MATHEMATICS OF COMPUTATION
Volume 68, Number 228, Pages 1717–1728
S 0025-5718(99)01139-4
Article electronically published on May 24, 1999

RELATIVE CLASS NUMBER OF IMAGINARY ABELIAN FIELDS OF PRIME CONDUCTOR BELOW 10000

M. A. SHOKROLLAHI

ABSTRACT. In this paper we compute the relative class number of all imaginary Abelian fields of prime conductor below 10000. Our approach is based on a novel multiple evaluation technique, and, assuming the ERH, it has a running time of $O(p^2 \log^2(p) \log\log(p))$, where p is the conductor of the field.

1. INTRODUCTION

In this paper we compute the relative class number of cyclotomic fields of prime conductor and their imaginary subfields for all primes below 10000. Motivated by his results on divisibility properties of class numbers of cyclotomic fields, Kummer [14] was the first to carry out computations of relative class numbers of cyclotomic fields of prime conductor, for primes below 163. It took more than 100 years to extend these computations: Schrutka von Rechtenstamm [35] computed relative class numbers of cyclotomic fields only, for all conductors below 256. In 1970, Newman [22], who was apparently unaware of Schrutka's tables, recomputed those values for primes below 200. Newman's method was based on a determinantal description of the relative class number due to Carlitz and Olson [6]. Eight years later, Lehmer and Masley [16] extended the results to all primes below 521. They employed two methods: one was similar to Newman's, and the other was based on a certain factorization of the relative class number. The second approach yielded a partial factorization of the class number, and had an asymptotic running time of $O(p^{5+\epsilon})$, where p is the conductor of the cyclotomic field. Fung et al. [11] combined that method with new algorithmic techniques to design an $O(p^2 \log^4(p))$-algorithm. They extended previous computations to all primes below 3000. Finally, Jha [13] gave an algorithm based on the classical class number formula, but did not perform any computations. According to the author, his algorithm has a running time of $O(p^2 \log(p))$. However, Jha's running time analysis contains an error. We will discuss this in Section 4.

Following a completely different line of thought, Louboutin [19] described an elegant method for computing the relative class numbers of imaginary Abelian fields and used it to compute relative class numbers of Abelian fields of small degree and large conductor. His method is based on computing good approximations of generalized Bernoulli numbers and then using class number formulas. Conjecturally, the running time of his algorithm is $O(nf^{0.5+\epsilon})$, where n is the degree of the field

Received by the editor November 17, 1997.
1991 *Mathematics Subject Classification.* Primary 11Y40, 11R18, 11R29.

and f is its conductor. Provided that the running time is correct, this algorithm is, to the best of our knowledge, the fastest known method for computing relative class numbers of Abelian fields.

Our algorithm combines the advantages of those of Fung et al. and Jha, and improves upon them, as it will compute class numbers of *all* the imaginary subfields of the cyclotomic field with basically no additional cost. To the best of our knowledge, the only published tables of relative class numbers of all imaginary Abelian fields of prime conductor are those of Hasse [12] for primes below 100, in part those of Schrutka of Rechtenstamm, and those of Yoshino and Hirabayashi [37], who extend Hasse's results to all primes below 200.

Like the approaches of Lehmer and Masley or Fung et al., we also obtain a partial factorization of the class number in a very natural way. Furthermore, assuming the ERH, the running time of our algorithm is, like Jha's algorithm, $O(p^2 \log^2(p) \log\log(p))$. This makes our algorithm the fastest known of its kind.

We will first start by showing that the generalized Bernoulli numbers are values of a certain polynomial at $(p-1)$st roots of unity. This result is essentially due to Kummer. The very heart of our approach is a novel algorithm for evaluating this polynomial modulo a prime q at $(p-1)$st roots of unity. Our algorithm is based on the multiple evaluation algorithm of Borodin and Moenck [3], [5]. However, we are able to use prime divisors of $(p-1)$ to considerably accelerate the computations. The very same method has been successfully used to compute all irregular primes below 8 million [32], [31], [4].

The multiple evaluation algorithm will be applied to several primes q. Chinese remaindering techniques will then ultimately yield the desired class numbers.

We close the paper with a description of our implementations, and provide several tables.

2. Preliminaries on cyclotomic fields

In this section we review some basic and well-known facts about cyclotomic fields of prime conductor.

Let p be an odd prime, and let ζ_p denote a primitive pth root of unity over $\mathbb{Q}$. The field $\mathbb{Q}(\zeta_p)$ is called the *cyclotomic field of conductor p*. It is a Galois extension of $\mathbb{Q}$, and its Galois group G is canonically isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, the isomorphism given by $c \mapsto (\sigma_c\colon\ \zeta \to \zeta^c)$ for $\gcd(c,p) = 1$.

Let χ be a Dirichlet character of $(\mathbb{Z}/p\mathbb{Z})^\times$. The generalized Bernoulli numbers $B_{1,\chi}$ are defined by

$$B_{1,1} = -\frac{1}{2}, \qquad B_{1,\chi} = \frac{1}{p}\sum_{a=1}^{p-1} \chi(a)a \quad \text{for } \chi \neq 1.$$

Let K be an imaginary subfield of $\mathbb{Q}(\zeta_p)$, and K^+ its maximal real subfield. The relative class number of K, denoted by $h^-(K)$, is the quotient h/h^+, where h and h^+ are the class number of K and K^+, respectively. It is well known [36, Theorem 4.17, Corollary 4.13] that

$$h(K)^- = Qw \prod_\chi (-\tfrac{1}{2}B_{1,\chi}),$$

where χ runs over all odd characters of the Galois group of $K/\mathbb{Q}$, w is the number of roots of unity in K, and $Q = [E\colon\ WE^+]$. Here E and E^+ are the group of units

of K and K^+ respectively, and W is the group of roots of unity in K. The following proposition is due to Latimer [15, Theorem 1] (see also [12, Satz 23]). The proof we present here is due to H. W. Lenstra [17].

Proposition 2.1. *For any imaginary subfield of $\mathbb{Q}(\zeta_p)$ we have $Q = 1$.*

Proof. Let H be the Galois group of $K/\mathbb{Q}$, σ a generator of H, and u a unit of K. Let n be the degree of K over $\mathbb{Q}$ denoted by a bar complex conjugation in K. It suffices to prove that $\overline{u}/u = \eta^2$ for a root of unity η, as then $u/\overline{\eta}$ is a real unit. Let $v := uu^\sigma \cdots u^{\sigma^{n/2}-1}$. Then $\overline{u}/u = v^\sigma/v$, and $\overline{v}v$ is the norm of u, which is equal to 1. Hence, v is a root of unity. H acts trivially on the group of roots of unity modulo squares, so v^σ/v is the square of a root of unity. □

Note that the above proof carries over to any cyclic CM-field.

Applying the proposition, we obtain

$$h(K)^- = \begin{cases} 2p\prod_\chi(-\frac{1}{2}B_{1,\chi}), & \text{if } K = \mathbb{Q}(\zeta_p), \\ 2\prod_\chi(-\frac{1}{2}B_{1,\chi}), & \text{if } K \neq \mathbb{Q}(\zeta_p). \end{cases} \tag{2.1}$$

In the following, we denote the relative class number of $\mathbb{Q}(\zeta_p)$, by $h^-(p)$ or h^- if p is clear from the context. As an imaginary subfield K of $\mathbb{Q}(\zeta_p)$ is uniquely determined by the odd number $e = [\mathbb{Q}(\zeta_p)\colon K]$, we denote $h^-(K)$ by $h_e^-(p)$, or h_e^- if p is clear from the context.

For a prime l and an element $s \in \mathbb{F}_l$ we denote by $R_l(s)$ the least nonnegative residue of s modulo l. For a fixed primitive root g modulo p we define the integer polynomial

$$\eta(x) := \sum_{j=0}^{p-2} R_p(g^{-j})x^j. \tag{2.2}$$

The following proposition is essentially due to Kummer [14].

Proposition 2.2. *Let ζ be a primitive $(p-1)$st root of unity over $\mathbb{Q}$. Furthermore, let τ be the generator of the group of Dirichlet characters of $(\mathbb{Z}/p\mathbb{Z})^\times$ given by $\tau(g) = \zeta$. Then for $i \not\equiv 0 \pmod{p-1}$ we have*

$$\eta(\zeta^i) = pB_{1,\tau^{-i}}.$$

Proof. The proof is a simple manipulation of the formula for $B_{1,\tau^{-i}}$, and is therefore omitted. □

We immediately obtain the following result.

Proposition 2.3. *Let p be an odd prime, and let $q \neq p$ be a prime such that $q \equiv 1 \bmod p$. Let e be an odd divisor of $p-1$, let $t := (p-1)/(2e)$, and let a be a primitive $((p-1)/e)$th root of unity in $\mathbb{F}_q$. Then*

$$h_e^- \equiv w\left(-\frac{1}{2p}\right)^{t-1}\prod_{i=0}^{t-1}\eta(a^{2i+1}) \bmod q,$$

where $w = 2p$ if $e = 1$, and $w = 2$ otherwise.

Proof. Let τ be as in Proposition 2.2 and let H be the subgroup of $\mathbb{Q}(\zeta_p)$ of order $(p-1)/e$. Then $\mu := \tau^e$ is a generator of the character group of H. By (2.1) we have

$$h_e^- = w \prod_{i=0}^{t-1} \left(-\frac{1}{2} B_{1,\mu^{-(2i+1)}} \right).$$

Proposition 2.2 shows that the right-hand side of the above equation is equal to

$$w \prod_{i=0}^{t-1} \left(-\frac{1}{2p} \eta(b^{2i+1}) \right),$$

where b is a primitive $2t$th root of unity over $\mathbb{Q}$. Taking everything modulo q implies the result. □

The proposition shows that the main problem for computing h_e^- mod q is that of computing the product of the values of η at the points a^{2i+1}. It can be solved by computing all the values of η at these points, and multiplying the results modulo q. This motivates the discussion in the next section.

3. Values of polynomials on cosets of subgroups of $\mathbb{F}_q^\times$

In this section we will design an algorithm to solve the following problem.

Problem 3.1. *Given a factor d of $q-1$ such that $(q-1)/d$ is even, a polynomial f over $\mathbb{F}_q$ of degree less than d, and a coset C of the cyclic subgroup of $\mathbb{F}_q^\times$ of order d, find $f(c)$ for all $c \in C$.*

Let us first see how the solution of this problem can be employed to compute the h^- mod q. There are several choices for the parameters involved. We will only describe the most economical ones: we choose $d := (p-1)/2$, $f := \eta(x) \bmod (x^{(p-1)/2}+1)$, and C as the coset of the subgroup of index two in the group of $(p-1)$st roots of unity of $\mathbb{F}_q$. (Note that this forces f and η to have the same values on C.)

3.1. **Basic version of the algorithm.** Let $f(x) = \sum_{i<d} f_i x^i$, and let u be a generator of the subgroup of order d of $\mathbb{F}_q^\times$. Further, let α be a representative of the coset C, i.e., $C = \{\alpha u^j | 0 \le j < d\}$. In a first step we multiply the f_i with α^i to obtain $g(x) = \sum_{i<d} f_i \alpha^i x^i =: \sum_{i<d} g_i x^i$. We thus need to compute the values of g on $\{u^j | 0 \le j < d\}$. The standard procedure to solve this problem is to employ a technique known as Bluestein's trick [2]: as $(p-1)/d$ is even, there exists $v \in \mathbb{F}_q$ such that $v^2 = u$. Since $g(u^j) = g(v^{2j})$, we obtain for all $0 \le j < d$

$$g(u^j) = \sum_i g_i v^{i^2+j^2-(j-i)^2} = v^{j^2} \sum_i (g_i v^{i^2}) v^{-(j-i)^2}.$$

Let $h_i := g_i v^{i^2}$ and $v_i := v^{-i^2}$. If d is odd, then $v^{d^2} = -1$; hence the above is a negacyclic convolution of the vectors (h_i) and (v_i). If d is even, this is a cyclic convolution of these vectors. In any event, one can obtain $v^{-j^2} g(u^j)$ by multiplying the polynomials $h(x) := \sum_i h_i x^i$ and $v(x) := \sum_i v_i x^i$, and performing a wrap-around (with negative or positive sign, according to whether d is even or odd). We have thus reduced the problem to that of multiplying two polynomials of degree less than d over $\mathbb{F}_q$. We now use Schönhage's technique as presented in [28]

to reduce this problem to that of multiplying integers. Let $m := \lceil \log(dq^2) \rceil$. (Here and in the following, log denotes $\log_2$.) Further, let

$$\left(\sum_{i=0}^{d-1} h_i 2^{mi}\right) \cdot \left(\sum_{i=0}^{d-1} v_i 2^{mi}\right) = \sum_{i=0}^{2d-2} c_i 2^{mi}.$$

As $\sum_{l+j=i} h_l v_j < 2^m$ for all i, we obtain $c_i = \sum_{l+j=i} h_l v_j$. Hence

$$h(x)v(x) = \sum_{i=0}^{2d-2} (c_i \bmod q) x^i.$$

The running time of this algorithm is clearly dominated by the time needed to multiply two integers of bit-length dm, which, using the Schönhage-Strassen algorithm [30], is $O(dm \log(dm) \log\log(dm))$.

3.2. **Second version of the algorithm.** A major improvement can be gained by employing an idea related to the multiple evaluation algorithm of Borodin and Moenck [3], [5, Chapter 3]. Let $d = q_1 \cdots q_t$. We first show how to recursively compute $\tilde{f}_j := f \bmod (x^{q_t} - (u^j\alpha)^{q_t})$ for $j = 0, 1, \ldots, d/q_t - 1$: start with $f_{0,0} := f \bmod (x^d - \alpha^d)$. Suppose that we have already computed $f_{i,j} := f \bmod (x^{d_i} - (u^j\alpha)^{d_i})$, where $d_i = q_i \cdots q_t$. From this we compute for l with $l < j + d/d_{i+1}$ and $l \equiv j \bmod d/d_i$ the q_i polynomials $f_{i+1,l} := f_{i,j} \bmod (x^{d_{i+1}} = (u^l\alpha)^{d_{i+1}})$. The computation of $f_{i+1,l}$ from $f_{i,j}$ can be done efficiently, as we are computing modulo binomials. At the end of the computation we obtain the set of f_j, which is equal to the set of $f_{t,l}$. Once the f_j have been computed, we use the basic version of our algorithm to find its values on the coset of size q_t consisting of all those elements x of $\mathbb{F}_q^\times$ such that $x^{q_t} = (\alpha u^j)^{q_t}$. Patching all the information for various j together, we obtain a solution to Problem 3.1.

The algorithm gives rise to a factor tree for d, similar to the tree obtained from the multiple evaluation algorithm of Borodin and Moenck. (Compare also [5, Chapter 3.3].) A simple induction shows that computing the polynomials $f_{i,j}$ uses $O((q_1 + \cdots + q_{t-1})d)$ operations in $\mathbb{F}_q$. As described above, the evaluation at the leaves of the tree, i.e., evaluation of the $\tilde{f}_j$ at the corresponding cosets, uses $O(dm \log(q_t m) \log\log(q_t m))$ bit-operations, where $m := \lceil \log(q_t q^2) \rceil$. (Note that we have d/q_t cosets.) Appropriate choice of the divisors $q_1, \ldots, q_t$ may thus lead to significant improvements in the running time.

3.3. **Speedy version of the algorithm.** Further savings can be achieved by noting that whenever we apply the solution of Problem 3.1 to compute the values of f in a certain coset of the subgroup of order q_t of $\mathbb{F}_q^\times$, we are actually computing the polynomial product of $h(x)$ and $v(x)$. The main point is now that v is fixed for all the cosets. So we are actually dealing with the problem of multiplying one integer with several other integers. This problem can be solved efficiently with the following strategy: we use the Schönhage-Strassen algorithm for multiplying integers. In a first step we generate v and its Fourier transform, and store it. Then, for each h encountered, we compute its transform, multiply it with the transform of v, and transform the product back. This reduces the number of Fourier transforms per polynomial multiplication from three to two.

Another improvement can be gained using an idea of D. Reischert [26]. If p is not a Fermat prime, then the largest prime factor q_t of $p - 1$ is odd; hence we have to perform a negacyclic convolution of $h(x)$ and $v(x)$. Translated into

integer multiplication, this means that we are performing multiplication modulo $2^m + 1$ for some m. If m is such that $32m = 2^k l < (2k-1)2^{2k}$, then one can perform the Schönhage-Strassen multiplication algorithm to compute this integer product. (See [29, p. 32].) The advantage over the method which multiplies h and v as integers and reduces the product mod $x^{q_t} + 1$ is that the length of the numbers to be multiplied is smaller. (We do not need zero-padding in this version.) However, since $32m$ might contain a small power of 2 (usually 2^6), the new method may be slower than the old one for some values of m. In our implementation the new method computes the smallest l' such that $q_t(p-1)^2/2 < 2^{32l'}$ and performs a Schönhage-Strassen multiplication modulo $2^{32l'}+1$, while the old method computes the smallest l such that $q_t(p-1)^2/2 < 2^l$ and performs multiplication modulo 2^m+1, where $m = \lceil 2lq_t/32 \rceil$. The final decision whether to use the old or the new method was made according to whether $\lceil l/32 \rceil q_t$ was larger than $\lceil 2lq_t/32 \rceil$ or not.

3.4. **Implementations.** We have implemented all three versions. The lion's share of the implementations has been done in TP-code. TP, which is an invention of A. Schönhage, simulates a multitape Turing machine. It is a software implementation of a Turing Processor, which can be programmed via *TPAL*, the Turing Processor Assembly Language. Currently, there exists a substantial collection of algorithms written in *TPAL*, including the classical routines for computing with integers and many of the asymptotically fast algorithms for this domain. These clean and efficient implementations made TP the natural choice to implement our algorithm in. For more information on this software and how to obtain it via ftp, the reader is referred to the TP-book [29].

4. Computing the relative class number

In this section we develop an algorithm for computing $h_e^-(p)$ for all odd divisors of $p-1$. Our algorithm is very similar to the one suggested by Jha [13]. However, we improve upon his results in the following ways:

(1) We compute not only the relative class number of $\mathbb{Q}(\zeta_p)$, but also the relative class numbers of all imaginary subfields thereof.
(2) We use the prime factors of $(p-1)$ to speed up the calculations.
(3) We give a new analysis of our algorithm, thereby correcting an error in Jha's running time estimates.

The main difficulty is the fact that h^- grows more than exponentially with p. In fact, Kummer conjectured in 1851 [14] that

$$h^-(p) \sim 2p \left(\frac{p}{4\pi^2}\right)^{(p-1)/4} =: G(p), \tag{4.1}$$

i.e., $\lim_{p\to\infty} h^-(p)/G(p) = 1$. No proof of this assertion is known. In fact, Fung et al. argue in [11] that this conjecture is probably false. However, in 1974 Lepistö [18] proved the bounds

$$\begin{aligned} &-\tfrac{1}{2}\ln(p) - 4\ln\ln(p) - 12.93 - \tfrac{4.66}{\ln(p)} \\ &\le \ln\left(\tfrac{h^-(p)}{G(p)}\right) \le 5\ln\ln(p) + 15.49 + \tfrac{4.66}{\ln(p)}, \end{aligned} \tag{4.2}$$

which shows that the growth of h^- is really fast.

First calculations of the relative class number were done by Kummer [14], who computed these numbers for all primes below 163. Later, Newman [22], Pajunen [25], and Lehmer and Masley [16] extended these calculations to all primes below 512. (Pajunen only gave approximate values for the relative class number.) The running time of the most sophisticated of these algorithms was $O(p^5 \log^2 p)$ (see [11]).

Fung et al. [11] could considerably improve upon this running time, and extended the computation to all primes below 3000. Their method has an asymptotic running time of $O(p^2 \log^4 p)$ and has the advantage that it computes a partial factorization of h^-.

Our algorithm is based on Proposition 2.3 and has an asymptotic running time of $O(p^2 \log^2(p) \log\log(p))$. It is the most general of the existing methods, as it also computes class numbers of imaginary subfields of $\mathbb{Q}(\zeta_p)$, at basically no additional cost, and also computes a partial factorization of h^-.

4.1. **The algorithm.** Given the odd prime p, our algorithm starts by finding primes $q_1, \ldots, q_s$ such that $q_i \equiv 1 \mod (p-1)$, and such that $\sum_i \ln(q_i)$ is larger than the right-hand side of (4.2). For each such q we compute $B_{1,\chi} \mod q$ for all the odd characters of the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ using Proposition 2.2 and the method described in Section 3. Once the $B_{1,\chi}$ have been computed, we use Proposition 2.3 to compute $h_e^- \mod q$ for various odd $e|(p-1)$. Finally, we compute h_e^- using Chinese remaindering. A partial factorization of $h^- = h_1^-$ can be obtained by taking the gcd of h^- and the h_e^- for the different e involved.

To assess the asymptotic running time of our algorithm we need to know how large the primes q are likely to become. For discussing this problem, we need explicit estimates for the error term in the prime number theorem for arithmetic progressions. Using any of the bounds in [23],[24], we see that assuming ERH, there is an explicit constant c such that for large enough p the number of primes between $p^{5/2}$ and $2p^{5/2}$ which are congruent to 1 modulo $(p-1)$ is bounded below by

$$c\frac{p^{5/2}}{\varphi(p-1)\ln(p^5)} \geq \frac{c}{5}\frac{p^{3/2}}{\ln(p)} > p.$$

In analyzing our algorithm we may thus assume that the primes $q_1, \ldots, q_s$ are between $p^{5/2}$ and $2p^{5/2}$, and hence $s = O(p)$.

Let us now discuss the cost of the different steps of the algorithm. In the following, we say that the running time of a subroutine is *negligible* if it is

$$o(p^2 \log^2(p) \log\log(p)).$$

In the first step, we have to generate $\eta(x)$. This involves finding a primitive root modulo p, and computing the different coefficients. Both these steps have clearly negligible cost.

The next step consists of finding the appropriate primes q. We start with $\lceil p^{5/2} \rceil$ and test in increments of $p-1$ the resulting integers for primality. We will need at most roughly $p^{3/2}$ primality tests on integers of size $O(\log(p))$ to obtain all the primes q we need. Assuming ERH, primes can be certified in poly-logarithmic time [21]. Hence, the cost of this step is negligible as well.

For each of the primes q we first reduce $\eta(x)$ modulo q. Next, we identify the group of $(p-1)$st roots of unity in $\mathbb{F}_q$. To do this, we need to find a primitive root modulo q, and raise it to the power $(q-1)/(p-1)$. Using common randomized algorithms, the cost for finding the primitive root is majorized by that of finding

the factorization of $(q-1)$. Using fast factorization algorithms, this task can be achieved in subexponential time [7]. Employing any of the versions of the algorithm given in Section 3, we can compute $B_{1,\chi} \mod q$ for all the odd characters in time $O(pm\log(pm)\log\log(pm))$, where $m = \lceil \log(pq^2) \rceil = O(\log(p))$, by evaluating $\eta(x)$ on the corresponding coset. Next, we compute $h_e^- \mod q$ using Proposition 2.3. Arranging the computation appropriately to avoid multiple calculation of the same numbers, this step uses $O(p)$ operations in $\mathbb{F}_q$, i.e., $O(p\log(p)\log\log(p))$ bit-operations for each q. Hence, the running time of computations for each q equals $O(p\log^2(p)\log\log(p))$.

Computing $h_e^- \mod q$ for all primes q takes $O(p^2\log^2(p)\log\log(p))$ operations, since there are $O(p)$ primes.

For each odd divisor e of $(p-1)$ we now have to perform a Chinese remaindering modulo $O(p)$ primes, each of size $O(\log(p))$. Using fast methods, this step can be performed in time proportional to the length of the result multiplied by logarithmic factors, i.e., in time $O(p\log^4(p))$ [8]. As the number of divisors of $p-1$ is $o(p)$, the Chinese remaindering step is negligible.

Once the h_e^- have been found, we compute the gcd of h^- and the different h_e^- to obtain a partial factorization of h^-. The numbers involved have bit-length $O(p\log(p))$, and fast gcd-algorithms [27] show that the running time of this step is negligible too.

In summary, assuming ERH, our algorithm runs in time $O(p^2\log^2(p)\log\log(p))$. It might seem that our algorithm is slower than Jha's [13]. This is due to an error in that paper. More precisely, the author claims on p. 1709 that "the DFT of the sequence of coefficients of ψ in $\mathbb{F}_q$ can be computed in $O(p\log(p))$ elementary arithmetic operations." However, using the fastest known algorithms, the number of bit-operations for this task is $O(p\log^2(p)\log\log(p))$. Hence, the running time of Jha's algorithm is the same as ours.

4.2. **Implementations and result checking.** The main routines of our algorithm, namely the evaluation routines, Chinese remaindering routines, and gcd-routines, were implemented in TP. The I/O routines were handled by C-programs. The Chinese remaindering routine was written by G. Sauer and was kindly provided to us by D. Reischert.

All the computations took approximately 1.5 CPU days on an ULTRASPARC with 167 MHz.

We used various results to check our computations.

(1) The evaluation routines were checked using the identity $\sum_t f(t) = \tau f(0)$, holding for all polynomials f over $\mathbb{F}_q$ of degree less than τ, where t runs over a subgroup of order τ of $\mathbb{F}_q^\times$.
(2) The second phase of checks consisted of comparing our results with known ones. In doing so we observed a mismatch between our results and Table VII in [11]. After contacting the authors, it turned out that Table VII contained errors, and that in all the mismatches our program had computed the correct data. We have recomputed that table with our program. The results are given in Table 2 of Section 5. Its first column corresponds to the first few primes, denoted by q; the second column gives the number of primes p between 100 and 3000 such that $h^-(p)$ is divisible by q, and the third column gives the first three smallest such primes p.

(3) We checked divisibility properties of h_e^- by the prime p and cross-checked that with the results of the Bernoulli computations. Note that if $(p, 2n)$ is an irregular pair, then p divides $B_{1,\omega^{2n-1}}$, where ω is the Teichmüller character. Hence, p divides h_e^-, where $e = (p-1)/\gcd(p-1, 2n-1)$.
(4) The last class of checks used the following observation: If $e = (p-1)/2$ is odd, then h_e^- is the class number of $\mathbb{Q}(\sqrt{-p})$. We checked these values against those computed independently by the `classno`() routine of PARI [1], and did not observe any mismatches.

All these tests were quite helpful in catching bugs during the early development phase of the program.

5. Results

5.1. **Parity of the class number.** The parity of the relative class number $h^-(p)$ of the field $\mathbb{Q}(\zeta_p)$ has attracted a lot of attention ever since Kummer's introduction of cyclotomic class numbers. We refer to [10] and [33] and the references therein for a discussion of the history of this problem. It has been conjectured [9] that $h^-(p)$ is odd whenever p and $(p-1)/2$ are both primes. The conjecture seems to go back to Taussky's work [34]. This conjecture has been verified by Estes [10] in the case that 2 is inert in the maximal real subfield of $\mathbb{Q}(\zeta_p)$. Stevenhagen [33] gives a different proof of this result and provides a heuristic argument in favour of the conjecture, and strengthens these arguments by extensive calculations. Metsänkylä [20] gives results analogous to Estes' for divisibility of $h^-(p)$ by primes other than 2, and also gives another proof of Estes' original result.

Our numerical results prove that the above conjecture is true for all primes p between 2 and 10000.

5.2. **Tables.** We basically performed the same statistics as Fung et al. [11], only omitting the computation of "high and low champions". Furthermore, we did not attempt to completely factor the relative class numbers we obtained. However, we did compute the growth of $h^-(p)$ and compared it against $G(p)$ defined in (4.1). The results are summarized in Table 4, which contains the lowest and highest values of $h^-(p)/G(p)$ observed for primes p with $3 < p < 10000$.

Table 1. $k = \mathrm{ord}_2(h^-)$

k	Number up to 10000	Smallest 3 such primes		
2	41	163	547	853
3	39	29	113	197
4	39	277	349	421
5	9	373	683	1117
6	27	239	337	397
7	1	3557		
8	6	941	1009	1021
9	1	5419		
10	2	311	4789	
13	2	7687	8191	
15	1	3067		

TABLE 2. Corrected version of Table VII in [11]

q	Number up to 3000	Smallest 3 such primes		
3	93	107	131	139
5	109	101	103	127
7	66	151	211	223
11	45	151	167	191
13	64	127	157	191
17	50	109	113	137
19	33	199	311	359
23	24	331	397	647
29	25	421	463	491

TABLE 3. Divisibility by small primes

q	Number up to 1000	Smallest 3 such primes		
3	97	23	31	59
5	111	47	79	101
7	67	71	151	211
11	46	41	151	167
13	64	127	157	191
17	50	109	113	137
19	33	199	311	359
23	24	331	397	647
29	25	421	463	491

TABLE 4. Lowest and highest values of $h^-(p)/G(p)$

p	$h^-(p)/G(p)$	p	$h^-(p)/G(p)$
3331	0.642429	4391	1.507776
7219	0.658084	6101	1.511405
9049	0.667614	4349	1.518571
8209	0.672045	9689	1.524372
6379	0.673523	5231	1.556562

We generated several different tables. The first one contains the relative class number of $\mathbb{Q}(\zeta_p)$ and its imaginary subfields for all primes between 2 and 10000. The second table contains partial factorizations of the relative class numbers. The third table contains several statistics, like divisibility by small primes, irregularity of the prime in question, and the ratio $h^-/G(p)$. It was used to compile Tables 1 and 3. The fourth table contains for each imaginary subfield of $\mathbb{Q}(\zeta_p)$ and each prime $q < 100$ the exact power of q dividing the relative class number of that subfield. The fifth table contains the class numbers of imaginary quadratic subfields of $\mathbb{Q}(\zeta_p)$ for primes $p \equiv 3 \mod 4$. It is only used for checking purposes.

All these tables are available (at least in 1997) from the URL `http://www.icsi.berkeley.edu/~amin/TAB.html`.

6. Concluding remarks

We have presented an algorithm with running time $O(p^2 \log^2(p) \log\log(p))$ for computing the relative class number of $\mathbb{Q}(\zeta_p)$ and all its imaginary subfields. The only lower bound we know for this task is $\Omega(p \log(p))$, which is the size of h^-. Our algorithm, however, has running time $O(p^{2+\epsilon})$. Conjecturally, Louboutin's algorithm [19] has a running time of $O(p^{1.5+\epsilon})$, so the discrepancy between the lower and the upper bound is a factor of $\sqrt{p}$. Unfortunately we do not know of any means to close this gap at the present time. We would like to pose this as an interesting challenge to the software engineering, computational number theory, and complexity theory communities.

7. Acknowledgments

I would like to thank H. W. Lenstra for communicating to me the reference [15] and the elegant proof of Proposition 2.1, S. Louboutin for sending me preprints of his work, Tauno Metsänkylä for communicating to me interesting and important information on the history of class number computations and for proofreading a preliminary version of the paper, D. Reischert for writing some of the more sophisticated parts of the TP-software, in particular the core of the speedy version of the evaluation algorithm, G. Sauer for providing the Chinese remaindering module, and A. Schönhage for his suggestion of using fast integer multiplication to find the zeros of a polynomial over a finite prime field. I would also like to thank J. Buhler, K. Girstmair, A. Granville, H. Williams, and an anonymous referee for interesting comments.

The financial support of the Deutsche Forschungsgemeinschaft, Habilitationsstipendium Sh-57/1, during the research on this paper is gratefully acknowledged.

References

1. C. Batut, D. Bernardi, H. Cohen, and M. Olivier, *User's Guide to PARI-GP*, Université Bordeaux, 351 Cours de la Libération, May 1995. Obtainable via anonymous ftp from `megrez.math.u-bordeaux.fr`.
2. L. I. Bluestein, *A linear filtering approach to the computation of the discrete Fourier transform*, IEEE Trans. Electroacoustics 18 (1970), 451–455.
3. A. Borodin and R. Moenck, *Fast modular transforms*, J. Comput. System Sci., 8 (1974), 366–386. MR **51:**7365
4. J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä and M. A. Shokrollahi, *Irregular primes below 8 million*, J. Symbolic Comput. (submitted)
5. P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic complexity theory*, Springer-Verlag, 1997. CMP 97:10
6. L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc., 6 (1955), 265–269. MR **16:**999d
7. H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993. MR **94i:**11105
8. G. E. Collins, M. Mignotte, and F. Winkler, *Arithmetic in basic algebraic domains*, Computer algebra, symbolic and algebraic computation, (B. Buchberger et al., eds.), 2nd ed., Springer-Verlag, Vienna, 1982, pp. 189–220. MR **87a:**68024
9. D. Davis, *Computing the number of totally positive circular units which are squares*, J. Number Theory 10 (1978), 1–9. MR **57:**16254
10. D. R. Estes, *On the parity of the class number of the field of qth roots of unity*, Rocky Mountain J. Math. 19 (1989), 675–682. MR **92b:**11078
11. G. Fung, A. Granville and H. C. Williams, *Computation of the first factor of the class number of cyclotomic fields*, J. Number Theory 42 (1992), 297–312. MR **93k:**11097

12. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952; reprinted with an introduction by J. Martinet, Springer-Verlag, 1985. MR **14:**141a; MR **87j:**11122
13. V. Jha, *Faster computation of the first factor of the class number of* $\mathbf{Q}(\zeta_p)$, Math. Comp. 64 (1995), 1705–1710. MR **95m:**11120
14. E. E. Kummer, *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers*, J. Math. Pures Appl. 16 (1851), 377–498; reprinted in his *Collected papers*, Vol. I, Springer-Verlag, 1975, pp. 363–484. MR **57:**5650
15. C. G. Latimer, *On the units in a cyclic field*, Amer. J. Math. 56 (1934), 69–74.
16. D. H. Lehmer and J. M. Masley, *Table of cyclotomic class numbers* $h^*(p)$ *and their factors for* $200 < p < 251$, Math. Comp. 32 (1978), 577–582. MR **58:**16594
17. H. W. Lenstra, Private communication, 1997.
18. T. Lepistö, *On the growth of the first factor of the class number of the prime cyclotomic field*, Ann. Acad. Sci. Fenn. Ser. A I No. 577 (1974). MR **50:**273
19. S. Louboutin, *Computation of relative class numbers of imaginary abelian fields*, Expositiones Math. (to appear).
20. T. Metsänkylä, *Some divisibility results for the cyclotomic class number*, Tatra Mt. Math. Publ. 11 (1997), 59–68. MR **98i:**11093
21. G. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. 13 (1976), 300–317. MR **58:**470
22. M. Newman, *A table of the first factor for prime cyclotomic fields*, Math. Comp. 24 (1970), 215–219. MR **41:**1684
23. A. M. Odlyzko, *On conductors and discriminants*, Algebraic number fields (A. Fröhlich, ed.), Academic Press, London, 1977, pp. 377–407. MR **56:**11961
24. J. Oesterlé, *Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée*, Astérisque 61 (1979), 165–167. MR **80j:**10003
25. S. Pajunen, *Computation of the growth of the first factor for prime cyclotomic fields*, BIT, 16 (1976), 85–87. MR **53:**5533
26. D. Reischert, Private communication, 1995.
27. A. Schönhage, *Schnelle Berechnung von Kettenbruchentwicklungen*, Acta Informatica 1 (1971), 139–144. MR **55:**9604
28. A. Schönhage, *Asymptotically fast algorithms for the numerical multiplication and division of polynomials with complex coefficients*, Computer Algebra EUROCAM '82 (J. Calmet, ed.), Lecture Nots in Computer Science 144 (1982), 3–15. MR **83m:**68064
29. A. Schönhage, A. Grotefeld, and E. Vetter, *Fast algorithms*, Bibliographisches Institut, Mannheim, 1994. MR **96c:**68043
30. A. Schönhage and V. Strassen, *Schnelle Multiplikation großer Zahlen*, Computing (Arch. Elektion. Rechnung) 7 (1971), 281–292.
31. M. A. Shokrollahi, *Computation of irregular primes up to eight million*, Technical Report TR-96-002, International Computer Science Institute, 1995.
32. M. A. Shokrollahi, *Stickelberger codes*, Designs, Codes and Cryptography, 9 (1996), 1–11.
33. P. Stevenhagen, *Class number parity for the pth cyclotomic field*, Math. Comp. 69 (1994), 773–784. MR **95a:**11099
34. O. Taussky, *Unimodular integral circulants*, Math. Z., 63 (1955), 286–298. MR **17:**347i
35. G. Schrutka von Rechtenstamm, *Tabelle der (Relativ)-klassenzahlen der Kreiskörper, deren Wurzelexponenten nicht größer als 256 sind*, Abh. Deutsch. Akad. Wiss. Berlin Kl. Math. Phys. Tech., 2 (1964), 1–64. MR **29:**4918
36. L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Springer-Verlag, 1997. MR **97h:**11130
37. K. Yoshino and M. Hirabayashi, *On the relative class number of imaginary abelian number field.* I, II Mem. Coll. Liberal Arts, Kanazawa Medical Univ., 9 (1981), 5–53; 10 (1982), 33–81.

Bell Labs 2C-353, Lucent Technologies, 700 Mountain Avenue, Murray Hill, New Jersey 07974-0636

E-mail address: amin@research.bell-labs.com