{E/K}\sum_{\substack{N\mathfrak{p}^k<x\\k>1}}\Lambda(\mathfrak{p}^k)\log\left(\frac{x}{N\mathfrak{p}^k}\right).$$

Noticing that, for a fixed rational prime p,

$$\sum_{\mathfrak{p}|p}\Lambda(\mathfrak{p}^k)\log\left(\frac{x}{N\mathfrak{p}^k}\right)\le n_K\Lambda(p^k)\log\left(\frac{x}{p^k}\right)$$

and that $n_{E/K} n_K = n_E$, this gives us the upper bound

$$p(x) \leq n_E \sum_{\substack{p^k < x \\ k > 1}} \Lambda(p^k) \log\left(\frac{x}{p^k}\right).$$

Using integration by parts, we obtain

$$n_E \int_1^x \log(x/t) d(\Psi(t) - \theta(t)) = n_E \int_1^x \frac{\Psi(t) - \theta(t)}{t} dt.$$

Asymptotically, this is $2n_E(\sqrt{x} + O(x^{1/3}))$. □

From Theorems 2, 4, and 5 in [11], we easily obtain the explicit bound $\Psi(t) - \theta(t) < 1.001\sqrt{t} + (4/3)t^{1/3}$ for $t > 0$. Hence,

$$p(x) \leq 2n_E(1.001\sqrt{x} + 2x^{1/3}). \tag{4.2}$$

For values of a near 1 it is better to use the bound

$$p(x) \leq \frac{n_E}{ea}(1.001\sqrt{x} + (4/3)x^{1/3}), \tag{4.3}$$

which is derived by using (2.11) to bound $(N\mathfrak{p}^k/x)^a \log(x/N\mathfrak{p}^k)$.

4.4. **Primes of degree exceeding 1.** We now estimate $d(x)$, the contribution to (3.2) by primes of degree greater than 1. We have

$$d(x) \leq |G| \sum_{\substack{N\mathfrak{p}^k < x \\ \deg \mathfrak{p} > 1}} \Lambda(\mathfrak{p}^k) \left(\frac{N\mathfrak{p}^k}{x}\right)^a \log\left(\frac{x}{N\mathfrak{p}^k}\right).$$

We now prove the following.

Lemma 4.12 (RH). *If* $n_K > 1$, *then*

$$d(x) \leq 2n_E(\sqrt{x} + O(x^{1/4})).$$

If $n_K = 1$, *then* $d(x) = 0$.

Proof. Observe that for a rational prime p, if $\mathfrak{p} \mid p$ and $\deg \mathfrak{p} > 1$, then $N\mathfrak{p} \geq p^2$. As in the previous lemma, we have

$$\begin{aligned} d(x) &\leq n_E \sum_{p^{2k} < x} \Lambda(p^k) \log\left(\frac{x}{p^{2k}}\right) = 2n_E \sum_{p^k < \sqrt{x}} \Lambda(p^k) \log\left(\frac{\sqrt{x}}{p^k}\right) \\ &= 2n_E \int_1^{\sqrt{x}} \log(\sqrt{x}/t) d\Psi(t) = 2n_E \int_1^{\sqrt{x}} (\Psi(t)/t) dt. \end{aligned}$$

If we assume the RH, this is $2n_E(\sqrt{x} + O(x^{1/4}))$. □

Noting that $\Psi(t) < 1.04t$ (see (3.35) of [30]) gives the explicit bound

$$d(x) \leq 2n_E(1.04\sqrt{x}). \tag{4.4}$$

Using (2.11), we also have

$$d(x) \leq \frac{n_E}{ea}(1.04\sqrt{x}). \tag{4.5}$$

4.5. **Ramified primes.**

Recall that $r(x)$ denotes the part of (3.2) contributed by primes ramified in $K/\mathbb{Q}$. Therefore,

$$r(x) \le |G| \sum_{\substack{N\mathfrak{p}^k < x \\ \mathfrak{p} \text{ ramified}}} \Lambda(\mathfrak{p}^k) \left(\frac{N\mathfrak{p}^k}{x} \right)^a \log \left(\frac{x}{N\mathfrak{p}^k} \right),$$

and we have the following bound.

Lemma 4.13. *If $n_K > 1$, then*

$$r(x) \le \frac{\log x}{ea \log 2} \log \Delta_E.$$

If $n_K = 1$, then $r(x) = 0$.

Proof. Since the ramified primes are exactly those dividing the different $\mathfrak{D}_{K/\mathbb{Q}}$ (see, e.g., [24, p. 62]), using (2.11), we have

$$\begin{aligned} r(x) &\le n_{E/K} \frac{\log x}{ea \log 2} \sum_{\substack{N\mathfrak{p} < x \\ \mathfrak{p} \text{ ramified}}} \log N\mathfrak{p} \le \frac{n_{E/K} \log x}{ea \log 2} \log N\mathfrak{D}_{K/\mathbb{Q}} \\ &= \frac{n_{E/K} \log x}{ea \log 2} \log \Delta_K \le \frac{\log x}{ea \log 2} \log \Delta_E. \quad \square \end{aligned}$$

5. Explicit bounds

In this final section, we give explicit versions of Theorem 3.1 and Corollary 3.4, and discuss the computer algorithms used in their derivation.

5.1. **An explicit version of the main result.**

Theorem 5.1 (ERH). *Let E/K be a Galois extension of number fields, with $E \neq \mathbb{Q}$. Let Δ denote the absolute value of E's discriminant. Let n denote the degree of E. Let $\sigma \in G$, the Galois group of E/K.*

Then there is a prime ideal $\mathfrak{p}$ of K with $\left(\frac{\mathfrak{p}}{E/K} \right) = \sigma$, of residue degree 1, satisfying

$$N\mathfrak{p} \le (4 \log \Delta + 2.5n + 5)^2.$$

The following tables provide more precise bounds. In each table, across the top are the ranges for n, and along the left side the ranges for $\log \Delta$. Each triple of the form (A, B, C) in the table corresponds to the bound $N\mathfrak{p} \le (A \log \Delta + Bn + C)^2$. (For smaller n, better bounds may be possible using explicit computations.)

The three tables correspond directly to the three cases in Theorem 3.1: Table 1 gives the most general bounds. Table 2 gives bounds for the norm of a prime ideal with Artin symbol equivalent to σ. Better bounds are possible in this case since $p(x)$ is zero. Table 3 is valid only when $K = \mathbb{Q}$. Better bounds are possible in this case because $d(x)$ and $r(x)$ are zero. The dashes in the tables indicate combinations of Δ and n that are not possible, owing to Minkowski's Theorem.

TABLE 1. Bounds for $N\mathfrak{p}$, $\deg \mathfrak{p} = 1$, $\left(\frac{\mathfrak{p}}{E/K}\right) = \sigma$

	$n = \deg(E/\mathbb{Q})$					
$\log \Delta_E$	2	3–4	5–9	10–14	15–49	50+
1–5	$(3.798, 2.59, 4.7)$	—	—	—	—	—
5–10	$(3.039, 2.12, 4.6)$	$(3.075, 1.98, 4.6)$	—	—	—	—
10–25	$(2.614, 1.97, 4.9)$	$(2.77, 1.9, 4.7)$	$(2.879, 1.81, 4.6)$	$(2.373, 1.67, 4.7)$	—	—
25–100	$(2.111, 1.86, 5.3)$	$(2.229, 1.8, 5.2)$	$(2.371, 1.74, 5)$	$(2.359, 1.7, 4.9)$	$(2.249, 1.6, 4.7)$	—
100–1000	$(1.574, 1.89, 6.3)$	$(1.641, 1.82, 6.1)$	$(1.725, 1.75, 5.9)$	$(1.742, 1.72, 5.8)$	$(1.796, 1.65, 5.6)$	$(1.743, 1.48, 4.9)$
1000–10000	$(1.163, 2.77, 9.8)$	$(1.183, 2.61, 9.4)$	$(1.21, 2.44, 8.9)$	$(1.219, 2.38, 8.7)$	$(1.239, 2.23, 8.3)$	$(1.336, 1.37, 5.2)$
10000–100000	$(1.042, 3.17, 17.9)$	$(1.047, 3.25, 17)$	$(1.054, 3.36, 16)$	$(1.057, 3.39, 15.6)$	$(1.062, 3.45, 15.1)$	$(1.196, 1.29, 5.3)$
100000+	$(1.011, 2.23, 45.7)$	$(1.013, 2.26, 42.9)$	$(1.014, 2.3, 39.6)$	$(1.015, 2.31, 38.5)$	$(1.016, 2.34, 36.6)$	$(1.019, 2.41, 32.9)$

TABLE 2. Bounds for $N\mathfrak{p}$, $\deg \mathfrak{p} = 1$, $\left(\frac{\mathfrak{p}}{E/K}\right)$ equivalent to σ

	$n = \deg(E/\mathbb{Q})$					
$\log \Delta_E$	2	3–4	5–9	10–14	15–49	50+
1–5	$(4.251, 0.58, 4.9)$	—	—	—	—	—
5–10	$(3.231, -0.02, 4.7)$	$(3.316, -0.1, 4.6)$	—	—	—	—
10–25	$(2.717, -0.15, 4.9)$	$(2.93, -0.18, 4.8)$	$(3.133, -0.21, 4.7)$	$(2.58, -0.28, 4.8)$	—	—
25–100	$(2.151, -0.23, 5.3)$	$(2.293, -0.25, 5.2)$	$(2.486, -0.27, 5)$	$(2.57, -0.27, 5)$	$(2.509, -0.29, 5)$	—
100–1000	$(1.582, -0.21, 6.3)$	$(1.653, -0.24, 6.1)$	$(1.749, -0.26, 5.9)$	$(1.787, -0.27, 5.8)$	$(1.884, -0.29, 5.6)$	$(2.192, -0.31, 5.3)$
1000–10000	$(1.164, 0.23, 9.8)$	$(1.184, 0.16, 9.4)$	$(1.211, 0.08, 8.9)$	$(1.222, 0.06, 8.7)$	$(1.243, 0, 8.4)$	$(1.331, -0.12, 7.5)$
10000–100000	$(1.042, 0.4, 17.9)$	$(1.047, 0.44, 17)$	$(1.054, 0.5, 15.9)$	$(1.057, 0.52, 15.6)$	$(1.062, 0.55, 15)$	$(1.096, 0, 8.5)$
100000+	$(1.011, -0.03, 41.2)$	$(1.012, 0, 37.4)$	$(1.014, 0.01, 36)$	$(1.014, 0.02, 35)$	$(1.016, 0.04, 33.4)$	$(1.019, 0.08, 30.2)$

TABLE 3. Bounds for p, $K = \mathbb{Q}$, $\left(\frac{p}{E/\mathbb{Q}}\right) = \sigma$

	$n = \deg(E/\mathbb{Q})$		
$\log \Delta_E$	2	3–4	5–9
1–5	$(3.29, 1.48, 4.9)$	—	—
5–10	$(2.662, 0.75, 4.8)$	$(2.808, 0.58, 4.7)$	—
10–25	$(2.301, 0.52, 5)$	$(2.524, 0.45, 4.9)$	$(2.736, 0.35, 4.7)$
25–100	$(1.881, 0.34, 5.5)$	$(2.035, 0.27, 5.3)$	$(2.231, 0.21, 5.1)$
100–1000	$(1.446, 0.23, 6.8)$	$(1.527, 0.17, 6.4)$	$(1.629, 0.11, 6.1)$
1000–10000	$(1.125, 0.63, 10.9)$	$(1.148, 0.5, 10.2)$	$(1.178, 0.37, 9.5)$
10000–100000	$(1.032, 0.44, 20.2)$	$(1.038, 0.5, 18.7)$	$(1.046, 0.56, 17.3)$
100000+	$(1.008, -0.06, 47.7)$	$(1.01, -0.03, 41.9)$	$(1.012, 0, 37.8)$

	$n = \deg(E/\mathbb{Q})$		
$\log \Delta_E$	10–14	15–49	50+
1–5	—	—	—
5–10	—	—	—
10–25	$(2.303, 0.19, 4.8)$	—	—
25–100	$(2.297, 0.19, 5)$	$(2.228, 0.1, 4.9)$	—
100–1000	$(1.667, 0.09, 6)$	$(1.745, 0.04, 5.8)$	$(1.755, 0, 5.7)$
1000–10000	$(1.189, 0.32, 9.2)$	$(1.212, 0.24, 8.8)$	$(1.257, 0, 7.3)$
10000–100000	$(1.049, 0.59, 16.8)$	$(1.054, 0.63, 16)$	$(1.095, 0, 8.2)$
100000+	$(1.012, 0, 37.8)$	$(1.014, 0.02, 35.9)$	$(1.017, 0.07, 31.8)$

5.2. **An explicit bound for primes in arithmetic progressions.** Next, we present our explicit bound for primes in arithmetic progressions. First, we observe that, for this case, a better bound for $i(x)$ is possible.

Lemma 5.2. *Let $K = \mathbb{Q}$ and $E = \mathbb{Q}(\omega)$, where ω is a primitive qth root of unity. Then*

$$i(x) \leq \frac{\log x}{ea \log 2} \log \Delta.$$

Proof. For each χ, we let $\hat{\chi}$ be a primitive character inducing χ, whose conductor is $\hat{q}$. Using (2.11), we have

$$|S(x, \chi) - S(x, \hat{\chi})| \leq \frac{1}{ea} \sum_{\substack{p^k < x \\ p \mid q}} \Lambda(p) \leq \frac{1}{ea} \sum_{p \mid q} \log p \left\lfloor \frac{\log x}{\log p} \right\rfloor \leq \frac{\omega(q) \log x}{ea}.$$

Noting $\omega(q) \leq \log_2 q$, $\Delta \leq q^{\varphi(q)}$, and summing over all $\varphi(q)$ characters χ completes the proof. □

Theorem 5.3 (ERH). *Let m and q be integers, with $\gcd(m, q) = 1$. There is a prime $p \equiv m \pmod{q}$ satisfying $p < 2(q \log q)^2$.*

Proof. First, assume $q \geq 1000$. Then by (3.41) from [30] we obtain that $n = \varphi(q) > 170$.

Let $E = \mathbb{Q}(\omega)$, where ω is a primitive qth root of unity. Then we have

$$\Delta = \frac{q^{\varphi(q)}}{\prod_{p \mid q} p^{\varphi(q)/(p-1)}},$$

from which we obtain that $\Delta \geq (q/2)^{\varphi(q)/2} \geq 22^{170}$.

We improved our program using the bound for $i(x)$ from the lemma above. Using the lower bounds for Δ and n given above, we obtain that $p \le (1.1 \log \Delta + 0.7n + 11)^2 \le (1.1q \log q + 0.7q + 11)^2$. Since q is at least 1000, this is at most $(1.3q \log q)^2 < 2(q \log q)^2$.

We wrote a second program to find the smallest prime $p \equiv m \pmod{q}$ for each pair m and q with $\gcd(m, q) = 1$ for all values of $q \le 1000$. From this, we have $p \le 1.56(q \log q)^2$, which completes the proof. □

5.3. **The program.** We conclude with a discussion of the methods used to derive the explicit bounds stated in Theorems 5.1 and 5.3.

The inputs to the program are an upper and lower limit for n, denoted as n_+ and n_-, an upper and lower limit for Δ, denoted as Δ_+ and Δ_-, and an indication of which case of which theorem applies for the bound sought.

The program was written in Turbo C++ on a CompuAdd 486/33MHz computer. All values were represented as 80-bit floating-point numbers (the `long double` data type in Turbo C++). Values of the digamma and trigamma functions were computed using methods from McCullagh [27].

In essence, the program consists of three layers; we elaborate below.

The bottom layer: applying the technical estimates. First, we wrote a set of functions to compute triples of the form (v_0, v_1, v_2) for bounding the absolute values of each of $p(x)$, $d(x)$, $i(x)$, $r(x)$, $I_{\le 0}$, $I_{1/2}$, A_1, and A_2. The bound is of the form $\le v_0 \log \Delta + v_1 n + v_2$, where each of the v_i is a function of x and a, and for $i(x)$, v_0 depends on n_+ as well. These functions take x, a, and an upper bound for n as input, and use the results of §4 to calculate their values. When more than one bound applies (equations (4.2) and (4.3) for $p(x)$, for example), the smaller of the two is returned.

As an example, suppose $x = 100$ and $a = 0.5$. Then the function for computing $I_{1/2}$ would return the triple

$$\left(\frac{\sqrt{x}}{2a+1}, \frac{\sqrt{x}(\psi(1+a) - \log 2\pi)}{2a+1}, \frac{2\sqrt{x}}{(a+1)(2a+1)} + \frac{2\sqrt{x}}{a(2a+1)} \right) \le (5, -9.01, 26.7).$$

Adding together the triples returned by these functions provides an upper bound on the absolute value of $I_1 = x/(1+a)^2$. Define

$$T(x, a) = (t_0, t_1, t_2) = \frac{(1+a)^2}{\sqrt{x}} \Sigma,$$

where Σ is the vector sum of the triples returned by the functions mentioned above. We have the inequality $\sqrt{x} \le T(x, a)$.

The middle layer: optimizing a. Given a value for x, an optimal value for a is found that minimizes the maximum bound for the ranges of n and Δ that were specified. The value that is minimized is

$$t_0 \log \Delta_+ + t_1 n_* + t_2 = (\log \Delta_+, n_*, 1) \cdot T(x, a),$$

where $n_* = n_+$ if t_1 is positive, $n_* = n_-$ if t_1 is negative, and the "$\cdot$" indicates dot-product. The optimal value for a is found using the Fibonacci unimodal minimization algorithm. Let $\mathrm{opt}(x)$ denote this optimal value for a, given x.

The top layer: finding x. Let $\mathrm{val}(x) = (\log \Delta_-, n_*, 1) \cdot T(x, \mathrm{opt}(x))$, where $n_* = n_-$ if $t_1 > 0$ and $n_* = n_+$ if $t_1 < 0$. Note that the $+$ and $-$ subscripts have been inverted (but $T(x,a)$ still uses n_+ when estimating $i(x)$). We explain the reason for this below.

Because the coefficients of $T(x, \mathrm{opt}(x))$ are decreasing functions of x, $\mathrm{val}(x)$ must also be decreasing. The correct value for x must satisfy $x \le (\mathrm{val}(x))^2$ for the bound to be valid. Since $\mathrm{val}(x)$ is decreasing, we wish to maximize x. When x is optimal, we have $x = (\mathrm{val}(x))^2$.

The choice for Δ and n in the definition of $\mathrm{val}(x)$ insure that other values for Δ and n from the ranges specified will only increase $\mathrm{val}(x)$, so the bound is still valid.

Once x is found, then $T(x, \mathrm{opt}(x)) = (t_0, t_1, t_2)$ provides a bound of the form

$$N\mathfrak{p} \le (t_0 \log \Delta + t_1 n + t_2)^2,$$

where Δ and n must come from the specified ranges.

In order to find x, we may assume $x \ge (\log \Delta_-)^2$ and $x \le \big(\mathrm{val}((\log \Delta_-)^2)\big)^2$. This provides an interval for search by bisection for the zero of the function $(\mathrm{val}(x))^2 - x$.

Additional remarks. We conclude with some additional remarks.

1. If no upper limit for Δ is specified, $1000n_+$ is used. Note that Δ_+ is used only in the middle layer, and so the only effect is that the leading coefficient is stressed when optimizing a.
2. If no upper limit for n is specified, Minkowski's Theorem is used to bound n in terms of $\log \Delta_+$ (see below).

   If Δ_+ was not given, Minkowski's Theorem is used with $\sqrt{x}$ instead, since we assume $x \ge (\log \Delta)^2$. This means that n_+ changes every time x does, and it affects the leading coefficient for the bound for $i(x)$. So if n is chosen to be larger, x can also be made larger, and the result is that $i(x)$'s leading coefficient will decrease. So the explicit bound derived this way is valid.
3. Finally, we note that in several instances, we rely on an explicit version of Minkowski's Theorem. This is obtained by noting that $0 < \sum 1/|\rho + a|^2$, where the sum is over ρ satisfying $\zeta_E(\rho) = 0$ and $\Re(\rho) = 1/2$. Then from Lemma 4.6 we have

   $$n_E < \frac{1}{\log 2\pi - \psi(1+a)}\left(\log \Delta_E + \frac{2}{a+1} + \frac{2}{a}\right),$$

   which can be minimized by optimizing a.

   (This technique is due to Stark and Odlyzko.)

References

1. M. Abramowitz and I. A. Stegun. *Handbook of Mathematical Functions.* Dover, 1970.
2. L. Adleman and H. W. Lenstra, Jr. Finding irreducible polynomials over finite fields. In *Proc. 18th Ann. ACM Symp. Theory of Computing*, pages 462–469, 1987.
3. N. C. Ankeny. An improvement of an inequality of Minkowski. *Proc. Nat. Acad. Sci. U.S.A.*, 37:711–716, 1951. MR **13:**538b
4. N. C. Ankeny. The least quadratic non residue. *Ann. Math.* 52:65–72, 1952. MR **13:**538c
5. E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55:355–380, 1990. MR **91m:**11096
6. E. Bach, M. Giesbrecht, and J. McInnes. The complexity of number-theoretic problems. Technical Report 247/91 (ITRC Lecture Series), Dept. of Computer Science, Univ. Toronto, 1991.

7. E. Bach and J. Shallit. Factoring with cyclotomic polynomials. *Math. Comp.*, 52:201–219, 1989. MR **89k:**11127
8. E. Bach and L. Huelsbergen. Statistical evidence for small generating sets. *Math. Comp.*, 61(203):69–82, 1993. MR **93k:**11089
9. R. P. Brent and H. T. Kung. The area-time complexity of binary multiplication. *J. ACM*, 28:521–534, 1981. [Erratum: ibid, 29:904, 1982.] MR **82i:**68027
10. S. Chowla. On the least prime in an arithmetical progression. *J. Indian Math. Soc.*, 2:1–3, 1934.
11. N. Costa Pereira. Estimates for the Chebyshev function $\psi(x)-\theta(x)$. *Math. Comp.*, 44:211–221, 1985. MR **86k:**11005
12. M. Deuring. Über den Tschebotareffschen Dichtigkeitssatz. *Math. Ann.*, 110:414–415, 1935.
13. P. G. Lejeune Dirichlet. Beweis eines Satzes über die arithmetische Progression. *Bericht Ak. Wiss. Berlin*, 108–110, 1837. Reprinted in *Werke*, 1:307–312.
14. P. G. Lejeune Dirichlet. Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhand. Ak. Wiss. Berlin*, 45–81, 1837–9. Reprinted in *Werke*, 1:313–342.
15. E. S. Golod and I. R. Shafarevich. On class field towers. *Izv. Akad. Nauk. SSSR*, 28:261-272, 1964. MR **28:**5056
16. H. Hasse. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper.* Third Edition, Physica-Verlag, Würzburg, 1970. MR **42:**1795
17. D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proc. London Math. Soc.*, 64:265-338, 1991. MR **93a:**11075
18. D. R. Heath-Brown. Almost-primes in arithmetic progressions and short intervals. *Mathematical Proceedings of the Cambridge Philosophical Society*, 83:357–375, 1978. MR **58:**10789
19. H. Heilbronn. Zeta-functions and L-functions. In *Algebraic Number Theory*, J. W. S. Cassels and A. Fröhlich, Eds. Academic Press, 1967. MR **36:**1414
20. D. Hilbert. Die Theorie der algebraischen Zahlkörper. *Jahresber. Deutsch. Math.-Verein.*, 4:175–546, 1897.
21. Ju. V. Linnik. On the least prime in an arithmetic progression, I. The basic theorem. *Mat. Sbornik*, 15:139-178, 1944. MR **6:**260b
22. J. Lagarias, H. Montgomery, and A. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54:271-296, 1979. MR **81b:**12013
23. J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic Number Fields*, pages 409–464, Academic Press, London, 1977. MR **56:**5506
24. S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1970. MR **44:**181
25. H. W. Lenstra Jr.. Miller's primality test. *Inform. Process. Letters*, 8(2):86–88, 1979. MR **80c:**10008
26. C. R. MacCluer. A reduction of the Čebotarev density theorem to the cyclic case. *Acta Arith.*, 15:45–47, 1968. MR **38:**2117
27. P. McCullagh. A rapidly convergent series for computing $\psi(z)$ and its derivatives. *Math. Comp.*, 36:247–248, 1981. MR **81m:**65028
28. A. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém Theor. Nombres Bordeaux*, 2:119-141, 1990. MR **91i:**11154
29. J. Oesterlé. Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann generalisée. *Soc. Math. France Astérisque*, 61:165–167, 1979.
30. J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Ill. J. Math.*, 6:64–94, 1962. MR **25:**1139
31. R. Rumely. Numerical computations concerning the ERH. *Math. Comp.*, 61(203):415–440, 1993. MR **94b:**11085
32. V. Shoup. Searching for primitive roots in finite fields. *Math. Comp.*, 58:369–380, 1992. MR **92e:**11140
33. N. Tchebotarev. Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.*, 95:191–228, 1926.
34. E. Titchmarsh. A divisor problem. *Rend. Circ. Mat. Palermo*, 54:414–429, 1930.

35. P. Turán. Über die Primzahlen der arithmetischen Progression. *Acta Sci. Math.*, 8:226–235, 1936/37.

36. S. S. Wagstaff, Jr. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.*, 33:1073–1080, 1979. MR **81e:**10038

37. Y. Wang, S.-K. Hsieh, and K.-J. Yu. Two results on the distribution of prime numbers. *Zhongguo Kexue Jishu Daxue Xuebao*, 1:32–38, 1965. In Chinese. MR **34:**7482

Computer Sciences Department, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: bach@cs.wisc.edu

Department of Mathematics and Computer Science, Butler University, Indianapolis, Indiana 46208
E-mail address: sorenson@butler.edu