MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 163
JULY 1983, PAGES 303-305

# The Calculation of a Large Cubic Class Number With an Application to Real Cyclotomic Fields

By Eric Seah, Lawrence C. Washington* and Hugh C. Williams**

**Abstract**. The class number of the cubic subfield of the $p$th cyclotomic field is calculated for the prime $p = 11290018777$. This is used to construct an example where the class number of the $p$th real cyclotomic field is larger than $p$.

In a recent paper [1], it is shown that if the Generalized Riemann Hypothesis holds, then $h_p^+ > p$ for the prime $p = 11290018777$. Here $h_p^+$ is the class number of $\mathbf{Q}(\cos(2\pi/p))$, the maximal real subfield of the $p$th cyclotomic field. In the present note we show that the GRH is not needed, so the result holds unconditionally.

It is a conjecture of Vandiver, with important consequences for Fermat's Last Theorem and the theory of cyclotomic fields, that $p$ never divides $h_p^+$. It had been suggested that perhaps $h_p^+ < p$ for all $p$, hence that Vandiver's conjecture might be trivially true. The present result shows this is not the case.

The method of [1] was to evaluate the class numbers $h_2$ and $h_3$ of the quadratic and cubic subfields. An easy argument shows that the product $h_2h_3$ divides $h_p^+$. Daniel Shanks computed $h_2$ to be 2685, using his algorithms for composition of quadratic forms. The main difficulty was the estimation of $h_3$. Since the cubic subfield was a "simplest cubic field" [5], arising from the polynomial $X^2 - aX^2 - (a+3)X - 1$ with $a = 106253$ ($p = a^2 + 3a + 9$), the regulator was known exactly (133.9480419...). Therefore it remained to estimate $|L(1,\chi)|^2$ for $\chi$ a cubic character mod $p$. In [1] this was done using the Euler product $\prod(1 - \chi(q)q^{-1})^{-1}$ for primes $q < 300000$. The remainder was estimated using the explicit effective Chebotarev Density Theorem of Lagarias-Odlyzko-Oesterlé [4], which assumes the GRH. This yielded $h_p^+ > 1.014p$, as desired. If the tail of the Euler product had been ignored, we would have obtained $h_3 \simeq 6.1954 \times 10^6$, $h_2h_3 \simeq 1.473p$.

We now give a different method for evaluating $h_3$, which takes longer but has the advantage of giving the exact value and avoiding the GRH. As in [6] we may write

$$\sqrt{p}\,L(1,\chi) = W_\chi \sum_{n=1}^{\infty} \bar{\chi}(n) \int_{n^2A}^{\infty} e^{-t}/t\,dt + \sum_{n=1}^{\infty} \chi(n) \frac{2}{n\sqrt{A}} \int_{n\sqrt{A}}^{\infty} e^{-t^2}\,dt,$$

where $A = \pi/p$ and $W_\chi = p^{-1/2}\sum_{b=1}^{p-1}\chi(b)e^{2\pi ib/p}$ (so $|W_\chi| = 1$). If we sum to $n = N$ in each sum, then the error on the right is at most $e^{-AN^2}/A^2N^3$ (cf. [6]).

Received November 29, 1982.
1980 *Mathematics Subject Classification.* Primary 12A35, 12A50.
* Research partially supported by NSF.
** Research supported by NSERC grant number A7649.


0025-5718/82/0000-1367/$01.75

There are two choices for $\chi$. For definiteness, choose $\chi$ such that $\chi(b) = 1, e^{2\pi i/3}$, $e^{4\pi i/3}$ if $b^{(p-1)/3} \equiv 1$, 7526643766, 3763375010 mod $p$, respectively. This is the cubic residue character modulo the prime $\pi = 106256 + 3e^{2\pi i/3}$. Standard formulas on Gauss sums [2, p. 115] yield

$$W_\chi^3 = (106256 + 3e^{2\pi i/3})p^{-1/2}.$$

This yields three choices for $W_\chi$, hence three possibilities for $h_3$. However, Benedict Gross suggested that perhaps if the error terms were made small enough in the above sums, only one of these would allow $h_3$ to be an integer. This turns out to be the case. Writing the above formula for $\sqrt{p}\,L(1, \chi)$ as $W_\chi\Sigma_1 + \Sigma_2$, we have, using $N = 250000$ terms,

$$\Sigma_1 = 56.437220121237002544 - 119.53491341223978301i,$$
$$\Sigma_2 = 57418.064811064652753 - 4731.1007581056751240i,$$

with an error in $|W_\chi\Sigma_1 + \Sigma_2|$ of at most $2.4 \times 10^{-5}$. This yields the following possible values for $|\sqrt{p}\,L(1, \chi)|$:

$$57678.8276378680269, \quad 57678.8886140727151, \quad 57480.4620277658337.$$

Therefore, $h_3 = p\,|L(1, \chi)|^2/4R$ has the following possibilities, respectively:

$$6209212.00, \quad 6209225.13, \quad 6166576.73.$$

The error is less than $10^{-2}$, so we must have

$$h_3 = 6209212 = 4 \times 223 \times 6961.$$

This yields that $h_p^+$ is a multiple of

$$h_2h_3 = 2685 \times 6209212 = 16{,}671{,}734{,}220,$$

hence

$$h_p^+ > 1.476p.$$

Of course, any of the above possibilities for $h_3$ would have yielded $h_p^+ > p$. Also, if more than one of them had been integral, then it probably would have been possible to find an ideal class of an appropriate order to eliminate all but one choice. However, there is even a better method, as Daniel Shanks pointed out to us. It is known [5] that $h_3$ is not divisible by 3, and every prime congruent to 2 mod 3 appears in $h_3$ with even exponent. It follows that none of the integers from 6166574 to 6166590 can be $h_3$, and that of the integers from 6209201 to 6209235, only 6209212 can be $h_3$. Therefore, in retrospect, we did not need such precise estimates; it would have sufficed to use about $N = 210000$ terms in the evaluation of $\Sigma_1$ and $\Sigma_2$.

The error in estimating the class number $h_3$ via the Euler product for $q < 300000$ was around 1 part in 450, which is slightly less than 1 part in $(300000)^{1/2}$. This phenomenon has been observed in the quadratic case [3] and is consistent with the GRH.

Note that we have also evaluated the Gauss sum

$$W_\chi = 0.9999999999667842 + 0.000008150482131131 0026i$$

since this choice corresponded to the correct value of $h_3$.

The above calculations were performed on the AMDAHL 470-V7 computer at the University of Manitoba. The main program was written in extended precision FORTRAN. A special, extended precision, assembler language routine was written to calculate the exponential integrals in $\Sigma_1$. This routine utilized a Chebyshev series approximation to produce results correct to 20 decimal digits. The integrals in $\Sigma_2$ were evaluated by using the IBM QERFC routine. The total CPU time required was about 32 minutes.

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

Department of Mathematics
University of Maryland
College Park, Maryland 20742

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

1. G. CORNELL & L. WASHINGTON, "Class numbers of cyclotomic fields," *J. Number Theory*. (To appear.)

2. K. IRELAND & M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

3. C. NEILD & D. SHANKS, "On the 3-rank of quadratic fields and the Euler product," *Math. Comp.*, v. 28, 1974, pp. 279–291.

4. J. OESTERLÉ, "Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée," *Astérisque*, v. 61, 1979, pp. 165–167.

5. D. SHANKS, "The simplest cubic fields," *Math. Comp.*, v. 28, 1974, pp. 1137–1152.

6. H. C. WILLIAMS & J. BROERE, "A computational technique for evaluating $L(1, \chi)$ and the class number of a real quadratic field," *Math. Comp.*, v. 30, 1976, pp. 887–893.