ON THE COMPUTATION OF CLASS NUMBERS OF REAL ABELIAN FIELDS (ABSTRACT OF POSTER)

TUOMAS HAKKARAINEN

Abstract. The class numbers of real abelian fields $K \subseteq \mathbf{Q}(\zeta_f + \zeta_f^{-1})$ have been investigated since Kummer. Yet, little has been known of their values for conductor $f \geq 71$. Recently R. Schoof presented an algorithm to compute divisors of class numbers when f is a prime, and produced a table of prime powers < 80000 dividing the class numbers for $f \leq 10000$. He also provided heuristics to predict that with 98% probability the computed factors are exactly the class numbers.

The heuristics easily generalize to fields with arbitrary conductor. We construct an effective procedure to compute class number divisors of real abelian fields of arbitrary conductor f by utilizing Leopoldt's results on the decomposition of the unit group. This decomposition allows to build up all the class numbers for a given conductor from a fixed set of factors that may be computed using techniques developed for fields of prime conductors. We choose an upper bound for primes to test. For natural reasons we have to exclude from the computation the prime 2 and the primes dividing the degree of the field K.

First we apply a result of W. Schwarz (1995) that gives a necessary condition for a prime to divide the class number. The condition is checked by gcd-computations of polynomials. On using this criterion we are left with a small set of primes to be handled further.

Then we apply a generalization of a method of van der Linden (1982) to give a second necessary condition for a prime to divide the class number. The method consists of a search for units that are pth powers. This amounts to checking a rational congruence relation modulo a set of prime numbers. This method is computationally more demanding than the first, thus it is essential to start the procedure by applying the first criterion.

Finally we prove that a prime satisfying the above conditions really divides the class number. To this end we compute the minimum polynomial of the unit found in the second step to prove that the unit is a pth power. The method is due to G. and M.-N. Gras (1977).

To check whether a higher prime power divides the class number, we present an additional technique that rests on the methods given above. This method is also based on the work of Gras.

As a result, we compute a table of class number divisors consisting of primes $p < 10000$ for fields of conductor $f \leq 2000$ and show using the heuristics that with 91% probability the table gives the class numbers (up to the excluded primes).

Department of Mathematics & TUCS - Turku Centre for Computer Science, University of Turku, FI-20014 Turku, Finland