AN APPLICATION OF THE \( p \)-ADIC ANALYTIC CLASS NUMBER FORMULA

CLAUS FIEKER AND YINAN ZHANG

Abstract. We propose an algorithm to verify the \( p \)-part of the class number for a number field \( K \), provided \( K \) 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 quotient of the group of invertible ideals of a number field \( K \), modulo principal ideals, is the class group of \( K \), denoted by \( \text{Cl}_K \). It is one of the fundamental invariants of the field, and of core importance to almost all multiplicative problems of number fields. As a result, the ability to compute \( \text{Cl}_K \) is an important task in algebraic number theory. Whilst there are conjectures about the structures of class groups, its computation is difficult and existing 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 Minkowski type bounds, 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 [8], much progress has been made in the past fifteen years, including most recently work by Hakkarainen [9], which focused on an algorithm to find prime divisors of class numbers, and Aoki and Fukuda [1], whose algorithm was more focused on \( p \)-adic decomposition of the class group. Both algorithms require the condition that \( p \) does not divide the field degree of \( K \) and \( p \neq 2 \), problematic as given a fixed degree, genus theory indicates that there are infinitely many fields with class number divisible by the degree. This prevents them from dealing with all fields \( K \) which are abelian extensions of the rational field \( \mathbb{Q} \), despite a theoretical result from Leopoldt showing that this is possible [10, 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 \( K \) and prime \( p \). The result is unconditional and can be used to verify 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 implement a \( p \)-adic algorithm to compute the \( p \)-part of the class

2010 Mathematics Subject Classification. Primary 11S40. Secondary 11-04, 11Y35, 11Y70.
group, this does present an 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 the 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 $O(\log^2 |D|)$, where $D$ is the discriminant of the number field, in the case where the generalised Riemann hypothesis is assumed, or of size $O(\sqrt{|D|})$ for unconditional results. As a consequence the running time is overwhelmingly dominated by the verification step in all but the trivial examples. In this paper, we propose a new method that can verify unconditionally the $p$-part of the class number in time polynomial in $O(n^{-1}\sqrt{|D|})$ 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. $p$-adic class number formula

Our algorithm is based on the $p$-adic class number formula, which provides a link between the $p$-adic $L$-function, the $p$-adic regulator and class number of a number field [12, Theorem 5.24].

**Theorem 2.1.** Suppose $K$ 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

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

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

Provided we are able to compute $L_p(1, \chi)$ for the required characters and $R_p$, it is possible for us to calculate $h$. To do so we make use of two formulae for computing $L_p(1, \chi)$. The first one, [7, Theorem 11.5.37], is a closed formula in terms of $(p$-adic) logarithms, similar to the formula for $L(1, \chi)$:

**Theorem 2.2.** Let $\chi$ be an even character with conductor $f_\chi$, and $\zeta$ a primitive $f_\chi$-th root of unity. If $\chi$ is the trivial character then $L_p(s, \chi)$ has a pole at $s = 1$. Otherwise

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

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

The second, [7, Proposition 11.3.8], is a convergent series:
Theorem 2.3. Let $\chi$ be a primitive character of conductor $f_\chi$, let $m = \text{lcm}(f_\chi, q_p)$, where $q_p = 4$ if $p = 2$ and $p$ otherwise. If $\chi$ is a non trivial character then $L_p(1, \chi)$ is given by the following formula

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

where $B_j$ is the $j$-th Bernoulli Number.

The main steps in computing the $p$-adic $L$-functions involve computing $p$-adic logarithm and creation of the $\mathbb{Q}_p$ extension fields required for parts of the formula. In addition, the appropriate characters for $K$ have to be selected, and $R_p$ calculated. We shall define these formally as we come to compute them.

3. Computing $p$-adic $L$-functions

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 $|.|_p$.

3.1. $p$-adic logarithm. Evaluating $L_p(1, \chi)$ requires the use of the $p$-adic logarithm, $\log_p$, in both cases. It is defined by the usual power series expansion

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

Here the series has a radius of convergence of 1, so the domain of $\log_p(x)$ is $U_1 = \{a \in \mathbb{C}_p \mid |x - 1|_p < 1\}$.

It is possible to extend this logarithm to $\mathbb{C}_p^\times$. We know that by [12, Proposition 5.4] that any element $x \in \mathbb{C}_p^\times$ can be written as

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

where $r$ is some rational number, $\omega$ is a root of unity of order prime to $p$, and $u \in U_1$, and that there is a unique extension of $\log_p$ from $U_1$ to $\mathbb{C}_p^\times$ given by

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

Remark 3.1. The above logarithm commutes with Frobenius endomorphism, which maps elements in a commutative ring of characteristic $p$ to their $p$-th powers.

A key problem in computing $L_p(1, \chi)$ is the need for the computation of $p$-adic logarithms of arbitrary elements - the straightforward power series is only valid for 1-units, that is, elements in $1 + p\mathbb{Z}_K$. The naive use of the definition would require us to extend the field which we want to avoid. As $r$ is rational ($r = a/b$), the field needs to be extended to contain a uniformising element of valuation $(1/b)$.

Algorithm 3.2. Computation of the $p$-adic logarithm of an arbitrary element $x$.

Input: $x$

Output: $\log_p x$

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

Proof. We know that \( x \) can be rewritten as \( p^r \omega u \). 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 \( \pi \) be a uniformising element of \( \mathbb{Q}_p(x) \), that is, an element with valuation 1. Then \( \pi^e = p \varepsilon \), for some unit \( \varepsilon \). Using this fact we compute \( \varepsilon \). Now, we rewrite \( x \) so that

\[
x = p^{\frac{v}{e}} \omega u \pi^{-\frac{v}{e}} = p^{\frac{v}{e}} u (p \varepsilon)^{-\frac{v}{e}} = u \varepsilon^{-\frac{v}{e}}
\]

Taking \( \log_p \) of both sides, we get

\[
\log_p (x) = \log_p (u \varepsilon^{-\frac{v}{e}}) = \log_p (u) - \frac{v}{e} \log_p (\varepsilon)
\]

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

\[\square\]

Recall that this logarithm commutes with the Frobenius endomorphism. This allows faster computations of the terms \( \log_p (1 - \zeta^{-i}) \) in Theorem 2.2 by making use of the Frobenius endomorphism (where applicable) to reduce the number of logarithms calculated, which is in general computationally tedious.

We can also evaluate \( 1/p^l \log_p (1 + X)^p \) instead of \( \log_p (1 + X) \). This reduces the number of terms that need to be computed from the power series, as it now converges more quickly due to larger valuations. However, this comes at the expense of requiring additional precision for the division by \( p^l \). For each explicit example we can calculate the optimal value of \( l \) for the logarithm computation.

An example of this is when \( p = 3 \) and \( \zeta \) is an 1423-th root of unity. The time taken to compute \( \log_p (1 - \zeta^{-1}) \) takes around 53 seconds without this optimisation (that is, \( l = 0 \)), decreasing to 27 seconds when \( l = 15 \) before increasing again with larger values of \( l \).

Bernstein outlined a fast algorithm for logarithm [2] which may be used here. This, along with other fast algorithms for logarithms, are intended for calculations requiring high precision (at least several thousand digits) and it is not clear whether this is required for our algorithm.

3.2. \( \mathbb{Q}_p \) extension field creation. We need to construct a field that enables us to compute \( L_p(1, \chi) \). Both approaches require roots of unity, either explicitly in the calculation or for the construction of the Dirichlet character \( \chi \). This calls for a cyclotomic extension of \( \mathbb{Q}_p \). Suppose we need an \( o \)-th root of unity for the calculations. We can write

\[
o = p^{v_p(o)} c
\]

so that \( p \) and \( c \) are relatively prime. The value of \( c \) and valuation of \( o \) determines whether we need a ramified or unramified extension, or possibly both.

The following algorithm constructs the necessary extension.

\textbf{Algorithm 3.3. Construction of an extension field of } \mathbb{Q}_p \text{ containing a } o \text{-th root of unity}\n
\textbf{Input: } o, \mathbb{Q}_p

\textbf{Output: } \mathbb{Q}_p[\zeta_o]

1: \( c := o \mod p^{v_p(o)} \)
2: \( f := \text{ order of } p \mod c \text{ or } 1 \text{ if } c = 1 \)
3: Construct $T$, unramified extension of $\mathbb{Q}_p$ of degree $f$

4: If $v_p(o) > 0$, $g(x) := ((x + 1)^p - 1)/(x)$

5: Construct $S$, totally ramified extension of $T$ defined by $g(x)$

6: If $v_p > 1$ then $h(x) := g(x + 1)^{v_p(o) - 1} - \pi - 1$, where $\pi$ is an uniformiser

7: Construct $R$, totally ramified extension of $S$ defined by $h(x)$

This is achieved through the construction of the intermediate fields below:

$$
\mathbb{Q}_p[\zeta_o] = \mathbb{Q}_p[\zeta_{p^v(o)}, \zeta_c]
$$

$$
\mathbb{Q}_p[\zeta_p, \zeta_c]
$$

$$
\mathbb{Q}_p[\zeta_c]
$$

$$
\mathbb{Q}_p
$$

Proof. $\mathbb{Q}_p[\zeta_c]$ is an unramified extension of $\mathbb{Q}_p$. Since $\mathbb{Q}_p$ contains the $(p - 1)$-th roots of unity, an unramified extension of degree $f$ would yield $(p^f - 1)$-th roots of unity. It is clear that if $n|(p^f - 1)$ then the smallest such $f$ is the order of $p$ modulo $c$, by definition.

The construction of the totally ramified extensions is simple once we have $\mathbb{Q}_p[\zeta_c]$. The only thing we need to be careful about is to ensure that the defining polynomials are Eisenstein. Since $g(x)$ is the $p$-th cyclotomic polynomial, evaluating it at $x + 1$ instead of $x$ satisfies our criterion. A similar process follows for $h(x)$. □

3.3. Computing $L_p(1, \chi)$. The computation based on Theorem 2.2 is mostly clear. The only issue that might arise is that the computation of $\log_p(1 - \zeta^i)$ in a field with large ramification degree can become slow, and we can use the Frobenius endomorphism to reduce the number of logarithms required. This maps $\log_p(1 - \zeta^i)$ to $\log_p(1 - \zeta^{ip})$ at a fraction of the cost of actually evaluating $\log_p(1 - \zeta^{ip})$.

On the other hand, when using the formula from Theorem 2.3, it is important to know how many terms in the infinite sum need to be calculated for the result have precision $\nu$, that is, correct in value modulo $p^\nu$. This follows as a corollary from the proof that the infinite sum converges.

Proposition 3.4. The infinite sum

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

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 lower bound of $v_p(s_j)$, using a result from [12, Theorem 5.10].

**Lemma 3.5** (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, $v_p(B_j) \geq -1$, since $B_j$ contains at most a single factor of $p$ in its denominator. Also, $v_p(j) \leq \log j / \log p$, so we have

\[
v_p(s_j) \geq r(j - 1) - \frac{\log j}{\log p} - 1
\]

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 3.6.** For the infinite sum to have the correct value modulo $p^\nu$, we need to sum up to the smallest $j$ such that

\[
\nu < v_p(m)(j - 1) - \frac{\log j}{\log p} - 1
\]

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

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

\[
v_p(m)(j - 1) - \frac{\log j}{\log p} - 1 - \nu
\]

\[
= \nu - \frac{\log(2\nu + 1)}{\log p} - 1
\]

\[
\geq \nu - \frac{\log(2\nu + 2)}{\log p} - 1
\]

since $v_p(m) \geq 1$

\[
= \nu - \frac{\log 2 + \log(\nu + 1)}{\log p}
\]

Consider this as a function in $\nu$. As it is monotonically increasing for $\nu > 0$ then it is positive when $\nu > k$ for some integer $k$, showing that it satisfies the condition in Corollary 3.6. □

**Remark 3.8.** In the case of $p = 2$ and $3$, $k = 3$ and $1$ respectively. For all other primes $p$, $k \leq 0$, so $j = \frac{2\nu + 1}{v_p(m)} + 1$ 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 $\nu$ values.

Possible optimisations to speed up the algorithm include caching common terms in the computation, and performing some computations in $\mathbb{Z}_p$ (most terms in the sum are elements of $\mathbb{Z}_p$ instead of the extension field).
4. Computing $R_p$

Let $K$ be a number field and $U_K$ its group of units. A system of fundamental units of $K$ is a set of units that form a basis of $U_K$, modulo torsion. Let $u_1, \ldots, u_{r+s-1}$ be such a system. By fixing an embedding from $\mathbb{C}_p$ to $\mathbb{C}$, we can consider any embedding from $K$ to $\mathbb{C}_p$ as either real or complex depending on the composite embedding from $K$ to $\mathbb{C}$. Dirichlet’s unit theorem tells us that there are $r$ real embeddings $(\sigma_1, \ldots, \sigma_r)$ and $s$ conjugate pairs of complex embeddings $(\sigma_{r+1}, \sigma_{r+1}, \ldots, \sigma_{r+s}, \sigma_{r+s})$. Let $\delta_i$ be 1 or 2 when $\sigma_i$ is respectively real or complex. The $p$-adic regulator is given by

$$R_p = \text{det}[\delta_i \log_p |\sigma_j(u_i)|]_{1 \leq i,j \leq r+s-1}$$

$R_p$ is independent of the choice of ordering of the units and embeddings. However, unless $K$ is totally real or CM, the choice of embedding from $\mathbb{C}_p$ to $\mathbb{C}$ will cause ambiguities. Furthermore, it is not clear that choosing an embedding from $\mathbb{C}_p$ to $\mathbb{C}$ and determining whether such an embedding is real or complex is practical, and this provided additional reasons to restrict our algorithms to totally real fields.

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 $u_i = \prod_{j=1}^{r+s} \alpha_i^{e_{i,j}}$ for some (small) elements $\alpha_i$ 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 $\alpha_i$ are not.

To obtain the correct valuation of the $p$-adic regulator we need a basis for any $p$-maximal subgroup of the unit group, that is, a subgroup $V$ of the $S$-unit group $U$ where $p \nmid (V : U)$. We do so by making use of the saturation techniques developed in [3], which computes such a group from any subgroup $V$ of full rank. In particular for abelian fields of moderate conductor, we can obtain such a group from the cyclotomic units of the surrounding cyclotomic field, which allows us to deal with fields of degree too large for the direct computation using class groups.

5. Character selection

Let $\chi$ be a Dirichlet character, which is a multiplicative homomorphism $\chi : (\mathbb{Z}/k\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$.

As $\chi$ 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 $\chi$, denoted $f_\chi$. Let $\overline{\chi}$ be the conjugate character with the usual definition.

**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 $K$ the fixed field $H$ in $\mathbb{Q}[\zeta_f]$. Then $X$ is the set of Dirichlet characters corresponding to the field $K$.

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

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 $K \subseteq \mathbb{Q}[\zeta_f]$. If $K$ is already a cyclotomic field, where we simply take all even characters of conductor $f$ that are non-trivial.

Note that since $f$, the conductor of the number field, 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 $\deg(K/\mathbb{Q})$. 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.

**Algorithm 5.3. Selecting characters corresponding to field $K$**

**Input:** $K$

**Output:** set of characters $X$

1. Set degree and conductor of $K$ to be $n$ and $f$ respectively
2. Denote the set of even Dirichlet characters with conductor $f$ and order $n$ be $S$
3. Construct map between the ray class group modulo $f$, $\text{Cl}_f$, and $(\mathbb{Z}/f\mathbb{Z})^\times$
4. Construct $H$, the norm group of $K$, from $\text{Cl}_f$
5. Let the set of characters in $S$ that act trivially on $H$ be $X$

*Proof.* We start with $\text{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q})$, which is isomorphic to $(\mathbb{Z}/f\mathbb{Z})^\times$. Consider the projection $\phi$:

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

The kernel of $\phi$ is $\text{Gal}(\mathbb{Q}[\zeta_f]/K)$, or the automorphisms of $\mathbb{Q}[\zeta_f]$ that fixes $K$. Any character corresponding to $K$ would act trivially on the kernel.

We know that, from class field theory,

$$\text{Gal}(K/\mathbb{Q}) \sim \text{Cl}_f/H$$

where $\text{Cl}_f$ is the ray class field of modulo $f$ [6, Algorithm 4.3.1], and $H$ is the norm group in $\mathbb{Z}$ generated by norms of ideals in $K$. With knowledge of $\text{Cl}_f$ and $\text{Gal}(K/\mathbb{Q})$, we can compute $H$ by taking norms of primes until $\text{Cl}_f/H$ reaches the appropriate size. The kernel of $\phi$ is $H$, so we need to find the characters that act trivially on $H$. While

$$\text{Cl}_f \sim (\mathbb{Z}/f\mathbb{Z})^\times$$

and $\chi$ acts on $(\mathbb{Z}/f\mathbb{Z})^\times$, there is no canonical map for the isomorphism. We construct one by examining how various primes map to both $\text{Cl}_f$ and $(\mathbb{Z}/f\mathbb{Z})^\times$. This allows us to find the characters required to act trivially on the generators, this allows us to test and restrict the characters to the appropriate ones.

Since we can compute every part of equation 2.1 except $h$, we can easily compute $h$ using this formula and find its valuation, which will give the $p$-part of $h$. 

6. Analysis and examples

We now estimate the complexity of computing $L_p(1, \chi)$, using each of the two methods. We will be using classical algorithms for multiplication and division in our comparison.

**Proposition 6.1.** The complexity to compute $L_p(1, \chi)$ using Theorem 2.2 to precision $\nu$ is $O(f\chi\nu^3d^2)$, where $d = [\mathbb{Q}_p(\zeta_n, \zeta_{f\chi}) : \mathbb{Q}_p]$.

*Proof.* Let $d_f$ be the degree of $\mathbb{Q}_p(\zeta_{f\chi})$. Performing each logarithm using classical algorithms to precision $\nu$ requires $\nu$ calculations, each of complexity $O(d_f\nu^2)$. The remaining multiplication has complexity $O(d^2\nu^2\log p)$, giving $O(f\chi\nu^3d^2)$ as required. □

**Proposition 6.2.** The complexity to compute $L_p(1, \chi)$ using Theorem 2.3 to precision $\nu$ is $O(\text{lcm}(f\chi, p)d_f^2\nu^3)$, where $d_f = [\mathbb{Q}_p(\zeta_{f\chi}) : \mathbb{Q}_p]$.

*Proof.* To compute the infinite sum with precision $\nu$ requires performing at most $2\nu + 2$ additions, each with complexity in the order of $\nu^2$, providing a complexity of $O(\nu^3)$ for this sum. The logarithm now has complexity $O(d_f^2\nu^3)$, and it must be computed for each of the $\text{lcm}(f\chi, p)$ additions in the formula (each of order $\nu$) for a final complexity of $O(\text{lcm}(f\chi, p)d_f^2\nu^3)$. □

Comparing the complexities of the two approaches, we see that in addition to the common $\nu^3$ term, the method based on Theorem 2.2 is dependent on $f\chi d^2$ whilst the approach based on Theorem 2.3 is related to $\text{lcm}(f\chi, p)$. 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 $f\chi$. This answers Cohen’s question in a remark from [7, p304] regarding which is better for computation.

In the classical algorithm to compute the entire class group, the unconditional verification of the computation requires $O(\sqrt{|D|})$ [5, Algorithm 6.5.6] steps. The proposed algorithm requires the computation of approximately $f$ steps. By the conductor-discriminant formula [11, Chapter VII 11.9], we know that for a number field $K$ with prime degree $n$, $D$ is of the magnitude $f^{n-1}$. This means that theoretically, the proposed algorithm is asymptotically 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.

We highlight three examples here. The first is a complete worked example, while the latter are instances where $p$-adic verification can be achieved in less time than the classical approach (using either a GRH or unconditional bound). These examples were performed using Magma v2.19 [4] (note that the default bound PARI uses assumes the GRH).

6.1. $\mathbb{Q}[\sqrt{40}]$, $p = 2$. Neither method from [1] nor [9] can deal with this example ($p = 2$ and $p$ divides the field degree).

Both $D$ and $f$ are 40. Using the Iwasawa approach, $40 = 2^3 \cdot 5$ and $2^4 = 1 \pmod{5}$, so we construct the unramified extension of $\mathbb{Q}_2$ defined by the polynomial $x^4 + x + 1$. Let $\alpha$ be a root of the defining polynomial in this extension. We then need to construct two ramified extensions of this field, first with the polynomial
\(x + 2\), followed by \(x^4 + 4x^3 + 6x^2 + 4x + 2\). Let \(\beta\) be the root of \(x^4 + 4x^3 + 6x^2 + 4x + 2\) in the final extension field.

We obtain an approximation to the 40-th root of unity (correct up to modulo \(2^5\)), which is required for later calculations, as

\[-13\alpha^3 + 8\alpha^2 + 14\alpha - 2)\beta - 13\alpha^3 + 8\alpha^2 + 14\alpha - 2.\]

The characters required are of order 2, with conductor 40. It turns out only a single character \(\chi\) is required, with \(\chi(17) = -1\), \(\chi(21) = -1\) and \(\chi(31) = 1\).

The \(p\)-adic zeta function and \(p\)-adic regulator work out to be \(\beta^4\) and \(\gamma\) (a root to the equation \(x^2 - 10\) in \(\mathbb{Q}_2\)), with valuation 4 and 1 respectively. Putting this into the \(p\)-adic class number formula, we get \(v_2(h) = 1\) as required.

6.2. \(\mathbb{Q}[\theta]\), \(p = 2\). Take the field of \(\mathbb{Q}\) adjoined by root of \(x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 2921075\). The conductor is 827 and the Minkowski bound is 3461471. The classical method provides a conditional class group of \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) in less than one second, but requires another 160 seconds to verify the result. 2-adic verification based on computing \(hR_p\) takes 1.5 seconds, significantly faster than the classical approach.

6.3. \(\mathbb{Q}[\phi]\), \(p = 11\). Here, \(\phi\) is a root of the polynomial

\[x^{11} - x^{10} - 930x^9 - 1049x^8 + 254577x^7 - 177105x^6 - 28898705x^5 + 105363794x^4 + 1065225462x^3 - 7828574944x^2 + 15893036840x - 7589985325.\]

The conductor is 2047 and the Minkowski bound is 5028348788074. The classical method is capable of computing a tentative class group of \(C_{11}\) for this field in approximately 13 seconds, and another 61 seconds to check up to the Bach bound (69752). It would be infeasible to verify this result using the Minkowski bound. 11-adic verification of the class group takes 4.5 seconds. Furthermore, a complete \(p\)-adic calculation determines the \(p\)-valuation of the class number to be 1, with the entire process taking 22 seconds. This is even faster than using the Bach bound and represents an improvement over the existing algorithm, even if GRH is assumed.

References


