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

$$16p^x = x^2 + 2qu^2 + 2qv^2 + qw^2, \quad (x, u, v, w, p) = 1,$$

$$xw = av^2 - 2buv - au^2, \quad x \equiv 4 \pmod{q}, a \geq 1.$$

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

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

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 $\mathbb{Q}(e^{\pi i/p})$.

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

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

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 $\prod_{k \in c_j} kf!$ and $\prod_{k \in c_{n+2}} kf!$, in terms of the parameters $x$ in the above partition of $16p^x$, 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 $p^x$ or $16p^x$, $x \geq 1$, such as

$$(1.1) \quad 16p^x = x^2 + 2qu^2 + 2qv^2 + qw^2, \quad (x, u, v, w, p) = 1,$$

$$xw = av^2 - 2buv - au^2, \quad x \equiv 4 \pmod{q},$$

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 $x$ is a deep and complex problem as it depends on the class number of the imaginary cyclic quartic field

$$(1.2) \quad K = \mathbb{Q}(i\sqrt{2q + 2a\sqrt{q}}),$$
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 $\pm 1$ (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,

$$16p^a = x^2 + 50u^2 + 50v^2 + 125w^2, \quad (x, u, v, w, p) = 1,$$

$$xw = v^2 - 2uw - u^2, \quad x \equiv 1 \pmod{5}.$$

Determination of binomial coefficients of the type $\binom{n}{s}$ modulo $p = qf + 1$, $1 \leq r < s \leq q - 1$, in terms of parameters in quadratic forms has been a topic of interest since the late 1820's when Gauss [3] determined $\binom{n}{s}$ 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

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

and

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

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

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

and

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

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 $\prod k!$ 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

$$\binom{4f}{f}^3 + \binom{7f}{2f}^3 \equiv x_{3,1} \pmod{p = 13f + 1},$$
PRODUCTS AND SUMS OF POWERS OF BINOMIAL COEFFICIENTS mod p

(1.9) \[ \binom{4f}{f} \left( \frac{7f}{2f} \right)^2 \equiv x_{3,2} \pmod{p = 13f + 1}, \]

(1.10) \[ \binom{4f}{f} \left( \frac{7f}{2f} \right)^2 \equiv x_{3,3} \pmod{p = 13f + 1}, \]

where the $x_{k,i}$, $1 \leq i \leq k$, 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) \[ s_j = \frac{1}{q} \sum_{t \in c_j} t, \quad j = 0, 1, 2, 3. \]

Define $h$ to be the odd positive integer given by

(1.12) \[ h = \max(|s_0 - s_2|, |s_1 - s_3|). \]

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 $\alpha$ satisfy $x_{3,i}^2 - qw_{3,i}^2 \neq 0 \pmod{p}$ 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 $\alpha_0$ denotes the exponent such that (1.1) is solvable for $\alpha_0$ but not for $\alpha < \alpha_0$, we would expect to find $4\alpha_0$ solutions to (1.1) for each $\alpha > \alpha_0$ and no solutions for $\alpha$ a multiple of $\alpha_0$. 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 $\alpha$ a not a multiple of $\alpha_0$.

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 \( \prod_{k \in c_{m+2}} kf! \) and \( \prod_{k \in c_{n+2}} kf! \mod p \) 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 $Q(\varepsilon_{2m+1})$. It follows from (5.33) and (5.59) of [7] that

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

and

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

\[
\left( \prod_{k \in c_{m+2}} k f_k ! \right)^2 + \left( \prod_{k \in c_{n+2}} k f_k ! \right)^2 = \frac{x^2}{2} + \frac{qw^2}{2} \quad (\text{mod } p).
\]

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 \( p \mid (x_{h,1} - qw_{h,1}) \), \( p \mid (bx_{h,1}w_{h,1} + qw_{h,1}v_{h,1}) \) provided \( s_m = s_n \). Let \( \alpha = 2h \). Then

\[
\left( \prod_{k \in c_{m+2}} k f_k ! \right)^2 + \left( \prod_{k \in c_{n+2}} k f_k ! \right)^2 = x_{2h,1} (\text{mod } p)
\]

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

\[
\left( \prod_{k \in c_{m+2}} k f_k ! \right) \left( \prod_{k \in c_{n+2}} k f_k ! \right) = x_{2h,2} (\text{mod } p)
\]

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

**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

\[
x_{2h,1} = \frac{1}{4} \left( x^2 - 2qu^2 - 2qv^2 - qw^2 \right).
\]

Clearly,

\[
x^2 + qw^2 = -2qu^2 - 2qv^2 \quad (\text{mod } p)
\]

so that

\[
x_{2h,1} = \frac{x^2 + qw^2}{2} \quad (\text{mod } p)
\]

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

\[
x_{2h,2} = \frac{x^2 - 2qw + 2qw - qw^2}{4} = \frac{x^2 - qw^2}{4}.
\]

Now (2.5) follows at once as

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

After easy simplifications we have

\[
w_{2h,1} = xw \quad \text{and} \quad w_{2h,2} = \frac{1}{4} (b(v^2 + 2aw - bu^2)).
\]

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

\[
(x^2 - qw^2)^2 = 256p^{2h} - 64qbp^h(u^2 + v^2) + 4q(bv^2 + 2aw - bu^2)^2
\]

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

\[
p^{2(s_m - s_n)} \parallel (x_{2h,2}^2 - qw_{2h,2}^2).
\]
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
\[
p \div \left( x_{2h,1}^2 - qw_{2h,1}^2 \right)
\]
as \( p^{s_m - s_n} \mid bv^2 + 2auw - bu^2 \) 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
\[
\prod_{k \in c_2} kf! = 4f!10f!12f! \equiv \binom{4f}{f} \pmod{p}
\]
and
\[
\prod_{k \in c_3} kf! = 7f!18f!11f! \equiv \binom{7f}{2f} \pmod{p}.
\]
Let \( p = 53 = 4q + 1 \). Then
\[
\left( \frac{16}{4} \right)^2 + \left( \frac{28}{8} \right)^2 = 18^2 + 26^2 = 6 + 40 = 46 \pmod{53},
\]
\[
\left( \frac{16}{4} \right) \left( \frac{28}{8} \right) = 9 \pmod{53}.
\]
It is easily checked from (2.6) and (2.8) that \( x_{2h,1} = -113 = 46 \pmod{53} \) and \( x_{2h,2} = 9 = 9 \pmod{53} \).

**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 \( p = 1193 = 1499 - 8 + 1 \),
\[
(2.11) \quad \prod_{k \in c_2} kf! \equiv 509(1193), \quad \prod_{k \in c_3} kf! \equiv 690 \pmod{1193}.
\]
From (2.6) and (2.8) we have
\[
\begin{align*}
x_{6,1} = -5931740060 & \equiv 293 \pmod{1193}, \quad x_{6,2} = -427169884 \equiv 486 \pmod{1193} \quad \text{and it is easily checked that} \\
(509)^2 + (690)^2 & \equiv 293 \pmod{1193}, \quad (509)(690) \equiv 486 \pmod{1193}.
\end{align*}
\]
Finally,
\[
p^{2(13-12)} = 1193^2 = 1423249(427169884^2 - 149 \cdot 521158592^2).
\]

### 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
\[
\left( \prod_{k \in c_{m+2}} kf! \right)^3 + \left( \prod_{k \in c_{n+2}} kf! \right)^3 \equiv x_{3h,1} \pmod{p},
\]
and four more satisfy
\[
\left( \prod_{k \in c_{m+2}} kf! \right) \left( \prod_{k \in c_{n+2}} kf! \right)^2 \equiv x_{3h,2} \pmod{p},
\]
and the remaining four solutions all have

\[ (3.3) \quad \left( \prod_{k \in \mathbb{E}_{m+2}} kf! \right)^2 \left( \prod_{k \in \mathbb{E}_{n+2}} kf! \right) \equiv x_{3h,3} \pmod{p}. \]

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

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

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

\[ x_{3h,1} = \frac{1}{4} \left[ \frac{x}{4} (x^2 - 2qu^2 - 2qv^2 + qw^2) - \frac{2qu}{4} (2xu + 2bw + 2auw) \right. \]
\[ - \frac{2qv}{4} (2xv + 2buw - 2avw) + qw(xw) \]
\[ = \frac{x^3}{16} - \frac{qxu^2}{8} - \frac{qxv^2}{16} + \frac{qxw^2}{4} - \frac{qbuw}{4} - \frac{qau^2w}{4} - \frac{qav^2w}{4} \]
\[ - \frac{qav^2w}{4} + \frac{qav^2w}{4} + \frac{qav^2w}{4} \]
\[ = \frac{w^2x}{16} - \frac{2(2xw - 2au^2 + 2av^2 - 4bw)}{16} = xw \text{ by (1.1)}. \]

However, we clearly have

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

and

\[ \frac{qav^2w}{4} - \frac{qbuw}{2} - \frac{qau^2w}{4} = \frac{qxw^2}{4}. \]

Thus, the above equation simplifies to

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

that is,

\[ (3.5) \quad x_{3h,1} = \frac{x^3}{4} + \frac{3qxw^2}{4} - 16p^h. \]

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 \(\pmod{p}\)).

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

\[ x_{3h,2} = \frac{x(x^2 - qw^2)}{16} - \frac{qxu^2}{8} + \frac{qbuw}{8} + \frac{qbu^2w}{8} + \frac{qau^2w}{8} - \frac{qauw}{8} \]
\[ - \frac{qxu^2}{8} + \frac{qxw^2}{8} - \frac{qbu^2w}{8} + \frac{qauw}{8} - \frac{qbuw}{8} + \frac{qau^2w}{8} - \frac{qauw}{8} - \frac{qxu^2}{8} \]
\[ + \frac{qbu^2w}{8} - \frac{qauw}{4} - \frac{qbuw}{8}. \]

But by (1.1) we have

\[ (3.6) \quad - \frac{qxw^2}{8} = - \frac{qau^2w}{8} + \frac{2qbuw}{8} + \frac{qau^2w}{8} . \]
Moreover, by (5.53) of [7] we have

\[
\frac{qbu^2}{4} \pm \frac{qaww}{2} - \frac{qbw^2}{4} = \pm \frac{x^2w\sqrt{q}}{8} \pm \frac{qw^3\sqrt{q}}{8} \quad (\text{mod } p)
\]

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

\[
x_{3h,2} = \frac{x^3}{8} - \frac{qbw^2}{8} - \frac{x^2w\sqrt{q}}{8} - \frac{qw^3\sqrt{q}}{8} \quad (\text{mod } p)
\]

and

\[
x_{3h,3} = \frac{x^3}{8} - \frac{qbw^2}{8} + \frac{x^2w\sqrt{q}}{8} - \frac{qw^3\sqrt{q}}{8} \quad (\text{mod } p).
\]

(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

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

**COROLLARY.**

\[
x_{3h,2} - x_{3h,3} = \frac{1}{2}qbw^2 - 2aww - bw^2.
\]

**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

\[
x_{9,1} = \frac{(-2380)^3}{4} + \frac{3(149)(-2380)(3392)^2}{4}
\]

\[
= (509)^3 + (690)^3 = 143 \quad (\text{and } 1193),
\]

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

\[
x_{9,2} = \frac{(-2380)^3}{8} - \frac{149(-2380)(3392)^2}{8} + \frac{149(10)(2744)^2(-3392)}{4}
\]

\[
- \frac{(149)(7)(2744)(8824)(-3392)}{2} - \frac{149(10)(8824)^2(-3392)}{4}
\]

\[
= 27 + 184 - 228 - 671 + 151 = 805 \equiv (509)(509)(690) \quad (\text{mod } 1193).
\]

Finally, by (3.10) we have

\[
x_{9,3} = 805 - \frac{1}{2}(149)(-3392)(10)(2744)^2 - (2)(7)(2744)(8824) - 10(8824)^2
\]

\[
= 805 + 981(358 - 185 - 415) = 810 \equiv (690)(690)(509) \quad (\text{mod } 1193).
\]

**4. The Number of Solutions of (1.1) When \(\alpha = 2h, s_m \neq s_n.\)** 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
A direct search for solutions of

\[
16(607)\alpha = x^2 + 202u^2 + 202v^2 + 101w^2, \quad xw = v^2 - 20uv - u^2, \quad x \equiv 4 \pmod{101}, (x, u, v, w, \alpha) = 1,
\]
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

\[
(407976475, 43028481, -21086784, 41031405)
\]
for \(\alpha = 6\) and we note that

\[
\left(\prod_{k \in c_n} k!\right)^2 \equiv (294)^2 \equiv 242 \equiv 407976475 \pmod{607}.
\]

However, when one applies Theorem 4.1 of [1] after applying the transformation

\[
u \rightarrow v, \quad v \rightarrow -u, \quad w \rightarrow -w \quad (or \ any \ of \ the \ other \ possible \ transformations) \quad \text{one \ does \ not}
\]

obtain a solution to (1.1). Indeed in general, it follows from (2.8), (2.9) and (5.39), (5.40) of [7] that \(p^{n-s_m} \mid x_{2h,2}\) and \(p^{n-s_m} \mid w_{2h,2}\). But

\[
p^{2(s_n-s_m)} \mid \left(x_{2h,2}^2 + qw_{2h,2}^2\right) \Rightarrow p^{12(s_n-s_m)} \mid \left(u_{2h,2}^2 + v_{2h,2}^2\right)
\]

and

\[
p^{s_n-s_m}(bx_{2h,2}w_{2h,2} + 2qu_{2h,2}v_{2h,2})
\]

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

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

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

\[
p^{2(s_n-s_m)} \mid \left(x_{2h,2}^2 + qw_{2h,2}^2\right) + 2qu_{2h,2}v_{2h,2} + qw_{2h,2}^2
\]

we see at once that

\[
\frac{1}{p^{s_n-s_m}}(x_{2h,2}, u_{2h,2}, v_{2h,2}, w_{2h,2})
\]
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 \(\alpha\) 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

\[
(x_{2h,2}, u_{2h,2}, v_{2h,2}, w_{2h,2})
\]

\[
= (-617788211, 6857886, -44077305, -12854439)
\]
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 \( p = qf + 1 \), \( q = 5 \)
(mod 8) > 5 (a fixed \( \equiv 1 \) (mod 4) and \( b \equiv -(q - 1)/2a \) (mod q)), given by \( \prod_k k! \)
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 \( a = h \) such that (with signs of
\( a, b \) fixed as above, and \( x \equiv -4 \) (mod q)) one has

\[
\prod_{k \in c_m} k! \equiv \frac{(1)^{s_n+1}}{4(-1)^{s_n+1}} \quad \text{(mod p)},
\]

\[
\prod_{k \in c_{m+2}} k! \equiv (-1)^{s_m}x \quad \text{(mod p)},
\]

\[
\prod_{k \in c_{m+2}} k! \equiv \frac{(-1)^{s_n}}{4p^{s_n-s_m}} \left( 2x + \frac{(1)(b-2(m-n))/4 abw(x^2 - qw^2)}{b^2xw + 2|b|qw} \right) \quad \text{(mod p)}.
\]

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

\[
\left( \prod_{k \in c_m} k! \right) \left( \prod_{k \in c_{m+2}} k! \right) p^{s_n-s_m} \equiv x_{2h,2} \quad \text{(mod p)}
\]

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

\[
\prod_{k \in c_m} k! \equiv \frac{(1)^{s_n}}{4(-1)^{s_n+1}} \quad \text{(mod p)},
\]

\[
\prod_{k \in c_m} k! \equiv \frac{(1)^{s_n}x}{x'} \quad \text{(mod p)},
\]

\[
\prod_{k \in c_{m+2}} k! \equiv (-1)^{s_m+1}x \quad \text{(mod p)},
\]

\[
\prod_{k \in c_{m+2}} k! \equiv \frac{(1)^{s_m+1}}{x'} \quad \text{(mod p)}.
\]
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
\[
(-1)^{s_0+1} \prod_{k \in c_{m+2}} k(f^! \equiv 294 \pmod{607})
\]
and
\[
(-1)^{s_0+1} \prod_{k \in c_{n+2}} k(f^! \equiv 302 \pmod{607}).
\]
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,
\[
\prod_{k \in c_{m+2}} k(f^! \equiv -303 \pmod{1571}) \quad \text{and} \quad \prod_{k \in c_{n+2}} k(f^! \equiv 1090 \pmod{1571}).
\]
By Theorem 5.1 we should have
\[
\prod_{k \in c_{n+2}} k(f^! \equiv (-1)^{s_0}360 \equiv 1090 \pmod{1571}),
\]
and this is easily verified.

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