An algorithm for verifying the p-part of the class group

Claus Fieker and Yinan Zhang

Technische Universität Kaiserslautern The University of Sydney

Why compute the class group?

The class group of a number field is a fundamental invariant of the field, and the ability to calculate it is an important task in number theory. Unfortunately, its computation is difficult and current implementations make use of the generalised Riemann hypothesis (GRH).

However, in certain areas of elliptic curves and Iwasawa theory, only the p-part of the class group is required. Here, an algorithm that could efficiently calculate only the p-part would be useful.

Verifying the p-part of the regulator can currently be achieved by the use of saturation, as first mentioned by Gras ([4]), but this still requires the assumption of GRH. Recent attempts to do this p-adically, such as by [1], are limited to only special examples, despite the fact that verification is theoretically possible for all totally real abelian fields.

Here, we present a method based on the p-adic class number formula to verify the p-part of the class group, without the need to assume GRH.

Classical results

If a totally real abelian number field K of degree n has class number h, p-adic regulator R_p, discriminant D with a group of corresponding Dirichlet characters X, then

$$\frac{2^{n-1}hR_p}{\sqrt{D}} = \prod_{\substack{\chi\in X\\ \chi\neq 1}} \left(1-\frac{\chi(p)}{p}\right)^{-1} L_p(1,\chi)$$

There are two closed formulae for evaluating $L_p(1,\chi)$. From Iwasawa [5]:

$$L_p(1,\chi) = -\left(1-\frac{\chi(p)}{p}\right)\frac{\sum_{a=1}^{f_\chi}\chi(a)\zeta^a}{f_\chi}\sum_{i=1}^{f_x}\overline{\chi}(i)\log_p(1-\zeta^{-i}) \qquad (1)$$

where χ has conductor f_χ and ζ a f_χ-th root of unity.

From Cohen [3]:

$$L_p(1,\chi) = \sum_{\substack{0\le a<m\\ (a,p)=1}}\chi(a)\left(-\frac{\log_p(a)}{m}+\sum_{j\ge 1}(-1)^j\frac{m^{j-1}}{a^j}\frac{B_j}{j}\right) \qquad (2)$$

where B_j is the j-th Bernoulli number and $m = \mathrm{lcm}(f_\chi, p)$ or $\mathrm{lcm}(f_\chi, 4)$ if $p = 2$.

Overview

We present an unconditional algorithm to verify the p-part of the class group for any totally real abelian field.

Implementation

For a totally real abelian field K with $n = \deg(K/\mathbb{Q})$, $L_p(1,\chi)$ is computed using either formula by the following method:

1. Find smallest f such that $K \subseteq \mathbb{Q}[\zeta_f]$.
2. Construct extension of $\mathbb{Q}_p$ containing f and n-th roots of unity.
3. Using Hensel lifting, construct f and n-th roots of unity.
4. Construct group of Dirichlet characters of conductor f with order n, using ζ_n.
5. Select the appropriate characters using class field theory.

From here, $L_p(1,\chi)$ is calculated using either formula 1 (Method 1) or formula 2 (Method 2).

This essentially gives us the p-adic value of hR_p. The p-part of R_p could be calculated in a similar way to [2], with saturation techniques required only at prime p. This provides a provable result for the p-part of h, which can be used to compute or verify the p-part of the class group.

Timing

To compute $L_p(1,\chi)$ with correct value modulo p^ρ, Method 1 is estimated to have complexity of order $f_\chi\rho^3d^2$, where $d = \mathbb{Q}_p[\zeta_n,\zeta_{f_\chi}]/\mathbb{Q}_p$; Method 2 has complexity of order $\mathrm{lcm}(f_\chi,p)\rho^3$. This answers the question from [3] regarding a comparison between the two methods.

Comparisons

In comparison to classical methods, there are two advantages for using this method to verify the class group:

- The p-adic value for hR_p can be computed exactly, unlike approximations to hR which assume convergence under GRH.
- Verification of R_p requires saturation at a single prime, as opposed to primes up to either the Bach (which assumes GRH, hence not provable) or the Minkowski (unconditional but exponential) bounds.

Examples

Example 1: Consider $f(x) = x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 715705x - 2921075$.

Here the Minkowski bound is 8125608241 and the class group ($\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, conductor 827) can be verified with the classical algorithm in around 160s (Magma v2.18-3). 2-adic verification would take only 1.5s.

Example 2: Now consider $f(x) = x^7 - x^6 - 10080x^5 + 167047x^4 + 26880800x^3 - 631101042x^2 - 16827155937x + 394878957903$.

By choosing a small enough bound, the unverified class group ($\mathbb{Z}/7\mathbb{Z}$, conductor 23521) can be computed in about 10s. The Bach bound is feasible, but the Minkowski bound ($\sim 10^{70}$) is simply too large. However, with this new p-adic implementation (which is not yet optimised), the 7-part of the class group can be verified in about 40s.

(Both examples use Method 2 to compute $L_p(1,\chi)$.)

Acknowledgements

The second author would like to thank his supervisor, Mark Watkins.

References

[1] Aoki, Miho; Fukuda, Takashi, *An algorithm for computing p-class groups of abelian number fields*. Algorithmic number theory, 56-71, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006.

[2] Biasse, Jean-François; Fieker, Claus, *New techniques for computing the ideal class group and a system of fundamental units in number theory*. To appear at ANTS X.

[3] Cohen, Henri, *Number theory. Vol. II. Analytic and modern tools*. Graduate Texts in Mathematics, 240. Springer, New York, 2007.

[4] Gras, Georges; Gras, Marie-Nicole, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de Q*. Bull. Sci. Math. (2) 101 (1977), no. 2, 97-129.

[5] Iwasawa, Kenkichi, *Lectures on p-adic L-functions*. Annals of Mathematics Studies, No. 74. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972.

Contact: y.zhang@sydney.edu.au

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN THE UNIVERSITY OF SYDNEY