MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 191
JULY 1990, PAGES 355–380

EXPLICIT BOUNDS FOR PRIMALITY TESTING AND RELATED PROBLEMS

ERIC BACH

ABSTRACT. Many number-theoretic algorithms rely on a result of Ankeny, which states that if the Extended Riemann Hypothesis (ERH) is true, any nontrivial multiplicative subgroup of the integers modulo m omits a number that is $O(\log^2 m)$. This has been generalized by Lagarias, Montgomery, and Odlyzko to give a similar bound for the least prime ideal that does not split completely in an abelian extension of number fields. This paper gives a different proof of this theorem, in which explicit constants are supplied. The bounds imply that if the ERH holds, a composite number m has a witness for its compositeness (in the sense of Miller or Solovay-Strassen) that is at most $2\log^2 m$.

1. INTRODUCTION

Many number-theoretic algorithms rely on the ability to quickly find a number outside a nontrivial subgroup of the multiplicative integers modulo m. In this context, one often appeals to a theorem of Ankeny [4]:

> Let G be a proper subgroup of the multiplicative group of integers modulo m. Then, assuming the Extended Riemann Hypothesis (ERH), the least positive integer outside G is $O(\log^2 m)$.

A generalization of this, due to Lagarias, Montgomery, and Odlyzko [24], replaces the rational numbers by any algebraic number field and states a similar bound for the least prime ideal outside a nontrivial subgroup of a "generalized class group":

> Let K be an algebraic number field whose discriminant has absolute value Δ, and let E be a nontrivial finite abelian extension of K, of conductor $\mathfrak{f}$. Then, assuming the ERH, the least prime ideal of K that does not split completely in the extension E/K has norm that is $O(\log^2(\Delta^2 N\mathfrak{f}))$.

The purpose of this paper is to supply explicit constants in the above theorems. In the author's dissertation [5], an explicit constant of "2" for Ankeny's

Received March 8, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y11; Secondary 11A15, 11M26, 11N25, 11R29, 11R44.
Key words and phrases. Primality, Extended Riemann Hypothesis.
This research was sponsored by the National Science Foundation, via grants DCR-8504485 and DCR-8552596.

theorem was proved. No constant for the second theorem has heretofore been published; we show below that "3" suffices. In addition, we show that both theorems hold with a coefficient of $1+o(1)$, and tabulate bounds that are close to the asymptotic value. Finally, we give bounds which are useful in situations where one wishes the small primes to satisfy other conditions; these extra requirements are explained in the two paragraphs below.

The first extra requirement arises because bounds on prime ideals are often used to derive bounds on ordinary prime numbers with specified properties. The idea is to choose E/K in such a way that a degree-1 prime ideal $\mathfrak{p}$ of K that does not split completely in the extension lies above a prime number p with the desired property. A bound on the norm of $\mathfrak{p}$ immediately implies a bound on p (see [6] for an example of this technique).

The second extra requirement is that the prime ideal should be unramified in E/K; in the case of Ankeny's theorem, this means that one seeks a number outside G and prime to m. Often this requirement is unnecessarily stringent; for instance, in testing m for primality, one would be happy to find a nontrivial divisor of it. Nevertheless, completeness demands that this case be treated; this fills in a lacuna in [5] in which no bound was given for the least *unit* outside a nontrivial subgroup of a multiplicative group of integers.

Before proceeding with the analysis, it will be useful to discuss the role of ERH-based results in the design and analysis of algorithms. The ERH encapsulates certain intuitions about the observed behavior of number-theoretic functions, and this fact alone gives it value as a heuristic principle. Though it has never been proved, it has been subjected to intense computational scrutiny, and no counterexample has ever been found [7, 13, 14, 23, 28, 33, 41, 42, 47]. A result based on this hypothesis can therefore be thought of as progress toward the ultimate goal of an unconditional result.

Among such algorithmic results that employ the ERH one may cite polynomial-time primality tests [30, 45], efficient algorithms for factoring polynomials over finite fields [2, 20, 38], methods for integer factoring [27, 39, 40], and an "almost" polynomial-time primality test [3, 11].

Lifting a term from the argot of computation theory, most of these algorithms are of "Las Vegas" type: any answer produced by them is correct, and the correctness does not depend on the ERH. However, the polynomial-time primality tests referred to above are different: they search for "witnesses" to a number's compositeness up to the bound given by Ankeny's theorem, and declare the number prime if none are found. To implement such algorithms, or even to compare them to other methods, explicit constants are essential.

Even assuming the ERH, it is an open question if the estimates given here are of the right order of magnitude. From the available numerical evidence, the least quadratic nonresidue modulo p appears to grow no more quickly than a small constant times $\log^2 p$ [26]. The scant evidence on prime testing [35] suggests a bound of perhaps $O(\log n)$ for the least witness to the compositeness of n. Graham and Ringrose [18] have shown that the least quadratic nonresidue

modulo a prime p is infinitely often $\Omega(\log p \log\log\log p)$, and Montgomery [31] gave a bound of $\Omega(\log p \log\log p)$ assuming the ERH. However, in our present ignorance about the vertical distribution of the roots of zeta and L functions, choosing among these growth rates seems impossible, even with the ERH.

The remainder of the paper is organized as follows. Motivation for the proof is given in §2, and then §3 is devoted to summarizing the definitions and results from algebraic number theory that will be needed later. The asymptotic result (Theorem 1) is proved in §4, assuming some messy details that are proved in §5. Because relatively more is known about the zeta functions involved, explicit constants for the rational case are presented in §6 (Theorems 2 and 3), with §7 treating the case of degree 2 and higher (Theorem 4).

2. Motivation

This section is intended as a guide to the more technical arguments that follow; details will be glossed over or even skipped altogether. For the moment we discuss the rational case only, following [5].

The proofs in this paper derive ultimately from a proof of the prime number theorem. Perhaps the most natural variant of this theorem says that about one in $\log n$ numbers near n is prime; this gives a heuristic for estimating sums over primes:

$$\sum_{p<x} f(p) \sim \sum_{n<x} \frac{f(n)}{\log n}.$$

Let $\Lambda(n)$ equal $\log p$ if n is a power of a prime p, and 0 otherwise. Then the above result says that whenever Λ appears in a sum, it should be disregarded; for example

$$g(x) = \sum_{n<x} \left(1 - \frac{n}{x}\right) \Lambda(n) \sim \sum_{n<x} \left(1 - \frac{n}{x}\right) \sim \frac{x}{2}.$$

How might one try to prove such an assertion? The basic idea in analytic number theory is to use transforms to decompose such sums into a main term (e.g., $x/2$) and other terms that grow less rapidly. In the above case, it can be shown that

$$g(x) = \frac{-1}{2\pi i} \int_{2-i\infty}^{2+i\infty} x^s \left\{ \frac{1}{s(s+1)} \cdot \frac{\zeta'}{\zeta}(s) \right\} ds,$$

where ζ denotes the Riemann zeta function.

One can therefore think of the transform

$$G(s) = \frac{1}{s(s+1)} \cdot \frac{\zeta'}{\zeta}(s)$$

as another representation of the original function g. Just as in the analysis of physical systems, the behavior of g is governed by the location of the poles of G.

Formally at least, one can evaluate the inverse transform by residues and find

$$g(x) = \frac{x}{2} - \sum_{\rho} \frac{x^{\rho}}{\rho(\rho+1)} + \cdots ,$$

where the sum is over zeros of the zeta function with $0 < \operatorname{Re}\rho < 1$ and "$\cdots$" indicates terms of smaller order that are of no concern here.

The pole of ζ at $s = 1$ contributes the main term, and the Riemann hypothesis implies good estimates on the second term. More precisely, if each root ρ is of the form $1/2 + i\omega$, then the latter sum has the form

$$-\sum_{\rho} \frac{\sqrt{x} e^{i\omega \log x}}{\rho(\rho+1)} ,$$

and each oscillatory term in this sum grows much less rapidly than the main term $x/2$. It would follow from the Riemann hypothesis and the estimate $\sum |\rho|^{-2} < \infty$ that

$$\sum_{n<x} \left(1 - \frac{n}{x}\right) \Lambda(n) = \frac{x}{2} + O(\sqrt{x}) .$$

Montgomery [31] used this idea to give a proof of Ankeny's theorem. Let χ be a character on $\mathbb{Z}/(m)^*$, and suppose that $\chi(n) = 1$ for all $n < x$. Then

$$\sum_{n<x} \left(1 - \frac{n}{x}\right) \Lambda(n) = \sum_{n<x} \left(1 - \frac{n}{x}\right) \Lambda(n)\chi(n) ,$$

and one can also consider the right-hand side as a transform:

$$\sum_{n<x} \left(1 - \frac{n}{x}\right) \Lambda(n)\chi(n) = \frac{-1}{2\pi i} \int_{2-i\infty}^{2+i\infty} x^s \left\{ \frac{1}{s(s+1)} \cdot \frac{L'}{L}(s) \right\} ds .$$

Here L denotes a function similar to the zeta function but lacking a pole or zero at 1. The expression is thus "all error term":

$$\sum_{n<x} \left(1 - \frac{n}{x}\right) \Lambda(n)\chi(n) = -\sum_{\rho} \frac{x^{\rho}}{\rho(\rho+1)} + \cdots .$$

If L satisfies the Riemann hypothesis, then combining the above results gives

$$\frac{x}{2} \le \sqrt{x} \sum_{\rho} \left| \frac{1}{\rho(\rho+1)} \right| + \cdots .$$

One now needs to estimate the sum over the roots of L; at this point we only offer an explanation, not an argument. In some sense, the roots of L have a "density" proportional to $\log m$, and since the corresponding sum for ζ is finite, one might expect that the above sum is $O(\log m)$. This is indeed true, and so for some $A > 0$, $\sqrt{x} \le 2A \log m + \cdots$ which implies that $x \le 4A^2 (\log m)^2$ asymptotically.

The basic trick in getting good numerical estimates is to derive a version of the above inequality with a *parameter* in it. (This idea appears in [16, p. 19-13].)

This is done by replacing the rational function $1/(s^2+s)$ in the transform by $(s+a)^2$, and using a formula due to Stark [44] to explicitly calculate $\sum|\rho+a|^{-2}$. Finding the best value of a involves a tradeoff; small a's give a good asymptotic constant (which is good for large m), but large a's make the error terms small (which is good for small m). To get the best results, a has to be chosen appropriately for the m of interest.

This section has discussed the rational case only, but the same ideas apply to the general case. Here sums over primes are replaced by sums over prime ideals, but the entire apparatus of zeta and L functions can be generalized, including Stark's formula. However, since less is known about these functions, the resulting bounds are correspondingly less sharp.

3. Notation and background

This section summarizes the notation and facts assumed in the remainder of the paper. The viewpoint is quite general, but the concepts easily specialize to the rational case (see the remarks at the end of the section). References for this material include [8, 17, 19, 25].

In this paper $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the integers, rational numbers, real numbers, and complex numbers, respectively. An inequality such as $x \le y$ for complex numbers indicates that the corresponding relation holds between real parts.

Throughout, K will denote an algebraic number field of degree n, with r_1 embeddings into $\mathbb{R}$ and $2r_2$ into $\mathbb{C}$ (thus $n = r_1 + 2r_2$). Let Δ denote the absolute value of K's discriminant; *Minkowski's theorem* (see [25, p. 121]) states that $n = O(\log \Delta)$.

Let O denote the ring of integers of K. If $\mathfrak{A}$ is an ideal of O, then $N\mathfrak{A}$ denotes the size of the quotient ring $O/\mathfrak{A}$. (In this paper, ideals are assumed to be nonzero, so that $N\mathfrak{A} < \infty$.) An ideal of O can be uniquely decomposed into a product of prime ideals, and two ideals $\mathfrak{A}$ and $\mathfrak{B}$ are called *relatively prime* — this is written $(\mathfrak{A}, \mathfrak{B}) = 1$ — if the prime factors of $\mathfrak{A}$ are distinct from the prime factors of $\mathfrak{B}$. If $\mathfrak{p}$ is a prime ideal, then for some (ordinary) prime number p, $N\mathfrak{p} = p^f$; the exponent f is called the *degree* of $\mathfrak{p}$.

A character χ is a function on the ideals of O that arises in the following fashion. Let $K \subset E$ be a finite field extension with an abelian Galois group. For a prime ideal $\mathfrak{p}$ unramified in this extension, let

$$\left(\frac{\mathfrak{p}}{E/K}\right) \in \mathrm{Gal}(E/K) = G$$

denote the Artin symbol of $\mathfrak{p}$. Let ϕ be a homomorphism from G into the complex roots of unity. This induces a function on prime ideals given by

$$\chi(\mathfrak{p}) = \phi\left(\frac{\mathfrak{p}}{K/E}\right)$$

when $\mathfrak{p}$ is unramified, and 0 otherwise; χ is then extended by multiplicativity to be a function on all ideals.

If E' is a proper subfield of E, then a character χ' defined using E' might agree with χ whenever $\chi \neq 0$. χ is then said to be *induced* by χ'. If no such subfield exists, χ is called *primitive*. A character that takes only the values 0, 1 is called *principal*.

A number $t \in K$ is said to be *totally positive* if it is positive in all real embeddings (for example, 1 is totally positive). For any character χ, there is an ideal $\mathfrak{f}$ of O such that $\chi((t)) = 1$ for all totally positive t congruent to 1 modulo $\mathfrak{f}$. In this case χ is said to be *defined* modulo $\mathfrak{f}$; the ideal of least norm with respect to which χ is defined is called its *conductor*. For primitive characters with conductor $\mathfrak{f}$, let

$$A_\chi = \Delta \cdot N\mathfrak{f}. \tag{3.1}$$

Each character has an associated parameter β that measures its dependence on signs. It is defined using the following fact: there exist numbers $a_i \in \{0, 1\}$, $1 \leq i \leq r_1$, such that for any $t \equiv 1 \pmod{\mathfrak{f}}$, $\chi((t)) = \prod(\operatorname{sign} t_i)^{a_i}$. Then β denotes the number of 1's occurring in the list $a_1, \ldots, a_{r_1}$ and α denotes $r_1 - \beta$; note that $0 \leq \alpha, \beta \leq n$.

Let ψ denote the logarithmic derivative of the gamma function. ψ satisfies the recurrence relation

$$\psi(z) = \psi(z+1) - 1/z \tag{3.2}$$

as well as the duplication formula

$$\psi(z/2) + \psi((z+1)/2) = 2(\psi(z) - \log 2). \tag{3.3}$$

Over the range $(0, \infty)$, the function ψ has derivatives of all orders that alternate in sign. Thus, ψ is increasing, ψ' decreasing, and so on. For future reference, differentiating (3.2) gives

$$\psi'(z) = \psi'(z+1) + 1/z^2. \tag{3.4}$$

The *Hecke L-function* associated with a character χ is

$$L(s, \chi) = \sum_{\mathfrak{A}} \frac{\chi(\mathfrak{A})}{N\mathfrak{A}^s}. \tag{3.5}$$

A special case is when χ is the trivial character (always 1); this gives the *Dedekind ζ function* of K:

$$\zeta(s) = \sum_{\mathfrak{A}} \frac{1}{N\mathfrak{A}^s}. \tag{3.6}$$

Hecke L-functions are analytic in the whole plane, with the exception of a simple pole at $s = 1$ (which occurs if and only if χ is principal). The functions associated with primitive characters satisfy a functional equation due to Hecke [19, p. 35] which implies that they have infinitely many zeros in the strip $0 < \operatorname{Re}(s) < 1$ (ρ will denote such a zero), as well as zeros at certain nonnegative integers. The *Extended Riemann Hypothesis* asserts that all Hecke L-functions are zero-free in the half-plane $\operatorname{Re}(s) > 1/2$.

The logarithmic derivatives of these functions will be used later, and we summarize some of their properties below. First, for $\mathrm{Re}(s) > 1$, there are absolutely convergent representations

$$\frac{\zeta'}{\zeta}(s) = -\sum_{\mathfrak{A}} \frac{\Lambda(\mathfrak{A})}{N\mathfrak{A}^s} \tag{3.7}$$

and

$$\frac{L'}{L}(s) = -\sum_{\mathfrak{A}} \frac{\Lambda(\mathfrak{A})\chi(\mathfrak{A})}{N\mathfrak{A}^s}, \tag{3.8}$$

where $\Lambda(\mathfrak{A}) = \log N\mathfrak{p}$ if $\mathfrak{A}$ is a power of a prime ideal $\mathfrak{p}$ and 0 otherwise. For any s, if

$$\psi_\zeta(s) = \frac{r_1 + r_2}{2}\psi\left(\frac{s}{2}\right) + \frac{r_2}{2}\psi\left(\frac{s+1}{2}\right) - \frac{n\log\pi}{2} \tag{3.9}$$

and

$$\psi_L(s) = \frac{r_2 + \alpha}{2}\psi\left(\frac{s}{2}\right) + \frac{r_2 + \beta}{2}\psi\left(\frac{s+1}{2}\right) - \frac{n\log\pi}{2}, \tag{3.10}$$

then

$$\frac{\zeta'}{\zeta}(s) = B + \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log\Delta - \frac{1}{s} - \frac{1}{s-1} - \psi_\zeta(s) \tag{3.11}$$

and (for primitive nonprincipal characters χ)

$$\frac{L'}{L}(s) = B_\chi + \sum_{\rho}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log A_\chi - \psi_L(s) \tag{3.12}$$

[22, p. 433]. The precise values of the constants B and B_χ are unimportant: if the sum is taken in symmetric order, then $B + \sum \rho^{-1} = 0$, and similarly for B_χ. Several later arguments will rely on the convergence of $\sum |\rho|^{-2}$; for the Riemann zeta function the sum is known:

$$\sum \frac{1}{|\rho|^2} = \gamma + 2 - \log(4\pi) = 0.04619\ldots. \tag{3.13}$$

(Here and elsewhere, γ is Euler's constant, approximately $0.57721\ldots$.)

For future reference, information about the poles of the logarithmic derivatives is summarized below; here, L is associated with a primitive, nonprincipal character, and roots ρ in the critical strip are to be counted with appropriate multiplicities.

Place	Residue of $\frac{\zeta'}{\zeta}$	Residue of $\frac{L'}{L}$	Residue of $\frac{\zeta'}{\zeta} - \frac{L'}{L}$
1	-1	0	-1
ρ (of ζ)	1	0	1
ρ (of L)	0	1	-1
0	$r_1 + r_2 - 1$	$r_2 + \alpha$	$\beta - 1$
$-1, -3, -5, \ldots$	r_2	$r_2 + \beta$	$-\beta$
$-2, -4, -6, \ldots$	$r_1 + r_2$	$r_2 + \alpha$	β

One may also interpret characters as discrete characters of the idele class group of K; as this group is constructed arithmetically from K, one may thus avoid reference to the extension E. The definition of this group is complicated and will not be given here (but see [8, p. 204 ff]). In special cases, however, characters may be defined using simpler groups associated with K; as these cases are important in the construction of algorithms, we review them below.

(1) If $K = \mathbb{Q}$, then $\Delta = r_1 = 1$ and $r_2 = 0$. A character χ on $\mathbb{Z}/(m)^*$ induces a character in the sense of this paper, by taking its value on (t), $t > 0$, to be $\chi(t)$. In this case, the conductor of χ is a divisor of m, ζ is the Riemann zeta function, and L is the Dirichlet L-function associated with χ. Also, β is the parity of χ; it is 0 if $\chi(-1) = 1$ and 1 if $\chi(-1) = -1$. See [12] for more discussion of this case.

(2) If K's ring of integers does not have unique factorization, then it has a nontrivial class group. This is a finite abelian group, and a character on this group induces a character in the sense of this section, for which $\mathfrak{f} = 1$. The parameter β's possible values are controlled by the possible signs of units in K. The case of quadratic fields is especially important. If $K = \mathbb{Q}(\sqrt{d})$ for a squarefree integer d, then Δ is at most $4|d|$. For imaginary quadratic fields $(d < 0)$, $r_1 = 0$ and $r_2 = 1$, so that $\beta = 0$. For real quadratic fields $(d > 0)$, $r_1 = 2$ and $r_2 = 0$, and $\beta = 0$ unless the fundamental unit of K has negative norm, in which case $0 \le \beta \le 2$. See [9] for more discussion of quadratic fields.

4. An asymptotic bound

In this section we prove an asymptotic bound for the least character nonresidue, assuming some details from §5. The first four lemmas prove an explicit formula on which all the theorems of this paper are based.

Lemma 4.1. *For $0 < a < 1$ and $y > 0$,*

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{y^s}{(s+a)^2}\,ds = \begin{cases} y^{-a}\cdot \log y & (y > 1), \\ 0 & (0 < y \le 1). \end{cases}$$

Proof. This is a residue calculation, and can be modeled on the proof of Theorem B in [21, p. 31]. □

Lemma 4.2. *For $0 < a < 1$, and any character χ (possibly the principal one),*

$$\frac{-1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\cdot\frac{L'}{L}(s)\,ds = \sum_{N\mathfrak{A}<x} \Lambda(\mathfrak{A})\chi(\mathfrak{A})\left(\frac{N\mathfrak{A}}{x}\right)^a \log\left(\frac{x}{N\mathfrak{A}}\right).$$

Proof. Expand L'/L by (3.8), then interchange summation and integration (this is justified because the integral is absolutely convergent). Then apply Lemma 4.1. □

Lemma 4.3. *Let χ be a character and let S be any set of ideals such that $\chi(\mathfrak{A}) = 1$ for all ideals $\mathfrak{A}$ outside S with $N\mathfrak{A} < x$. Then, if $0 < a < 1$,*

$$\frac{-1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(s)\,ds = \sum_{\substack{N\mathfrak{A}<x \\ \mathfrak{A}\in S}} \Lambda(\mathfrak{A})[1-\chi(\mathfrak{A}]\left(\frac{N\mathfrak{A}}{x}\right)^a \log\left(\frac{x}{N\mathfrak{A}}\right).$$

Proof. Subtract two instances of Lemma 4.2. □

Lemma 4.4. *Let χ be a nonprincipal primitive character, and let S be a set of ideals such that $\chi(\mathfrak{A}) = 1$ for all ideals $\mathfrak{A}$ outside S with $N\mathfrak{A} < x$. Then, if $0 < a < 1$,*

$$\frac{x}{(a+1)^2} = \sum_{\rho} \pm \frac{x^\rho}{(\rho+a)^2} + I_0 + I_- + \sum_{\substack{N\mathfrak{A}<x \\ \mathfrak{A}\in S}} \Lambda(\mathfrak{A})[1-\chi(\mathfrak{A})]\left(\frac{N\mathfrak{A}}{x}\right)^a \log\left(\frac{x}{N\mathfrak{A}}\right),$$

where in the first sum a '+' sign is taken for each root of $\zeta(s)$ and a '−' sign for each root of $L(s, \chi)$, and

$$I_0 = (\beta-1)\frac{1}{a^2} + \frac{\log x}{x^a}\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(-a) + \frac{1}{x^a}\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)'(-a) - \beta\frac{1}{x(a-1)^2},$$

$$I_- = \beta\sum_{k=2}^{\infty} \frac{(-1)^k}{(a-k)^2 x^k}.$$

Proof. Formally, this results from evaluating the integral in Lemma 4.3 by residues, using the table at the end of §3. It can be justified similarly to the proof of Theorem 28 in [21], using estimates for L'/L given in (5.6), (6.2) and (6.3) of [22]. □

The equality in Lemma 4.4 implies that x cannot be too large, as its left-hand side is proportional to x, whereas its right-hand side is $O(\sqrt{x})$ if the ERH is true. To derive actual bounds on x, it is necessary to estimate the terms on the right-hand side. Section 5, assuming the ERH, provides the following bounds, in which the implied constants in "O" terms can depend on a, but not on n

or χ:

$$(1)\quad \sum \frac{1}{|\rho + a|^2} \le \frac{1}{2a+1}[\log(\Delta^2 N\mathfrak{f}) + 2n(\psi(a+1) - \log(2\pi)) + O(1)],$$

$$(2)\quad I_0 = O(n) + O(\log x)\sum \frac{1}{|\rho + a|^2},$$

$$(3)\quad I_- = O(n),$$

$$(4)\quad \sum_{\substack{N\mathfrak{A}<x \\ (\mathfrak{A},\mathfrak{f})\neq 1}} \Lambda(\mathfrak{A})[1 - \chi(\mathfrak{A})](N\mathfrak{A}/x)^a \log(x/N\mathfrak{A}) = O(\log x \cdot \log N\mathfrak{f}),$$

$$(5)\quad \sum_{\substack{N\mathfrak{p}^k<x \\ \deg \mathfrak{p}>1}} \Lambda(\mathfrak{p}^k)[1 - \chi(\mathfrak{p}^k)](N\mathfrak{p}^k/x)^a \log(x/N\mathfrak{p}^k) \le 4n(\sqrt{x} + O(x^{1/4})).$$

(These are proved in Lemmas 5.6, 5.4, 5.1, 5.7, and 5.8, respectively.)

Theorem 1 (ERH). *For $i = 1, 2, \ldots$ let K_i be a number field whose discriminant has absolute value Δ_i, with a nonprincipal character χ_i defined modulo $\mathfrak{f}_i$. Let $\mathfrak{p}_i$ be a prime ideal of minimal norm such that $\chi_i(\mathfrak{p}_i) \neq 0, 1$ and $\deg \mathfrak{p}_i = 1$. Assume that $\Delta_i N\mathfrak{f}_i \to \infty$ as $i \to \infty$. Then*

$$N\mathfrak{p}_i \le (1 + o(1))\log^2(\Delta_i^2 N\mathfrak{f}_i).$$

Proof. Let $\varepsilon > 0$. We will show that as $\Delta N\mathfrak{f} \to \infty$ (dropping the subscripts),

$$N\mathfrak{p} \le (1 + \varepsilon)\log^2(\Delta^2 N\mathfrak{f})(1 + o(1)).$$

Choose a in the range $0 < a < 1$ such that

$$\frac{(1+a)^4}{(2a+1)^2} < 1 + \varepsilon \quad \text{and} \quad \frac{\psi(a+1) - \log(2\pi)}{2a+1} \le -2$$

(this is possible because $\psi(1) = -\gamma = -0.57721\ldots$). Consider the set of ideals $\mathfrak{A}$ for which either $\chi(\mathfrak{A}) \in \{0, 1\}$ or $\mathfrak{A}$ has a prime ideal factor of residue degree greater than 1. This set is multiplicatively closed, so any least-norm ideal $\mathfrak{p}$ outside the set will be prime. Let $x = N\mathfrak{p}$, $S = \{\mathfrak{p}^k : \deg \mathfrak{p} > 1$ or $(\mathfrak{p}, \mathfrak{f}) \neq 1\}$, and apply Lemma 4.4, using the primitive character induced by χ. This character is defined modulo some divisor of $\mathfrak{f}$ whose norm does not exceed $N\mathfrak{f}$. By (2)–(5) above and ERH,

$$\frac{x}{(a+1)^2} \le (\sqrt{x} + O(\log x))\left(\sum \frac{1}{|\rho + a|^2} + 4n\right) + O(n) + O(\log x \log N\mathfrak{f}) + O(nx^{1/4}).$$

By (1) and the second requirement on a,

$$\sum_\rho \frac{1}{|\rho + a|^2} + 4n \le \frac{1}{2a+1}(\log(\Delta^2 N\mathfrak{f}) + O(1)).$$

Also, $n = O(\log\Delta)$ (by Minkowski's theorem), so that

$$\frac{x}{(a+1)^2} \le \frac{1}{2a+1}(\log(\Delta^2 N\mathfrak{f}) + O(1))(\sqrt{x} + O(x^{1/4}))\,.$$

Divide by $\sqrt{x}$ to get

$$\frac{\sqrt{x}}{(a+1)^2} \le \frac{1}{2a+1}\log(\Delta^2 N\mathfrak{f})(1 + O(1/\log(\Delta^2 N\mathfrak{f})))(1 + O(x^{-1/4}))\,.$$

If $x \le \log^2(\Delta^2 N\mathfrak{f})$, there is nothing to prove, otherwise

$$\sqrt{x} \le \frac{(a+1)^2}{2a+1}\log(\Delta^2 N\mathfrak{f})(1 + o(1))\,,$$

which gives the desired bound. □

Before giving the detailed proofs of (1)–(5) above, we should mention some analytic issues connected with the above theorem. First, the full ERH is not necessary for the bound to be polynomial in $\log(\Delta N\mathfrak{f})$. It would suffice that the relevant functions be zero-free in a strip $\mathrm{Re}(s) > 1 - \varepsilon$ for some $\varepsilon > 0$, but even such a "weak Riemann hypothesis" is not known. Second, the presence of a so-called "Siegel zero" ρ of L with $1/2 < \rho < 1$ would improve the ultimate bound.

5. Detailed estimates

This section fills in the missing details in the proof of Theorem 1. The results will be used later, and so are done in explicit form.

Lemma 5.1. *Let I_- be defined as in Lemma* 4.4. *Then*

$$I_- \le \frac{\beta}{(a-2)^2 x^2} = O(n)\,.$$

Proof. It will suffice to show that for k, $x \ge 1$ and $0 < a < 1$,

$$\frac{1}{x^k(a-k)^2} \ge \frac{1}{x^{k+1}(a-(k+1))^2}\,,$$

which can be seen by noting that a is closer to k than to $k+1$. □

Lemma 5.2. *Let χ be a primitive character. Then the following representations are valid for all s (taking in the sums a '+' sign for a root of ζ and a '−' for a root of $L(s,\chi)$ in the critical strip):*

$$\left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(s) = \sum_\rho \pm\left(\frac{1}{s-\rho) - \frac{1}{(2-\rho)}\right) - \frac{1}{s} - \frac{1}{s-1}$$
$$- \frac{\beta}{2}\left[\psi\left(\frac{s}{2}\right) - \psi\left(\frac{s+1}{2}\right) - \psi(1) + \psi\left(\frac{3}{2}\right)\right]$$
$$+ \left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(2) + \frac{3}{2}$$

and

$$\left(\frac{\zeta'}{\zeta}-\frac{L'}{L}\right)'(s)=\sum_{\rho}\mp\frac{1}{(s-\rho)^2}+\frac{1}{s^2}+\frac{1}{(s-1)^2}-\frac{\beta}{4}\left[\psi'\left(\frac{s}{2}\right)-\psi'\left(\frac{s+1}{2}\right)\right].$$

Proof. To get the first equation, express $(\zeta'/\zeta)(s)-(\zeta'/\zeta)(2)$ using (3.11) and $(L'/L)(s)-(L'/L)(2)$ using (3.12), subtract the results and rearrange terms. To get the second, differentiate; the formal computation can be justified knowing that $\sum|\rho|^{-2}<\infty$. □

Lemma 5.3. *Let* $x\geq 1$ *and* $0<a<1$. *Then*

$$\frac{1}{a^2}-\frac{1}{a^2x^a}-\frac{\log x}{ax^a}\geq 0 \quad \textit{and} \quad \frac{1}{(a-1)^2}-\frac{1}{(a-1)^2x^{a-1}}+\frac{\log x}{x^{a-1}(1-a)}\geq 0.$$

Proof. The function $f(t)=x^t$ is convex, so

$$\frac{1}{a}\left(\frac{f(0)-f(-a)}{a}-f'(-a)\right)\geq 0.$$

Multiply this by $1/a$ and rearrange to get the first inequality. The second inequality is proved similarly by considering $f(0)$ and $f(1-a)$. □

Lemma 5.4 (ERH). *Let* I_0 *be defined as in Lemma* 4.4. *Then for* $0<a<1$ *and* $x\geq 1$,

$$I_0\leq \max\left\{0,\frac{\beta-1}{a^2}\right\}+\frac{\log x}{x^a}\left[\sum_{\rho}\frac{a+2}{|\rho+a|^2}+\frac{5}{2}\right]+\frac{1}{x^a}\left[\sum_{\rho}\frac{1}{|\rho+a|^2}+1\right].$$

Proof. First assume that $\beta=0$. Then, taking $s=-a$ in Lemma 5.2 and using the definition in Lemma 4.4 yields

$$I_0=-\left[\frac{1}{a^2}-\frac{\log x}{ax^a}-\frac{1}{a^2x^a}\right]+\frac{\log x}{x^a}\left[\sum{}^{+}\frac{1}{a+1}+\left(\frac{\zeta'}{\zeta}-\frac{L'}{L}\right)(2)+\frac{3}{2}\right]$$
$$+\frac{1}{x^a}\left[\sum{}'^{+}\frac{1}{(a+1)^2}\right],$$

where

$$\sum=\sum_{\rho}\pm\left(\frac{1}{-a-\rho}-\frac{1}{2-\rho}\right),\qquad \sum'=\sum_{\rho}\mp\frac{1}{(\rho+a)^2}.$$

If the ERH holds, then

$$\left|\sum\right|\leq\sum_{\rho}\left|\frac{1}{(\rho+a)}+\frac{1}{2-\rho}\right|\leq\sum_{\rho}\frac{2+a}{|(\rho+a)(\rho-2)|}\leq\sum_{\rho}\frac{2+a}{|\rho+a|^2},$$

and the result follows in this case by estimating $\sum'$ in a similar fashion and using (3.7) and (3.8) to show $(\zeta'/\zeta-L'/L)(2)<0$.

Now assume that $\beta \geq 1$. Using Lemmas 4.4 and 5.2 and using (3.2) and (3.4) to rewrite $\psi((1-a)/2)$ and $\psi'((1-a)/2)$ produces

$$I_0 = \frac{\beta-1}{a^2} + \frac{\log x}{x^a}\left[\sum{}' + \frac{1}{a} + \frac{1}{a+1} - \frac{\beta}{2}\left\{\psi\left(-\frac{a}{2}\right) - \psi\left(\frac{3-a}{2}\right) - \psi(1) + \psi\left(\frac{3}{2}\right)\right\} + \left(\frac{\zeta'}{\zeta} - \frac{L'}{L}\right)(2) + \frac{3}{2}\right]$$
$$+ \frac{1}{x^a}\left[\sum{}' + \frac{1}{a^2} + \frac{1}{(a+1)^2} - \frac{\beta}{4}\left\{\psi'\left(-\frac{a}{2}\right) - \psi'\left(\frac{3-a}{2}\right)\right\}\right]$$
$$- \frac{\beta}{x}\left[\frac{1}{(a-1)^2} - \frac{\log x}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2 x^{a-1}}\right].$$

Only the middle two terms must be estimated (the first occurs in the lemma, and the last is negative by Lemma 5.3). To estimate the second term, apply (3.2) twice to $\psi(-a/2)$ and use the monotonicity of ψ to see that $\psi(-a/2) - \psi((3-a)/2) - \psi(1) + \psi(3/2)$ is nonnegative. Then replace β by 1 and cancel the pole at $a = 0$ to get an upper bound for this term of

$$\frac{\log x}{x^a}\left[\sum{}' + \frac{1}{a+1} - \frac{1}{2}\left\{\psi\left(1-\frac{a}{2}\right) - \psi\left(\frac{3-a}{2}\right) - \psi(1) + \psi\left(\frac{3}{2}\right)\right\} + \frac{3}{2}\right].$$

The function $1/(a+1) - \frac{1}{2}\{\psi(1-a/2) - \psi((3-a)/2) - \psi(1) + \psi(3/2)\}$ is convex when $0 \leq a \leq 1$, so it is maximized at the endpoints and therefore is at most 1. To estimate the third term, apply (3.4) to $\psi'(-a/2)$ and then use the monotonicity of ψ'. □

Lemma 5.5. *Let* $a > 0$, $\sigma = a + 1$ *and* $\rho = 1/2 + i\omega$. *Then*

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

Proof. This is an algebraic identity. □

Lemma 5.6 (ERH). *If* χ *is primitive, then*

$$\sum_\rho \frac{1}{|\rho + a|^2} = \frac{1}{2a+1}\left[\log\frac{\Delta A_\chi}{\pi^{2n}} + 2\left(\frac{1}{a+1} + \frac{1}{a}\right) + (n+\alpha)\psi\left(\frac{a+1}{2}\right) + (n-\alpha)\psi\left(\frac{a+2}{2}\right) + 2\frac{\zeta'}{\zeta}(1+a) + 2\,\mathrm{Re}\,\frac{L'}{L}(1+a)\right]$$
$$\leq \frac{1}{2a+1}\left[\log(\Delta A_\chi) + 2n(\psi(a+1) - \log(2\pi)) + 2\left(\frac{1}{a} + \frac{1}{a+1}\right)\right],$$

where the sum is over the roots of ζ *and* L *(with multiplicities).*

Proof. Let $\sigma > 0$; substitute $s = \sigma$ in (3.11) and (3.12) and add the results to their conjugates to get Stark's formula

$$\sum_{\rho} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}} \right)$$
$$= \log(\Delta A_\chi) + 2\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1} \right) + 2(\psi_\zeta(\sigma) + \psi_L(\sigma)) + 2\frac{\zeta'}{\zeta}(\sigma) + 2\,\mathrm{Re}\,\frac{L'}{L}(\sigma)$$

[44]. Use (3.9) and (3.10) to express $\psi_\zeta + \psi_L$; then substitute $\sigma = a + 1$ in the above formula and use Lemma 5.5 to get the first equality. The upper bound uses the duplication formula (3.3), monotonicity of ψ, and the estimate $(\zeta'/\zeta)(1+a) + \mathrm{Re}(L'/L)(1+a) < 0$ (a consequence of (3.8)). □

The above estimate and results derived from it are the most critical ones in the paper. In particular, any sharper estimate than $(\zeta'/\zeta)(1+a)+\mathrm{Re}(L'/L)(1+a) < 0$ is useful; this can be provided in the rational case, as explained in the next section.

Lemma 5.7. *Let* $\omega(\mathfrak{f})$ *denote the number of distinct prime ideals dividing* $\mathfrak{f}$. *For* $0 < a < 1$,

$$\sum_{\substack{N\mathfrak{A} < x \\ (\mathfrak{A}, \mathfrak{f}) \neq 1}} \Lambda(\mathfrak{A})[1 - \chi(\mathfrak{A})] \left(\frac{N\mathfrak{A}}{x} \right)^a \log\left(\frac{x}{N\mathfrak{A}} \right) \leq \frac{2\log x}{ea}\omega(\mathfrak{f}) \leq \frac{2\log x \log N\mathfrak{f}}{ea \log 2},$$

where $e = 2.718281\ldots$ *is the base of the natural logarithm.*

Proof. When $1 \leq t < \infty$, the function $t^{-a}\log t$ is maximized when $\log t = 1/a$, so it is bounded above by $1/ea$. Therefore, the sum is at most

$$\frac{2}{ea} \sum_{\substack{N\mathfrak{A} < x \\ (\mathfrak{A}, \mathfrak{f}) \neq 1}} \Lambda(\mathfrak{A}) = \frac{2}{ea} \sum_{\mathfrak{p} | \mathfrak{f}} \log N\mathfrak{p} \left\lfloor \frac{\log x}{\log N\mathfrak{p}} \right\rfloor \leq \frac{2\log x}{ea} \sum_{\mathfrak{p} | \mathfrak{f}} 1;$$

this proves the first inequality. The second is true because every prime ideal has norm at least 2. □

Lemma 5.8 (RH). *We have*

$$\sum_{\substack{N\mathfrak{p}^k < x \\ \deg \mathfrak{p} > 1}} \Lambda(\mathfrak{p}^k)[1 - \chi(\mathfrak{p}^k)] \left(\frac{N\mathfrak{p}^k}{x} \right)^a \log\left(\frac{x}{N\mathfrak{p}^k} \right) \leq 4n(\sqrt{x} + O(x^{1/4})),$$

where the constant implied by the " O *" symbol is absolute.*

Proof. Since $0 < a < 1$, the sum is at most

$$2 \sum_{\substack{N\mathfrak{p}^k < x \\ \deg \mathfrak{p} > 1}} \Lambda(\mathfrak{p}^k) \log\left(\frac{x}{N\mathfrak{p}^k} \right).$$

Consider the contribution to the above sum from the prime ideals lying above a fixed rational prime p, and for some fixed value of k. This is

$$2 \sum_{\substack{\mathfrak{p}|p \\ \deg \mathfrak{p}>1}} \Lambda(\mathfrak{p}^k) \log\left(\frac{x}{N\mathfrak{p}^k}\right) = 2 \sum_{\substack{\mathfrak{p}|p \\ \deg \mathfrak{p}>1}} f_{\mathfrak{p}} \log p \log\left(\frac{x}{N\mathfrak{p}^k}\right)$$

$$\leq 2 \sum_{\substack{\mathfrak{p}|p \\ \deg \mathfrak{p}>1}} f_{\mathfrak{p}} \log p \log\left(\frac{x}{p^{2k}}\right)$$

$$\leq 2n\Lambda(p^k) \log\left(\frac{x}{p^{2k}}\right)$$

(here $f_{\mathfrak{p}}$ denotes the residue degree of $\mathfrak{p}$). Hence, the whole sum is at most

$$2n \sum_{m<\sqrt{x}} \Lambda(m) \log\left(\frac{x}{m^2}\right) = 4n \sum_{m<\sqrt{x}} \Lambda(m) \log\left(\frac{\sqrt{x}}{m}\right).$$

Since the Riemann zeta function has no pole at 0, we can take $a = 0$ in Lemma 4.2, integrate by residues and get the explicit formula

$$\sum_{m<t} \Lambda(m) \log\left(\frac{t}{m}\right) = t + \sum_{\rho} \frac{t^{\rho}}{\rho^2} + O(1).$$

The result follows from (3.13). □

Lemma 5.9. *We have*

$$\sum_{\substack{N\mathfrak{p}^k<x \\ \deg \mathfrak{p}>1}} \Lambda(\mathfrak{p}^k)[1 - \chi(\mathfrak{p}^k)] \left(\frac{N\mathfrak{p}^k}{x}\right)^a \log\left(\frac{x}{N\mathfrak{p}^k}\right) \leq \frac{2n}{ea} \sum_{m<\sqrt{x}} \Lambda(m).$$

Proof. Similar to that of Lemma 5.8. □

6. Explicit bounds for the rational case

This section gives explicit versions of Theorem 1 when K is the field of rational numbers. This is worth treating separately because much more is known about the Riemann zeta function than for zeta functions of general number fields, and the results are correspondingly sharper. The case where K has degree greater than 1 is left to §7.

By the Kronecker-Weber theorem, any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension whose Galois group is isomorphic to a multiplicative group of integers. One may also identify characters (in the sense of this paper) with ordinary Dirichlet characters, which are essentially homomorphisms from such groups into the complex roots of unity.

Therefore, this section deals with Dirichlet characters exclusively. In this section, $K = \mathbb{Q}$, so $n = \Delta = 1$, $r_1 = 1$, and $r_2 = 0$. χ is a nonprincipal character on $\mathbb{Z}(m)^*$, $m > 2$, whose parity is β (0 if $\chi(-1) = 1$, 1 otherwise).

Thus, $\alpha = 1 - \beta$. ζ and L denote the Riemann zeta function and Dirichlet L-function of χ, respectively; they are defined by (3.7) and (3.8), where sums over ideals are replaced by sums over positive integers.

The general plan of this section is the following. The explicit estimates of §5 combined with the proof of Theorem 1 produce inequalities (Lemmas 6.1 and 6.2) that the least "good" positive integer n must satisfy. These inequalities lead to simple bounds (Theorems 2 and 3) that can be verified by hand, as well as more complicated machine-generated bounds that are tabulated in the appendix.

Lemma 6.1. *Let χ be a nonprincipal character on $\mathbb{Z}/(m)^*$ with $\chi(n) = 1$ for all positive $n < x$. Then, if $0 < a < 1$,*

$$\frac{\sqrt{x}}{(a+1)^2} \le \frac{1}{2a+1}(1 + r(x))[\log m + t(x)] + s(x),$$

where

$$r(x) = \frac{(a+2)\log x + 1}{x^{a+1/2}}, \qquad s(x) = \frac{\frac{5}{2}\log x + 1}{x^{a+1/2}} + \frac{\beta}{(a-2)^2 x^{5/2}},$$

and

$$t(x) = -\log \pi + \psi\left(\frac{a+\beta+1}{2}\right) + (2a+1)(\gamma + 2 - \log(4\pi)) + 2\frac{\zeta'}{\zeta}(1+a) + 4\sum_{n \ge x} \frac{\Lambda(n)}{n^{1+a}}.$$

Proof. Take $S = \varnothing$ in Lemma 4.4, and use Lemmas 5.1 and 5.4 to estimate I_- and I_0 (note that $\beta \le 1$); this produces

$$\frac{\sqrt{x}}{(a+1)^2} \le \frac{1}{2a+1}(1 + r(x)) \sum \frac{1}{|\rho + a|^2} + s(x).$$

By Lemma 5.6,

$$\sum \frac{1}{|\rho + a|^2} \le \frac{1}{2a+1}\left[\log \frac{m}{\pi^2} + 2\left(\frac{1}{a} + \frac{1}{a+1}\right) + \psi\left(\frac{a+1}{2}\right) + \psi\left(\frac{a+\beta+1}{2}\right) + 2\frac{\zeta'}{\zeta}(1+a) + 2\,\mathrm{Re}\,\frac{L'}{L}(1+a)\right].$$

Put $s = 1 + a$ in (3.11), and use Lemma 5.5 and (3.12) to get

$$2\frac{\zeta'}{\zeta}(1+a) + \psi\left(\frac{a+1}{2}\right) - \log \pi + 2\left(\frac{1}{a} + \frac{1}{a+1}\right) \le (2a+1)\sum_{\rho \text{ of } \zeta} \frac{1}{|\rho + a|^2} \le (2a+1)(\gamma + 2 - \log(4\pi))$$

(note that the roots of ζ are symmetric about the real axis). Since $\chi(n) = 1$ for all $n < x$, (3.7) and (3.8) with $s = 1 + a$ imply

$$\frac{L'}{L}(1+a) \le \frac{\zeta'}{\zeta}(1+a) + 2\sum_{n \ge x} \frac{\Lambda(n)}{n^{1+a}}.$$

Combining the last three inequalities shows that the sum over the roots of ζ and L is at most $\log m + t(x)$, and the result follows. □

Lemma 6.2. *Let χ be a nonprincipal character on $\mathbb{Z}/(m)^*$ with $\chi(n) \in \{0, 1\}$ for all positive $n < x$. Then, if $0 < a < 1$,*

$$\frac{\sqrt{x}}{(a+1)^2} \le \frac{1}{2a+1}(1 + r(x))[\log m + t^*(x)] + s(x) + u(x)\omega(m),$$

where $s(x)$ and $r(x)$ are defined as in Lemma 6.1 and

$$t^*(x) = -\log \pi + \psi\left(\frac{a+\beta+1}{2}\right) + (2a+1)(\gamma + 2 - \log 4\pi) + 2\sum_{n \ge x} \frac{\Lambda(n)}{n^{1+a}},$$

$$u(x) = \frac{2\log x}{ea\sqrt{x}}.$$

Proof. This is like the proof of Lemma 6.1, with the following exceptions. In Lemma 4.4, $S = \{n\colon \gcd(m, n) \ne 1\}$, the first inequality of Lemma 5.7 is used to estimate the new term which results, and L'/L is estimated with

$$\frac{L'}{L}(1+a) \le \sum_{n \ge x} \frac{\Lambda(n)}{n^{1+a}}. \quad \square$$

To use these inequalities, it is helpful to have estimates for the prime number functions appearing therein.

Lemma 6.3. *Let $\mu(x) = \sum_{n \le x} \Lambda(n)$, and choose A, $B > 0$ so that $\mu(t) \le At$ (for all positive t), and $\mu(x) > x - B\sqrt{x}$. Then*

$$\sum_{n \ge x} \frac{\Lambda(n)}{n^{1+a}} \le \left(A\frac{(a+1)}{a} - 1 + \frac{B}{\sqrt{x}}\right)\frac{1}{x^a}.$$

Proof. The sum is $\int_{x^-}^{\infty} t^{-(1+a)}\, d\mu(t)$; apply Stieltjes integration by parts. □

For $x \le 10^8$, (3.35) and (4.5) of [37] give the explicit values $A = 1.03883$, $B = 2.05282$.

Lemma 6.4 (RH). *Let $\omega(m)$ denote the number of distinct prime factors of m. Then for $m \ge 210$,*

$$\omega(m) \le \overline{\omega}(m) = \mathrm{li}(\log m) + 0.12\sqrt{\log m},$$

where $\mathrm{li}(x)$ is the Cauchy principal value of $\int_0^x dt/\log t$. Moreover, for such m, $\overline{\omega}(m)/(\log m)$ is a decreasing function.

Proof. The first assertion is due to Robin [36], under the assumption of the Riemann hypothesis. To prove the second, note that there is a number $\hat{x}$, between 3 and 4, for which $\mathrm{li}(\hat{x})/\hat{x} = 1/\log \hat{x}$. For $x > \hat{x}$, $\mathrm{li}(x)/x$ is a decreasing function of x. This easily implies the second assertion. □

Theorem 2 (ERH). *Let G be a nontrivial subgroup of $\mathbb{Z}/(m)^*$ such that $n \in G$ for all positive $n < x$. Then $x < 2(\log m)^2$.*

Proof. Without loss of generality, G is maximal. There is then a nonprincipal character χ with $G \subset \mathrm{kernel}(\chi)$, and it will suffice to assume that $\chi(n) = 1$ for all $n < x$.

First assume $m \geq 1000$, and take $a = 1/2$ in Lemma 6.1. By Lemma 6.3, $0 \leq \log m + t(x) \leq \log m$ (appropriate values for ψ and ζ'/ζ can be found in [1, 46]). Thus,

$$\sqrt{x} \leq \frac{9}{8} \log m \left[1 + r(x) + \frac{2s(x)}{\log m}\right] \leq \frac{9}{8} \log m \left[1 + r(x) + \frac{2s(x)}{\log 1000}\right].$$

But the right side is less than $\sqrt{2} \log m$, which proves the bound.

Now let $m < 1000$. If $m < 3$, there are no nontrivial subgroups of $\mathbb{Z}/(m)^*$, so there is nothing to prove. If $m \geq 3$ is a prime, m has a primitive root less than $1.7(\log m)^2$ [48]. Finally, if m is composite, it must have a divisor that is at most $\sqrt{m}$, and $\sqrt{m} < 2(\log m)^2$ for $6 \leq m \leq 1000$, by a convexity argument. □

Theorem 3 (ERH). *Let G be a nontrivial subgroup of $\mathbb{Z}/(m)^*$ such that $n \in G$ for all positive $n < x$ relatively prime to m. Then $x < 3(\log m)^2$.*

Proof. We will show this holds for $m \geq m_0 = 10^6$; the other values of m can be checked by computation. By Lemmas 6.2 and 6.4,

$$\frac{\sqrt{x}}{(a+1)^2} \leq \left[\frac{1 + r(x)}{2a+1} + u(x)\frac{\overline{\omega}(m_0)}{\log m_0}\right] \log m + \left[s(x) + t^*(x)\frac{1 + r(x)}{2a+1}\right].$$

Let $a = 0.6$; for $x \geq 3 \log^2 m_0$, the second term on the right-hand side is negative and can be ignored. The first term gives a bound for $\sqrt{x}$ that is proportional to $\log m$, and direct substitution shows that the coefficient is less than $\sqrt{3}$. □

To verify Theorem 3 for all $m \leq 10^6$, the author wrote a program to find, for each such m, a set of small primes that generates $\mathbb{Z}/(m)^*$. Since m is relatively small, the task can be done by the following procedure. Factor m and compute $\phi(m)$, then express $\mathbb{Z}/(m)^*$ as a direct product of its p-Sylow subgroups for all $p | \phi(m)$. For each such p, use the characters of order p to find a generating set for the subgroup; then take the union of these generating sets.

Two consequences of Theorems 2 and 3 are notable. First, if the ERH is true, then a composite number m has a witness for its compositeness (in the

sense of [30 or 43]) that is at most $2\log^2 m$. Second, if the ERH is true, then $\mathbb{Z}/(m)^*$ is generated by the numbers less than $3\log^2 m$ that are relatively prime to m.

The process used to prove Theorems 2 and 3 can be automated. We will illustrate using Lemma 6.1, which implies bounds of the form $x \le (C_1 \log m + C_2)^2$, valid for all $m \ge m_0$, in the following way. First, the result of Lemma 6.1 is equivalent to

$$\sqrt{x} \le \frac{(a+1)^2}{2a+1}(1 + r(x))[\log m + t(x)] + (a+1)^2 s(x).$$

For the moment assume that m and a are fixed. Then any value of x greater than $\exp((a+1/2)^{-1})$ that makes the above inequality false is an upper bound on the least number outside G (this holds because for any $x' > x$, either $\log m + t(x') < 0$ — in which case x' is too large — or the right-hand side of the inequality is a decreasing function of x). The minimal such value x_0 can be found by binary search.

For any given value of m_0, choose a value of a that makes x_0 small. (The resulting function $x_0(a)$ seems to be convex, and a bisection-style minimization procedure works well in practice.) Once values of a and x_0 have been found, set

$$C_1 = \frac{(a+1)^2}{2a+1}(1 + r(x_0)), \qquad C_2 = (a+1)^2\left[t(x_0)\frac{1 + r(x_0)}{2a+1} + s(x_0)\right].$$

Then, whenever $m \ge m_0$, it must be true that $x \le (C_1 \log m + C_2)^2$. For, assume this is not the case (otherwise the job is done). Then by the definition of x, $\log m + t(x) > 0$, so

$$\begin{aligned}\sqrt{x} &\le \frac{(a+1)^2}{2a+1}(1 + r(x))[\log m + t(x)] + (a+1)^2 s(x) \\ &\le \frac{(a+1)^2}{2a+1}(1 + r(x_0))[\log m + t(x_0)] + (a+1)^2 s(x_0) \le C_1 \log m + C_2.\end{aligned}$$

Similarly, Lemma 6.2 gives bounds of the form $x \le (C_1^* \log m + C_2^*)^2$, where

$$C_1^* = (a+1)^2\left[\frac{1 + r(x_0)}{2a+1} + u(x_0)\frac{\overline{\omega}(m_0)}{\log m_0}\right]$$

and

$$C_2^* = (a+1)^2\left[t^*(x_0)\frac{1 + r(x_0)}{2a+1} + s(x_0)\right].$$

The author wrote programs to implement the above ideas, ψ and li were computed via published approximations [29, 10], and ζ and ζ' were computed by Euler-Maclaurin summation [15]. The results are summarized in Tables 1 and 2 of the appendix.

These computations, and the computations used to verify Theorem 3 for small m, showed that in Theorem 2, one can replace "2" by $2/\log^2 3 = 1.657071\ldots$, which is the best possible constant. Possibly this is also true of Theorem 3, but no attempt has been made to verify such a claim.

7. Explicit bounds for the algebraic case

The purpose of this section is to provide explicit versions of Theorem 1 for number fields besides the rationals. The computations are similar to those of §6.

In this section, K denotes a number field of degree $n \geq 2$ and absolute discriminant Δ (so $\Delta > 1$). Let χ be a nonprincipal character on the ideals of K that is defined modulo $\mathfrak{f}$. We will first prove an explicit degree bound in the spirit of [32].

Lemma 7.1. *Let* $\theta(a) = \log(2\pi) - \psi(a+1)$. *Then, for any* $a > 0$,

$$n \leq \frac{1}{\theta(a)}\left[\frac{\log(\Delta^2 N\mathfrak{f})}{2} + \left(\frac{1}{a+1} + \frac{1}{a}\right)\right].$$

Proof. Consider the primitive character induced by χ, and use the nonnegativity of the expression in Lemma 5.6. □

To get a concise analog to Lemmas 6.1 and 6.2, we introduce the following "options":

1. The sign parameter β is nonzero.
2. $\mathfrak{f} \neq 1$, and the prime ideal $\mathfrak{p}$ should be relatively prime to $\mathfrak{f}$.
3. The prime ideal $\mathfrak{p}$ should have residue degree 1.

With each choice of the above options associate an index set $I \subset \{1, 2, 3\}$, and define the exceptional set S_I accordingly. For instance, $I = S = \varnothing$ if $\beta = 0$ and a bound is needed for the smallest $\mathfrak{p}$ with $\chi(\mathfrak{p}) \neq 1$.

Lemma 7.2. *Let* I *be a set of options (in the above sense) and assume that* $\chi(\mathfrak{A}) = 1$ *for all ideals with* $N\mathfrak{A} < x$ *such that* $\mathfrak{A} \notin S_I$. *Then, if* $0 < a < 1$,

$$\frac{\sqrt{x}}{(a+1)^2} \leq \frac{1}{2a+1}(1 + r(x))[\log(\Delta^2 N\mathfrak{f}) + t(x)] + s_0(x) + \sum_{i \in I} s_i(x),$$

where $r(x)$ *is defined as in Lemma* 6.1, *and*

$$t(x) = 2n(\psi(a+1) - \log(2\pi)) + 2\left(\frac{1}{a+1} + \frac{1}{a}\right),$$

$$s_0(x) = \frac{\frac{5}{2}\log x + 1}{x^{a+1/2}}, \qquad s_1(x) = \frac{\beta - 1}{a^2\sqrt{x}} + \frac{\beta}{(a-2)^2 x^{5/2}},$$

$$s_2(x) = \frac{2\log x}{ea\log 2\sqrt{x}}\log N\mathfrak{f}, \qquad s_3(x) = \frac{2n}{ea\sqrt{x}}\sum_{m \leq \sqrt{x}} \Lambda(m).$$

Proof. Combine Lemmas 4.4, 5.1, 5.4, 5.6, 5.7, and 5.9 as in the proof of Theorem 1. □

To get estimates valid for a wide range of fields and characters, it seems reasonable to "normalize" the s_i's to be in terms of $\log(\Delta^2 N\mathfrak{f})$. First, Lemma 7.1 gives positive constants A and B such that

$$\beta \le n \le A\log(\Delta^2 N\mathfrak{f}) + B$$

(taking $a = 1$ provides $A = 0.36$, $B = 1.07$). Evidently, $\log N\mathfrak{f} \le \log(\Delta^2 N\mathfrak{f})$. Finally, the prime number theorem implies that there is a positive constant C for which

$$\sum_{m \le \sqrt{x}} \Lambda(m) \le C\sqrt{x}.$$

(Rosser and Schoenfeld [37] give $C = 1.03883$.) Combining the results cited in this paragraph gives estimates that are summarized in the following table.

Bounds of the form $s_i(x) \le \sigma_i(x)\log(\Delta^2 N\mathfrak{f}) + \tau_i$

i	Case	σ_i	τ_i	Remarks
0	always	0	$\frac{\frac{5}{2}\log x + 1}{x^{a+1/2}}$	
1	$\beta > 0$	$\frac{A}{a^2\sqrt{x}} + \frac{A}{(a-2)^2 x^{5/2}}$	$\frac{B-1}{a^2\sqrt{x}} + \frac{B}{(a-2)^2 x^{5/2}}$	$A = 0.36$, $B = 1.07$
2	$(\mathfrak{p}, \mathfrak{f}) = 1$	$\frac{2}{ea\log 2} \cdot \frac{\log x}{\sqrt{x}}$	0	
3	$\deg \mathfrak{p} = 1$	$\frac{2AC}{ea}$	$\frac{2BC}{ea}$	$C = 1.03883$

Analogs to Theorems 2 and 3 are given in the following theorem.

Theorem 4 (ERH). *Let K be a number field of degree greater than 1, and let Δ be the absolute value of the discriminant of K. Let χ be a nonprincipal character of the ideals of K that is defined modulo $\mathfrak{f}$. Then:*

$$\chi(\mathfrak{p}) \ne 1 \text{ occurs for } N\mathfrak{p} \le 3\log^2(\Delta^2 N\mathfrak{f}),$$

$$\chi(\mathfrak{p}) \ne 0, 1 \text{ occurs for } N\mathfrak{p} \le 12\log^2(\Delta^2 N\mathfrak{f}),$$

$$\chi(\mathfrak{p}) \ne 0, 1 \text{ and } \deg(\mathfrak{p}) = 1 \text{ occurs for } N\mathfrak{p} \le 18\log^2(\Delta^2 N\mathfrak{f}).$$

Proof. It is first necessary to find an absolute lower bound on $\Delta^2 N\mathfrak{f}$. Lemma 7.1 (with $a = 1$), together with the data on quadratic fields in [9], shows that $\Delta^2 N\mathfrak{f} \ge 27$, attained when $K = \mathbb{Q}(\sqrt{-3})$ and $N\mathfrak{f} = 3$ ($N\mathfrak{f} \ne 1, 2$ because this field has class number 1, and no prime ideal of norm 2). Now take $a = 1$ in

Lemma 7.2 and rewrite the results, using the above estimates for $s_i(x)$. Since $n \geq 2$, $t(x)/3 + \sum_{i=0}^{3} \tau_i(x)$ is (barely!) negative for $x \geq 3\log^2 27$. Therefore, x, the norm of the least appropriate prime ideal, satisfies

$$\sqrt{x} \leq 4\left[\frac{1 + r(x)}{3} + \sum_{i \in I} \sigma_i(x)\right] \log(\Delta^2 N\mathfrak{f}),$$

and the results follow from checking that each coefficient is less than the square root of the stated bound. □

It is interesting to compare these bounds with those given by Oesterlé [34], which estimate prime ideals $\mathfrak{p}$ with a particular value of $\chi(\mathfrak{p})$. Here, Theorem 4 only estimates $\mathfrak{p}$ for which $\chi(\mathfrak{p})$ is nontrivial in some sense. However, the two bounds are similar when χ has degree 2; in the present notation, Oesterlé gives $70\log^2(\Delta^2 N\mathfrak{f})$ as a bound for a $\mathfrak{p}$ of least norm with $\chi(\mathfrak{p}) \neq 0, 1$, whereas Theorem 4 gives a bound of $12\log^2(\Delta^2 N\mathfrak{f})$.

Theorem 4 implies also that the class group of a field of discriminant Δ is generated by the prime ideals of norm at most $12\log^2 \Delta$. In the quadratic case, this may be improved by working directly with Lemma 7.2 (take $n = 2$, $a = 0.7$, and use Minkowski's bound [25, p. 119] for small values of Δ), to show that the prime ideals of norm less than $6\log^2 \Delta$ generate the class group.

As explained in the previous section, one can find a good value of a, compute the least x_0 for which a bound holds, and use this to get explicit estimates of the form $x \leq (C_1 \log(\Delta^2 N\mathfrak{f}) + C_2)^2$. The relevant formulas are

$$C_1 = (a+1)^2\left[\frac{1 + r(x)}{2a+1} + \sum \sigma_i(x)\right]$$

and

$$C_2 = (a+1)^2\left[t(x)\frac{(1 + r(x))}{2a+1} + \sum \tau_i(x)\right].$$

Computed bounds based on these formulas are presented in Table 3 of the appendix.

Acknowledgments

I would like to again thank Andrew Odlyzko, who suggested that I use Stark's formula in my dissertation. The idea of using two constants in the tables was

suggested by a referee. I also thank the referees and other readers of the paper for many helpful comments.

APPENDIX

This appendix contains tabulated bounds that give improvements to Theorems 2, 3 and 4. Besides providing values of the constants C_1 and C_2, the tables show x_0 (rounded down) and the value of a at which this was attained.

TABLE 1

ERH $\Rightarrow$ *the least* $x \in \mathbb{Z}/(m) - G$ *is* $\leq (C_1 \log m + C_2)^2$ *for* $m \geq m_0$.

	$-1 \in G$				$-1 \notin G$			
m_0	x_0	C_1	C_2	a	x_0	C_1	C_2	a
10^3	31	1.415	−4.123	0.621	39	1.374	−3.192	0.617
10^4	57	1.336	−4.729	0.521	69	1.307	−3.719	0.523
10^5	92	1.284	−5.168	0.461	108	1.263	−4.109	0.467
10^6	137	1.248	−5.500	0.422	158	1.232	−4.422	0.426
10^8	259	1.200	−5.994	0.371	289	1.190	−4.889	0.375
10^{10}	423	1.170	−6.364	0.338	463	1.163	−5.243	0.342
10^{15}	1020	1.128	−7.011	0.289	1086	1.124	−5.865	0.293
10^{20}	1887	1.105	−7.453	0.262	1980	1.103	−6.304	0.264
10^{50}	12778	1.059	−8.847	0.193	13035	1.058	−7.662	0.195
10^{100}	52564	1.038	−9.846	0.156	53106	1.038	−8.641	0.156
10^{200}	212956	1.025	−10.733	0.127	214077	1.025	−9.504	0.127
10^{500}	1337754	1.015	−11.477	0.096	1340649	1.015	−10.217	0.096
10^{1000}	5350275	1.009	−11.307	0.076	5356178	1.009	−10.026	0.076

TABLE 2

ERH $\Rightarrow$ *the least* $x \in \mathbb{Z}/(m)^* - G$ *is* $\leq (C_1^* \log m + C_2^*)^2$ *for* $m \geq m_0$.

	$-1 \in G$				$-1 \notin G$			
m_0	x_0	C_1^*	C_2^*	a	x_0	C_1^*	C_2^*	a
10^3	158	2.133	−2.140	0.703	176	2.102	−1.240	0.717
10^4	246	1.942	−2.178	0.652	269	1.919	−1.260	0.662
10^5	347	1.811	−2.203	0.615	375	1.794	−1.272	0.623
10^6	461	1.716	−2.220	0.584	494	1.702	−1.279	0.592
10^8	726	1.585	−2.242	0.537	769	1.576	−1.285	0.545
10^{10}	1042	1.500	−2.256	0.504	1095	1.493	−1.283	0.508
10^{15}	2042	1.374	−2.268	0.443	2121	1.370	−1.271	0.447
10^{20}	3342	1.305	−2.267	0.404	3447	1.302	−1.249	0.406
10^{50}	17227	1.159	−2.171	0.297	17493	1.158	−1.087	0.297
10^{100}	62946	1.098	−1.939	0.232	63487	1.098	−0.829	0.234
10^{200}	237295	1.061	−1.474	0.182	238402	1.061	−0.345	0.184
10^{500}	1413413	1.033	−0.359	0.133	1416260	1.033	0.857	0.133
10^{1000}	5529565	1.021	1.238	0.104	5535372	1.021	2.486	0.104

TABLE 3

ERH $\Rightarrow$ *a suitable* $\mathfrak{p}$ *exists with* $N\mathfrak{p} \le (C_1 \log(\Delta^2 N\mathfrak{f}) + C_2)^2$ *for* $\Delta^2 N\mathfrak{f} \ge \Delta_0$.

$\chi(\mathfrak{p}) \ne 1$

	$\beta = 0$				$\beta = n$			
Δ_0	x_0	C_1	C_2	a	x_0	C_1	C_2	a
10^2	13	1.571	−3.570	0.998	21	1.776	−3.498	0.998
10^5	130	1.259	−3.077	0.727	169	1.416	−3.291	0.836
10^{10}	599	1.166	−2.350	0.541	712	1.280	−2.773	0.639
10^{20}	2475	1.110	−1.367	0.410	2800	1.194	−2.067	0.496
10^{50}	15145	1.065	0.439	0.289	16469	1.122	−0.797	0.361
10^{100}	58881	1.044	2.336	0.223	62751	1.086	0.471	0.287
10^{1000}	5483128	1.011	14.236	0.094	5627299	1.027	7.283	0.141

$\chi(\mathfrak{p}) \ne 0, 1$

	$\beta = 0$				$\beta = n$			
Δ_0	x_0	C_1	C_2	a	x_0	C_1	C_2	a
10^2	123	3.166	−3.468	0.932	133	3.268	−3.510	0.986
10^5	585	2.379	−3.189	0.775	616	2.441	−3.269	0.820
10^{10}	1811	1.974	−2.885	0.666	1888	2.017	−2.997	0.705
10^{20}	5625	1.682	−2.471	0.564	5820	1.714	−2.618	0.598
10^{50}	26169	1.420	−1.701	0.445	26876	1.441	−1.913	0.473
10^{100}	87338	1.287	−0.887	0.367	89266	1.303	−1.166	0.391
10^{1000}	6164175	1.076	4.206	0.182	6226716	1.082	3.384	0.197

$\chi(\mathfrak{p}) \ne 1$; degree $\mathfrak{p} = 1$

	$\beta = 0$				$\beta = n$			
Δ_0	x_0	C_1	C_2	a	x_0	C_1	C_2	a
10^2	119	2.421	−0.211	0.934	133	2.564	−0.256	0.988
10^5	740	2.357	0.083	0.789	782	2.430	−0.001	0.828
10^{10}	2933	2.339	0.293	0.721	3025	2.379	0.216	0.746
10^{20}	11639	2.333	0.442	0.682	11838	2.354	0.391	0.695
10^{50}	72314	2.331	0.560	0.654	72840	2.340	0.527	0.662
10^{100}	288614	2.331	0.606	0.645	289688	2.335	0.588	0.648
10^{1000}	28800718	2.330	0.643	0.637	28811673	2.331	0.643	0.637

$\chi(\mathfrak{p}) \ne 0, 1$; degree $\mathfrak{p} = 1$

	$\beta = 0$				$\beta = n$			
Δ_0	x_0	C_1	C_2	a	x_0	C_1	C_2	a
10^2	300	3.807	−0.209	0.934	311	3.885	−0.235	0.965
10^5	1359	3.203	−0.013	0.828	1393	3.247	−0.055	0.852
10^{10}	4452	2.891	0.150	0.766	4529	2.918	0.111	0.781
10^{20}	15280	2.678	0.308	0.717	15451	2.693	0.270	0.729
10^{50}	83457	2.505	0.458	0.678	83936	2.513	0.443	0.682
10^{100}	313974	2.431	0.534	0.660	314986	2.435	0.526	0.662
10^{1000}	29152988	2.345	0.634	0.639	29163843	2.345	0.634	0.639

BIBLIOGRAPHY

1. M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions*, Dover, New York, 1965.
2. L. Adleman, K. Manders, and G. Miller, *On taking roots in finite fields*, Proc. 18th IEEE Symposium on Foundations of Computer Science, 1977, pp. 175–177.
3. L. Adleman, C. Pomerance, and R. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), 173–206.
4. N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) **55** (1952), 65–72.
5. E. Bach, *Analytic methods in the analysis and design of number-theoretic algorithms*, MIT Press, Cambridge, Mass., 1985.
6. E. Bach and J. Shallit, *Factoring with cyclotomic polynomials*, Math. Comp. **52** (1989), 201–219.

7. R. P. Brent, *On the zeros of the Riemann zeta function in the critical strip*, Math. Comp. **33** (1979), 1361–1372.
8. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, London, 1986.
9. H. Cohn, *Advanced number theory*, Dover, New York, 1980.
10. W. J. Cody and H. C. Thacher, Jr., *Chebyshev approximations for the exponential integral* $\mathrm{Ei}(x)$, Math. Comp. **23** (1969), 289–303.
11. H. Cohen and H. W. Lenstra, Jr., *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), 287–330.
12. H. Davenport, *Multiplicative number theory*, Springer, Berlin, 1980.
13. D. Davies and C. B. Haselgrove, *The evaluation of Dirichlet L-functions*, Proc. Roy. Soc. London Ser. A **264** (1961), 122–132.
14. D. Davies, *An approximate functional equation for Dirichlet L-functions*, Proc. Roy. Soc. London Ser. A **284** (1965), 224–236.
15. H. M. Edwards, *Riemann's zeta function*, Academic Press, New York, 1974.
16. R. P. Feynman, R. B. Leighton, and M. Sands, *The Feynman lectures on physics*, vol. 2, Addison-Wesley, Reading, Mass., 1964.
17. L. J. Goldstein, *Analytic number theory*, Prentice-Hall, Englewood Cliffs, N. J., 1971.
18. S. Graham and R. J. Ringrose, *Lower bounds for least quadratic non-residues*, manuscript, 1988.
19. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, 3rd ed., Physica-Verlag, Würzburg-Wien, 1970.
20. M. A. Huang, *Riemann hypothesis and finding roots over finite fields*, Proc. 17th ACM Symposium on Theory of Computing, 1985, pp. 121–130.
21. A. E. Ingham, *The distribution of prime numbers*, Cambridge Univ. Press, Cambridge, 1932.
22. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in Algebraic Number Fields (A. Fröhlich, ed.), Academic Press, London, 1977.
23. ——, *On computing Artin L-functions in the critical strip*, Math. Comp. **33** (1979), 1081–1095.
24. J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296.
25. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1971.
26. D. H. Lehmer, E. Lehmer, and D. Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. **24** (1970), 433–451.
27. A. K. Lenstra, *Fast and rigorous factorization under the extended Riemann hypothesis*, Indag. Math. **50** (1988), 443–454.
28. J. van de Lune, H. J. J. te Riele, and D. T. Winter, *On the zeros of the Riemann zeta function in the critical strip.* IV, Math. Comp. **46** (1986), 667–681.
29. P. McCullagh, *A rapidly convergent series for computing* $\psi(z)$ *and its derivatives*, Math. Comp. **36** (1981), 247–248.
30. G. L. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13** (1976), 300–317.
31. H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Math., vol. 227, Springer, Berlin, 1971.
32. A. M. Odlyzko, *Lower bounds for discriminants of number fields*, Acta Arith. **29** (1976), 275–297.
33. ——, *On the distribution of spacings between zeros of the zeta function*, Math. Comp. **48** (1987), 273–308.
34. J. Oesterlé, *Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée*, Soc. Math. France Astérisque **61** (1979), 165–167.

35. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **25** (1980), 1003–1026.
36. G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le* k*-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de* n, Acta Arith. **42** (1983), 367–389.
37. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
38. L. Rónyai, *Factoring polynomials over finite fields*, J. Algorithms **9** (1988), 391–400.
39. C. P. Schnorr and H. W. Lenstra, Jr., *A Monte Carlo factoring algorithm with linear storage*, Math. Comp. **43** (1984), 289–311.
40. M. Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Math. Comp. **48** (1987), 757–780.
41. D. Shanks, *Systematic examination of Littlewood's bounds on* $L(1, \chi)$, Proc. Sympos. Pure Math., vol. 24, Amer. Math. Soc., Providence, R. I., 1973, pp. 294–311.
42. R. Spira, *Calculation of Dirichlet L-functions*, Math. Comp. **23** (1969), 489–497.
43. R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), 84–85.
44. H. M. Stark, *Effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152.
45. J. Vélu, *Tests for primality under the Riemann hypothesis*, SIGACT News **10** (1978), 58–59.
46. A. Walther, *Anschauliches zur Riemannschen Zetafunktion*, Acta Math. **48** (1926), 393–400.
47. P. J. Weinberger, *On small zeros of Dirichlet L-functions*, Math. Comp. **29** (1975), 319–328.
48. A. E. Western and J. C. P. Miller, *Tables of indices and primitive roots*, Royal Society, Cambridge, 1968.

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