PACIFIC JOURNAL OF MATHEMATICS
Vol 114, No 1, 1984

SOLUTIONS OF CERTAIN QUATERNARY QUADRATIC SYSTEMS

DUNCAN A. BUELL AND RICHARD H. HUDSON

For primes $p = qf + 1$, Diophantine systems of the type

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

have been studied by Dickson, Whiteman, Lehmer, Hasse, Zee, and Muskat and Zee. Virtually all these studies have centered on the special cases $q = 5, 13$ (the correspondence between the system (1) when $q = 5$ and the well-known system introduced by Dickson is discussed in §3). For $q = 13, 29, 37, 53$, and 61, Hudson and Williams have proved that (1) has exactly eight solutions when $k = 1$. For values of $q \equiv 5 \pmod 8$ $= a^2 + b^2$ for which the class number of the imaginary cyclic quartic field $K = Q(i\sqrt{2q + 2a\sqrt{q}})$ is greater than one, (1) may or may not be solvable when $k = 1$. In §5 we examine families of values of q and p for which there are eight solutions of (1) when $k = 1$ independent of any class number considerations. The existence of such families is somewhat surprising, as is the fact that the question of solvability for these families is independent of the primality of p or q (clearly we must have $q = a^2 + b^2$) or the restriction $p = qf + 1$. Indeed the entire study of systems of type (1) is restricted in the literature to primes $p = qf + 1$ artificially, as any completely general study should treat all primes $p = qf + r$, $(r/q)_4 = +1$.

Hudson and Williams have proved that when the class number of K is not a perfect square there are always solutions of (1) with $p \mid (x^2 - qw^2)$. We call these zero solutions and in this paper we examine the properties of such solutions in some detail (see, particularly, §2).

A major contribution of our paper appears in §4 where we derive explicit formulae for inductively generating all soutions of (1) for $k > 1$ given a basic solution for $k = 1$. Finally in §7 we apply the formulae in §4 to illustrate the Hudson-Williams-Buell extension of a theorem of Cauchy and Jacobi (see [15]).

1. Introduction and summary. Throughout this paper q will denote a positive integer $\equiv 5 \pmod 8$, $q = a^2 + b^2$, with a odd, so that

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

is an imaginary cyclic quartic field. For primes $p = qf + 1$, systems of the type

$$16p^k = x^2 + 2qu^2 + 2qv^2 + qw^2, \tag{1.2}$$
$$xw = av^2 - 2buv - au^2, \qquad (x, u, v, w, p) = 1,$$

have been studied by Dickson [3], Whiteman [**16**], Lehmer [**10, 11**], Hasse [**6**], Zee [**19**], and Muskat and Zee [**13**].

When (1.2) is solvable for, say (x, u, v, w), it is clearly solvable for

$$(1.3) \qquad (x, -u, -v, w), (x, v, -u, -w), (x, -v, u, -w),$$

and for the four solutions obtained from these four 4-tuples by changing the sign throughout. The number of solutios of (1.2) may be as great as $4 \times k \times$ the number of roots of unity, m, in K. Throughout the paper, in enumerating solutions, we will list only $km/2$ of these $4km$ solutions, and will call these the basic solutions. For $q > 5$, K has only two roots of unity, ± 1 (see, for example, [**1**], or [**8**, p. 4]), and we adopt the following notation. A basic solution of (1.2) when $q > 5$ will be denoted by $(x_{k,i}, u_{k,i}, v_{k,i}, w_{k,i})$, $1 \leq i \leq k$. It follows from Hudson's and Williams' proof of Theorem 7.1 of this paper, see [**9**], that one of these basic solutions, which we denote by $(x_{k,1}, u_{k,1}, v_{k,1}, w_{k,1})$, has the property that

$$(1.4) \qquad x_{k,1}^2 - w_{k,1}^2 \not\equiv 0 \pmod{p}$$

if the class number of K is 1. Throughout we let h^* denote the class number of K, h' the class number of its unique quadratic subfield, and define

$$(1.5) \qquad S_j = S_j(\chi_1) = \frac{1}{q} \cdot \sum_{\substack{n=1 \\ \chi_1(n)=i^j}}^{q-1} n, \qquad j = 0, 1, 2, 3,$$

where (for convenience) we distinguish the nonprincipal characters mod q of order 4, say χ_1 and χ_3, by the choice $\chi_1(2) = i$.

We call a basic solution satisfying (1.4) a nonzero solution. In the literature to date q has been small and, consequently, there has always been a nonzero basic solution. Indeed, Hudson has proved using Jacobi sums (to appear elsewhere), that if $p = qf + 1$ and q is less than 101 (so that $h^*(K)/h'(Q(\sqrt{q})) = 1$ (see [**14**])), then for every $k \geq 1$ there is exactly one nonzero basic solution of (1.2) and $k - 1$ basic solutions satisfying

$$(1.6) \quad (x_{k,i})^2 - q(w_{k,i})^2 \equiv b x_{k,i} \cdot w_{k,i} + 2q \cdot u_{k,i} \cdot v_{k,i} \equiv 0 \pmod{p}, \qquad i = 2, \ldots, k.$$

Henceforth all solutions satisfying (1.6) will be called zero solutions.

In view of the above, it appears rather surprising that, for example, for $q = 101$, $p = 607$, the system (1.2) has no nonzero basic solution for the smallest exponent for which it is solvable (see §2). We investigate the

phenomenon of zero solutions in some depth. In Theorem 2.1 we determine the zero solutions mod p in terms of the solutions of a quartic equation over $GF(p)$.

Moreover, in §2, we generalize the context in which results in this paper apply. The restriction $p = qf + 1$ has been employed in the papers of Lehmer [**10, 11**], Whiteman [**17**], and Zee [**19**]. However, Guidici, Muskat, and Robinson [**5**] have investigated solutions of quaternary systems not only for primes $p = 16f + 1$ but also for $16f + 7$. This suggests that solvability of (1.2) for $p = qf + 1$ may be generalized to the primes $p = qf + r$ where $(r/q)_4 = +1$. Such an extension requires using Brewer sums in place of the Jacobi sums considered when $p = qf + 1$. The general theory behind such solutions will not be developed here.

In §3 we see that if $q = 5$, then (1.2) has exactly 5 basic nonzero solutions and $5(k - 1)$ basic zero solutions. If, however, (1.2) is replaced (as Dickson [**3**], Lehmer [**10, 11**], and Whiteman [**16**] have done) by

$$\begin{aligned} 16p^k &= x^2 + 50u^2 + 50v^2 + 125w^2, \qquad x \equiv 1 \pmod 5, \\ xw &= v^2 - 4uv - u^2, \end{aligned} \tag{1.7}$$

then (1.7) has exactly k basic solutions of which $k - 1$ are zero solutions. (For the appropriately modified definition of zero solution when $q = 5$ see (3.2).)

In §4 we develop our central tool, Theorem 4.1, for generating explicit solutions of (1.2) for $p = qf + r$, $(r/q)_4 = +1$ (and of (1.7), when $q = 5$) for exponents $k > 1$ and values of q and p for which a solution exists when $k = 1$.

The problem of determining the smallest exponent k for which (1.2) is solvable seems very deep if $h^*(K) \neq 1$. Hudson and Williams [**9**] have shown that if $p = qf + 1$ the exponent cannot be greater than the maximum of $|S_0 - S_2|$ and $|S_1 - S_3|$. However, the size of this smallest exponent depends on whether certain ideals are principal ideals, and as a consequence, when $h^*(K)$ is not 1, it depends not only on q but also on p as well as the values of $|S_0 - S_2|$ and $|S_1 - S_3|$.

Motivated by the above remarks we examine in §5 certain families of values of q and p for which (1.2) is solvable when $k = 1$, independent of the value of $h^*(K)$. We do not attempt an exhaustive survey of all such solutions but rather derive a few which are of some interest for their aesthetic characteristics.

In §6 we use the results in §5, in conjunction with Theorem 4.1, to explicitly generate families of solutions of (1.2) when $k > 1$.

Finally, in §7, we use the tools developed in this paper to illustrate Theorem 7.1 in a number of cases with $h^*(K) > 1$, including one with $k = 7$. Also, see Theorems 7.2, 7.3, we derive congruences for the family discussed in §6.

2. A theorem on zero solutions. The following theorem may be used to determine the values x, u, v, and w mod p in any zero solution of (1.2), once any of them has been determined mod p. Since Hudson and Williams [**9**] (see Theorem 7.1) have shown that a certain product of Gauss sums determines a unique value of x mod p, which is often a value in a zero solution, the following theorem may be regarded as an extension of Theorem 7.1 relating this product of Gauss sums to all four of the parameters in a solution of (1.2) when $k = \max\{|S_0 - S_2|, |S_1 - S_3|\}$, provided that $p = qf + 1$ and that the solution is a zero solution. Moreover, the following theorem is applicable under much more general conditions. In particular, we do not require $r = 1$ ($p = qf + r$) nor even that q or p be prime, although it is necessary that q be expressible as $a^2 + b^2$.

THEOREM 2.1. *Let* (x, u, v, w) *be a zero solution of* (1.2), *that is, a solution of* (1.2) *for which* (1.6) *holds. The values of* u, v, $-u$, *and* $-v$ *are precisely the four roots in GF*(p) *of the quartic equation in* t *given by*

$$4qt^4 + 4qw^2t^2 + b^2w^4 = 0.$$

Proof. Clearly, w is determined mod p up to sign by x (see Theorem 7.1) and the equation $x^2 - qw^2 \equiv 0 \pmod{p}$. Since (x, u, v, w) is a zero solution we have that

$$u^2 + v^2 + w^2 \equiv 0 \pmod{p}, \tag{2.1}$$

as we have

$$x^2 - qw^2 \equiv x^2 + 2qu^2 + 2qv^2 + qw^2 \equiv 0 \pmod{p}.$$

Consider the quartic equation

$$4qt^4 + 4qw^2t^2 + b^2w^4 = 0.$$

Working mod p and using the fact that $q = a^2 + b^2$ it is easily seen that

$$t^2 \equiv \frac{-4qw^2 \pm \sqrt{16q^2w^4 - 16qb^2w^4}}{8q} \tag{2.2}$$

$$\equiv \frac{-4qw^2 \pm 4qw^2\sqrt{1 - b^2/q}}{8q} \equiv \frac{1}{2}w^2 \cdot \left(-1 \pm \frac{a}{\sqrt{q}}\right) \pmod{p}.$$

Next, using (1.6) and (2.1), we have

$$4q(\pm v)^4 + 4q(\pm v)^2 w^2 + b^2 w^4 \equiv 4q(\pm u)^4 + 4q(\pm u)^2 w^2 + b^2 w^4 \equiv 0 \pmod{p},$$

so that the four solutions of h given by (2.2) are precisely u, v, $-u$, and $-v$, mod p.

EXAMPLE 2.1. Let $q = 101$, $p = 607$. There are no solutions of (1.2) with $k = 1$ or 2. However, Theorem 7.1 asserts that there is a solution for $k = 3$ with

$$\prod af! \equiv -x \pmod{p = qf + 1}, \tag{2.3}$$

where the product runs over the quartic residues of q.

For $f = 6$ the product on the left-hand-side of (2.3) is congruent to 294 (mod 607). Indeed this solution, which is the only basic solution for $q = 101, p = 607$, is

$$(-8185, 966, -1971, -5013). \tag{2.4}$$

Reducing modulo p this solution becomes

$$(-294, 359, -150, 450). \tag{2.5}$$

It is easy to see that (2.5) follows from Theorem 2.1. For, choosing square root signs to yield the solution as given in (2.5) (rather than one of its other seven transforms) we have $\sqrt{q} \equiv 56 \pmod{607}$ which implies $w \equiv 450 \pmod{607}$ and

$$u \equiv \sqrt{\frac{1 - 56}{122}} \cdot w \equiv 359 \pmod{607},$$

$$v \equiv \sqrt{\frac{-1 - 56}{112}} \cdot w \equiv -150 \pmod{607}.$$

REMARK. Precise determination of $\sqrt{q} \pmod{p}$ (beginning with the determination mod prime ideal factors of p) is given in [**9**]. As the determination is complicated it will not be duplicated here although it is understood throughout that the legitimacy of operations such as the above rests on such a prior determination.

Theorem 2.1 is most useful when the Theorem derived in §4 is not applicable. For example, there are no solutions to (1.2) if $q = 101$, $p = 607$, and $k = 1$, (so that Theorem 4.1 is not applicable) but for the

solution with $k = 3$ we have

$$(x, u, v, w) \equiv (x, 517x, 112x, 271x) \pmod{p} \tag{2.6}$$

(in agreement with (2.5)) so that even in the absence of Theorem 7.1 the search for a solution is complete when the computer has checked values of x with $x^2 < 16p^k$.

EXAMPLE 2.2. $q = 101$, $p = q + r$, $(r/q)_4 = +1$, p prime. In agreement with Theorem 2.1 (see Example 2.4) we have

$$(x, u, v, w) = (247, 419, 14, 235) \equiv (110, 8, 14, 98) \pmod{137},$$
$$(x, u, v, w) = (1579, 116, 505, 589) \equiv (147, 116, 147, 52) \pmod{179},$$
$$(x, u, v, w) = (3565, 177, 482, -535) \equiv (126, 177, 120, 8) \pmod{181},$$
$$(x, u, v, w) = (31, 27, 578, 685) \equiv (31, 27, -1, 106) \pmod{193}.$$

We remark that a direct computer search revealed that the above solutions are the only basic solutions for $k = 3$ and there are no solutions for $k = 1$ or 2. Obviously this suggests that a theorem analogous to Theorem 7.1 exists when $r \neq 1$, but it would seem to be very difficult to prove such a result in full generality.

Next we reformulate Theorem 2.1 to obtain the general expression analogous to (2.6).

THEOREM 2.2. *Let q and p be odd positive integers > 1 with $q = a^2 + b^2$, a odd, $b > 0$, $p = qf + r$, $(r/q)_4 = +1$. For each value of x which is a parameter in a basic zero solution (if any exist) of* (1.2), *all parameters of this solution are given modulo p for a fixed quadratic partition of q by*

$$\left(x, \left(\frac{-a - \sqrt{q}}{2q\sqrt{q}} \right)^{1/2} \cdot x, \left(\frac{a - \sqrt{q}}{2q\sqrt{q}} \right)^{1/2} \cdot x, \frac{x}{\sqrt{q}} \right).$$

Proof. The result is immediate from the proof of Theorem 2.1. However, note directly that

$$x^2 + 2q\left(\frac{-a - \sqrt{q}}{2q^{3/2}} \right) \cdot x^2 + 2q\left(\frac{a - \sqrt{q}}{2q^{3/2}} \right) \cdot x^2 + qx^2/q$$
$$\equiv x^2 - 2x^2 + x^2 \equiv 0 \pmod{p},$$

and that modulo p,

$$\frac{x^2}{\sqrt{q}} \equiv a\left(\frac{a-\sqrt{q}}{2q\sqrt{q}}\right)x^2 - a\left(\frac{-a-\sqrt{q}}{2q\sqrt{q}}\right) - 2b\left(\frac{q-a^2}{4q^3}\right)^{1/2}$$

if and only if $q = a^2 + b^2$.

EXAMPLE 2.3. Let $q = 85$, $p = 101$, $r = 16$. Then (1.2) is solvable for $k = 1$ with the solution $(-1, 1, 2, 3)$ for the partition $q = 7^2 + 6^2$. For $k = 2$, (1.2) has two basic solutions with basic zero solution

$$(-191, 20, 9, 23). \tag{2.7}$$

Theorem 2.2 asserts that the parameters u, v, w, satisfy (selecting sign as before),

$$u \equiv \left(\frac{-7-40}{33}\right)^{1/2} \cdot (11) \equiv 20 \pmod{101},$$

$$v \equiv \left(\frac{7-40}{33}\right)^{1/2} \cdot (11) \equiv 9 \pmod{101},$$

$$w \equiv \frac{11}{-40} \equiv 23 \pmod{101}.$$

These congruences clearly hold for (2.7).

EXAMPLE 2.4. Let $q = 101$, $p = 193$, $r = 92$. For the fourth congruence in Example 2.2 we have

$$(x, u, v, w) \equiv \left(31, \left(\frac{-1-115}{123}\right)(31), \left(\frac{1-115}{123}\right)(31), \frac{31}{115}\right)$$
$$\equiv (31, 27, -1, 106) \pmod{193}.$$

3. The case $q = 5$ and the quaternary system of Dickson. For $q = 5$ the quartic field $K = Q(i(\sqrt{5+2\sqrt{5}}))$ has ten roots of unity (see, for example, [**9**]). The correspondence between the quaternary system given by (1.2) when $q = 5$ and the system

$$16p^k = x^2 + 50u^2 + 50v^2 + 125w^2, \qquad x \equiv 1 \pmod{5}, \tag{3.1}$$
$$xw = v^2 - 4uv - u^2, \qquad (x, u, v, w, p) = 1,$$

first studied by Dickson, is easy to establish (see, also, Guidici, Muskat, and Robinson [**5**, p. 345].). For example, when $k = 1$, $q = 5$, $p = 11$, the system (1.2) has the five basic solutions (x, u, v, w) equal to

$$(1, 2, -1, 5), (-4, 2, 2, 4), (1, 1, 4, -1), (11, 1, -2, 1), (-9, 3, 0, 1).$$

Only the first, however, with $5 \mid (u^2 + v^2)$ and $5 \mid w$, gives rise to the unique basic solution of (3.1) when $k = 1$, namely $(1, 0, 1, 1)$.

Hudson has proved (to appear elsewhere) that the system (3.1) has exactly k basic solutions for each exponent k. The system (1.2) when $q = 5$ appears to have 5 nonzero basic solutions and $5(k-1)$ basic zero solutions for each exponent k. Exactly one of the nonzero solutions (the one for which $5 \mid (u^2 + v^2)$ and $5 \mid w$) gives rise to the unique nonzero basic solution of (3.1) where we interpret a zero solution of (3.1) to be a solution satisfying

$$x^2 - 125w^2 \equiv xw + 5uv \equiv 0 \pmod{p}. \tag{3.2}$$

Similarly, exactly $k - 1$ of the zero solutions of (1.2) give rise to the $k - 1$ zero solutions of (3.1).

EXAMPLE 3.1. Among the fifteen solutions of (1.2) when $q = 5$, $p = 11$, and $k = 3$, there are three with $5 \mid (u^2 + v^2)$ and $5 \mid w$, namely

$$(36, 6, 42, 20), (-89, 25, 20, 25), (61, 8, 41, 5).$$

Of these the first and second are zero solutions. These clearly give the three basic solutions of (3.1) when $k = 3$, namely

$$(36, 6, 18, -4), (-89, 13, 6, 5), (61, 5, 18, -1).$$

Note that the first and second are the zero solutions of (3.1).

4. Generation of solutions for exponents greater than 1. We assume in what follows some knowledge of the properties of integers of imaginary quartic fields; see, for example, [**1**], [**4**]. The following theorem provides the basic tool for generating all solutions of (1.2) or of (3.1) for exponents greater than 1, when a solution exists for the exponent 1.

THEOREM 4.1. *Let* $q = a^2 + b^2 \equiv 5 \pmod 8$, *with* $a > 0$ *and odd*, $b > 0$, $q > 5$, *and assume that* (x, u, v, w) *is a basic solution of the system* (1.2) *for* $k = 1$. *Let* (x', u', v', w') (*dropping the subscripts*) *denote any of the basic solutions of* (4.1) *for* $k = t$. *Then the basic solutions of* (4.1) *for* $k = t + 1$ *may be generated from the solutions with exponents* 1 *and* k *and are included in the set of* 4*-tuples* (x'', u'', v'', w'') *obtained by setting*

$$\begin{aligned}
x'' &= \tfrac{1}{4} \cdot [xx' - 2quu' - 2qvv' + qww'], \\
u'' &= \tfrac{1}{4} \cdot [x'u + bvw' + bv'w + auw' + au'w + xu'], \\
v'' &= \tfrac{1}{4} \cdot [xv' + bu'w + buw' - av'w - avw' + x'v], \\
w'' &= \tfrac{1}{4} \cdot [x'w - 2auu' + 2avv' - 2uv'b - 2u'vb + xw'],
\end{aligned} \tag{4.2}$$

together with the 4*-tuples obtained by applying* (4.2) *after performing the transformations*

$$u' \to v', \quad v' \to -u', \quad w' \to -w', \tag{4.3}$$

$$u' \to -v', \quad v' \to u', \quad w' \to -w', \tag{4.4}$$

$$u' \to -u', \quad v' \to -v', \quad w' \to w'. \tag{4.5}$$

For $q = 5$ *all the above hold if* (4.1) *is replaced by*

$$16p^k = x^2 + 50u^2 + 50v^2 + 125w^2, \qquad xw = v^2 - 4uv - u^2, \tag{4.6}$$

$2quu'$ *and* $2qvv'$ *are replaced by* $50uu'$ *and* $50vv'$, *respectively, in* (4.2), *and* qww' *is replaced by* $125ww'$.

Proof. Let (x, u, v, w) be a basic solution of (4.1) for an arbitrary exponent k. Then

$$\alpha_k = \tfrac{1}{4} \cdot \left(x + iu\sqrt{2q + 2a\sqrt{q}} + iv\sqrt{2q - 2a\sqrt{q}} + w\sqrt{q} \right)$$

is an integer of K and we let (α_k) denote the principal ideal generated by α_k.

Let P_1, P_2, P_3, and P_4 denote the prime ideal factors of p in the ring of integers of $Q(e^{2\pi i/q})$. Then we have

$$(\alpha_k) \cdot (\bar{\alpha}_k) = (p)^k = \pm P_1^k P_2^k P_3^k P_4^k,$$

as the only units in K are ± 1 [**9**, p. 4]. Thus

$$(\alpha_k) = \pm P_1^c P_2^d P_3^e P_4^f, \quad (\bar{\alpha}_k) = \pm P_1^e P_2^f P_3^c P_4^d,$$

with $k = c + e = d + f$. Thus

$$(\alpha_k) = \pm P_1^c P_2^d P_3^{k-c} P_4^{k-d}.$$

It follows that solutions of (1.2) when $k = t + 1$ may be generated by considering products of integers of K of the form $\alpha_1 \alpha_t$, $t \geq 1$. There are, of course, eight choices for α_1 and eight for α_t. However, the symmetric nature of (4.2) allows us to fix $\alpha_1 = (x, u, v, w)$ and generate the solutions via (4.2), (4.3), (4.4), and (4.5). (It is easily seen that changing the sign throughout does not yield new solutions and Example 4.1 shows that all the transformations above may indeed be required to generate the solutions of (4.1).)

Before proceeding further in the proof we require the following equations. For the sake of typographic convenience, we shall denote $\sqrt{q}$ by s for the remainder of the proof.

We have

$$\begin{aligned} \sqrt{4q^2 - 4a^2q} &= 2bs \\ s\sqrt{2q + 2as} &= a\sqrt{2q + 2as} + b\sqrt{2q - 2as} \\ s\sqrt{2q - 2as} &= b\sqrt{2q + 2as} - a\sqrt{2q - 2as}\,. \end{aligned} \tag{4.3}$$

These equations are easy consequences of the fact that $q = a^2 + b^2$. To obtain the first equation in (4.3), simply note that

$$\sqrt{4q - 4a^2q} = \sqrt{4q(q - a^2)} = 2bs.$$

To obtain the second and third equations in (4.3) note first that

$$s\sqrt{2q + 2as} = a\sqrt{2q + 2as} + b\sqrt{2q - 2as}$$

$$\Rightarrow q(2q + 2as) = a^2 \cdot (2q + 2as) + b^2 \cdot (2q - 2as) + 2ab\sqrt{4q^2 - 4a^2q}$$

$$\Rightarrow 2q^2 + 2aqs = 2q^2 + 2a^3s - 2ab^2s + 4ab^2s$$

$$\Rightarrow q = a^2 - b^2 + 2b^2 = a^2 + b^2.$$

The equations now follow from reversing these steps and including the positive and negative signs for $\sqrt{q} = s$ in the last step.

Next, using (4.3), we derive (4.2) by multiplying

$$\frac{1}{4} \cdot \left[x + iu\sqrt{2q + 2as} + iv\sqrt{2q - 2as} + ws\right]$$

times

$$\frac{1}{4} \cdot \left[x' + iu'\sqrt{2q + 2as} + iv'\sqrt{2q - 2as} + w's\right],$$

and collecting the coefficients of $1/4$, $i\sqrt{2q + 2as}\,/4$, $i\sqrt{2q - 2as}\,/4$, and $s/4$ as the rational integers x'', u'', v'', and w'', respectively. This completes the proof of the theorem for $q \neq 5$. The proof for $q = 5$, being similar, is omitted.

EXAMPLE 4.1. Let $q = 29$ and $p = 59$. Since $p = qf + 1$ and $h^*(K)/h'(Q(\sqrt{q})) = 1$ it follows from Hudson's and Williams' proof of Theorem 7.1 that there is a basic solution of (4.1) when $k = 1$, which we take to be $(-4, 2, 2, 4)$.

Using (4.2) and (4.3) we obtain the primitive solutions of (1.2), $(4, 24, -16, -16)$, $(-112, -12, 20, -20)$: $k = 2$.

Again applying (4.2) and (4.3) we obtain the primitive solutions

$$(-700, 10, 170, -196), (-700, -134, -170, 52),$$
$$(1620, -54, 90, 28): k = 3.$$

These solutions are somewhat interesting as they imply that it is possible to have $x_1'' = x_2''$ for the leading parameters in two different basic solutions.

To obtain the primitive solutions for $k = 4$ we need to apply (4.2), (4.4), and (4.5). From (4.2) we obtain the solutions

$$(11024, -1044, 324, -324), (-1852, 872, 120, 2240): k = 4.$$

From (4.4) and (4.5) respectively we obtain

$$(-1744, -966, 244, 2116), (-6608, 708, -1180, -1180): k = 4.$$

Of course imprimitive solutions (that is, $(x'', u'', v'', w'') \neq 1$) are generated by (4.2)–(4.5) as well, but we do not delineate these as they are of presumably less interest.

EXAMPLE 4.2. Let $q = 85$, $p = 101$, so $r = 16$. In Example 2.1 we showed that the zero solution for $k = 2$ was $(-191, 20, 9, 23)$. This may be obtained by applying (4.2) with $(x, u, v, w) = (x', u', v', w') = (-1, 1, 2, 3)$. The nonzero solution for $k = 2$ is $(-21, 28, -13, -3)$, obtained by applying (4.1).

The primitive solutions for $k = 3$, obtained by applying (4.1) and (4.2) to the solution for $k = 1$ and to the two primitive solutions for $k = 2$ are

$$(-271, 62, 193, -333), (-2736, -112, -200, 28), (3129, -182, 79, -5).$$

5. Families of values of q and p having the same basic solution when $k = 1$. In view of the insolvability of (1.2) for k less than

$$h = \max\{|S_0 - S_2|, |S_1 - S_3|\} \tag{5.1}$$

when, for example, $q = 101$ and $p = 137$, 173, 179, 193, or 607, it is somewhat surprising when one first confronts the fact that (1.2) is solvabe for $k = 1$ when, for example, $q = 173$, $p = 347$, with $h^*(K) = 5$, and for $q = 293$, $p = 587$, with $h^*(K) = 9$. It is even more surprising at first that for these totally different values of q and p the system (1.2) has, for $k = 1$, precisely the same basic solution, namely, $(x, u, v, w) = (-4, 2, 2, 4)$. In this section we explain this phenomenon.

We define a family of values of q and p to be a set of ordered pairs (q, p) having the same basic solution when $k = 1$. These are of interest for several reasons, including, in particular, the following:

1. In §6 we will show, using Theorem 4.1, that such families have solutions for each exponent k larger than 1, whether or not q and p are prime or $h^*(K) = 1$, and that the solutions are given by explicit functions of a and b.

2. The consequences of Theorem 7.1 cannot be studied directly when the value of h in (5.1) is greater than 3 unless (1.2) is solvable when $k = 1$, as a direct search by computer in such cases could take centuries. However, using the results in this and in the following section, we are able to examine the consequences of Theorem 7.1 for k at least as large as 7.

We consider first the solutions of (1.2) of the form $(x, u, v, w) = (-4, m, m, w)$. Applying the defining conditions in (1.2) for $k = 1$ we have that $16(qf + 1) = 16 + 2qm^2 + 2qm^2 + qw^2$ and thus that $f = (4m^2 + w^2)/16$. Further, we obtain $w = bm^2/2$. It follows that (independent of class number considerations or of the primality of q or p) the system (1.2) has, for $k = 1$, $q = a^2 + b^2$, the same basic solution, namely,

$$(-4, m, m, bm^2/2) \tag{5.3}$$

for every integer $p = (m^2/4 + b^2m^4/64)^+ 1$.

As x is even in (5.3), it is easy to see that u, v, and w must also be even. Moreover, taking $q \equiv 5 \pmod 8$, we have that $b \equiv 2 \pmod 4$. The following theorem includes (5.3) as a special case.

THEOREM 5.1. *Let $q = a^2 + b^2 \equiv 5 \pmod 8$, $q > 5$, with $a > 0$ and odd, $b > 0$, and let $p = qf + 1$ be an odd positive integer. Then for $m \geq 0$ and n an odd positive integer ≥ 1, the 4-tuple*

$$(-4, 2m, 2mn, w)$$

is a basic solution of (1.2) with $k = 1$ provided that

$$w = m^2(2bn - a(n^2 - 1))$$

and

$$f = m^2\left[2s + 1 + (b'n)^2 - absn + (as)^2\right],$$

where $s = (n^2 - 1)/4$ and $b' = b/2$.

Proof. Using the defining conditions in (1.2) we have

$$16qf + 16 = 16 + 2q(n^2 + 1)(2m)^2 + qw^2$$

$$\Rightarrow f = (n^2 + 1)m^2/2 + w^2/16$$

and

$$-4w = a(n^2 - 1)(2m)^2 - 2bn(2m)^2$$
$$\Rightarrow w = m^2(2bn - a(n^2 - 1)).$$

The result is then immediate.

EXAMPLE 5.1. Taking $n = 1$ so that $w = 2bm^2$ and $s = 0$ in Theorem 5.1, we have that for $q = a^2 + b^2$, $p = qf + 1$, $k = 1$, the system (1.2) has the basic solutions

(5.4) $(-4, 2, 2, 2b)$ if and only if $f = b^2/4 + 1$,
(5.5) $(-4, 4, 4, 8b)$ if and only if $f = 4b^2 + 4$,
(5.6) $(-4, 6, 6, 18b)$ if and only if $f = 81b^2/4 + 9$,
(5.7) $(-4, 8, 8, 32b)$ if and only if $f = 64b^2 + 16$,
(5.8) $(-4, 10, 10, 50b)$ if and only if $f = 625b^2/4 + 25$,

In particular, $(-4, 2, 2, 2b)$ is a basic solution of (1.2) with $k = 1$ for the following prime values of q and p:

(5.9)

q	p	b
173	349	2
293	587	2
1229	2459	2
157	1571	6
661	6661	6
197	9851	14
349	28619	18

To cite just one of many examples of Theorem 5.1 when $n \neq 1$, take $n = 3$ so that $s = 2$. Then $f = 6$ and (1.2) has as basic solution when $k = 1$ and $m = 1$, $(-4, 2, 6, 6b - 8a)$ if and only if $f = 5 + (3b - 4a)^2/4$. In particular, for $q = 61 = 5^2 + 6^2$, $(-4, 2, 6, -4)$ is a basic solution of (1.2) for $k = 1$ when $p = 367 = 6q + 1$.

Next we consider the family which arises when one considers values of q and p with basic solution

(5.10) $$(q - 4, a, 2b, -a).$$

Using the defining conditions in (1.2) we have for $p = qf + 1$ that (5.10) is a solution of (1.2) when $k = 1$ if $f = (q + 3)/4$. Such solutions arise

frequently; we cite three:

(5.11)

q	p	solution
13	53	$(9, 3, 4, -3)$
53	743	$(49, 7, 4, -7)$
293	21683	$(289, 17, 4, -17)$.

We close this section by noting that similar results are easily established when $p = qf + r$, $r \neq 1$, $(r/q)_4 = +1$, and by giving a theorem about families with the rather aesthetic basic solution $(a, a, -b, a)$.

THEOREM 5.2. *Let q be as in Theorem* 5.1, *and let $p = qf + r$ be a positive integer. Then for each q satisfying $a^2 - 16r = sq$ with s an integer and each f with $(s + 3a^2 + 2b^2)/16$ an integer, $(a, a, -b, a)$ is a basic solution of* (1.2) *when $k = 1$ if and only if $a^2 + a = 3b^2$.*

Proof. We have from (1.2), substituting $(a, a, -b, a)$, that $a^2 - 16r = sq$ with $s = 16f - 3a^2 - 2b^2$ if and only if $f = (s + 3a^2 + 2b^2)/16$. Also, we have from (1.2) that $a^2 = ab^2 - a(a^2) - 2ba(-b)$ if and only if $3b^2 = a^2 + a$.

EXAMPLE 5.2. For $q = 13$, $r = 3$, we have $9 - 16r = -39 = -3q$, and $9 + 3 = 3(2^2)$. Since $(s + 3a^2 + 2b^2)/16 = 2$ we have that $(3, 3, -2, 3)$ is a basic solution of (1.2) when $k = 1$ if $q = 13$ and $p = 29$.

6. Solutions for exponents greater than 1 for families of values of q and p. As in §5 we define a family of values of q and p to be a set of ordered pairs (q, p) for which (1.2) has the same basic solution when $k = 1$.

We consider in this section the family

$$q = a^2 + b^2, \qquad p = \big((1 + b^2)/4\big)q + 1$$

which, by Theorem 5.1, has the basic solution $(-4, 2, 2, 2b)$ for $k = 1$. Using Theorem 4.1 we explicitly generate all solutions of (1.2) when $k = 2$ and $k = 3$ for all members of this family. Moreover we show that there are exactly two generatable basic solutions when $k = 2$. We conjecture but cannot prove (generally) that there are $k - 1$ zero solutions for every k.

THEOREM 6.1. *Let $q = a^2 + b^2 \equiv 5 \pmod 8$, $q > 5$, $a > 0$ and odd, $b > 0$, and let $p = ((1 + b^2/4)q) + 1$. Then*

$$16p^2 = x^2 + 2qu^2 + 2qv^2 + qw^2, \qquad xw = av^2 - 2buv - au^2, \tag{6.1}$$

$$(x, u, v, w, p) = 1 \tag{6.2}$$

has two solutions, namely,

$$(6.3)\quad (4 - 4q + qb^2, -4 + 2ab + 2b^2, -4 - 2ab + 2b^2, -8b),$$

$$(6.4)\quad (4 - qb^2, -4 - 2b^2, 2ab, -4a),$$

of which only the latter is a zero solution.

Proof. Applying (4.2) with

$$(x, u, v, w) = (x', u', v', w') = (-4, 2, 2, 2b)$$

we obtain (6.3). Similarly (6.4) follows upon applying (4.3). Next, as

$$q \equiv -1/(1 + b^2/4) \pmod{p},$$

we have

$$x \equiv \frac{32}{b^2 + 4} \equiv -8q \pmod{p}, \qquad w \equiv -8b \pmod{p},$$

so that (6.3) is not a zero solution as $p \nmid 64qa^2$. To show that (6.4) is a zero solution we need to show in view of (2.1), that $u^2 + v^2 + w^2 \equiv 0 \pmod{p}$. Indeed we have from (6.4) that

$$u^2 + v^2 + w^2 = 16 + 16q + 4b^2q = 16p.$$

Finally, if it straightforward to show that application of (4.5) yields a solution of (6.1) which does not satisfy (6.2). (This follows also from the fundamental property $\alpha\bar{\alpha} = p$.). Similarly it is easy to see that application of (4.4) gives the solution (6.4). By Theorem 4.1 these are the only solutions of (1.2) which can be generated from the basic solution $(-4, 2, 2, 2b)$.

THEOREM 6.2. *Let* $q = a^2 + b^2 \equiv 5 \pmod{8}$, $q > 5$, $a > 0$ *and odd*, $b > 0$, *and let* $p = ((1 + b^2/4)q) + 1$. *Then the system*

$$(6.5)\quad 16p^3 = x^2 + 2qu^2 + 2qv^2 + qw^2, \qquad xw = av^2 - 2buv - au^2,$$

$$(6.6)\quad (x, u, v, w, p) = 1,$$

has three basic solutions,

$$(x_{3,1}, u_{3,1}, v_{3,1}, w_{3,1}), (x_{3,2}, u_{3,2}, v_{3,2}, w_{3,2}), (x_{3,3}, u_{3,3}, v_{3,3}, w_{3,3}),$$

where the parameters in these ordered 4*-tuples are given explicitly by*

$$(6.7)\quad x_{3,1} = q(12 - 9b^2) - 4,$$

$$(6.8)\quad u_{3,1} = q(b^2/2 - 2) + 6 - 8b^2 + a^2b^2 + b^4 - 8ab,$$

$$(6.9)\quad v_{3,1} = q(b^2/2 - 2) + 6 - 8b^2 + a^2b^2 + b^4 + 8ab,$$

$$w_{3,1} = q(b^3/2 - 2b) + 18b - 4a^2b - 4b^3, \tag{6.10}$$

$$x_{3,2} = q(3b^2 - 4ab + 4) - 4, \tag{6.11}$$

$$u_{3,2} = q(-b^2/2) + 6 - 4ab - 2a^2 + 2b, \tag{6.12}$$

$$v_{3,2} = q(-b^2/2) + 2 - 4ab - 2b^2 - b^4 + 2a^2 - a^2b^2, \tag{6.13}$$

$$w_{3,2} = q(-b^3/2) + 6b + 8a + 2a^2b + 2b^3, \tag{6.14}$$

$$x_{3,3} = q(3b^2 + 4ab + 4) - 4 = x_{3,2} + 8abq, \tag{6.15}$$

$$u_{3,3} = q(b^2/2 - 2) + 6 + 4b^2 + 4ab - a^2b^2 - b^4, \tag{6.16}$$

$$v_{3,3} = q(b^2/2 - 2) - 2 + 4b^2 + 4ab + a^2b^2 + b^4, \tag{6.17}$$

$$w_{3,3} = q(b^3/2 - 2b) - 6b + 8a. \tag{6.18}$$

Proof. Applying (4.2) with $(x, u, v, w) = (-4, 2, 2, 2b)$ and with (x', u', v', w') given by (6.3) we obtain (6.7)–(6.10). Applying (4.2) with $(x, u, v, w) = (-4, 2, 2, 2b)$ and with (x', u', v', w') given by (6.4) we obtain (6.11)–(6.14). Finally, applying (4.3) with $(x, u, v, w) = (-4, 2, 2, 2b)$ and with (x', u', v', w') given by (6.3) we obtain (6.15)–(6.18). It is straightforward, though rather tedious, to show that applications of (4.4) and of (4.5) yield no new primitive solutions (that is solutions satisfying not only (6.5) but also (6.6)).

EXAMPLE 6.1. Theorem 6.1 holds for the following ordered pairs (q, p) with both q and p prime and $p < 100{,}000$:

$$\begin{aligned} &(29, 59), (53, 107), (157, 1571), (173, 347), (197, 9851), \\ &(293, 587), (349, 28619), (461, 11987), (509, 62099), \\ &(557, 27851), (773, 94307), (821, 41051), (1229, 2459). \end{aligned} \tag{6.19}$$

Of these we are particularly interested in the pairs (q, p) with q such that $h^*(K)/h'(Q(\sqrt{q})) = 5$ or 9 as it follows from Theorem 7.1 that products of factorials appearing in (7.2) are congruent (mod p) to parameters in solutions of (6.5)–(6.6) if q and p are prime (as then we have $h = \max\{|S_0 - S_2|, |S_1 - S_3|\} = 3$). We include a brief table.

REMARKS. The primes $q = 149, 373, 661$ are the only primes $< 10{,}000$ with $h^*(K)/h'(Q(\sqrt{q})) = 3$ or 5 for which no ordered pair (q, p) appears above. Of course, for such primes, if one can find prime values of p for which (1.2) is solvable when $k = 1$, it is easy to use Theorem 4.1 to generate the solutions for the exponent 3 whose parameters are related to

the appropriate product of factorials as given in (7.2). Of course, if no solution exists when $k = 1$, as for $(q, p) = (101, 607)$, the methods of this section do not apply and one must use different techniques, such as the one given in §2, to generate the solution for $k = 3$.

It may appear at first glance that the results of this section carry over unchanged if (1.2) is solvable for $k = m > 1$ and not for $k < m$ with one basic solution when $k = m$, 2 primitive solutions when $k = 2m$, etc. Although this is nearly the case the fact is that the zero solution for $(q, p) = (101, 607)$ when $k = 3$, given by (2.4), generates only one primitive solution when $k = 6$. Moreover direct computation of solutions for $(101, 3)$ and $(101, 5)$ when $k = 6$ yields only one basic (zero) solution. Thus it appears that when the basic solution for the minimal exponent is a zero solution the number of primitive solutions for multiples of the minimal exponent is less than when the basic solution is a nonzero solution. This is certainly surprising and underscores the significance of zero solutions.

7. Consequences of a quartic extension of a theorem of Cauchy and Jacobi. In [9] Hudson and Williams prove a quartic analog of a theorem of Cauchy and Jacobi (see H. J. S. Smith [15] for a discussion of Jacobi's proof). We numerically illustrate in Examples 7.1–7.3 only one of the cases arising in this rather complicated theorem. However, our results apply also to the companion case (Case B in [9]).

THEOREM 7.1. *Let* $q = a^2 + b^2 \equiv 5 \pmod 8$, $q > 5$, *be prime so that* $K = Q(i(\sqrt{2q + 2a\sqrt{q}}))$ *is an imaginary cyclic quartic field with class number given by* (*see* [8])

$$h^*(K) = \left((S_0 - S_2)^2 + (S_1 - S_3)^2\right) \cdot h'\left(Q\left(\sqrt{q}\right)\right)/2$$

where S_j, $j = 0, 1, 2, 3$, *are given by* (1.5), S_m *denotes the smallest value of* S_j, *and* S_e *is the smallest or the second smallest value of* S_j (*these coincide iff* $|S_0 - S_2| = |S_1 - S_3|$); $h'(Q(\sqrt{q}))$ *denotes the class number of* $Q(\sqrt{q})$.

Let h be defined by $h = \max\{|S_0 - S_2|, |S_1 - S_3|\}$ and let the signs of x, a, and b be fixed by $x \equiv -4 \pmod q$, $a \equiv 1 \pmod 4$, $b \equiv -((q-1)/2)! \cdot a \pmod q$. Then there is a solution of the quaternary quadratic system

$$(7.2) \qquad 16p^h = x^2 + 2qu^2 + 2qv^2 + qw^2, \quad av^2 - 2|b|uv - au^2,$$

such that for $j = 0$ or 1 we have

$$F_{j,r} \cdot p^{S_e - S_m} \equiv \frac{-x}{2} \pm \frac{a(x^2 - qw^2)w}{8(bxw/2 + quv)} \pmod{p^{S_e - S_m + 1}} \tag{7.2}$$

for every prime $p = qf + 1$. In this notation we have

$$F_{j,r} = \frac{(-1)^{\min(S_j, S_{j+2})}}{\prod_{\alpha \in C_{j+r}} \alpha f!}$$

with C_{j+r} being the $j + r$th coset formed with respect to the fourth powers (mod p) and $r = 0$ or 2 according as S_j is less than S_{j+2} or conversely. The plus sign holds on the right-hand-side of the congruence (7.2) if and only if $j = 1$ and $|S_1 - S_3| \geq |S_0 - S_2|$; the minus sign holds if and only if $j = 0$ and the above inequality is reversed; both signs hold if

$$h^*(K)/h'\left(Q\left(\sqrt{q}\right)\right) = (S_0 - S_2)^2 = (S_1 - S_3)^2.$$

Lastly, the expression on the right-hand-side of the congruence simplifies to $-x$ if (x, u, v, w) is a zero solution, that is, satisfies (1.6).

The proof of Theorem 7.1, as one might imagine, is quite complex, requiring not only the Davenport-Hasse relation in a form given by Yamamoto [**18**] and Stickelberger's Theorem, but also the recent explicit evaluation of the quartic Gauss sum given by Matthews [**12**].

Duncan Buell contributed to [**9**] in several ways, including, in particular, providing examples of the consequences of this theorem for $(q, p) = (101, 607)$ and $(157, 1571)$ with class number 5 and for $(q, p) = (149, 1193)$ with class number 9. In this section we note that the methods developed in §§2, 4 and 6 of this paper make it possible to illustrate the consequences of Theorem 7.1 for values of q with h^*/h' quite large. In particular, we include an example for which the class number is 25 and

$$h = \max\{|S_0 - S_2|, |S_1 - S_3|\} = 7.$$

We begin by proving two theorems relating to solutions when $h = 3$ for the family defined in Theorem 6.1 ($h = 3$ iff $h^*/h' = 5$ or 9).

THEOREM 7.2. *Let* $q = a^2 + b^2 \equiv 5 \pmod 8$, $q > 5$, *be prime, with* $a \equiv 1 \pmod 4$, $b \equiv -(q-1)/2!a \pmod q$, $p = ((1 + b^2/4)q) + 1$. *Let* $h^*/h' = 9$, *so that* $h = 3$ *in* (7.1). *Then we have, using the notation of Theorem* 7.1, *that*

$$F_{j,r} \cdot p^{S_e - S_m} \equiv \frac{64 - 32b^2}{2b^2 + 8} \pm \left(12b + b^3(a^2 + b^2)\right) \cdot (a^2 + b^2)^{1/2}$$

modulo $p^{S_e - S_m + 1}$, *where the plus sign holds for exactly one of* $j = 0$ *or* 1 *and the minus sign for the other. Further,*

$$F_{0,r} + F_{1,r} \equiv \frac{64 - 32b^2}{b^2 + 4} \pmod{p}. \tag{7.3}$$

Proof. From the proof of Theorem 7.1 we have that

$$F_{j,r} \cdot p^{S_e - S_m} \equiv -x/2 \pm w\sqrt{q}\,/2 \pmod{p^{S_e - S_m + 1}}$$

where the plus sign holds for exactly one of $j = 0$ or 1. When the class number is 9, the products of factorials in (7.3) cannot correspond to parameters in a zero solution as then one of $-x/2 \pm w\sqrt{q}\,/2$ is congruent to 0 (mod p) and thus not to any product of factorials (mod p).

We now appeal to (6.7) and the congruence $q \equiv -4/(b^2 + 4)$ to obtain

$$\frac{-x_{3,1}}{2} \equiv \frac{64 - 32b^2}{2b^2 + 8} \pmod{p}.$$

To complete the proof we need to show that

$$w_{3,1}/2 \equiv 12b + b^3(a^2 + b^2) \pmod{p}.$$

This appears difficult to establish directly from (6.10). However, from $(x, u, v, w) = (-4, 2, 2, 2b)$ we have, using the binomial theorem and cancelling $\sqrt{q}$, that

$$w\sqrt{q} \equiv \left(2 + b\sqrt{q}\right)^3 - \left(2 - b\sqrt{q}\right)^3 \Rightarrow w \equiv 24b + 2b^3q \pmod{p} \tag{7.4}$$

from which the result follows immediately.

REMARK. Again, we emphasize that the sign of $\sqrt{q}$ is determined unambiguously in [**9**] and this determination is necessary to establish the legitimacy of the above operations (the reader is directed to [**9**] for more precise information.) This result (7.3) is rather remarkable as it shows that the expression on the left-hand-side of (7.3) is congruent to a simple function of the one variable b, which arises from the basic solution $(-4, 2, 2, 2b)$, for very different values of q, p, and a.

EXAMPLE 7.1. For $(q, p) = (173, 347)$, $a = 13$, and for $(q, p) = (293, 587)$, $a = 17$, we have $b = 2$, so that $-x_{3,1} \equiv (32b^2 - 64)/(b^2 + 4) \equiv 8 \pmod{p}$; see Table 1. Also, we have from (7.4) that

$$w_{3,1} \equiv 24b + 2b^3q \equiv 48 + 16q \equiv 48 - 64/(b^2 + 4) \equiv 40 \pmod{p}.$$

For $q = 293$ we have $h^*/h' = 9$, $S_0 = 35$, $S_1 = 38$, $S_2 = 38$, $S_3 = 35$ (see [8]) so that, appealing to the generalized Wilson Theorem, see, for example, [15], we have, as $(q-1)/4$ is odd if q is congruent to 5 mod 8,

$$\prod_{\alpha \in C_2} \alpha f! + \prod_{\alpha \in C_1} \alpha f! \equiv \frac{64 - 32b^2}{b^2 + 4} \equiv -8 \pmod{p}$$

for $(q, p) = (293, 587)$. Using a simple computer program we obtain

$$\prod_{\alpha \in C_2} \alpha f! \equiv 274 \pmod{587}, \qquad \prod_{\alpha \in C_1} \alpha f! \equiv 305 \pmod{587},$$

and $274 + 305 = 579 \equiv -8 \pmod{587}$. For $q = 173$ we have $h^*/h' = 5$ and this case will be considered next.

THEOREM 7.3. *Let q and p be as in Theorem 7.2. Let $h^*/h' = 5$, so that $h = 3$ in (7.1). If the product of factorials on the left-hand-side of (7.2) is determined in terms of the solutions $(x_{3,2}, u_{3,2}, v_{3,2}, w_{3,2})$ or $(x_{3,3}, u_{3,3}, v_{3,3}, w_{3,3})$, given by (6.11)–(6.18), then*

$$F_{j,r} \equiv \frac{-16(b^2 \pm ab + 2)}{b^2 + 4} \pmod{p} \tag{7.5}$$

where the $\pm$ sign on the right-hand-side of (7.5) depends on which of these is the determining solution.

Proof. As it is proved in [9] that the indicated solutions are zero solutions, we have by Theorem 7.1 that $F_{j,r} \equiv -x_{3,2}$ or $-x_{3,3} \pmod{p}$, where $j = 0$ if $|S_0 - S_2| = 3$ and $j = 1$ if $|S_1 - S_3| = 3$ and $r = 0$ or 2 according as $S_j < S_{j+2}$ or conversely.

By (6.11), we have, as $q \equiv -4/(b^2 + 4) \pmod{p}$, that

$$-x_{3,2} = q(3b^2 - 4ab + 4) - 4 \equiv \frac{-12b^2 - 16ab - 16 - 4b^2 - 16}{b^2 + 4}$$

$$\equiv \frac{-16(b^2 + ab + 2)}{b^2 + 4} \pmod{p}.$$

Similarly, by (6.15) we have $-x_{3,3} \equiv -16(b^2 - ab + 2)/(b^2 + 4)$, completing the proof.

EXAMPLE 7.2. We give an example which shows that both possibilities in Theorem 7.3 can occur. For $(q, p) = (173, 347)$ we have $h^*/h' = 5$,

$S_0 = 23$, $S_1 = 22$, $S_2 = 20$, $S_3 = 21$, so that by Theorems 7.1 and 7.3 we have

$$(7.6)\qquad \frac{(-1)^{20}}{\prod_{\alpha\in C_2}\alpha f!} \equiv -x_{3,2} \quad \text{or} \quad -x_{3,3} \equiv \frac{-16(b^2 \pm ab + 2)}{b^2 + 4} \pmod p.$$

As the product on the left-hand-side of (7.6) is congruent to 64 (mod 347) it is clear from Table 1 that it is determined in terms of the solution $(x_{3,3}, u_{3,3}, v_{3,3}, w_{3,3})$.

For $(q, p) = (157, 1571)$, we have $h^*/h' = 5$, $S_0 = 19$, $S_1 = 18$, $S_2 = 20$, $S_3 = 21$, so that

$$(7.7)\qquad \frac{(-1)^{18}}{\prod_{\alpha\in C_1}\alpha f!} \equiv -x_{3,2} \quad \text{or} \quad -x_{3,3} \equiv \frac{-16(b^2 \pm ab + 2)}{b^2 + 4} \pmod p$$

and in this case we see from Table 1 that the product is determined in terms of the solution $(x_{3,2}, u_{3,2}, v_{3,2}, w_{3,2})$.

We close by showing how Theorem 4.1 can be used to illustrate the consequences of Theorem 7.1 when $h = \max\{|S_0 - S_2|, |S_1 - S_3|\} > 3$. (When $h > 3$ a direct computer search for solutions of (7.1) without a generating formula is infeasible.)

EXAMPLE 7.3. Let $q = 1229$, $p = 2459$. Then $S_0 = 154$, $S_1 = 157$, $S_2 = 153$, $S_3 = 150$, so that $h = 7$ and $h^*/h' = 25$. By Example 6.1 the solution $(-4, 2, 2, 4)$ is a basic solution of (1.2) when $k = 1$. Appealing to Theorem 4.1 we find k basic solutions to (1.2) for each $k \le 7$. For at least one of the seven solutions (x, u, v, w) when $k = 7$ we should have, by Theorem 7.1, that

$$\frac{(-1)^{150}}{\prod_{\alpha\in C_3}\alpha f!} \equiv -x \pmod p.$$

Indeed, we have the following six values for x parameters in the six zero solutions.

x	$-x \pmod p$
1941085913380	−1580
158420410516	−1905
195628041396	−2149
2176521176300	−1167
1698617112964	−1088
−2408791636396	−2427

For $q = 1229$, $p = 2459$, direct computation shows that the solution implied by Theorem 7.1 is the second listed above, whose other parameters are

$$u = 29578204262$$
$$v = -22409982278$$
$$w = -65596421516.$$

8. Computing. The numerical examples in this paper were computed in BASIC on the Xerox Sigma 9 at Carleton University, Ottawa, Canada, in FORTRAN G, FORTRAN H, VS FORTRAN, and PL/I on the IBM 3033 of the System Network Computer Center, Louisiana State University, in FORTRAN and Business BASIC on the Data General Eclipse S/140 of the Computer Science Department, Louisiana State University, and using additional computing and telecommunications equipment supplied by Rudd Computer Systems, Inc., of Baton Rouge, Louisiana.

9. Acknowledgement. We are deeply indebted to Kenneth S. Williams for a key idea leading to the proof of Theorem 4.1.

TABLE 1

Solutions when $k = 3$ and $h^*(K)/h'\left(Q\left(\sqrt{q}\right)\right) = 5$ or 9

q	p	h*/h'	Solution				mod p			
157	1571	5	(-48988,	7354,	8410,	11412)	(-287,	-501,	555,	415)
			(-23868,	-3254,	-8570,	-14948)	(-303,	-112,	-715,	762)
			(59028,	-2726,	8042,	15124)	(-670,	-1155,	187,	-586)
173	347	5	(-4156,	458,	874,	-1348)	(8,	111,	180,	40)
			(-15228,	-774,	-810,	116)	(40,	-80,	-116,	116)
			(20756,	-566,	602,	92)	(-64,	128,	-92,	92)
197	9851	5	(-345148,	55850,	56074,	253988)	(-363,	-3256,	-3032,	-2138)
			(105588,	-18966,	-58362,	-264676)	(-2773,	736,	744,	1301)
			(127652,	-18854,	58250,	264692)	(-411,	848,	-856,	-1285)
293	587	9	(-7036,	874,	1418,	-2308)	(8,	287,	244,	40)
			(-35164,	-1286,	-1322,	148)	(56,	112,	-148,	148)
			(44532,	-1014,	1050,	124)	(-80,	-160,	-124,	124)
349	28619	5	(-1013500,	165610,	167050,	980316)	(-11835,	-6104,	-4664,	7270)
			(214980,	-56294,	-170570,	-1004972)	(13972,	944,	1144,	-3307)
			(466260,	-55574,	169850,	1005052)	(8356,	1664,	-1864,	3387)

REFERENCES

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

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

[3] L. E. Dickson, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc., **37** (1935), 363–380.

[4] Hugh Edgar and Brian Peterson, *Some contributions to the theory of cyclic quartic extensions of the rationals*, J. Number Theory, **12** (1980), 77–83.

[5] Reinaldo E. Giudici, Joseph B. Muskat, and Stanley F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc., **171** (1972), 317–346.

[6] Helmut Hasse, *Der 2^n-te Potenzcharakter von 2 im Korper der 2^n-ten Einheitswurzeln*, Rend. Circ. Mat. Palermo, Series 2, **7** (1958), 185–244.
[7] _____, *Vorlesungen uber Zahlentheorie*, Zweite Auf., Springer-Verag, Berlin, 1964.
[8] Richard H. Hudson and Kenneth S. Williams, *A class number formula for certain quartic fields*, Carleton Mathematical Series No. 174, 1981, Carleton University, Ottawa.
[9] Richard H. Hudson, Kenneth S. Williams, and Duncan A. Buell, *Extension of a theorem of Cauchy and Jacobi*, (submitted).
[10] Emma Lehmer, *The quintic character of 2 and 3*, Duke Math. J., **18** (1951), 11–18.
[11] _____, *On Euler's criterion*, J. Austral. Math. Soc., **1** (1959), 64–70.
[12] C. R. Matthews, *Gauss sums and elliptic functions, II. The quartic sum*, Invent. Math., **54** (1979), 23–52.
[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] Bennett Setzer, *The determination of all imaginary, quartic, Abelian number fields with class number* 1, Math. Comp., **35** (1980), 1383–1386.
[15] H. J. S. Smith, *Report on the Theory of Numbers*, Chelsea, New York, 1964.
[16] Albert Leon Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math., **74** (1952), 89–97.
[17] Albert Leon Whiteman, *Theorems on Brewer and Jacobsthal Sums, II.*
[18] Koichi Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combinatorial Theory-Ser. A, **1** (1966), 476–489.
[19] Yun-Cheng Zee, *The Jacobi sums of orders thirteen and sixty and related quadratic decompositions*, Math. Z., **115** (1970), 259–272.

Received June 2, 1982. Research by second author was supported by Natural Sciences and Engineering Research Council Canada grant #A-7233.

DEPARTMENT OF COMPUTER SCIENCE
LOUISIANA STATE UNIVERSITY
BATON ROUGE, LA 70803

AND

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF SOUTH CAROLINA
COLUMBIA, SC 29208