AN APPLICATION OF THE p-ADIC ANALYTIC CLASS NUMBER FORMULA

CLAUS FIEKER AND YINAN ZHANG

Abstract. We propose an algorithm to compute the p-part of the class number for a number field $\mathbb{K}$, provided $\mathbb{K}$ is totally real and an abelian extension of the rational field $\mathbb{Q}$, and p is any prime. On fields of degree 4 or higher, this algorithm is theoretically faster than classical algorithms that compute the entire class number with improvement increasing with larger field degrees.

1. Introduction

The class group of a number field $\mathbb{K}$, which is the quotient of the group of invertible ideals modulo principal ideals, is one of the fundamental invariants of the field. It is of core importance to almost all multiplicative problems of number fields, therefore the ability to compute the class group of a number field $\mathbb{K}$ is an important task in algebraic number theory. Whilst there are conjectures about the structures of class groups, its computation is difficult and exisiting approaches to obtain provable results are slow. These either assume some generalised Riemann hypothesis, thus delivering results that are not proven, or make use of the Minkowski bound, which is computationally infeasible for most examples.

There are, however, circumstances where only the p-part of the class group is required. This is especially important in certain areas in Iwasawa theory and elliptic curves, where they are used in descents to find rational points on elliptic curves. Here, it would be useful to have an algorithm that could efficiently compute only the p-part.

Whilst there has been approaches to this problem in the past, including attempts by Gras and Gras [4], much progress has been made in the past fifteen years, including most recently work by Aoki and Fukuda [1], which presented an algorithm for the case when p does not divide the field degree of $\mathbb{K}$ and $p \neq 2$. None of these algorithms, though, can deal with all fields $\mathbb{K}$ which are abelian extensions of the rational field $\mathbb{Q}$, despite a theoretical result from Leopoldt showing that this is possible [5, Section 5.5].

In this paper we propose a new algorithm to compute the p-part of the class number for any totally real abelian number field $\mathbb{K}$ and prime p. The result is unconditional and can be used to verify the the p-part of the class group. Just as classical algorithms use the class number formula for their computation, this algorithm makes use of the p-adic version of the formula. Whilst this may not be the most efficient way to approach the problem, this does present a unconditional method that runs in polynomial time of the conductor of the field.

The computation of the p-part of the class number, apart from few special cases, is usually done through a computation of the structure of the full class group using a variation of Buchmann's subexponential algorithm. The method essentially

proceeds in two steps: first, a (small) finite set of prime ideals is chosen. The algorithm then proceeds to determine the subgroup of the class group generated by those ideals. In a second step the choice of the initial ideals is verified by checking all prime ideals of norm bounded by some bound. Depending on the application, the bound can be of size $O((\log |D|)^2)$, where D is the discriminant of the number field, in case the Riemann hypotheses are assumed or of size $O(\sqrt{|D|})$ for unconditional results. As a consequence, in non-trivial examples, the running time is overwhelmingly dominated by the verification step. In this paper, we propose a new method that can verify the p-part of the class number in time polynomial in $O(\sqrt[n-1]{|D|})$ for cyclic fields of prime degree n. This allows an asymptotically much faster unconditional verification than any previously known method. At the end of the paper, we produce examples showing the approach to be practical as well.

2. Computing p-adic L-functions

We start by reviewing the necessary tools from p-adic fields and p-adic analysis that we are going to need. Let p be a prime number. Denote by $\mathbb{Q}_p$ the field of rational p-adic numbers, with the usual p-adic norm $|.|_p$ and valuation v_p. Let $\overline{\mathbb{Q}_p}$ be the algebraic closure of $\mathbb{Q}_p$, and $\mathbb{C}_p$ the topological closure of $\overline{\mathbb{Q}_p}$ with respect to $|.|_p$.

Definition 2.1. Let the p-adic logarithm $\log_p$ be given by

$$\log_p(1+X) = \sum_{i=1}^{\infty} \frac{(-1)^{i+1} X^i}{i}$$

The series has a radius of convergence of 1, so the domain of $\log_p(x)$ is $T = \{a \in \mathbb{C}_p \mid |x-1|_p < 1\}$.

Proposition 2.2. *Let $x \in \mathbb{C}_p^\times$. Then we can write*

$$x = p^r \omega t$$

Where r is some rational number, ω is a root of unity of order prime to p, and $t \in T$.

Proposition 2.3. *Let $x = p^r \omega t$ as defined by the previous proposition. Then*

$$\log_p(x) := \log_p(t)$$

is the unique extension of $\log_p$ from T onto $\mathbb{C}^\times$.

Remark 2.4. The above logarithm commutes with Frobenius endomorphism, which maps elements in a commutative ring of characteristic p to their p-th powers.

Definition 2.5. A Dirichlet character, χ, is a multiplicative homomorphism $\chi : (\mathbb{Z}/k\mathbb{Z})^\times \to \mathbb{C}^\times$.

As χ can also be considered as a multiplicative homomorphism on $(\mathbb{Z}/m\mathbb{Z})^\times$ if $k|m$, let the minimal of such k be called the conductor of χ, denoted f_χ.

Definition 2.6. Let χ be a Dirichlet character. Its conjugate character, $\overline{\chi}$, is defined as

$$\overline{\chi}(a) = \begin{cases} \frac{1}{\chi(a)} & \text{if } \chi(a) \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

The L–series attached to a Dirichlet character χ is given by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

if $\Re(s) > 1$.

Apart from a pole at $s = 1$ when χ is the trivial character, this series can be analytically continued to the entire complex plane. This continuation is the Dirichlet L-function.

There are several approaches to construct the p-adic analogue of Dirichlet L-functions. One method relies on the fact that $L(s,\chi)$ is algebraic for negative integers s, and these values can be considered as elements of $\overline{\mathbb{Q}_p}$. From this one can look for a p-adic function that obtains the same values at negative integers as $L(s,\chi)$, and with some modifications, such a function can be found and proven to be unique. This function is the p-adic L-function $L_p(s,\chi)$. A more detailed explanation can be found in [5, Section 3] and [7, Chapter 5].

There is a formula for evaluating $L_p(1,\chi)$, given by [5, Section 5 Theorem 3]

Theorem 2.7. *Let χ be an even character with conductor f_χ, and ζ a primitive $f\chi$-th root of unity. If χ is the trivial character then $L_p(s,\chi)$ has a pole at $s = 1$. Otherwise*

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

Note that $\sum_{a=1}^{f_\chi} \chi(a)\zeta^a$ is a Gauss sum.

This formula can be used for our calculations. A key problem in using the above formula is the need for the computation of p-adic logarithms of arbitrary elements - the straight forward power series is only valid for 1-units, ie. elements in $1 + p\mathbb{Z}_K$. The naive use of Proposition 2.3 would require to extend the field which we want to avoid.

Algorithm 2.8. *Computation of the p-adic logarithm of an arbitrary element x.*

Input: x
Output: $\log x$

1: $k := v_p(x)$ *and* $y := \pi^{-k}x$
2: $z := y^{n-1}$ *where* $n := \#\mathbb{F}$ *for the residue class field* $\mathbb{F}$
3: *use the power series to compute* $\log z$ *and* $\log y := 1/(n-1)\log z$
4: $\epsilon := \pi^e/p$
5: *return* $\log x = \frac{k}{e}\log\epsilon + \log y$

Theorem 2.9. *The above code returns the same result as Proposition 2.3.*

Proof. We know that x can be rewritten as $p^r\omega t$. Let e be the ramification index of $\mathbb{Q}_p(x)/\mathbb{Q}_p$, and the valuation of x be v. Then we have $r = \frac{v}{e}$.

Let π be a uniformising element of $\mathbb{Q}_p(x)$, that is, an element with valuation 1. Then $\pi^e = p\epsilon$, for some unit ϵ. Using this fact we compute ϵ. Now, we redefine x so that

$$x = p^{\frac{v}{e}}\omega t\pi^{-\frac{v}{e}} = p^{\frac{v}{e}}t(p\epsilon)^{-\frac{v}{e}} = t\epsilon^{-\frac{v}{e}}$$

Taking $\log_p$ of both sides, we get

$$\log_p(x) = \log_p(t\epsilon^{-\frac{v}{e}}) = \log_p(t) - \frac{v}{e}\log_p(\epsilon)$$

Since $\log_p(x) = \log_p(t)$, we need to add a correction factor of $\frac{v}{e}\log_p(\epsilon)$ to return the correct value, and this completes our algorithm. □

Recall that this logarithm commutes with the Frobenius endomorphism. This allows faster computations of the terms $\log_p(1-\zeta^{-i})$ by making use of the Frobenius endomorphism (where applicable) to reduce the number of logarithms calculated, which is in general computationally tedious.

We need to construct a field that enables us to compute $L_p(1,\chi)$. Since the calculation requires two roots of unity of possibly different degrees we must perform the computation in a cyclotomic extension field of $\mathbb{Q}_p$. According to Theorem 2.7 a primitive f_χ-th root of unity, ζ, is required. In addition to this, to be able to construct the Dirichlet character χ, we also need a primitive l-th root of unity, where l is the order of χ.

We start with $\mathbb{Q}_p$. In order to generate both ζ and χ we need a root of unity of order $\mathrm{lcm}(f_\chi, l)$. We can write

$$\mathrm{lcm}(f_\chi, l) = p^r o$$

where p and o are relatively prime. To obtain the necessary extension field, we first take an unramified extension on $\mathbb{Q}_p$ to obtain $\mathbb{Q}_p[\zeta_o]$, then take a ramified extension on this new field to obtain one with the necessary root of unity.

We have essentially two natural options when constructing the unramified extension of $\mathbb{Q}_p$ of degree o. In one approach we can take the defining polynomial of the default degree o extension of the residue class field of $\mathbb{Q}_p$. In this case we have a defining polynomial with small coefficients, but no natural o-th root of unity. This is overcome by performing Hensel lifting to obtain $\mathbb{Q}_p[\zeta_o]$, a method analogous to using the Newton-Raphson method to find roots of polynomials in $\mathbb{R}$.

Alternatively, instead of using the default defining polynomial for the residue class extension, we can use an appropriate p-adic factor of the o-th cyclotomic polynomial. This construction provides us with ζ_o as the default element of the unramified extension, but with a defining polynomial with many terms and large coefficients. It does, however, allow faster Frobenius automorphisms. It is not clear at this point in time which of the two approaches is faster.

We now estimate the complexity of the computation. Suppose that $d_f = \mathbb{Q}_p[\zeta_{f_\chi}]/\mathbb{Q}_p$ and $d = \mathbb{Q}_p[\zeta_n, \zeta_{f_\chi}]/\mathbb{Q}_p$. Using classical algorithms for multiplication and division, we find that to perform the logarithms required with correct value modulo p^ρ would require performing ρ calculations at a complexity in the order of $d_f^2\rho^2$. The remaining multiplication has complexity of $d^2\rho^2\log^2 p$, giving an overall complexity of order $f_\chi\rho^3 d^2$.

3. An Alternative Approach

In this section we provide an alternate approach to compute $L_p(1,\chi)$, based on a formula from [3, Proposition 11.3.8].

Theorem 3.1. *Let χ be a primitive character of conductor f_χ, let $m = \mathrm{lcm}(f_\chi, q_p)$, where $q_p = 4$ if $p = 2$ and p otherwise. If χ is a non trivial character then $L_p(1,\chi)$ is given by the following formula*

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

where B_j is the j-th Bernoulli Number.

Proposition 3.2. *The infinite sum*

$$\sum_{j\ge 1}(-1)^j \frac{m^{j-1}}{a^j}\frac{B_j}{j}$$

converges with respect to $|.|_p$

Proof. Let s_j be the j-th term of the sequence. Since $|.|_p$ is a non-Archimedian norm it is sufficient to show that $\lim_{j\to\infty} s_j = 0$.

Consider the valuation of the individual terms in s_j. Since $(a,p)=1$,

$$v_p(s_j) = v_p(m^{j-1}) + v_p(B_j) - v_p(j)$$

We want to show that $v_p(s_j)\to\infty$ as $j\to\infty$. We do this by finding the upper bound of $v_p(s_j)$, using a result from [7, Theorem 5.10].

Lemma 3.3 (von Staudt-Clausen theorem)**.** *Let B_j be a Bernoulli number. Then the fractional part of B_j is given by*

$$\sum_{(p-1)|j}\frac{1}{p}$$

Suppose $v_p(m)=r$. Then $v_p(m^{j-1}) = r(j-1)$. By the above lemma, $v_p(B_j)\ge -1$, since B_j contains at most a single factor of p in its denominator. Also, $v_p(j)\le \frac{\log j}{\log p}$, so we have

$$v_p(s_j) \ge r(j-1) - \frac{\log j}{\log p} - 1$$

From here is is clear that $v_p(s_j)\to\infty$ as $j\to\infty$, and $|s_j|_p\to 0$, which completes our proof. □

Corollary 3.4. *For the infinite sum to have the correct value modulo p^ρ, we need to sum up to the smallest j such that*

$$\rho < v_p(m)(j-1) - \frac{\log j}{\log p} - 1 \tag{3.1}$$

To be able to compute using this formula we need to know how many terms of the infinite sum we need to calculate to guarantee correctness up to a given precision.

Proposition 3.5. *For sufficiently large ρ calculating the partial sum of s_j up to $j = \frac{2\rho+1}{v_p(m)} + 1$ provides the correct result modulo p^ρ.*

Proof. We need to show $j = \frac{2\rho+1}{v_p(m)} + 1$ satisfies inequality 3.1. Substituting the value for j we obtain

$$\begin{aligned}
& v_p(m)(j-1) - \frac{\log j}{\log p} - 1 - \rho \\
=& \rho - \frac{\log(\frac{2\rho+1}{v_p(m)} + 1)}{\log p} \\
\geq& \rho - \frac{\log(2\rho+2)}{\log p} && \text{since } v_p(m) \geq 1 \\
=& \rho - \frac{\log 2 + \log(\rho+1)}{\log p}
\end{aligned}$$

Consider this as a function in ρ. As it is monotonically increasing for $\rho > 0$ then it is positive when $\rho > k$ for some integer k, showing that it satisfies the condition in Corollary 3.4. □

Remark 3.6. In the case of $p = 2$ and 3, $k = 3$ and 1 respectively. For all other primes p, $k \leq 0$, so $j = \frac{2\rho+1}{v_p(m)} + 1$ could be used for almost all cases.

In practice, one can achieve a better bound on j by solving the inequality 3.1 for the particular m, p and ρ values.

We can thus compute $L_p(1, \chi)$ using this formula. The calculation is mostly straightforward, with some caching of repeated terms such as the logarithms and Bernoulli numbers to speed up calculation.

Again, using classical algorithms for multiplication and division, we can analyse the complexity of the computation. To compute the infinite sum with correct value modulo p^ρ we need to perform at most $2\rho + 2$ additions, each of which has complexity of roughly ρ^2, giving a complexity of the order of ρ^3 for this part. There are $\operatorname{lcm}(f_\chi, q_p)$ additions in the formula, each of order ρ, giving a total complexity of order $\operatorname{lcm}(f_\chi, q_p)\rho^3$.

Comparing the complexities of the two approaches, we see that in addition to the common ρ^3 term, the method based on Theorem 2.7 is dependent on $f_\chi d^2$ whilst the approach based on Theorem 3.1 is related to $\operatorname{lcm}(f_\chi, q_p)$. Thus in the case where the degree of the p-adic field constructed is small, the first approach will be faster, the second method would be superior if p is a factor of f_χ. In general no single approach is superior, and we shall see some examples of these later.

4. p-adic Regulator

Suppose $\mathbb{K}$ is a totally real number field, with field degree n. Then the structure of the unit group of $\mathbb{K}$, $U_\mathbb{K}$, can be represented as $C_k \times \mathbb{Z}^{n-1}$, where C_k is a finite cyclic group.

A system of fundamental units of $U_\mathbb{K}$ is a set of units that form a basis of $U_\mathbb{K}$, modulo torsion. Let $u_1, \ldots, u_{n-1}$ be such a system. Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of $\mathbb{K}$ into $\mathbb{R}$. Then for any rational integer such that $\log_p(u_n) \neq 0$, the p-adic regulator of $\mathbb{K}$, R_p, is defined to be

$$(n \log_p(u_n))^{-1} \det[\log_p |\sigma_j(u_i)|]_{ij}$$

Since the embeddings do not affect the rational number u_n, this simplifies to the following expression

$$\frac{1}{n}\det\begin{bmatrix} \log|\sigma_1 u_1| & \cdots & \log|\sigma_n u_1| \\ \vdots & \ddots & \vdots \\ \log|\sigma_1 u_{n-1}| & \cdots & \log|\sigma_{n-1} u_{n-1}| \\ 1 & \cdots & 1 \end{bmatrix}$$

Thus, for any system of independent units we can easily compute the p-adic regulator from there. All we need are the different p-adic embeddings, but they are either trivial to compute using standard techniques for p-adic factorisation or root finding, or else, make use of the $\mathbb{Q}$-automorphisms of the field and one fixed p-adic embedding. We note that typically the units are not represented with respect to a fixed basis of the field, but as power products $u_i = \prod_{j=1}^{r} \alpha_j^{e_{i,j}}$ for some (small) elements α_i and some (large) exponents $e_{i,j} \in \mathbb{Z}$. While the computation of logarithms of power products is of course trivial, we note that this requires the computation of logarithms of non-units; although u_i is a unit, the α_i are not.

Therefore to get the valuation of the p-adic regulator we need a basis for some p-maximal subgroup of the unit group, ie. we need $V < U$ such that $(U : V) < \infty$ and $p \nmid (U : V)$. Using saturation techniques such a group V can be computed from any subgroup $\tilde{V}$ of full rank. In particular for abelian fields of moderate conductor, we can obtain such a group $\tilde{V}$ from the cyclotomic units of the surrounding cyclotomic field, thus to fields of degree too large for the direct computation using class groups.

5. Main result

There is a link between the p-adic L-function and the p-adic regulator of a number field [7, Theorem 5.24].

Definition 5.1. Let X be a finite group of Dirichlet characters. Denote by f the lowest common multiple of the conductors of all the characters in X. Let H be the intersection of the kernels of all characters in X, and $\mathbb{K}$ the fixed field H in $\mathbb{Q}[\zeta_f]$. Then X is the set of Dirichlet characters corresponding to the field $\mathbb{K}$.

Corollary 5.2. *X is a subgroup of the characters of* $\mathrm{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q})$*. In fact, X is isomorphic to* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*, and the degree of $\mathbb{K}/\mathbb{Q}$ is the order of X.*

Theorem 5.3. *Suppose $\mathbb{K}$ is a totally real abelian number field, with discriminant D, regulator R_p and class number h. Let its group of corresponding Dirichlet characters be X. Then*

$$\frac{2^{n-1} h R_p}{\sqrt{D}} = \prod_{\substack{\chi \in X \\ \chi \neq 1}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi) \tag{5.1}$$

where n is the field degree of $\mathbb{K}$, up to choice of sign for $\sqrt{D}$.

For each required component in the formula we have already highlighted their computations in the earlier sections. However, we still need to find X to be able to evaluate $L_p(1, \chi)$. We start by computing the minimal f so that $\mathbb{K} \subseteq \mathbb{Q}[\zeta_f]$. If $\mathbb{K}$ is already a cyclotomic field, where we simply take all even characters of conductor f that are non trivial. Note: since f, the conductor, can be large in relation to the degree, we do not want to compute $\mathbb{Q}(\zeta_f)$ explicitly. Also, since

we start with K, we do not have any embedding into $\mathbb{Q}(\zeta_f)$ explicitly, so we want to compute X without explicitly using the full cyclotomic field. Otherwise, we start with characters of conductor f with order $\deg(\mathbb{K}/\mathbb{Q})$. Any further restrictions depends on the field in question, in particular the value of f.

If the field is cyclic and f is prime then the characters required are only the primitive ones. However, if f is not prime, then the primitive elements would correspond to the different fields with the same f. In this case we would need to be able to select the ones corresponding to the field in question.

We start with $\mathrm{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q})$, which is isomorphic to $(\mathbb{Z}/f\mathbb{Z})^\times$. Let $U = \mathrm{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{K})$. Now consider the projection

$$\mathrm{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$$

The kernel of the projection is U, and the characters corresponding to $\mathbb{K}$ should have the preimage of U in their kernel.

From class field theory,

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong Cl_f/H$$

where Cl_f is the ray class field of modulo f, and H is $\langle N_{F/\mathbb{K}}(a)\rangle$. With knowledge of Cl_f and $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, we can compute H by taking the norm of primes until we reach the appropriate size for Cl_f/H. From here we can find the generators of the kernel of H, under the projection stated earlier. By testing the characters on the generators we restrict our set of characters to only those that are trivial on the generators.

Since we can compute every part of equation 5.1 except h, we can easily compute h using this formula and find its valuation, which will give the p-part of h.

In the classical algorithm to compute the entire class group, the unconditional verification of the computation requires $O(\sqrt{|D|})$ [2, Algorithm 6.5.6] steps. The proposed algorithm requires the computation of approximately f steps. By the conductor-discriminant formula [6, Chapter VII 11.9], we know that for a number field $\mathbb{K}$ with prime degree n, D is of the magnitude f^{n-1}. This means that theoretically the proposed algorithm would be faster than the existing algorithms for number fields of degree 4 or higher, with improvement increasing for larger n. When only the p-part of the class group is required this would yield a faster computation.

6. Examples

All calculations were performed in Magma V2.18-3, with default precision of 20. ζ values are given with a precision of 10 to simplify their expressions.

Example 1 Let $\mathbb{K} = \mathbb{Q}[\xi]$ where ξ is a root of $x^3 - 273x - 1729$, and $p = 3$. We find that $\mathbb{K}$ is a subfield of $\mathbb{Q}[\zeta_{819}]$, with $\zeta =$ `(4*$.1^5 - 2*$.1^4 + 2*$.1^3 + 2*$.1^2 + 3*$.1 + 4)*$.1 + 4*$.1^5 - 2*$.1^4 + 2*$.1^3 + 2*$.1^2 + 3*$.1 + 4`. This calculations yields a zeta function value of `-126233993*3` and a p-adic regulator value of `-1001*3^2`. The valuation of the class number is 2, which matches with $h = 9$.

Example 2 Let $\mathbb{K} = \mathbb{Q}[\xi]$ where ξ is a root of $x^5 - x^4 - 312x^3 + 531x^2 + 9397x + 10933$, and $p = 5$. We find that $\mathbb{K}$ is a subfield of $\mathbb{Q}[\zeta_{781}]$, with $\zeta =$ `17*$.1^4 - 35*$.1^3 - 4*$.1^2 - 42*$.1 - 16`. This calculations yields a zeta function value of `-5069186272204*5^5` and a p-adic regulator value of `3243922906*5^8`. The valuation of the class number is 1, which matches with $h = 5$.

The following are a table of the valuations of h of different number fields $\mathbb{K} = \mathbb{Q}[\xi]$, where ξ is a root of the polynomial $f(x)$. Timings for the calculation using the method from Theorem 2.7 to calculate $L_p(1,\chi)$ are given under the label I (Iwasawa), and C (Cohen) when Theorem 3.1 is used instead. Timings are given in seconds.

$f(x)$	p	$v_p(h)$	I	C	h
$x^3 - x^2 - 72x - 209$	11	0	0.718	1.264	3
$x^5 - 341x^3 - 2046x^2 + 6820x + 29667$	5	1	1.342	0.936	5
$x^3 - x^2 - 184x + 512$	3	1	2.012	0.499	3
$x^3 - x^2 - 292x - 1819$	7	1	23.088	2.917	7
$x^5 - 410x^3 - 205x^2 + 39360x + 3649$	5	1		1.170	5
$x^5 - x^4 - 76x^3 + 359x^2 - 437x + 155$	11	1	0.983	1.451	11
$x^5 + x^4 - 508x^3 - 6965x^2 - 33107x - 52571$	11	1	17.722	9.032	55
$x^3 - 2109x - 37259$	3	3		2.419	27

Now suppose $f(x) = x^5 - x^4 - 376x^3 - 3877x^2 - 13445x - 15271$. Existing algorithm computes the class number of $\mathbb{K}$ as 16 in 2.356 seconds. Both p-adic methods verify that the 2-part of the class number is the same, with the Cohen method returning a result in 1.732 seconds, a small improvement over the existing algorithm.

References

[1] Aoki, Miho; Fukuda, Takashi, *An algorithm for computing p-class groups of abelian number fields*. Algorithmic number theory, 5671, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006

[2] Cohen, Henri, *A course in computational algebraic number theory* Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[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.

[6] Neukirch, Jürgen, *Algebraic number theory*. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G Harder. Grundlehren der Mathematischen Wissenschaften, 322. Springer-Verlag, Berlin, 1999.

[7] Washington, Lawrence C. *Introduction to cyclotomic fields*. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

Technische Universität Kaiserslautern
E-mail address: fieker@mathematik.uni-kl.de

The University of Sydney
E-mail address: y.zhang@sydney.edu.au