TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 281, Number 2, February 1984

BINOMIAL COEFFICIENTS AND JACOBI SUMS

BY

RICHARD H. HUDSON AND KENNETH S. WILLIAMS[1]

ABSTRACT. Throughout this paper e denotes an integer $\geqslant 3$ and p a prime $\equiv 1 \pmod{e}$. With f defined by $p = ef + 1$ and for integers r and s satisfying $1 \leqslant s < r \leqslant e - 1$, certain binomial coefficients $\binom{rf}{sf}$ have been determined in terms of the parameters in various binary and quaternary quadratic forms by, for example, Gauss [**13**], Jacobi [**19, 20**], Stern [**37–40**], Lehmer [**23**] and Whiteman [**42, 45, 46**].

In §2 we determine for each e the exact number of binomial coefficients $\binom{rf}{sf}$ not trivially congruent to one another by elementary properties of number theory and call these representative binomial coefficients. A representative binomial coefficient is said to be of order e if and only if $(r, s) = 1$.

In §§3–4, we show how the Davenport-Hasse relation [**7**], in a form given by Yamamoto [**50**], leads to determinations of $n^{(p-1)/m}$ in terms of binomial coefficients modulo $p = ef + 1 = mnf + 1$. These results are of some interest in themselves and are used extensively in later sections of the paper.

Making use of Theorem 5.1 relating Jacobi sums and binomial coefficients, which was first obtained in a slightly different form by Whiteman [**45**], we systematically investigate in §§6–21 all representative binomial coefficients of orders $e = 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16, 20$ and 24, which we are able to determine explicitly in terms of the parameters in well-known binary quadratic forms, and all representative binomial coefficients of orders $e = 5, 10, 13, 15, 16$ and 20, which we are able to explicitly determine in terms of quaternary quadratic decompositions of $16p$ given by Dickson [**9**], Zee [**51**] and Guidici, Muskat and Robinson [**14**]. Some of these results have been obtained by previous authors and many new ones are included.

For $e = 7$ and 14 we are unable to explicitly determine representative binomial coefficients in terms of the six variable quadratic decomposition of $72p$ given by Dickson [**9**] for reasons given in §10, but we are able to express these binomial coefficients in terms of the parameter x_1 in this system in analogy to a recent result of Rajwade [**34**].

Finally, although a relatively rare occurrence for small e, it is possible for representative binomial coefficients of order e to be congruent to one another (mod p). Representative binomial coefficients which are congruent to ± 1 times at least one other representative for all $p = ef + 1$ are called Cauchy-Whiteman type binomial coefficients for reasons given in [**17**] and §21. All congruences between such binomial coefficients are carefully examined and proved (with the sign ambiguity removed in each case) for all values of e considered. When $e = 24$ there are 48 representative binomial coefficients, including those of lower order, and it is shown in §21 that an astonishing 43 of these are Cauchy-Whiteman type binomial coefficients. It is of particular interest that the sign ambiguity in many of these congruences does not arise from any expression of the form $n^{(p-1)/m}$ in contrast to the case for all $e < 24$.

Received by the editors February 8, 1983.

1980 *Mathematics Subject Classification.* Primary 10-02, 10C05, 10B35; Secondary 12C25.

Key words and phrases. Binomial coefficients (mod p) in terms of binary and quaternary quadratic forms, Jacobi sums.

[1]Research suported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233.

0002-9947/84 $1.00 + $.25 per page

1. Introduction and summary. Throughout this paper e denotes an integer $\geqslant 3$ and p a prime $\equiv 1 \pmod{e}$. The integer f is defined by $p = ef + 1$. For integers r and s satifying $1 \leqslant s < r \leqslant e - 1$, certain binomial coefficients

$$\binom{rf}{sf} \tag{1.1}$$

have been determined modulo p by, for example, Gauss [**13**], Jacobi [**20**], Stern [**37–40**], Lehmer [**23**], and Whiteman [**42, 45, 46**] in terms of representations of p by certain quadratic forms. The first result of this kind is due to Gauss [**13**, Vol. 2, p. 90] who showed that for $e = 4$, $p = 4f + 1 = a^2 + b^2$, $a \equiv 1 \pmod 4$,

$$\binom{2f}{f} \equiv 2a \pmod{p}. \tag{1.2}$$

Emma Lehmer [**23**] used Jacobsthal sums to obtain congruences for $\binom{2f}{f}$ and $\binom{3f}{f}$ when $p = 5f + 1$ in terms of the system $16p = x^2 + 50u^2 + 50v^2 + 125w^2$, $xw = v^2 - 4uv - u^2$, $x \equiv 1 \pmod 5$, introduced by Dickson [**8**].

In this paper we systematically use Jacobi sums to obtain congruences modulo primes $p = ef + 1$ for binomial coefficients of the type (1.1). These include old as well as new ones. The cases treated in §§6–19 are $e = 3, 4, 5, \ldots, 16$. In §§20–21 we handle in some detail the cases $e = 20$ and $e = 24$, relying heavily on recent evaluations by, e.g., Berndt and Evans [**4**] of bidecic and biduodecic Jacobi sums.

Our results are obtained in terms of the parameters in the following Diophantine systems:

(1) $p = a^2 + b^2, \quad a \equiv 1 \pmod 4, \quad 4 \mid e,$

(2) $p = x^2 + 3y^2, \quad x \equiv 1 \pmod 3, \quad 3 \mid e,$

(3) $4p = A^2 + 27B^2, \quad A \equiv 1 \pmod 3, \quad 3 \mid e,$

(4) $16p = x^2 + 50u^2 + 50v^2 + 125w^2, \quad xw = v^2 - 4uv - u^2,$
$x \equiv 1 \pmod 5, \quad 5 \mid e,$

(5) $p = x^2 + 7y^2, \quad x \equiv 1 \pmod 7, \quad e = 7, 14,$

(6) $72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \quad x_1 \equiv 1 \pmod 7,$
$e = 7, 14,$

(7) $p = c^2 + 2d^2, \quad c \equiv 1 \pmod 4, \quad e = 8, 16, 24,$

(8) $16p = x^2 + 26u^2 + 26v^2 + 13w^2, \quad xw = 3v^2 - 4uv - 3u^2,$
$x \equiv 9 \pmod{13}, \quad e = 13,$

(9) $p = g^2 + 15h^2, \quad g \equiv 1 \pmod 3, \quad e = 15,$

(10) $p = x^2 + 2u^2 + 2v^2 + 2w^2, \quad 2xv = u^2 - 2uw - w^2, \quad x \equiv 1 \pmod 8,$
$u \equiv v \equiv w \equiv 0 \pmod 2, \quad e = 16,$

(11) $p = e^2 + 5f^2, \quad e \equiv a \pmod 5$ if $5 \mid b$ and $e \equiv \mid b \mid \pmod 5$ if $5 \mid a,$
$e = 20,$

(12) $p = u^2 + 6v^2$, $u \equiv -1 \pmod 4$ if $3 \mid b$ and $u \equiv 1 \pmod 4$ if $3 \mid a$,

$e = 24$.

Although the sign of b is not fixed in (1) it is clear that for $p = 4f + 1$ there exists at least one primitive root $g(p)$ such that $g^{ef/4} \equiv a/|b| \pmod p$. For $e = 20$ and 24 some of our determinations require fixing g in this manner (see, in connection, [**19**]).

The following congruences are typical of those proved in §§6–21.

$$\binom{2f}{f} \equiv -A \pmod{p = 3f + 1} \qquad \text{(Jacobi [20])},$$

$$\binom{2f}{f} \equiv 2a \pmod{p = 4f + 1} \qquad \text{(Gauss [13])},$$

$$\binom{2f}{f} \equiv \frac{1}{2}\left(-x + \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right) \pmod{p = 5f + 1} \qquad \text{(Lehmer [23])},$$

$$\binom{3f}{f} \equiv 2x \pmod{p = 6f + 1},$$

$$\binom{3f}{f} \equiv -2x \pmod{p = 7f + 1} \qquad \text{(Jacobi [19])},$$

$$\binom{2f}{f} + \binom{4f}{f} + \binom{4f}{2f} \equiv -x_1 \pmod{p = 7f + 1},$$

$$\binom{2f}{f} \equiv (-1)^{b/4} 2c \pmod{p = 8f + 1},$$

$$\binom{5f}{f} \equiv \frac{1}{2}\left(-x - \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right) \pmod{p = 10f + 1},$$

$$\binom{5f}{f} \equiv -A \pmod{p = 12f + 1}, \qquad \binom{6f}{f} \equiv 2a \pmod{12f + 1},$$

$$a \equiv 1 \pmod 4 \Leftrightarrow 3 \mid b,$$

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

$$\binom{7f}{2f} \equiv \begin{cases} 2g \pmod{p = 15f + 1}, & AB \equiv 0 \pmod 5, \\ \dfrac{2Af + 18Bg}{A - 9B} \pmod{p = 15f + 1}, & A \equiv B \text{ or } -2B \pmod 5, \\ \dfrac{2Ag - 18Bg}{A + 9B} \pmod{p = 15f + 1}, & A \equiv -B \text{ or } 2B \pmod 5, \end{cases}$$

$$\binom{5f}{2f} \equiv (-1)^f 2c \text{ or } (-1)^{f+1} 2c \pmod{p = 16f + 1}$$

according as $b \equiv 0$ or $8 \pmod{16}$,

$$\binom{8f}{f} \equiv 2(-1)^f \left(x - \frac{v(x^2 - 2v^2)}{u^2 - w^2 + 2uw}\right) \pmod{p = 16f + 1},$$

$$\binom{8f}{f} + \binom{8f}{3f} \equiv 4(-1)^f x \pmod{p = 16f + 1},$$

$$\binom{10f}{f} \equiv 2e \text{ or } 2ea/|b| \pmod{p = 20f + 1}, \quad 5 \mid b \text{ or } 5 \mid a \qquad \text{(Whiteman [45])},$$

$$\binom{7f}{3f} \equiv \frac{1}{2}\left(-x + \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right) \pmod{p = 20f + 1}$$

for the solution $(x, -v, u, -w)$ of (4),

$$\binom{5f}{f} \equiv (-1)^{f+y/4+1} A \pmod{p = 24f + 1},$$

$$\binom{12f}{f} \equiv (-1)^f 2u \pmod{p = 24f + 1}.$$

In so far as possible we determine all binomial coefficients for the cases considered if they can be given in terms of the systems (1)–(12). Binomial coefficients which are not treated are related to the parameters in more complicated quadratic partitions. In some cases, see §§18–21, we are able to determine these binomial coefficients up to sign in terms of the parameters in (1)–(12).

For each e_i there are $\frac{1}{2}(e - 1)(e - 2)$ binomial coefficients of the type (1.1) which are of order e. In §1 it is shown by an application of a simple generalization of Wilson's theorem that it suffices to determine $N(e)$ of these binomial coefficients (for large e, $N(e) \cong e^2/12$) where $N(e)$ is given explicitly by

$$N(e) = \begin{cases} (e^2 - \alpha)/12 & \text{if } e \equiv \alpha \pmod 6, \quad \alpha = -3, 0, 1, 4, \\ (e^2 + \alpha)/12 & \text{if } e \equiv \alpha \pmod 6, \quad \alpha = -4, -1. \end{cases} \tag{1.3}$$

These $N(e)$ binomial coefficients will be called representatives.

When e is composite, say $e = mn$, it is useful to have a congruence of the type

$$n^{(p-1)/m} \equiv \frac{a_1 f! a_2 f! \cdots a_l f!}{b_1 f! b_2 f! \cdots b_l f!} \pmod p \tag{1.4}$$

where the a_i, b_j are integers between 1 and $e - 1$ inclusive. Such a congruence follows from the Davenport-Hasse relation for Gauss sums [7] and a congruence of Yamamoto [50]; see (3.11). For values of m and n for which m or n is small we show in §4 that the expression on the right-hand side of (3.11) can be given in terms of binomial coefficients (mod p). Together with known results for $n^{(p-1)/m} \pmod p$ in terms of representations of p by quadratic forms we deduce congruences (mod p) relating certain binomial coefficients which are used in later sections. For example, if $p = 2mf + 1$, it is shown in Theorem 4.1 that we have

$$2^{(p-1)/m} \equiv (-1)^f \binom{(m+2)f}{f} \Big/ \binom{(m+2)f}{2f} \pmod p. \tag{1.5}$$

Putting (1.5) together with a result of Emma Lehmer [23], see (4.5), we obtain Corollary 4.1.1 which is used in §§9, 15, and 21. The results in §4 appear to us of

some interest, totally apart from their use in later sections. For example, an easy application of (2.1), (2.2) and (3.11) gives

$$3^{(p-1)/16} \equiv (-1)^f \binom{18f}{f} \Big/ \binom{18f}{3f} \pmod{p = 48f + 1}.$$

We note that criteria for 3 to be a 16th power in terms of the parameters in Diophantine systems is an open problem.

In 1840, Cauchy [**5**, p. 37] show that

$$\binom{10f}{f} \equiv \pm \binom{10f}{3f} \pmod{p = 20f + 1}, \tag{1.6}$$

and in 1965 Whiteman resolved the sign ambiguity in this congruence. Representative binomial coefficients which are congruent to ± 1 times another representative modulo p for all $p = ef + 1$ are said to be of Cauchy-Whiteman type for reasons given in [**17**] and §21. We systematically investigate all such congruences. The 27 congruences of this type given in Theorems 21.1 and 21.2 far exceed the number of such congruences for all $e < 24$. Moreover, the congruences in Theorem 21.2 do not arise (as do all other known Cauchy-Whiteman type congruences) as expressions of the form $(n^{(p-1)/m})^t$, $p = mnf + 1$.

For $p = 11f + 1$, $4p = a^2 + 11b^2$, $a \equiv 2 \pmod{11}$, Jacobi [**19**] showed that

$$\binom{3f}{f}\binom{6f}{3f} \Big/ \binom{4f}{2f} \equiv a \pmod{p}.$$

For larger values of e with many representative binomial coefficients it is not appropriate to list all such congruences, and we cite only one.

For $p = 20f + 1 = e^2 + 5f^2$ ($e \equiv a \pmod 5$ if $5 \mid b$ and $e \equiv |b| \pmod 5$ if $5 \mid a$) we have

$$\binom{4f}{f}\binom{8f}{f} \Big/ \binom{11f}{3f} \equiv (-1)^{[2e/5]} 2e \pmod{p}.$$

The sign may be given unambiguously in this congruence (and in many other congruences in §20) only because of an important sign ambiguity resolution obtained by Muskat and Whiteman [**31**] in determining the cyclotomic numbers of order 20.

In all that follows we are heavily indebted to Berndt, Evans, Muskat, and Whiteman for their pioneering work on Jacobi sums of higher orders.

2. The number of distinct binomial coefficients of the type (1.1). If m and n are positive integers such that $m + n = e$, then a simple modification of Wilson's theorem yields

$$mf!nf! \equiv (-1)^{mf-1} \equiv (-1)^{nf-1} \pmod{p}. \tag{2.1}$$

Making use of (2.1) and the elementary property $\binom{a}{b} = \binom{a}{a-b}$ of binomial coefficients, we deduce that for $1 \leqslant s < r \leqslant e-1$ we have

$$\begin{aligned}(2.2)\quad \binom{rf}{sf} &\equiv \binom{rf}{(r-s)f} \equiv (-1)^{(r+s)f}\binom{(e-s)f}{(e-r)f}(-1)^{(r+s)f}\binom{(e-s)f}{(r-s)f} \\ &\equiv (-1)^{sf}\binom{(e-r+s)f}{(e-r)f} \equiv (-1)^{sf}\binom{(e-r+s)f}{sf} \pmod{p}.\end{aligned}$$

If $r \neq 2s$, $2r - s \neq e$, $r + s \neq e$ then the entry pairs in the six coefficients in (2.2) are distinct and we call (2.2) a 6-cycle. If exactly one of $r = 2s$, $2r - s = e$, $r + s = e$ holds, then there are three distinct entry pairs in the coefficients in (2.2) and we call (2.2) a 3-cycle. Finally, if at least two of $r = 2s$, $2r - s = e$, $r + s = e$ hold, then in fact all three hold so that $e = 3s$ and the coefficients in (2.2) reduce to the 1-cycle $\binom{2sf}{sf}$.

The number N_1 of 1-cycles is clearly 1 if $e \equiv 0 \pmod 3$ and 0 if $e \not\equiv 0 \pmod 3$. The number N_3 of 3-cycles is the number of pairs (r, s) satisfying exactly one of $r = 2s$, $2r - s = e$, $r + s = e$. Thus N_3 is the number of integers t satisfying $1 < t < e/2$, $t \neq e/3$, so that

$$(2.3)\qquad N_3 = \begin{cases} e/2 - 2 & \text{if } e \equiv 0 \pmod 6, \\ (e-1)/2 & \text{if } e \equiv 1 \pmod 6, \\ e/2 - 1 & \text{if } e \equiv 2 \pmod 6, \\ (e-3)/2 & \text{if } e \equiv 3 \pmod 6, \\ e/2 - 1 & \text{if } e \equiv 4 \pmod 6, \\ (e-1)/2 & \text{if } e \equiv 5 \pmod 6. \end{cases}$$

The number N_6 of 6-cycles is now easily deduced from the values for N_1 and N_3 and the identity

$$(2.4)\qquad N_1 + 3N_3 + 6N_6 = \tfrac{1}{2}(e-1)(e-2).$$

Since the coefficients in (2.2) are congruent (mod p) it suffices, for each e, to determine $N(e) = N_1 + N_3 + N_6$ of them. For the convenience of the reader Table 1 is given summarizing the above and indicating the representative to be chosen from each cycle.

A representative binomial coefficient of the type (1.1) with $(r, s) > 1$ is the same as the lower order binomial coefficient $\binom{r_1 f_1}{s_1 f_1}$, where

$$r_1 = r/(r, s, e), \quad s_1 = s/(r, s, e), \quad e_1 = e/(r, s, e) < e,$$

$f_1 = (r, s, e)f$, $p = e_1 f_1 + 1$. Henceforth, a *representative binomial coefficient will be said to be of order e* only if it is not the same as one of lower order. It is easy to see that if $R(e)$ denotes the number of representatives with lower order ones excluded, we have

$$\begin{aligned}(2.5)\quad &R(3) = R(4) = 1, \quad R(5) = R(6) = 2, \quad R(7) = R(8) = 4, \\ &R(9) = R(10) = 6, \quad R(11) = 10, \quad R(12) = 8, \quad R(13) = 14, \\ &R(14) = 12, \quad R(15) = R(16) = 16, \quad R(20) = 24, \quad R(24) = 33.\end{aligned}$$

TABLE 1

$e \pmod 6$	N_1	N_3	N_6	$N_1 + N_3 + N_6$	*REPRESENTATIVES*
0	1	$e/2 - 2$	$\frac{1}{12}(e^2 - 6e + 12)$	$\frac{1}{12}e^2$	$\binom{2if}{if}, \binom{(2i+1)f}{if}, \ldots, \binom{(e/2 + [i/2])f}{if}$, $i = 1, 2, \ldots, (e-2)/3$
1	0	$(e-1)/2$	$\frac{1}{12}(e-1)(e-5)$	$\frac{1}{12}(e^2 - 1)$	$\binom{2if}{if}, \binom{(2i+1)f}{if}, \ldots, \binom{(\frac{1}{2}(e-1) + i - [i/2])f}{if}$, $i = 1, 2, \ldots, (e-1)/3$
2	0	$e/2 - 1$	$\frac{1}{12}(e-2)(e-4)$	$\frac{1}{12}(e^2 - 4)$	$\binom{2if}{if}, \binom{(2i+1)f}{if}, \ldots, \binom{(e/2 + [i/2])f}{if}$, $i = 1, 2, \ldots, e/3$
3	1	$(e-3)/2$	$\frac{1}{12}(e-3)^2$	$\frac{1}{12}(e^2 + 3)$	$\binom{2if}{if}\binom{(2i+1)f}{if}, \ldots, \binom{(\frac{1}{2}(e-1) + i - [i/2])f}{if}$, $i = 1, 2, \ldots, e/3$
4	0	$e/2 - 1$	$\frac{1}{12}(e-2)(e-4)$	$\frac{1}{12}(e^2 - 4)$	$\binom{2if}{if}, \binom{(2i+1)f}{if}, \ldots, \binom{(e/2 + [i/2])f}{if}$, $i = 1, 2, \ldots, (e-1)/3$
5	0	$(e-1)/2$	$\frac{1}{2}(e-1)(e-5)$	$\frac{1}{12}(e^2 - 1)$	$\binom{2if}{if}, \binom{(2i+1)f}{if}, \ldots, \binom{(\frac{1}{2}(e-1) + i - [i/2])f}{if}$, $i = 1, 2, \ldots, (e-2)/3$

TABLE 2

f	p	a	x	A	θ	$\binom{2f}{f}$	$\binom{3f}{f}$	$\binom{4f}{f}$	$\binom{5f}{f}$	$\binom{6f}{f}$	$\binom{5f}{2f}$	$\binom{7f}{2f}$	$\binom{7f}{3f}$	$\binom{6f}{2f}$	$\binom{6f}{3f}$	$\binom{8f}{4f}$	ϕ	ϕ^2
1	13	−3	1	−5	8	2	3	4	5	6	10	8	9	2	7	5	3	9
3	37	1	−5	−11	−1	20	10	35	11	2	10	22	2	27	2	11	26	10
5	61	5	7	1	1	8	14	10	60	10	14	18	51	14	10	60	47	13
6	73	−3	−5	7	27	48	22	57	66	6	51	19	57	63	67	66	64	8
8	97	9	7	19	22	66	17	8	78	79	80	49	8	14	18	78	35	61

We close this section with a lemma which will be useful when $R(e) > 1$ in that it makes it possible to further reduce the number of binomial coefficients which must be treated separately.

LEMMA 2.1. *If g, h, k are integers satisfying $1 \leqslant h < g \leqslant e-1$, $1 \leqslant h < k \leqslant e-1$, $e-k < g-h$, then*

$$\binom{gf}{hf}\binom{(e-g)f}{(k-h)f} \equiv (-1)^{(g+k)f}\binom{kf}{hf}\binom{(e-k)f}{(g-h)f} \pmod{p}. \tag{2.6}$$

3. Basic properties of Gauss and Jacobi sums. For a positive integer n we set $\zeta_n = \exp(2\pi i/n)$. For $(a, e) = 1$, we define the automorphism σ_a by

$$\sigma_a\colon \zeta_e \to \zeta_e^a, \qquad \sigma_a\colon P \to P_a, \tag{3.1}$$

where P denotes any of the $\phi(e)$ prime ideals dividing p in $Q(\zeta_e)$. Let g be a primitive root (mod p) such that $g^{(p-1)/e} \equiv \zeta_e \pmod{P}$. We define a character χ_e (mod p) of order e by

$$\chi_e(x) = \begin{cases} \zeta_e^a & \text{if } x \not\equiv 0 \pmod{p},\ x^{(p-1)/e} \equiv \zeta_e^a \pmod{P}, \\ 0 & \text{if } x \equiv 0 \pmod{p}, \end{cases} \tag{3.2}$$

so that $\chi_e(g) = \zeta_e$. If $x \not\equiv 0 \pmod{p}$, the index of x with respect to g, written $\operatorname{ind}_g(x)$, is the unique integer b such that $x \equiv g^b \pmod{p}$, $0 \leqslant b \leqslant p-2$. Clearly $\chi_e(x) = \zeta_e^{\operatorname{ind}_g(x)}$. Let r and s denote positive integers. The Gauss sum $G_e(r)$ of order e is defined by

$$G_e(r) = \sum_{x=0}^{p-1} \chi_e^r(x)\zeta_p^x = \sum_{x=1}^{p-1} \zeta_e^{r\operatorname{ind}_g(x)}\zeta_p^x.$$

The Jacobi sum $J_e(r, s)$ of order e is defined by

$$J_e(r, s) = \sum_{x=0}^{p-1} \chi_e^r(x)\chi_e^s(1-x) = \sum_{x=2}^{p-1} \zeta_e^{r\operatorname{ind}_g(x)+s\operatorname{ind}_g(1-x)}.$$

Gauss and Jacobi sums are related by

$$J_e(r, s) = G_e(r)G_e(s)/G_e(r+s), \tag{3.3}$$

provided e does not divide r, s, or $r+s$. Moreover (see, for example, Muskat [**30**]), we have

$$J_e(r, s) = J_e(s, r) = (-1)^{sf}J_e(-r-s, s), \tag{3.4}$$

$$J_e(r, s)J_e(-r, -s) = p \qquad (r, s, r+s \not\equiv 0 \pmod{e}), \tag{3.5}$$

$$G_e(r)G_e(-r) = (-1)^{rf}p \qquad (r \not\equiv 0 \pmod{e}), \tag{3.6}$$

$$J_m(r, s) = J_e(rn, sn) \quad \text{if } e = mn, \tag{3.7}$$

and if e is prime and $e \nmid r$, s, or $r+s$, then

$$J_e(r, s) \equiv -1 \quad \left(\operatorname{mod}(1-\zeta_e)^2\right). \tag{3.8}$$

An important relation involving Gauss sums is provided by the Davenport-Hasse relation [7], namely,

$$\zeta_n^{t\operatorname{ind}_g(n)} = \frac{G_e(tn)\prod_{j=1}^{n-1}G_e(mj)}{\prod_{j=0}^{n-1}G_e(m_j+t)}, \qquad t = 1,2,\ldots,m-1. \tag{3.9}$$

Further, it follows from the work of Yamamoto [**50**] that if $\prod_{j=1}^{e-1}\{G_e(j)\}^{c_j}$ (c_j an integer) is a unit of $Q(\zeta_{ep})$, then

$$\sum_{j=1}^{e-1} c_j = 0$$

and

$$\prod_{j=1}^{e-1}\{G_e(j)\}^{c_j} \equiv \prod_{j=1}^{e-1}\{jf!\}^{c_j} \pmod{P}. \tag{3.10}$$

Applying this to (3.9) we obtain

$$n^{(p-1)t/m} \equiv \frac{ntf!\prod_{j=1}^{n-1}(mjf)!}{\prod_{j=0}^{n-1}((mj+t)f)!} \pmod{p}. \tag{3.11}$$

Finally, it follows from Stickelberger [**41**] that if $e \nmid r$, s or $r+s$, and $\langle J_e(r,s)\rangle$ denotes the ideal generated by $J_e(r,s)$, then

$$\langle J_e(r,s)\rangle = \prod_{\substack{t=1\\(t,e)=1\\\{rt^{-1}/e\}+\{st^{-1}/e\}<1}}^{e-1} P_t \tag{3.12}$$

where t^{-1} denotes the inverse of t modulo e, and $\{\ \}$ denotes, as is customary, the fractional part of the quantity inside the braces.

4. $n^{(p-1)/m}$ as a product of binomial coefficients (mod p). In this section for values of m and n for which either m or n is small and $t = 1$ we show that the expression on the right-hand side of (3.11) can be expressed as a quotient of products of binomial coefficients (mod p). Making use of known results in the literature for $n^{(p-1)/m}$ (mod p) in terms of representations of p by quadratic forms, we deduce congruences (mod p) relating certain binomial coefficients of the type (1.1). These congruences will be used in later sections.

Throughout this section we have $p = mnf + 1$. Taking $n = 2$ in (3.11) and appealing to (2.2), we obtain for each $t = 1,2,\ldots,m-1$ and $p = 2mf+1$,

$$2^{(p-1)t/m} \equiv (-1)^{mf}\binom{2tf}{tf}\Big/\binom{mf}{tf} \pmod{p}.$$

Binomial coefficients (mod $p = ef + 1$), when e is composite, are often related to one another by powers of $n^{(p-1)t/m}$ where n is a divisor of e (not necessarily prime). For $e \leqslant 12$ we are able to determine these interrelationships by simply taking $t = 1$ in (3.11) so we may appeal directly to results in this section. Beginning with $e = 14$ in §17 the number of powers of $n^{(p-1)t/m}$ which need be considered becomes

sufficiently large that it is convenient to use the full strength of the congruence (3.11). We postpone this generalization for now and it will be understood throughout this section that $t = 1$ in applying (3.11).

Taking $n = 2$ in (3.11), and appealing to (2.2), we obtain

THEOREM 4.1. *If* $p = 2mf + 1$ *is prime then*

$$2^{(p-1)/m} \equiv (1)^f \binom{(m-1)f}{f} \Big/ \binom{mf}{2f} \pmod{p}. \tag{4.1}$$

When $m = 2$ we have, as is well known,

$$2^{(p-1)/2} \equiv (-1)^f \pmod{p = 4f + 1}. \tag{4.2}$$

When $m = 3$, Theorem 4.1 gives

$$(-1)^f \binom{2f}{f} \equiv 2^{(p-1)/3} \binom{3f}{f} \pmod{p = 6f + 1}. \tag{4.3}$$

As p is a prime $\equiv 1 \pmod 3$, there are integers x, y such that

$$p = x^2 + 3y^2, \qquad x \equiv 1 \pmod 3. \tag{4.4}$$

The determination of $2^{(p-1)/3} \pmod p$ in terms of x and y is given by

$$2^{(p-1)/3} \equiv \begin{cases} 1 \pmod p & \text{if } y \equiv 0 \pmod 3 \qquad \text{(Jacobi [19]),} \\ \dfrac{x+3y}{x-3y} \pmod p & \text{if } y \equiv 1 \pmod 3 \\ \dfrac{x-3y}{x+3y} \pmod p & \text{if } y \equiv 2 \pmod 3 \end{cases} \qquad \text{(Lehmer [23]).} \tag{4.5}$$

Primes $p \equiv 1 \pmod 3$ are also expressible in the form $4p = A^2 + 27B^2$, $A \equiv 1 \pmod 3$, where A and B are related to x and y in (4.4) by

$$\begin{cases} A = -2x, & B = \pm 2y & \text{if } y \equiv 0 \pmod 3, \\ A = x + 3y, & B = \pm\tfrac{1}{3}(x - y) & \text{if } y \equiv 1 \pmod 3, \\ A = x - 3y, & B = \pm\tfrac{1}{3}(x + y) & \text{if } y \equiv 2 \pmod 3. \end{cases} \tag{4.6}$$

Thus (4.5) may be reformulated in terms of A and B as follows:

$$2^{(p-1)/3} \equiv \begin{cases} 1 \pmod p & \text{if } A \equiv B \equiv 0 \pmod 2, \\ \dfrac{A+9B}{A-9B} \pmod p & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv B \pmod 4, \\ \dfrac{A-9B}{A+9B} \pmod p & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv -B \pmod 4. \end{cases} \tag{4.7}$$

Combining (4.3) and (4.5) we obtain

COROLLARY 4.1.1. *If* $p = 6f + 1 = x^2 + 3y^2$, $x \equiv 1 \pmod 3$, *is prime, then*

$$\binom{3f}{f} \equiv \begin{cases} (-1)^f \binom{2f}{f} \pmod p & \text{if } y \equiv 0 \pmod 3, \\ (-1)^f \dfrac{x - 3y}{x + 3y} \binom{2f}{f} \pmod p & \text{if } y \equiv 1 \pmod 3, \\ (-1)^f \dfrac{x + 3y}{x - 3y} \binom{2f}{f} \pmod p & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

Combining (4.3) and (4.7) we obtain

COROLLARY 4.1.2. *If* $p = 6f + 1$, *with* $4p = A^2 + 27B^2$, $A \equiv 1 \pmod 3$, *is prime, then*

$$\binom{3f}{f} \equiv \begin{cases} (-1)^f \binom{2f}{f} \pmod p, & \text{if } A \equiv B \equiv 0 \pmod 2, \\ (-1)^f \dfrac{A - 9B}{A + 9B} \binom{2f}{f} \pmod p, & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv B \pmod 4, \\ (-1)^f \dfrac{A + 9B}{A - 9B} \binom{2f}{f} \pmod p, & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv -B \pmod 4. \end{cases}$$

When $m = 4$, Theorem 4.1 gives

$$\binom{3f}{f} \equiv (-1)^f 2^{(p-1)/4} \binom{4f}{2f} \pmod{p = 8f + 1}. \tag{4.8}$$

As $p \equiv 1 \pmod 8$ there are integers a and b such that

$$p = a^2 + b^2, \qquad a \equiv 1 \pmod 4, \quad b \equiv 0 \pmod 4, \tag{4.9}$$

and by a result of Gauss [**13**, Vol. 2, p. 89] we have

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

Hence from (4.9) and Lemma 2.1, we have

COROLLARY 4.1.3. *If* $p = 8f + 1 = a^2 + b^2$ ($a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$) *is prime, then*

$$\binom{3f}{f} \equiv (-1)^{f + b/4} \binom{4f}{2f} \pmod p.$$

When $m = 5$, Theorem 4.1 gives

$$\binom{4f}{f} \equiv (-1)^f 2^{(p-1)/5} \binom{5f}{2f} \pmod{p = 10f + 1}. \tag{4.10}$$

As $p \equiv 1 \pmod 5$ there are integers x, u, v, w such that

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2, & x \equiv 1 \pmod 5, \\ xw = v^2 - 4uv - u^2. \end{cases} \tag{4.11}$$

It is known (see, for example, [**49**, p. 544]) that (4.11) specifies x uniquely. If $x \equiv 0 \pmod 2$, Lehmer [**21**] has shown that $2^{(p-1)/5} \equiv 1 \pmod p$. Moreover, if $x \equiv 1 \pmod 2$, then there is a unique solution (x, u, v, w) of (4.11) satisfying

$$u \equiv 0 \pmod 2, \qquad x + u - v \equiv 0 \pmod 4, \tag{4.12}$$

and for this solution we have $2^{(p-1)/5} \equiv \alpha(x, u, v, w) \pmod p$ where

$$\alpha(x, u, v, w) = \frac{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)}. \tag{4.13}$$

Combining these we have

COROLLARY 4.1.4. *If $p = 10f + 1$ is prime, and (x, u, v, w) is a solution of* (4.11) *satisfying* (4.12) *we have*

$$\left(\frac{4f}{f}\right) \equiv \begin{cases} (-1)^f \left(\frac{5f}{2f}\right) \pmod p, & \text{if } x \equiv 0 \pmod 2, \\ (-1)^f \alpha(x, u, v, w) \left(\frac{5f}{2f}\right) \pmod p & \text{if } x \equiv 1 \pmod 2, \end{cases}$$

where $\alpha(x, u, v, w)$ is given by (4.13).

When $m = 6$, Theorem 4.1 gives

$$\left(\frac{5f}{f}\right) \equiv (-1)^f 2^{(p-1)/6} \left(\frac{6f}{2f}\right) \pmod{p = 12f + 1}. \tag{4.14}$$

Since $2^{(p-1)/2} \equiv (-1)^f \pmod p$, we have

$$\left(\frac{5f}{f}\right) \equiv (2^{(p-1)/3})^2 \left(\frac{6f}{2f}\right) \pmod p. \tag{4.15}$$

Appealing to (4.5), we obtain

COROLLARY 4.1.5. *If $p = 12f + 1 = x^2 + 3y^2$ $(x \equiv 1 \pmod 3)$ is prime, then*

$$\left(\frac{5f}{f}\right) \equiv \begin{cases} \left(\frac{6f}{2f}\right) \pmod p & \text{if } y \equiv 0 \pmod 3, \\ \frac{x - 3y}{x + 3y} \left(\frac{6f}{2f}\right) \pmod p & \text{if } y \equiv 1 \pmod 3, \\ \frac{x + 3y}{x - 3y} \left(\frac{6f}{2f}\right) \pmod p & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

When $m = 7$, Theorem 4.1 gives

$$\left(\frac{6f}{f}\right) \equiv (-1)^f 2^{(p-1)/7} \left(\frac{7f}{2f}\right) \pmod{p = 14f + 1}. \tag{4.16}$$

The determination of $2^{(p-1)/7} \pmod p$ has been given by Nashier and Rajwade [**33**]. Since this determination is extremely complicated, we just illustrate it below for the case when 2 is a seventh power $(\bmod p)$.

COROLLARY 4.1.6. *Let $p = 14f + 1$ be a prime. Then there are integers $x_1, \ldots, x_6$ such that*

$$
(4.17)\qquad \begin{cases} 72_p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5 + 3x_6)^2, \\ 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 \\ \qquad +24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 = 0, \\ 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 \\ \qquad +48x_2x_3 + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0, \end{cases}
$$

with $x_1 \equiv 1 \pmod 7$. All the solutions of (4.17), except the two trivial solutions $(x_1, x_2, x_3, x_4, x_5, x_6) = (-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$, where $p = t^2 + 7u^2$, $t \equiv 1 \pmod 7$, have the same value of x_1. If $x_1 \equiv 0 \pmod 2$, then 2 is a seventh power (mod p), and we have

$$
(4.18)\qquad \binom{6f}{f} \equiv (-1)^f \binom{7f}{2f} \pmod p.
$$

EXAMPLE. We illustrate Corollary 4.1.6 by taking $p = 673$ so that $f = 48$ and $x_1 = 22 \equiv 0 \pmod 2$ (see [**47**, p. 1136]). In agreement with (4.16), we have

$$
\binom{6f}{f} = \binom{288}{48} \equiv 346 \pmod{673},
$$

$$
(-1)^f \binom{7f}{2f} = \binom{336}{96} \equiv 346 \pmod{673}.
$$

When $m = 8$, Theorem 4.1 gives

$$
(4.19)\qquad \binom{7f}{f} (-1)^f 2^{(p-1)/8} \binom{8f}{2f} \pmod{p = 16f + 1}.
$$

From Lehmer [**23**, p. 66] we have

$$
(4.20)\qquad 2^{(p-1)/8} \equiv \begin{cases} +1 & \text{if } b \equiv 0 \pmod{16}, \\ +b/a & \text{if } b \equiv 4 \pmod{16}, \\ -1 & \text{if } b \equiv 8 \pmod{16}, \\ -b/a & \text{if } b \equiv 12 \pmod{16}, \end{cases}
$$

where a and b are defined as in (4.9). Combining (4.19) and (4.20) we obtain

COROLLARY 4.1.7. *Let $p = 16f + 1 = a^2 + b^2$ ($a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$) be prime. Then*

$$
\binom{7f}{f} \equiv (-1)^f \left(\frac{b}{a}\right)^{b/4} \binom{8f}{2f} \pmod p.
$$

Since expressions for $2^{(p-1)/m} \pmod p$ are also known for $m = 10, 12, 15, 16, 20, 24, 32$ and 40 (see [**23**, p. 70; **18**]), similar congruences to those given in Corollaries 4.1.1–4.1.7 can be deduced.

Next we take $n = 3$ in (3.11) to obtain

THEOREM 4.2. *If $p = 3mf + 1$ is prime then*

$$(-3)^{(p-1)/m} \equiv \binom{(m+2)f}{f} \Big/ \binom{(m+2)f}{3f} \pmod{p}.$$

When $m = 3$, Theorem 4.2 gives

$$\binom{5f}{f} \equiv 3^{(p-1)/3} \binom{5f}{2f} \pmod{p = 9f + 1}. \tag{4.21}$$

By a result of Lehmer [**23**, p. 67] (see also [**48**, p. 279]) we have

$$3^{(p-1)/3} \equiv \begin{cases} 1 \pmod{p} & \text{if } B \equiv 0 \pmod 3, \\ \dfrac{A - 9B}{A + 9B} \pmod{p} & \text{if } B \equiv 1 \pmod 3, \\ \dfrac{A + 9B}{A - 9B} \pmod{p} & \text{if } B \equiv 2 \pmod 3, \end{cases} \tag{4.22}$$

where

$$4p = A^2 + 27B^2, \qquad A \equiv 1 \pmod 3. \tag{4.23}$$

Combining (4.21) and (4.22) we obtain

COROLLARY 4.2.1. *If $p = 9f + 1$ is prime then*

$$\begin{aligned} \binom{5f}{2f} &\equiv \binom{5f}{f} \pmod{p} && \text{if } B \equiv 0 \pmod 3, \\ &\equiv \frac{A + 9B}{A - 9B} \binom{5f}{f} \pmod{p} && \text{if } B \equiv 1 \pmod 3, \\ &\equiv \frac{A - 9B}{A + 9B} \binom{5f}{f} \pmod{p} && \text{if } B \equiv 2 \pmod 3. \end{aligned}$$

When $m = 4$, Theorem 4.2 gives

$$\binom{6f}{f} \equiv (-3)^{(p-1)/4} \binom{6f}{3f} \pmod{p = 12f + 1}. \tag{4.24}$$

From the work of Gosset [**15**] we have

$$(-3)^{(p-1)/4} \equiv \begin{cases} 1 \pmod{p} & \text{if } b \equiv 0 \pmod 3, \\ -1 \pmod{p} & \text{if } a \equiv 0 \pmod 3, \end{cases} \tag{4.25}$$

where $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$ ($(-3)^{(p-1)/4} \equiv \pm 1 \pmod{p}$ as $p \equiv 1 \pmod{12}$). Combining (4.24) and (4.25) we have

COROLLARY 4.2.2. *If $p = 12f + 1 = a^2 + b^2$ ($a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$) is prime then*

$$\binom{6f}{f} \equiv \begin{cases} \binom{6f}{3f} \pmod{p} & \text{if } b \equiv 0 \pmod 3, \\ -\binom{6f}{3f} \pmod{p} & \text{if } a \equiv 0 \pmod 3. \end{cases}$$

When $m = 5$, Theorem 4.2 gives

$$\binom{7f}{f} \equiv 3^{(p-1)/5}\binom{7f}{3f} \pmod{p = 15f + 1}. \tag{4.26}$$

An explicit determination of $3^{(p-1)/5}$ has been given in [**49**, Theorem 2]. Using this together with Jacobi sums of order 15 given by Muskat [**30**] an explicit determination of $\binom{7f}{f}$ and $\binom{7f}{3f}$ is obtained in §18.

Taking $n = 4$ in (3.11), and appealing to (2.2), we obtain

THEOREM 4.3. *If $p = 4mf + 1$ is prime then*

$$4^{(p-1)/m} \equiv \binom{2f}{f}\binom{3f}{f}\binom{4f}{f} \Big/ \binom{mf}{f}\binom{(m+1)f}{f}\binom{2mf}{f} \pmod{p}.$$

Taking $m = 3$ in Theorem 4.3 we obtain

COROLLARY 4.3.1. *If $p = 12f + 1$ is prime then*

$$\binom{6f}{f} \equiv 2^{(p-1)/3}\binom{2f}{f} \pmod{p}.$$

We note that it is possible to obtain a simpler form for the determination of $4^{(p-1)/m} \pmod{p}$ by using (2.1) together with (3.11). In particular, we have

$$4^{(p-1)/m} \equiv \frac{4f!\prod_{j=1}^{3}(mjf)!}{\prod_{j=0}^{3}((mj+1)f)!} \equiv \frac{4f!\,(-1)^{mf-1}(2mf)!}{f!\,((m+1)f)!\,((2m+1)f)!\,((3m+1)f)!}$$

$$\equiv \frac{(-1)^f 4f!\,(2mf)!\,(m-1)f!}{f!\,((m+1)f)!\,((2m+1)f)!} \equiv (-1)^f \frac{\binom{(m+3)f}{f}\binom{(m+2)f}{f}}{\binom{(m+3)f}{4f}\binom{(2m+1)f}{f}}.$$

Thus we have obtained the following variation of Theorem 4.3.

THEOREM 4.4. *If $p = 4mf + 1$ is prime then*

$$4^{(p-1)/m} \equiv (-1)^f \binom{(m+3)f}{f}\binom{(m+2)f}{f} \Big/ \binom{(m+3)f}{4f}\binom{(2m+1)f}{f} \pmod{p}.$$

Although Theorems 4.1 and 4.4 clearly give the same result for $m = 3$, this is not the case in general.

The following congruence, which will be referred to again in §14, is particularly interesting, since it shows that representative binomial coefficients may be identical modulo $p = ef + 1$. Several of these identities are established in §21. It would be interesting to know for which values of e such congruences are possible.

COROLLARY 4.4.1. *If* $p = 12f + 1$ *is prime then*

$$\binom{5f}{f} \equiv \binom{8f}{4f} \pmod{p}.$$

PROOF. Using (3.4) together with Theorems 4.1 or 4.4 (appealing to (2.2) to see that $(-1)^f\binom{6f}{f} \equiv \binom{7f}{f} \pmod{p}$ in the latter case),

$$\binom{4f}{2f} \Big/ \binom{6f}{2f} \equiv \binom{6f}{2f} \Big/ \binom{5f}{f} \pmod{p}.$$

On the other hand,

$$\binom{4f}{2f}\binom{8f}{4f} \equiv \binom{6f}{2f}\binom{6f}{2f} \pmod{p}$$

is an immediate consequence of Lemma 2.1 with $g = 4$, $h = 2$, $k = 6$.

We remark that one can also obtain the last step in the proof by expanding in terms of factorials using (2.1). This corollary is important to us, as using it, other representative binomial coefficients of order 12 are determined in §14 using the simple determination of $\binom{2f}{f}$, $p = 3f + 1$, given by, e.g., Jacobi [**20**]. Taking $n = 5$ in (3.11), and appealing to (2.2), we obtain

THEOREM 4.5. *If* $p = 5mf + 1$ *is prime then*

$$5^{(p-1)/m} \equiv \binom{(m+2)f}{f}\binom{(3m-1)f}{(m+2)f} \Big/ \binom{(m+4)f}{5f}\binom{(3m+1)f}{(m+4)f} \pmod{p}.$$

Taking $m = 3$ in Theorem 4.4 we obtain

$$\binom{5f}{f} \equiv 5^{(p-1)/3}\binom{7f}{2f} \pmod{p = 15f + 1} \tag{4.27}$$

By a theorem of Williams [**48**, pp. 282–283] we have

$$5^{(p-1)/3} \equiv \begin{cases} 1 \pmod{p} & \text{if } AB \equiv 0 \pmod 5, \\ \dfrac{A + 9B}{A - 9B} \pmod{p} & \text{if } A \equiv B \text{ or } -2B \pmod 5, \\ \dfrac{A - 9B}{A + 9B} \pmod{p} & \text{if } A \equiv -B \text{ or } 2B \pmod 5, \end{cases} \tag{4.28}$$

where $4p = A^2 + 27B^2$, $A \equiv 1 \pmod 3$. Combining (4.27) and (4.28) we obtain

COROLLARY 4.5.1. *If* $p = 15f + 1$ *is prime then*

$$\binom{5f}{f} \equiv \begin{cases} \binom{7f}{2f} \pmod{p}, & \text{if } AB \equiv 0 \pmod 5, \\ \dfrac{A + 9B}{A - 9B}\binom{7f}{2f} \pmod{p}, & \text{if } A \equiv B \text{ or } -2B \pmod 5, \\ \dfrac{A - 9B}{A + 9B}\binom{7f}{2f} \pmod{p}, & \text{if } A \equiv -B \text{ or } 2B \pmod 5. \end{cases}$$

Finally, taking $m = 4$ in Theorem 4.4, we obtain

$$\binom{10f}{f} \equiv 5^{(p-1)/4}\binom{10f}{3f} \pmod{p = 20f + 1}.$$

Since

$$5^{(p-1)/4} \equiv \begin{cases} 1 \pmod p, & \text{if } b \equiv 0 \pmod 5, \\ -1 \pmod p, & \text{if } a \equiv 0 \pmod 5, \end{cases}$$

where $a \equiv 1 \pmod 4$, we have

COROLLARY 4.5.2. *If $p = 20f + 1$ is prime then*

$$\binom{10f}{f} \equiv \begin{cases} \binom{10f}{3f} \pmod p & \text{if } b \equiv 0 \pmod 5, \\ -\binom{10f}{3f} \pmod p & \text{if } a \equiv 0 \pmod 5. \end{cases}$$

Corollary 4.5.2 was first proved by Whiteman [**45**], although the congruence $\binom{10f}{f} \equiv \pm\binom{10f}{3f} \pmod p$ had been established by Cauchy [**5**, p. 37] one hundred and twenty-five years earlier.

5. The basic theorem. We prove the following theorem which shows how each binomial coefficient of type (1.1) can be determined modulo P by means of Jacobi sums. This theorem provides a basic tool which will be used through the rest of the paper.

THEOREM 5.1. *If $p = ef + 1$ is prime and r, s are integers such that $1 \leqslant s < r \leqslant e - 1$, then*

$$\binom{rf}{sf} \equiv (-1)^{sf+1} J_e(r, e - s) \pmod P. \tag{5.1}$$

PROOF. Since

$$\chi_e(x) \equiv x^f \pmod P$$

we have

$$\begin{aligned} J_e(r, e - s) &\equiv \sum_{x=1}^{p-1} x^{rf}(1 - x)^{(e-s)f} \pmod P \\ &\equiv \sum_{x=1}^{p-1} x^{rf} \sum_{t=0}^{(e-s)f} (-1)^t \binom{(e-s)f}{t} x^t \\ &\equiv \sum_{t=0}^{(e-s)f} (-1)^t \binom{(e-s)f}{t} \sum_{x=1}^{p-1} x^{rf+t}. \end{aligned}$$

However,

$$\sum_{x=1}^{p-1} x^k \equiv \begin{cases} 0 \pmod p & \text{if } k \not\equiv 0 \pmod{p-1}, \\ -1 \pmod p & \text{if } k \equiv 0 \pmod{p-1}, \end{cases} \tag{5.2}$$

so that we have, appealing to (2.2),

$$(5.3)\quad J_e(r, e-s) \equiv \sum_{t=0}^{(e-s)f} (-1)^{t+1} \binom{(e-s)f}{tf}$$

$$\equiv (-1)^{(e-r)f+1} \binom{(e-s)f}{(e-r)f} \equiv (-1)^{sf+1} \binom{rf}{sf} \pmod{P}.$$

We note that Whiteman [**45**] has already proved a result similar to, but not exactly the same as Theorem 5.1. Letting $\beta = e^{2\pi i/e}$ be replaced by g^f for a primitive root g of $p = ef + 1$ our $J_e(r, s)$ becomes Whiteman's $\psi_{r,s}$. In Lemma 6 of [**45**] Whiteman showed that

(i) $$\psi_{r,s} \equiv 0 \pmod{p} \qquad (r + s < e),$$

(ii) $$\psi_{r,s} \equiv -\binom{(2e-r-s)f}{(e-r)f} \pmod{p} \qquad (r + s > e).$$

In view of (2.2), condition (ii) can be rewritten in the simpler form

(ii)′ $$\psi(r, s) \equiv (-1)^{sf+1} \binom{rf}{(e-s)f} \pmod{p}.$$

In later sections we will refer again to Whiteman's very useful Lemma 6.

6. $e = 3$. There is a single representative binomial coefficient of order 3, namely $\binom{2f}{f}$. With A and B defined as in (4.23), we choose $P = (\pi)$, where

$$(6.1)\qquad \pi = \frac{1}{2}\left(A + 3B\sqrt{-3}\right),$$

so that $P \mid p$. It is well known that

$$(6.2)\qquad J_3(1, 1) = \pi,$$

(see, for example, [**4**, p. 357]), so by (6.1) and (6.2)

$$(6.3)\qquad J_3(2, 2) = \bar{\pi} = \frac{1}{2}\left(A - 3B\sqrt{-3}\right) \equiv A \pmod{\pi}.$$

Hence, by Theorem 5.1 (with $e = 3$, $r = 2$, $s = 1$) we have (as f is even),

$$(6.4)\qquad \binom{2f}{f} \equiv -J_3(2, 2) \equiv -A \pmod{\pi}.$$

As $\binom{2f}{f}$ and $-A$ are both rational integers, and $\pi \mid p$, we have

THEOREM 6.1. *If $p = 3f + 1$ is prime and A is given uniquely by $4p = A^2 + 27B^2$, $A \equiv 1 \pmod 3$, then*

$$\binom{2f}{f} \equiv -A \pmod{p}.$$

This result is due to Jacobi [**20**]; see also Whiteman [**42**] and von Schrutka [**35**]. Thus, appealing to (4.6), Theorem 6.1 can also be given in the form

THEOREM 6.2. *If $p = 3f + 1$ is prime and x is given uniquely by $p = x^2 + 3y^2$, $x \equiv 1 \pmod 3$, then*

$$\binom{2f}{f} \equiv \begin{cases} 2x \pmod p, & \text{if } y \equiv 0 \pmod 3, \\ -x - 3y \pmod p, & \text{if } y \equiv 1 \pmod 3, \\ -x + 3y \pmod p, & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

7. $e = 4$. There is a single representative binomial coefficient of order 4, namely $\binom{2f}{f}$.

With $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, we choose $P = (\pi)$, where $\pi = a + bi$, so that $P \mid p$. Then it is known that $J_4(1,2) = (-1)^{f+1}\pi$ (see, for example, [**4**, p. 361]), so

$$J_4(2,3) = \overline{J_4(1,2)} = (-1)^{f+1}\bar{\pi} = (-1)^{f+1}(a - bi) \equiv (-1)^{f+1}2a \pmod \pi.$$

Thus, by Theorem 5.1, we have

$$\binom{2f}{f} \equiv (-1)^{f+1}J_4(2,3) \equiv 2a \pmod \pi,$$

and hence

THEOREM 7.1. *If $p = 4f + 1$ is prime and a is given uniquely by $p = a^2 + b^2$, $a \equiv 1 \pmod 4$, then*

$$\binom{2f}{f} \equiv 2a \pmod p.$$

This is the result of Gauss mentioned in §1; see also Whiteman [**42**, p. 95].

8. $e = 5$. There are two representative binomial coefficients of order 5, namely $\binom{2f}{f}$ and $\binom{3f}{f}$. For convenience we set $\beta = \zeta_5$. It is known that the ring of integers R or $Q(\beta)$ is a unique factorization domain [**27**]. In R, p factors into primes as

$$p = \pi_1\pi_2\pi_3\pi_4, \tag{8.1}$$

where π is any prime factor of p in R and $\pi_i = \sigma_i(\pi)$ $(i = 1, 2, 3, 4)$. We can set

$$\pi = a_1\beta + a_2\beta^2 + a_3\beta^3 + a_4\beta^4, \tag{8.2}$$

where a_1, a_2, a_3, a_4 are rational integers (see, for example, [**49**]). Clearly $a_1 + a_2 + a_3 + a_4 \not\equiv 0 \pmod 5$, as $1 - \beta \mid 5$, $5 \nmid p$. Replacing π by its associate $\alpha\pi$, where α is the unit of R given by

$$\alpha = \begin{cases} +1 & \text{if } a_1 + a_2 + a_3 + a_4 \equiv 1 \pmod 5, \\ -(\beta + \beta^4) & \text{if } a_1 + a_2 + a_3 + a_4 \equiv 2 \pmod 5, \\ +(\beta + \beta^4) & \text{if } a_1 + a_2 + a_3 + a_4 \equiv 3 \pmod 5, \\ -1 & \text{if } a_1 + a_2 + a_3 + a_4 \equiv 4 \pmod 5, \end{cases} \tag{8.3}$$

we may suppose that $\pi \equiv 1 \pmod{(1 - \beta)}$.

Replacing the new value of π by its associate $\beta^{-(a_1 + 2a_2 + 3a_3 + 4a_4)}\pi$, we may suppose further that

$$\pi \equiv 1 \pmod{(1 - \beta)^2}. \tag{8.4}$$

By a theorem of Stickelberger, see (3.12), we have

$$J_5(1,1) \equiv 0 \pmod{\pi_1\pi_3}, \tag{8.5}$$

so

$$J_5(1,1) = u\pi_1\pi_3, \tag{8.6}$$

where $u \in R$. From (3.5), (8.1) and (8.6) we have

$$u\bar{u}\pi_1\pi_2\pi_3\pi_4 = (u\pi_1\pi_3)\overline{(u\pi_1\pi_3)} = J_5(1,1)\overline{J_5(1,1)} = p = \pi_1\pi_2\pi_3\pi_4,$$

so

$$u\bar{u} = 1, \tag{8.7}$$

showing that u is a unit of R, that is (see, for example, [**36**]),

$$u = \pm(\beta + \beta^4)^k\beta^l \qquad (k = 0, \pm1, \pm2, \ldots; l = 0,1,2,3,4). \tag{8.8}$$

Now (8.7) guarantees that $k = 0$ in (8.8) so

$$u = \pm\beta^l \qquad (l = 0,1,2,3,4). \tag{8.9}$$

By (3.8), (8.4), (8.6) and (8.9), we have

$$\begin{aligned} \pm\beta^l &= u \\ &\equiv u\pi_1\pi_3 \pmod{(1-\beta)^2} \\ &\equiv J_5(1,1) \pmod{(1-\beta)^2} \\ &\equiv -1 \pmod{(1-\beta)^2}, \end{aligned}$$

so in (8.9) the minus sign holds with $l = 0$, that is, $u = -1$, giving

$$J_5(1,1) = -\pi_1\pi_3. \tag{8.10}$$

We set

$$J_5(1,1) = c_1\beta + c_2\beta^2 + c_3\beta^3 + c_4\beta^4. \tag{8.11}$$

As $J_5(1,1) \equiv -1 \pmod{(1-\beta)^2}$, by (3.12), we have

$$\begin{cases} c_1 + c_2 + c_3 + c_4 \equiv -1 \pmod 5, \\ c_1 + 2c_2 + 3c_3 + 4c_4 \equiv 0 \pmod 5. \end{cases} \tag{8.12}$$

Next, since $\beta - \beta^2 - \beta^3 + \beta^4 = \sqrt{5}$, we have

$$\begin{aligned} (c_1 - c_2 - c_3 + c_4)\sqrt{5} &\equiv (c_1 - c_2 - c_3 + c_4)(\beta - \beta^2 - \beta^3 + \beta^4) \\ &\quad - (1 + c_1 + c_2 + c_3 + c_4) \pmod{(1-\beta)^4} \\ &\equiv 2\big((c_1 + c_4)(\beta + \beta^4) + (c_2 + c_3)(\beta^2 + \beta^3) + 2\big) \pmod{(1-\beta)^4} \\ &\equiv 2\big(J_5(1,1) + \overline{J_5(1,1)} + 2\big) \pmod{(1-\beta)^4} \\ &\equiv 2\big(J_5(1,1) + 1\big)\big(\overline{J_5(1,1)} + 1\big) \pmod{(1-\beta)^4} \\ &\equiv 0 \pmod{(1-\beta)^4}, \end{aligned}$$

so

$$c_1 - c_2 - c_3 + c_4 \equiv 0 \pmod 5. \tag{8.13}$$

Congruences (8.12) and (8.13) enable us to define integers x, u, v, w by

$$\begin{cases} x = -(c_1 + c_2 + c_3 + c_4), & 5u = c_1 + 2c_2 - 2c_3 - c_4, \\ 5v = 2c_1 - c_2 + c_3 - 2c_4, & 5w = c_1 - c_2 - c_3 + c_4. \end{cases} \tag{8.14}$$

Using (3.5), (8.11), (8.12) and (8.14), it is easy to check that (x, u, v, w) is a solution of

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2, & x \equiv 1 \pmod 5, \\ xw = v^2 - 4uv - u^2. \end{cases} \tag{8.15}$$

From (8.14), we obtain

$$\begin{cases} 4c_1 = -x + 2u + 4v + 5w, & 4c_2 = -x + 4u - 2v - 5w, \\ 4c_3 = -x - 4u + 2v - 5w, & 4c_4 = -x - 2u - 4v + 5w, \end{cases} \tag{8.16}$$

and so (8.11) and (8.16) give

$$J_5(1,1) = \frac{1}{4}\big(x + u(2\beta + 4\beta^2 - 4\beta^3 - 2\beta^4) + v(4\beta - 2\beta^2 + 2\beta^3 - 4\beta^4) + 5w\sqrt{5}\big). \tag{8.17}$$

Next, from (8.17), we deduce that

$$J_5(1,1) + J_5(4,4) = \frac{1}{2}\big(x + 5w\sqrt{5}\big). \tag{8.18}$$

Since

$$J_5(1,1) \equiv 0 \pmod \pi, \tag{8.19}$$

by (8.5), we deduce from (3.4), (8.18) and (8.19) that

$$J_5(2,4) = J_5(4,4) \equiv \frac{1}{2}\big(x + 5w\sqrt{15}\big) \pmod \pi. \tag{8.20}$$

Hence, by Theorem 5.1, we have

$$\binom{2f}{f} \equiv -J_5(2,4) \equiv -\frac{1}{2}\big(x + 5w\sqrt{5}\big) \pmod \pi. \tag{8.21}$$

It now remains to determine $\sqrt{5} \pmod \pi$ in terms of x, u, v, w.

Since

$$\begin{cases} \beta + 2\beta^2 - 2\beta^3 - \beta^4 = \frac{1}{2}i\sqrt{50 + 10\sqrt{5}}, \\ 2\beta - \beta^2 + \beta^3 - 2\beta^4 = \frac{1}{2}i\sqrt{50 - 10\sqrt{5}}, \end{cases} \tag{8.22}$$

we obtain from (8.17) and (8.19):

$$x + iu\sqrt{50 + 10\sqrt{5}} + iv\sqrt{50 - 10\sqrt{5}} + 5w\sqrt{5} \equiv 0 \pmod \pi. \tag{8.23}$$

Also from (8.5) we have

$$J_5(1,1) \equiv 0 \pmod{\pi_3}. \tag{8.24}$$

Applying the automorphism σ_2 to (8.24), we obtain

$$J_5(2,2) \equiv 0 \pmod{\pi_1}. \tag{8.25}$$

Hence from (8.17) and (8.22) we have

$$x - iu\sqrt{50 - 10\sqrt{5}} + iv\sqrt{50 + 10\sqrt{5}} - 5w\sqrt{5} \equiv 0 \pmod{\pi}. \tag{8.26}$$

Adding (8.23) and (8.26) we obtain

$$2x + i(u+v)\sqrt{50 + 10\sqrt{5}} - i(u-v)\sqrt{50 - 10\sqrt{5}} \equiv 0 \pmod{\pi}. \tag{8.27}$$

Taking the term $2x$ over to the right-hand side of (8.27) and squaring, we obtain after some simplification,

$$10(u^2 - uv - v^2)\sqrt{5} \equiv x^2 + 25u^2 + 25v^2 \pmod{\pi}. \tag{8.28}$$

From (8.15) and (8.28), we obtain

$$\sqrt{5} \equiv -(x^2 + 25u^2 + 25v^2)/10(xw + 5uv) \pmod{\pi}. \tag{8.29}$$

Using (8.29) in (8.21), we get, appealing to (8.15),

$$\binom{2f}{f} \equiv -\frac{x}{2} + \frac{w(x^2 - 125w^2)}{8(xw + 5uv)} \pmod{\pi}. \tag{8.30}$$

As both sides of the congruence (8.30) are integers (mod p), and since x, $x^2 - 125w^2$ and $x + 5uv/w$ are independent of the choice of solution (x, u, v, w) of (8.15), (8.30) holds mod p. Similarly, using $J_5(2,2)$ in place of $J_5(1,1)$, we obtain an analogous congruence to (8.30) for $\binom{3f}{f}$. These congruences are due to Emma Lehmer [**23**, p. 69]. Summarizing, we have

THEOREM 8.1. *If $p = 5f + 1$ is prime and (x, u, v, w) is any solution of* (8.15), *then*

$$\binom{2f}{f} \equiv \frac{1}{2}\left(-x + \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right) \pmod{p},$$

$$\binom{3f}{f} \equiv \frac{1}{2}\left(-x - \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right) \pmod{p}.$$

The next corollary follows immediately from Theorem 8.1. It was recently rediscovered by Rajwade [**34**].

COROLLARY 8.1.1. *If $p = 5f + 1$ is prime and x is given uniquely by* (8.15), *then*

$$x + \binom{2f}{f} + \binom{3f}{f} \equiv 0 \pmod{p}.$$

9. $e = 6$. There are two representative binomial coefficients of order 6, namely $\binom{2f}{f}$ and $\binom{3f}{f}$. In this section we establish a congruence for $\binom{2f}{f}$ which, in conjunction with Corollary 4.1.1, gives

$$\binom{3f}{f} \equiv 2x \pmod{p = 6f + 1}. \tag{9.1}$$

We have been unable to find a reference to this result.

Consider the Jacobi sum $J_6(2,5)$. By (3.4) and a result of Jacobi [**19**, p. 69], we have

$$J_6(2,5) = (-1)^f J_6(5,5) = \chi_6^{-1}(4) J_6(4,4),$$

that is (by (3.7))

$$J_6(2,5) = \chi_3^{-1}(2) J_3(2,2).$$

Since $\chi_3(2) \equiv 2^{(p-1)/3} \pmod{\pi}$ from (4.7) and (6.3) we obtain

$$J_6(2,5) \equiv \begin{cases} A \pmod{\pi}, & \text{if } A \equiv B \equiv 0 \pmod 2, \\ -\frac{1}{2}(A + 9B) \pmod{\pi}, & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv B \pmod 4, \\ -\frac{1}{2}(A - 9B) \pmod{\pi}, & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv -B \pmod 4. \end{cases}$$

Thus by Theorem 5.1 we have

THEOREM 9.1. *If $p = 6f + 1$ is prime and A, B are defined by* (4.23), *then*

$$\binom{2f}{f} \equiv \begin{cases} (-1)^{f+1} A \pmod p & \text{if } A \equiv B \equiv 0 \pmod 2, \\ (-1)^f \frac{1}{2}(A + 9B) \pmod p & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv B \pmod 4, \\ (-1)^f \frac{1}{2}(A - 9B) \pmod p & \text{if } A \equiv B \equiv 1 \pmod 2,\ A \equiv -B \pmod 4. \end{cases}$$

Appealing to (4.6), we obtain

THEOREM 9.2. *If $p = 6f + 1$ is prime and x, y are defined by* (4.4), *then*

$$\binom{2f}{f} \equiv \begin{cases} 2(-1)^f x \pmod p & \text{if } y \equiv 0 \pmod 3, \\ (-1)^f(-x + 3y) \pmod p & \text{if } y \equiv 1 \pmod 3, \\ (-1)^f(-x - 3y) \pmod p & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

EXAMPLE. We illustrate Theorems 9.1 and 9.2 by taking $p = 991$, so that $f = 165$, $x = 22$, $y = 13$, $A = 61$, $B = 3$. We have

$$\binom{2f}{f} = \binom{330}{165} \equiv 974 \equiv -17 \pmod{991},$$

$$(-1)^f(-x + 3y) = (-1)^f \frac{1}{2}(A - 9B) = -17.$$

10. $e = 7$. There are four representative binomial coefficients of order 7, namely,

$$\binom{2f}{f}, \binom{3f}{f}, \binom{4f}{f} \quad \text{and} \quad \binom{4f}{2f}.$$

By (2.2) and Lemma 2.1, we have

$$\binom{2f}{f}\binom{4f}{2f} \equiv \binom{3f}{f}\binom{4f}{f} \pmod{p} \tag{10.1}$$

so that it suffices to determine

$$\binom{2f}{f}, \binom{3f}{f} \quad \text{and} \quad \binom{4f}{f}$$

modulo p. In order to do this by means of Theorem 5.1 one must consider the Jacobi sums $J_7(2,6)$, $J_7(3,6)$ and $J_7(4,6)$, respectively. Of these, $J_7(3,6)$ is an integer of the subfield $Q\sqrt{-7}$ of $Q(\zeta_7)$, as

$$\sigma_2(J_7(3,6)) = J_7(6,5) = J_7(3,6),$$

and we are able to reprove Jacobi's result [**19**] for $\binom{3f}{f} \pmod{p}$ using Theorem 5.1. The other two Jacobi sums are related to $J_7(1,1)$ by

$$J_7(2,6) = J_7(6,6) = \sigma_6(J_7(1,1)), \quad J_7(4,6) = J_7(4,4) = \sigma_4(J_7(1,1)),$$

so that to determine $\binom{2f}{f}$ and $\binom{4f}{f}$ modulo p it suffices to consider $J_7(1,1)$. This Jacobi sum, unlike $J_7(3,6)$, does not belong to a subfield of $Q(\zeta_7)$. We are able to express $J_7(1,1)$ in the form $C_1\zeta_7 + C_2\zeta_7^2 + C_3\zeta_7^3 + C_4\zeta_7^4 + C_5\zeta_7^5 + C_6\zeta_7^6$ where the C_i, $i = 1,\ldots,6$, are linear combinations of a nontrivial solution $(x_1,\ldots,x_6)$ of (4.17). Using Theorem 5.1 we are able to obtain the congruence

$$\binom{2f}{f} \equiv -2(2x_1 + 7x_5R + 21x_6S) \pmod{\pi}$$

where

$$R = \zeta_7 + \zeta_7^2 - 2\zeta_7^3 - 2\zeta_7^4 + \zeta_7^5 + \zeta_7^6, \qquad S = \zeta_7 - \zeta_7^2 - \zeta_7^5 + \zeta_7^6,$$

and π denotes any prime factor of p in the ring of integers of $Q(\zeta_7)$, but, unfortunately, we have not been able to determine R and S mod π in any aesthetic form. Consequently, unlike the case $e = 5$, we are unable to give $\binom{2f}{f}$ and $\binom{4f}{f}$ mod p explicitly in terms of invariants of the system (4.17), although a result analogous to Theorem 8.1 (but more complicated) may well exist.

We are (in analogy to Rajwade's result [**34**]) able to evaluate

$$\binom{2f}{f} + \binom{4f}{f} + \binom{4f}{2f} \pmod{p}.$$

First we show, however, how Theorem 5.1 can be used to deduce Jacobi's result [**19**].

The ring R of integers of $Q(\zeta_7)$ is a unique factorization domain [**27**]. In R, p factors into primes as

$$p = \pi_1\pi_2\pi_3\pi_4\pi_5\pi_6, \tag{10.2}$$

where π is any prime factor of p in R and $\pi_i = \sigma_i(\pi)$, $i = 1, 2, 3, 4, 5, 6$. In precise analogy to the case $e = 5$ (see 8.4) we may normalize π so that

$$\pi \equiv 1 \pmod{(1-\zeta_7)^2}. \tag{10.3}$$

By (3.12) we have

$$J_7(1,2) \equiv 0 \pmod{\pi_1\pi_2\pi_4}$$

so

$$J_7(1,2) \equiv u\pi_1\pi_2\pi_4,$$

where u is an integer of $Q(\zeta_7)$. In view of (3.5) we have $u\bar{u} = 1$ so u is a unit of $Q(\zeta_7)$. As all units of $Q(\zeta_7)$ are of the form

$$\pm(\beta + \beta^6)^{k_1}(\beta^2 + \beta^5)^{k_2}\beta^l \tag{10.4}$$

(see, for example, [**36**, p. 99]), it follows from (10.4) that $k_1 = k_2 = 0$, therefore

$$u = \pm\beta^l, \qquad l = 0, 1, 2, 3, 4, 5, 6. \tag{10.5}$$

But $J_7(1,2) \equiv -1 \pmod{(1-\zeta_7)^2}$ and $\pi_1\pi_2\pi_4 \equiv 1 \pmod{(1-\zeta_7)^2}$ so

$$u \equiv -1 \pmod{(1-\zeta_7)^2}.$$

Thus (10.5) must hold with the minus sign and with $l = 0$, that is,

$$J_7(1,2) = -\pi_1\pi_2\pi_4.$$

Next, as

$$\sigma_2(J_7(1,2)) = \sigma_2(-\pi_1\pi_2\pi_4) = -\pi_2\pi_4\pi_1 = J_7(1,2),$$

we deduce that $J_7(1,2) \in Q(\sqrt{-7})$. Since $J_7(1,2)$ is an integer of $Q(\zeta_7)$, it must be an integer of $Q(\sqrt{-7})$, so there are integers X and Y with $X \equiv Y \pmod 2$ such that

$$J_7(1,2) = \frac{1}{2}\left(X + Y\sqrt{-7}\right). \tag{10.6}$$

As $J_7(1,2)\overline{J_7(1,2)} = p$, by (3.5), we have

$$4p = X^2 + 7Y^2, \tag{10.7}$$

which implies there exist integers x and y with $X = 2x$, $Y = 2y$, and (from (10.6) and (10.7))

$$J_7(1,2) = x + y\sqrt{-7}, \qquad x^2 + 7y^2 = p.$$

As $J_7(1,2) \equiv -1 \pmod{1-\zeta_7}^2$ and (as is easily checked),

$$\sqrt{-7} = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6 \equiv 0 \pmod{(1-\zeta_7)^2},$$

we have $x \equiv -1 \pmod{(1-\zeta_7)^2}$ so $x \equiv -1 \pmod 7$.

Finally, using Theorem 5.1 we have

$$\begin{aligned}\binom{3f}{f} &\equiv -J_7(3,6) \equiv -J_7(5,6) \equiv -\overline{J_7(1,2)} \\ &\equiv -\left(x - y\sqrt{-7}\right) \equiv -2x \pmod{\pi}.\end{aligned} \tag{10.8}$$

As the quantitites in the congruence (10.8) are rational integers, we have the following theorem due to Jacobi [**19**].

THEOREM 10.1. *If $p = 7f + 1$ is prime and x and y are integers with $p = x^2 + 7y^2$, $x \equiv -1 \pmod 7$, then*

$$\binom{3f}{f} \equiv -2x \pmod p.$$

We now show that a result analogous to that of Rajwade [**34**] follows easily from Theorem 5.1 and the basic properties of Jacobi sums listed in §3.

First, note that a precisely analogous argument to the one above for $J_7(1,2)$ gives

$$J_7(1,1) = -\pi_1\pi_4\pi_5 \quad \text{so} \quad J_7(1,1) \equiv J_7(2,2) \equiv J_7(3,3) \equiv 0 \pmod \pi.$$

By Theorem 5.1 we have

$$\binom{2f}{f} \equiv -J_7(2,6) \equiv -J_7(6,6) \pmod \pi, \tag{10.9}$$

$$\binom{4f}{f} \equiv -J_7(4,6) \equiv -J_7(4,4) \pmod \pi, \tag{10.10}$$

$$\binom{4f}{2f} \equiv -J_7(4,5) \equiv -J_7(5,5) \pmod \pi. \tag{10.11}$$

Adding (10.9)–(10.11) we obtain

$$\binom{2f}{f} + \binom{4f}{f} + \binom{4f}{2f} \equiv -1 \sum_{i=1}^{6} J_7(i,i) \pmod \pi.$$

Since

$$\sum_{i=1}^{6} J_7(i,i) = x_1, \qquad x_1 \equiv 1 \pmod 7,$$

we have

THEOREM 10.2. *If $p = 7f + 1$ is prime and $(x_1,\ldots,x_6)$ is a solution of* (4.17) *with $x_1 \equiv 1 \pmod 7$, then*

$$\binom{2f}{f} + \binom{4f}{f} + \binom{4f}{2f} \equiv -x_1 \pmod p.$$

EXAMPLE. We illustrate Theorem 10.2 by taking $p = 29$ so that $f = 4$ and $x_1 = 1$ (see [**47**]). In agreement with Theorem 10.2 we have, for $f = 4$,

$$\binom{2f}{f} + \binom{4f}{f} + \binom{4f}{2f} \equiv 12 + 22 + 23 \equiv -1 \pmod{29}.$$

11. $e = 8$. There are four representative binomial coefficients of order 8, namely,

$$\binom{2f}{f}, \binom{3f}{f}, \binom{4f}{f} \quad \text{and} \quad \binom{5f}{2f}.$$

Now, by Corollary 4.1.2, we have

$$\binom{3f}{f} \equiv (-1)^{f+b/4}\binom{4f}{2f} \pmod{p}, \tag{11.1}$$

and appealing to Theorem 7.1, we obtain

THEOREM 11.1. *If $p = 8f + 1$ is prime and a is given uniquely by $p = a^2 + b^2$, $a \equiv 1 \pmod 4$, then*

$$\binom{3f}{f} \equiv (-1)^{f+b/4} 2a \pmod{p}.$$

Next, from Lemma 2.1 and (2.2), we obtain

$$\binom{4f}{f}\binom{4f}{2f} \equiv (-1)^f \binom{3f}{f}\binom{5f}{2f} \pmod{p}. \tag{11.2}$$

Thus from (11.1) and (11.2) we have

$$\binom{5f}{2f} \equiv (-1)^{b/4}\binom{4f}{f} \pmod{p}. \tag{11.3}$$

Again, appealing to Lemma 2.1 and (2.2) we have

$$\binom{4f}{f}^2 \equiv (-1)^f \binom{2f}{f}\binom{5f}{2f} \pmod{p},$$

which gives, in view of (11.3),

$$\binom{2f}{f} \equiv (-1)^{f+b/4}\binom{4f}{f} \pmod{p}. \tag{11.4}$$

(11.3) and (11.4) show that it suffices to determine $\binom{4f}{f} \pmod p$. In order to do this we must consider $J_8(1,4)$.

We set $\beta = \zeta_8 = (1 + i)/\sqrt{2}$. The ring R of integers of $Q(\beta)$ is a unique factorization domain [27]. Let π denote a prime factor of p in R. We have

$$\sigma_3(J_8(1,4)) = J_8(3,4) = \frac{G_8(3)G_8(4)}{G_8(7)} = \frac{G_8(1)G_8(4)}{G_8(5)} = J_8(1,4),$$

so $J_8(1,4)$ belongs in the subfield $Q\sqrt{-2}$ of $Q(\beta)$. As $J_8(1,4)$ is an integer of $Q(\beta)$, it must be an integer of $Q(\sqrt{-2})$. Thus we can set

$$J_8(1,4) = -\left(c + d\sqrt{-2}\right), \tag{11.5}$$

where c and d are integers. As $J_8(1,4)\overline{J_8(1,4)} = p$, we have $p = c^2 + 2d^2$. Clearly, we have

$$\left(\frac{1-n}{p}\right) - 1 \equiv 0 \pmod 2 \quad \text{if } p \nmid 1 - n. \tag{11.6}$$

Further, since $\sqrt{-2} = \beta(i + i)$, we have

$$\chi_8(n) - 1 \equiv 0 \left(\mathrm{mod}\sqrt{-2}\right) \quad \text{if } \left(\frac{n}{p}\right) = +1, \tag{11.7}$$

$$\chi_8(n) - \beta \equiv 0 \left(\mathrm{mod}\sqrt{-2}\right) \quad \text{if } \left(\frac{n}{p}\right) = -1. \tag{11.8}$$

We now combine (11.6)–(11.8) and note that

$$\sum_{n=2}^{p-1} \left(\frac{1-n}{p}\right) = \begin{cases} -1, & \left(\frac{n}{p}\right) = +1, \\ 0, & \left(\frac{n}{p}\right) = -1, \end{cases}$$

$$\sum_{n=2}^{p-1,} 1 = \begin{cases} \frac{1}{2}(p-3), & \left(\frac{n}{p}\right) = +1, \\ \frac{1}{2}(p-1), & \left(\frac{n}{p}\right) = -1. \end{cases}$$

It clearly follows that

$$J_8(1,4) \equiv -1 \quad \left(\mathrm{mod}\, 2\sqrt{-2}\right), \tag{11.9}$$

so

$$c \equiv 1 \pmod 4. \tag{11.10}$$

Then by Theorem 5.1, we have

$$\begin{aligned} \binom{4f}{f} &\equiv (-1)^{f+1}\overline{J_8(4,7)} \pmod{\pi} \\ &\equiv (-1)^{f+1}\overline{J_8(1,4)} \pmod{\pi} \\ &\equiv (-1)^f\left(c - d\sqrt{-2}\right) \pmod{\pi}. \end{aligned}$$

But $J_8(1,4) \equiv 0 \pmod{\pi}$ by (3.12), so $c + d\sqrt{-2} \equiv 0 \pmod{\pi}$. Hence

$$\binom{4f}{f} \equiv (-1)^f 2c \pmod{\pi}.$$

Thus we have proved

THEOREM 11.2. *If $p = 8f + 1$ is prime with a and c defined uniquely by $p = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$,*

$$\begin{aligned} \binom{4f}{f} &\equiv (-1)^f 2c \pmod{p}, \\ \binom{5f}{2f} &\equiv (-1)^{f+b/4} 2c \pmod{p}, \\ \binom{2f}{f} &\equiv (-1)^{b/4} 2c \pmod{p}. \end{aligned}$$

The first congruence in Theorem 11.2 is due to Jacobi [**20**] and Stern [**40**].

12. $e = 9$. There are six representative binomial coefficients of order 9, and using (4.21) it is easy to show that all six are expressible in terms of

$$\binom{2f}{f}, \binom{3f}{f}, \binom{5f}{f}.$$

In particular,

$$\binom{2f}{f} \equiv 3^{(p-1)/3}\binom{4f}{f} \pmod{p}, \tag{12.1}$$

$$\binom{3f}{f} \equiv 3^{(p-1)/3}\binom{4f}{2f} \pmod{p}, \tag{12.2}$$

$$\binom{5f}{f} \equiv 3^{(p-1)/3}\binom{5f}{2f} \pmod{p}. \tag{12.3}$$

Unfortunately, we have been unable to determine any of these binomial coefficients explicitly. However, we are able to prove the following theorem analogous to a result of Jacobi; see Theorem 14.1.

THEOREM 12.1. *For* $p = 9f + 1$, $4p = A^2 + 27B^2$, $A \equiv 1 \pmod 3$, *we have*

$$\binom{2f}{f}\binom{5f}{f}\Big/\binom{4f}{2f} \equiv \binom{4f}{f}\binom{5f}{2f}\Big/\binom{3f}{f} \equiv -A \pmod{p}.$$

PROOF. Since

$$\binom{4f}{f}\binom{5f}{2f}\Big/\binom{3f}{f} = \frac{4f!\,5f!\,6f!}{3f!\,3f!\,6f!},$$

the result follows immediately from (2.1) and (12.1)–(12.3).

13. $e = 10$. There are six representatives binomial coefficients of order 10, namely,

$$\binom{2f}{f}, \binom{3f}{f}, \binom{4f}{f}, \binom{5f}{f}, \binom{5f}{2f}, \binom{6f}{3f}. \tag{13.1}$$

We show that all of the binomial coefficients in (13.1) can be determined from the lower order binomial coefficients $\binom{4f}{2f}$ and $\binom{6f}{2f}$ which are given explicitly in Theorem 8.1.

We begin by taking the Davenport-Hasse relation (3.9) with $e = 10$, $m = 5$, $t = 3$, to obtain

$$G_{10}(5)G_{10}(6) = \chi_5^3(2)G_{10}(3)G_{10}(8).$$

By (3.3) we have

$$\begin{aligned} J_{10}(5,8) &= G_{10}(5)G_{10}(8)/G_{10}(3) = \chi_5^3(2)G_{10}(8))^2/G_{10}(6) \\ &= \chi_5^3(2)J_{10}(8,8) = \chi_5^3(2)J_{10}(8,4) \end{aligned}$$

so, by Theorem 5.1, we have

$$\binom{5f}{2f} \equiv (2^{(p-1)/5})^3\binom{4f}{2f} \pmod{\pi},$$

where π is defined as in §8, so

$$\binom{5f}{2f} \equiv (2^{(p-1)/5})^3 \binom{4f}{2f} \pmod{p}. \tag{13.2}$$

From (4.10) and (13.2) we have

$$\binom{4f}{f} \equiv (-1)^f (2^{(p-1)/5})^4 \binom{4f}{2f} \pmod{p}. \tag{13.3}$$

Applying Lemma 2.1 (with $g = 5$, $h = 2$, $k = 4$) we have

$$\binom{6f}{3f} \equiv (-1)^f \binom{5f}{2f}^2 \Big/ \binom{4f}{2f} \pmod{p}. \tag{13.4}$$

Using (13.2) in (13.4) we obtain

$$\binom{6f}{3f} \equiv (-1)^f 2^{(p-1)/5} \binom{4f}{2f} \pmod{p}. \tag{13.5}$$

Applying Lemma 2.1 (with $g = 3$, $h = 1$, $k = 4$), using (2.2), (13.3), and (13.5), we obtain

$$\binom{3f}{f} \equiv (2^{(p-1)/5})^3 \binom{6f}{2f} \pmod{p}. \tag{13.6}$$

Next, applying Lemma 2.1 (with $g = 3$, $h = 1$, $k = 5$), using (2.2), (13.4)–(13.6), we get

$$\binom{5f}{f} \equiv 2^{(p-1)/5} \binom{6f}{2f} \pmod{p}. \tag{13.7}$$

Finally, applying Lemma 2.1 (with $g = 2$, $h = 1$, $k = 5$) and using (13.7) we obtain

$$\binom{2f}{f} \equiv (-1)^f (2^{(p-1)/5})^2 \binom{6f}{2f} \pmod{p}. \tag{13.8}$$

Combining (13.2), (13.3), and (13.5)–(13.8), we have the following new theorem.

THEOREM 13.1. *Let $p = 10f + 1$ be a prime and let (x, u, v, w) be a solution of* (8.15). *If 2 is a quintic residue of p (equivalently, x is even), we have*

$$\begin{aligned}
\binom{2f}{f} &\equiv (-1)^f \binom{3f}{f} \equiv (-1)^f \binom{5f}{f} \equiv (-1)^f \binom{6f}{2f} \\
&\equiv (-1)^f \left(-\frac{x}{2} - \frac{w(x^2 - 125w^2)}{8(xw + 5uv)} \right) \pmod{p}, \\
\binom{4f}{f} &\equiv (-1)^f \binom{4f}{2f} \equiv (-1)^f \binom{5f}{2f} \equiv \binom{6f}{3f} \\
&\equiv (-1)^f \left(-\frac{x}{2} + \frac{w(x^2 - 125w^2)}{8(xw + 5uv)} \right) \pmod{p}.
\end{aligned}$$

If 2 *is a quintic nonresidue of* p (*equivalently* x *is odd*), *we can choose a solution* (x, u, v, w) *of* (8.15) *satisfying* $u \equiv 0 \pmod 2$, $x + u - v \equiv 0 \pmod 4$ *so that* (*see Lehmer* [**21**])

$$2^{(p-1)/5} \equiv \alpha(x, u, v, w) \pmod p$$

where $\alpha = \alpha(x, u, v, w)$ *is given by* (4.13). *Then we have*

$$\begin{aligned}\binom{2f}{f} &\equiv (-1)^f \alpha^4 \binom{3f}{f} \equiv (-1)^f \alpha \binom{5f}{f} \equiv (-1)^f \alpha^2 \binom{6f}{2f} \\ &\equiv (-1)^f \alpha^2 \left(\frac{-x}{2} - \frac{w(x^2 - 125w^2)}{8(xw + 5uv)} \right) \pmod p, \\ \binom{4f}{f} &\equiv (-1)^f \alpha^4 \binom{4f}{2f} \equiv (-1)^f \alpha \binom{5f}{2f} \equiv \alpha^3 \binom{6f}{3f} \\ &\equiv (-1)^f \alpha^4 \left(\frac{x}{2} + \frac{w(x^2 - 125w^2)}{8(xw + 5uv)} \right) \pmod p.\end{aligned}$$

We close this section with two examples illustrating Theorem 13.1.

EXAMPLE. Let $p = 151$ so that $f = 15$ and 2 is a quintic residue of p. Then

$$\begin{aligned}\binom{30}{15} &\equiv -\binom{45}{15} \equiv -\binom{75}{15} \equiv -\binom{90}{30} \equiv 52 \pmod{151}, \\ \binom{60}{15} &\equiv -\binom{60}{30} \equiv -\binom{75}{30} \equiv \binom{90}{45} \equiv 95 \pmod{151}.\end{aligned}$$

A solution (x, u, v, w) of (8.15) with x even is given by $(x, u, v, w) = (-4, 2, 2, 4)$. In agreement with Theorem 13.1, we have

$$(-1)^f \left(-\frac{x}{2} - \frac{w(x^2 - 125w^2)}{8(xw + 5uv)} \right) = \frac{-4}{2} + \frac{4(16 - 2000)}{8(-16 + 20)} \equiv 52 \pmod{151},$$

and

$$(-1)^f \left(-\frac{x}{2} + \frac{w(x^2 - 125w^2)}{8(xw + 5uv)} \right) = \frac{-4}{2} - \frac{4(16 - 2000)}{8(-16 + 20)} \equiv 95 \pmod{151}.$$

EXAMPLE. Let $p = 11$ so that $f = 1$ and 2 is a quintic nonresidue of p. Note that $\alpha = 4$ so $\alpha^2 \equiv 5 \pmod{11}$, $\alpha^3 \equiv 9 \pmod{11}$, $\alpha^4 \equiv 3 \pmod{11}$. Now it is easily checked that

$$\binom{2}{1} \equiv -3\binom{3}{1} \equiv -4\binom{5}{1} \equiv -5\binom{6}{2} \equiv 2 \pmod{11}$$

and, similarly,

$$\binom{4}{1} \equiv -3\binom{4}{2} \equiv -4\binom{5}{2} \equiv 9\binom{6}{3} \equiv 4 \pmod{11}.$$

Moreover, solutions of (8.15) are

$$(x, u, v, w) = (1, 0, 1, 1), (1, -1, 0, -1), (1, 1, 0, -1), (1, 0, -1, 1).$$

The first of these solutions satisfies (4.12) ($u \equiv 0 \pmod 2$, $x + u - v \equiv 0 \pmod 4$) and, in agreement with Theorem 13.1, we have

$$(-1)^f\alpha^2\left(-\frac{x}{2} - \frac{w(x^2 - 125w^2)}{8(xw + 5uv)}\right) \equiv -5\left(-\frac{1}{2} - \frac{1 - 125}{8(1 + 0)}\right) \equiv 2 \pmod{11}$$

and

$$(-1)^f\alpha^4\left(-\frac{x}{2} - \frac{w(x^2 - 125w^2)}{8(xw + 5uv)}\right) \equiv -3\left(-\frac{1}{2} + \frac{1 - 125}{8(1 + 0)}\right) \equiv 4 \pmod{11}.$$

14. $e = 11$. There are ten representative binomial coefficients of order 11, namely

$$\binom{2f}{f}, \binom{3f}{f}, \binom{4f}{f}, \binom{5f}{f}, \binom{6f}{f}, \tag{14.1}$$
$$\binom{4f}{2f}, \binom{5f}{2f}, \binom{6f}{2f}, \binom{6f}{3f}, \binom{7f}{3f}.$$

It appears to be difficult to determine any of these explicitly modulo p in terms of the variables of a quadratic partition of p such as

$$4p = a^2 + 11b^2, \qquad a \equiv 2 \pmod{11}, \tag{14.2}$$

or the representation given in [**25**]. We first show that Theorem 5.1 can be used to reprove a theorem of Jacobi [**19**] relating $\binom{3f}{f}$, $\binom{4f}{2f}$ and $\binom{6f}{3f}$ modulo p.

Let π be a prime factor of p in the unique factorization domain R of integers of $Q(\zeta_{11})$. By Stickelberger's theorem (3.12), we have

$$J_{11}(1,2) \sim \pi_1\pi_2\pi_4\pi_6\pi_8, \quad J_{11}(2,2) \sim \pi_1\pi_2\pi_6\pi_7\pi_8, \quad J_{11}(3,3) \sim \pi_1\pi_3\pi_5\pi_7\pi_9,$$

where, if α_1 and α_2 are integers of $Q(\zeta_{11})$, $\alpha_1 \sim \alpha_2$ means that α_1/α_2 is a unit of the ring of integers of $Q(\zeta_{11})$. Hence,

$$\gamma = J_{11}(1,2)J_{11}(3,3)/J_{11}(2,2) \sim \pi_1\pi_3\pi_4\pi_5\pi_9, \tag{14.3}$$

showing that γ is an integer of $Q(\zeta_{11})$. Next, appealing to (3.3), we have

$$\gamma = G_{11}(1)G_{11}(3)G_{11}(4)/G_{11}(2)G_{11}(6),$$

so

$$\sigma_3(\gamma) = G_{11}(3)G_{11}(9)G_{11}(1)/G_{11}(6)G_{11}(7).$$

Since, by (3.6), $G_{11}(2)G_{11}(9) = G_{11}(4)G_{11}(7) = p$, we obtain $\sigma_3(\gamma) = \gamma$, which shows that γ belongs in the subfield $Q(\sqrt{-11})$ of $Q(\zeta_{11})$. As γ is an integer of $Q(\zeta_{11})$, it must be an integer of $Q(\sqrt{-11})$, and so has the form

$$\gamma = -\frac{1}{2}\left(a + b\sqrt{-11}\right), \tag{14.4}$$

where a, b are integers such that $a \equiv b \pmod 2$. From (14.3) and (3.5) we have $\gamma\bar{\gamma} = p$. Hence a and b satisfy the equation given in (14.2). The congruence in (14.2) follows as

$$a \equiv a + b\sqrt{-11} \equiv -2\gamma \equiv 2 \pmod{(1 - \zeta_{11})^2},$$

by (3.8).

Finally by Theorem 5.1 we have

$$J_{11}(9,10) \equiv -\binom{9f}{f} \pmod{\pi},$$

$$J_{11}(8,8) \equiv -\binom{8f}{3f} \pmod{\pi},$$

$$J_{11}(9,9) \equiv -\binom{9f}{2f} \pmod{\pi},$$

so

$$\binom{9f}{f}\binom{8f}{3f}\Big/\binom{9f}{2f} \equiv -\bar{\gamma} \equiv \frac{1}{2}\left(a - b\sqrt{-11}\right) \pmod{\pi}. \tag{14.5}$$

But from (14.3) and (14.4) we have

$$\frac{1}{2}\left(a + b\sqrt{-11}\right) \equiv 0 \pmod{\pi}. \tag{14.6}$$

Hence from (14.5) and (14.6) we have

$$\binom{9f}{f}\binom{8f}{3f}\Big/\binom{9f}{2f} \equiv a \pmod{\pi},$$

and so appealing to (2.2), we obtain

THEOREM 14.1. *If $p = 11f + 1$ is prime and a is defined uniquely by $4p = a^2 + 11b^2$, $a \equiv 2 \pmod{11}$, we then have*

$$\binom{3f}{f}\binom{6f}{3f}\Big/\binom{4f}{2f} \equiv a \pmod{p}.$$

This is equivalent to Jacobi's result [**19**]

$$a \equiv \frac{1}{f!\,3f!\,4f!\,5f!\,9f!} \pmod{p}.$$

EXAMPLE. With $p = 89$, so that $f = 8$, $a = -9$, $b = 5$, we have

$$\binom{24}{8}\binom{48}{24}\Big/\binom{32}{16} \equiv \frac{(64)(72)}{22} \equiv \frac{79}{11} \equiv -9 \pmod{89}.$$

15. $e = 12$. There are eight representative binomial coefficients of order 12, namely,

$$\binom{2f}{f}, \binom{3f}{f}, \binom{4f}{f}, \binom{5f}{f}, \binom{6f}{f}, \binom{5f}{2f}, \binom{7f}{2f}, \binom{7f}{3f}. \tag{15.1}$$

We show that all the binomial coefficients in (15.1) can be determined from the lower order binomial coefficients $\binom{6f}{2f}$, $\binom{6f}{3f}$ and $\binom{8f}{4f}$.

We begin by determining $\binom{3f}{f}$ in terms of $\binom{6f}{2f}$ modulo p. Let P be a prime ideal divisor of p in $Q(\zeta_{12})$ and define g and χ_{12} as in §3. Then it is known (see, for example, Whiteman [**44**, p. 61]) that $J_{12}(3,3) = -a + bi$ where $p = a^2 + b^2$, $a \equiv 1 \pmod 4$.

Appealing to Whiteman's cyclotomic numbers of order 12 [**44**] we have

$$J_{12}(1,2) = (-1)^f c\chi_{12}(3)J_{12}(2,4), \tag{15.2}$$

where c is given by

$$c = \begin{cases} (-1)^f & \text{if } a \equiv 1 \pmod 3,\ b \equiv 0 \pmod 3, \\ (-1)^{f+1} & \text{if } a \equiv 2 \pmod 3,\ b \equiv 0 \pmod 3, \\ (-1)^{f+1} i & \text{if } b \equiv 1 \pmod 3,\ a \equiv 0 \pmod 3, \\ (-1)^f i & \text{if } b \equiv 2 \pmod 3,\ a \equiv 0 \pmod 3. \end{cases} \tag{15.3}$$

Now 3 is clearly a quadratic residue of p so that $\chi_4(3) = (-1)^f$ if $b \equiv 0 \pmod 3$ and $\chi_4(3) = (-1)^{f+1}$ if $a \equiv 0 \pmod 3$ (see, for example, [**22**, p. 24]). Taking conjugates on both sides of (15.2) we have

$$J_{12}(10,11) = \varepsilon\bar{c}J_{12}(10,8),$$

where

$$\varepsilon = \begin{cases} +1 & \text{if } b \equiv 0 \pmod 3, \\ -1 & \text{if } a \equiv 0 \pmod 3. \end{cases}$$

Appealing to Theorem 5.1, we have

$$(-1)^{f+1}\binom{10f}{f} \equiv -\varepsilon\bar{c}\binom{10f}{4f} \pmod P.$$

Finally, as $J_{12}(3,3) = -a + bi \equiv 0 \pmod P$ we have, using (2.2),

$$\binom{3f}{f} \equiv \theta\binom{6f}{2f} \pmod p, \tag{15.4}$$

where

$$\theta = \begin{cases} (-1)^f & \text{if } a \equiv 1 \pmod 3,\ b \equiv 0 \pmod 3, \\ (-1)^{f+1} & \text{if } a \equiv 2 \pmod 3,\ b \equiv 0 \pmod 3, \\ (-1)^f b/a & \text{if } b \equiv 1 \pmod 3,\ a \equiv 0 \pmod 3, \\ (-1)^{f+1} b/a & \text{if } b \equiv 2 \pmod 3,\ a \equiv 0 \pmod 3. \end{cases} \tag{15.5}$$

We now show that the 7 remaining binomial coefficients of order 12 may be determined in terms of lower order binomial coefficients.

Corollary 4.1.5 relates $\binom{5f}{f}$ and $\binom{6f}{2f}$ modulo p. However, Corollary 4.4.1 gives a simpler congruence, namely,

$$\binom{5f}{f} \equiv \binom{8f}{4f} \pmod p. \tag{15.6}$$

Corollary 4.2.2 gives the congruence

$$\binom{6f}{f} \equiv \varepsilon\binom{6f}{3f}.$$

Corollary 4.3.1 gives the congruence

$$\binom{2f}{f} \equiv (2^{(p-1)/3})^2 \binom{6f}{f} \equiv \varepsilon(2^{(p-1)/3})^2 \binom{6f}{3f} \pmod{p}. \tag{15.7}$$

Appealing to (2.2) and Lemma 2.1 ($g = 2, h = 1, k = 9$) we have

$$\binom{2f}{f} \Big/ \binom{3f}{f} \equiv (-1)^f \binom{9f}{f} \Big/ \binom{10f}{2f} \equiv \binom{4f}{f} \Big/ \binom{4f}{2f} \pmod{p}.$$

Thus, using (4.3), we obtain

$$\binom{4f}{f} \equiv \binom{2f}{f}\binom{4f}{2f} \Big/ \binom{3f}{f} \equiv 2^{(p-1)/3} \binom{2f}{f}\binom{6f}{2f} \Big/ \binom{3f}{f} \pmod{p}.$$

Now using (15.4) and (15.7) we have

$$\binom{4f}{f} \equiv \theta \binom{6f}{3f} \pmod{p}. \tag{15.8}$$

Next using Lemma 2.1 ($g = 7, h = 3, k = 4$) we have

$$\binom{7f}{3f} \Big/ \binom{8f}{4f} \equiv (-1)^f \binom{4f}{f} \Big/ \binom{5f}{f} \pmod{p},$$

so, using (15.5) and (15.8), we obtain

$$\binom{7f}{3f} \equiv (-1)^f \theta \binom{6f}{3f} \pmod{p}. \tag{15.9}$$

Again appealing to Lemma 2.1 ($g = 6, h = 3, k = 5$), we have

$$\binom{6f}{3f} \Big/ \binom{7f}{3f} \equiv (-1)^f \binom{5f}{3f} \Big/ \binom{6f}{2f} \pmod{p}.$$

Using (15.9) we have

$$\binom{5f}{2f} \equiv \theta^{-1} \binom{6f}{2f} \pmod{p}. \tag{15.10}$$

Finally, appealing to Lemma 2.1 ($g = 4, h = 2, k = 5$) and using (2.2), we have

$$\binom{4f}{2f} \Big/ \binom{5f}{2f} \equiv (-1)^f \binom{7f}{2f} \Big/ \binom{8f}{3f} \equiv \binom{7f}{2f} \Big/ \binom{7f}{3f} \pmod{p}.$$

Using (4.3), (15.9) and (15.10) we have

$$\begin{aligned} \binom{7f}{f} &\equiv \binom{4f}{2f}\binom{7f}{3f} \Big/ \binom{5f}{2f} \\ &\equiv \left(2^{(p-1)/3}\binom{6f}{2f}\right)\left((-1)^f \theta \binom{6f}{3f}\right) \Big/ \theta^{-1}\binom{6f}{2f} \pmod{p}, \end{aligned}$$

so that after cancellation we obtain

$$\binom{7f}{2f} \equiv (-1)^f 2^{(p-1)/3} \varepsilon \binom{6f}{3f} \pmod{p}. \tag{15.11}$$

Combining (15.4) and (15.11) and appealing to (4.5), Corollary 4.1.1, and Theorems 6.1, 7.1 and 9.2, we have

THEOREM 15.1. *Let* $p = 12f + 1 = a^2 + b^2 = x^2 + 3y^2$ *be a prime with* $a \equiv 1 \pmod 4$, $x \equiv 1 \pmod 3$, *and let* $4p = A^2 + 27B^2$ *with* $A \equiv 1 \pmod 3$. *Then we have the following congruences modulo* p:

$$\binom{2f}{f} \equiv 2\theta^2\phi^2 a, \quad \binom{3f}{f} \equiv 2\theta x, \quad \binom{4f}{f} \equiv 2\theta a, \quad \binom{5f}{f} \equiv -A, \quad \binom{6f}{f} \equiv 2\theta^2 a,$$

$$\binom{5f}{2f} \equiv \frac{2x}{\theta}, \quad \binom{7f}{2f} \equiv 2(-1)^f \theta^2 \phi a, \quad \binom{7f}{3f} \equiv 2(-1)^f \theta a,$$

where θ *is given by* (15.5) *and* ϕ *by*

$$\phi = \begin{cases} 1 & \text{if } y \equiv 0 \pmod 3, \\ (x + 3y)/(x - 3y) & \text{if } y \equiv 1 \pmod 3, \\ (x - 3y)/(x + 3y) & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

EXAMPLE. For $p \leqslant 97$, formulas (15.4)–(15.11) and Theorem 14.1 can be easily checked from the following brief table of values. (See Table 2.)

16. $e = 13$. Since $\sigma_3(J_{13}(1,3)) = J_{13}(3,9) = J_{13}(1,3)$, $J_{13}(1,3)$ is an integer of the field $Q(i\sqrt{26 + 6\sqrt{13}})$. Zee [**15**, p. 263] has shown that

$$J_{13}(1,3) = \frac{1}{4}\left(x + w\sqrt{13} + i\left(u\sqrt{26 + 6\sqrt{13}} + v\sqrt{26 - 6\sqrt{13}}\right)\right), \tag{16.1}$$

where (x, u, v, w) is a solution of the system

$$\begin{cases} 16p = x^2 + 26u^2 + 26v^2 + 13w^2, & x \equiv 9 \pmod{13}, \\ xw = 3v^2 - 4uv - 3u^2. \end{cases} \tag{16.2}$$

We prove

THEOREM 16.1. *If* $p = 13f + 1$ *is prime then*

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

and

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

where (x, u, v, w) *is any solution of* (16.2).

PROOF. The ring of integers of $Q(\zeta_{13})$ is a unique factorization domain (see, for example, [**27**]). Let π be a prime dividing p in $Q(\zeta_{13})$. By Theorem 5.1 and (2.2), we have

$$\binom{4f}{f} \equiv \binom{10f}{f} \equiv -J_{13}(10,12) \pmod \pi. \tag{16.3}$$

Since, by (3.12), we have

$$J_{13}(1,3) \equiv 0 \pmod{\pi}, \tag{16.4}$$

adding (16.3) and (16.4) and appealing to (16.1), we obtain

$$2\,\Re e\big(J_{13}(1,3)\big) \equiv -\binom{4f}{f} \pmod{\pi},$$

that is,

$$\binom{4f}{f} \equiv -\frac{1}{2}\big(x + w\sqrt{13}\big) \pmod{\pi}. \tag{16.5}$$

For brevity we set $\beta = \zeta_{13}$. We have (see, for example, [**51**, pp. 262–263])

$$\beta + \beta^3 + \beta^4 + \beta^9 + \beta^{10} + \beta^{12} = \frac{1}{2}\big(\sqrt{13} - 1\big), \tag{16.6}$$

$$\beta^2 + \beta^5 + \beta^6 + \beta^7 + \beta^8 + \beta^{11} = \frac{1}{2}\big(-\sqrt{13 - 1}\big), \tag{16.7}$$

$$\beta^2 + \beta^5 + \beta^6 - \beta^7 - \beta^8 - \beta^{11} = \frac{i}{2}\sqrt{26 + 6\sqrt{13}}\,, \tag{16.8}$$

$$\beta + \beta^3 - \beta^4 + \beta^9 - \beta^{10} - \beta^{12} = \frac{i}{2}\sqrt{26 - 6\sqrt{13}}\,. \tag{16.9}$$

By (3.12) and (16.1) we have

$$\frac{1}{4}\Big(x + w\sqrt{13} + i\Big(u\sqrt{26 + 6\sqrt{13}} + v\sqrt{26 - 6\sqrt{13}}\Big)\Big) \equiv 0 \pmod{\pi}. \tag{16.10}$$

Applying the automorphism σ_2 to (16.10) and appealing to (16.1)–(16.9), we obtain

$$\frac{1}{4}\Big(x - w\sqrt{13} - i\Big(u\sqrt{26 - 6\sqrt{13}} - v\sqrt{26 + 6\sqrt{13}}\Big)\Big) \equiv 0 \pmod{\pi}. \tag{16.11}$$

From (16.1) and (16.4) we have

$$\frac{1}{4}\Big(x + w\sqrt{13} + i\Big(u\sqrt{26 + 6\sqrt{13}} + v\sqrt{26 - 6\sqrt{13}}\Big)\Big) \equiv 0 \pmod{\pi}. \tag{16.12}$$

Adding (16.11) and (16.12) we get

$$\begin{aligned} 2x + iu\Big(\sqrt{26 + 6\sqrt{13}} - \sqrt{26 - 6\sqrt{13}}\Big) \\ + iv\Big(\sqrt{26 + 6\sqrt{13}} + \sqrt{26 - 6\sqrt{13}}\Big) \equiv 0 \pmod{\pi}. \end{aligned} \tag{16.13}$$

Taking the term $2x$ to the right-hand side of (16.13) and squaring, we obtain, after some simplication,

$$\sqrt{13} \equiv (x^2 + 13u^2 + 13v^2)/(2u^2 - 6uv - 2v^2) \pmod{\pi}. \tag{16.14}$$

Next, using (16.2), we get

$$\sqrt{13} \equiv -3(x^2 - 13w^2)/4(xw + 13uv) \pmod{\pi}. \tag{16.15}$$

Substituting (16.15) into (16.5), we have

$$\binom{4f}{f} \equiv -\frac{x}{2} + \frac{3(x^2 - 13w^2)w}{8(xw + 13uv)} \pmod{\pi}. \tag{16.16}$$

R. J. Evans (personal communication) has shown that all solutions of (16.2) are given by

$$(x, u, v, w), \quad (x, -u, -v, w), \quad (x, v, -u, -w), \quad (x, -v, u, -w).$$

Hence, x, w^2 and uv/w are independent of the choice of solution of (16.2), and thus (16.16) holds (mod p). This completes the proof of the first part of the theorem. The second part follows similarly, by considering $J_{13}(7, 11) = J_{13}(7, 8) = \sigma_7(J_{13}(1, 3))$ in place of $J_{13}(1, 3)$.

COROLLARY 16.1. *If $p = 13f + 1$ is prime and x is given uniquely by* (16.2), *then*

$$x \equiv -\binom{4f}{f} - \binom{7f}{2f} \pmod{p}.$$

EXAMPLE. We taken $p = 53$ so that $f = 4$. A solution of (16.2) is given by $(x, u, v, w) = (9, 3, 4, -3)$, so that

$$-x/2 \equiv 22, \qquad 3(x^2 - 13w^2)w/8(xw + 13uv) \equiv 49 \pmod{53}.$$

Hence, by Theorem 6.1, we have (mod 53),

$$\binom{4f}{f} \equiv 22 + 49 \equiv 18, \qquad \binom{7f}{2f} \equiv 22 - 49 \equiv 26.$$

Indeed, we have

$$\binom{4f}{f} = \binom{16}{4} = 1820 \equiv 18 \pmod{53},$$

$$\binom{7f}{2f} = \binom{28}{8} = 3108105 \equiv 26 \pmod{53}.$$

17. $e = 14$. There are 16 representative binomial coefficients to consider when $e = 14$ (see Table in §2), four of which are of lower order. The binomial coefficient $\binom{6f}{2f}$ is given by Theorem 10.1. In this section we show that the 12 representatives of order 14 can all be expressed in terms of the lower order binomial coefficients

$$\binom{4f}{2f}, \binom{8f}{2f}, \quad \text{and} \quad \binom{8f}{4f}.$$

In particular, we prove

THEOREM 17.1. *If $p = 14f + 1$ is prime then the sixteen representative binomial coefficients can all be expressed in terms of the lower order binomial coefficients*

$$\binom{4f}{2f}, \binom{8f}{2f}, \binom{8f}{4f}.$$

We have (mod p),

$$\binom{2f}{f} = 2^{5(p-1)/7}\binom{4f}{f} \equiv (-1)^f 2^{(p-1)/7}\binom{7f}{f}$$

$$\equiv 2^{(p-1)/7}\binom{8f}{3f} \equiv (-1)^f 2^{2(p-1)/7}\binom{8f}{2f},$$

$$\binom{3f}{f} \equiv (-1)^f 2^{6(p-1)/7}\binom{6f}{f} \equiv \binom{7f}{2f} \equiv 2^{2(p-1)/7}\binom{9f}{4f} \equiv 2^{5(p-1)/7}\binom{4f}{2f},$$

$$\binom{5f}{f} \equiv 2^{5(p-1)/7}\binom{5f}{2f} \equiv (-1)2^{4(p-1)/7}\binom{6f}{3f} \equiv \binom{7f}{3f} \equiv 2^{3(p-1)/7}\binom{8f}{4f}.$$

PROOF. We begin by noting that

$$\binom{2f}{f}\Big/\binom{4f}{f} = \binom{3f}{f}\Big/\binom{4f}{2f}, \qquad \binom{4f}{f}\Big/\binom{8f}{3f} = \binom{5f}{f}\Big/\binom{8f}{4f}, \tag{17.1}$$

$$\binom{5f}{2f}\Big/\binom{6f}{3f} = \binom{3f}{f}\Big/\binom{6f}{f}.$$

For brevity we denote ζ_{14} by β.

From the work of Dickson [**9**] (see also Muskat [**28**]) we have

$$J_{14}(1,4) = \beta^{8\text{ind}} g^{(2)} J_{14}(4,4) \qquad [\mathbf{28}, (4.7)], \tag{17.2}$$

and

$$J_{14}(1,6) = \beta^{12\text{ind}} g^{(2)} J_{14}(6,6) \qquad [\mathbf{28}, (4.8)]. \tag{17.3}$$

Applying the automorphisms σ_{13} and σ_{11} to (17.2) and (17.3), respectively, we obtain

$$J_{14}(13,10) = \beta^{6\text{ind}} g^{(2)} J_{14}(10,10)$$

and

$$J_{14}(11,10) = \beta^{6\text{ind}} g^{(2)} J_{14}(10,10),$$

so

$$J_{14}(13,10) = J_{14}(11,10).$$

Hence by Theorem 5.1 we have

$$\binom{10f}{f} \equiv \binom{10f}{3f} \pmod{\pi},$$

where π is a prime ideal divisor of P in $Q(\beta)$. Appealing to (2.2), we obtain

$$\binom{5f}{f} \equiv \binom{7f}{3f} \pmod{p}. \tag{17.4}$$

The proof of

$$\binom{3f}{f} \equiv \binom{7f}{2f} \pmod{p} \tag{17.5}$$

is similar.

Next, appealing to (3.11) with $n = 2$ and $t = 1, 2, \ldots, m-1$ we have, using (2.2),

$$2^{t(p-1)/m} \equiv (-1)^{mf} \binom{2tf}{tf} \Big/ \binom{mf}{tf} \pmod{p}.$$

Applying Lemma 2.1 with $g = 2t$, $h = t$, $k = m$, $e = 2m$, we have from (17.1),

$$2^{t(p-1)/m} \equiv \binom{mf}{tf} \Big/ \binom{(2m-2t)f}{(m-t)f} \pmod{p}.$$

Appealing to (17.2) and (17.3) with $t = 1, 2, 3$, and $m = 7$, and using (2.2) we obtain (mod p),

$$\text{(17.6)} \qquad \binom{2f}{f} \equiv (-1)^f 2^{(p-1)/7} \binom{7f}{f}, \quad \binom{7f}{f} \equiv 2^{(p-1)/7} \binom{8f}{2f},$$

$$\text{(17.7)} \qquad \binom{4f}{2f} \equiv 2^{2(p-1)/7} \binom{7f}{2f}, \quad \binom{7f}{2f} \equiv 2^{2(p-1)/7} \binom{9f}{4f},$$

$$\text{(17.8)} \qquad \binom{6f}{3f} \equiv (-1)^f 2^{3(p-1)/7} \binom{7f}{3f}, \quad \binom{7f}{3f} \equiv 2^{3(p-1)/7} \binom{8f}{4f}.$$

Moreover, from (4.16) we have

$$\text{(17.9)} \qquad \binom{6f}{f} \equiv (-1)^f 2^{(p-1)/7} \binom{7f}{2f}.$$

Theorem 17.1 now follows easily from (17.1)–(17.9).

REMARK. The congruences in (17.4), (17.5), and

$$\binom{7f}{f} \equiv (-1)^f \binom{8f}{3f} \pmod{p}$$

(Theorem 17.1) are of Cauchy-Whiteman type (see [**17**], (1.6), and §21).

18. $e = 15$. There are 19 representative binomial coefficients to consider when $e = 15$, including 3 of lower order. We begin this section by establishing seven congruences relating these representatives solely by powers of $5^{(p-1)/3}$ or $3^{(p-1)/5}$. We prove the following.

THEOREM 18.1. *If* $p = 15f + 1$ *then we have the following congruences* (mod p):

$$\binom{5f}{f} \equiv 5^{(p-1)/3} \binom{7f}{2f},$$

$$\binom{3f}{f} \equiv 3^{(p-1)/5} \binom{6f}{2f} \equiv 3^{2(p-1)/5} \binom{7f}{f} \equiv 3^{3(p-1)/5} \binom{7f}{3f},$$

$$\binom{8f}{2f} \equiv 3^{2(p-1)/5} \binom{9f}{3f}, \quad \binom{4f}{f} \equiv 3^{(p-1)/5} \binom{6f}{3f}.$$

PROOF. The first and fourth congruences in Theorems 18.1 are exactly (4.26) and (4.27).

The third congruence can be established using (2.2) and Lemma 2.1 with $g = 3$, $h = 2$, $k = 6$ to obtain

$$\binom{3f}{f}\binom{7f}{3f} \equiv \binom{6f}{2f}\binom{7f}{f};$$

the second congruence follows at once from this, and the third follows from the second.

The fourth, sixth and seventh congruences are easy consequences of (2.1) and (3.11). For, using (3.11) with $n = 3$, $t = 3$, $m = 5$, it follows from (2.1) that

$$3^{3(p-1)/5} \equiv \frac{9f!\,10f!\,15f!}{3f!\,8f!\,13f!} \equiv \frac{7f!}{f!\,6f!} \cdot \frac{2f!\,f!}{3f!} \pmod{p}.$$

Similarly, using (3.11) with $n = 3$, $t = 2$, $m = 5$, it follows from (2.1) that

$$3^{2(p-1)/5} \equiv \frac{6f!\,10f!\,15f!}{2f!\,7f!\,12f!} \equiv \frac{8f!}{2f!\,6f!} \cdot \frac{3f!\,6f!}{9f!} \pmod{p}.$$

Next, using (3.11) with $n = 3$, $t = 1$, $m = 5$ it follows from (2.1) that

$$3^{(p-1)/5} \equiv \frac{3f!\,5f!\,10f!}{f!\,6f!\,11f!} \equiv \frac{4f!}{f!\,3f!} \cdot \frac{3f!\,3f!}{6f!} \pmod{p}.$$

Finally the fifth congruence clearly follows from the second and the fourth.

The last two congruences in Theorem 18.1 are particularly interesting because they relate binomial coefficients of order 15 to the lower order binomial coefficients given explicitly in terms of the system (8.15) in Theorem 8.1. In particular, we have

$$\binom{4f}{f} \equiv 3^{(p-1)/5}\left(-\frac{x}{2} + \frac{w(x^2 - 125w^2)}{8(xw + 5uv)}\right) \pmod{p} \tag{18.1}$$

and

$$\binom{8f}{2f} \equiv 3^{2(p-1)/5}\left(-\frac{x}{2} - \frac{w(x^2 - 125w^2)}{8(xw + 5uv)}\right) \pmod{p}. \tag{18.2}$$

EXAMPLE. Let $p = 31 = 15(2) + 1$ so that $(x, u, v, w) = (11, 1, -2, 1)$ is a solution of (8.15). As $3^6 \equiv 16 \pmod{31}$ and $3^{13} \equiv 8 \pmod{31}$, we have

$$\binom{8}{2} = 28 \equiv 16\left(-\frac{11}{2} - \frac{4}{8}\right) \equiv -96 \pmod{31},$$

$$\binom{16}{4} \equiv 22 \equiv 8\left(-\frac{11}{2} + \frac{4}{8}\right) \equiv -40 \pmod{31},$$

in agreement with (18.1) and (18.2).

Next we use the Jacobi sum $J_{15}(1, 4)$ to explicitly determine $\binom{5f}{f}$ and $\binom{7f}{2f}$ in terms of parameters in the quadratic forms $p = g^2 + 15h^2$ and $4p = A^2 + 27B^2$. In particular we prove

THEOREM 18.2. *Let* $p = 15f + 1 = g^2 + 15h^2$, $4p = A^2 + 27B^2$, $A \equiv g \equiv 1 \pmod 3$. *Then we have*

$$\left(\frac{5f}{f}\right) \equiv \begin{cases} 2g \pmod p & \text{if } AB \equiv 0 \pmod 5, \\ \dfrac{2Ag - 18Bg}{A + 9B} \pmod p & \text{if } A \equiv B \text{ or } -2B \pmod 5, \\ \dfrac{2AG + 18Bg}{A - 9B} \pmod p & \text{if } A \equiv -B \text{ or } 2B \pmod 5, \end{cases}$$

$$\left(\frac{7f}{2f}\right) \equiv \begin{cases} 2g \pmod p & \text{if } AB \equiv 0 \pmod 5, \\ \dfrac{2Ag + 18Bg}{A - 9B} \pmod p & \text{if } A \equiv B \text{ or } -2B \pmod 5, \\ \dfrac{2Ag - 18Bg}{A + 9B} \pmod p & \text{if } A \equiv -B \text{ or } 2B \pmod 5. \end{cases}$$

PROOF. From Muskat [**30**, p. 498] we have $J_{15}(1,4) = 5^{(p-1)/3}(-g + h\sqrt{15}\,i)$. Appealing directly to Lemma 6 of [**45**] and noting that

$$J_{15}(14,11) = (5^{(p-1)/3})^2\left(-g - h\sqrt{15i}\right),$$

one immediately deduces (by adding and using (4.28)) the first congruence in Theorem 18.2.

The second congruence is then an immediate consequence of (4.27), completing the proof of Theorem 18.2.

Consider now the Diophantine system

$$(18.3) \qquad \begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2, & x \equiv 1 \pmod 5, \\ xw = v^2 - 4uv - u^2; \end{cases}$$

let $\alpha = 1$ if $3^{(p-1)/5} = +1$, and if 3 is a quintic nonresidue of p, let

$$(18.4) \qquad \alpha(x,u,v,w) = \frac{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)},$$

where (x, u, v, w) is the unique solution of one of

$$(18.5) \qquad \begin{array}{llll} \text{(a)} & x \equiv 1, & u \equiv 1, & v \equiv 0, \quad w \equiv 2 \pmod 3, \\ \text{(b)} & x \equiv 2, & u \equiv 2, & v \equiv 0, \quad w \equiv 1 \pmod 3, \\ \text{(c)} & x \equiv 1, & u \equiv 2, & v \equiv 1, \quad w \equiv 1 \pmod 3, \\ \text{(d)} & x \equiv 2, & u \equiv 1, & v \equiv 2, \quad w \equiv 2 \pmod 3. \end{array}$$

Then Williams [**49**] has shown that

$$(18.6) \qquad 3^{(p-1)/5} \equiv \alpha(x,u,v,w) \pmod p.$$

A straightforward calculation shows that

$$(18.7) \qquad (3^{(p-1)/5})^2 \equiv \alpha(x,-v,u,-w) \pmod p,$$

$$(18.8) \qquad (3^{(p-1)/5})^3 \equiv \alpha(x,v,-u,-w) \pmod p,$$

$$(18.9) \qquad (3^{(p-1)/5})^4 \equiv \alpha(x,-u,-v,w) \pmod p.$$

Using Jacobi sums first given by Dickson [**10**] with a sign ambiguity, and later by Muskat [**30**] with the sign ambiguity neatly removed, we obtain

THEOREM 18.3. *Let* $p = 15f + 1 = g^2 + 15h^2$, $g \equiv 1 \pmod 3$, *and let* (x, u, v, w) *be the unique solution of* (18.5) *satisfying* (18.3). *Then we have, modulo* p,

$$\binom{3f}{f} \equiv (-1)^{[2g/5]} 2g\alpha(x, -u, -v, w), \qquad \binom{7f}{f} \equiv (-1)^{[2g/5]} 2g\alpha(x, -v, u, -w),$$

$$\binom{6f}{2f} \equiv (-1)^{[2g/5]} 2g\alpha(x, v, -u, -w), \qquad \binom{7f}{3f} \equiv (-1)^{[2g/5]} 2g\alpha(x, u, v, w).$$

PROOF. From Muskat [**30**, p. 487] we have

$$J_{15}(1,4) = b(5^{(p-1)/3})^2(3^{(p-1)/5})J_{15}(1,2),$$

where $b = (-1)^{[2g/5]}$ by [**30**, p. 498]. Thus

$$J_{15}(14,11) = b5^{(p-1)/3}(3^{(p-1)/5})^4 J_{15}(14,13),$$

so that, again appealing to Lemma 6 of [**45**], we deduce that

$$\binom{5f}{f} \equiv (-1)^{[2g/5]} 5^{(p-1)/3}(3^{(p-1)/5})^4 \binom{3f}{f} \pmod p$$

from which the first congruence in Theorem 18.3 follows in view of (4.28), Theorem 18.2, and (18.9). Theorem 18.1 now gives the remaining congruences.

EXAMPLE. Let $p = 661$ so that $3^{(p-1)/5} \equiv 1 \pmod{661}$,

$$5^{(p-1)/3} \equiv \frac{A + 9B}{A - 9B} = \frac{76}{22} \equiv 364 \pmod{661},$$

$$(5^{(p-1)/3})^2 \equiv 22/76 \equiv 296 \pmod{661},$$

$g = -11$ so that $(-1)^{[2g/5]} = -1$. From Theorems 18.2 and 18.3 we have, for $f = 4$,

$$\binom{5f}{f} = (-22)(296) \equiv 98 \pmod{661},$$

$$\binom{7f}{2f} \equiv (-22)(364) \equiv 585 \pmod{661},$$

and

$$\binom{3f}{f} \equiv \binom{7f}{f} \equiv \binom{6f}{2f} \equiv \binom{7f}{3f} \equiv (-1)^{[2g/5]} 2g \equiv 22 \pmod{661},$$

all in agreement with values for these binomial coefficients obtained from computer data.

The remaining binomial coefficients of order 15, namely

$$\binom{2f}{f}, \binom{6f}{f}, \binom{8f}{f}, \binom{8f}{3f}, \binom{4f}{2f}, \binom{5f}{2f}, \binom{8f}{4f}, \binom{9f}{4f}$$

are related to one another in the following theorem.

THEOREM 18.4. *Let* $p = 15f + 1$. *Then we have*

$$\binom{6f}{f}\Big/\binom{2f}{f} \equiv \alpha^2\binom{8f}{3f}\Big/\binom{8f}{f} \equiv \alpha^4\binom{4f}{2f}\Big/\binom{5f}{2f} \equiv \alpha\binom{9f}{4f}\Big/\binom{8f}{4f}$$
$$\equiv (-1)^{[2g/5]}\alpha^3 5^{(p-1)/3} \pmod{p}.$$

PROOF. Theorem 18.4 follows immediately from Theorems 18.2 and 18.3 as

$$\binom{6f}{f}\Big/\binom{2f}{f} = \binom{7f}{2f}\Big/\binom{7f}{f}, \qquad \binom{8f}{3f}\Big/\binom{8f}{f} = \binom{7f}{2f}\Big/\binom{3f}{f},$$
$$\binom{4f}{2f}\Big/\binom{5f}{2f} = \binom{7f}{2f}\Big/\binom{7f}{3f}$$

and, making use of (2.2),

$$\binom{9f}{4f}\Big/\binom{8f}{4f} \equiv (-1)^f\binom{7f}{f}\Big/\binom{5f}{f} = \binom{7f}{f}\Big/\binom{5f}{f}$$

as f is even.

An explicit determination of the 8 binomial coefficients in Theorem 18.4 appears to require the quadratic form discussed on p. 198 of [**10**]. An easy computation shows that each of these binomial coefficients may be determined given an explicit determination for any one of them. The following theorem provides a determination of $\binom{5f}{2f}$ which involves only the forms $p = g^2 + 15h^2$, $4p = A^2 + 27B^2$, and $16p = x^2 + 50u^2 + 50v^2 + 125w^2$, $x \equiv 1 \pmod 5$, $xw = v^2 - 4uv - u^2$; this determination has a sign ambiguity in the form of a square root.

THEOREM 18.5. *Let* $p = 15f + 1 = g^2 + 15h^2$, $4p + A^2 + 27B^2$, $A \equiv g \equiv 1 \pmod 3$, *and let* (x, u, v, w) *be the unique solution of* (18.5) *which is a solution of* (18.3). *Then we have*

$$\binom{5f}{2f} \equiv \begin{cases} (-2g\alpha(x, -v, u, -w)\gamma_-\gamma_+/A)^{1/2} & \text{if } AB \equiv 0 \pmod 5, \\ (-2g\alpha(x, -v, u, -w)\gamma_-(A + 9B)\gamma_+/(A^2 - 9AB))^{1/2} & \\ \qquad \text{if } A \equiv B \text{ or } -2B \pmod 5, & \\ (-2g\alpha(x, -v, u, -w)\gamma_-(A - 9B)\gamma_+/(A^2 + 9AB))^{1/2} & \\ \qquad \text{if } A \equiv -B \text{ or } 2B \pmod 5, & \end{cases}$$

where

$$\gamma_+ = \gamma_+(x, u, v, w) = -x/2 + w(x^2 - 125w^2)/8(xw + 5uv),$$
$$\gamma_- = \gamma_-(x, u, v, w) = -x/2 - w(x^2 - 125w^2)/8(xw + 5uv).$$

PROOF. We have

$$\binom{8f}{3f}\Big/\binom{6f}{3f} \equiv \binom{8f}{2f}\Big/\binom{5f}{2f}, \quad \binom{8f}{3f}\Big/\binom{10f}{5f} \equiv \binom{5f}{2f}\Big/\binom{7f}{2f} \pmod{p}$$

from which it follows

$$\binom{5f}{2f}^2 \equiv \binom{8f}{2f}\binom{7f}{2f}\binom{6f}{3f}\Big/\binom{10f}{5f} \pmod{p}.$$

Hence Theorem 18.5 follows from Theorem 6.1, (18.2), Theorem 8.1, and Theorem 18.2.

EXAMPLE. Let $p = 661$ so that we may take $(x, u, v, w) = (1, 3, 0, -9)$, $-2g = 22$, $A = 49 \equiv -6 \equiv -2B \pmod 5$, and $(A + 9B)/(A - 9B) \equiv 364 \pmod{661}$. Then

$$\gamma_+ = -\frac{1}{2} + \frac{-9(1 - 125(81))}{8(-9)} = \frac{-1 + 113}{2} = 56, \qquad \gamma_- = \frac{-1 - 113}{2} = -57.$$

As $\alpha = 1$, Theorem 18.5 gives

$$\binom{5f}{2f} \equiv \sqrt{(22)(604)(364)(56)/49} \equiv \sqrt{\frac{-5}{7}} \pmod{661}.$$

Computer data gives

$$\binom{220}{88} \equiv 325 \pmod{661},$$

which clearly is in agreement as $((325)(7))^2 \equiv -5 \pmod{661}$.

19. $e = 16$. There are 16 representative binomial coefficients of order 16, namely,

$$\binom{2f}{f}, \binom{3f}{f}, \binom{4f}{f}, \binom{5f}{f}, \binom{5f}{2f}, \binom{6f}{f}, \binom{6f}{3f}, \binom{7f}{f},$$
$$\binom{7f}{2f}, \binom{7f}{3f}, \binom{8f}{f}, \binom{8f}{3f}, \binom{9f}{2f}, \binom{9f}{3f}, \binom{9f}{4f}, \binom{10f}{5f}.$$

We begin by noting the following congruences between binomial coefficients of lower order; these are immediate consequences of (11.1), (11.3), and (11.4) respectively. Throughout this section $p = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$.

$$\binom{6f}{2f} \equiv (-1)^{b/4}\binom{8f}{4f} \pmod{p}, \tag{19.1}$$

$$\binom{10f}{4f} \equiv (-1)^{b/4}\binom{8f}{2f} \pmod{p}, \tag{19.2}$$

$$\binom{4f}{2f} \equiv (-1)^{b/4}\binom{8f}{2f} \pmod{p}. \tag{19.3}$$

Two of the above 16 binomial coefficients may be related to the lower order binomial coefficients $\binom{8f}{2f}$ and $\binom{4f}{2f}$ as follows:

$$\binom{7f}{f} \equiv (-1)^f 2^{(p-1)/8}\binom{8f}{2f} \pmod{p}, \tag{19.4}$$

$$\binom{5f}{2f} \equiv (-1)^f 2^{(p-1)/8} \binom{4f}{2f} \pmod{p}. \tag{19.5}$$

The first congruence is an immediate consequence of Theorem 4.1. To prove (19.5) note first that from (3.11) we have

$$(2^{(p-1)/8})^3 \equiv \frac{6f!\,8f!\,3f!}{3f!\,11f!\,3f!} \equiv \binom{6f}{3f} \Big/ \binom{11f}{3f} \pmod{p}. \tag{19.6}$$

Next, using (2.6) with $g = 11$, $h = 3$, $k = 6$, we have

$$\binom{11f}{3f}\binom{5f}{3f} \equiv (-1)^f \binom{6f}{3f}\binom{10f}{2f} \pmod{p}.$$

By (19.3) and (2.2) we have

$$\binom{8f}{2f} \equiv (-1)^{b/4}\binom{4f}{2f} \quad \text{and} \quad \binom{10f}{2f} \equiv \binom{8f}{2f}$$

from which (19.5) follows immediately as $2^{(p-1)/4} \equiv (-1)^{b/4} \pmod{p}$.

Now as $2^{(p-1)/8} \equiv +1$ or -1 modulo p according as $b \equiv 0 \pmod{16}$ or $b \equiv 8 \pmod{16}$, we have the following theorem analogous to Theorem 11.2.

THEOREM 19.1. *Let* $p = 16f + 1 = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$, *be a prime for which* $b \equiv 0 \pmod 8$. *Then*

$$(-1)^f \binom{7f}{f} \equiv (-1)^f \binom{5f}{2f} \equiv 2c \text{ or } -2c \pmod{p}$$

according as $b \equiv 0 \pmod{16}$ *or* $b \equiv 8 \pmod{16}$.

When $b \not\equiv 0 \pmod 8$ we can use [**23**, (50), p. 70] to obtain

THEOREM 19.2. *Let* $p = 16f + 1 = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$, *be a prime for which* $b \not\equiv 0 \pmod 8$. *Then*

$$\binom{7f}{f} \equiv -\binom{5f}{2f} \equiv \frac{2bc}{a} \text{ or } \frac{-2bc}{a} \pmod{p}$$

according as $b \equiv 4 \pmod{16}$ *or* $b \equiv 12 \pmod{16}$.

Next, we establish 8 congruences which show that each of the remaining 14 representative binomial coefficients of order 16 are related to at least one other by the quantity $2^{(p-1)/8}$. All such interrelationships are easily deducible from these 8 congruences. We first establish 8 congruences which relate

$$\binom{2f}{f}, \binom{9f}{2f}, \binom{6f}{3f}, \quad \text{and} \quad \binom{10f}{5f}$$

to either $\binom{8f}{f}$ or $\binom{8f}{3f}$, since for these two binomial coefficients we will give an explicit determination in terms of the system given in [**14**] (see also [**26**, p. 366]).

$$\binom{2f}{f} \equiv (-1)^f 2^{(p-1)/8} \binom{8f}{f} \pmod{p}, \tag{19.7}$$

$$\binom{9f}{2f} \equiv (2^{(p-1)/8})^3 \binom{8f}{f} \pmod{p}, \tag{19.8}$$

$$\binom{6f}{3f} \equiv (-1)^f (2^{(p-1)/8})^3 \binom{8f}{3f} \pmod{p}, \tag{19.9}$$

$$\binom{10f}{5f} \equiv (-1)^f 2^{(p-1)/8} \binom{8f}{3f} \pmod{p}. \tag{19.10}$$

To prove (19.7) we use (19.4), (2.2), and (2.6). Taking $g = 14$, $h = 8$, $k = 9$, in (2.6) we have

$$\binom{14f}{8f}\binom{2f}{f} \equiv (-1)^f \binom{9f}{f}\binom{7f}{f} \pmod{p}.$$

Since

$$\binom{14f}{8f} \equiv \binom{8f}{2f} \pmod{p} \quad \text{and} \quad \binom{9f}{f} \equiv (-1)^f \binom{8f}{f} \pmod{p},$$

by (2.2), the result follows at once from (19.4). Next taking $g = 7$, $h = 1$, $k = 8$, in (2.6) we have

$$\binom{7f}{f}\binom{9f}{2f} \equiv (-1)^f \binom{8f}{f}\binom{8f}{2f} \pmod{p}$$

so (19.9) follows from (19.4).

Now (19.9) is immediate from (19.6) as

$$\binom{8f}{3f} \equiv (-1)^f \binom{11f}{3f} \pmod{p}$$

by (2.2). Next, taking $g = 8$, $h = 3$, $k = 6$ in (2.6) we have

$$\binom{8f}{3f}\binom{8f}{3f} \equiv \binom{6f}{3f}\binom{10f}{5f}$$

so (19.10) follows from (19.9).

Similarly, we may establish the following congruences:

$$\binom{9f}{4f} \equiv 2^{(p-1)/8} \binom{6f}{f} \pmod{p}, \tag{19.11}$$

$$\binom{9f}{3f} \equiv 2^{(p-1)/8} \binom{4f}{f} \pmod{p}, \tag{19.12}$$

$$\binom{7f}{3f} \equiv (-1)^f 2^{(p-1)/8} \binom{7f}{2f} \pmod{p}, \tag{19.13}$$

$$\binom{5f}{f} \equiv (-1)^f 2^{(p-1)/8} \binom{3f}{f} \pmod{p}. \tag{19.14}$$

Taking $g = 7$, $h = 6$, $k = 10$, in (2.6), we have

$$\binom{7f}{6f}\binom{9f}{4f} \equiv (-1)^f \binom{10f}{6f}\binom{6f}{f} \pmod{p}.$$

However,

$$\binom{10f}{6f} \equiv (-1)^{b/4}\binom{8f}{2f} \pmod{p}$$

by (19.2) so (19.11) follows from (19.4).

Taking $g = 6$, $h = 1$, $k = 4$, in (2.6) we have

$$\binom{6f}{f}\binom{10f}{3f} \equiv \binom{4f}{f}\binom{12f}{5f} \pmod{p}$$

so (19.12) is an immediate consequence of (19.11), noting that

$$\binom{10f}{3f} \equiv (-1)^f\binom{9f}{3f} \pmod{p} \quad \text{and} \quad \binom{12f}{5f} \equiv (-1)^f\binom{9f}{4f} \pmod{p}$$

by (2.2).

Taking $g = 11$, $h = 9$, $k = 12$ in (2.6) we have

$$\binom{11f}{9f}\binom{5f}{3f} \equiv (-1)^f\binom{12f}{9f}\binom{4f}{2f} \pmod{p}$$

so (19.13) follows from (19.5), noting that

$$\binom{11f}{9f} \equiv \binom{7f}{2f} \pmod{p} \quad \text{and} \quad \binom{12f}{9f} \equiv (-1)^f\binom{7f}{3f} \pmod{p}$$

by (2.2).

Finally, taking $g = 13$, $h = 11$, $k = 12$, in (2.6) we have

$$\binom{13f}{11f}\binom{3f}{f} \equiv (-1)^f\binom{12f}{11f}\binom{4f}{2f} \pmod{p}$$

so (19.14) also follows from (19.5), noting that

$$\binom{13f}{11f} \equiv (-1)^f\binom{5f}{2f} \pmod{p} \quad \text{and} \quad \binom{12f}{11f} \equiv (-1)^f\binom{5f}{f} \pmod{p}$$

by (2.2).

Before proceeding to our determination of $\binom{8f}{f}$ and $\binom{8f}{3f}$ we wish to note that all congruences between representative binomial coefficients of order 16 of Cauchy-Whiteman type (see [**17**], (1.6), and §21) are readily deduced from the above congruences. Computer data shows that the only such congruences are

$$\binom{10f}{5f} \equiv (-1)^{b/4}\binom{6f}{3f} \pmod{p}, \tag{19.15}$$

$$\binom{2f}{f} \equiv (-1)^{f+b/4}\binom{9f}{2f} \pmod{p}, \tag{19.16}$$

$$\binom{7f}{f} \equiv (-1)^{b/4}\binom{5f}{2f} \pmod{p}. \tag{19.17}$$

From (19.9) and (19.10) we have at once (19.15), and from (19.7) and (19.8) we have (19.16). Finally, (19.17) follows from (19.3)–(19.5).

Now, appealing to (2.2) and Theorem 5.1, we have

$$J_{16}(15,9) \equiv -\binom{8f}{f} \pmod{\pi},$$

where π is a prime ideal divisor of p in $Q(\zeta_{16})$,

$$p = x^2 + 2u^2 + 2v^2 + 2w^2, \qquad 2xv = u^2 - 2uw - w^2, \tag{19.18}$$

$x \equiv 1 \pmod 8$, $u \equiv v \equiv w \equiv 0 \pmod 2$. For the duration of this section we let $\zeta = \zeta_{16}$.

From (3.5) and [**43**, p. 405] one obtains

$$J_{16}(15,9) = (-1)^f\left[-x - v(\zeta^2 - \zeta^6) - u(\zeta + \zeta^7) - w(\zeta^3 + \zeta^5)\right].$$

It is easy to see from [**26**] (see, e.g., [**18**, (3.20)] with $x \equiv -1 \pmod 8$) that

$$-x - v(\zeta^2 - \zeta^6) + u(\zeta + \zeta^7) + w(\zeta^3 + \zeta^5) \equiv 0 \pmod{\pi} \tag{19.19}$$

and

$$2v^2 - x^2 \equiv (u^2 - w^2 + 2uw)(\zeta^2 - \zeta^6) \pmod{\pi}. \tag{19.20}$$

Thus

$$\begin{aligned}\binom{8f}{f} &\equiv -J_{16}(15,9) \equiv 2(-1)^{f+1}\{-x - v(\zeta^2 - \zeta^6)\} \pmod{\pi} \\ &\equiv 2(-1)^f\{x - v(x^2 - 2v^2)/(u^2 - w^2 + 2uw)\} \pmod{\pi}.\end{aligned} \tag{19.21}$$

As the expressions on the left and right of (19.21) are rational integers, the congruence holds (mod p).

Similarly (mapping $\theta \to \theta^3$) we have

$$J_{16}(13,11) = (-1)^f\{-x + v(\zeta^2 - \zeta^6) - u(\zeta^3 + \zeta^5) + w(\zeta + \zeta^7)\}.$$

Moreover, (19.19) becomes

$$-x + v(\zeta^2 - \zeta^6) - u(\zeta^3 + \zeta^5) + w(\zeta + \zeta^7) \equiv 0 \pmod{\pi}. \tag{19.22}$$

As

$$J_{16}(13,11) \equiv -\binom{8f}{3f} \pmod{\pi}$$

from Theorem 5.1 we have

$$\begin{aligned}\binom{8f}{3f} &\equiv -J_{16}(13,11) \equiv 2(-1)^{f+1}\{-x + v(\zeta^2 - \zeta^6)\} \pmod{\pi} \\ &\equiv 2(-1)^f\{x + v(x^2 - 2v^2)/(u^2 - w^2 + 2uw)\} \pmod{\pi},\end{aligned} \tag{19.23}$$

so, as before, this congruence holds (mod p).

Combining (19.7)–(19.10), (19.21), and (19.23) we have

THEOREM 19.3. *Let* $p = 16f + 1 = a^2 + b^2 = x^2 + 2u^2 + 2v^2 + 2w^2$, $2xv = u^2 - 2uw - w^2$, *with signs chosen so that* $a \equiv 1 \pmod 4$, $x \equiv 1 \pmod 8$, *and* $u \equiv v \equiv w \equiv 0 \pmod 2$. *Then we have*

$$(-1)^f\theta\binom{8f}{f} \equiv \binom{2f}{f} \equiv 2\theta\left\{x - \frac{v(x^2 - 2v^2)}{u^2 - w^2 + 2uw}\right\} \equiv (-1)^f\theta^2\binom{9f}{2f} \pmod p$$

and

$$(-1)^f\theta\binom{8f}{3f} \equiv \binom{10f}{5f} \equiv 2\theta\left\{x + \frac{v(x^2 - 2v^2)}{u^2 - w^2 + 2uw}\right\} \equiv \theta^2\binom{6f}{3f} \pmod p$$

where $\theta \equiv +1, -b/a, -1,$ *or* $+b/a \pmod p$ *according as* $b \equiv 0, 4, 8$ *or* $12 \pmod{16}$.

EXAMPLE. For $p = 113$, $f = 7$, $b = 8$, $(x, u, v, w) = (1, -6, 4, -2)$. In agreement with Theorem 19.3 we have

$$\binom{8f}{f} \equiv \binom{2f}{f} \equiv -\binom{9f}{2f} \equiv 42 \pmod{113}, \quad -2\left(1 - \frac{4(-31)}{56}\right) \equiv 42 \pmod{113},$$

$$\binom{8f}{3f} \equiv \binom{10f}{5f} \equiv \binom{6f}{3f} \equiv 67 \pmod{113}, \quad -2\left(1 - \frac{4(-31)}{56}\right) \equiv 67 \pmod{113}.$$

The remaining 8 representative binomial coefficients of order 16 we are only able to determine up to sign. Let

$$\delta_1 = \delta_1(x, u, v, w) = 2(-1)^f\{x - v(x^2 - 2v^2)/(u^2 - w^2 + 2uw)\},$$

$$\delta_2 = \delta_2(x, u, v, w) = 2(-1)^f\{x + v(x^2 - 2v^2)/(u^2 - w^2 + 2uw)\}.$$

Then we have

THEOREM 19.4. *Let* $p = 16f + 1 = a^2 + b^2 = c^2 + 2d^2 = x^2 + 2u^2 + 2v^2 + 2w^2$, $2xv = u^2 - 2uw - w^2$, *with signs chosen so that* $a \equiv c \equiv 1 \pmod 4$, $x \equiv 1 \pmod 8$, $u \equiv v \equiv w \equiv 0 \pmod 2$. *Then we have the following congruences* (mod p):

$$\binom{7f}{2f} \equiv \left((-1)^{b/4}4ac\frac{\delta_2}{\delta_1}\right)^{1/2}, \qquad \binom{7f}{3f} \equiv \left(4ac\frac{\delta_2}{\delta_1}\right)^{1/2},$$

$$\binom{3f}{f} \equiv \left((-1)^{b/4}4ac\frac{\delta_1}{\delta_2}\right)^{1/2}, \qquad \binom{5f}{f} \equiv \left(4ac\frac{\delta_1}{\delta_2}\right)^{1/2},$$

$$\binom{4f}{f} \equiv \left(\delta_1\delta_2\frac{c}{a}\right)^{1/2}, \quad \binom{9f}{4f} \equiv \left(\delta_1\delta_2\frac{a}{c}\right)^{1/2}, \quad \binom{9f}{3f} \equiv \left((-1)^{b/4}\delta_1\delta_2\frac{c}{a}\right)^{1/2},$$

$$\binom{6f}{f} \equiv \left((-1)^{b/4}\delta_1\delta_2\frac{a}{c}\right)^{1/2}.$$

PROOF. In view of (19.11)–(19.14) it suffices to prove the congruences for

$$\binom{7f}{2f}, \binom{3f}{f}, \binom{4f}{f}, \text{ and } \binom{6f}{f}.$$

To prove the congruences for $\binom{7f}{2f}$ and $\binom{3f}{f}$ we note that

$$\binom{3f}{f}\binom{8f}{3f} = \binom{7f}{2f}\binom{8f}{f}, \qquad \binom{3f}{f}\binom{7f}{3f} = \binom{7f}{f}\binom{6f}{2f},$$

and

$$\binom{7f}{2f}\binom{5f}{f} = \binom{6f}{2f}\binom{7f}{f},$$

so that appealing to Theorem 11.1, (19.4), (19.13), (19.14) and Theorem 11.2 we have (mod p throughout)

$$\begin{aligned}\binom{7f}{2f}^2 &\equiv \binom{6f}{2f}\binom{7f}{f}\binom{8f}{3f}\binom{3f}{f}\Big/\binom{5f}{f}\binom{8f}{f}\\ &\equiv (-1)^{b/4}2a(2^{(p-1)/8})(2c\delta_2)(2^{(p-1)/8})^3/\delta_1,\end{aligned}$$

and

$$\begin{aligned}\binom{3f}{f}^2 &\equiv \binom{7f}{f}\binom{6f}{2f}\binom{7f}{2f}\binom{8f}{f}\Big/\binom{7f}{3f}\binom{8f}{3f}\\ &\equiv (-1)^f 2^{(p-1)/8}2c(-1)^{b/4}2a(-1)^f(2^{(p-1)/8})^3\delta_1/\delta_2.\end{aligned}$$

To prove the congruences for $\binom{4f}{f}$ and $\binom{6f}{f}$ we use Lemma 2.2 and (19.12) to see that

$$\binom{4f}{f}\binom{6f}{f} \equiv \frac{(-1)^f\delta_1\delta_2}{2^{(p-1)/8}} \tag{19.24}$$

and we use (19.5) and Theorems 11.1 and 11.2 to see that

$$\begin{aligned}\binom{4f}{f}\Big/\binom{6f}{f} &= \binom{5f}{2f}\Big/\binom{6f}{2f} \qquad (19.25)\\ &\equiv \frac{(-1)^f 2^{(p-1)/8}(-1)^{b/4}2c}{(-1)^{b/4}2a} = (-1)^f 2^{(p-1)/8}\frac{c}{a}.\end{aligned}$$

From (19.24) and (19.25) the stated congruences for $\binom{4f}{f}$ and $\binom{6f}{f}$ follow at once.

The next theorem taken in conjunction with (19.11)–(19.14) shows that a correct sign determination for one of the congruences in Theorem 19.4 suffices to fix the sign for the remaining seven.

THEOREM 19.5. *Let* $p = 16f + 1 = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$. *Then we have*

$$\binom{5f}{f}\binom{7f}{3f} \equiv 4ac \pmod p, \qquad \binom{4f}{f}\Big/\binom{9f}{4f} \equiv (-1)^f\frac{c}{a} \pmod p.$$

PROOF. The first congruence in Theorem 19.5 follows by combining (19.13) and

$$\binom{5f}{f}\binom{7f}{2f} = \binom{6f}{2f}\binom{7f}{f} \equiv (-1)^f 4ac(2^{(p-1)/8})^3 \pmod p$$

(see (19.4), Theorems 11.1, 11.2). The second congruence follows at once from (19.11) and (19.25).

We close this section by noting that results similar to Theorem 19.1 may be deduced for $e = 32$ and $e = 64$, making use of the system given by (19.18), as $2^{(p-1)/16}$ and $2^{(p-1)/32}$ have recently been determined (see Evans [**12**] and Hudson and Williams [**18**]) in terms of the parameters in this system and those in Theorem 19.1.

20. $e = 20$. For $p = 20f + 1$ there are 24 representative binomial coefficients of order 20 and 9 lower order representatives. We begin this section by showing that 10 of the 33 binomial coefficients of order 20 may be expressed in terms of the parameters in the representations $p = a^2 + b^2 = e^2 + 5f^2$, $a \equiv 1 \pmod 4$. In [**45**, Theorem 3] Whiteman proved that for $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$, $a \equiv 1 \pmod 4$, we have

$$\binom{10f}{f}\binom{10f}{3f} \equiv 4e^2 \pmod p, \tag{20.1}$$

and according as $b \not\equiv 0 \pmod 5$ or $b \equiv 0 \pmod 5$,

$$\binom{10f}{f} \equiv \binom{10f}{3f} \text{ or } -\binom{10f}{3f} \pmod p, \tag{20.2}$$

resolving the ambiguity in the congruence of Cauchy [**5**, p. 37]. If $b \not\equiv 0 \pmod 5$ then (as the sign of a is determined by the condition $a \equiv 1 \pmod 4$) Whiteman showed that e may be expressed unambiguously by the condition $e \equiv a \pmod 5$, so for $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$, $b \equiv 0 \pmod 5$, we have

$$\binom{10f}{f} \equiv \binom{10f}{3f} \equiv 2e \pmod p \qquad (a \equiv 1 \pmod 4,\ e \equiv a \pmod 5). \tag{20.3}$$

The sign of b is not fixed. However, comparing formulas (4.7) and (4.13) of [**45**] one sees readily that e may be expressed unambiguously by the condition $e \equiv |b| \pmod 5$. (Set $e = (-1)^f b'$ (where b' denotes Whiteman's b) when $5 \mid b$; the determination in (20.4) requires choosing a primitive root g with $g^{5f} = a/|b| \pmod p$.) Then from [**45**, Theorem 3] we have, for $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$, $b \not\equiv 0 \pmod 5$,

$$\binom{10f}{f} \equiv -\binom{10f}{3f} \equiv \frac{2ea}{|b|} \pmod p. \tag{20.4}$$

Let $\beta = 2^{(p-1)/10}$. We show in the next two theorems that 8 representative binomial coefficients are related to $\binom{10f}{f}$ and $\binom{10f}{3f}$ by powers of β.

THEOREM 20.1. *Let $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$ be a prime with the signs of a and e chosen so that $a \equiv 1 \pmod 4$, $e \equiv a \pmod 5$, if $b \equiv 0 \pmod 5$ and $e \equiv |b| \pmod 5$ if $a \equiv 0 \pmod 5$. Then we have the following congruences modulo p:*

$$\binom{2f}{f} \equiv (-1)^f 2e\beta \quad \text{or} \quad (-1)^f \frac{2ea\beta}{|b|},$$

$$\binom{13f}{6f} \equiv (-1)^f 2e\beta^2 \quad or \quad (-1)^{f+1}\frac{2ea\beta^2}{|b|},$$

$$\binom{6f}{3f} \equiv (-1)^f 2e\beta^3 \quad or \quad (-1)^{f+1}\frac{2ea\beta^3}{|b|},$$

$$\binom{11f}{2f} \equiv (-1)^f 2e\beta^4 \quad or \quad (-1)^f\frac{2ea\beta^4}{|b|},$$

according as $b \equiv 0 \pmod 5$ *or* $a \equiv 0 \pmod 5$.

PROOF. For the duration of this section all congruences are interpreted modulo $p = 20f + 1$ unless otherwise stated. By (3.11) and (2.2) we have

$$2^{(p-1)/10} \equiv \frac{2f!\,10f!\,f!}{f!\,11f!\,f!} \equiv \binom{2f}{f} \Big/ \binom{11f}{f} \equiv (-1)^f \binom{2f}{f} \Big/ \binom{10f}{f}, \tag{20.5}$$

so the first congruence in Theorem 20.1 follows at once from (20.3) and (20.4).

Next we have

$$(2^{(p-1)/10})^3 \equiv \frac{6f!\,10f!\,7f!}{3f!\,13f!\,7f!} \equiv \binom{10}{3f} \Big/ \binom{13f}{6f}, \tag{20.6}$$

and the second congruence follows as above, noting that $\beta^{-3} \equiv (-1)^f\beta^2$ as $(2/p) = +1 \Rightarrow p \equiv 1 \pmod 8 \Rightarrow f \equiv 0 \pmod 2$.

Similarly,

$$(2^{(p-1)/10})^3 \equiv \frac{6f!\,10f!\,3f!}{3f!\,13f!\,3f!} \equiv \binom{6f}{3f} \Big/ \binom{13f}{3f} \equiv (-1)^f \binom{6f}{3f} \Big/ \binom{10f}{3f}, \tag{20.7}$$

yielding the third congruence in Theorem 20.1, and

$$2^{(p-1)/10} \equiv \frac{2f!\,10f!\,9f!}{f!\,11f!\,9f!} \equiv \binom{10f}{f} \Big/ \binom{11f}{2f}, \tag{20.8}$$

completing the proof of Theorem 20.1.

EXAMPLE. Let $p = 241 = 14^2 + 5(3)^2$. Note that $f = 12$, $2^{(p-1)/5} \equiv 1 \pmod p$, $2ea/|b| \equiv 136 \pmod{241}$. In agreement with Theorem 20.1 we have

$$\binom{24}{12} \equiv -\binom{72}{36} \equiv \binom{132}{34} \equiv -\binom{156}{72} \equiv 136 \pmod{241}.$$

THEOREM 20.2. *Let* $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$ *be a prime with the signs of* a *and* e *chosen so that* $a \equiv 1 \pmod 4$, $e \equiv a \pmod 5$ *if* $b \equiv 0 \pmod 5$ *and* $e \equiv |b| \pmod 5$ *if* $a \equiv 0 \pmod 5$. *Then we have the following congruences modulo* p:

$$\binom{4f}{f} \equiv (-1)^{[2e/5]} 2e\beta, \qquad \binom{8f}{f} \equiv (-1)^{f+[2e/5]} 2e\beta^2,$$

$$\binom{11f}{3f} \equiv (-1)^{f+[2e/5]} 2e\beta^3, \qquad \binom{11f}{4f} \equiv (-1)^{[2e/5]} 2e\beta^4.$$

PROOF. To prove the first congruence in Theorem 20.2 we need to show that

$$\binom{4f}{f}\Big/\binom{2f}{f} \equiv (-1)^{f+[2e/5]} \quad \text{or} \quad (-1)^{f+[2e/5]}\frac{|b|}{a} \pmod{p} \tag{20.9}$$

according as $b \equiv 0 \pmod 5$, $e \equiv a \pmod 5$, or $a \equiv 0 \pmod 5$, $e \equiv |b| \pmod 5$.

The Jacobi sums $J_{20}(1, 1)$ and $J_{20}(1, 3)$ are related by (see [**31**, Lemma 3])

$$uJ_{20}(1,1) = J_{20}(1,3), \tag{20.10}$$

so by Lemma 6 of [**45**] we must have

$$\binom{4f}{f}\Big/\binom{2f}{f} \equiv \bar{u} \pmod{p}. \tag{20.11}$$

Clearly $(-1)^{[2e/5]} = +1$ if $e \equiv 1 \pmod 5$ and $(-1)^{[2e/5]} = -1$ if $e \equiv 4 \pmod 5$. We now use Lemma 4 of [**31**]. As $e \equiv a \pmod 5$ if $b \equiv 0 \pmod 5$, we have

$$(-1)^f \bar{u} \equiv \begin{cases} +1 & \text{if } e \equiv 1 \pmod 5, \\ -1 & \text{if } e \equiv 4 \pmod 5 \end{cases}$$

($(-1)^f$ arising from $a \equiv \pm(-1)^f \pmod 5$ in Lemma 4). Moreover, with $\beta^5 = g^{5f} \equiv a/|b| \pmod p$, $a \equiv 0 \pmod 5$, we have

$$(-1)^f \bar{u} \equiv \begin{cases} |b|/a & \text{if } e \equiv 1 \pmod 5, \\ a/|b| & \text{if } e \equiv 4 \pmod 5. \end{cases}$$

To prove the second congruence in Theorem 20.2 we first use (3.11) and (2.2) to obtain

$$(2^{(p-1)/10})^4 \equiv \frac{8f!\,10f!\,4f!}{4f!\,14f!\,4f!} \equiv \binom{8f}{4f}\Big/\binom{14f}{4f} \equiv \binom{8f}{4f}\Big/\binom{10f}{4f}. \tag{20.12}$$

Next from Theorem 20.1, (20.3), and (20.4) we have

$$\binom{6f}{3f}\Big/\binom{10f}{3f} \equiv (-1)^f (2^{(p-1)/10})^3. \tag{20.13}$$

Now we have

$$\frac{8f!}{f!\,7f!}\,\frac{f!\,3f!}{4f!}\,\frac{6f!}{3f!\,3f!}\,\frac{3f!\,7f!}{10f!} = \binom{8f}{4f}\Big/\binom{10f}{4f}, \tag{20.14}$$

so

$$\binom{8f}{f}\Big/\binom{4f}{f} \equiv \frac{(2^{(P-1)/10})^4}{(-1)^f (2^{(p-1)/10})^3} = (-1)^f 2^{(p-1)/10}, \tag{20.15}$$

proving the second congruence in Theorem 20.2.

Next using (3.11), (2.1) and (2.2) we have

$$(2^{(p-1)/10})^2 \equiv \frac{4f!\,10f!}{2f!\,12f!} \equiv \frac{4f!\,8f!\,6f!}{2f!\,10f!\,6f!} \equiv \binom{8f}{2f}\Big/\binom{10f}{4f}. \tag{20.16}$$

From Theorem 20.1, (20.3) and (20.4) we have

$$\binom{11f}{2f}\Big/\binom{10f}{f} \equiv (-1)^f (2^{(p-1)/10})^4 \equiv \binom{11f}{3f}\binom{8f}{2f}9f!\Big/\binom{4f}{f}\binom{10f}{4f}9f!, \tag{20.17}$$

so

$$\binom{11f}{3f}\Big/\binom{4f}{f} \equiv (-1)^f (2^{(p-1)/10})^2, \tag{20.18}$$

proving the third congruence in Theorem 20.2.

Finally, we have

$$\frac{11f!}{4f!7f!}\cdot\frac{f!7f!}{8f!}\,\frac{8f!}{2f!6f!}\,\frac{4f!6f!}{10f!} = \binom{11f}{2f}\Big/\binom{10f}{f} \tag{20.19}$$

so from (20.16) and (20.17) we deduce that

$$\binom{11f}{4f}\Big/\binom{8f}{f} = (-1)^f (2^{(p-1)/10})^2, \tag{20.20}$$

completing the proof of Theorem 20.2.

Let (x, u, v, w) be a solution of

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2, \quad x \equiv 1 \pmod 5, \qquad xw = v^2 - 4uv - u^2. \tag{20.21}$$

EXAMPLE. Let $p = 3121$ so $f \equiv 0 \pmod 2$, $2^{(p-1)/5} = +1$, $a = -39$, $b = 40 \equiv 0 \pmod 5$, and $e = -49 \equiv a \equiv 1 \pmod 5$. We have

$$\binom{10f}{f} \equiv \binom{10f}{3f} \equiv \binom{2f}{f} \equiv \binom{6f}{3f} \equiv \binom{11f}{2f} \equiv \binom{13f}{6f} \equiv \binom{4f}{f} \equiv \binom{8f}{f} \equiv \binom{11f}{3f} \equiv \binom{11f}{4f} \equiv -98 \pmod{3121}. \tag{20.22}$$

Resolving the sign ambiguity in Cauchy's congruence (see (20.2)) involves showing that $\binom{10f}{f}$ and $\binom{10f}{3f}$ differ multiplicatively by $5^{(p-1)/4} \equiv \pm 1 \pmod p$. The congruences in the following Theorem are related by a fourth root of unity, u, which does not arise from any expression of the form $(n^{(p-1)/m})^t$, $e = mn$, $t \geqslant 1$. Thus Muskat's and Whiteman's determination of u in Lemma 3 of [**31**] is an important and valuable result. In our notation this determination takes the form

$$u = \begin{cases} (-1)^{f+[2e/5]} & \text{if } b \equiv 0 \pmod 5, \\ (-1)^{f+[2e/5]} a/|b| & \text{if } a \equiv 0 \pmod 5. \end{cases} \tag{20.24}$$

THEOREM 20.3. *Let* $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$ *be a prime with the signs of* a *and* e *chosen so that* $a \equiv 1 \pmod 4$, $e \equiv a \pmod 5$ *if* $b \equiv 0 \pmod 5$ *and* $e \equiv |b| \pmod 5$ *if* $a \equiv 0 \pmod 5$. *Then we have*

$$\begin{aligned}\binom{2f}{f}\Big/\binom{4f}{f} &\equiv \binom{11f}{2f}\Big/\binom{11f}{4f} \equiv (-1)^f\binom{8f}{f}\Big/\binom{13f}{6f}\\ &\equiv (-1)^f\binom{11f}{3f}\Big/\binom{6f}{3f} \equiv \binom{3f}{f}\Big/\binom{4f}{2f} \equiv \binom{5f}{f}\Big/\binom{5f}{2f}\\ &\equiv (-1)^f\binom{8f}{3f}\Big/\binom{11f}{5f} \equiv \binom{7f}{2f}\Big/\binom{9f}{4f} \equiv \binom{4f}{2f}\Big/\binom{9f}{2f}\\ &\equiv \binom{12f}{6f}\Big/\binom{9f}{3f} \equiv \binom{7f}{f}\Big/\binom{12f}{6f} \equiv \binom{6f}{f}\Big/\binom{12f}{5f} \equiv u \pmod p.\end{aligned}$$

PROOF. The first four congruences in Theorem 20.3 are an immediate consequence of Theorems 20.1 and 20.2. The next two congruences follow from the first as

(20.25)

$$\binom{3f}{f}f!\Big/\binom{4f}{2f}f! = \binom{2f}{f}\Big/\binom{4f}{f} = \binom{3f}{f}5f!\Big/\binom{4f}{2f}5f! = \binom{5f}{f}\Big/\binom{5f}{2f}.$$

Next we have, using (2.2) and Theorems 20.1, 20.2

(20.26)

$$\begin{aligned}\binom{8f}{3f}3f!\Big/\binom{11f}{5f}3f! &= \binom{6f}{3f}\Big/\binom{11f}{3f} \equiv \binom{8f}{3f}14f!\Big/\binom{11f}{5f}14f!\\ &= \binom{14f}{3f}\Big/\binom{14f}{6f} \equiv (-1)^f\binom{9f}{3f}\Big/\binom{12f}{6f} \equiv (-1)^f\bar{u},\end{aligned}$$

(20.27)

$$\begin{aligned}\binom{7f}{f}13f!\Big/\binom{12f}{6f}13f! &= \binom{13f}{3f}\Big/\binom{13f}{6f} \equiv (-1)^f\binom{8f}{f}\Big/\binom{13f}{6f}\\ &\equiv \binom{7f}{f}5f!\Big/\binom{12f}{6f}5f! \equiv \binom{6f}{f}\Big/\binom{12f}{5f} \equiv u,\end{aligned}$$

(20.28)

$$\binom{7f}{2f}11f!\Big/\binom{9f}{4f}11f! = \binom{11f}{2f}\Big/\binom{11f}{4f} = \binom{9f}{2f}2f!\Big/\binom{7f}{2f}2f! \equiv u,$$

completing the proof of Theorem 20.3.

COROLLARY. *For every prime* $p = 20f + 1$ *we have*

$$\binom{7f}{f}\binom{9f}{3f} \equiv \binom{12}{6f}^2 \pmod p, \quad \binom{3f}{f}\binom{9f}{2f} \equiv \binom{4f}{2f}^2 \pmod p.$$

As $2^{(p-1)/5}$ is given explicitly by (4.13) we have, if $(2/p)_5 \neq 1$

$$\text{(20.29)}\quad \binom{8f}{f} \equiv (-1)^{f+[2e/5]} \cdot \frac{2e(w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v))}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)},$$

$a \equiv 1 \pmod 4$, $e \equiv a \pmod 5$ if $b \equiv 0 \pmod 5$ and $e \equiv |b| \pmod 5$ if $a \equiv 0 \pmod 5$, $u \equiv 0 \pmod 2$, $x + u - v = 0 \pmod 4$. Moreover, we have the following (using the result of Emma Lehmer in formula (48) of [**23**]):

$$\text{(20.30)}\quad \binom{11f}{4f} \equiv (-1)^{[2e/5]} \cdot \frac{2e(w(125w^2 - x^2) - 2(xw + 5uv)(25w + x + 10u + 20v))}{w(125w^2 - x^2) - 2(xw + 5uv)(25w + x - 10u - 20v)}$$

if $(2/p)_5 \neq 1$ ($\Leftrightarrow$ replace (x, u, v, w) by $(x, -v, u, -w)$ on the right-hand side of (20.30)).

EXAMPLE. Let $p = 41$ so $x = -9$, $u = 0$, $v = 3$, $w = -1$, $e = -6$. Then we have

$$\binom{8f}{f} = \binom{16}{2} \equiv 38 \pmod{41}$$

and

$$\binom{8f}{f} \equiv (-1)^{[-12/5]} \frac{-12(-1(125 - 81) + 2(9)(-25 + 9 - 30))}{-1(125 - 81) + 2(9)(-25 + 9 + 30)}$$
$$\equiv 12(-3 + 33)/(-3 + 6) \equiv 38 \pmod{41}.$$

Moreover, we have

$$\binom{11f}{4f} = \binom{22}{8} \equiv 11 \pmod{41}$$

and

$$\binom{11f}{4f} \equiv (-1)^{[-12/5]} \frac{-12(-1(125 - 81)) - 2(9)(-25 - 9 + 60)}{-1(125 - 81) - 2(9)(-25 - 9 - 60)}$$
$$\equiv 12(-3 - 17)/(-3 + 11) \equiv 11 \pmod{41}.$$

Now $\binom{4f}{f} = \binom{8}{2} = 28$ and, replacing (x, u, v, w) by $(x, v, -u, -w)$, we have

$$\binom{4f}{f} \equiv (-1)^{[-12/5]} \frac{-12(125 - 81) + 2(-9)(25 + 9 + 60)}{(125 - 81) + 2(-9)(25 + 9 - 60)}$$
$$\equiv 12(3 - 11)/(3 + 17) \equiv 28 \pmod{41}.$$

Finally we have

$$\binom{11f}{3f} = \binom{22}{6} \equiv 34 \pmod{41}$$

and, replacing (x, u, v, w) by $(x, -u, -v, w)$, we have

$$\begin{aligned}\binom{11f}{3f} &\equiv (-1)^{[-12/5]}\frac{-12(-1(125-81)+2(9)(-25+9+30))}{-1(125-81)+2(9)(-25+9-30)}\\ &\equiv 12(-3+6)/(-3+33) \equiv 34 \pmod{41}.\end{aligned}$$

The binomial coeffcients in the above corollary are of Cauchy-Whiteman type. Moreover it is clear from the above congruences that

$$\binom{7f}{f}, \binom{9f}{3f}, \binom{3f}{f}, \binom{9f}{2f}$$

are expressible in terms of the parameters in (20.21) rather than the parameter e in $p = e^2 + 5f^2$.

Before proceeding to determine the binomial coefficients which may be given explicitly in terms of the system (20.1) we note that the above theorems yield a large number of congruences relating products and/or quotients of representative binomial coefficients (as in (20.1) or in Theorem 14.1) and the parameter e in $p = e^2 + 5f^2$. We cite only a few.

$$\begin{aligned}\binom{10f}{f}\binom{10f}{3f} &\equiv (-1)^f\binom{4f}{f}\binom{11f}{4f}\\ &\equiv (-1)^f\binom{8f}{f}\binom{11f}{3f} \equiv 4e^2 \pmod{p},\end{aligned} \tag{20.31}$$

$$\begin{aligned}\binom{10f}{f}^2 \equiv \binom{10f}{3f}^2 &\equiv (-1)^f\binom{6f}{3f}\binom{13f}{6f}\\ &\equiv (-1)^f\binom{2f}{f}\binom{11f}{2f} \equiv 4e^2 \text{ or } -4e^2 \pmod{p},\end{aligned} \tag{20.32}$$

according as $b \equiv 0 \pmod 5$ or $a \equiv 0 \pmod 5$.

$$\binom{4f}{f}\binom{8f}{f}\Big/\binom{11f}{3f} \equiv (-1)^{[2e/5]}2e \pmod{p}; \tag{20.33}$$

$$\binom{7f}{f}\binom{4f}{f}\Big/\binom{8f}{2f} \equiv 2e \text{ or } 2ea/|b| \pmod{p}, \tag{20.34}$$

according as $b \equiv 0 \pmod 5$ or $a \equiv 0 \pmod 5$.

The congruence (20.32) may be obtained from Theorem 20.2 after noting that

$$\begin{aligned}\binom{8f}{2f}\binom{2f}{f}\Big/\binom{7f}{f} = \binom{8f}{f} &\Rightarrow \binom{7f}{f}\Big/\binom{8f}{2f}\\ &\equiv \binom{2f}{f}\Big/\binom{8f}{f} \equiv u\beta^4 \pmod{p};\end{aligned} \tag{20.35}$$

(20.31), (20.32), and (20.33) are clearly immediate consequences of Theorems 20.1 and 20.2. Also we note in view of Gauss's congruence given in Theorem 7.1 that we have

$$\binom{10f}{f}\binom{10f}{5f} \equiv 2ea \text{ or } -2e|b| \pmod{p} \tag{20.36}$$

according as $b \equiv 0 \pmod 5$ or $a \equiv 0 \pmod 5$.

Apart from $\binom{10f}{5f}$ all 8 lower order binomial coefficients are given explicitly by the congruences in §§8 and 13. We now prove that 6 representative binomial coefficients of order 20 may be given explicitly in terms of the system (20.21).

THEOREM 20.4. *For each prime* $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$, $a \equiv 1 \pmod 4$, *with* (x, u, v, w) *a solution of* (20.21), *set* $\gamma_+(x, u, v, w)$ (*upper signs*) *and* $\gamma_-(x, u, v, w)$ *equal to*

$$\frac{1}{2}\left[-x \pm w(x^2 - 125w^2)/4(xw + 5uv)\right]$$

if $(2/p)_5 = 1$, *and to*

$$\frac{1}{2}\left[\frac{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)}\right] \cdot \left[-x \pm \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right]$$

if 2 *is a quintic nonresidue of* p. *Then with* $e \equiv a \pmod 5$ *if* $b \equiv 0 \pmod 5$, $e \equiv |b| \pmod 5$ *if* $a \equiv 0 \pmod 5$, *with a fixed primitive root* g *such that* $g^{5f} \equiv a/|b| \pmod p$, *and with* $u \equiv 0 \pmod 2$, $x + u - v \equiv 0 \pmod 4$, *we have the following congruences* $(\mathrm{mod}\ p)$.

$$\binom{7f}{3f} \equiv \gamma_+(x, u, v, w)$$

for the solution $(x, -v, u, -w)$ *of* (20.21), *and*

$$\binom{7f}{f} \equiv \pm\binom{9f}{3f} \equiv (-1)^{f+[2e/5]}\gamma_+(x, u, v, w)$$

or

$$(-1)^{f+[2e/5]}(a/|b|)\gamma_+(x, u, v, w)$$

according as $b \equiv 0 \pmod 5$, *in which case the* + *sign holds and* $e \equiv a \pmod 5$, *or* $a \equiv 0 \pmod 5$, *in which case the* − *sign holds and* $e \equiv |b| \pmod 5$.

Moreover, we have

$$\binom{9f}{f} \equiv (-1)^f\gamma_-(x, u, v, w)$$

for the solution $(x, -u, -v, w)$ *of* (20.21), *and*

$$\binom{3f}{f} \equiv \pm\binom{9f}{2f} \equiv (-1)^{f+[2e/5]}\gamma_-(x, u, v, w)$$

or

$$(-1)^{f+[2e/5]}(a/|b|)\gamma_-(x,u,v,w)$$

according as $b \equiv 0 \pmod 5$, *in which case the* + *sign holds and* $e \equiv a \pmod 5$, *or* $a \equiv 0 \pmod 5$, *in which case the* − *sign holds and* $e \equiv |b| \pmod 5$; (x,u,v,w) *is replaced by* $(x,-v,u,-w)$.

PROOF. The first congruence follows directly from Theorem 20.2 noting that

$$\binom{7f}{f}\Big/\binom{8f}{4f} = \frac{7f!\,4f!\,4f!\,11f!}{3f!\,4f!\,8f!\,11f!} = \binom{11f}{3f}\Big/\binom{11f}{4f}.$$

The Cauchy-Whiteman type congruences

$$\binom{7f}{f} \equiv \pm\binom{9f}{3f} \quad \text{and} \quad \binom{3f}{f} \equiv \pm\binom{4f}{2f} \pmod p,$$

holding with the + sign if $b \equiv 0 \pmod 5$ and the − sign if $a \equiv 0 \pmod 5$, are proved in [**17**]; the congruences stated in Theorem 20.4 for $\binom{7f}{f}$ and $\binom{3f}{f}$ follow immediately from Theorems 13.1 and 20.3.

Finally, the congruence for $\binom{9f}{f}$ follows from Theorem 20.2, noting that (using (2.2) and $\beta^3 = (-1)^f\beta^2$),

$$\binom{9f}{f}13f!\Big/\binom{12f}{4f}13f! = \binom{13f}{f}\Big/\binom{13f}{4f}$$

$$\equiv (-1)^f\binom{8f}{f}\Big/\binom{11f}{4f} \equiv (-1)^f\beta^3 \pmod p.$$

EXAMPLE. Let $p = 41$ so $(x,u,v,w) = (-9,0,3,-1)$ and

$$\binom{7f}{3f} = \binom{14}{6} \equiv 10 \pmod{41}, \quad \binom{7f}{f} = \binom{14}{2} \equiv 9 \pmod{41},$$

$$\binom{9f}{3f} = \binom{18}{6} \equiv -9 \pmod{41}.$$

We have

$$\gamma_+(x,-v,u,-w) = \frac{1}{2}\left[\frac{125-81+2(-9)(25+9-60)}{125-81+2(-9)(25+9+60)}\right]\left[9+\frac{(81-125)}{4(-9)}\right]$$

$$\equiv 10 \pmod{41};$$

$$(-1)^{f+[2e/5]}(a/|b|)\gamma_+(x,u,v,w)$$

$$= \frac{9}{2}\left[\frac{-1(125-81)+2(9)(-25+9-30)}{-1(125-81)+2(9)(-25+9+30)}\right]\left[9+\frac{(81-125)}{4(-9)}\right] \equiv 9 \pmod{41}.$$

Moreover,

$$\binom{9f}{f} = \binom{18}{2} \equiv 30 \pmod{41}, \qquad \binom{3f}{f} = \binom{6}{2} = 15,$$

$$\binom{9f}{2f} = \binom{18}{4} \equiv -15 \pmod{41},$$

and we have

$$(-1)^f \gamma_-(x,-u,-v,w)$$
$$= \frac{1}{2}\left[\frac{-1(125-81)+2(9)(-25+9+30)}{-(125-81)+2(9)(-25+9-30)}\right]\left[9-\frac{(81-125)}{4(-9)}\right] \equiv 30 \pmod{41},$$
$$(-1)^{f+[2e/5]}(a/|b|)\gamma_-(x,-v,u,-w)$$
$$= \frac{9}{2}\left[\frac{(125-81)+2(-9)(25+9-60)}{(125-81)+2(-9)(25+9+60)}\right]\left[9-\frac{(81-125)}{4(-9)}\right] \equiv 15 \pmod{41}.$$

Having explicitly determined 16 of the 24 representative binomial coefficients of order 20 in Theorems 20.1, 20.2, and 20.4 there remain

$$\binom{5f}{f}, \binom{5f}{2f}, \binom{8f}{3f}, \binom{11f}{5f}, \binom{7f}{2f}, \binom{9f}{4f}, \binom{6f}{f} \quad \text{and} \quad \binom{12f}{5f}.$$

In light of Theorem 20.3 it suffices to determine

$$\binom{5f}{f}, \binom{8f}{3f}, \binom{7f}{2f}, \quad \text{and} \quad \binom{12f}{5f}.$$

In the following theorem we determine these 4 binomial coefficients up to sign. Clearly such complicated determinations are almost solely of theoretical interest. However, we make no apology, as the same may be said of far simpler determinations. Moreover, the proof of Theorem 20.5 yields some neat explicit determinations for certain products and quotients of the remaining 8 representative binomial coeffcients; these are enumerated in Theorem 20.6.

THEOREM 20.5. *Let* $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$, *define* $\gamma_+(x,u,v,w)$ *and* $\gamma_-(x,u,v,w)$ *as in Theorem* 20.4, *and for a fixed primitive root* g *with* $g^{5f} \equiv a/|b| \pmod p$, *choose the signs of* a, e, x, u, *and* v *so that* $e \equiv a \pmod 5$ *if* $b \equiv 0 \pmod 5$, $e \equiv |b| \pmod 5$ *if* $a \equiv 0 \pmod 5$, $u \equiv 0 \pmod 2$, *and* $x + u - v \equiv 0 \pmod 4$. *The following congruences determine the binomial coefficients*

$$\binom{5f}{f}, \binom{8f}{3f}, \binom{7f}{2f}, \quad \text{and} \quad \binom{12f}{5f}$$

modulo p *up to sign.*

$$\binom{5f}{f} \equiv \begin{cases} \left((-1)^f \frac{e}{a}\gamma_+(x,-u,-v,w)\gamma_-(x,u,v,w)\right)^{1/2} & \text{if } b \equiv 0 \pmod 5, \\ \left((-1)^f \frac{e}{|b|}\gamma_+(x,-u,-v,w)\gamma_-(x,u,v,w)\right)^{1/2} & \text{if } a \equiv 0 \pmod 5, \end{cases}$$

$$\binom{8f}{3f} \equiv \begin{cases} (4ea\gamma_+(x,-v,u,-w)/\gamma_-(x,u,v,w))^{1/2} & \text{if } b \equiv 0 \pmod 5, \\ (4e|b|\gamma_+(x,-v,u,-w)/\gamma_-(x,u,v,w))^{1/2} & \text{if } a \equiv 0 \pmod 5, \end{cases}$$

$$\binom{7f}{2f} \equiv \begin{cases} \left((-1)^f \frac{a}{e}\gamma_+(x,-u,-v,w)\gamma_-(x,u,v,w)\right)^{1/2} & \text{if } b \equiv 0 \pmod 5, \\ \left((-1)^{f+1} \frac{|b|}{e}\gamma_+(x,-u,-v,w)\gamma_-(x,u,v,w)\right)^{1/2} & \text{if } a \equiv 0 \pmod 5, \end{cases}$$

$$\binom{12f}{5f} \equiv \begin{cases} \left((-1)^f 4ea\gamma_-(x,v,-u,-w)/\gamma_+(x,u,v,w)\right)^{1/2} & \text{if } b \equiv 0 \pmod 5, \\ \left((-1)^f 4e|b|\gamma_-(x,v,-u,-w)/\gamma_+(x,u,v,w)\right)^{1/2} & \text{if } a \equiv 0 \pmod 5. \end{cases}$$

PROOF. We have

$$\text{(20.37)} \quad \binom{5f}{f} \Big/ \binom{10f}{f} = \binom{9f}{4f} \Big/ \binom{10f}{5f}$$

$$\Rightarrow \binom{5f}{f} \Big/ \binom{9f}{4f} = \binom{10f}{f} \Big/ \binom{10f}{5f} \equiv \frac{e}{a} \quad \text{or} \quad \frac{e}{|b|}$$

according as $b \equiv 0 \pmod 5$ or $a \equiv 0 \pmod 5$ in view of (20.3), (20.4) and Theorem 7.1. Moreover,

$$\text{(20.38)} \quad \binom{5f}{f}\binom{9f}{4f} = \binom{9f}{f}\binom{8f}{4f} = (-1)^f \gamma_+(x,-u,-v,w)\gamma_-(x,u,v,w)$$

in view of Theorem 20.4 (the mapping $(x,u,v,w) \to (x,-u,-v,w)$ for either $\gamma_+(x,u,v,w)$ or $\gamma_-(x,u,v,w)$ has the effect of multiplying by $\beta^3 = (2^{(p-1)/10})^3$). Combining (20.37) and (20.38) we have the first congruence in Theorem 20.5.

Next, we have

$$\text{(20.39)} \quad \binom{8f}{3f} \Big/ \binom{12f}{5f} = \binom{7f}{3f} \Big/ \binom{12f}{4f} \equiv \gamma_+(x,-v,u,-w)/\gamma_-(x,u,v,w)$$

in view of Theorems 8.1 and 20.4. Also, using (2.2), we have

(20.40)

$$\binom{8f}{3f} 15f! \Big/ \binom{10f}{3f} 15f! = \binom{15f}{5f} \Big/ \binom{15f}{7f} \equiv (-1)^f \binom{10f}{5f} \Big/ (-1)^f \binom{12f}{5f}$$

$$\Rightarrow \binom{8f}{3f}\binom{12f}{5f} \equiv 4ea \quad \text{or} \quad 4e|b|$$

according as $b \equiv 0 \pmod 5$ or $a \equiv 0 \pmod 5$ in view of (20.3), (20.4), and Theorem 7.1. Combining (20.37) and (20.38) we have the second congruence in Theorem 20.5.

Now we have

(20.41)

$$\binom{5f}{2f} 5f! \Big/ \binom{10f}{3f} 5f! = \binom{7f}{2f} \Big/ \binom{10f}{5f}$$

$$\Rightarrow \binom{5f}{2f} \Big/ \binom{7f}{2f} \equiv \binom{10f}{3f} \Big/ \binom{10f}{5f} \equiv \frac{e}{a} \quad \text{or} \quad \frac{-e}{|b|}$$

according as $b \equiv 0 \pmod 5$ or $a \equiv 0 \pmod 5$ by (20.3), (20.4), and Theorem 7.1. Also,

$$\text{(20.42)} \quad \binom{5f}{2f}\binom{7f}{2f} = \binom{7f}{3f}\binom{4f}{2f} = (-1)^f \gamma_+(x,-u,-v,w)\gamma_-(x,u,v,w)$$

in view of Theorem 20.4 and (13.8) (noting that $\beta^8 = (-1)^f \beta^3$). Combining (20.41) and (20.42) we have the third congruence in Theorem 20.5.

Finally, combining (20.39) and (20.40) and noting that $(x, u, v, w) \to (x, -v, u, -w)$ has the effect of multiplying by β^4, $(x, u, v, w) \to (x, v, -u, -w)$ of multiplying by β, and $1/\beta^4 = (-1)^f\beta$, we have the last congruence in Theorem 20.5.

The following theorem is an immediate consequence of (20.37), (20.40), (20.41) and similarly derived congruences together with Theorem 20.3.

THEOREM 20.6. *Let* $p = 20f + 1 = a^2 + b^2 = e^2 + 5f^2$ *with* a *and* e *chosen as in Theorem* 20.4 *and with* g *a fixed primitive root such that* $g^{5f} \equiv a/|b| \pmod p$. *Then we have*

$$\binom{5f}{2f} \Big/ \binom{7f}{2f} \equiv \binom{5f}{f} \Big/ \binom{9f}{4f} \equiv \frac{e}{a}$$

or

$$\binom{5f}{2f} \Big/ \binom{7f}{2f} \equiv -\binom{5f}{f} \Big/ \binom{9f}{4f} \equiv -\frac{e}{|b|}$$

according as $b \equiv 0 \pmod 5$ *or* $a \equiv 0 \pmod 5$. *Moreover*,

$$\binom{8f}{3f}\binom{12f}{5f} \equiv (-1)^f \binom{6f}{f}\binom{11f}{5f} \equiv 4ea$$

or

$$\binom{8f}{3f}\binom{12f}{5f} \equiv (-1)^{f+1} \binom{6f}{f}\binom{11f}{5f} \equiv 4e|b|$$

according as $b \equiv 0 \pmod 5$ *or* $a \equiv 0 \pmod 5$,

$$\binom{5f}{f} \Big/ \binom{7f}{2f} \equiv \binom{5f}{2f} \Big/ \binom{9f}{4f} \equiv (-1)^f \frac{e}{a} \quad \text{or} \quad (-1)^{f+1}\frac{e}{a}$$

and

$$\binom{12f}{5f}\binom{11f}{5f} \equiv \binom{6f}{f}\binom{8f}{3f} \equiv 4ea \quad \text{or} \quad -4ea$$

according as $e \equiv 1 \pmod 5$ *or* $e \equiv 4 \pmod 5$.

EXAMPLE. Let $p = 641$ so $(x, u, v, w) = (16, 4, 12, -4)$, $2^{(p-1)/5} \equiv 1 \pmod 5$ ($\Leftrightarrow x \equiv 0 \pmod 2$), $a = 25$, $b = 4$, $e = -6$, and $f = 32$. We have, in agreement with Theorem 20.5, the following congruences modulo 641:

$$\binom{5f}{f}^2 = \binom{160}{32}^2 \equiv 13 \quad \text{and} \quad \frac{-6}{4}(434)(191) \equiv 13,$$

$$\binom{8f}{3f}^2 = \binom{256}{96}^2 \equiv 443 \quad \text{and} \quad (4)(-6)(4)(434)/191 \equiv 443,$$

$$\binom{7f}{2f}^2 = \binom{224}{64}^2 \equiv 564 \quad \text{and} \quad -4(434)(191)/-6 \equiv 564,$$

$$\binom{12f}{5f}^2\binom{156}{65}^2 \equiv 70 \quad \text{and} \quad (4)(-6)(4)(191)/434 \equiv 70,$$

for it is easily checked that

$$\gamma_+(x,u,v,w) = \frac{-16}{2} + \frac{-4(256-2000)}{8(-64+240)} \equiv \frac{199}{126} \equiv 434 \pmod{641},$$

$$\gamma_-(x,u,v,w) \equiv 191 \pmod{641}.$$

Moreover, we have as $e \equiv 4 \pmod 5$,

$$\binom{5f}{2f}\Big/\binom{7f}{2f} \equiv \frac{275}{397} \equiv -\binom{5f}{f}\Big/\binom{9f}{4f} \equiv \frac{-44}{398} \equiv \frac{-e}{b} \equiv \frac{3}{2} \pmod{641},$$

$$\binom{5f}{f}\Big/\binom{7f}{2f} \equiv \frac{44}{397} \equiv \binom{5f}{2f}\Big/\binom{9f}{4f} \equiv \frac{275}{398} \equiv \frac{-e}{b} \equiv \frac{6}{25} \pmod{641},$$

$$\binom{8f}{3f}\binom{12f}{5f} \equiv (468)(460) \equiv 4e|b| \equiv -\binom{6f}{f}\binom{11f}{5f} \equiv (330)(280) \pmod{641},$$

$$\binom{12f}{5f}\binom{11f}{5f} \equiv (460)(280) \equiv -4ea \equiv \binom{6f}{f}\binom{8f}{3f} \equiv (330)(468) \pmod{641}.$$

21. $e = 24$. For $p = 24f + 1$ there are 33 representative binomial coefficients of order 24 and 15 lower order representatives. An astonishing 43 of these 48 binomial coefficients may be related to at least one other by what we henceforth call a Cauchy-Whiteman type congruence, that is, a congruence relating two representative binomial coefficients of the type.

$$\binom{rf}{sf} \text{ and } \binom{r'f}{s'f} \text{ so that } \binom{rf}{sf} \equiv \pm\binom{r'f}{s'f} \pmod p$$

for all $p = ef + 1$. (The name derives from the facts that Cauchy proved

$$\binom{10f}{f} \equiv \pm\binom{10}{3f} \pmod p$$

for all $p = 20f + 1$ and Whiteman showed how to remove the sign ambiguity in this congruence).

We begin this section by using the Davenport-Hasse relation in the form given by Yamamoto (3.11), together with (2.1), (2.2), and (2.6), to prove all Cauchy-Whiteman type congruences for $e = mn = 24$ in which representatives are related by a term of the form $(n^{(p-1)/m})^t = \pm 1$, $t \geqslant 1$.

For the rest of this section, all congruences are understood to be taken (mod $p = 24f + 1$) unless otherwise stated.

THEOREM 21.1. *The following congruences hold for all prime* $p = 24f + 1 = a^2 + b^2$, $a \equiv 1 \pmod 4$; $\alpha = 1$ *if* $a \equiv 0 \pmod 3$ *and* $\alpha = 2$ *if* $b \equiv 0 \pmod 3$.

$$\binom{2f}{f} \equiv \binom{14f}{7f}, \binom{4f}{f} \equiv (-1)^{b/4}\binom{13f}{3f},$$

$$\binom{5f}{f} \equiv \binom{11f}{4f}, \binom{6f}{f} \equiv (-1)^{f+\alpha}\binom{13f}{6f},$$

$$\binom{9f}{2f} \equiv (-1)^{f+b/4}\binom{9f}{4f}, \quad \binom{10f}{f} \equiv (-1)^{b/4}\binom{13f}{4f}$$

$$\binom{4f}{2f} \equiv (-1)^{f+b/4}\binom{7f}{2f}, \quad \binom{5f}{2f} \equiv (-1)^{f+b/4}\binom{7f}{3f},$$

$$\binom{12f}{f} \equiv \binom{12f}{5f}, \quad \binom{10f}{5f} \equiv (-1)^{f}\binom{13f}{2f},$$

$$\binom{11f}{f} \equiv (-1)^{f+b/4}\binom{14f}{4f}, \qquad \binom{7f}{f} \equiv \binom{11f}{5f}, \quad \binom{8f}{2f} \equiv \binom{14f}{6f},$$

$$\binom{6f}{3f} \equiv (-1)^{f+b/4}\binom{12f}{3f} \equiv (-1)^{f}\binom{15f}{6f}, \quad \binom{6f}{2f} \equiv (-1)^{\alpha}\binom{10f}{4f},$$

$$\binom{9f}{3f} \equiv (-1)^{f+b/4+\alpha}\binom{12f}{2f} \equiv (-1)^{f+b/4}\binom{12f}{6f}, \qquad \binom{10f}{2f} \equiv \binom{16f}{8f}.$$

PROOF. The theorem follows directly from the following 19 congruences, noting that 2 and 3 are quadratic residues of every prime $p = 24f + 1$, $2^{(p-1)/4} \equiv (-1)^{b/4} \pmod{p}$ (Gauss) and $3^{(p-1)/4} \equiv 1$ or $-1 \pmod{p}$, according as $b \equiv 0 \pmod 3$ or $a \equiv 0 \pmod 3$.

	Congruence	*Reason*
(21.1)	$\binom{6f}{3f} \equiv (-1)^{f}\binom{15f}{6f}$	Theorem 11.2
(21.2)	$\binom{6f}{3f} \equiv (-1)^{f+b/4}\binom{12f}{3f}$	Theorem 11.2
(21.3)	$\binom{9f}{3f} \equiv (-1)^{f+b/4}\binom{12f}{6f}$	Corollary 4.1.3
(21.4)	$\binom{6f}{2f} \equiv (-1)^{\alpha}\binom{10f}{4f}$	Theorem 15.1
(21.5)	$\binom{12f}{2f} \equiv (-1)^{\alpha}\binom{12f}{6f}$	Corollary 4.2.2
(21.6)	$\binom{10f}{2f} \equiv \binom{16f}{8f}$	Corollary 4.4.1
(21.7)	$\binom{8f}{2f} \equiv \binom{14f}{6f}$	Theorem 11.2

Next, using (3.11), (2.1), and (2.2) we have

$$3^{(p-1)/8} \equiv \frac{3f!\,8f!\,16f!}{f!\,9f!\,17f!} \equiv \frac{-3f!}{f!\,9f!\,17f!}$$

$$\equiv (-1)^{f}\frac{3f!\,23f!\,14f!}{9f!\,17f!\,14f!} \equiv (-1)^{f}\binom{10f}{f}\Big/\binom{10f}{3f},$$

$$(3^{(p-1)/8})^3 \equiv \frac{9f!\,8f!\,16f!}{3f!\,11f!\,19f!} \equiv (-1)^{f}\binom{13f}{3f}\Big/\binom{19f}{9f} \equiv \binom{13f}{3f}\Big/\binom{14f}{5f}.$$

It follows that

$$1 \equiv 3^{(p-1)/2} \equiv (-1)^f \binom{13f}{3f}\binom{10f}{f} \Big/ \binom{14f}{5f}\binom{10f}{3f}$$
$$\equiv (-1)^f \frac{13f!}{3f!\,10f!}\,\frac{5f!\,9f!}{14f!}\,\frac{3f!\,7f!}{10f!}\,\frac{10f!}{f!\,9f!}$$
$$\equiv \frac{5f!\,7f!\,6f!}{f!\,11f!\,6f!} \equiv \binom{7f}{f} \Big/ \binom{11f}{5f}.$$

Moreover,

$$\binom{12f}{f} \Big/ \binom{12f}{5f} = \frac{12f!}{f!\,11f!}\,\frac{5f!\,7f!\,6f!}{12f!\,6f!} = \binom{7f}{f} \Big/ \binom{11f}{5f}$$
$$= \frac{7f!}{f!\,6f!}\,\frac{5f!\,6f!\,4f!}{11f!\,4f!} = \binom{5f}{f} \Big/ \binom{11f}{4f}.$$

Combining these we have

$$\binom{7f}{f} \equiv \binom{11f}{5f}, \tag{21.8}$$

$$\binom{12f}{f} \equiv \binom{12f}{5f}, \tag{21.9}$$

$$\binom{5f}{f} \equiv \binom{11f}{4f}. \tag{21.10}$$

Next using (3.11) and (2.2) we have

$$2^{(p-1)/12} \equiv \frac{2f!\,12f!\,11f!}{f!\,13f!\,11f!} = \binom{12f}{f} \Big/ \binom{13f}{2f},$$

$$(2^{(p-1)/12})^5 \equiv \frac{10f!\,12f!\,7f!}{5f!\,17f!\,7f!} \equiv (-1)^f \binom{12f}{5f} \Big/ \binom{14f}{7f}.$$

Taking $g = 12$, $h = 1$, $k = 2$ in (2.6), and using (2.2), gives

$$\binom{12f}{f}\binom{12f}{f} \equiv \binom{2f}{f}\binom{22f}{11f} \equiv (-1)^f \binom{2f}{f}\binom{13f}{2f}.$$

Making use of (21.9) we obtain

$$1 \equiv 2^{(p-1)/2} \equiv (2^{(p-1)/12})(2^{(p-1)/12})^5$$
$$\equiv \binom{2f}{f}\binom{12f}{f} \Big/ \binom{12f}{f}\binom{14f}{7f},$$

giving

$$\binom{2f}{f} \equiv \binom{14f}{7f}. \tag{21.11}$$

In establishing the remaining congruences we will use (21.8)–(21.11) without specifically citing them.

Taking $g = 14$, $h = 7$, $k = 12$ in (2.6) we have

$$\binom{14f}{7f}\binom{10f}{5f} \equiv \binom{12f}{7f}\binom{12f}{7f},$$

so

$$(-1)^f\binom{12f}{f}\Big/\binom{10f}{5f} \equiv (-1)^f\binom{2f}{f}\Big/\binom{12f}{f} \equiv \binom{12f}{f}\Big/\binom{13f}{2f} \equiv 2^{(p-1)/12},$$

from which follows

$$\binom{10f}{5f} \equiv (-1)^f\binom{13f}{2f}. \tag{21.12}$$

Appealing to (3.11), we get

$$2^{(p-1)/3} = (2^{(p-1)/12})^4 \equiv \frac{8f!\,12f!\,8f!}{4f!\,16f!\,8f!}$$

$$= \binom{12f}{4f}\Big/\binom{16f}{8f} \equiv \binom{12f}{4f}\Big/\binom{10f}{2f};$$

moreover,

$$\binom{10f}{f}\binom{13f}{2f}\Big/\binom{13f}{4f}\binom{12f}{f} = \frac{10f!}{f!\,9f!}\,\frac{4f!\,9f!}{13f!}\,\frac{f!\,11f!}{12f!}\,\frac{13f!}{2f!\,11f!}$$

$$= \frac{4f!\,10f!\,12f!}{2f!\,12f!\,8f!} = \binom{12f}{4f}\Big/\binom{10f}{2f},$$

and it follows that

$$\binom{10f}{f} \equiv (-1)^{b/4}\binom{13f}{4f}. \tag{21.13}$$

Since

$$\binom{10f}{f}\Big/\binom{13f}{4f} = \frac{10f!\,4f!\,3f!}{f!\,13f!\,3f!} = \frac{10f!\,4f!\,14f!}{f!\,13f!\,14f!},$$

we obtain, using (2.2),

$$\binom{4f}{f} \equiv (-1)^{b/4}\binom{13f}{3f}, \tag{21.14}$$

$$\binom{11f}{f} \equiv (-1)^{f+b/4}\binom{14f}{4f}. \tag{21.15}$$

Next, using the previously established congruence for $2^{(p-1)/12}$,

$$\binom{4f}{2f}\Big/\binom{7f}{2f}\cdot\binom{12f}{2f}\Big/\binom{4f}{2f} = \frac{12f!\,5f!\,5f!}{7f!\,10f!\,5f!}$$

$$\equiv \binom{12f}{f}\Big/\binom{10f}{5f} \equiv (-1)^f 2^{(p-1)/12}.$$

From (15.7) we have

$$2^{(p-1)/3} \equiv \binom{12f}{2f} \Big/ \binom{4f}{2f}$$

so

$$\binom{4f}{2f} \equiv (-1)^{f+b/4}\binom{7f}{2f}. \tag{21.16}$$

Since

$$\binom{4f}{2f}\Big/\binom{7f}{2f} = \frac{4f!\,5f!\,9f!}{2f!\,7f!\,9f!} = \frac{4f!\,5f!\,3f!}{2f!\,7f!\,3f!},$$

we have at once that

$$\binom{9f}{2f} \equiv (-1)^{f+b/4}\binom{9f}{4f}, \tag{21.17}$$

$$\binom{5f}{2f} \equiv (-1)^{f+b/4}\binom{7f}{3f}. \tag{21.18}$$

Now, appealing to (2.1), (2.2), and (3.11) we have

$$\begin{aligned}(6^{(p-1)/4})^3 &\equiv \frac{18f!\,4f!\,8f!\,12f!\,16f!\,20f!}{3f!\,7f!\,11f!\,15f!\,19f!\,23f!}\\ &\equiv (-1)^{f+1}\left(\frac{18f!\,12f!\,5f!\,f!\,13f!\,6f!}{3f!\,7f!\,11f!\,13f!\,6f!}\right)\\ &\equiv (-1)^f\binom{18f}{3f}\binom{13f}{6f}12f!\,5f!\,f!\,6f!\Big/6f!\,18f!\\ &\equiv \binom{9f}{3f}\binom{13f}{6f}\Big/\binom{12f}{6f}\binom{6f}{f}.\end{aligned}$$

Thus, using Theorem 11.2, we obtain

$$\binom{6f}{f} \equiv (-1)^{f+\alpha}\binom{13f}{6f}. \tag{21.19}$$

This completes the proof of Theorem 21.1.

The number of Cauchy-Whiteman type congruences in Theorem 21.1 exceeds that of all such congruences for all lower order cases ($e < 24$). Perhaps, even more surprisingly, it does *not* include all the Cauchy-Whiteman type congruences for $e = 24$. In contrast to the lower order cases (and anything we can find elsewhere in the literature), there are Cauchy-Whiteman type congruences for $e = mn = 24$ for which the ± 1 relating

$$\binom{rf}{sf} \quad \text{and} \quad \binom{r'f}{s'f} \quad \text{modulo } p$$

is not an expression of the form $(n^{(p-1)/m})^t$, $t \geqslant 1$. We have, instead, the following theorem which, in conjunction with Theorem 21.1, gives all Cauchy-Whiteman type congruences for $e = 24$.

THEOREM 21.2. *The following congruences hold for all primes* $p = 24f + 1 = a^2 + b^2 = x^2 + 3y^2 = u^2 + 6v^2$, $a \equiv u \equiv 1 \pmod 4$, $x \equiv 1 \pmod 3$:

$$\binom{2f}{f} \equiv (-1)^{v/2}\binom{8f}{f}, \qquad \binom{7f}{f} \equiv (-1)^{v/2}\binom{8f}{2f},$$

$$\binom{7f}{3f} \equiv (-1)^{f+y/4}\binom{11f}{3f}, \qquad \binom{4f}{f} \equiv (-1)^{f+y/4}\binom{8f}{3f},$$

$$\binom{5f}{f} \equiv (-1)^{f+y/4}\binom{8f}{4f}, \qquad \binom{9f}{f} \equiv (-1)^{v/2}\binom{9f}{2f},$$

$$\binom{10f}{f} \equiv (-1)^{f+v/2}\binom{15f}{7f}, \qquad \binom{13f}{2f} \equiv (-1)^{v/2}\binom{13f}{5f}.$$

PROOF. From Berndt [**3**, p. 3.23] we have

$$J_{24}(1,4) = (-1)^{f+v/2}2^{(p-1)/12}J_{24}(8,8),$$

so that, appealing again to Theorem 5.1 we have that for a prime ideal divisor π of P in $Q(e^{2\pi i/24})$,

$$\binom{5f}{f} \equiv (-1)^{f+v/2}(2^{(p-1)/12})^5\binom{16f}{8f} \pmod{\pi}$$

$$\Rightarrow \binom{5f}{f} \equiv (-1)^{f+y/4}(2^{(p-1)/6})\binom{16f}{8f} \pmod{\pi}$$

(as $2^{(p-1)/4} = (-1)^{b/4}$ and $(-1)^{b/4+v/2} = (-1)^{y/4}$ follows from [**3**, pp. 317, 3.25]).

Next Theorems 6.2 and 9.2 give

$$\binom{8f}{4f} \Big/ \binom{16f}{8f} \equiv 2^{(p-1)/6} \pmod{\pi}$$

in view of 4.5 (and $(2^{(p-1)/3})^2 = 2^{(p-1)/6}$). It follows at once that

$$\binom{5f}{f} \equiv (-1)^{f+y/4}\binom{16f}{8f} \pmod{p}.$$

Moreover, we have using

$$\binom{5f}{f} \equiv \binom{11f}{4f}$$

from Theorem 21.1,

$$\binom{5f}{f} \Big/ \binom{8f}{4f} = \binom{4f}{f} \Big/ \binom{8f}{3f} \equiv \binom{7f}{3f} \Big/ \binom{11f}{3f},$$

giving all congruences for which $\pm 1 = (-1)^{f+y/4}$.

Next, using Theorem 21.1,

$$\binom{5f}{f} \Big/ \binom{8f}{4f} = \binom{9f}{f} \Big/ \binom{9f}{4f} \Rightarrow \binom{9f}{f} \Big/ \binom{9f}{2f} = (-1)^{v/2}$$

and, using

$$\left(\frac{7f}{f}\right) \equiv \left(\frac{11f}{5f}\right)$$

from Theorem 21.1, we have

$$\left(\frac{9f}{f}\right)\Big/\left(\frac{9f}{2f}\right) = \left(\frac{2f}{f}\right)\Big/\left(\frac{8f}{f}\right) = \left(\frac{7f}{f}\right)\Big/\left(\frac{8f}{2f}\right) \equiv \left(\frac{13f}{5f}\right)\Big/\left(\frac{13f}{2f}\right),$$

giving all congruences for which $\pm 1 = (-1)^{v/2}$.

Finally, using (2.2) and

$$\left(\frac{14f}{6f}\right) \equiv \left(\frac{8f}{2f}\right)$$

from Theorem 21.1, we have

$$\left(\frac{15f}{7f}\right)\Big/\left(\frac{10f}{f}\right) \equiv (-1)^f\left(\frac{15f}{7f}\right)\Big/\left(\frac{15f}{f}\right) = (-1)^f\left(\frac{7f}{f}\right)\Big/\left(\frac{14f}{6f}\right)$$

$$= (-1)^f\left(\frac{7f}{f}\right)\Big/\left(\frac{8f}{2f}\right) \equiv (-1)^{f+v/2},$$

completing the proof of Theorem 21.2.

THEOREM 21.3. *Let* $p = 24f + 1 = a^2 + b^2 = u^2 + 6v^2$ *with* $a \equiv u \equiv 1 \pmod 4$. *Then we have, according as* $b \equiv 0 \pmod 3$, *or* $a \equiv 0 \pmod 3$, *the following congruences*:

$$\left(\frac{12f}{f}\right) \equiv \left(\frac{12f}{5f}\right) \equiv (-1)^f 2u \quad \text{or} \quad (-1)^{f+1}2u \pmod p.$$

PROOF. From Berndt and Evans [**4**, pp. 374, 377] we have

$$J_{24}(12, 23) = u - iv\sqrt{6} \quad \text{for } u \equiv 1 \pmod 4;$$

moreover, applying Theorem 5.1 and using (2.2), we have

$$J_{24}(12, 23) = -\left(\frac{13f}{f}\right) \equiv (-1)^{f+1}\left(\frac{12f}{f}\right) \pmod \pi.$$

As $J_{24}(1, 12) \equiv 0 \pmod \pi$ we obtain, as before,

$$\left(\frac{12f}{f}\right) \equiv (-1)^{f+1}2u \pmod p \quad \text{for } u \equiv 1 \pmod 4.$$

From Berndt [**4**, Theorem 3.18] we have $u \equiv 1 \pmod 4$ iff $a \equiv 0 \pmod 3$ and $u \equiv -1 \pmod 4$ iff $b \equiv 0 \pmod 3$, completing the proof of Theorem 21.3 in view of Theorem 21.1.

Using previously established congruences from §§5, 6, 7, 9, 11, 15 and Theorems 21.1–21.3, we now prove the following theorems.

THEOREM 21.4. *Let* $p = 24f + 1 = a^2 + b^2 = x^2 + 3y^2$, $a \equiv 1 \pmod 4$, $x \equiv 1 \pmod 3$. *Let* $\alpha = 1$ *if* $a \equiv 0$ *if* $a \equiv 0 \pmod 3$, $\beta = 1$ *if* a *or* $b \equiv 2 \pmod 3$, $\alpha = 2$ *if* $b \equiv 0 \pmod 3$, $\beta = 2$ *if* a *or* $b \equiv 1 \pmod 3$. *We have the following congruences modulo* p.

$$(-1)^{f+b/4}\binom{9f}{3f} \equiv (-1)^{\alpha}\binom{12f}{2f} \equiv \binom{12f}{6f} \equiv 2a,$$

$$(-1)^{v/2+\beta}\binom{7f}{f} \equiv (-1)^{\beta}\binom{8f}{2f} \equiv (-1)^{v/2+\beta}\binom{11f}{5f}$$

$$\equiv (-1)^{\beta}\binom{14f}{6f} \equiv 2a \quad or \quad 2b$$

according as $b \equiv 0 \pmod 3$ *or* $a \equiv 0 \pmod 3$,

$$(-1)^{\alpha}\binom{4f}{2f} \equiv (-1)^{f+b/4+\alpha}\binom{7f}{2f} \equiv \begin{cases} 2a & \text{if } y \equiv 0 \pmod 3, \\ \dfrac{2ax - 6ay}{x + 3y} & \text{if } y \equiv 1 \pmod 3, \\ \dfrac{2ax + 6ay}{x - 3y} & \text{if } y \equiv 2 \pmod 3, \end{cases}$$

$$(-1)^{f+b/4+\alpha}\binom{11f}{f} \equiv (-1)^{\alpha}\binom{14f}{4f} \equiv \begin{cases} 2a & \text{if } y \equiv 0 \pmod 3, \\ \dfrac{2ax + 6ay}{x - 3y} & \text{if } y \equiv 1 \pmod 3, \\ \dfrac{2ax - 6ay}{x + 3y} & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

PROOF. The first three congruences follow immediately from Theorems 11.1, 15.1, and 7.1, respectively. The congruences for

$$\binom{8f}{2f}, \binom{4f}{2f}, \quad \text{and} \quad \binom{14f}{4f}$$

follow from Theorem 15.1 and the remaining congruences then follow from Theorems 21.1 and 21.2.

THEOREM 21.5. *Let* $p = 24f + 1 = c^2 + 2d^2$, $c \equiv 1 \pmod 4$. *Then we have*

$$(-1)^{b/4}\binom{6f}{3f} \equiv (-1)^{f}\binom{12f}{3f} \equiv (-1)^{f+b/4}\binom{15f}{6f} \equiv 2c \pmod p.$$

PROOF. This is immediate from Theorem 11.2.

THEOREM 21.6. *Let* $p = 24f + 1 = a^2 + b^2 = x^2 + 3y^2$, $4p = A^2 + 27B^2$, $a \equiv 1 \pmod 4$, $A \equiv x \equiv 1 \pmod 3$. *Let* $\beta = 1$ *if* a *or* $b \equiv 2 \pmod 3$, $\beta = 2$ *if* a *or* $b \equiv 1 \pmod 3$. *Then we have the following congruences modulo* p.

$$\binom{12f}{4f} \equiv 2x,$$

$$(-1)^{\beta}\binom{6f}{2f} \equiv 2x \quad or \quad 2bx/a \equiv (-1)^{\beta}\binom{10f}{4f} \equiv 2x \quad or \quad 2ax/b$$

according as $b \equiv 0 \pmod 3$ *or* $a \equiv 0 \pmod 3$,

$$\left(\begin{matrix} 10f \\ 2f \end{matrix}\right) \equiv \left(\begin{matrix} 16f \\ 8f \end{matrix}\right) \equiv -A \equiv \begin{cases} 2x & \text{if } y \equiv 0 \pmod 3, \\ -x - 3y & \text{if } y \equiv 1 \pmod 3, \\ -x + 3y & \text{if } y \equiv 2 \pmod 3, \end{cases}$$

$$(-1)^{f+y/4}\left(\begin{matrix} 5f \\ f \end{matrix}\right) \equiv \left(\begin{matrix} 8f \\ 4f \end{matrix}\right) \equiv (-1)^{f+y/4}\left(\begin{matrix} 11f \\ 4f \end{matrix}\right)$$

$$\equiv \begin{cases} 2x & \text{if } y \equiv 0 \pmod 3, \\ -x + 3y & \text{if } y \equiv 1 \pmod 3, \\ -x - 3y & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

PROOF. The first congruence in Theorem 21.6 follows from Corollary 4.1.1 and Theorem 9.2 (also from (15.4) and Theorem 15.1). The rest of the congruences in this theorem follow easily from Theorems 6.1, 6.2, 15.1, and 21.2.

THEOREM 21.7. *Let* $p = 24f + 1 = a^2 + b^2 = x^2 + 3y^2 = u^2 + 6v^2$, $a \equiv u \equiv 1 \pmod 4$, $x \equiv 1 \pmod 3$. *Let* $\alpha = 1$ *if* $a \equiv 0 \pmod 3$, $\beta = 1$ *if* a *or* $b \equiv 2 \pmod 3$, $\alpha = 2$ *if* $b \equiv 0 \pmod 3$, $\beta = 2$ *if* a *or* $b \equiv 1 \pmod 3$. *We have the following congruences modulo* p.

$$\left(\begin{matrix} 12f \\ f \end{matrix}\right) \equiv \left(\begin{matrix} 12f \\ 5f \end{matrix}\right) \equiv (-1)^{f+\alpha} 2u,$$

$$(-1)^{f+v/2+\beta}\left(\begin{matrix} 6f \\ f \end{matrix}\right) \equiv (-1)^{v/2+\alpha+\beta}\left(\begin{matrix} 13f \\ 6f \end{matrix}\right) \equiv 2u \quad \text{or} \quad 2au/b$$

according as $b \equiv 0 \pmod 3$ *or* $a \equiv 0 \pmod 3$,

$$(-1)^{b/4+\alpha}\left(\begin{matrix} 10f \\ 5f \end{matrix}\right) \equiv (-1)^{f+b/4+\alpha}\left(\begin{matrix} 13f \\ 2f \end{matrix}\right) \equiv (-1)^{f+y/4+\alpha}\left(\begin{matrix} 13f \\ 5f \end{matrix}\right)$$

$$\equiv \begin{cases} 2u & \text{if } y \equiv 0 \pmod 3, \\ (2xu - 6yu)/(x + 3y) & \text{if } y \equiv 1 \pmod 3, \\ (2xu + 6yu)/(x - 3y) & \text{if } y \equiv 2 \pmod 3, \end{cases}$$

$$(-1)^{f+b/4+\alpha}\left(\begin{matrix} 2f \\ f \end{matrix}\right) \equiv (-1)^{f+y/4+\alpha}\left(\begin{matrix} 8f \\ f \end{matrix}\right) \equiv (-1)^{f+b/4+\alpha}\left(\begin{matrix} 14f \\ 7f \end{matrix}\right)$$

$$\equiv \begin{cases} 2u & \text{if } y \equiv 0 \pmod 3, \\ (2xu + 6yu)/(x - 3y) & \text{if } y \equiv 1 \pmod 3, \\ (2xu - 6yu)/(x + 3y) & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

PROOF. Theorem 21.3 constitutes the first two congruences in this theorem.

To prove the last six congruences in Theorem 21.7 we use (3.11) and (2.2) to obtain

$$2^{(p-1)/12} \equiv \frac{2f!\,12f!\,11f!}{f!\,13f!\,11f!} \equiv \binom{12f}{f} \Big/ \binom{13f}{2f}$$
$$\equiv \frac{2f!\,12f!\,f!}{f!\,13f!\,11f!} \equiv (-1)^f \binom{2f}{f} \Big/ \binom{12f}{f}.$$

The last six congruences follow immediately from the above congruence and Theorems 21.1–21.3.

To prove the third and fourth congruences in Theorem 21.7 we note that earlier (see (21.3) and the congruence following (21.7)) we showed that

$$2^{(p-1)/4} \equiv (-1)^f \binom{9f}{3f} \Big/ \binom{12f}{6f}$$

and

$$3^{(p-1)/8} \equiv (-1)^f \binom{10f}{f} \Big/ \binom{10f}{3f}.$$

Using (2.2) we have

$$(2^{(p-1)/4})(3^{(p-1)/8}) \equiv \frac{9f!}{3f!\,6f!} \frac{6f!\,6f!}{12f!} \frac{10f!}{f!\,9f!} \frac{3f!\,7f!}{10f!} \frac{5f!}{5f!}$$
$$\equiv \binom{6f}{f} \Big/ \binom{12f}{5f}.$$

The result now follows from Theorems 21.1 and 21.3.

REMARK. The first author has shown (unpublished) that the criteria of Hudson and Williams [**16**] for 3 to be an eighth power (mod p) is derivable from the above theorems (in a more general form). This derivation is neater than the one given in [**16**] requiring cyclotomy. A complete determination of the Jacobi sums of order 40 would, in our opinion, undoubtedly lead to a criteria for determining when $5^{(p-1)/8} \equiv +1, -1, b/a$, or $-b/a \pmod p$ in terms of the parameters a, b, l, m in $p = a^2 + b^2 = l^2 + 10m^2$. This would be of interest if it is new and as simple as the classical criteria.

Finally, the remaining binomial coefficients of order 24 can be determined up to sign as in §§18–20. We cite just one example, as the details are easily obtained.

THEOREM 21.8. *Let* $p = 24f + 1 = a^2 + b^2 = c^2 + 2d^2 = x^2 + 3y^2 = u^2 + 6v^2$, $a \equiv c \equiv u \equiv 1 \pmod 4$, $x \equiv 1 \pmod 3$. *Then we have*

$$\binom{9f}{f} \equiv \left((-)^f \binom{16f}{8f} \binom{8f}{f} \binom{7f}{f} \Big/ \binom{15f}{6f}\right)^{1/2} \pmod p,$$

where the binomial coefficients on the right-hand side of the congruence are given in Theorems 21.4–21.7.

PROOF. The theorem follows immediately from the easily established congruences

$$\binom{9f}{f}\binom{15f}{7f} \equiv (-1)^f \binom{16f}{8f}\binom{8f}{f}$$

and

$$\binom{9f}{f} \Big/ \binom{15f}{7f} \equiv \binom{7f}{f} \Big/ \binom{15f}{6f}.$$

REMARK. As before each of the binomial coefficients, which we are only able to determine up to sign, is completely determined if the sign ambiguity can be removed for any one of these.

REFERENCES

1. P. Bachman, *Die Lehre von der Kreisteilung*, Leipzig, 1872.
2. Bruce C. Berndt, *Classical theorems on quadratic residues*, Enseignement Math. (2) **22** (1976), 261–304.
3. _____, *Gauss and Jacobi sums*, unpublished course notes, Univ. of Illinois, Urbana, Ill., 1978.
4. Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory **11** (1979), 349–398.
5. L'Augustin Cauchy, *Mémoire sur la théorie des nombres*, Mém. Institut de France, no. 17, 1840, pp. 249–768 (Ouvres Complétes (1) Vol. 3, 1911, pp. 5–83).
6. T. Clausen, *Beweis der theorems von Hrn. Dr. Stern*, J. Reine Angew. Math. **8** (1932), 140.
7. Harold Davenport and Helmut Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182.
8. Leonard Eugene Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
9. _____, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. **37** (1935), 363–380.
10. _____, *Cyclotomy when e is composite*, Trans. Amer. Math. Soc. **38** (1935), 187–200.
11. _____, *History of the theory of numbers*, Vol. 3, 2nd ed., Chelsea, New York, 1966.
12. Ronald J. Evans, *Resolution of sign ambiguities in Jacobi and Jacobsthal sums*, Pacific J. Math. **81** (1979), 71–80.
13. Carl Friedrich Gauss, *Theoria residuorum biquadraticorum*, Comment. I, Comment. soc. reg. sci. Gottingensis rec. **6** (1828), 27 (*Werke*, Vol. 2, pp. 89–90.)
14. Reinaldo E. Guidici, Joseph B. Muskat and Stanley F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc. **171** (1972), 317–347.
15. Thorold Gosset, *On the law of quartic reciprocity*, Messenger of Math. **41** (1911), 65–90.
16. Richard H. Huson and Kenneth S. Williams, *Some new residuacity criteria*, Pacific J. Math. **91** (1980), 135–143.
17. _____, *Cauchy-type congruences for binomial coefficients*, Proc. Amer. Math. Soc. **85** (1982), 169–174.
19. C. G. J. Jacobi, *De Residuis cubicis commentatio numerosa*, J. Reine Angew. Math. **2** (1827), 66–69.
20. _____, *Uber die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, J. Reine Angew. Math. **30** (1846), 166–182.
21. Emma Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J. **18** (1951), 11–18.
22. _____, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.
23. _____, *On Euler's criterion*, J. Austral. Math. Soc. **1** (1959), 64–70.
24. Philip A. Leonard and Kenneth S. Williams, *The septic character of* 2, 3, 5 *and* 7, Pacific J. Math. **52** (1974), 143–147.
25. Philip A. Leonard, Brian C. Mortimer, and Kenneth S. Williams, *The eleventh power character of* 2, J. Reine Angew. Math. **286/287** (1976), 213–222.
26. Philip A. Leonard and Kenneth S. Williams, *A rational sixteenth power reciprocity law*, Acta Arith. **33** (1977), 365–377.
27. J. Myron Masley and Hugh L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.

28. Joseph B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. **11** (1966), 263–279.
29. _____, *Reciprocity and Jacobi sums*, Pacific J. Math. **20** (1967), 275–280.
30. _____, *On Jacobi sums of certain composite orders*, Trans. Amer. Math. Soc. **134** (1968), 483–502.
31. Joseph B. Muskat and Albert Leon Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. **19** (1970), 185–216.
32. Joseph B. Muskat and Yun-Cheng Zee, *Sign ambiguities of Jacobi sums*, Duke Math. J. **40** (1973), 313–334.
33. Budh Sing Nashier and A. R. Rajwade, *Determination of a unique solution of the quadratic partition for primes* $p \equiv 1 \pmod 7$, Pacific J. Math. **72** (1977), 513–521.
34. A. R. Rajwade, *Some congruences in algebraic integers and rational integers*, Indian J. Pure Appl. Math. **7** (1976), 431–435.
35. Lothar von Schrukta, *Ein Beweis für die Zerlegbarkeit der Primzahlen von der Form* $6N + 1$ *in ein einfaches und ein dreifaches Quadrat*, J. Reine Angew. Math. **140** (1911), 252–265.
36. Henry John Stephen Smith, *Report on the theory of numbers*, Chelsea, New York, 1964.
37. M. A. Stern, *Aufgaben und Lehrsätze, Theorem* 17, J. für Math. **7** (1831), 104.
38. _____, In Folge Angew Math. **9** (1832), 97.
39. _____, *Aufgaben and Lehrsätze, problem* 4, J. Reine Angew. Math. **18** (1838), 375–376.
40. _____, *Eine Bemerkung zur Zahlentheorie*, J. Reine Angew. Math. **32** (1846), 89–90.
41. L. Stickelberger, *Ueber eine Verallemeinerung der Kreisteilung*, Math. Ann. **37** (1890), 321–367.
42. Albert Leon Whiteman, *Cyclotomy and Jacobsthal sums*, Amer. J. Math. **74** (1952), 89–99.
43. _____, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. **86** (1957), 401–413.
44. _____, *The cyclotomic numbers of order twelve*, Acta Arith. **6** (1960), 53–76.
45. _____, *Theorems on Brewer and Jacobsthal sums*. I, Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc., Providence, R.I., 1965, pp. 44–55.
46. _____, *Theorems on Brewer and Jacobsthal sums*, II, Michigan Math. J. **12** (1965), 65–80.
47. Kenneth S. Williams, *A quadratic partition of primes* $\equiv 1 \pmod 7$, Math. Comp. **28** (1974), 1133–1136.
48. _____, *On Euler's criterion for cubic nonresidues*, Proc. Amer. Math. Soc. **49** (1975), 277–283.
49. _____, *On Euler's criterion for quintic nonresidues*, Pacific J. Math. **61** (1975), 543–550.
50. Koichi Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combin. Theory Ser. A **1** (1966) 476–489.
51. Yun-Cheng Zee, *The Jacobi sums of orders thirteen and sixty and related quadratic decompositions*, Math. Z. **115** (1970), 259–272.

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

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada