On the computation of class numbers of real abelian fields

by MSc Tuomas Hakkarainen
supervised by Prof. Tauno Metsänkylä
TUCS & University of Turku
tuheha@utu.fi
July 2006

Department of Mathematics
University of Turku
FI-20014 Turku
Finland

Turku Centre for Computer Science
Lemminkäisenkatu 14 A
FI-20540 Turku
Finland

Abstract

We give a procedure to search for odd prime divisors of class numbers of real abelian fields, excluding primes dividing the degree of the field. We show an extract of our table of odd primes < 10000 that divide the class numbers of fields of conductor < 2000. Cohen–Lenstra heuristics allow us to conjecture that no larger prime divisors should exist. Previous computational results have been mainly limited to prime power conductors.

Introduction

- Van der Linden [4] showed that the class number $h_K = 1$ for real fields K of prime conductor < 163 and $h_K = 4$ for $K = \mathbf{Q}(\zeta_{163} + \zeta_{163}^{-1})$. For composite conductors he presented results for some fields up to conductor 200. These results are the best known and it is difficult to go beyond these limits.
- Recently Schoof [5] computed class number divisors < 80000 for fields of prime conductor < 10000 and provided heuristics that predict these divisors to be class numbers.
- We apply Leopoldt's results on the rational decomposition of the class group and propose a method to compute class number divisors for fields of arbitrary conductor.

1 Leopoldt's result

Leopoldt in his thesis [3] presented an arithmetic characterization of a real abelian field, continuing work of Hasse. A main idea was to apply the Wedderburn decomposition of the rational (and p-adic) Galois group ring to the group of units of an abelian field. Leopoldt was able to reduce the study of the class groups of abelian fields with noncyclic Galois group essentially to the cyclic subfields corresponding to the classes of conjugate characters of the field.

$\mathbf{Q}[G]$-module: $Cl \simeq \cdots \oplus Cl^{e_{\widetilde{\chi}}} \oplus \cdots$

$\mathbf{Q}_p[G]$-module: $Cl \simeq \cdots \oplus (Cl^{e_{\chi_1}} \oplus \cdots \oplus Cl^{e_{\chi_s}}) \oplus \cdots$

$\overline{\mathbf{Q}}_p[G]$-module: $Cl \simeq \cdots \oplus (Cl^{e_{\chi}} \oplus \cdots \oplus Cl^{e_{\chi^k}}) \oplus \cdots$

Figure 1: Different levels of decomposition of the class group Cl

Notation

G: the Galois group of K
g: the order of G
f: the conductor of K
χ: a character of K
$\widetilde{\chi}$: a rational conjugacy class of characters ($\widetilde{\chi} = \{\chi^k \mid (k, g_\chi) = 1\}$)
g_χ: the order of χ
f_χ: the conductor of χ
K_χ: the subfield of K with character group $\langle\chi\rangle$
G_χ: the Galois group of K_χ
$\Phi_n(x)$: the nth cyclotomic polynomial

- Let E_χ be a subgroup of units of K_χ of norm ± 1 to any proper subfield and F_χ an explicitly given subgroup (the χ-cyclotomic units; see [3]) of E_χ. Both groups (modulo torsion ± 1) are cyclic $\mathbf{Z}[G_\chi]$-modules that only depend on $\widetilde{\chi}$.
- The class number admits the decomposition

$$h_K = \frac{Q_K}{Q_G} \prod_{\widetilde{\chi}} h_\chi$$

with the product running through the nontrivial rational conjugacy classes of characters and $h_\chi = [E_\chi : F_\chi]$. The rational integers Q_K and Q_G only contain primes dividing g.

2 The method

The outline of the method is as follows. We first put an upper bound for the primes p to be tested. We assume p is odd and not a divisor of the degree of K. We give a necessary but not sufficient condition for the divisibility of the class number and check the condition for all the primes and all the h_χ. We are left with a small set of primes to be checked further.

Then we present an additional technique to sieve out the primes not dividing the class number. Finally the remaining primes are proved to be actual class number divisors. This three-part verification procedure is necessary in order to preserve efficiency.

- This procedure is not capable of testing the divisibility of a higher pth power. But using similar methods and some elementary group theory we have given a generalization of the method to verify this also. We used an idea of G. and M.-N. Gras [1].

2.1 Schwarz's method

Schwarz [6] provided the following condition to effectively test the p-divisibility. Let $\zeta_n = e^{2\pi i/n}$.

Proposition 1 (Schwarz) *Let*

$$\lambda : (\mathbf{Z}/f_\chi\mathbf{Z})^\times \to \{0, \ldots, g_\chi - 1\}$$

be defined by $\chi(i) = \zeta_{g_\chi}^{\lambda(i)}$. If the prime $p \nmid 2 f_\chi g_\chi$ divides the h_χ-part of the class number of K_χ, then

$$\mathrm{GCD}_{\mathbf{F}_p[x]}\Big(\sum_{\substack{i=1 \\ (i,f_\chi)=1}}^{f_\chi - 1} a_i x^{\lambda(i)}, \Phi_{g_\chi}(x) \Big) \neq \overline{1},$$

where a_i are certain rational integers.

- This condition is efficient to check. In the computations we did, for any h_χ, the condition was satisfied on average for only 0 to 2 primes from all the odd primes < 10000 not dividing g_χ.

2.2 Second condition for p-divisibility

To check the remaining primes and the odd primes $p \mid f_\chi$, we continue as follows. We generalize an idea of van der Linden [4].

The group $(E_\chi/F_\chi)_p$ of elements of order p is an $\mathbf{F}_p[G_\chi]$-module isomorphic to $(E_\chi^p \cap F_\chi)/F_\chi^p$. If nontrivial, it must contain a minimal submodule of F_χ/F_χ^p. Since the intersection of two minimal submodules is zero, the p-exponent of h_χ is at least the number of minimal submodules F_i/F_χ^p satisfying $F_i \subseteq E_\chi^p$. Denote by η the generator of $F_\chi/\{\pm 1\}$.

Proposition 2 *Assume that $p \equiv 1 \pmod{g_\chi}$. The minimal $\mathbf{F}_p[G_\chi]$-submodules of F_χ/F_χ^p are $\langle \eta^{\Phi_{g_\chi}(\sigma)/(\sigma - i)} \rangle$, where i runs through all the zeros of $\Phi_{g_\chi}(x) \pmod p$ and σ is a generator of G_χ.*

- The proposition generalizes easily to all odd primes p not dividing g_χ.
- To check the condition, we choose a prime $q \equiv 1 \pmod{p f_\chi}$ and some $b \in \mathbf{Z}$ satisfying the conditions $b^{f_\chi} \equiv 1 \pmod q$, $b \not\equiv 1 \pmod q$. Then $\zeta_{f_\chi} \equiv b \pmod{\mathcal{Q}}$ for some prime ideal $\mathcal{Q}$ above q in $\mathbf{Q}(\zeta_{f_\chi})$. By writing $\eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ as a rational function $r(\zeta_{f_\chi})$, we examine whether

$$r(b)^{\frac{q-1}{p}} \equiv 1 \pmod q. \qquad (1)$$

If this congruence holds, we choose another pair (q, b) and repeat the test. Passing the test for many pairs is a strong evidence for the p-divisibility; failing the test means that $p \nmid h_\chi$.

2.3 Final verification

We show how to verify that $p \mid h_\chi$, following Gras [1]. For some $\alpha = \eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ satisfying (1) for many pairs (q, b), we want to prove that α is a pth power. This is equivalent to showing that $\sqrt[p]{\alpha}$ is an element of K_χ. As a unit of K_χ the element α has g_χ conjugates in K_χ which we all compute. We are able to calculate a real approximation of α and its conjugates α^σ.

If the polynomial $m_p(x) = \prod_\sigma (x - \sqrt[p]{\alpha^\sigma})$ has integral coefficients, then α is a pth power; by rounding off the coefficients we obtain the minimum polynomial of $\sqrt[p]{\alpha}$ if the precision is adequate. By checking whether $m_p(x) \mid m(x^p)$, where $m(x)$ is the minimum polynomial of α we arrive at the final conclusion.

The verification step is practical only for fields of small degree, but it was sufficient in all the cases we confronted.

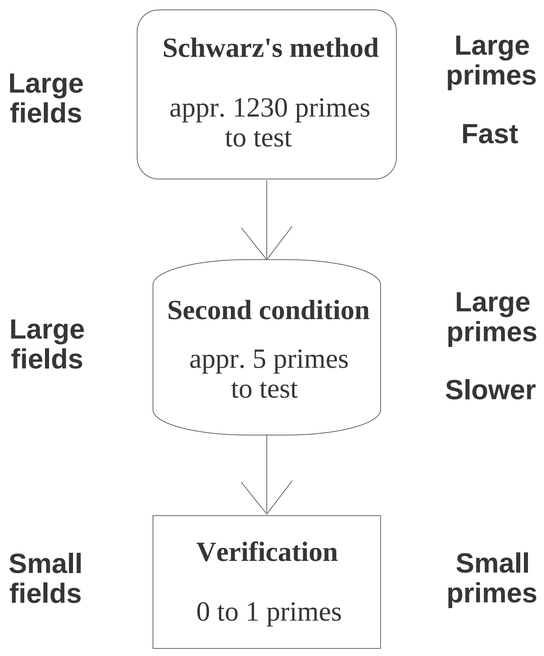

Figure 2: Scheme of computation for primes $p < 10000$ for any h_χ

3 Cohen-Lenstra heuristics

Cohen and Lenstra gave conjectural heuristic assumptions on the properties of finite modules over direct products of Dedekind domains. Schoof [5] predicted, based on a speculative extension of the Cohen–Lenstra heuristics, that the class numbers of real abelian fields of prime conductor most likely are relatively small. This generalizes to fields of arbitrary conductor without difficulty. We list some "probabilities" concerning our computations that arise from this heuristic approach.

- There are a total of 11018 different h_χ for fields of conductors < 2000. The predicted number of nontrivial h_χ-parts (excluding the primes dividing the degree and 2) would be 443. We found 231 nontrivial h_χ in the computations (49 of those were with f_χ prime; they can also be found in the tables in [5]).
- The "probability" that there are no prime divisors > 10000 of any h_χ is at least 91%. Since the largest prime divisor we found is 379 and since the prime divisors found were usually of the form $p = k g_\chi + 1$ with k small, we find it reasonable to believe that our table is a table of class number parts h_χ (omitting the prime divisors $p \mid 2 g_\chi$ from study).

4 Results of the computation

We computed prime divisors $2 < p < 10000$, $p \nmid g_\chi$ of any h_χ for fields up to conductor 2000. The complete table is in [2]; we provide here the class number divisors for fields of composite conductor < 1000. The conjugacy classes of characters are represented by characters of $(\mathbf{Z}/\mathbf{Z}_{f_\chi})^\times$.

f_χ	χ	g_χ	p
212	$\omega_4^1\chi_{53}^{13}$	4	5
316	$\omega_4^1\chi_{79}^{39}$	2	3
321	$\chi_3^1\chi_{107}^{53}$	2	3
427	$\chi_7^3\chi_{61}^{15}$	4	5
469	$\chi_7^3\chi_{67}^{33}$	2	3
473	$\chi_{11}^5\chi_{43}^{21}$	2	3
481	$\chi_{13}^2\chi_{37}^4$	18	19
551	$\chi_{19}^9\chi_{29}^7$	4	5
556	$\omega_4^1\chi_{139}^{23}$	6	7
568	$\chi_8^1\chi_{71}^{14}$	10	11
	$\omega_4^1\chi_8^1\chi_{71}^{35}$	2	3
629	$\chi_{17}^8\chi_{37}^2$	18	19
	$\chi_{17}^4\chi_{37}^{18}$	4	5
651	$\chi_3^1\chi_7^3\chi_{31}^6$	10	11
652	$\omega_4^1\chi_{163}^9$	18	19
676	$\omega_4^1\chi_{169}^3$	52	53
692	$\omega_4^1\chi_{173}^{43}$	4	5
697	$\chi_{17}^8\chi_{41}^{20}$	2	3
703	$\chi_{19}^9\chi_{37}^1$	36	37
	$\chi_{19}^3\chi_{37}^9$	12	13
728	$\chi_8^1\chi_7^3\chi_{13}^3$	4	5
753	$\chi_3^1\chi_{251}^{25}$	10	11
756	$\omega_4^1\chi_{27}^2\chi_7^1$	18	19

f_χ	χ	g_χ	p
763	$\chi_7^3\chi_{109}^9$	12	13
779	$\chi_{19}^9\chi_{41}^1$	40	41
785	$\chi_5^2\chi_{157}^{78}$	2	3
793	$\chi_{13}^1\chi_{61}^{55}$	12	37
808	$\omega_4^1\chi_8^1\chi_{101}^{25}$	4	5
817	$\chi_{19}^9\chi_{43}^{21}$	2	5
819	$\chi_9^1\chi_7^1\chi_{13}^2$	6	7
832	$\omega_4^1\chi_{64}^1\chi_{13}^3$	16	7^2
869	$\chi_{11}^5\chi_{79}^1$	78	79
889	$\chi_7^3\chi_{127}^{21}$	6	7
892	$\omega_4^1\chi_{223}^{111}$	2	3
916	$\omega_4^1\chi_{229}^{57}$	4	5
923	$\chi_{13}^3\chi_{71}^7$	20	61
928	$\omega_4^1\chi_{32}^1\chi_{29}^7$	8	17
935	$\chi_5^1\chi_{11}^5\chi_{17}^4$	4	5
940	$\omega_4^1\chi_5^2\chi_{47}^{23}$	2	3
944	$\omega_4^1\chi_{16}^1\chi_{59}^{29}$	4	5
976	$\omega_4^1\chi_{16}^1\chi_{61}^{15}$	4	5
980	$\omega_4^1\chi_5^1\chi_{49}^6$	28	29
985	$\chi_5^2\chi_{197}^{98}$	2	3
988	$\omega_4^1\chi_{13}^2\chi_{19}^3$	6	7
993	$\chi_3^1\chi_{331}^{165}$	2	3
999	$\chi_{27}^2\chi_{37}^{16}$	9	37

Conclusion

The class numbers of real abelian fields of composite conductor seem to show statistical behaviour similar to the class numbers of fields of prime conductor.

References

[1] G. and M.-N. Gras, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de* $\mathbf{Q}$, Bull. Sci. Math. (2) **101** (1977), no. 2, pp. 97–129.

[2] T. Hakkarainen, *On the computation of class numbers of real abelian fields*, submitted.

[3] H. W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat. 1953, no. 2 (1954), 48 pp.

[4] F. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), pp. 693–707.

[5] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), pp. 913–937.

[6] W. Schwarz, *Über die Klassenzahl abelscher Zahlkörper*, PhD Thesis, University of Saarbrücken (1995), 125 pp.