SMALL GENERATORS OF THE IDEAL CLASS GROUP

KARIM BELABAS, FRANCISCO DIAZ Y DIAZ, AND EDUARDO FRIEDMAN

Abstract. Assuming the Generalized Riemann Hypothesis, Bach has shown that the ideal class group $\mathcal{C}\ell_K$ of a number field K can be generated by the prime ideals of K having norm smaller than $12\big(\log|\text{Discriminant}(K)|\big)^2$. This result is essential for the computation of the class group and units of K by Buchmann's algorithm, currently the fastest known. However, once $\mathcal{C}\ell_K$ has been computed, one notices that this bound could have been replaced by a much smaller value, and so much work could have been saved. We introduce here a short algorithm which allows us to reduce Bach's bound substantially, usually by a factor 20 or so. The bound produced by the algorithm is asymptotically worse than Bach's, but favorable constants make it useful in practice.

Contents

1. Introduction 1
2. Proof of Theorem 4
3. An algorithm 7
4. How good is $T(K)$? 9
5. Unconditional results 10
6. Numerical experiments 12
References 14

1. Introduction

In the 1980's, building on earlier work of Hafner and McCurley [Ha], Buchmann [Bu] introduced a remarkable probabilistic algorithm for computing a finite presentation for the ideal class group $\mathcal{C}\ell_K$ and units $U(K)$ of a number field K. Buchmann's algorithm selects first a *factor base*

$$\mathcal{B} = \mathcal{B}(T) := \{\mathfrak{p}\colon \mathfrak{p} \text{ prime ideal of } \mathcal{O}_K,\ N\mathfrak{p} < T\}\,,$$

which is a set of ideals of norm less than T whose classes generate $\mathcal{C}\ell_K$, for a large enough T. We then looks for relations among the elements of $\mathcal{B}$ in $\mathcal{C}\ell_K$: given a random product I of ideals from the factor base, the LLL algorithm produces an

Date: December 5th, 2005.
1991 *Mathematics Subject Classification.* Primary 11R04; Secondary 11R29.
Key words and phrases. Ideal Class Group, Generalized Riemann Hypothesis,
This work was partially supported by Chilean Fondecyt grant N^{o}1040585.

element α of small height in I, hence a supposedly nicer representative $J = I/(\alpha)$ in the ideal class of I. If J factors on the factor base, we have found a relation in $\mathcal{C}\ell_K$. To check whether enough relations have been accumulated, a tentative class number $\hat{h}$ is computed from the available relations via linear algebra. The latter elimination produces trivial relations $(\alpha) = (\alpha')$, hence units α/α', from which a tentative regulator $\hat{R}$ is computed. It now computes an approximation $\widehat{hR}$ of the product of the class number by the regulator, from a truncated Euler product converging to the residue of the Dedekind zeta function of K. Finally, $\hat{h}\hat{R}$ is an integral multiple of hR; so, if $\hat{h}\hat{R}/\widehat{hR}$ is not close enough to 1, we look for more relations, otherwise we are done (see also [Co] for algorithmic details).

As far as linear algebra goes, it is desirable to take T as small as possible, such that $\mathcal{B}(T)$ generates $\mathcal{C}\ell_K$. (Of course, relations are correspondingly harder to find; on the other hand, fewer are needed.) To date the best unconditional result known is Zimmert's $T < C\sqrt{\Delta_K}$, see [Zi, dM], where Δ_K is the absolute value of the discriminant of K and C is an explicit constant depending on the signature of K. Although Zimmert's bound is a considerable improvement on Minkowski's [La, V §4], its exponential dependence on $\log \Delta_K$ thwarts any hope of a subexponential algorithm.

Let $T_{\min} = T_{\min}(K) \geq 1$ be the minimal value of T such that the primes in $\mathcal{B}(T_{\min})$ generate $\mathcal{C}\ell_K$, and let $t_{\min}(K) := T_{\min}(K)/(\log \Delta_K)^2$. Assuming the Generalized Riemann Hypothesis (GRH), Bach [Ba] showed $t_{\min} \leq 12$. In fact, he even showed that for large discriminants, $t_{\min} < 4 + \varepsilon$ for any $\varepsilon > 0$. Still under GRH, a companion result [Ba2] shows that a small Euler product yields a good enough approximation to hR that we may apply our halting criterion. On these grounds, Buchmann's algorithm conjecturally runs in probabilistic subexponential time. If K is quadratic, and GRH holds, this is actually a theorem ([Ha, Bu]).

The above factor of 12 (and even of $4 + \varepsilon$), is much too large in practice: to our knowledge, experimental evidence thus far has not yielded any example where $t_{\min}(K) > \frac{1}{2}$. It even looks plausible that the *average* value of $T_{\min}(K)$ as the discriminant of K increases is $O(\log \Delta_K)^{1+\varepsilon}$ for any $\varepsilon > 0$. This is true, for instance, under GRH for the related problem of finding small generators of $\mathbb{F}_p^*$ [Mu]. To take advantage of this, one fixes an arbitrary factor base $\mathcal{B}(T_0)$, for some

$$T_0(K) \leq T(K) \tag{1}$$

independently optimized so as to balance the cost of the linear algebra and the relation search. A priori $\mathcal{B}(T_0)$ now generates a subgroup $H \subset \mathcal{C}\ell_K$. Then one proves directly that the elements of $\mathcal{B}(T) \setminus \mathcal{B}(T_0)$ belong to H, using the same ideas as to find relations, thereby proving that $H = \mathcal{C}\ell_K$. (If that check fails, we increase T_0 and restart.) When building tables of class groups of "small" fields, most of the computing time is spent in this last phase.

In Bach's approach, GRH is needed to control the size of two sums, say A and B, appearing in Weil's explicit formula [We]. Sum A is over the zeroes of an L-function attached to a non-trivial character of $\mathcal{C}\ell_K$, while B is over the zeroes of the Dedekind zeta function of K.

In this paper we introduce two modifications to Bach's method in order to obtain a smaller T. Weil's formula involves an auxiliary function carefully chosen by Bach so as to heavily weigh the prime ideals of small norm. Still assuming GRH, we modify Bach's choice of auxiliary function so that $A \geq 0$. This allows us to simply drop A, instead of having to estimate it unfavorably as Bach did.

Our second modification is not to estimate B either, even though its sign is unfavorable. Instead, we compute it quickly and exactly using Weil's very formula [We, Po]. We remark that A involves a non-trivial character of $\mathcal{C}\ell_K$, so it cannot be computed without prior knowledge of $\mathcal{C}\ell_K$.

The cost of these changes is that we do not obtain a general constant, such as Bach's 12. Instead, we calculate a permissible value of T for each field K using the following result.

Theorem 1.1. *Let K be a number field of degree n, having exactly r_1 real embeddings, and which satisfies the Riemann Hypothesis for each L-function attached to a non-trivial character of its ideal class group $\mathcal{C}\ell_K$. Then the inequality*

$$\sum_{N\mathfrak{p}^m<T} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}} \left(1 - \frac{\log(N\mathfrak{p}^m)}{\log T}\right) > \frac{1}{2}\log \Delta_K - 1.9\, n - .785\, r_1 + \frac{2.468\, n + 1.832\, r_1}{\log T} \tag{2}$$

is a sufficient condition for $\mathcal{C}\ell_K$ to be generated by the ideal classes corresponding to the prime ideals of K having norm strictly smaller than T.

The sum above is over all prime ideals $\mathfrak{p}$ of K and all positive integers m satisfying $N\mathfrak{p}^m < T$. It is a divergent sum as $T \to +\infty$ (see Lemma 4.1), so inequality (2) is certainly satisfied for some large enough T.

Definition 1.2. We call $T(K)$ the integral part of the smallest value of $T \geq 1$ satisfying the inequality (2), and let $t(K) := T(K)/(\log \Delta_K)^2$.

Unfortunately, we are not able to prove that (2) will be satisfied for a T smaller than Bach's bound, *i.e.* that $t(K) < 12$. In fact, as $\Delta_K \to +\infty$ while the degree n remains fixed, we shall see that $t(K) \to +\infty$ (see Theorem 4.3), whereas Bach proves that $t_{\min}(K) \lesssim 4$. Nonetheless, $t(K)$ grows so very slowly that, in practical computations, its value is usually around $\frac{1}{2}$, and very rarely above 1 (see §6). In any case, computing $T(K)$ takes negligible time (essentially, quadratic time), compared with the cost of running the rest of Buchmann's algorithm (see §3).

It is possible, and in fact quite frequent, that $T(K) < T_0$, the value estimated by balancing linear algebra and relation search. In this case we choose $T = T_0$ as in (1), and happily skip the final checks.

2. Proof of Theorem

We begin by sketching Bach's main idea. Suppose S is a set of prime ideals whose classes we would like to show generate the ideal class group $\mathcal{C}\ell_K$. Let $\langle S\rangle \subset \mathcal{C}\ell_K$ be the subgroup generated by the classes in S. If $\langle S\rangle \neq \mathcal{C}\ell_K$, then there exists a nontrivial character $\kappa : \mathcal{C}\ell_K \to \mathbb{C}^*$ which is trivial on $\langle S\rangle$. If we specialize S to be the set of all prime ideals of norm at most T (with T chosen large enough below), we find that the beginning of the Euler product of the non-trivial L-function $L(s,\kappa)$ coincides with that of the Dedekind zeta function $L(s,\chi_0)$.

More generally, weighted sums of character values begin identically for κ and χ_0. If we take weights of compact support, we can make the (finite) weighted sums identical. However, Weil's formula [We, La] for a weighted sum involving κ differs from that involving χ_0 by a large term coming from the pole of $L(s,\chi_0)$. They also differ by another term involving the zeroes ρ of the L-functions in the critical strip $0 < \mathrm{Re}(\rho) < 1$, but these are controlled by assuming GRH. Taking T large enough, Bach shows that the pole term dominates the term coming from the zeroes. This contradiction implies that S generates $\mathcal{C}\ell_K$, as desired.

To flesh out the sketch above we need to recall Weil's formula. We let K denote a number field of degree $n = [K : \mathbb{Q}]$, having exactly r_1 real embeddings, and whose discriminant has absolute value Δ_K. If χ is a character of the ideal class group of K, Weil's explicit formula [We, La], as simplified by Poitou [Po], is the identity

$$\begin{aligned}\sum_{\rho_\chi} \Phi(\rho_\chi) = 4\delta_\chi \int_0^{+\infty} F(x)\cosh(x/2)\,dx + F(0)\big(\log\Delta_K - n\gamma - n\log(8\pi) - \frac{r_1\pi}{2}\big)\\ - \sum_{\mathfrak{p}} \log N\mathfrak{p} \sum_{m=1}^{+\infty} \frac{F(m\log N\mathfrak{p})}{N\mathfrak{p}^{m/2}}(\chi(\mathfrak{p})^m + \chi(\mathfrak{p})^{-m}) \qquad (3)\\ + r_1\int_0^{+\infty} \frac{F(0)-F(x)}{2\cosh(x/2)}\,dx + n\int_0^{+\infty}\frac{F(0)-F(x)}{2\sinh(x/2)}\,dx.\end{aligned}$$

We begin by explaining the notation on the right-hand side of Weil's formula and the assumptions we make. We have let $\delta_\chi = 1$ if χ is trivial, and $\delta_\chi = 0$ otherwise. The "arbitrary" weight function $F : [0,+\infty) \to \mathbb{C}$ is assumed to be continuous and such that for some $\varepsilon > 0$, the function $F(x)\mathrm{e}^{(\frac{1}{2}+\varepsilon)x}$ is of bounded variation and integrable over $[0,+\infty)$. We also assume that $\big(F(0) - F(x)\big)/x$ is itself of bounded variation on $[0,+\infty)$. By γ we mean Euler's constant $0.5772\cdots$. This takes care of the right-hand side of first line.

On the second line, $\mathfrak{p}$ runs over all prime ideals of the ring of algebraic integers of K, the absolute norm of $\mathfrak{p}$ is denoted by $N\mathfrak{p}$, and $\chi(\mathfrak{p})$ is the value of the character χ on the ideal class of $\mathfrak{p}$. The third line is self-explanatory, but we must add that it was not at all so in Weil's version [We, La], where it was a

principal value of a related integral. Poitou [Po] simplified the term coming from the archimedean places appearing on the third line.

The sum on the left-hand side of (3) runs over all zeroes ρ_χ in the critical strip of the L-function $L(s,\chi)$, with multiple zeroes repeated accordingly. The transform $\Phi(s)$ of F is defined by

$$\Phi(s) := 2\int_0^{+\infty} F(x)\cosh\left(x(s-\tfrac{1}{2})\right)dx \qquad (0 \le \mathrm{Re}(s) \le 1). \tag{4}$$

Under the above assumptions on F, the sum over ρ_χ converges when understood as

$$\lim_{R\to+\infty}\sum_{|\mathrm{Im}(\rho_\chi)|<R}\Phi(\rho_\chi).$$

In comparing the above version of Weil's formula against those in the literature [We, La, Po], the reader should bear in mind that we have taken advantage of some minor simplifications. Following Poitou [Po], instead of taking $F : \mathbb{R} \to \mathbb{C}$, we have taken $F : [0,+\infty) \to \mathbb{C}$, implicitly extending F to $\mathbb{R}$ by requiring $F(-x) = F(x)$. This allows us to rewrite all integrals over $\mathbb{R}$ as integrals over $[0,+\infty)$ and simplifies the sum over m in (3). We have also required F to be continuous, instead of allowing jump discontinuities, since the F in our applications below will be continuous. A more substantial simplification stems from the assumption that χ is an unramified character, rather than the ray class character allowed by Weil in general. This makes the contribution to the formula for χ coming from the archimedean places of K, and also from the finite places ramified in $K/\mathbb{Q}$, identical with that of the trivial character χ_0. We can therefore take advantage of Poitou's carefully proved and simplified form of Weil's formulas [Po, pp. 6-7].

We now turn to our main result, where all notation is as in (3).

Theorem 2.1. *Let K be a number field satisfying the Riemann Hypothesis for all L-functions attached to non-trivial characters of its ideal class group $\mathcal{C}\ell_K$, and let $F : [0,+\infty) \to \mathbb{R}$ satisfy the assumptions in Weil's explicit formula* (3)*. Assume furthermore that $F(0) = 1$, that F is supported on a finite interval $[0, \log T]$, and that its Fourier cosine transform is non-negative. Then the inequality*

$$\begin{aligned} 2\sum_{\mathfrak{p}}\log N\mathfrak{p}\sum_{m=1}^{+\infty}\frac{F(m\log N\mathfrak{p})}{N\mathfrak{p}^{m/2}} &> \log\Delta_K - n\gamma - n\log(8\pi) - \frac{r_1\pi}{2} \\ &\quad + r_1\int_0^{+\infty}\frac{1-F(x)}{2\cosh(x/2)}\,dx + n\int_0^{+\infty}\frac{1-F(x)}{2\sinh(x/2)}\,dx \end{aligned} \tag{5}$$

is a sufficient condition for $\mathcal{C}\ell_K$ to be generated by the classes of prime ideals $\mathfrak{p}$ of K having norm $N\mathfrak{p} < T$.

Proof. Assume that the prime ideals of norm smaller than T do not generate $\mathcal{C}\ell_K$. As explained above, there is then a non-trivial character κ of $\mathcal{C}\ell_K$ which is trivial

on the classes of all primes of norm smaller than T. Since we are assuming GRH, $\mathrm{Re}(\rho_\kappa) = \frac{1}{2}$ for the zeroes ρ_κ appearing in (3). Writing,

$$\rho_\kappa = \frac{1}{2} + i\gamma_\kappa,$$

we have $\Phi(\rho_\kappa) = \widehat{F}(\gamma_\kappa)$, where $\widehat{F}$ is the Fourier cosine transform of F

$$\widehat{F}(t) := 2\int_0^{+\infty} F(x)\cos(xt)\,dx. \tag{6}$$

Since we have assumed $\kappa(\mathfrak{p}) = 1 = \chi_0(\mathfrak{p})$ for $N\mathfrak{p} < T$, and $F(m\log N\mathfrak{p}) = 0$ for $N\mathfrak{p}^m \geq T$, we obtain the equality between the finite sums corresponding to the second line of (3) for the characters κ and χ_0. Now subtract Weil's formula (3) for κ from Weil's formula for χ_0. As several terms cancel, we simply obtain

$$\sum_{\rho_{\chi_0}} \Phi(\rho_{\chi_0}) - \sum_{\rho_\kappa} \Phi(\rho_\kappa) = 4\int_0^{+\infty} F(x)\cosh(x/2)\,dx. \tag{7}$$

Since $\Phi(\rho_\kappa) = \widehat{F}(\gamma_\kappa)$, and we have assumed $\widehat{F}(t) \geq 0$ for all real t, we may drop the sum over the ρ_κ to obtain

$$\sum_{\rho} \Phi(\rho) \geq 4\int_0^{+\infty} F(x)\cosh(x/2)\,dx, \tag{8}$$

where we have now written ρ instead of ρ_{χ_0}. Thus, ρ runs over all zeroes of the Dedekind zeta function of K in the critical strip. If we now substitute the value of $\sum_\rho \Phi(\rho)$ given by (3) for $\chi = \chi_0$, we obtain exactly the negation of inequality (5). This contradiction shows that κ cannot exist, *i.e.*, the class group is generated by the primes of norm not exceeding T. □

In Theorem 2.1, let us consider the function

$$F_T(x) := \begin{cases} 1 - \dfrac{x}{L} & \text{if } 0 \leq x \leq L, \\ 0 & \text{if } x \geq L, \end{cases} \tag{9}$$

with $L = \log T$. Theorem 1.1 is the numerical version of the following.

Corollary 2.2. *Suppose K satisfies GRH as above and that for some $T > 1$ we have*

$$2\sum_{\substack{\mathfrak{p},m \\ N\mathfrak{p}^m < T}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}\left(1 - \frac{\log(N\mathfrak{p}^m)}{\log T}\right) > \log\Delta_K - n\left(\gamma + \log(8\pi) - \frac{c_1}{\log T}\right) - r_1\left(\frac{\pi}{2} - \frac{c_2}{\log T}\right), \tag{10}$$

where

$$c_1 := \int_0^{+\infty} \frac{x}{2\sinh(x/2)}\,dx = \frac{\pi^2}{2}, \qquad c_2 := \int_0^{+\infty} \frac{x}{2\cosh(x/2)}\,dx = 4C.$$

(Here $C = \sum_{k\ge 0}(-1)^k(2k+1)^{-2} = 0.915965\cdots$ is Catalan's constant.)

Then the ideal class group of K is generated by the prime ideals of K having norm less than T.

Proof. The function F_T satisfies the hypotheses on F made in the Theorem. Indeed, only $\widehat{F_T} \ge 0$ is not obvious. One can either compute directly

$$\widehat{F_T}(t) = L\left(\frac{\sin(tL/2)}{tL/2}\right)^2, \tag{11}$$

or note that $F_T(x) = (1/L)(f * f)(x)$, where f is the characteristic function of the interval $(-L/2, L/2)$ and $*$ is the convolution product (here we regard F_T as an even function on $\mathbb{R}$). Let

$$k(x) := \frac{n}{2\sinh(x/2)} + \frac{r_1}{2\cosh(x/2)}, \tag{12}$$

and calculate

$$\begin{aligned}\int_0^{+\infty} \big(1 - F_T(x)\big)k(x)\,dx &= \frac{1}{L}\int_0^L xk(x)\,dx + \int_L^{+\infty} k(x)\,dx \\ &= \frac{1}{L}\int_0^{+\infty} xk(x)\,dx + \int_L^{+\infty} (1 - \frac{x}{L})k(x)\,dx \\ &= \frac{1}{L}(nc_1 + r_1c_2) + \int_L^{+\infty} (1 - \frac{x}{L})k(x)\,dx \qquad (13)\\ &< \frac{1}{L}(nc_1 + r_1c_2).\end{aligned}$$

Hence (10) implies (5). □

The reader may be surprised at our dropping of $\int_L^{+\infty}(1 - \frac{x}{L})k(x)\,dx$ at the end of the above proof, as we could have kept it at little computational cost. However, the term dropped is of order $n/\sqrt{T}$ while the left-hand side of (10) is the beginning of a divergent series. In practice, we are willing to compute up to primes of norm T much larger than n^2. Admittedly, this is because we cannot yet compute the ideal class group of a field of large degree.

3. An algorithm

Corollary 2.2 leads to a simple and fast algorithm for computing a T such that $\mathcal{B}(T)$ generates $\mathcal{C}\ell_K$, assuming GRH. We assume that K is given in the form $\mathbb{Q}[x]/\big(f(x)\big)$, where $f \in \mathbb{Z}[x]$ is an irreducible monic polynomial, and we compute a $\mathbb{Z}$-basis for the ring of algebraic integers $\mathbb{Z}_K$ of K. We also compute the absolute

value of the discriminant Δ_K and r_1, the number of real places of K. We then store

$$D = D(K) := \log \Delta_K - n(\gamma + \log(8\pi)) - r_1 \frac{\pi}{2}.$$

Let

$$S(T) = -\frac{nc_1 + r_1 c_2}{\log T} + 2 \sum_{\substack{\mathfrak{p},m \\ N\mathfrak{p}^m < T}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}} \left(1 - \frac{\log(N\mathfrak{p}^m)}{\log T}\right). \tag{14}$$

We may find $T(K)$ by dichotomy once we know an upper bound for it, 1 being an obvious lower bound. As an initial guess, we set $T = T_0(K)$, with T_0 chosen as in (1), and double this value until $S(T) > D$ or $T > 12(\log \Delta_K)^2$, whichever comes first. In the latter case, we are not able to improve Bach's bound; this unwelcome outcome has not occurred in our calculations, but will occur as $\Delta_K \to +\infty$ (see Theorem 4.3). Otherwise, we may compute the exact value of $T(K)$ by dichotomy ($O(\log D)$ evaluations of S). Whenever we evaluate $S(T)$ we calculate and save the splitting pattern in $K/\mathbb{Q}$ of all primes $p < T$ not stored so far.

Lemma 3.1. *We fix the degree n, so that $D \sim \log \Delta_K$. Disregarding the time needed to compute splitting patterns of primes, the above dichotomy computes the value $T(K)$ in time $O_n(D^2(\log D)^2)$ and space $O_n(D^2)$.*

Proof. We are only concerned with values of T which are $O(D^2) = O_n(D^2)$, since we abort the computation when reaching Bach's bound. We need to store the splitting patterns in $K/\mathbb{Q}$ of all primes $p < T$, each of which takes constant space if the degree is fixed. For $0 < x < T$ let

$$g_T(x) := \frac{1}{\sqrt{x}} \left(1 - \frac{\log(x)}{\log T}\right). \tag{15}$$

Given this data, an evaluation of $\log N\mathfrak{p} \cdot g_T(N\mathfrak{p}^m)$ for $N\mathfrak{p}^m < T$, requires $O(\log^2 T)$ bit operations using naïve arithmetic. On the other hand, using the standard formulae

$$\sum_{1 \le m \le M} q^m = \frac{q(1-q^M)}{1-q}, \quad \sum_{1 \le m \le M} mq^m = \frac{q(1 - q^M(M+1-Mq))}{(1-q)^2},$$

where $M = \lfloor \log T / \log N\mathfrak{p} \rfloor$ and $q = N\mathfrak{p}^{-1/2}$, we need only sum $O(T/\log T)$ terms to evaluate $S(T)$, hence $O(T \log T)$ bit operations. We make $O(\log D)$ such evaluations. □

Note that the splitting patterns of all primes less than T are needed in any case to apply Buchmann's algorithm with factor base $\mathcal{B}(T)$. In fact, it requires further technical data, so as to be able to multiply them and compute valuations.

Fixing n is realistic, since it is bounded by 50 or so in practice.

4. How good is $T(K)$?

Recall that $T(K)$ is the integral part of the minimal $T \geq 1$ such that $S(T) > D$, where S is defined in (14). We shall use $\sim_K$ below for asymptotic estimates with implied constants depending on Δ_K, and $\sim$ when they depend only on $[K : \mathbb{Q}]$.

Lemma 4.1. *As T tends to $+\infty$, we have $S(T) \sim_K 8\sqrt{T}/\log T$.*

Proof. By the prime ideal theorem

$$\psi_K(x) := \sum_{\substack{\mathfrak{p},m \\ N\mathfrak{p}^m<x}} \log N\mathfrak{p} \sim_K x.$$

Integration by parts yields

$$2 \sum_{\substack{\mathfrak{p},m \\ N\mathfrak{p}^m<T}} \log N\mathfrak{p} \cdot g_T(N\mathfrak{p}^m) = -2 \int_1^T \psi_K(x)\, dg_T(x) \sim_K \frac{8\sqrt{T}}{\log T},$$

where g_T was defined in (15). The lemma now follows from the definition of $S(T)$ in (14). □

Assume now that we can drop the dependency on K in Lemma 4.1. Then the equality $S(T) = D$ would imply $\log T \sim 2 \log D$, and suggests the following

Guess 4.2. *We fix the degree n, so that $D \sim \log \Delta_K$. As $\Delta_K \to +\infty$, we have*

$$T(K) \overset{?}{\sim} \left(\frac{1}{4} D \log D\right)^2.$$

If our guess is correct, we expect to lose against Bach's $(4 + o(1))(\log \Delta_K)^2$ when $(\frac{1}{4} \log D)^2 \approx 4$, that is $\log \Delta_K \approx e^8 \approx 2980.96$, so $T(K)$ would stand a good chance of being more useful for any practical computation. In fact, we are not aware of a single successful application of Buchmann's algorithm for a field K with $\log \Delta_K > 150$, say. Rigorously, we can prove

Theorem 4.3. *Fix the degree n; as $\Delta_K \to +\infty$, we have*

$$T(K) > \left(\frac{1 + o(1)}{4n} \log \Delta_K \log\log \Delta_K\right)^2.$$

Proof. We need the sum $S(T)$ to satisfy $S(T) > \log \Delta_K + O(1)$. Let $L = \log T$ and $g(x) = x(1 - x/L)e^{-x/2}$, so that $g'(x)$ has the sign of $x^2 - (4 + L)x + 2L$. Since the latter is positive at 0 and negative at 2, it has a root in $[0, 2]$; the other root is $> L$ since their product is $2L$. Hence g is decreasing on $[2, L]$. It follows

that

$$\sum_{\substack{\mathfrak{p},m\\ N\mathfrak{p}^m<T}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}\left(1-\frac{\log(N\mathfrak{p}^m)}{\log T}\right) \le \sum_{\substack{\mathfrak{p},m\\ N\mathfrak{p}^m<T}} g(m\log N\mathfrak{p})$$
$$\le n\sum_{\substack{p,m\\ p^m<T}} g(m\log p) \sim 8n\frac{\sqrt{T}}{\log T}$$

by Lemma 4.1 applied to $K=\mathbb{Q}$ and the fact that the sum for $m\ge 2$ is $O(\log T)$. It follows that $(8n+o(1))\frac{\sqrt{T}}{\log T} > \log\Delta_K$ as $T\to+\infty$ from which we obtain $\left(\frac{1}{2}+o(1)\right)\log T > \log\log\Delta_K$ and

$$\sqrt{T} > \left(\frac{1}{4n}+o(1)\right)\log\Delta_K\log\log\Delta_K.$$

□

5. Unconditional results

In this section we drop GRH and prove

Theorem 5.1. *Let K be a number field of of degree n, having exactly r_1 real embeddings. Suppose that $f:[0,+\infty)\to\mathbb{R}$ is supported on a finite interval $[0,\log T]$, that f has a non-negative Fourier cosine transform, $f(0)=1$, and that $F(x):=f(x)/\cosh(x/2)$ satisfies the assumptions in Weil's explicit formula* (3). *Then the inequality*

$$4\sum_{\mathfrak{p}}\log N\mathfrak{p}\sum_{m=1}^{+\infty}\frac{f(m\log N\mathfrak{p})}{1+N\mathfrak{p}^m} > \log\Delta_K - n\gamma - n\log(4\pi) - r_1$$
$$+ r_1\int_0^{+\infty}\frac{1-f(x)}{2\cosh^2(x/2)}\,dx + n\int_0^{+\infty}\frac{1-f(x)}{\sinh(x)}\,dx \qquad (16)$$

is a sufficient condition for $\mathcal{C}\ell_K$ to be generated by the classes of prime ideals $\mathfrak{p}$ of K having norm $N\mathfrak{p}<T$.

Proof. Reviewing the proof in §2, we see that GRH. was not used until after equation (7). On taking real parts in (7) we obtain

$$\sum_{\rho_{\chi_0}}\mathrm{Re}\left(\Phi(\rho_{\chi_0})\right) - \sum_{\rho_\kappa}\mathrm{Re}\left(\Phi(\rho_\kappa)\right) = 4\int_0^{+\infty} f(x)\,dx. \qquad (17)$$

We now need $\mathrm{Re}\left(\Phi(\rho_\kappa)\right)\ge 0$ for all ρ_κ in the critical strip, rather than just on the critical line. Faced with a similar problem in his work on discriminant bounds, Odlyzko observed [Po] that the maximum principle for harmonic functions implies that $\mathrm{Re}\left(\Phi(s)\right)\ge 0$ for s in a strip if and only if $\mathrm{Re}\left(\Phi(s)\right)\ge 0$ for s on its

boundary. As $\Phi(s) = \Phi(1-s)$ (see (4)), Odlyzko deduced that $\mathrm{Re}\big(\Phi(s)\big) \geq 0$ for s in the critical strip follows from $\mathrm{Re}\big(\Phi(1+it)\big) \geq 0$ for $t \in \mathbb{R}$. Now,

$$\begin{aligned}\mathrm{Re}\big(\Phi(1+it)\big) &= 2\int_0^{+\infty} \mathrm{Re}\big(F(x)\cosh(\tfrac{x}{2}+ixt)\big)\,dx \\ &= 2\int_0^{+\infty} F(x)\cosh(x/2)\cos(xt)\,dx = \widehat{f}(t) \geq 0, \end{aligned} \tag{18}$$

by assumption. Thus, from(17),

$$\sum_{\rho} \mathrm{Re}\big(\Phi(\rho)\big) \geq 4\int_0^{+\infty} f(x)\,dx, \tag{19}$$

where we have again written ρ for ρ_{χ_0}.

To evaluate the sum over ρ above it proves useful to re-write Weil's formula (3) in terms of $f(x) = F(x)\cosh(x/2)$, rather than $F(x)$. On taking real parts, the result is [Po]

$$\begin{aligned}\sum_{\rho} \mathrm{Re}\big(\Phi(\rho)\big) &= 4\int_0^{+\infty} f(x)\,dx + \log\Delta_K - n\gamma - n\log(4\pi) - r_1 \\ &\quad - 4\sum_{\mathfrak{p}} \log N\mathfrak{p} \sum_{m=1}^{+\infty} \frac{f(m\log N\mathfrak{p})}{1+N\mathfrak{p}^m} \\ &\quad + r_1\int_0^{+\infty} \frac{1-f(x)}{2\cosh^2(x/2)}\,dx + n\int_0^{+\infty} \frac{1-f(x)}{\sinh(x)}\,dx. \end{aligned} \tag{20}$$

Here ρ again runs over all zeroes (counting multiplicities) of the Dedekind zeta function of K and

$$\Phi(\rho) = 2\int_0^{+\infty} \frac{f(x)}{\cosh(x/2)} \cosh\big(x(\rho-\tfrac{1}{2})\big)\,dx. \tag{21}$$

As before, the Theorem is proved by observing that (19) and (20) contradict inequality (16), which we had assumed. □

Exactly as in §2, on taking

$$f(x) := \begin{cases} 1 - \dfrac{x}{\log T} & \text{if } 0 \leq x \leq \log T, \\ 0 & \text{if } x \geq \log T. \end{cases} \tag{22}$$

we obtain,

Corollary 5.2. *Suppose that for some $T > 1$ we have*

$$4 \sum_{\substack{\mathfrak{p},m \\ N\mathfrak{p}^m<T}} \frac{\log N\mathfrak{p}}{1+N\mathfrak{p}^m}\left(1-\frac{\log(N\mathfrak{p}^m)}{\log T}\right) > \log\Delta_K - n\left(\gamma+\log(4\pi)-\frac{h_1}{\log T}\right) - r_1\left(1-\frac{h_2}{\log T}\right), \tag{23}$$

where

$$h_1 := \int_0^{+\infty} \frac{x}{\sinh(x)}\,dx = \frac{\pi^2}{4}, \qquad h_2 := \int_0^{+\infty} \frac{x}{2\cosh^2(x/2)}\,dx = \log 4.$$

Then the ideal class group of K is generated by the prime ideals of K having norm less than T.

Now, let

$$S_{\mathrm{uncond}}(T) = -\frac{nh_1+r_1h_2}{\log T} + 4 \sum_{\substack{\mathfrak{p},m \\ N\mathfrak{p}^m<T}} \frac{\log N\mathfrak{p}}{1+N\mathfrak{p}^m}\left(1-\frac{\log(N\mathfrak{p}^m)}{\log T}\right). \tag{24}$$

Since this sum diverges again, we may easily adapt the algorithm of §3 to try and improve on Zimmert's bound in practice:

Lemma 5.3. *As T tends to $+\infty$, we have $S_{uncond}(T) \sim_K 2\log T$.*

Proof. Let $g(x) := (1+x)^{-1}(1-\log x/\log T)$. Integration by parts yields

$$2 \sum_{\substack{\mathfrak{p},m \\ N\mathfrak{p}^m<T}} \log N\mathfrak{p}\cdot g(N\mathfrak{p}^m) = -2\int_1^T \psi_K(x)\,dg(x) \sim_K 2\log T.$$

□

The analog of our Guess 4.2 is now to expect that the value of the smallest T such that $S_{\mathrm{uncond}}(T) > \Delta_K$ is of the order of $\sqrt{\Delta_K}$.

6. Numerical experiments

All computations were performed with the PARI/GP system [PARI] on a 1.6GHz Pentium IV. For any K with $\log\Delta_K > 150$, it would be a major computation to try and find $\mathcal{C}\ell_K$ with the PARI implementation: at least a few weeks, with little hope of success.

We start with a very simple example, the 11-th cyclotomic field $K = \mathbb{Q}(\zeta_{11})$, which is of course principal, so $T_{\min}(K) = 1$. We compute $T(K) = 19$, so $t(K) \approx 0.0408 \ll 12$. Using the value $T = 0.05$, the PARI implementation of Buchmann's algorithm experimentally succeeds in 0.03s on average. Without our algorithm, checking the remaining primes up to $4(\log\Delta_K)^2$ requires 1s, and 3s up to Bach's universal bound. In fact, running over all cyclotomic fields $K = \mathbb{Q}(\zeta_p)$ for prime $p \le 101$, the largest value seen is $t(K) \approx 0.257$. On the other hand,

the imaginary quadratic field of discriminant $-4\prod_{p<3000} p \approx -1.3\cdot 10^{1274}$ satisfies $t(K) \approx 4.87$ and the pure field $K = \mathbb{Q}(\prod_{p<500} p^{1/30})$ of discriminant $\approx 1.28\cdot 10^{6201}$ has $t(K) \approx 6.75$ (p runs over primes in both products).

The small value of $t(K)$ for cyclotomic fields is typical for fields of small discriminant, given a signature. We ran our algorithm on all quadratic fields of discriminant less than 10^6 and all fields in the Bordeaux database [NF], which contains fields of degree ≤ 7, sorted by signature and increasing discriminant. We stigmatize a field K as *bad* if $t(K) > 0.7$. The results are as follows

n	r_1	average $t(K)$	$\max_K t(K)$	# of fields	# of bad fields
2	0	0.326	1.86	303968	5525
	2	0.255	1.39	303957	559
3	1	0.155	0.806	182417	12
	3	0.137	0.528	112444	0
4	0	0.123	0.450	81322	0
	2	0.107	0.301	90671	0
	4	0.107	0.238	13073	0
5	1	0.0819	0.200	28993	0
	3	0.0839	0.169	10800	0
	5	0.0758	0.171	22740	0
6	0	0.0768	0.107	442	0
	2	0.0780	0.100	1179	0
	4	0.0760	0.0994	405	0
	6	0.0695	0.0880	398	0
7	1	0.0671	0.0750	121	0
	3	0.0654	0.0718	162	0
	5	0.0608	0.0681	201	0
	7	0.0550	0.0633	154	0

We next try abelian fields: for a fixed integer d, we pick ten random $n < 10^5$ such that $d \mid \phi(n)$, then apply the algorithm to all subfields of degree d of the cyclotomic field $\mathbb{Q}(\zeta_n)$.

d	average $t(K)$	$\max_K t(K)$	average $\log \Delta_K$	# of fields	# of bad fields
3	0.283	0.571	13.3	19	0
4	0.178	1.04	18.4	876	1
5	0.261	0.674	28.2	20	0
6	0.249	1.06	33.8	89	5
7	0.309	0.809	48.9	10	1
8	0.235	1.30	47.3	3198	97
9	0.147	0.435	49.4	40	0
10	0.236	0.903	54.6	89	5
15	0.264	0.800	112.7	39	3
20	0.365	1.38	126.8	256	30
30	0.390	1.52	201.4	257	43

We finish with pure fields: for each d, we pick ten integers α at random in $(-2^{16}, 2^{16}]$ such that $X^d - \alpha$ is irreducible. This time the discriminants are huge and the asymptotics speak: most fields are bad, but $t(K)$ remains way below 4.

d	average $t(K)$	$\max_K t(K)$	average $\log \Delta_K$	# of fields	# of bad fields
3	0.588	0.533	40.4	10	2
4	0.767	1.29	66.2	10	5
5	0.878	0.985	89.5	10	9
6	0.879	1.31	107.2	10	7
7	1.02	1.20	129.4	10	9
8	0.964	1.51	153.6	10	9
9	1.19	1.45	171.8	10	10
10	1.19	1.49	200.3	10	10
15	1.40	1.65	311.1	10	10
20	1.44	1.86	406.0	10	10
30	1.97	2.42	673.4	10	10

References

[Ba] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 355–380.

[Ba2] E. Bach, *Improved approximations for Euler products*, in *Number theory (Halifax, NS, 1994)*, Amer. Math. Soc., 1995, pp. 13–28.

[Bu] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, in *Séminaire de Théorie des Nombres, Paris 1988–1989*, Progr. Math., vol. 91, Birkhäuser, 1990, pp. 27–41.

[Co] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math. **139**, Berlin: Springer-Verlag (1996).

[dM] A.-C. de la Maza, *Bounds for the smallest norm in an ideal class*, *Math. Comp.* **71** (2002), no. 240, pp. 1745–1758.

[Ha] J. L. Hafner and K. S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, *J. Amer. Math. Soc.* **2** (1989), no. 4, pp. 837–850.

[La] S. Lang, *Algebraic Number Theory* second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[Mu] L. Murata, *On the magnitude of the least prime primitive root*, *J. Number Theory* **37** (1991), no. 1, pp. 47–66.

[NF] Number fields database, Bordeaux, available at `ftp://megrez.math.u-bordeaux.fr/pub/numberfields`.

[PARI] PARI/GP, version `2.2.10`, Bordeaux, 2005, `http://pari.math.u-bordeaux.fr/`.

[Po] G. Poitou, *Sur les petits discriminants*, Séminaire Delange-Pisot-Poitou (Théorie des Nombres) (1976/1977), no 6.

[We] A. Weil, Sur les "formules explicites" de la théorie des nombres premiers, *Comm. Sém. Math. Univ. Lund* **1952** pp. 252–265. Also in *Collected Papers* **II**, pp. 48–61, Berlin: Springer-Verlag (1979).

[Zi] R. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung*, *Invent. Math.* **62** (1981), no. 3, pp. 367–380.

Université Paris-Sud, Mathématiques Bât. 425, F-91405 Orsay, France
E-mail address: Karim.Belabas@math.u-psud.fr

Université de Bordeaux I, Mathématiques Pures, 351 Cours de la Libération, F-33405 Talence cédex, France
E-mail address: diaz@math.u-bordeaux1.fr

Departamento de Matemática, Universidad de Chile, Casilla 653, Santiago, Chile
E-mail address: friedman@uchile.cl