MATHEMATICS OF COMPUTATION
VOLUME 43, NUMBER 168
OCTOBER 1984, PAGES 603-613

Products and Sums of Powers of Binomial Coefficients mod p and Solutions of Certain Quaternary Diophantine Systems

By Richard H. Hudson*

Abstract. In this paper we prove that certain products and sums of powers of binomial coefficients modulo $p = qf + 1$, $q = a^2 + b^2$, are determined by the parameters x occurring in distinct solutions of the quaternary quadratic partition

$$16p^\alpha = x^2 + 2qu^2 + 2qv^2 + qw^2, \qquad (x, u, v, w, p) = 1,$$
$$xw = av^2 - 2buv - au^2, \qquad x \equiv 4 \pmod q), \alpha \geqslant 1.$$

The number of distinct solutions of this partition depends heavily on the class number of the imaginary cyclic quartic field

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

as well as on the number of roots of unity in K and on the way that p splits into prime ideals in the ring of integers of the field $Q(e^{2\pi i p/q})$.

Let the four cosets of the subgroup A of quartic residues be given by $c_j = 2^j A, j = 0, 1, 2, 3$, and let

$$s_j = \frac{1}{q} \sum_{t \in c_j} t, \qquad j = 0, 1, 2, 3.$$

Let s_m and s_n denote the smallest and next smallest of the s_j respectively. We give new, and unexpectedly simple determinations of $\prod_{k \in c_n} kf!$ and $\prod_{k \in c_{n+2}} kf!$, in terms of the parameters x in the above partition of $16p^\alpha$, in the complicated case that arises when the class number of K is > 1 and $s_m \neq s_n$.

1. Introduction and Summary. Throughout, p will denote a prime $= qf + 1$ with $q = a^2 + b^2 \equiv 5 \pmod 8$ prime, $a \equiv 1 \pmod 2$, $b > 0$. Quaternary quadratic representations of p^α or $16p^\alpha$, $\alpha \geqslant 1$, such as

$$\begin{aligned} 16p^\alpha &= x^2 + 2qu^2 + 2qv^2 + qw^2, \qquad (x, u, v, w, p) = 1, \\ xw &= av^2 - 2buv - au^2, \qquad x \equiv 4 \pmod q), \end{aligned} \tag{1.1}$$

have been studied by, e.g., Dickson [2], Whiteman [15], Lehmer [9], Hasse [5], Giudici, Muskat, and Robinson [4], Muskat and Zee [12], and Hudson, Williams, and Buell [7]. Determination of the number of solutions (if any) of (1.1) for an arbitrary exponent α is a deep and complex problem as it depends on the class number of the imaginary cyclic quartic field

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

Received December 23, 1982.
1980 *Mathematics Subject Classification*. Primary 10C05; Secondary 12C20, 12C25.
*Research supported by National Research Council Canada Grant #A-7233.

on the number of roots of unity in K, and on the way that p splits into prime ideals in the ring of integers of the cyclotomic field $Q(e^{2\pi i p/q})$.

For $q \neq 5$, the only roots of unity in K are ± 1 (see, e.g., [6, p. 4]). However, for $q = 5$, there are 10 roots of unity in K and (as a consequence discussed in Section 3 of [1]) the appropriate system to consider in this case is the system given first by Dickson [2], namely,

$$(1.3)\qquad \begin{gathered} 16p^\alpha = x^2 + 50u^2 + 50v^2 + 125w^2, \qquad (x, u, v, w, p) = 1, \\ xw = v^2 - 2uv - u^2, \qquad x \equiv 1 \pmod 5. \end{gathered}$$

Determination of binomial coefficients of the type $\binom{rf}{sf}$ modulo $p = qf + 1$, $1 \leqslant r < s \leqslant q - 1$, in terms of parameters in quadratic forms has been a topic of interest since the late 1820's when Gauss [3] determined $\binom{2f}{f}$ modulo $p = 4f + 1$ in terms of the parameter a in the quadratic form $p = a^2 + b^2$. For a survey of known results see [8].

In [10] Emma Lehmer showed that for $p = 5f + 1$ and (x, u, v, w) any of the four solutions of (1.3) with $\alpha = 1$ one has

$$(1.4)\qquad \binom{2f}{f} \equiv -\frac{x}{2} + \frac{(x^2 - 125w^2)w}{8(xw + 50uv)} \pmod{p = 5f + 1},$$

and

$$(1.5)\qquad \binom{3f}{f} \equiv -\frac{x}{2} - \frac{(x^2 - 125w^2)w}{8(xw + 50uv)} \pmod{p = 5f + 1}.$$

For $p = 13f + 1$ and (x, u, v, w) any of the four solutions of (1.1) when $\alpha = 1$, Hudson and Williams [8, Theorem 16.1] proved that

$$(1.6)\qquad \binom{4f}{f} \equiv -\frac{x}{2} + \frac{3(x^2 - 13w^2)w}{8(xw + 13uv)} \pmod{p = 13f + 1},$$

and

$$(1.7)\qquad \binom{7f}{2f} \equiv -\frac{x}{2} - \frac{3(x^2 - 13w^2)w}{8(xw + 13uv)} \pmod{p = 13f + 1}.$$

Results analogous to (1.4)–(1.7) have recently been obtained for all $q > 13$; see [7, Section 6]. The starting point for these results was Matthews' [11] explicit evaluation of the quartic Gauss sum and a congruence for factorials modulo p derived from the Davenport-Hasse relation in a form given by Yamamoto [16]. Using these tools and Stickelberger's theorem [14], Hudson and Williams explicitly determined $\prod kf!$ modulo $p = qf + 1$ for all $q > 5$, where k runs over any of the four cosets which may be formed with respect to the subgroup of quartic residues modulo q, in terms of parameters in systems of the type (1.1).

We begin this paper by proving that certain products and sums of powers of products of factorials modulo $p = qf + 1$ determine (and conversely are determined by) the parameters x occurring in distinct solutions of (1.1) when $\alpha > 1$. For example we show that

$$(1.8)\qquad \binom{4f}{f}^3 + \binom{7f}{2f}^3 \equiv x_{3,1} \pmod{p = 13f + 1},$$

$$(1.9)\qquad \binom{4f}{f}\binom{7f}{2f}^2 \equiv x_{3,2} \pmod{p = 13f + 1},$$

$$(1.10)\qquad \binom{4f}{f}^2\binom{7f}{2f} \equiv x_{3,3} \pmod{p = 13f + 1},$$

where the $x_{k,i}$, $1 \leqslant i \leqslant k$, denote from this point on the solution(s) of (1.1) when $\alpha > 1$. (The subscripts will be dropped when there is no ambiguity (as when, e.g., $\alpha = 1$).)

Let the four cosets of the subgroup A of quartic residues be given by $c_j = 2^j A$, $j = 0, 1, 2, 3$, and let

$$(1.11)\qquad s_j = \frac{1}{q} \sum_{t \in c_j} t, \qquad j = 0, 1, 2, 3.$$

Define h to be the odd positive integer given by

$$(1.12)\qquad h = \max(|s_0 - s_2|, |s_1 - s_3|).$$

When (1.1) is solvable for $\alpha = 1$, exactly four of the solutions $(x_{3,i}, u_{3,i}, v_{3,i}, w_{3,i})$ for each α satisfy $x_{3,i}^2 - q w_{3,i}^2 \not\equiv 0 \pmod{p}$ and it is convenient to let this value of i be 1. Using Stickelberger's theorem [14], Hudson and Williams [7] have shown that (1.1) is always solvable for $\alpha = h$. If α_0 denotes the exponent such that (1.1) is solvable for α_0 but not for $\alpha < \alpha_0$, we would expect to find $4\alpha/\alpha_0$ solutions to (1.1) for each α a multiple of α_0 and no solutions for α not a multiple of α_0. This appears to be the case whenever $|s_0 - s_2| = |s_1 - s_3|$ and so, certainly, for all $q < 101$ (as then the class number of K is 1—see [6], [13]). Moreover, this is the case for all numerical examples which may be computed by direct search techniques. A major point in this paper appears in Section 4 where we show that the unexpected does occur (and frequently). Indeed, whenever $|s_0 - s_2| \neq |s_1 - s_3|$ (which will always be the case when the class number is not a perfect square) and $\alpha_0 = h$, we show that there are only $4\alpha_0$ solutions to (1.1) when $\alpha = 2\alpha_0$. More significantly and surprisingly, the "missing" $4\alpha_0$ solutions (these fail to be genuine solutions as they do not satisfy $(x_{2,2}, u_{2,2}, v_{2,2}, w_{2,2}, p) = 1$) turn out, upon division by a certain power of p to be solutions of (1.1) for α not a multiple of α_0.

Henceforth, s_m denotes the smallest and s_n the next smallest of the s_j. In the closing section of this paper, Section 5, we give new, simple, and unexpected determinations of $\prod_{k \in c_n} kf!$ and $\prod_{k \in c_{n+2}} kf!$ modulo p in the most complicated case treated in [7], namely, the case that $s_m \neq s_n$.

2. Explicit Binomial Coefficient Theorems When $\alpha = 2h$ and $s_m = s_n$. Let P_r be a prime ideal divisor of p in the ring of integers of $Q(e^{2\pi i p/q})$. It follows from (5.33) and (5.59) of [7] that

$$(2.1)\qquad \prod_{k \in c_{m+2}} kf! \equiv (1)^{s_{m+2}}\left(\frac{x}{2} + \frac{w}{2}\sqrt{q}\right) \pmod{P_r}, \qquad r \in c_{2-(m+2)},$$

and

$$(2.2)\qquad \prod_{k \in c_{n+2}} kf! \equiv (-1)^{s_{n+2}}\left(\frac{x}{2} + \frac{w}{2}\sqrt{q}\right) \pmod{P_r}, \qquad r \in c_{2-(n+2)}.$$

However, we have assumed $s_m = s_n$ in this section so we have that (having interpreted $\sqrt{q}$ as a rational expression (mod p) and finding that $\sqrt{q}$ differs by a sign in (2.1), (2.2)—see (5.3), (5.4) of [7]),

$$\left(\prod_{k \in c_{m+2}} kf!\right)^2 + \left(\prod_{k \in c_{n+2}} kf!\right)^2 \equiv \frac{x^2}{2} + \frac{qw^2}{2} \pmod{p}. \tag{2.3}$$

Using Theorem 4.1 of [1] we now prove the following theorem.

THEOREM 2.1. *There exist four solutions of* (1.1) *with*

$$\alpha = h = \max(|s_0 - s_2|, |s_1 - s_3|),$$

namely $(x_{h,1}, u_{h,1}, v_{h,1}, w_{h,1})$, $(x_{h,1}, -u_{h,1}, -v_{h,1}, w_{h,1})$, $(x_{h,1}, v_{h,1}, -u_{h,1}, -w_{h,1})$, $(x_{h,1}, -v_{h,1}, u_{h,1}, -w_{h,1})$ *such that* $p \nmid (x_{h,1} - qw_{h,1}^2)$, $p \nmid (bx_{h,1}w_{h,1} + qu_{h,1}v_{h,1})$ *provided* $s_m = s_n$. *Let* $\alpha = 2h$. *Then*

$$\left(\prod_{k \in c_{m+2}} kf!\right)^2 + \left(\prod_{k \in c_{n+2}} kf!\right)^2 \equiv x_{2h,1} \pmod{p} \tag{2.4}$$

for four solutions of (1.1) *which satisfy* $p \nmid (x_{2h,1}^2 - qw_{h,1}^2)$ *and*

$$\left(\prod_{k \in c_{m+2}} kf!\right)\left(\prod_{k \in c_{n+2}} kf!\right) \equiv x_{2h,2} \pmod{p} \tag{2.5}$$

for four solutions of (1.1) *which satisfy* $p^{2(s_n - s_m)} \parallel (x_{2h,2}^2 - qw_{2h,2}^2)$.

Proof. For brevity let $(x_{h,1}, u_{h,1}, v_{h,1}, w_{h,1}) = (x, u, v, w)$. Then by Theorem 4.1 of [1] we have

$$x_{2h,1} = \tfrac{1}{4}(x^2 - 2qu^2 - 2qv^2 - qw^2). \tag{2.6}$$

Clearly,

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

so that

$$x_{2h,1} \equiv \frac{x^2 + qw^2}{2} \pmod{p} \tag{2.7}$$

and (2.4) follows immediately from (2.3). Applying the transformation $u \to v$, $v \to -u$, $w \to -w$, and then using (2.6) we obtain

$$x_{2h,2} = \frac{x^2 - 2quv + 2quv - qw^2}{4} = \frac{x^2 - qw^2}{4}. \tag{2.8}$$

Now (2.5) follows at once as

$$\left(\frac{x}{2} + \frac{w}{2}\sqrt{q}\right)\left(\frac{x}{2} - \frac{w}{2}\sqrt{q}\right) = \frac{x^2 - qw^2}{4}.$$

After easy simplifications we have

$$w_{2h,1} = xw \quad \text{and} \quad w_{2h,2} = -\tfrac{1}{2}(bv^2 + 2auv - bu^2). \tag{2.9}$$

Appealing to (1.1) with $\alpha = h$ (see (5.42) of [7]) we note that

$$(x^2 - qw^2)^2 = 256p^{2h} - 64qp^h(u^2 + v^2) + 4q(bv^2 + 2auv - bu^2)^2$$

and it follows that (see (5.40) of [7])

$$p^{2(s_n - s_m)} \parallel (x_{2h,2}^2 - qw_{2h,2}^2). \tag{2.10}$$

Moreover, we have

$$\left(\frac{x^2+qw^2}{2}\right)^2 - q(xw)^2 = \frac{(x^2-qw^2)^2}{4}$$

from which it follows that

$$p \nmid (x_{2h,1}^2 - qw_{2h,1}^2)$$

as $p^{s_n - s_m} \parallel bv^2 + 2auv - bu^2$ and by assumption $s_n = s_m$. Note that in [7] the signs of a and b are fixed to allow for a positive or negative choice of sign for b in contrast to [1]. The different notations will in some cases imply a switching of roles of u and v in applying formulae from [7] but will not otherwise present a problem here.

Example 1. Let $q = 13$ so that $s_m = s_n = 1$. Then

$$\prod_{k \in c_2} kf! \equiv 4f!10f!12f! \equiv \binom{4f}{f} \pmod p$$

and

$$\prod_{k \in c_3} kf! \equiv 7f!8f!11f! \equiv \binom{7f}{2f} \pmod p.$$

Let $p = 53 = 4q + 1$. Then

$$\binom{16}{4}^2 + \binom{28}{8}^2 \equiv 18^2 + 26^2 \equiv 6 + 40 \equiv 46 \pmod{53},$$

$$\binom{16}{4}\binom{28}{8} \equiv 9 \pmod{53}.$$

It is easily checked from (2.6) and (2.8) that $x_{2h,1} = -113 \equiv 46 \pmod{53}$ and $x_{2h,2} = 9 \equiv 9 \pmod{53}$.

Example 2. Let $q = 149$ so that the class number of K is 9 and $s_m = s_n = 17$ (see [6], [7]). A solution of (1.1) with $\alpha = h = 3$ is (−2380, 2744, 8824, −3392). Direct computation yields for $p = 1193 = 1499 \cdot 8 + 1$,

$$\prod_{k \in c_2} kf! \equiv 509(1193), \qquad \prod_{k \in c_3} kf! \equiv 690 \pmod{1193}. \tag{2.11}$$

From (2.6) and (2.8) we have

$$x_{6,1} = -5931740060 \equiv 293 \pmod{1193}, \qquad x_{6,2} = -427169884 \equiv 486 \pmod{1193}$$

and it is easily checked that

$$(509)^2 + (690)^2 \equiv 293 \pmod{1193}, \qquad (509)(690) \equiv 486 \pmod{1193}.$$

Finally,

$$p^{2(13-12)} = 1193^2 = 1423249 \mid (427169884^2 - 149 \cdot 521158592^2).$$

3. Explicit Binomial Coefficient Theorems When $\alpha = 3$ and $s_m = s_n$.

THEOREM 3.1. *Let $s_m = s_n$ and let $\alpha = 3h$ in* (1.1). *Then four solutions of* (1.1) *satisfy*

$$\left(\prod_{k \in c_{m+2}} kf!\right)^3 + \left(\prod_{k \in c_{n+2}} kf!\right)^3 \equiv x_{3h,1} \pmod p, \tag{3.1}$$

four more satisfy

$$\left(\prod_{k \in c_{m+2}} kf!\right)\left(\prod_{k \in c_{n+2}} kf!\right)^2 \equiv x_{3h,2} \pmod p, \tag{3.2}$$

and the remaining four solutions all have

$$\left(\prod_{k\in c_{m+2}} kf!\right)^2\left(\prod_{k\in c_{n+2}} kf!\right) \equiv x_{3h,3} \pmod p. \tag{3.3}$$

Proof. We first establish (3.1). By the binomial theorem we have

$$\left(\frac{x}{2}+\frac{w}{2}\sqrt{q}\right)^3+\left(\frac{x}{2}-\frac{w}{2}\sqrt{q}\right)^3=\frac{x^3}{4}+\frac{3qxw^2}{4}. \tag{3.4}$$

Next for (x, u, v, w) a solution of (1.1) when $\alpha = h$ we have from [1] that

$$x_{3h,1}=\frac{1}{4}\left[\frac{x}{4}(x^2-2qu^2-2qv^2+qw^2)-\frac{2qu}{4}(2xu+2bvw+2auw)\right.$$
$$\left.-\frac{2qv}{4}(2xv+2buw-2avw)+qw(xw)\right]$$
$$=\frac{x^3}{16}-\frac{qxu^2}{8}-\frac{qxv^2}{16}+\frac{qxw^2}{16}-\frac{qxu^2}{4}-\frac{qbuvw}{4}-\frac{qau^2w}{4}$$
$$-\frac{qxv^2}{4}-\frac{qbuvw}{4}+\frac{qav^2w}{4}+\frac{qxw^2}{4}$$

as $w_{2,1}=\frac{1}{4}(2xw-2au^2+2av^2-4buv)=xw$ by (1.1).

However, we clearly have

$$-\frac{3qxu^2}{8}-\frac{3qxv^2}{8}=\frac{3x^2}{16}+\frac{3qxw^2}{16}-16p^h$$

and

$$\frac{qav^2w}{4}-\frac{qbuvw}{2}-\frac{qau^2w}{4}=\frac{qxw^2}{4}.$$

Thus, the above equation simplifies to

$$x_{3h,1}=\frac{x^3}{16}+\frac{5qxw^2}{16}+\frac{qxw^2}{4}+\frac{3x^3}{16}+\frac{3qxw^2}{16}-16p^h,$$

that is,

$$x_{3h,1}=\frac{x^3}{4}+\frac{3qxw^2}{4}-16p^h. \tag{3.5}$$

The result (3.1) is now immediate from (2.1), (2.2), (3.4) (as again we note that $\sqrt{q}$ differs by a sign in (2.1) and (2.2) when interpreted as a rational expression mod p).

Next applying the same formulae, but after first performing the transformation $u \to v$, $v \to -u$, $w \to -w$, we obtain

$$x_{3h,2}=\frac{x(x^2-qw^2)}{16}-\frac{qxu^2}{8}+\frac{qbuvw}{8}+\frac{qbu^2w}{8}+\frac{qau^2w}{8}-\frac{qauvw}{8}$$
$$-\frac{qxuv}{8}+\frac{qxuv}{8}-\frac{qbv^2w}{8}+\frac{qbuvw}{8}-\frac{qauvw}{8}-\frac{qav^2w}{8}-\frac{qxv^2}{8}$$
$$+\frac{qbu^2w}{8}-\frac{qauvw}{4}-\frac{qbv^2w}{8}.$$

But by (1.1) we have

$$-\frac{qxw^2}{8}=-\frac{qav^2w}{8}+\frac{2qbuvw}{8}+\frac{qau^2w}{8}. \tag{3.6}$$

Moreover, by (5.53) of [7] we have

$$(3.7)\qquad \frac{qbu^2w}{4} - \frac{qauvw}{2} - \frac{qbv^2w}{4} \equiv \pm\frac{x^2w\sqrt{q}}{8} \pm \frac{qw^3\sqrt{q}}{8} \pmod{p}$$

with the sign ambiguity resulting from the two possible sign choices for $\sqrt{q}$. Corresponding to the plus and minus choices of sign we have from (3.6) and (3.7) that

$$(3.8)\qquad x_{3h,2} \equiv \frac{x^3}{8} - \frac{qxw^2}{8} - \frac{x^2w\sqrt{q}}{8} - \frac{qw^3\sqrt{q}}{8} \pmod{p}$$

and

$$(3.9)\qquad x_{3h,3} \equiv \frac{x^3}{8} - \frac{qxw^2}{8} + \frac{x^2w\sqrt{q}}{8} - \frac{qw^3\sqrt{q}}{8} \pmod{p}.$$

(Verification of (3.9) using Theorem 4.1 is straightforward and left to the reader.)

The rest of the theorem now follows at once from (2.1), (2.2), upon noting that

$$\left(\frac{x}{2} \mp \frac{w}{2}\sqrt{q}\right)\left(\frac{x}{2} \mp \frac{w}{2}\sqrt{q}\right)\left(\frac{x}{2} \pm \frac{w}{2}\sqrt{q}\right) = \frac{x^3}{8} \mp \frac{x^2w\sqrt{q}}{8} - \frac{qxw^2}{8} \pm \frac{qw^2\sqrt{q}}{8}.$$

COROLLARY.

$$(3.10)\qquad x_{3h,2} - x_{3h,3} = \tfrac{1}{2}qw(bu^2 - 2auv - bv^2).$$

Proof. The expressions for $x_{3h,2}$ and $x_{3h,3}$ differ precisely by a change of sign in the expression on the left-hand side of (3.7).

Example 3. Let $q = 149$ so that $a = 7$, $b = 10$, $s_m = s_n = 17$, and a solution of (1.1) with $\alpha = h = 3$ is (−2380, 2744, 8824, −3392). Then

$$x_{9,1} \equiv \frac{(-2380)^3}{4} + \frac{3(149)(-2380)(3392)^2}{4} \equiv (509)^3 + (690)^3 \equiv 143 \text{ (and } 1193),$$

in agreement with Theorem 3.1 in view of (2.11). Moreover, appealing to (3.7), (3.8), (3.9), we have

$$x_{9,2} \equiv \frac{(-2380)^3}{8} - \frac{149(-2380)(3392)^2}{8} + \frac{149(10)(2744)^2(-3392)}{4} - \frac{(149)(7)(2744)(8824)(-3392)}{2} - \frac{149(10)(8824)^2(-3392)}{4}$$
$$= 27 + 184 - 228 - 671 + 151 = 805 \equiv (509)(509)(690) \pmod{1193}.$$

Finally, by (3.10) we have

$$x_{9,3} \equiv 805 - \tfrac{1}{2}(149)(-3392)(10)(2744)^2 - (2)(7)(2744)(8824) - 10(8824)^2$$
$$\equiv 805 + 981(358 - 185 - 415) \equiv 810 \equiv (690)(690)(509) \pmod{1193}.$$

4. The Number of Solutions of (1.1) When $\alpha = 2h$ and $s_m \neq s_n$. It is exceedingly difficult to obtain numerical data giving solutions of (1.1) with $\alpha = 2h$, $s_m \neq s_n$. The smallest value of q with $s_m \neq s_n$ is $q = 101$ and the smallest prime $p = 101f + 1$ is

607. A direct search for solutions of

$$(4.1)\qquad \begin{gathered} 16(607)^{\alpha} = x^2 + 202u^2 + 202v^2 + 101w^2, \\ xw = v^2 - 20uv - u^2, \qquad x \equiv 4 \pmod{101}, (x, u, v, w, p) = 1, \end{gathered}$$

is already very time consuming for $\alpha = h = 3$ and appears to be hopeless for $\alpha > 3$. Making use of theorems in [1] and [7], Buell and Hudson showed that

$$(8185, -966, 1971, 5013)$$

is a solution of (4.1) when $\alpha = 3$ (there are no solutions when $\alpha = 1$ or 2). Applying Theorem 4.1 of [1] one finds the solution

$$(4.2)\qquad (407976475, 43028481, -21086784, 41031405)$$

for $\alpha = 6$ and we note that

$$(4.3)\qquad \Big(\prod_{k\in c_n} kf!\Big)^2 \equiv (294)^2 \equiv 242 \equiv 407976475 \pmod{607}.$$

However, when one applies Theorem 4.1 of [1] after applying the transformation $u \to v$, $v \to -u$, $w \to -w$ (or any of the other possible transformations) one does *not* obtain a solution to (1.1). Indeed in general, it follows from (2.8), (2.9) and (5.39), (5.40) of [7] that $p^{s_n - s_m} \parallel x_{2h,2}$ and $p^{s_n - s_m} \parallel w_{2h,2}$. But

$$p^{2(s_n - s_m)} \parallel \left(x_{2h,2}^2 + qw_{2h,2}^2\right) \Rightarrow p^{(2s_n - s_m)} \parallel \left(u_{2h,2}^2 + v_{2h,2}^2\right)$$

and

$$p^{s_n - s_m} | \left(bx_{2h,2}w_{2h,2} + 2qu_{2h,2}v_{2h,2}\right)$$

by (5.40) of [7]. Together these clearly imply that

$$p^{s_n - s_m} | \left(x_{2h,2}, u_{2h,2}, v_{2h,2}, w_{2h,2}\right)$$

so that $(x_{2h,2}, u_{2h,2}, v_{2h,2}, w_{2h,2}, p) \neq 1$ if $s_n > s_m$ (that is the four-tuple obtained is not a solution of (1.1) when $\alpha = 6$ in view of the restriction in (1.1) that a solution be relatively prime to p). Nonetheless, it is clear that the difficulty arises precisely because the parameters in the four-tuple have precisely $s_n - s_m$ too many p's as factors. From

$$p^{2(s_n - s_m)} \parallel \left(x_{2h,2}^2 + 2qu_{2h,2}^2 + 2qv_{2h,2}^2 + qw_{2h,2}^2\right)$$

we see at once that

$$\frac{1}{p^{s_n - s_m}}\left(x_{2h,2}, u_{2h,2}, v_{2h,2}, w_{2h,2}\right)$$

is a solution of (1.1) for $\alpha = 2h - 2(s_n - s_m)$. By (2.4) of [7] we have $2(s_n - s_m) < h$. Thus we have established that for $s_n \neq s_m$, the system (1.1) is not only solvable for $\alpha = h$ [7, Section 4], but also for a value of α that is not a multiple of h, namely $\alpha = 2h - 2(s_n - s_m)$.

Example 4. For $q = 101$, $p = 607$, we have $s_m = 11$, $s_n = 12$ and in contrast to the case $s_m = s_n$ there appears to be only one solution to (1.1) when $\alpha = 6$, namely the solution given by (4.2). However, the four-tuple

$$\begin{aligned} &\left(x_{2h,2}, u_{2h,2}, v_{2h,2}, w_{2h,2}\right) \\ &\quad = (-617788211, 6857886, -44077305, -12854439) \end{aligned}$$

satisfies all the conditions of (1.1) except that each parameter is divisible by $p^{s_n - s_m} = p = 607$. Consequently, the four-tuple

$$(1017773, -11298, 72615, 21177)$$

is a solution of (1.1) when $\alpha = 2h - 2(s_n - s_m) = 6 - 2 = 4$.

5. A New Determination of Certain Products of Factorials mod $p = qf + 1$. Extending work of Cauchy and Jacobi (who treated the quadratic case), Hudson and Williams determined in [7] the four products of factorials modulo $p = qf + 1$, $q \equiv 5 \pmod 8 > 5$ (a fixed $\equiv 1 \pmod 4$ and $b \equiv -(q-1)/2!a \pmod q$), given by $\prod_k kf!$ where k runs through the four cosets which may be formed with respect to the subgroup of quartic residues modulo q. In particular, they showed that for $s_m \neq s_n$ (Case B in [7]) there are four solutions of (1.1) when $\alpha = h$ such that (with signs of a, b fixed as above, and $x \equiv -4 \pmod q$) one has

$$\prod_{k \in c_m} kf! \equiv \frac{(-1)^{s_m+1}}{x} \pmod p, \tag{5.1}$$

$$\prod_{k \in c_n} kf! \equiv \frac{4(-1)^{s_n+1}}{\left(2x + \dfrac{(-1)^{(b-2(m-n))/4} abw(x^2 - qw^2)}{b^2xw + 2|b|quv}\right)/p^{s_n - s_m}} \pmod p, \tag{5.2}$$

$$\prod_{k \in c_{m+2}} kf! \equiv (-1)^{s_m} x \pmod p, \tag{5.3}$$

$$\prod_{k \in c_{n+2}} kf! \equiv \frac{(-1)^{s_n}}{4p^{s_n - s_m}} \left(2x + \frac{(-1)^{(b-2(m-n))/4} abw(x^2 - qw^2)}{b^2xw + 2|b|quv}\right) \pmod p. \tag{5.4}$$

Obviously, the congruences (5.2) and (5.4) are rather unwieldy. As an easy consequence of the arguments in Section 2 and Section 4 of this paper we have

$$\left(\prod_{k \in c_n} kf!\right)\left(\prod_{k \in c_{n+2}} kf!\right) p^{s_n - s_m} \equiv x_{2h,2} \pmod p$$

for four solutions of (1.1) with $\alpha = 2h$ and this yields alternative determinations which are much neater as exhibited in the following theorem.

THEOREM 5.1. *There are four solutions of* (1.1) *when* $\alpha = h$, *any one of which we denote by* (x, u, v, w), *and four solutions with* $\alpha = 2h - 2(s_n - s_m)$ *which we denote by* (x', u', v', w') *such that for any of these* 8 *solutions we have*

$$\prod_{k \in c_m} kf! \equiv \frac{(-1)^{s_m}}{x} \pmod p, \tag{5.5}$$

$$\prod_{k \in c_n} kf! \equiv \frac{(-1)^{s_m} x}{x'} \pmod p, \tag{5.6}$$

$$\prod_{k \in c_{m+2}} kf! \equiv (-1)^{s_m+1} x \pmod p, \tag{5.7}$$

$$\prod_{k \in c_{n+2}} kf! \equiv \frac{(-1)^{s_m+1} x'}{x} \pmod p. \tag{5.8}$$

Example 5. Let $q = 101, p = 607$ so that

$$(x, u, v, w) = (8185, -966, 1971, 5013) \equiv (294, 248, 150, 157) \pmod p$$

and

$$(x', u', v', w') = (-1017773, 11298, 72615, 21177) \equiv (166, 372, 382, 539) \pmod{607}.$$

From Example 7.1 of [7] we have

$$(-1)^{s_m+1} \prod_{k \in c_{m+2}} kf! \equiv 294 \pmod{607}$$

and

$$(-1)^{s_m+1} \prod_{k \in c_{n+2}} kf! \equiv 302 \pmod{607}.$$

These congruences are clearly in agreement with (5.6) and (5.8) as $(-1)^{11+1}166/294 \equiv 302 \pmod{607}$ and (5.6) follows as a consequence of (5.59) of [7].

Example 6. Let $q = 157, p = 1571$. Among the 12 solutions of (1.1) with $\alpha = h = 3$ we have

$$(23868, 3254, 8570, 14948) \equiv (303, 112, 715, 809) \pmod{1571}.$$

Now $((23868)^2 - 157(14948)^2)/4p^{s_n - s_m} \equiv 360 \pmod{1571}$ as $s_0 = 19, s_1 = 18, s_2 = 20, s_3 = 21$ (see [7, Example 2]). Moreover,

$$\prod_{k \in c_{m+2}} kf! \equiv -303 \pmod{1571} \quad \text{and} \quad \prod_{k \in c_{n+2}} kf! \equiv 1090 \pmod{1571}.$$

By Theorem 5.1 we should have

$$\prod_{k \in c_{n+2}} kf! \equiv \frac{(-1)^{19}360}{-303} \equiv 1090 \pmod{1571},$$

and this is easily verified.

Department of Mathematics and Statistics
University of South Carolina
Columbia, South Carolina 29208

1. DUNCAN A. BUELL & RICHARD H. HUDSON, "Solutions of certain quaternary quadratic systems," *Pacific J. Math.*, v. 114, 1984, pp. 23–45.

2. L. E. DICKSON, "Cyclotomy and trinomial congruences," *Trans. Amer. Math. Soc.*, v. 37, 1935, pp. 363–380.

3. C. F. GAUSS, "Theoria residuorum biquadraticorum, Comment. I," Comment. soc. reg. sci. Gottingensis rec., v. 6, 1828, p. 27. (Werke vol. 2, p.90.)

4. REINALDO E. GIUDICI, JOSEPH B. MUSKAT & STANLEY F. ROBINSON, "On the evaluation of Brewer's character sums," *Trans. Amer. Math. Soc.*, v. 171, 1972, pp. 317–347.

5. HELMUT HASSE, "Der 2^n-te Potenzcharakter von 2 im Körper der 2^n-ten Einheitswurzeln," *Rend. Circ. Mat. Palermo* (2), v. 7, 1958, pp. 185–244.

6. RICHARD H. HUDSON & KENNETH S. WILLIAMS, *A Class Number Formula for Certain Quartic Fields*, Carleton Mathematical Series No. 174, Carleton University, Ottawa, 1981.

7. RICHARD H. HUDSON, KENNETH S. WILLIAMS & DUNCAN A. BUELL, "Extension of a theorem of Cauchy and Jacobi," *J. Number Theory* (To appear.)

8. RICHARD H. HUDSON & KENNETH S. WILLIAMS, "Binomial coefficients and Jacobi sums," *Trans. Amer. Math. Soc.*, v. 281, 1984, pp. 431–505.

9. EMMA LEHMER, "The quintic character of 2 and 3," *Duke Math. J.*, v. 18, 1951, pp. 11–18.

10. EMMA LEHMER, "On Euler's criterion," *J. Austral. Math. Soc.*, v. 1, 1959, pp. 64–70.

11. C. R. Matthews, "Gauss sums and elliptic functions II. The quartic sums," *Invent. Math.*, v. 54, 1979, pp. 23–52.

12. Joseph B. Muskat & Yun-Cheng Zee, "On the uniqueness of solutions of certain Diophantine equations," *Proc. Amer. Math. Soc.*, v. 49, 1975, pp. 13–19.

13. Bennett Setzer, "The determination of all imaginary, quartic, Abelian number fields with class number 1," *Math. Comp.*, v. 35, 1980, pp. 1383–1386.

14. Lothar Stickelberger, "Ueber eine Verallgemeinerung der Kreisteilung," *Math. Ann.*, v. 37, 1890, pp. 321–367.

15. Albert Leon Whiteman, "Theorems analogous to Jacobsthal's theorem," *Duke Math. J.*, v. 16, 1949, pp. 619–626.

16. Koichi Yamamoto, "On a conjecture of Hasse concerning multiplicative relation of Gaussian sums," *J. Combin. Theory*, v. 1, 1966, pp. 476–489.