MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 212
OCTOBER 1995, PAGES 1705-1710

FASTER COMPUTATION OF THE FIRST FACTOR OF THE CLASS NUMBER OF $\mathbb{Q}(\zeta_p)$

VIJAY JHA

ABSTRACT. We describe two fast methods for computing the first factor of the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$ in $\mathcal{O}(p^2 \log^5 p)$ and $\mathcal{O}(p^2 \log p)$ steps of elementary arithmetic operations on the numbers of size p, respectively. The first is deterministic, while the second holds under the GRH. This is an improvement over the previous method of Lehmer and Masley, which has complexity $\mathcal{O}(p^{3.81})$.

1. INTRODUCTION

1.1. Let p be an odd prime. Kummer deduced the classical class number formula [12] and used it to compute the first factor h^- of the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$ for $p < 164$. Newman [13] and Lehmer and Masley [12] extended the table to $p \leq 521$. The latter authors found the classical class number formula inefficient for the larger p, and based their computation on the evaluation of the determinant of a 0-1 matrix N_p of order $(p-3)/2$ [2]. By using the faster Strassen's method [9] for computing the determinant, the complexity of their method can be reduced to $\mathcal{O}(p^{3.81})$ steps of elementary arithmetic operations (we measure complexity in terms of elementary arithmetic operations on the numbers of size p). In fact, for the size of h^- we have [3]

$$\log h^- < (p/4) \log p. \tag{1}$$

Hence, the number of digits N in the number h^- satisfies

$$N = \mathcal{O}(p \log p). \tag{2}$$

Further, for the complexity L of multiplying two N-digit numbers we have

$$L = \mathcal{O}(N \log N) = \mathcal{O}(p \log^2 p). \tag{3}$$

(For basic concepts and algorithms regarding the arithmetic of large numbers, we refer to [4] and [9]). Now keeping in mind (1), choose $p/4$ primes q_i, $p \leq q_i < p^2$. By Strassen's method of computing the determinant, all the residues $\det(N_p) \pmod{q_i}$ can be computed in $(p/4)\mathcal{O}(p^{2.81}) = \mathcal{O}(p^{3.81})$ steps

Received by the editor December 10, 1991 and, in revised form, April 27, 1992 and December 7, 1993.

1991 *Mathematics Subject Classification.* Primary 11Y40, 11R29.

This work is a part of the author's Ph.D. thesis (Panjab University, India).

Editor's Note: Because we were unable to locate the author, page proofs have not been read by the author.

[9]. Knowing these residues, one can find the determinant by the Chinese remainder theorem in $\mathcal{O}(N \log^2 N) = \mathcal{O}(p \log^3 p)$ steps [9]. Hence, by Lehmer and Masley's method one can find h^- in $\mathcal{O}(p^{3.81})$ steps.

In this paper we propose two fast methods for evaluating the first factor of the class number. The first method uses complex arithmetic, while the second uses modular arithmetic and is faster, but its assumptions are difficult to prove. However, these assumptions are satisfied if we assume the Generalized Riemann Hypothesis. The choice of the method depends upon the availability of the appropriate software. The second method can be further accelerated by using parallel processors to compute distinct modular computations.

In §2 we give a more convenient form of the classical class number formula, which we use in later sections.

In §3, by using multiple-precision complex arithmetic and the Fast Fourier Transform, we prove the following theorem:

1.2. **Theorem.** *The first factor of the class number of the cyclotomic field of prime level p can be computed in $\mathcal{O}(p^2 \log^5 p)$ number of steps of elementary arithmetic operations on numbers of size p.*

In §4 we describe a faster method based upon modular arithmetic, the Chinese remainder theorem, and the Discrete Fourier Transform. Precisely, we prove the following theorem:

1.3. **Theorem.** *Let p be an odd prime for which there exists an integer $t \geq 1$ and primes $q_i \equiv 1 \pmod{p-1}$, $1 \leq i \leq t$, coprime to p, such that*

(i) $q_i < p^3$;

(ii) $Q/q_i < p^{p/4} < Q$ *for all* i, $1 \leq i \leq t$, *where* $Q = \prod_{i=1}^{t} q_i$;

(iii) *The primes q_i, $1 \leq i \leq t$, can be found in $\mathcal{O}(p^2 \log p)$ steps of elementary arithmetic operations on integers of size p.*

Then the first factor h^- of the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$ can be computed in $\mathcal{O}(p^2 \log p)$ number of steps of elementary arithmetic operations on integers of size p.

1.4. *Remark.* If one assumes the Generalized Riemann Hypothesis, the interval $(p^{2.5}, 2p^{2.5})$ contains a sufficient number of primes $q_i \equiv 1 \pmod{p-1}$ which satisfy (ii). (See [6, p. 125].) The total number of integers in this interval, congruent to $1 \bmod p-1$, is roughly $p^{2.5}/(p-1) = \mathcal{O}(p^{1.5})$. Since each of these can be tested for primality in $\mathcal{O}(p^{1/3})$ steps [15], all these numbers can be tested for primality in $\mathcal{O}(p^2)$ steps. Hence, (iii) is also satisfied. This shows the strength of the theorem. The author acknowledges the referee's suggestions for this remark.

1.5. *Remark.* There are known faster methods [5, 8, and 10] for obtaining information on the structure of the minus part $\mathfrak{C}^-$ of the class group of $\mathbb{Q}(\zeta_p)$ once some factors of h^- are known. Lehmer and Masley [12] used a costly method for computing some factors of h^-. Our method is equally applicable to the computation of the first factor of the class number [11] of any imaginary subfield $\mathbb{K}$ of $Q(\zeta_p)$ in $\mathcal{O}(p^2 \log p)$ steps. It is known that the first factor of the class numbers of $\mathbb{K}$ divides h^- [11]. Thus, we get many factors of h^- by a faster method, and in conjunction with the results of [5, 8, and 10], can obtain information on the structure of $\mathfrak{C}^-$ with less effort.

1.6. The author thanks the referee for communicating the manuscript [7], in which (see p. 6 of [7]) Fung, Granville and Williams used modular arithmetic to compute h^- in $\mathcal{O}(p^3 \log^2 p)$ steps and used it to compute h^- for all $p < 3000$. Paraphrasing the referee, it did not occur to them to use the DFT at the second stage of computing their polynomials, by which they might have obtained a complexity only slightly inferior to ours.

2. A CLASS NUMBER FORMULA

In this section we derive a class number formula which is interesting in itself. Let $\rho = (p-1)/2$, let g be a primitive root modulo p, and let for an integer i, g_i be the unique integer such that $g^i \equiv g_i \pmod{p}$ and $1 \le g_i \le p-1$. Let further β be a complex primitive $(p-1)$st root of unity. We now prove the following lemma.

2.1. **Lemma.** *Let*

$$H(X) = \sum_{i=0}^{\rho-1} (p - 2g_i) X^i$$

be a polynomial of degree $(p-3)/1$. *Then the coefficients of* H *can be computed in* $\mathcal{O}(p)$ *steps. Let further* B *be the group of all complex* $(p-1)$*st roots of unity and* $B^- \subseteq B$ *be the subset of all* $b \in B$ *such that* $b^{(p-1)/2} = -1$. *Then we have the following class number formulae*:

$$h^- = \frac{1}{(2p)^{(p-3)/2}} H(\beta) H(\beta^3) \cdots H(\beta^{p-2}) = \frac{1}{(2p)^{(p-3)/2}} \prod_{\alpha \in B^-} H(\alpha). \tag{4}$$

Proof. Since $p-1$ can be factored in $\mathcal{O}(p^{1/3})$ steps ([15, p. 111]), and if the factorization of $p-1$ is known, a primitive root $g \bmod p$ can be computed in $\mathcal{O}(p^{1/3})$ steps ([15, p. 111]), and the coefficients of the polynomial H can be computed in $\mathcal{O}(p)$ steps. Next, by the classical class number formula [2, 10],

$$h^- = \frac{1}{(2p)^{(p-3)/2}} \varphi(\beta) \varphi(\beta^3) \cdots \varphi(\beta^{p-2}),$$

where

$$\varphi(X) = -\sum_{i=0}^{p-2} g_i X^i.$$

Now let α be a $(p-1)$st root of unity such that $\alpha^{(p-1)/2} = -1$. Then

$$\begin{aligned} -\varphi(\alpha) &= \sum_{i=0}^{p-2} g_i \alpha^i = \sum_{i=0}^{\rho-1} g_i \alpha^i + \sum_{i=\rho}^{p-2} g_i g^i \\ &= \sum_{i=0}^{\rho-1} (g_i \alpha^i + g_{\rho+i} \alpha^{\rho+i}) = \sum_{i=0}^{\rho-1} (g_i + g_i - p) \alpha^i = \sum_{i=0}^{\rho-1} (2g_i - p) \alpha^i. \end{aligned}$$

Clearly, for odd n, $1 \le n \le p-2$, we have $\beta^{n\rho} = -1$. Hence,

$$\varphi(\beta^n) = H(\beta^n), \qquad n \text{ odd}, \ 1 \le n \le p-2.$$

This gives (4). □

We will now propose two methods for evaluating h^- by using (4).

3. Proof of Theorem 1.2

To prove Theorem 1.2, we represent numbers in B (see Lemma 2.1) as complex numbers evaluated with the precision N given by (2), and make use of the Fast Fourier Transform [4, 9] of sequences of such numbers. We employ the following steps of computation:

(a) Compute π and a complex $(p-1)$st primitive root $\beta = \exp(2\pi i/(p-1))$ with the precision N defined by (2).

(b) Compute β^n for odd n, $1 \le n \le p-2$, with the precision N.

(c) Computer $H(\beta^n)$ for odd n, $1 \le n \le p-2$, with the precision N.

(d) Multiply the above values together, divide the result by $(2p)^{(p-3)/2}$, and take the absolute value.

Now we can compute the values of $\pi = \arctan(x)$ and $\beta = \exp(2\pi i/(p-1))$ with the precision of N digits in $\mathcal{O}(L \log N)$ steps [1], where L is given by (3). The task (b) can be completed in $\mathcal{O}(pL)$ steps. Now the numbers $H(\beta^{2n+1})$, $0 \le n \le (p-3)/2$, are the values of the polynomial H of degree $(p-3)/2$ at $(p-1)/2$ points, and this sequence (with the precision N) can be computed in $\mathcal{O}(N \log^2 NL)$ steps [4, 9]. Finally, to multiply these values together, and then divide $(p-3)/2$ times repeatedly by $2p$ will take $\mathcal{O}(pL)$ steps. Hence, the total complexity is $\mathcal{O}(N \log^2 NL) = \mathcal{O}(N^2 \log^3 N)$ by (3). Now (2) gives the theorem. To avoid roundoff errors, one can double the number of digits N involved in all intermediate computations. □

4. Proof of Theorem 1.3

The proof consists of several stages.

4.1. Let the integer $t \ge 1$ and primes $q_1, q_2, \ldots, q_t$ satisfy conditions (i)–(iii) of the theorem. To prove the theorem, for each q_i, $1 \le i \le t$, we define epimorphisms of the ring of integers $\mathbb{Z}[\beta]$ of the field $\mathbb{Q}(\beta)$ onto the finite field $\mathbb{F}_{q_i}$ consisting of q_i elements, compute the images of $H(\beta^n)$, n odd, $1 \le n \le p-2$, multiply them together and then divide by $(2p)^{\rho-1}$ to get the residues $h^- \pmod{q_i}$ (see the right-hand side of (4)). Let Q be the product of the primes q_i, $1 \le i \le t$. By the Chinese remainder theorem we can uniquely determine $h^- \pmod{Q}$ from its residues $\bmod q_i$. By (1) and the condition (ii) of the theorem, $Q > h^-$. Since $h^- > 0$, we can uniquely determine h^- by knowing its residue $\bmod Q$.

Further, (i) and (ii) imply that $t < p$. Now there exists an algorithm with complexity $\mathcal{O}(N \log^3 N)$ which, from the sequence $a_i = h^- \pmod{q_i}$, $1 \le i \le t$, computes the unique positive integer $< Q$, of at most N digits, whose residues $\bmod q_i$ are a_i [4, 9]. By (2), $N = \mathcal{O}(p \log p)$. Hence, to prove the theorem, it suffices to show that all these residues can be computed in $\mathcal{O}(p^2 \log p)$ steps. Since $t < p$, it is sufficient to show that each of these residues can be computed in $\mathcal{O}(p \log p)$ steps.

4.2. Let q be one of these q_i, $1 \le i \le t$. We remark that by (i), $q < p^3$, and hence $\log q = \mathcal{O}(\log p)$. Now $q-1$ can be factored in $\mathcal{O}(q^{1/3}) = \mathcal{O}(p)$ steps ([15, p. 111]). Once the factors of $q-1$ are known, a primitive root $g \bmod q$ can be found in $\mathcal{O}(\log^3 q) = \mathcal{O}(\log^3 p)$ steps ([15, p. 111]). Now let $\beta_q \equiv g^{(q-1)/(p-1)} \pmod{q}$. Then β_q belongs to the exponent $p-1 \bmod q$ and

can be computed in $\mathscr{O}(\log((q-1)/(p-1))) = \mathscr{O}(\log p)$ steps. Let further B_q^- be the set of all odd powers of β_q. Clearly, the set B_q^- can be computed in $\mathscr{O}(p)$ steps. Thus, all these computations can be carried out in $\mathscr{O}(p)$ steps.

Since $q \equiv 1 \pmod{p-1}$, q splits in $\mathbb{Q}(\beta)$ as a product of prime ideals of degree 1; let q be one of these. Then $\mathbb{Z}[\beta]/q$ is a finite field with q elements; and thus, it is isomorphic to $\mathbb{F}_q$. Now the elements $\beta, \beta^3, \ldots, \beta^{p-2}$ are the roots of the polynomial X^p+1 and have distinct images in $\mathbb{F}_q$, which are clearly the zeros of X^p+1 in $\mathbb{F}_q$. Clearly, the correspondence $\beta \to \beta_q$ induces an isomorphism of $\mathbb{Z}[\beta]/q$ onto $\mathbb{F}_q$ that maps B^- onto B_q^-. It is also clear that this epimorphism can be constructed in $\mathscr{O}(p)$ steps. Now, by (4),

$$h^- \equiv \frac{1}{(2p)^{(p-3)/2}} \prod_{\alpha \in B_q^-} H(\alpha) \pmod{q}.$$

Let $\alpha \equiv \beta_q^{2n+1}$ be an element of B_q^-. Then

$$H(\alpha) \equiv H(\beta_q^{2n+1}) \equiv \sum_{i=0}^{p-1} (p-2g_i)\beta_q^{(2n+1)i}$$
$$\equiv \sum_{i=0}^{p-1} (p-2g_i)\beta_q^i \beta_q^{2ni} \equiv \sum_{i=0}^{p-1} \{(p-2g_i)\beta_q^i\}\gamma_q^{ni},$$

where $\gamma_q \equiv \beta_q^2 \pmod{q}$. Now define a polynomial ψ of degree $(p-1)/2$ as follows:

$$\psi(X) = \sum_{i=0}^{p-1} \{(p-2g_i)\beta_q^i\} X^i.$$

Clearly, the coefficients of ψ can be computed in $\mathscr{O}(p)$ steps. The sequence

$$H(\beta_q^{2n+1}) = \psi(\gamma_q^n), \qquad 0 \le n \le (p-3)/2,$$

is nothing but the Discrete Fourier Transform of the sequence of coefficients of ψ in $\mathbb{F}_q$, and as it follows from [14], this can be computed in $\mathscr{O}(p \log p)$ steps of elementary arithmetic operations on numbers of size p. Further, the elements of this sequence can be mutually multiplied together in $\mathbb{F}_q$ in $\mathscr{O}(p)$ steps. Let their product be R. It can be verified that the complexity to compute the inverse of $2p \bmod q$, raised to the power $(p-3)/2$, is $\mathscr{O}((\log p))$ (see [9]). Multiply the latter by R in $\mathbb{F}_q$ to get $h^- \bmod q$. Clearly, all these residues can be computed in $\mathscr{O}(p \log p)$ steps, and the theorem follows. □

5. Concluding remarks

In light of Remark 1.4 one can expect that conditions (i)–(iii) of Theorem 1.3 require only $\mathscr{O}(p^2)$ steps. Similarly, from the proof of Theorem 1.3 we observe that for each q_i, $1 \le i \le t$, all other computations, except that of DFT, require $\mathscr{O}(p)$ steps. Hence, for all q_i, $1 \le i \le t$, these computations can be carried out in $\mathscr{O}(p^2)$ steps. Hence, the cost is due to the cost of computing the DFT (see §4.2) $\bmod q_i$. This shows that by this method one might not expect the cost to be less than $\mathscr{O}(p^2 \log p)$. This suggests the following conjecture:

Conjecture. *There cannot be a method which computes* h^- *in less than* $\mathcal{O}(p^2 \log p)$ *steps for all the primes* p.

BIBLIOGRAPHY

1. R. P. Brent, *Fast multiple precision evaluation of elementary functions*, J. Assoc. Comput. Mach. **23** (1976), 242–251.
2. L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. **6** (1955), 265–269.
3. L. Carlitz, *A generalization of Maillet's determinant and a bound for the first factor of the class number*, Proc. Amer. Math. Soc. **12** (1961), 256–261.
4. G. E. Collins, M. Mignotte, and F. Winkler, *Arithmetic in basic algebraic domains*, Computer Algebra Symbolic and Algebraic Computation (B. Buchberger, G. E. Collins, and R. Loos, eds.), Springer-Verlag, New York, 1982, pp. 189–220.
5. G. Cornell and M. Rosen, *Group-theoretic constraints on the structure of the class group*, J. Number Theory **13** (1981), 1–11.
6. H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York, 1980.
7. G. Fung, A. Granville, and H. C. Williams, *Computation of the first factor of the class number of cyclotomic fields* (to appear).
8. F. Gerth, *The ideal class group of two cyclotomic fields*, Proc. Amer. Math. Soc. **78** (1980), 321–322.
9. E. Horowitz and S. Sahni, *Fundamentals of computer algorithms*, Galgotia Publications, New Delhi, India, 1988, pp. 422–458.
10. K. Iwasawa, *A note on ideal class groups*, Nagoya Math. J. **27** (1966), 239–247.
11. T. Kimura and K. Horie, *On the Stickelberger ideal and the relative class number*, Trans. Amer. Math. Soc. **302** (1987), 727–739.
12. D. H. Lehmer and J. M. Masley, *Table of the cyclotomic class number and their factors for* $200 < p < 521$, Math. Comp. **32** (1978), 577–582.
13. M. Newman, *A table of the first factor for prime cyclotomic fields*, Math. Comp. **24** (1970), 215–219.
14. F. P. Preparata and D. V. Sarvate, *Computational complexity of Fourier tranforms over finite fields*, Math. Comp. **31** (1977), 740–751.
15. P. Ribenboim, *The book of prime number records*, Springer-Verlag, New York, 1989.

CENTER FOR ADVANCED STUDY IN MATHEMATICS, PANJAB UNIVERSITY, CHANDIGARH-160014, INDIA