MATHEMATICS OF COMPUTATION
Volume 84, Number 291, January 2015, Pages 357–369
S 0025-5718(2014)02843-3
Article electronically published on May 7, 2014

COMPUTING THE RESIDUE OF THE DEDEKIND ZETA FUNCTION

KARIM BELABAS AND EDUARDO FRIEDMAN

Abstract. Assuming the Generalized Riemann Hypothesis, Bach has shown that one can calculate the residue of the Dedekind zeta function of a number field K by a clever use of the splitting of primes $p < X$, with an error asymptotically bounded by $8.33 \log \Delta_K/(\sqrt{X} \log X)$, where Δ_K is the absolute value of the discriminant of K. Guided by Weil's explicit formula and still assuming GRH, we make a different use of the splitting of primes and thereby improve Bach's constant to 2.33. This results in substantial speeding of one part of Buchmann's class group algorithm.

1. Introduction

Given a number field K, Buchmann's algorithm [4] computes the ideal class group $\mathcal{C}\ell_K$ and units $U(K)$. It uses an index calculus strategy which requires a *factor base* $\mathcal{B}$ of prime ideals generating $\mathcal{C}\ell_K$, and a halting criterion based on a computed approximation $\widehat{hR}$ of the product of the class number h by the regulator R. Indeed, it produces elements in the kernel Λ of the natural surjective map $\mathbb{Z}^{\mathcal{B}} \twoheadrightarrow \mathcal{C}\ell_K$ by factoring principal ideals (α), then proceeds to find dependencies between those, yielding pairs α, α' generating the same principal ideals, *i.e.*, units α/α'. This gives a tentative class number $\hat{h}$ and a tentative regulator $\hat{R}$, both integral multiples of h and R, respectively. If we find $\hat{h}\hat{R} < 2hR$, then $h = \hat{h}$ and $R = \hat{R}$, thereby halting the algorithm.

Buchmann's algorithm requires two important inputs:

- a factorbase $\mathcal{B} = \mathcal{B}(K)$ so that $\mathbb{Z}^{\mathcal{B}} \twoheadrightarrow \mathcal{C}\ell_K$,
- an approximate value of $\log(hR)$, with a rigorous error term.[1]

Assuming a suitable Generalized Riemann Hypothesis (GRH), Bach [1, 2] showed how to choose a reasonably small $\mathcal{B}$ *and* found an approximation for $\log(hR)$ using averages of truncated Euler products. Schoof [10] had previously found a simpler approximation, but with a worse error bound.

This paper is a companion to [3], where we improved *numerically* on Bach's first result (factorbase choice) using the Poitou-Weil explicit formula [9]. Our main aim

Received by the editor June 18, 2012 and, in revised form, April 30, 2013.
2010 *Mathematics Subject Classification.* Primary 11R42, Secondary 11Y40.
Key words and phrases. Dedekind zeta function, Buchmann's algorithm.
The first author was supported by the ANR projects ALGOL (07-BLAN-0248) and PEACE (ANR-12-BS01-0010-01).
The second author was partially supported by the Chilean Programa Iniciativa Científica Milenio grant ICM P07-027-F and Fondecyt grant 1110277.

[1] It suffices to make the error less than $\frac{1}{2} \log 2$.

here is to improve on Bach's second result. Let

$$B_K(X) := \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}\mathfrak{p}^m<X}}^{K-\mathbb{Q}} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}}\Big(\frac{\sqrt{X}\log X}{\mathrm{N}\mathfrak{p}^{m/2}\log \mathrm{N}\mathfrak{p}^m}-1\Big),$$

$$f_K(X) := \frac{3\big(B_K(X)-B_K(X/9)\big)}{2\sqrt{X}\log(3X)},$$

where in the definition of B_K the sum is over all prime ideal powers $\mathfrak{p}^m$ with absolute norm $\mathrm{N}\mathfrak{p}^m < X$ and the notation $\sum^{K-k}$ means that the sum for k is subtracted from the corresponding sum for K.

Theorem 1. *Let K be a number field of degree $n>1$, let κ_K be the residue of the Dedekind zeta $\zeta_K(s)$ at $s=1$, and let Δ_K be the absolute value of the discriminant of K. Assume GRH, i.e., that $\zeta_K(s)\neq 0$ and $\zeta_{\mathbb{Q}}(s)\neq 0$ whenever $\mathrm{Re}(s)>\frac{1}{2}$. Then, for any real $X\geq 69$, the difference $|\log\kappa_K - f_K(X)|$ is bounded above by*

$$\frac{2.324\log\Delta_K}{\sqrt{X}\log(3X)}\left(\Big(1+\frac{3.88}{\log(X/9)}\Big)\Big(1+\frac{2}{\sqrt{\log\Delta_K}}\Big)^2+\frac{4.26(n-1)}{\sqrt{X}\log\Delta_K}\right).$$

Bach's original result [2, Lemma 4.7 and §7], also assuming GRH, is of the form

$$|\log\kappa_K - g_K(X)| \leq \frac{8.324\log\Delta_K}{\sqrt{X}\log(X/2)}\big(1+E(\Delta_K,X)\big),$$

where $g_K(X)$ is a function involving prime ideals of norm $\leq X$ (different from $f_K(X)$), and $E(\Delta,X)\to 0$.[2] Both Bach's and our results show that choosing $X = O(\log\Delta_K/\log\log\Delta_K)^2$ computes $\log(hR)$ with an error bounded by $\frac{1}{2}\log 2$. Our better error bounds translate to a shorter list of prime ideals, by an asymptotic factor of $(8.324/2.324)^2\approx 12.8$, and correspondingly faster computations for $\log\kappa_K$. In Section 5, we give tables comparing Schoof's, Bach's and our method for various ranges of Δ_K and $[K:\mathbb{Q}]$.

2. The explicit formula

Weil's explicit formula [12], as simplified by Poitou [9], is the identity

$$\begin{aligned}\sum_\rho \widehat{F}(\gamma_\rho) = &-2\sum_{\mathfrak{p},m}\frac{\log\mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}}F(m\log\mathrm{N}\mathfrak{p})+4\int_0^\infty F(x)\cosh(x/2)\,dx\\ &+F(0)\Big(\log\Delta_K - n_K C - n_K\log(8\pi) - r_K\frac{\pi}{2}\Big)\\ &+n_K\int_0^\infty\frac{F(0)-F(x)}{2\sinh(x/2)}\,dx + r_K\int_0^\infty\frac{F(0)-F(x)}{2\cosh(x/2)}\,dx.\end{aligned}\tag{1}$$

Here K is a number field of degree $n_K=[K:\mathbb{Q}]$, having exactly r_K real embeddings, and Δ_K is the absolute value of its discriminant. The auxiliary function $F\colon\mathbb{R}\to\mathbb{C}$ is assumed to be even, and such that for some $\varepsilon>0$, the function $F(x)e^{(\frac{1}{2}+\varepsilon)x}$ is of bounded variation and integrable over $[0,+\infty)$. Also

[2] Here $8.324\approx\sqrt{2}\cdot\frac{2}{3}\cdot\big(2^{3/2}+6\big)$ [2, p. 22]. In comparing our result with Bach's, one should bear in mind that Bach's x is our $X/2$, since X bounds the biggest rational prime whose splitting must be computed.

$\big(F(0) - F(x)\big)/x$ is assumed of bounded variation on $[0, +\infty)$ and F must be assigned the average value at any jump discontinuity. By C we mean Euler's constant $0.5772\cdots$.

The Fourier transform $\widehat{F}$ of F on the left-hand side of (1) is

$$\widehat{F}(\gamma) := \int_{-\infty}^{+\infty} F(t)e^{it\gamma}\,dt. \tag{2}$$

The sum of the $\widehat{F}(\gamma_\rho)$ runs over all nontrivial zeroes $\rho = \frac{1}{2} + i\gamma_\rho$ of the Dedekind zeta function $\zeta_K(s)$, with multiple zeroes repeated accordingly. The Riemann Hypothesis (GRH) for ζ_K states that $\gamma_\rho \in \mathbb{R}$. Given our assumptions on F, the sum over ρ converges when understood as

$$\lim_{R\to+\infty} \sum_{|\mathrm{Im}(\rho)|<R} \widehat{F}(\gamma_\rho).$$

In the sum on the right of (1), $\mathfrak{p}$ runs over all prime ideals of (the ring of algebraic integers of) K, m runs over all positive integers, and the absolute norm of $\mathfrak{p}$ is denoted by $\mathrm{N}\mathfrak{p}$.

If K and k are number fields, on subtracting Weil's formula for k from (1), we obtain the form we shall use most often:

$$\begin{aligned}\sum_{\rho}^{K-k} \widehat{F}(\gamma_\rho) = -2\sum_{\mathfrak{p},m}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} F(m\log N\mathfrak{p}) + F(0)L_{K/k} \\ + (n_K - n_k)\int_0^\infty \frac{F(0)-F(t)}{2\sinh(t/2)}\,dt + (r_K - r_k)\int_0^\infty \frac{F(0)-F(t)}{2\cosh(t/2)}\,dt,\end{aligned} \tag{3}$$

where

$$L_{K/k} := \log\left(\frac{\Delta_K}{\Delta_k}\right) - (n_K - n_k)\big(C + \log(8\pi)\big) - (r_K - r_k)\frac{\pi}{2}.$$

3. The auxiliary function

In this section we explain how our choice of auxiliary function $F = F_{s,X}$ is motivated by the form of the explicit formula and the need to avoid bounding conditionally convergent expressions.

If K and k are number fields, the obvious path to computing

$$\kappa_{K/k} := \lim_{s\to 1} \frac{\zeta_K}{\zeta_k}(s)$$

is via the Euler product $\zeta_K(s) = \prod_{\mathfrak{p}}(1 - \mathrm{N}\mathfrak{p}^{-s})^{-1}$, *i.e.*,

$$\log\frac{\zeta_K}{\zeta_k}(s) = -\sum_{\mathfrak{p}}^{K-k} \log(1 - \mathrm{N}\mathfrak{p}^{-s}) = \sum_{\mathfrak{p}}^{K-k}\sum_{m=1}^{\infty} \frac{\mathrm{N}\mathfrak{p}^{-ms}}{m} \quad (\mathrm{Re}(s) > 1). \tag{4}$$

A naïve attempt to approximate $\log\frac{\zeta_K}{\zeta_k}(s)$ by a partial sum would therefore be

$$\log\frac{\zeta_K}{\zeta_k}(s) - \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}\mathfrak{p}^m<X}}^{K-k} \frac{\mathrm{N}\mathfrak{p}^{-ms}}{m} = \sum_{\mathfrak{p},m}^{K-k} \log \mathrm{N}\mathfrak{p}\,\frac{H(\log \mathrm{N}\mathfrak{p}^m)}{\mathrm{N}\mathfrak{p}^{m/2}}, \tag{5}$$

where (for X not a prime power)

$$H(t) = H_{s,X}(t) := \begin{cases} g_s(t) & \text{if } |t| \geq \log X, \\ 0 & \text{otherwise,} \end{cases}$$

and where

$$g_s(t) := \frac{\exp(-h|t|)}{|t|}, \quad h := s - \frac{1}{2}. \tag{6}$$

The explicit formula (3) gives an expression for the right-hand side of (5). Its most interesting term is $\sum_\rho^{K-k} \widehat{H}(\gamma_\rho)$. While there is no simple closed expression for $\widehat{H}$, it is easy to write its leading term. After two integrations by parts using

$$g_s'(t) = -\Big(h + \frac{1}{t}\Big) g_s(t), \quad g_s''(t) = \Big(h^2 + \frac{2ht+2}{t^2}\Big) g_s(t), \tag{7}$$

and setting $T := \log X > 0$, we obtain

$$\begin{aligned} \widehat{H}(\gamma) = &- g_s(T) \left(\frac{2\gamma \sin(\gamma T)}{h^2+\gamma^2} - \frac{2\big(h + \frac{1}{T}\big)\cos(\gamma T)}{h^2+\gamma^2} \right) \\ &- \frac{4}{h^2+\gamma^2} \int_T^{+\infty} \cos(\gamma t) g_s(t) \frac{(ht+1)}{t^2}\, dt. \end{aligned} \tag{8}$$

Even assuming GRH, the first term is highly unwelcome since we cannot control

$$\sum_\rho^{K-k} \frac{2\gamma_\rho \sin(\gamma_\rho T)}{h^2+\gamma_\rho^2} \tag{9}$$

by its absolute value.[3] The simple identity

$$\frac{\gamma \sin(\gamma T)}{h^2+\gamma^2} = \frac{\sin(\gamma T)}{\gamma} - \frac{h^2}{(h^2+\gamma^2)} \frac{\sin(\gamma T)}{\gamma}, \tag{10}$$

shows that our troubles in (9) come from $\sum_\rho \frac{2\sin(\gamma_\rho T)}{\gamma_\rho}$. Fortunately, this is just the term that appears in the explicit formula when we use as auxiliary function the step function

$$\widetilde{H}(t) := \begin{cases} 1 & \text{if } |t| \leq T, \\ 0 & \text{otherwise.} \end{cases}$$

To cancel the bad term $\sin(\gamma T)/\gamma$ in (10) we must therefore choose the auxiliary function to be $H(t) + g_s(T)\widetilde{H}(t)$. Normalizing so that $F(0) = 1$ leads to our auxiliary function

$$F(t) = F_{s,X}(t) := \begin{cases} 1 & \text{if } |t| \leq \log X, \\ f_{s,X}(t) & \text{otherwise,} \end{cases} \tag{11}$$

where

$$f_{s,X}(t) := \frac{g_s(t)}{g_s(T)} = \frac{T}{|t|} e^{-h(|t|-T)} \quad \big(h := s - \tfrac{1}{2},\ T := \log X\big). \tag{12}$$

We shall see in the next section that this choice of F leads to a sum $\sum_\rho^{K-k} \widehat{F}(\gamma_\rho)$ which can be controlled well under GRH.

Using (8), we obtain:

[3]The rest of the terms are easily bounded under GRH, as we shall see in the next section.

Lemma 2. *For* $\mathrm{Re}(s) > \frac{1}{2}$ *and* $X > 1$, *let* $T := \log X$, *let* $F_{s,X}$ *be as in* (11) *and let* $\widehat{F}_{s,X}$ *be its Fourier transform* (2). *Then, for* $\gamma \in \mathbb{R}$ *and notation as in* (12), *we have*

$$\widehat{F}_{s,X}(\gamma) = \frac{2h^2 \sin(\gamma T)}{(h^2+\gamma^2)\gamma} + \frac{2\big(h+\frac{1}{T}\big)\cos(\gamma T)}{h^2+\gamma^2} - \frac{4}{(h^2+\gamma^2)} \int_T^{+\infty} \cos(\gamma t) f_{s,X}(t) \frac{(ht+1)}{t^2}\, dt.$$

4. Proof of Theorem 1

We now apply Lemma 2 to the explicit formula.

Lemma 3. *Let* K *and* k *be number fields such that the Riemann Hypothesis holds for* ζ_K *and* ζ_k. *Then, for* $\mathrm{Re}(s) > \frac{1}{2}$, $T := \log X > 0$, *and notation as in* (3), (6) *and* (12), *we have*

$$\begin{aligned} &\frac{1}{g_s(T)} \log \frac{\zeta_K}{\zeta_k}(s) - \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}\mathfrak{p}^m < X}}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} \big(f_{s,X}(m \log \mathrm{N}\mathfrak{p}) - 1\big) \\ &= -h^2 \sum_{\rho}^{K-k} \frac{\sin(\gamma_\rho T)}{(h^2+\gamma_\rho^2)\gamma_\rho} - \Big(h + \frac{1}{T}\Big) \sum_{\rho}^{K-k} \frac{\cos(\gamma_\rho T)}{h^2+\gamma_\rho^2} \\ &\quad + \sum_{\rho}^{K-k} \frac{2}{h^2+\gamma_\rho^2} \int_T^{+\infty} \frac{(ht+1)}{t^2} \cos(\gamma_\rho t) f_{s,X}(t)\, dt + \frac{1}{2} L_{K/k} \\ &\quad + \frac{n_K - n_k}{2} \int_T^{\infty} \frac{1 - f_{s,X}(t)}{2\sinh(t/2)}\, dt + \frac{r_K - r_k}{2} \int_T^{\infty} \frac{1 - f_{s,X}(t)}{2\cosh(t/2)}\, dt. \end{aligned} \tag{13}$$

The branch of $\log \frac{\zeta_K}{\zeta_k}(s)$ in (13) is real for real $s > 1$.

Proof. Assume first that $\mathrm{Re}(s) > 1$. Then the assumptions in the explicit formula (3) apply to $F_{s,X}$ in (11), so we find

$$\begin{aligned} 2 \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}\mathfrak{p}^m < X}}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} \big(1 - f_{s,X}(m \log \mathrm{N}\mathfrak{p})\big) + 2 \sum_{\mathfrak{p},m}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} f_{s,X}(m \log \mathrm{N}\mathfrak{p}) \\ + \sum_{\rho}^{K-k} \widehat{F}_{s,X}(\gamma_\rho) = L_{K/k} + (n_K - n_k) \int_T^{\infty} \frac{1 - f_{s,X}(t)}{2\sinh(t/2)}\, dt \\ + (r_K - r_k) \int_T^{\infty} \frac{1 - f_{s,X}(t)}{2\cosh(t/2)}\, dt. \end{aligned}$$

Note that (cf. (4)),

$$\begin{aligned} \sum_{\mathfrak{p},m}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} f_{s,X}(m \log \mathrm{N}\mathfrak{p}) &= \frac{1}{g_s(T)} \sum_{\mathfrak{p},m}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} g_s(m \log \mathrm{N}\mathfrak{p}) \\ &= \frac{1}{g_s(T)} \log \frac{\zeta_K}{\zeta_k}(s). \end{aligned}$$

The lemma for $\mathrm{Re}(s) > 1$ now follows from Lemma 2.

To obtain (13) for $\mathrm{Re}(s) > \frac{1}{2}$ by analytic continuation, note that GRH implies $\gamma_\rho^2 + h^2 \neq 0$ for $\mathrm{Re}(s) > \frac{1}{2}$, and that $\log \frac{\zeta_K}{\zeta_k}(s)$ is analytic in that half-plane. Hence we only need to estimate for $\mathrm{Re}(s) = \sigma > \frac{1}{2}$,

$$\int_T^{+\infty} \Big| \frac{(ht+1)}{t^2} \cos(\gamma_\rho t) f_{s,X}(t) \Big| \, dt \le \frac{|h|T+1}{T^3 g_\sigma(T)} \int_T^{+\infty} e^{-(\sigma-\frac{1}{2})t} \, dt$$
$$= \frac{|h|T+1}{T^2(\sigma-\frac{1}{2})}. \qquad \square$$

Lemma 3 nearly takes us to our goal since $g_s(T) = 1/(X^{s-\frac{1}{2}} \log X)$ for $T = \log X$. Indeed, multiplying (13) by $g_s(T)$ and letting $\sigma = \mathrm{Re}(s) > \frac{1}{2}$, we see that to obtain

$$\Big| \log \frac{\zeta_K}{\zeta_k}(s) - g_s(T) \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}\mathfrak{p}^m < X}}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} \big(f_{s,X}(m \log \mathrm{N}\mathfrak{p}) - 1 \big) \Big| < \frac{c \log \Delta_K}{X^{\sigma-\frac{1}{2}} \log X}$$

it would suffice to bound the right-hand side of (13) by $c \log \Delta_K$. It is well known (see Lemma 5) that

$$\sum_{\substack{\rho \\ \zeta_K(\rho)=0}} \frac{1}{h^2 + \gamma_\rho^2} = \mathcal{O}\big(\log \Delta_K \big).$$

Unfortunately, the terms $\sin(\gamma_\rho T)/\gamma_\rho$ in (13) impede our desired bound since we can only bound them by $T = \log X$, even under GRH. This leads to the loss of a factor of $\log X$.

To prevent this loss, our next step is to use Lemma 3 for T and $T-a$, with $a > 0$ to be selected presently.

Lemma 4. *Let K/k be an extension of number fields such that the Riemann Hypothesis holds for ζ_K and ζ_k. Then, for $0 < a < T$, we have*

$$\Big| \Big(\frac{1}{g(T)} - \frac{1}{g(T-a)} \Big) \log \kappa_{K/k} - A(T) + A(T-a) \Big|$$
$$\le (n_K - n_k) a e^{-(T-a)/2} \beta(T-a) + c_{a,T} \sum_{\rho}^{K+k} \frac{1}{\frac{1}{4} + \gamma_\rho^2}, \tag{14}$$

where the sum $\sum_\rho^{K+k}$ runs over the zeroes of ζ_K and over those of ζ_k (repeating any common zeroes),

$$g(t) := \frac{e^{-t/2}}{t}, \quad \kappa_{K/k} := \lim_{s \to 1} \log \frac{\zeta_K}{\zeta_k}(s), \tag{15}$$
$$A(t) := \sum_{\substack{\mathfrak{p},m \\ \mathrm{N}\mathfrak{p}^m < e^t}}^{K-k} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{m/2}} \left(\frac{g(m \log \mathrm{N}\mathfrak{p})}{g(t)} - 1 \right),$$

$$c_{a,T} := 1 + \frac{a}{4} + \frac{6}{T-a}, \quad \beta(t) := \frac{1}{2}\Big(\frac{1}{2} + \frac{1}{t}\Big) e^t \log \Big(\frac{e^t+1}{e^t-1} \Big). \tag{16}$$

Proof. The left-hand side of (14) is simply the absolute value of the difference at $s = 1$ of the expressions on the left-hand side of (13) for T and $T-a$. Thus, we need to estimate the difference of terms on the right-hand side of (13) for T and

$T-a$ at $s=1$. Since all sums in (13) are absolutely convergent, these estimations are straightforward, but we proceed with the details.

The mean value theorem gives $|\sin(\gamma T)-\sin(\gamma(T-a)|\le|\gamma a|$ for $\gamma\in\mathbb{R}$. As GRH means that $\gamma_\rho\in\mathbb{R}$, we have (using $s=1$, so $h=\frac12$),

$$\left|-h^2\sum_\rho^{K-k}\frac{\sin(\gamma_\rho T)}{(h^2+\gamma_\rho^2)\gamma_\rho}-(-h^2)\sum_\rho^{K-k}\frac{\sin\big(\gamma_\rho(T-a)\big)}{(h^2+\gamma_\rho^2)\gamma_\rho}\right|\le\frac{a}{4}\sum_\rho^{K+k}\frac{1}{\frac14+\gamma_\rho^2}.$$

The difference of terms involving $(h+\frac1T)\cos(\gamma_\rho T)$ on the right-hand side of (13) can be estimated trivially by $\frac12+\frac1T+\frac12+\frac{1}{T-a}<1+\frac{2}{T-a}$. As for the third term, using $g=g_1$ and $f_{1,X}(t)=\frac{Te^{T/2}}{te^{t/2}}$, we have

$$\left|2\int_T^{+\infty}\frac{(\frac{t}{2}+1)}{t^2}\cos(\gamma_\rho t)f_{1,X}(t)\,dt\right|\le\frac{2}{T}\int_T^{+\infty}\Big(\frac12+\frac1t\Big)\frac{Te^{T/2}}{te^{t/2}}\,dt=\frac{2}{T},$$

where we used (7) to evaluate the integral. Applying this with T replaced by $T-a$, we find that the difference of the first three sums on the right-hand side of (13) contribute at most c_a times the sums over the zeroes in (14).

We now consider the difference of the remaining terms on the right-hand side of (13), *i.e.*, those not involving the zeroes ρ. Note that $\frac12 L_{K/k}$ simply cancels. We can assume $k\ne K$, for otherwise the difference vanishes. To control the integrals, abbreviate

$$q(T):=\int_T^\infty\frac{1-f_{1,X}(t)}{2\sinh(t/2)}\,dt,\quad \widetilde{q}(T):=\int_T^\infty\frac{1-f_{1,X}(t)}{2\cosh(t/2)}\,dt.$$

Then we have

$$\begin{aligned}-q'(T)=\int_T^\infty\frac{(1+\frac{T}{2})e^{T/2}}{t(e^t-1)}\,dt&\le\Big(\frac12+\frac1T\Big)e^{T/2}\int_T^\infty\frac{dt}{e^t-1}\\&=-\Big(\frac12+\frac1T\Big)e^{T/2}\log\big(1-e^{-T}\big).\end{aligned}\tag{17}$$

Similarly, we have

$$|\widetilde{q}\,'(T)|\le\Big(\frac12+\frac1T\Big)e^{T/2}\log\big(1+e^{-T}\big).$$

Moreover, the sign of the derivative in (17) shows that q and $\widetilde{q}$ are decreasing functions.

Let s_K denote the number of complex places of K, so that $n_K=r_K+2s_K$. Using $k\subset K$ we have $|r_K-r_k|\le n_K-n_k$; indeed, both sides vanish if $k=K$, and

$$-n_K+n_k\le-n_k\le-r_k\le r_K-r_k=n_K-n_k-2(s_K-s_k)\le n_K-n_k,$$

otherwise (the leftmost inequality uses $n_K \geq 2n_k$). Hence

$$\begin{aligned}
&\left|\frac{n_K - n_k}{2}\big(q(T) - q(T-a)\big) + \frac{r_K - r_k}{2}\big(\widetilde{q}(T) - \widetilde{q}(T-a)\big)\right| \\
&\quad\leq \frac{n_K - n_k}{2}\big(q(T-a) - q(T)\big) + \frac{n_K - n_k}{2}\big(\widetilde{q}(T-a) - \widetilde{q}(T)\big) \\
&\quad= -\frac{(n_K - n_k)a}{2}\big(q'(U) + \widetilde{q}\,'(U)\big) \qquad \text{(for some } T-a \leq U \leq T\text{)} \\
&\quad\leq \frac{(n_K - n_k)a}{2}\Big(\frac{1}{2} + \frac{1}{U}\Big)e^{U/2}\big(\log(1+e^{-U}) - \log\big(1-e^{-U}\big)\big) \\
&\quad= (n_K - n_k)ae^{-U/2}\beta(U).
\end{aligned}$$

Since $\beta(U)$ is a decreasing function of $U > 0$, the result follows from $T - a \leq U$. □

Next we give the traditional estimate for the term $\sum_\rho \left(\frac{1}{4} + \gamma_\rho^2\right)^{-1}$ in Lemma 4.

Lemma 5 (Landau, Stark [11])**.** *Suppose $\sigma > 1$ and assume the Riemann hypothesis for ζ_K. Then*

$$\sum_{\substack{\rho \\ \zeta_K(\rho)=0}} \frac{1}{\frac{1}{4} + \gamma_\rho^2} \leq (2\sigma - 1)\left(\log \Delta_K + \frac{2}{\sigma - 1} - d_{K,\sigma}\right),$$

where, $\Psi(\sigma) := \Gamma'(\sigma)/\Gamma(\sigma)$, and

$$d_{K,\sigma} := -2\frac{\zeta_K'}{\zeta_K}(\sigma) + n_K\big(\log(2\pi) - \Psi(\sigma)\big) + r_K\frac{\Psi\big(\frac{\sigma+1}{2}\big) - \Psi\big(\frac{\sigma}{2}\big)}{2} - \frac{2}{\sigma}. \tag{18}$$

Proof. For $h := \sigma - \frac{1}{2} > \frac{1}{2}$ and $\gamma \in \mathbb{R}$, we have

$$\frac{1}{\frac{1}{4} + \gamma^2} = \frac{4h^2}{h^2 + (2h\gamma)^2} < \frac{4h^2}{h^2 + \gamma^2}.$$

Now, since $\sigma \in \mathbb{R}$ and the zeroes $\rho = \frac{1}{2} + i\gamma_\rho$ come in conjugate pairs,

$$\sum_\rho \frac{h}{h^2 + \gamma_\rho^2} = \sum_\rho \mathrm{Re}\Big(\frac{1}{\sigma - \rho}\Big) = \mathrm{Re}\Big(\sum_\rho \frac{1}{\sigma - \rho}\Big) = \sum_\rho \frac{1}{\sigma - \rho},$$

where the latter sums are understood as $\lim_{R\to\infty} \sum_{|\gamma_\rho| < R} (\sigma - \rho)^{-1}$. This sum was evaluated by Stark [11, eq. (9)] (cf. [6, Satz 180]). Namely,[4]

$$\sum_\rho \frac{1}{\sigma - \rho} = \frac{\log \Delta_K}{2} + \frac{1}{\sigma - 1} + \frac{1}{\sigma} - \frac{1}{2}d_{K,\sigma}, \tag{19}$$

where we have used the duplication formula

$$\Psi(\sigma) = \log 2 + \frac{\Psi(\frac{\sigma}{2}) + \Psi(\frac{\sigma+1}{2})}{2}.$$

□

Proof of Theorem 1. In Lemma 4, take $k = \mathbb{Q}$, $a := \log(9)$ and $T := \log X$. The hypothesis $0 < a < T$ in Lemma 4 is satisfied since $X > 9$. A short calculation shows

$$\frac{1}{g(T)} - \frac{1}{g(T-a)} = \frac{2\sqrt{X}\log(3X)}{3}, \tag{20}$$

[4] One can prove (19) with the explicit formula, using $F(x) := \exp(-(\sigma - \frac{1}{2})|x|)$. However, the classical proof in [11] with the Weierstraß product and functional equation is faster.

with g as in (15). Since $\kappa_{K/\mathbb{Q}} = \kappa_K$ and

$$A(T) - A(T-a) = B_K(X) - B_K(X/9),$$

Lemma 4 yields for any $\sigma > 1$,

$$\frac{2\sqrt{X}\log(3X)}{3}\,|\log \kappa_K - f_K(X)| \le c_{a,T}\sum_{\rho}^{K+\mathbb{Q}} \frac{1}{\frac{1}{4}+\gamma_\rho^2} + (n_K - n_{\mathbb{Q}})ae^{-(T-a)/2}\beta(T-a). \tag{21}$$

The sum over the nontrivial zeroes of $\zeta_{\mathbb{Q}}$ is classical [5, §12, eqs. (10) and (11)],

$$\sum_{\substack{\rho\\ \zeta_{\mathbb{Q}}(\rho)=0}} \frac{1}{\frac{1}{4}+\gamma_\rho^2} = \frac{C}{2} + 1 - \frac{\log(4\pi)}{2} = .023095\cdots.$$

We also have

$$c_{a,T} = 1 + \frac{\log 9}{4} + \frac{6}{\log(X/9)},$$
$$(n_K - n_{\mathbb{Q}})ae^{-(T-a)/2} = \frac{(n-1)3\log 9}{\sqrt{X}}.$$

We have already noted in the proof of Lemma 4 that $\beta(T-a) = \beta\big(\log(X/9)\big)$ is a decreasing function of X, for $X > 9$. Moreover, $\beta\big(\log(X/9)\big) < 1$ for $X > 68.1$.

We turn to Lemma 5 to bound the sum over the zeroes of ζ_K. The main term in that lemma (say for $1 < \sigma < 3$) is

$$(2\sigma-1)\Big(\log\Delta_K + \frac{2}{\sigma-1}\Big).$$

This is minimized when $\sigma := 1 + (\log\Delta_K)^{-\frac{1}{2}}$. We fix this value of σ for the rest of this proof. Then

$$(2\sigma-1)\Big(\log\Delta_K + \frac{2}{\sigma-1}\Big) = \Big(\sqrt{\log\Delta_K} + 2\Big)^2.$$

Since $\Delta_K \ge 3$ for $K \ne \mathbb{Q}$, we have $1 < \sigma \le 1 + \big(\log 3\big)^{-\frac{1}{2}} < 3$.

We now estimate $d_{K,\sigma}$ in Lemma 5. Since $\frac{\zeta_K'}{\zeta_K}(\sigma) < 0$, $n_K \ge 2$ and $\Psi(x)$ is increasing for $x > 0$, we have

$$\begin{aligned} d_{K,\sigma} &> 2\big(\log(2\pi) - \Psi(\sigma)\big) - \frac{2}{\sigma} \qquad (\text{since } \log(2\pi) - \Psi(3) > 0)\\ &= 2\log(2\pi) - 2\Psi(\sigma+1) > 2\log(2\pi) - 2\Psi(4) = 1.163\cdots. \end{aligned}$$

Since $2\sigma - 1 > 1$, it follows that

$$\sum_{\substack{\rho\\ \zeta_{\mathbb{Q}}(\rho)=0}} \frac{1}{\frac{1}{4}+\gamma_\rho^2} - (2\sigma-1)d_{K,\sigma} < 0.$$

Hence (21) and Lemma 5 give, for $X \ge 68.1$,

$$\frac{2\sqrt{X}\log(3X)}{3}\,|\log\kappa_K - f_K(X)| \le \Big(1 + \frac{\log 9}{4} + \frac{6}{\log(X/9)}\Big)\Big(\sqrt{\log\Delta_K} + 2\Big)^2 + \frac{(n-1)3\log 9}{\sqrt{X}}.$$

Pulling out a factor of $(1+\frac{\log 9}{4})\log\Delta_K$ gives Theorem 1, since

$$\frac{3}{2}\left(1+\frac{\log 9}{4}\right)<2.324,\quad \frac{6}{1+\frac{\log 9}{4}}<3.88,\quad \frac{3\log 9}{1+\frac{\log 9}{4}}<4.26. \qquad \square$$

An examination of the proof shows that the choice of $a=\log 9=2.197\cdots$ is only nearly optimal. The optimal $a\approx 3.01$ improves the constant 2.324 in Theorem 1 to about 2.253. We have chosen $a=\log 9$ because it simplifies several expressions, beginning with (20).

Remark 6. *Although the proof requires $X>e^a=9$, the restriction $X\ge 69$ was only needed to ensure $\beta\big(\log(X/9)\big)<1$. The conclusion of Theorem 1 holds for $X>9$ provided the final term $\frac{4.26(n-1)}{\sqrt{X}\log\Delta_K}$ is replaced by $\frac{4.26(n-1)\beta(\log(X/9))}{\sqrt{X}\log\Delta_K}$.*

We can improve slightly on Theorem 1 by not dropping some favorable terms.

Theorem 7. *Let K be a number field of degree n_K with r_K real places. With the same assumptions and notation as in Theorem 1, except we now only assume $X>9$, we have for any $\sigma>1$,*

$$|\log\kappa_K-f_K(X)|\le\frac{2.324(2\sigma-1)}{\sqrt{X}\log(3X)}\cdot\left(\delta(K,\sigma,X)\Big(1+\frac{3.88}{\log(X/9)}\Big)+\frac{4.26(n_K-1)\beta\big(\log(X/9)\big)}{(2\sigma-1)\sqrt{X}}\right),$$

where

$$\delta(K,\sigma,X):=\log\Delta_K+\frac{\frac{C}{2}+1-\frac{\log(4\pi)}{2}}{2\sigma-1}+\frac{2}{\sigma-1}+\frac{2}{\sigma}-2\sum_{\substack{\mathfrak{p}\\ \mathrm{N}\mathfrak{p}<X}}\frac{\log\mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^\sigma-1}-n_K\big(\log(2\pi)-\Psi(\sigma)\big)-r_K\frac{\Psi\big(\frac{\sigma+1}{2}\big)-\Psi\big(\frac{\sigma}{2}\big)}{2}.$$

Here $\Psi(\sigma):=\Gamma'(\sigma)/\Gamma(\sigma)$ and $\beta(t)$ is defined in (16).

Proof. We proceed as in the proof of the previous theorem, fixing again $a=\log 9$, but we do not fix σ. If in $d_{K,\sigma}$ (see (18)) we truncate $-\frac{\zeta_K'}{\zeta_K}(\sigma)=\sum_{\mathfrak{p}}\frac{\log\mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^\sigma-1}$, instead of (21) we obtain

$$|\log\kappa_K-f_K(X)|\le\frac{3(2\sigma-1)}{2\sqrt{X}\log(3X)}\cdot\left(\delta(K,\sigma,X)\Big(1+\frac{\log 9}{4}+\frac{6}{\log(X/9)}\Big)+\frac{(n_K-1)3\log 9\cdot\beta\big(\log(X/9)\big)}{(2\sigma-1)\sqrt{X}}\right).$$

$\square$

In Theorem 7, $\sigma=1+1/\sqrt{\log\Delta_K}$ is usually a good choice. Taking instead $\sigma=1.5$, the value used by Bach [2, Lemma 4.2], we obtain

Corollary 8. *With the same assumptions and notation as in Theorem 7, we have*

$$|\log \kappa_K - f_K(X)| \le \frac{4.65}{\sqrt{X}\log(3X)}\left(\frac{2.23 n_K \beta\big(\log(X/9)\big)}{\sqrt{X}} + \left(1+\frac{3.88}{\log(X/9)}\right)\left(\log\Delta_K + 3.35 - 1.801 n_K - .619 r_K - 2\sum_{\substack{\mathfrak{p}\\ \mathrm{N}\mathfrak{p}<X}} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{1.5}}\right)\right).$$

5. Examples

This section compares, experimentally, three algorithms evaluating $\log\kappa_K$, by splitting rational primes up to a fixed bound X. These involve the functions $A_K(X)$, $g_K(X)$ and $f_K(X)$ defined below. All programs were implemented in the PARI/GP system [8].

We first define Schoof's approximation

$$A_K(X) := \log \prod_{p<X} \frac{1-p^{-1}}{\prod_{\mathfrak{p}|p,\mathrm{N}\mathfrak{p}<X} 1-\mathrm{N}\mathfrak{p}^{-1}},$$

originating in [10] and whose distance to $\log\kappa_K$ is bounded by Bach [2, Theorem 6.2 and Table 2] under GRH.[5] It is in principle weaker than our $f_K(X)$ or Bach's $g_K(X)$, since it only satisfies

$$|\log\,\kappa_K - A_K(X)| \ll \frac{\log\Delta_K}{\sqrt{X}}$$

(see also the remark at the end of [2, §8]). For X even, Bach's approximation to $\log\kappa_K$ is

$$g_K(X) := \sum_{i=0}^{x-1} a_i A_K(x+i),$$

where $x = X/2$, and

$$a_i := \frac{(x+i)\log(x+i)}{\sum_{j=0}^{x-1}(x+j)\log(x+j)}.$$

The distance $|g_K(X) - \log\kappa_K|$ is bounded in [2, Theorem 6.3 and Table 1], assuming GRH. Finally, our function

$$f_K(X) := \frac{3\big(B_K(X) - B_K(X/9)\big)}{2\sqrt{X}\log(3X)}$$

appears in Theorem 1. We assume $X \ge 10$ and include the term $\beta\big(\log(X/9)\big)$ from Remark 6 in the error bound.

We evaluate these three functions by first splitting all primes $p \le X$, and then by using $O(X)$ elementary operations in $\{+,\times,/,\log,\sqrt{\cdot}\}$. We can thus approximate those functions at X to a fixed accuracy in time $\widetilde{O}(X)$, softly linear in X. The application to Buchmann's algorithm requires the computation of $\log\kappa_K$ with an error bounded by $\frac{1}{2}\log 2$.

[5] As Bach warns, this bound assumes a result of Oesterlé's [2, equation (12)] whose proof has never been published.

TABLE 1. Least X so that $|f_K(X) - \log \kappa_K| < \frac{1}{2}\log 2$

Δ	$n = 2$	$n = 6$	$n = 10$	$n = 20$	$n = 50$
10^5	1,619	1,632	–	–	–
10^{10}	3,169	3,181	3,194	–	–
10^{20}	6,838	6,850	6,861	–	–
10^{50}	21,619	21,629	21,639	21,665	–
10^{100}	56,332	56,341	56,351	56,374	56,445
10^{200}	156,151	156,160	156,169	156,191	156,256

TABLE 2. Least X so that $|g_K(X) - \log \kappa_K| < \frac{1}{2}\log 2$

Δ	$n = 2$	$n = 6$	$n = 10$	$n = 20$	$n = 50$
10^5	4,469	6,493	–	–	–
10^{10}	9,799	11,324	13,857	–	–
10^{20}	22,476	25,621	28,935	–	–
10^{50}	91,044	96,596	99,999	110,802	–
10^{100}	268,680	276,338	284,088	303,864	366,575
10^{200}	866,110	878,749	891,468	923,610	1,000,000

TABLE 3. Least X so that $|A_K(X) - \log \kappa_K| < \frac{1}{2}\log 2$

Δ	$n = 2$	$n = 6$	$n = 10$	$n = 20$	$n = 50$
10^5	13,420	46,329	–	–	–
10^{10}	31,829	65,465	119,149	–	–
10^{20}	76,617	130,922	212,428	–	–
10^{50}	347,503	476,196	566,686	1,000,001	–
10^{100}	1,080,396	1,298,034	1,541,474	2,268,510	5,559,680
10^{200}	4,054,695	4,502,259	4,979,474	6,305,841	11,493,924

For each function $h \in \{f_K, g_K, A_K\}$, given a bound of the number field degree $n_K \le n$ and discriminant $\Delta_K \le \Delta$, Tables 1, 2 and 3 list the first integer X such that

$$|h(X) - \log \kappa_K| < \frac{1}{2}\log 2,$$

according to the error bounds mentioned above (all of which assume GRH). A dash (–) indicates that this value of n_K and Δ_K is forbidden by Odlyzko's discriminant bounds [7, Table 1].

Besides the asymptotic improvement for large discriminants, the weak dependency on the number field degree in secondary error terms makes our bound almost impervious to the degree, while Bach's and Schoof's are noticeably affected by n, even for relatively large discriminants.

References

[1] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380, DOI 10.2307/2008811. MR1023756 (91m:11096)

[2] Eric Bach, *Improved approximations for Euler products*, Number theory (Halifax, NS, 1994), Amer. Math. Soc., 1995, pp. 13–28. MR96i:11124

[3] Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), no. 262, 1185–1197, DOI 10.1090/S0025-5718-07-02003-0. MR2373197 (2009c:11179)

[4] Johannes Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 27–41. MR1104698 (92g:11125)

[5] Harold Davenport, *Multiplicative number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 1980. Revised by Hugh L. Montgomery. MR606931 (82m:10001)

[6] Edmund Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale* (German), Chelsea Publishing Company, New York, N. Y., 1949. MR0031002 (11,85d)

[7] Jacques Martinet, *Petits discriminants des corps de nombres* (French), Number theory days, 1980 (Exeter, 1980), London Math. Soc. Lecture Note Ser., vol. 56, Cambridge Univ. Press, Cambridge, 1982, pp. 151–193. MR697261 (84g:12009)

[8] *PARI/GP, version* `2.6.0`, Bordeaux, 2012, `http://pari.math.u-bordeaux.fr/`.

[9] Georges Poitou, *Sur les petits discriminants* (French), Séminaire Delange-Pisot-Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French), Secrétariat Math., Paris, 1977, pp. Exp. No. 6, 18. MR551335 (81i:12007)

[10] R. J. Schoof, *Class groups of complex quadratic fields*, Math. Comp. **41** (1983), no. 163, 295–302, DOI 10.2307/2007782. MR701640 (84h:12005)

[11] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152. MR0342472 (49 #7218)

[12] André Weil, *Sur les "formules explicites" de la théorie des nombres premiers* (French), Comm. Sém. Math. Univ. Lund [Medd. Lunds Univ. Mat. Sem.] **1952** (1952), no. Tome Supplementaire, 252–265. MR0053152 (14,727e)

Université Bordeaux, IMB, UMR 5251, F-33400 Talence; France; CNRS, IMB, UMR 5251, F-33400 Talence, France; INRIA, F-33400 Talence, France

E-mail address: `Karim.Belabas@math.u-bordeaux1.fr`

Departamento de Matemática, Universidad de Chile, Casilla 653, Santiago, Chile

E-mail address: `friedman@uchile.cl`