PACIFIC JOURNAL OF MATHEMATICS
Vol 115, No. 1, 1984

CLASS NUMBERS OF IMAGINARY CYCLIC QUARTIC FIELDS AND RELATED QUATERNARY SYSTEMS

RICHARD H. HUDSON

A proof is given of an explicit Dirichlet-type class number formula for imaginary cyclic quartic fields obtained in 1980 by Hudson and Williams and, in a slightly different form, by Setzer. The Hudson-Williams formula is used to study the solvability of the quaternary quadratic form

$$16p^k = x^2 + 2qu^2 + 2qv^2 + qw^2,$$
$$xw = av^2 - 2buv - au^2, \qquad (x, u, v, w, p) = 1$$

for exponents $k \geq 1$. Included is a table from which every class number $h(k)$ of the quartic field $k = Q(i\sqrt{2q + 2a\sqrt{q}})$, $q \equiv 5 \pmod 8$ a prime, may be determined for $q < 10000$. Finally, a quartic analog of the well-known result that the number of quadratic residues in $(0, p/2)$ exceeds the number in $(p/2, p)$ if $p \equiv 3 \pmod 4$ is proven using one of Dirichlet's less well-known class number formulas.

1. Introduction. Explicit Dirichlet-type class number formulas for imaginary cyclic quartic fields were obtained in 1980 by Hudson and Williams and independently by Setzer. In this paper we sketch in §2 the proof of the Hudson-Williams formula and show that these two formulas are easy consequences of one another. However, the Hudson-Williams formulation is particularly useful for studying the solvability of the quaternary quadratic form

$$\begin{aligned} &16p^k = x^2 + 2qu^2 + 2qv^2 + qw^2, \\ &xw = av^2 - 2buv - au^2, \qquad (x, u, v, w, p) = 1, \end{aligned} \tag{1.1}$$

for $k \geq 1$. We show in §§3–5 that solvability of this form depends heavily on the relative class number $h^* = h(k)/h(Q(\sqrt{q}))$ of the imaginary cyclic quartic field

$$K = Q\left(i\sqrt{2q + 2a\sqrt{q}}\right) = Q\left(i\sqrt{2q - 2a\sqrt{q}}\right) \tag{1.2}$$

where $q \equiv 5 \pmod 8 = a^2 + b^2$ (a odd, $b > 0$) will denote a prime > 5 throughout and $h(Q(\sqrt{q}))$ the class number of the unique quadratic subfield $Q(\sqrt{q})$ of K.

Recall the well-known result that the number of quadratic residues in the interval $(0, p/2)$ exceeds the number in the interval $(p/2, p)$ if $p \equiv 3 \pmod 4$. Using a class number formula of Dirichlet we prove an analogous result for quartic residues in §6 for primes $q \equiv 5 \pmod 8$.

Finally, in §7, we enclose a table of values of h^* for every $q < 10000$. These were computed on two different home computers and cross-checked for accuracy.

2. The Hudson-Williams formula. Let N_0, N_1, N_2, N_3 denote the number of quartic residues in the intervals $(0, p/4)$, $(p/4, p/2)$, $(p/2, 3p/4)$, $(3p/4, p)$, respectively. Bennett Setzer [**16**] proved that

$$h^* = h(k)/h\left(Q\left(\sqrt{q}\right)\right) = \tfrac{1}{2}\left((N_3 - N_0)^2 + (N_2 - N_1)^2\right). \tag{2.1}$$

Let χ_1 denote the nonprincipal character (mod q) of order 4 such that $\chi_1(2) = +i$ and let c_1, c_2, c_3 denote the cosets which may be formed with respect to the subgroup of fourth powers (mod q) which we denote by c_0. Define the coset sums S_0, S_1, S_2, S_3 by

$$S_j = S_j(\chi_1) = \frac{1}{q}\sum_{n=i^j}^{q-1}, \qquad j = 0, 1, 2, 3. \tag{2.2}$$

Hudson and Williams [**11**] proved that

$$h^* = \tfrac{1}{5}\left((S_2 - S_0)^2 + (S_3 - S_1)^2\right). \tag{2.3}$$

The formulation (2.3), announced by Hudson at the A.M.S. meeting in Ann Arbor in 1980, is more convenient to use than (2.1) in investigating solutions of the quaternary quadratic form

$$\begin{aligned} &16p^k = x^2 + 2qu^2 + 2qv^2 + qw^2, \\ &xw = av^2 - 2buv - au^2, \qquad (x, u, v, w, p) = 1. \end{aligned} \tag{2.4}$$

The form (2.4) has been studied by, among others, Dickson [**6**], Lehmer [**12**], Whiteman [**17**], Muskat and Zee [**13**], and Hudson, Williams, and Buell [**10**].

Throughout the paper we let

$$f = \max\left\{|S_0 - S_3|, |S_1 - S_2|\right\}. \tag{2.5}$$

Hudson and Williams [**10**, §4] proved that (2.4) is always solvable when $k = f$ for primes $p \equiv 1 \pmod q$. Although authors to-date have dealt exclusively with primes $p \equiv 1 \pmod q$, Hudson and Buell [**4**] noticed that

this restriction is artificial, as existence (or non-existence) of solutions of (2.4) depends only on the condition that $p = qf + r$, where r is any quartic residue of q. It would be highly desirable to have a proof analogous to that in §4 of [**10**] when $(r/q)_4 = +1$, $r \neq 1$ (see remark following Theorem 4.1).

We now sketch the proof of (2.3). Since the degree of K over the rational field Q is 4, K is an Abelian extension of Q. Hence the class number $h(K)$ is given by (see, e.g. [**14**, p. 372]),

$$h(K) = \frac{w(K)|d(K)|^{1/2}}{2^{r_1+r_2}\pi^{r_2}R(K)} \prod_{\chi} L(1, \chi'). \tag{2.6}$$

Appealing to Edgar and Peterson [**8**] it is easy to see that all the units of K are given by $\pm\varepsilon^k$ $(k = 0, 1, \ldots)$ where ε is the fundamental unit (> 1) of $Q(\sqrt{q})$ and, consequently, to deduce that $w(K) = 2$ (as $q > 5$) and $R(K) = 2\log\varepsilon$.

Appealing to the work of Adrian Albert [**1**] we obtain that $d(K) = q^3$ (see, in particular, equations 9, 34–37 and Theorem 10 of [**1**]).

Let $\zeta_q = e^{2\pi i/q}$. It is not difficult to show (see Hasse [**9**]) that the nonprincipal characters $\chi \pmod q$ which are trivial on the subgroup c_0 (the fourth powers (mod q)) are precisely χ_1 and χ_3, the two nonprincipal characters (mod q) of order 4, and the Legendre symbol (n/q). For convenience we distinguish χ_1 from χ_3 by choosing $\chi_1(2) = i$, $\chi_3(2) = -i$ so that 2 belongs to c_1 throughout the paper.

Let χ' be the primitive character induced by χ and note that $\chi' = \chi$ since q is prime. Hence

$$\prod_{\chi} L(1, \chi') = L(1, \chi_1)L(1, \chi_2)L(1, \chi_3).$$

Appealing to Berndt [**2**, Th. 3.2] we obtain (as χ_1 is an odd character) that

$$L(1, \chi_1)L(1, \chi_3) = \pi^2 \frac{\sum_{0<n<q/2} \chi_1(n) \sum_{0<n<q/2} \chi_3(n)}{-G(\chi_1)G(\chi_3)(\chi_1(2) - 2)(\chi_3(2) - 2)} \tag{2.7}$$

where

$$G(\chi) = \sum_{j=1}^{q-1} \chi(j)\zeta_q^j.$$

Since $G(\chi_3) = \overline{-G(\chi_1)}$ we have $-G(\chi_1)G(\chi_3) = q$ and, moreover, $(\chi_1(2) - 2)(\chi_3(2) - 2) = 5$ so (2.7) becomes

$$L(1, \chi_1)L(1, \chi_3) = \frac{\pi^2}{5q} \sum_{0<n<q/2} \chi_1(n) \sum_{0<n<q/2} \chi_3(n). \tag{2.8}$$

From Dirichlet's class number formula [7] we have

$$L(1, \chi_2) = \sum_{n=1}^{\infty} \left(\frac{n}{q}\right)/n = \frac{2\log\varepsilon}{\sqrt{q}} h\left(Q\left(\sqrt{q}\right)\right) \tag{2.9}$$

and using an easy generalization of an identity of Cauchy [5] given in [11] we obtain

$$\sum_{0<n<q/2} \chi(n) = (2 + \chi(2))((S_2 - S_0) + (S_3 - S_1)i).$$

It now follows at once from (2.1)–(2.4) that

$$h^* = \tfrac{1}{5}\left((S_2 - S_0)^2 + (S_3 - S_1)^2\right),$$

proving (2.3).

REMARK. The above proof is given here both for completeness and in the hope that this proof will be helpful to a future author in deriving an analogous formula for real cyclic quartic fields.

3. Solutions of (1.1) when h^* is a perfect square. As mentioned in the introduction, the author and Kenneth Williams opted not to publish the class number formula (2.3) after jointly deriving the following formulas relating the coset sums S_j to the numbers of quartic residues N_i, $i = 0, 1, 2, 3$, in subintervals of p. Such formulas are easily derivable in the quadratic and quartic cases and may well have higher power analogues.

THEOREM 3.1. *For S_j defined as in* (2.2), $j = 0, 1, 2, 3$, *we have the following formulas.*

$$\begin{aligned}
S_0 &= \frac{1}{2}\left(\frac{q-1}{4} - \frac{3}{5}(N_0 - N_3) - \frac{1}{5}(N_1 - N_2)\right),\\
S_1 &= \frac{1}{2}\left(\frac{q-1}{4} - \frac{1}{5}(N_0 - N_3) + \frac{3}{5}(N_1 - N_2)\right),\\
S_2 &= \frac{1}{2}\left(\frac{q-1}{4} + \frac{3}{5}(N_0 - N_3) + \frac{1}{5}(N_1 - N_2)\right),\\
S_3 &= \frac{1}{2}\left(\frac{q-1}{4} + \frac{1}{5}(N_0 - N_3) - \frac{3}{5}(N_1 - N_2)\right).
\end{aligned} \tag{3.1}$$

Proof. Since (3.1) may be reformulated as

$$\frac{-3}{10}(N_0 - N_3) - \frac{1}{10}(N_1 - N_2) = S_0 - \frac{q-1}{8},$$
$$\frac{3}{10}(N_0 - N_3) + \frac{1}{10}(N_1 - N_2) = S_2 - \frac{q-1}{8},$$
$$\frac{-1}{10}(N_0 - N_3) + \frac{3}{10}(N_1 - N_2) = S_1 - \frac{q-1}{8},$$
$$\frac{1}{10}(N_0 - N_3) - \frac{3}{10}(N_1 - N_2) = S_3 - \frac{q-1}{8},$$

we have, after subtracting the second equation from the first and the fourth from the third above, and squaring, that

$$\frac{9}{100}(N_0 - N_3)^2 + \frac{1}{100}(N_1 - N_2)^2 = (S_0 - S_2)^2$$

and

$$\frac{1}{100}(N_0 - N_3)^2 + \frac{9}{100}(N_1 - N_2)^2 = (S_1 - S_3)^2.$$

Upon adding we obtain

$$\frac{1}{2}\left((N_0 - N_3)^2 + (N_1 - N_2)^2\right) = \frac{1}{5}\left((S_0 - S_2)^2 + (S_1 - S_3)^2\right).$$

These are equal by the formula of Setzer (2.1) and the formula of Hudson-Williams (2.3), completing the proof of Theorem 3.1.

Solutions to the Diophantine system (1.1) fall into two distinct cases (Cases A and B in [**10**]). Throughout this section we assume we are in the former case so that

$$f = |S_0 - S_2| = |S_1 - S_2|. \tag{3.2}$$

It follows from (2.3) that h^* is a perfect square. The converse is not true as evidenced by the data (see Tables in §7) for $q = 181$ ($S_0 = 26$, $S_1 = 22$, $S_2 = 19$, $S_3 = 23$; $h^* = 25$). We therefore begin by noting a simple condition that (3.2) holds for all q when h^* is a perfect square.

LEMMA 3.1. *Let h^* be a perfect square. Then $f = |S_0 - S_2| = |S_1 - S_3|$ for all q provided h^* has no prime factor* $\equiv 1 \pmod 4$.

Proof. In view of (2.3) it is an immediate consequence of elementary number theory that $5h^*$ can be expressed as the sum of two squares in exactly one way since h^* has no prime factor of form $4n + 1$ by assumption. Thus

$$h^* = |S_0 - S_2|^2 = |S_1 - S_3|^2 = f^2.$$

We note in passing that if $5h^*$ contains S more prime factors of form $4n + 1$ than of form $4n + 3$ so that $5h^*$ can be expressed as the sum of two squares in S ways, then there generally exist q for which each of the S possibilities occurs. For example, for $5h^* = 5 \cdot 289 = 5 \cdot 17 \cdot 17 = 22^2 + 31^2 = 34^2 + 17^2 = 38^2 + 1^2$, we have

q	$\lvert N_0 - N_3\rvert$	$\lvert N_1 - N_2\rvert$
2797	22	31
3581	34	17
9293	38	1

In order to understand how these S possibilities arise in terms of the N_i, $i = 0,\ldots,3$, we need to prove the following theorem.

THEOREM 3.2. *Let q be a prime with $f = |S_0 - S_2| = |S_1 - S_3|$. Then we have*

$$h^* = |N_3 - N_0| = f, \qquad |N_1 - N_2| = 2f,$$

or

$$h^* = |N_1 - N_2| = f, \qquad |N_0 - N_3| = 2f.$$

Proof. We need only prove, in view of Lemma 3.1, that

$$h^* = |(N_3 - N_0) - (N_2 - N_1)|.$$

To do this we use (3.1) assuming, w.l.o.g., that $(h^*)^{1/2} = S_2 - S_0$. Then from (3.1) we have

$$5(S_2 - S_0) = 3N_0 + N_1 - N_2 - 3N_3,$$

$$5(S_3 - S_1) = -N_0 + 3N_1 - 3N_2 + N_3,$$

so that $4N_0 - 2N_1 + 2N_2 - 4N_3 = 0$ since $|S_2 - S_0| = |S_3 - S_1|$ by hypothesis. Upon addition we obtain

$$-5N_0 + 5N_1 - 5N_2 + 5N_3 = 5(S_3 - S_1),$$

so that

$$|(N_3 - N_0) - (N_2 - N_1)| = |S_3 - S_1| = f.$$

If $(h^*)^{1/2} = S_0 - S_2$, $S_3 - S_1$, or $S_1 - S_3$ the proof is obtained similarly and may be omitted.

It follows from (4.20) of [**10**] that (1.1) is solvable for the exponent $k = f$ in view of (3.2). It may also be solvable for $k = 1$ depending on how

p splits as a prime ideal but this is rarely the case for small p unless, of course, $f = 1$. Data suggests that Theorem 3.2 has the consequence that (1.1) is solvable only for exponents k which are multiples of f with exactly α solutions for each multiple αf unless p is an "exceptional" prime such that (1.1) is solvable when $k = 1$ even though $f > 1$. If $q \leq 61$ there are exactly k solutions for each exponent k (see [**10**, §6], [**4**], [**16**]).

EXAMPLE. Let $q = 149$. Using the generating techniques developed in [**4**] one can illustrate the above remarks for $p = 1193 \equiv 1 \pmod{q}$. However one can find and check solutions if p is small without using vast amounts of computer time, so we choose to illustrate the above (see Remark in §4) for $p = 5$ noting $(5/101)_4 = +1$. Direct computation for $(q, p) = (101, 5)$ gives the following solutions (x, u, v, w) of (1.1):

Exponent	Solution(s)
$k \neq 3\alpha, \alpha \leq 11$	NONE
$k = 3$	(19, 1, 2, 1)
$k = 6$	(53, 3, 20, 29), (245, 4, 21, 19)
$k = 9$	(289, 14, 115, 427), (3287, 43, 254, 67), (4032, 120, 168, 124).

4. Solvability of (1.1) when $h^* = 5$, 13, and 17. For $q = 109$ with $h^* = 17$ and $p = 3$, 5, and 7, the system (1.1) is solvable for the seemingly random sequence of exponents 5, 8, 10, 11, 13, 14, 15,.... In this section we show exactly which exponent (1.1) is solvable for when it is not solvable for $k = 1$, $h^* \leq 17$ and $|S_0 - S_3| \neq |S_1 - S_2|$.

It is easy to see that $h^* \equiv 1 \pmod 4$ since $S_0 + S_2 = S_1 + S_3 = (q - 1)/4 \equiv 1 \pmod 2$ as $q \equiv 5 \pmod 8$ so that

$$\frac{1}{5}\left((S_2 - S_0)^2 + (S_3 - S_1)^2\right) \equiv 1 \pmod 4.$$

It may be worth noting from Table 1, §7, the values of $q < 10{,}000$ for which $h^* = 1$, 5, 9, 13, and 17:

$h^* = 1$: $q = 5, 13, 29, 37, 53, 61,$

$h^* = 5$: $q = 101, 157, 173, 197, 349, 373,$

$h^* = 9$: $q = 149, 293, 661,$

$h^* = 13$: $q = 269, 317, 397, 509, 557, 1789,$

$h^* = 17$: $q = 109, 229, 227, 821, 853.$

Quartic class numbers grow rapidly so that it is unlikely that the above list does not include all such q. Setzer [**16**] has proved that $q \leq 61$ when $h^* = 1$ and it should be possible to modify his elegant argument to obtain upper bounds for q for larger values of h^*.

For $q = 101$, $p = 607$, we have $f = 3$ and (1.1) is solvable for $k = 3$ with $(x, u, v, w) = (-8185, -966, 1971, -5013)$. One would anticipate from §3 that (1.1) would be solvable for the exponent $k = 6$ and have two solutions. However, determination of exponents for which (1.1) is solvable is far more complicated when $|S_0 - S_2| \neq |S_1 - S_3|$. For reasons developed in §4 the "missing" second solution for $k = 6$ is, in fact, a solution for the exponent $k = 4$, namely $(x, u, v, w) = (1017773, -11298, 72615, 21177)$. This is obtained by generating an imprimitive "solution" of (1.1) for $k = 6$ (that is, one which fails to be a solution only since $(x, u, v, w, p) \neq 1$) and then dividing each of x, u, v, and w by p. The legitimacy of this procedure is rooted in Theorem 4.1 of [**4**] and the deep properties (5.41)–(5.43) of [**10**] which show that

$$p^{(S_n - S_m)} \| (x^2 - qw^2), \qquad p^{(S_n - S_m)} \| (bxw + quv), \tag{4.1}$$

where S_m is the smallest and S_n the next smallest coset sum.

We consider now the typical case of a pair (q, p) with $h^* > 1$ and $S_n - S_m = 1$ for which (1.1) is not solvable for any exponent k less than

$$f = \max\{|S_0 - S_2|, |S_1 - S_3|\} \tag{4.2}$$

but is solvable for $k = 2f - 2$. Given these conditions we now show that (1.1) is solvable for every $k \geq 3$ if $h^* = 5$ and for the exponents 5, 8, 10, 11, and every exponent greater than 12 if $h^* = 13$ or 17.

THEOREM 4.1. *If* $h^* = 1$ *then* (1.1) *is solvable for every* $k > 1$. *If* $h^* = 1$ *then* (1.1) *is solvable for every* $k \geq 1$ *iff it is solvable for* $k = 1$. *If* $h^* = 5$ *and* (1.1) *is not solvable for* $k < f$ *then it is insolvable for at most* 2 *values of* k $(k = 1, 2)$. *If* $h^* = 13$ *or* 17 *and* (1.1) *is not solvable for* $k < f$ *then it is insolvable for at most* 8 *values of* k $(k = 1, 2, 3, 4, 5, 7, 9,$ *and* $12)$.

Proof. The Theorem follows immediately from [**10**] and [**4**, Th. 4.1] noting simply that solutions for $k = m$ where $m \leq f$ and for $k = 2m - 2$ (which exist in view of [**10**]) yield solutions (see Example below) for $k = 2m$, $3m - 4$, $3m - 2$, $3m$, $4m - 6$, $4m - 4$, $4m - 2$, $4m$, etc., and $\alpha m - (2\alpha - 2) < (\alpha - 1)m$ for $\alpha \geq 3$ if $h^* = 5$ as we then have $f = 3$ and for $\alpha \geq 4$ if $h^* = 13$ or 17 as then $f = 5$.

REMARK. Since the proof of solvability of (1.1) for $k = f$ rests on the assumption that $p \equiv 1 \pmod{q}$ the above argument is not valid for $p = qf + r$, $(r/q)_4 = +1$; however, data proved by Duncan A. Buell favors the truth of all theorems presented in §§3–5 for all such quartic residues r.

We now show how to use Theorem 4.1 to actually generate the explicit solutions of (1.1) for $(q, p) = (109, 3)$.

EXAMPLE. Let $q = 109$ and let $p = 3$. With the signs of a and b chosen so that $a = -3$, $b = 10$, it is easy to see that $(x, u, v, w) = (10, -2, 2, 4)$ is a solution of (1.5) for $k = 5$. Computer data shows that there are no solutions for $k = 1, 2, 3, 4, 5, 7, 9$ and 12. The solution for $k = 8$ arises as follows.

Using Theorem 4.1 of [**4**], noting that $S_n - S_m = 1$ (see Table 2), so that by (5.4.1)–(5.4.3) of [**10**] the imprimitive "solution" of (1.5) for $k = 10$ has each of x, u, v, w divisible by p (and so $x^2 + 2q(u^2 + v^2) + qw^2$ divisible by p^2) we obtain, applying (4.2) and (4.3) of [4], that

$$x_8 = \frac{x^2 - qw^2}{4p} = 112, \qquad u_8 = \frac{xu - auw + avw + xv}{4p} = -4,$$

$$v_8 = \frac{-xu + bvw - buw - auw + avw + xv}{4p} = 20,$$

$$w_8 = -\tfrac{1}{2}(bv^2 + 2auv - bu^2) = -4.$$

It is easily checked that $(x_8, u_8, v_8, w_8) = (-112, -4, +20, -4)$ is indeed a solution of (1.1) for $k = 8$. The solution for $k = 10$ is obtained from the solutions for exponents 5 and 8 by applying (4.2) and (4.3) of [**4**] and dividing by p as for $k = 8$. In this way the author has generated solutions for exponents up to 17 and checked these against direct computer data.

5. Solvability of (1.1) in the general case. We begin this section by proving the following theorem.

THEOREM 5.1. *The system* (1.1) *is solvable for every sufficiently large exponent k provided* $h^* = 1$ *or* $|S_0 - S_3| \neq |S_1 - S_2|$ *and the smallest exponent m that* (1.1) *is solvable for is odd.*

Proof. It follows from [**10**, §6] and Theorem 4.1 of [**4**] that (1.1) is solvable for every k if $h^* = 1$. If on the other hand $|S_0 - S_3| \neq |S_1 - S_2|$ and m is the smallest exponent that (1.1) is solvable for, then by Theorem

4.1 of [**4**], (1.1) is solvable for the exponents $k = m$, $2m - 2(S_n - S_m)$, $2m$, $3m - 4(S_n - S_m)$, $3m - 2(S_n - S_m)$, $3m$, $4m - 6(S_n - S_m)$, etc., that is for each $\alpha \geq 1$ for the exponents $k = \alpha m - (2\alpha - 2)(S_n - S_m)$, $\alpha m - (2\alpha - 4)(S_n - S_m)$, $\alpha m - (2\alpha - 6)(S_n - S_m), \ldots, \alpha_m - 2(S_n - S_m)$, αm, where the products in parentheses are interpreted to be zero if they are not positive. Each of these expressions is congruent to m modulo $2(S_n - S_m)$. Since m is assumed odd and $2(S_n - S_m)$ is even the terms αm run through a complete residue class modulo $2(S_n - S_m)$ as α runs through any $2(S_n - S_m)$ consecutive integers. Thus an upper bound (although not best possible) for the exponent b such that (1.1) is solvable for all $k > b$ is provided by determining the value of α such that

$$(5.1) \qquad \alpha m - (\alpha - 1)(2S_n - 2S_m) \leq (\alpha - 2(S_n - S_m))(m).$$

Since (5.1) clearly holds for $\alpha \geq m + 1$, (1.1) is solvable for every exponent $k \geq m^2 - (S_n - S_m)(m)$.

EXAMPLE. Let $q = 181$, $p = 7$, so that $h^* = 25$. For $p \equiv 1 \pmod{q}$ Hudson and Williams [**10**] have proved that (1.1) is solvable for $f = 7$ (see Table 2) and direct computation shows that this is the smallest exponent for which (1.1) is solvable for the pair (181, 7). Since $S_m = 22$ and $S_n = 23$, Theorem 5.1 asserts that (1.1) is solvable for every $k \geq 42$. This is, we note, not a best possible bound although we also note that there is an exponent greater than $(m - 1)^2 - 2(S_n - S_m)(m - 1) = 30$ for which a solution to (1.1) cannot be generated via Theorem 4.1 of [**4**] so it may not be possible to improve the bound greatly.

COROLLARY. *If for a pair* (q, p) *the system* (1.1) *is solvable for* $k \leq 2(S_n - S_m) + 1$ *then it is solvable for every* $k \geq 4(S_n - S_m) + 2$.

Proof. The theorem is immediate from the last sentence of the proof of Theorem 5.1.

EXAMPLE. Let $q = 181$, $p = 5$. Computer data provided by Duncan Buell shows that (1.1) is solvable for $(q, p) = (181, 5)$ when $k = 3$. (The solution is $(x, u, v, w) = (3, 0, 1, 3)$). Since $S_n - S_m = 23 - 22 = 1$, $3 = 2(S_n - S_m) + 1$, and it follows from the above corollary that (1.1) is solvable for this pair for every $k \leq 4(S_n - S_m) + 2 = 6$ (in contrast to the previous example). In fact as it is easily seen to be solvable for $k = 4$ and 5 with $(x, u, v, w) = (81, 0, 3, 1)$ in the former case and $(15, 4, 9, 9)$ in the latter so that $k = 1$ and 2 are the only exponents for which (1.5) is

insolvable. In general if (1.1) is solvable for $k < f = \max\{|S_0 - S_2|, |S_1 - S_3|\}$ the system is solvable for exponents one would expect for a smaller value of h^* (in this case the exponents one would expect when $h^* = 5$: see §4).

REMARKS. The results in this section are unsatisfactory in two major aspects. First, the results (4.20) and (5.41)–(5.43) of [**10**] have only been proved for $p \equiv 1 \pmod q$ although they appear to hold for $p = qf + r$, $(r/q)_4 = +1$. The generating technique given in Theorem 4.1 of [**4**] does not depend on the assumption that $r = 1$. It would be highly desirable to have a proof in the general case (such a proof would require Brewer sums and Stickelberger's theorem). Second, the bound in Theorem 5.1 is not best possible and a more precise bound (holding for all q) would be desirable.

6. A consequence of a class number formula of Dirichlet. I close this paper with a theorem on the distribution of quartic residues in the subintervals $(0, q/4)$, $(q/4, q/2)$, $(q/2, 3q/4)$, $(3q/4, q)$ (see the last two columns of Table 2).

For every prime $q \equiv 5 \pmod 8$ it is the case that

$$N_0 + N_3 > N_1 + N_2. \tag{6.1}$$

Proof. Let c_0, c_1, c_2, c_3 be defined as before, let R_1 and T_1 denote the numbers of quadratic residues and quadratic nonresidues respectively in $(0, q/4)$, and let R_2 and T_2 denote the numbers of quadratic residues and quadratic nonresidues respectively in $(q/4, q/2)$. Then $N_0 + N_3$ is the number of elements of c_0 in $(0, q/4)$ plus the number in $(3q/4, q)$. But N_3 is clearly also the number of elements of c_2 in $(0, q/4)$ as $q \equiv 5 \pmod 8$ rather than $\equiv 1 \pmod 8$. Thus $N_0 + N_3 = R_1$. Similarly $N_1 + N_2 = R_2$.

As $q \equiv 1 \pmod 4$ we have trivially

$$\sum_{0<n<q/2} \left(\frac{n}{q}\right) = 0$$

so that

$$\sum_{q/4<n<q/2} \left(\frac{n}{q}\right) < 0$$

in view of (1.2) of [**2**] (proved first by Dirichlet). It follows that $R_2 < T_2$. Assume now that $N_0 + N_3 < N_1 + N_2$, that is $R_1 < R_2$. As $T_2 = R_1$ we must have $R_1 < R_2 < T_2 = R_1$, an obvious contradiction. This completes the proof.

REMARK. Let u_0, u_1, u_2, u_3 denote the numbers of integers in the subintervals $(0, q/4)$, $(q/4, q/2)$, $(q/2, 3q/4)$, $(3q/4, q)$, respectively, which are quadratic residues but not quartic residues (mod q). It is clear from the proof of Theorem 6.1 that we have, in addition, that for all $q \equiv 5 \pmod 8$,

$$u_0 + u_3 > u_1 + u_2.$$

TABLE 1

Class Numbers of $h^*(K) = h(K)/h\left(Q\left(\sqrt{q}\right)\right)$ *for* $5 \le q < 10{,}000$

q	h^*	q	h^*	q	h^*	q	h^*	q	h^*	q	h^*	q	h^*	q	h^*	q	h^*
5	1	773	29	1741	65	2837	157	4013	221	5309	257	6373	181	7717	673	8893	173
13	1	797	37	1789	13	2861	261	4021	361	5333	149	6389	197	7741	421	8933	425
29	1	821	17	1861	53	2909	145	4093	325	5381	181	6397	137	7757	401	8941	505
37	1	829	145	1877	53	2917	61	4133	205	5413	481	6421	613	7789	289	9013	637
53	1	853	17	1901	53	2957	85	4157	173	5437	369	6469	677	7829	405	9029	169
61	1	877	37	1933	29	3037	61	4229	101	5477	197	6581	225	7853	173	9109	277
101	5	941	41	1949	125	3061	65	4253	181	5501	149	6637	305	7877	145	9133	625
109	17	997	25	1973	45	3109	117	4261	53	5557	481	6653	229	7901	149	9157	245
149	9	1013	25	1997	85	3181	185	4349	325	5573	269	6661	1165	7933	245	9173	317
157	5	1021	41	2029	169	3221	85	4357	85	5581	53	6701	145	7949	125	9181	169
173	5	1061	73	2053	41	3229	641	4373	185	5653	153	6709	125	8053	541	9221	197
181	25	1069	29	2069	89	3253	229	4397	261	5669	85	6733	625	8069	157	9277	549
197	5	1093	185	2141	61	3301	49	4421	85	5693	229	6781	401	8093	425	9293	289
229	17	1109	29	2213	85	3373	241	4493	197	5701	505	6829	265	8101	369	9341	257
269	13	1117	85	2221	101	3389	125	4517	145	5717	261	6869 6917	233 425	8117	221	9349	185
277	17	1181	37	2237	97	3413	153	4549	65	5741	233	6949	325	8221	365	9397	169
293	9	1213	157	2269	125	3461	157	4597	89	5749	1105	6997	601	8237	173	9413	405
317	13	1229	25	2293	29	3469	229	4621	145	5813	205	7013	325	8269	481	9421	577
349	5	1237	125	2309	109	3517	73	4637	145	5821	305	7069	433	8293	225	9437	261
373	5	1277	89	2333	85	3533	117	4733	225	5861	265	7109	369	8317	173	9461	441
389	41	1301	25	2341	73	3541	65	4789	81	5869	293	7213	157	8389	313	9533	377
397	13	1373	45	2357	121	3557	121	4813	145	5981	405	7229	233	8429	397	9613	641
421	25	1381	153	2381	37	3581	289	4861	801	6029	313	7237	909	8461	365	9629	221
461	25	1429	41	2389	25	3613	125	4877	193	6037	113	7253	265	8501	241	9661	1105
509	13	1453	221	2437	53	3637	405	4909	325	6053	109	7309	89	8573	261	9677	221
541	61	1493	37	2477	85	3677	121	4933	389	6101	305	7333	425	8581	85	9733	205
557	13	1549	25	2549	149	3701	145	4957	245	6133	137	7349	305	8597	521	9749	205
613	25	1597	89	2557	205	3709	145	4973	137	6173	233	7477	865	8629	477	9781	493
653	25	1613	45	2621	145	3733	365	5021	365	6197	325	7517	317	8669	293	9829	625
661	9	1621	233	2677	361	3797	125	5077	125	6221	305	7541	725	8677	657	9901	1429
677	25	1637	85	2693	89	3821	365	5101	565	6229	281	7549	85	8693	401	9941	225
701	25	1669	85	2741	85	3853	245	5189	261	6269	257	7573	841	8741	585	9949	377
709	61	1693	53	2749	85	3877	73	5197	117	6277	125	7589	225	8821	449	9973	1009
733	45	1709	25	2789	181	3917	73	5237	125	6301	857	7621	485	8837	205		
757	125	1733	81	2797	289	3989	113	5261	185	6317	233	7669	1585	8861	169		

TABLE 2

Coset sums and numbers of quartic residues in subintervals of q

q	S_0	S_1	S_2	S_3	N_0	N_1	N_2	N_3	$N_0 + N_3$	$N_1 + N_2$
13	1	1	2	2	2	0	1	0	2	1
29	4	3	3	4	2	0	2	3	5	2
37	4	5	5	4	3	3	1	2	5	4
53	7	7	6	6	3	3	2	5	8	5
61	7	8	8	7	5	4	2	4	9	6
101	14	12	11	13	6	3	6	10	16	9
109	11	12	16	15	12	5	7	3	15	12
149	17	17	20	20	14	6	9	8	22	15
157	19	18	20	21	12	7	11	9	21	18
173	23	22	20	21	10	9	9	15	25	18
181	19	22	26	23	18	11	9	7	25	20
197	25	26	24	23	12	13	9	15	27	22
229	27	26	30	31	19	10	16	12	31	26
269	31	34	36	33	23	16	12	16	39	28
277	36	32	33	37	17	12	21	19	36	33
293	35	38	38	35	22	19	13	19	41	32
317	39	37	40	42	23	15	22	19	42	37
349	45	44	42	43	21	20	20	26	47	40
373	45	46	48	47	27	22	22	22	49	44
389	44	48	53	49	34	23	20	20	54	43
397	49	52	50	47	25	28	20	26	51	48
421	52	49	53	56	30	20	30	25	55	50
461	58	61	57	54	30	30	20	35	65	50
509	64	61	63	66	36	24	32	35	71	56
541	62	68	73	67	43	36	29	27	70	65
557	70	72	69	67	35	36	29	39	74	65
613	73	76	80	77	45	38	36	34	79	74
653	79	84	84	79	45	44	34	40	85	78
661	81	84	84	81	45	42	36	42	87	78
677	87	87	82	82	41	41	36	51	92	77

Acknowledgement. I am grateful to Duncan A. Buell for making available extremely helpful computer data and additionally indebted to Kenneth S. Williams for advice and assistance in preparing this paper.

REFERENCES

[1] Adrian Albert, *The integers of normal quartic fields*, Annals of Math., **31** (1930), 381–418.

[2] Bruce Berndt, *Classical theorems on quadratic residues*, Enseignement Math., **22** (1976), 261–304.

[3] Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory, **11** (1979), 349–398.

[4] Duncan A. Buell and Richard H. Hudson, *Solutions of certain quaternary quadratic systems*, Pacific J. Math., **114** (1984), 23–45.
[5] A. Cauchy, Mém. Institut de France, **17** (1840), 697; Oeuvres, (1), III, 388, Comptes Réndus, Paris **10** (1840), 451.
[6] L. E. Dickson, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc., **37** (1935), 363–380.
[7] P. G. Lejeune Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew Math., **281** (1840), 134–155.
[8] Hugh Edgar and Brian Peterson, *Some contributions to the theory of cyclic quartic extensions of the rationals*, J. Number Theory, **12** (1980), 77–83.
[9] Helmut Hasse, *Über die Klassenzahl abelscher Zahlkorper Akademie-Verlag*, Berlin, 1952.
[10] Richard H. Hudson, Kenneth S. Williams, and Duncan A. Buell, *Extension of a Theorem of Cauchy and Jacobi*, submitted for publication.
[11] Richard H. Hudson and Kenneth S. Williams, *A class number formula for certain quartic fields*, Carleton Mathematical Series, No. 174, 1981, Carleton University, Ottawa, Canada.
[12] Emma Lehmer, *On Euler's criterion*, J. Austral. Math. Soc., **1** (1959), 64–70.
[13] Joseph B. Muskat and Yun-Cheng Zee, *On the uniqueness of solutions of certain Diophantine equations*, Proc. Amer. Math. Soc., **49** (1975), 13–19.
[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warsaw, 1974.
[15] Ivan Niven and Herbert S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley and Sons Inc., New York, 1972.
[16] Bennett Setzer, *The determination of all imaginary, quartic, Abelian number fields with class number* 1, Math. Comp., **35** (1980), 1383–1386.
[17] Albert Leon Whiteman, *Theorems analogous to Jacobsthal's theorem*, Duke Math., **16** (1949), 619–626.

Received February 16, 1983.

UNIVERSITY OF SOUTH CAROLINA
COLUMBIA, SC 29208