ACTA ARITHMETICA
121.4 (2006)

Some congruences for binomial coefficients

by

TSUNEO ISHIKAWA (Osaka)

1. Introduction. Throughout this paper e denotes an integer ≥ 3 and p a prime $\equiv 1 \pmod{e}$. The integer f is defined by $p = ef + 1$. For integers r and s satisfying $1 \leq s < r < e$, we consider binomial coefficients of the form $\binom{rf}{sf}$. In the cases where p is represented by well known binary quadratic forms, the congruences modulo p or p^2 have been studied by many authors (for example, see [3]). In particular, the congruence modulo p^2 for $e = 3, 4, 6$ was explicitly obtained by Yeung in [7].

In the case of $e = 5$, Rajwade proved in [6] that

$$\binom{2f}{f} + \binom{3f}{f} + x \equiv 0 \pmod{p} \tag{1}$$

where x is given uniquely by Dickson's equations

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

The explicit formula for $\binom{rf}{sf} \pmod{p}$ for $e = 5$ was given by Hudson and Williams in [3].

In this paper, we study the generalization of (1) for any e and the congruences modulo p^2, using Jacobi sums. The main theorem is Theorem 1 in §3. In §4, §5, and §6, we obtain explicit formulas by applying our theorem in the cases where $e = 5$, 7, and 8.

2. Jacobi sums. For a positive integer n we set $\zeta_n = \exp(2\pi\sqrt{-1}/n)$. For $(a, e) = 1$, we define the automorphism σ_a by $\sigma_a(\zeta_e) = \zeta_e^a$, and let $\mathcal{P}$ denote any of the $\phi(e)$ prime ideals dividing p in the cyclotomic field $\mathbb{Q}(\zeta_e)$. We define a multiplicative character $\chi_e \pmod{p}$ of order e by

$$\chi_e(n) = \begin{cases} \zeta_e^a & \text{if } n \not\equiv 0 \pmod{p},\ n^f \zeta_e^a \equiv 1 \pmod{\mathcal{P}}, \\ 0 & \text{if } n \equiv 0 \pmod{p}. \end{cases}$$

2000 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B65, 11T24.

For any positive integers r and s, the Jacobi sum $J_e(r,s)$ of order e is defined by

$$J_e(r,s) = -\sum_{n=0}^{p-1} \chi_e(n)^r \chi_e(1-n)^s.$$

Basic properties of Jacobi sums are as follows.

PROPOSITION 1 (see [3]). *We have*

(a) $J_e(r,s) = J_e(s,r)$,
(b) $J_e(r,s) = (-1)^{sf} J_e(e-r-s,s)$ *for* $r+s<e$,
(c) $J_e(r,s)J_e(e-r,e-s) = p$,
(d) $J_e(r,r) = \sigma_r(J_e(1,1))$ *for* $1 \le r \le e-1$,
(e) $J_e(e-r,e-s) \equiv 0 \pmod{\mathcal{P}}$ *for* $r+s<e$,
(f) $\binom{rf+sf}{sf} \equiv J_e(r,s) \pmod{\mathcal{P}}$ *for* $r+s<e$.

The following proposition is important to determine the congruence modulo p^2. It was proved by Yeung (see Proposition 4.1 of [7]).

PROPOSITION 2. *Let* $r+s<e$ *and* $r \ge s$. *Then*

$$\binom{(r+s)f}{sf} \equiv J_e(r,s)\left\{1 + ((r+s)B_{r+s} - rB_r - sB_s)\,\frac{p}{e}\right\} \pmod{\mathcal{P}^2}$$

where $B_t = \sum_{i=1}^{tf}(1/i)$, $1 \le t \le e$.

3. Main theorem

THEOREM 1. *Let* $e \ge 3$ *be an integer and* $p = ef+1$ *a prime. Then for* $1 \le r \le e-1$ *with* $(r,e)=1$,

$$\sum_{\substack{1 \le i \le [e/2] \\ (i,e)=1}} \left\{(e-2i)\binom{2if}{if} + 2i(-1)^{if}\binom{(e-i)f}{if}\right\} \equiv e \cdot \mathrm{tr}_{K/\mathbb{Q}}\left(2\Re J_e(r,r) - \frac{p}{2\Re J_e(r,r)}\right) \pmod{p^2},$$

where $\mathrm{tr}_{K/\mathbb{Q}}(x)$ *is the trace of* x *in the maximal real subfield* $K = \mathbb{Q}(\zeta_e + \zeta_e^{-1})$ *of* $\mathbb{Q}(\zeta_e)$ *over* $\mathbb{Q}$ *and* $\Re z = \mathrm{tr}_{\mathbb{Q}(\zeta_e)/K}(z)/2$ *is the real part of* z.

Proof. By Proposition 2, we have

$$\begin{aligned}\binom{2if}{if} &\equiv J_e(i,i)\left\{1 + (2iB_{2i} - 2iB_i)\,\frac{p}{e}\right\} \\ &\equiv J_e(i,i)\left\{1 + 2i(B_{2i} - B_i)\,\frac{p}{e}\right\} \pmod{\mathcal{P}^2}.\end{aligned}$$

Since $B_e = \sum_{i=1}^{p-1}(1/i) \equiv 0 \pmod{p}$, we obtain $B_{e-i} \equiv B_i \pmod{p}$ and

$B_{e-2i} \equiv B_{2i} \pmod{p}$. Then, by Proposition 2, we have

$$\begin{aligned}\binom{(e-i)f}{if} &\equiv J_e(e-2i,i)\left\{1+((e-i)B_{e-i}-(e-2i)B_{e-2i}-iB_i)\,\frac{p}{e}\right\}\\ &\equiv J_e(e-2i,i)\left\{1-(e-2i)(B_{2i}-B_i)\,\frac{p}{e}\right\} \pmod{\mathcal{P}^2}.\end{aligned}$$

Hence, by Proposition 1(b) we obtain

$$(3)\qquad (e-2i)\binom{2if}{if}+2i(-1)^{if}\binom{(e-i)f}{if} \equiv eJ_e(i,i) \pmod{\mathcal{P}^2}.$$

Put $J_e(i,i) = R_i + S_i\sqrt{-1} \in \mathbb{Q}(\zeta_e)$, where R_i and S_i are real numbers. By Proposition 1(e), for any $1 \le i \le [e/2]$, we have

$$\sigma_{e-1}(J_e(i,i)) = J_e(e-i,e-i) = R_i - S_i\sqrt{-1} \equiv 0 \pmod{\mathcal{P}},$$

so $R_i \equiv S_i\sqrt{-1} \pmod{\mathcal{P}}$. Then, by Proposition 1(c), we have

$$R_i - S_i\sqrt{-1} = \frac{p}{R_i+S_i\sqrt{-1}} \equiv \frac{p}{2R_i} \pmod{\mathcal{P}^2},$$

hence,

$$J_e(i,i) \equiv 2R_i - \frac{p}{2R_i} \pmod{\mathcal{P}^2}.$$

Since

$$\sum_{\substack{1\le i\le [e/2]\\ (i,e)=1}} \sigma_i(x) = \operatorname{tr}_{K/\mathbb{Q}}(x) \in \mathbb{Q}, \qquad x \in K = \mathbb{Q}(\zeta_e+\zeta_e^{-1}),$$

we have

$$\begin{aligned}\sum_{\substack{1\le i\le [e/2]\\ (i,e)=1}} J_e(i,i) &= \sum_i \sigma_i(J_e(r,r)) \equiv \sum_i \sigma_i\left(2R_r - \frac{p}{2R_r}\right) \pmod{p^2}\\ &\equiv \operatorname{tr}_{K/\mathbb{Q}}\left(2\Re J_e(r,r) - \frac{p}{2\Re J_e(r,r)}\right) \pmod{p^2},\end{aligned}$$

where r is an integer satisfying $1 \le r \le e-1$ and $(r,e)=1$. ∎

By the reduction modulo p, we obtain the following corollary which is a generalization of (1).

Corollary 1. *For* $1 \le r \le e-1$ *with* $(r,e)=1$,

$$\sum_{\substack{1\le i\le [e/2]\\ (i,e)=1}} \binom{2if}{if} \equiv \operatorname{tr}_{\mathbb{Q}(\zeta_e)/\mathbb{Q}}(J_e(r,r)) \pmod{p}.$$

4. The case of $e = 5$. Let p be a prime $\equiv 1 \pmod 5$. The properties of Jacobi sums of order 5 were shown by Dickson (see [2] and [3]). We know that

$$\begin{aligned} J_5(1,1) = & -\frac{1}{4}\{x + u(2\zeta_5 + 4\zeta_5^2 - 4\zeta_5^3 - 2\zeta_5^4) \\ & + v(4\zeta_5 - 2\zeta_5^2 + 2\zeta_5^3 - 4\zeta_5^4) + 5w\sqrt{5}\} \\ = & -\frac{1}{4}\{x + 5w\sqrt{5} + \sqrt{-1}(u\sqrt{50+10\sqrt{5}} + v\sqrt{50-10\sqrt{5}})\}, \end{aligned}$$

where (x, u, v, w) is one of four solutions of (2). Therefore,

$$\begin{aligned} \mathrm{tr}_{K/\mathbb{Q}}\left(2\Re J_e(1,1) - \frac{p}{2\Re J_e(1,1)}\right) &= \mathrm{tr}_{K/\mathbb{Q}}\left(-\frac{x+5w\sqrt{5}}{2} + \frac{2p}{x+5w\sqrt{5}}\right) \\ &\equiv -x\left(1 - \frac{4p}{x^2 - 125w^2}\right) \pmod{p^2}. \end{aligned}$$

Note that x and w^2 are invariants under the change of the solution of (2). By Theorem 1, we obtain the following theorem. Moreover, by Corollary 1, we obtain the congruence (1). For $p < 1000$, the values of x, u, v, w are given in [4].

THEOREM 2. *If $p = 5f + 1$ is prime and (x, w) is any solution of (2), then*

$$\binom{4f}{2f} + 2\binom{4f}{f} + 3\binom{2f}{f} + 4\binom{3f}{f} + 5x\left(1 - \frac{4p}{x^2 - 125w^2}\right) \equiv 0 \pmod{p^2}.$$

5. The case of $e = 7$. Let p be a prime $\equiv 1 \pmod 7$. We consider the triple of diophantine equations

$$(4)\qquad \begin{cases} 72p = 2a_1^2 + 42(a_2^2 + a_3^2 + a_4^2) + 343(a_5^2 + 3a_6^2), \\ 12(a_2^2 - a_4^2 + 2a_2a_3 - 2a_2a_4 + 4a_3a_4) \\ \qquad + 49(3a_5^2 + 2a_5a_6 - 9a_6^2) + 56a_1a_6 = 0, \\ 12(a_2^2 - a_4^2 + 4a_2a_3 + 2a_2a_4 + 2a_3a_4) \\ \qquad + 49(a_5^2 + 10a_5a_6 - 3a_6^2) + 28a_1(a_5 + a_6) = 0, \\ a_1 \equiv 1 \pmod 7. \end{cases}$$

This simultaneous system has six nontrivial solutions in addition to the two trivial solutions $(-6b_1, \pm 2b_2, \pm 2b_2, \mp 2b_2, 0, 0)$, where b_1 and b_2 are given by $p = b_1^2 + 7b_2^2$ and $b_1 \equiv 1 \pmod 7$. If $(a_1, a_2, a_3, a_4, a_5, a_6)$ is one of the six nontrivial solutions of (4), we know that for some r,

$$J_7(r,r) = c_1\zeta_7 + c_2\zeta_7^2 + c_3\zeta_7^3 + c_4\zeta_7^4 + c_5\zeta_7^5 + c_6\zeta_6$$

where

$$\begin{aligned} 12c_1 &= -2a_1 + 6a_2 + 7a_5 + 21a_6, & 12c_2 &= -2a_1 + 6a_3 + 7a_5 - 21a_6, \\ 12c_3 &= -2a_1 + 6a_4 - 14a_5, & 12c_4 &= -2a_1 - 6a_4 - 14a_5, \\ 12c_5 &= -2a_1 - 6a_3 + 7a_5 - 21a_6, & 12c_6 &= -2a_1 - 6a_2 + 7a_5 + 21a_6. \end{aligned}$$

The other five nontrivial solutions correspond to Jacobi sums $\sigma_i(J_7(r,r))$ for $2 \le i \le 6$. These results were proved by Leonard and Williams in [5]. For $p < 1000$, the values of $a_1, a_2, a_3, a_4, a_5, a_6$ are given in [4]. The right-hand side of the congruence in Theorem 1 is

$$(\sigma_1 + \sigma_2 + \sigma_3)(2R_r) + p\,\frac{(\sigma_1\sigma_2 + \sigma_2\sigma_3 + \sigma_3\sigma_1)(2R_r)}{(\sigma_1\sigma_2\sigma_3)(2R_r)}$$

where $2R_r = 2\Re J_7(r,r) = (\sigma_1 + \sigma_6)(J_7(r,r))$. By Theorem 1 and direct calculation, we obtain the following theorem.

THEOREM 3. *If $p = 7f+1$ is prime and $(a_1, a_2, a_3, a_4, a_5, a_6)$ is any nontrivial solution of* (4), *then*

$$\binom{6f}{3f} + 2\binom{6f}{2f} + 3\binom{4f}{2f} + 4\binom{5f}{2f} + 5\binom{2f}{f} + 6\binom{4f}{f} + 7\left(a_1 - \frac{18p(4a_1^2 - 343(a_5^2 + 3a_6^2))}{8a_1^3 - 2058a_1(a_5^2 + 3a_6^2) - 2041V}\right) \equiv 0 \pmod{p^2}$$

where $V = a_5^3 - 27a_5^2a_6 - 9a_5a_6^2 + 27a_6^3$.

The next corollary follows immediately from Corollary 1. It was shown by Hudson and Williams in [3].

COROLLARY 2. *If a_1 is given by* (4), *then*

$$\binom{2f}{f} + \binom{4f}{f} + \binom{4f}{2f} + a_1 \equiv 0 \pmod{p}.$$

6. The case of $e = 8$. Let p be a prime $\equiv 1 \pmod 8$. We can find the properties of Jacobi sums of order 8 in [1]. We know that

$$J_8(1,1) = C + D\sqrt{-2}, \qquad C \equiv \eta \pmod 4 \tag{5}$$

where

$$\eta = \begin{cases} 1 & \text{if 2 is a quartic residue } (\mathrm{mod}\ p), \\ -1 & \text{otherwise.} \end{cases}$$

But, since $\sigma_3(\sqrt{-2}) = \sqrt{-2}$ in $\mathbb{Q}(\zeta_8)$, we have $J_8(1,1) = J_8(3,3)$. From (3), we obtain

THEOREM 4. *If $p = 8f+1$ is prime and C is given uniquely by* (5), *then*

$$3\binom{2f}{f} + (-1)^f\binom{7f}{f} \equiv \binom{5f}{2f} + 3(-1)^f\binom{5f}{3f} \equiv 4\left(2C - \frac{p}{2C}\right) \pmod{p^2}.$$

References

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

[2] L. E. Dickson, *Cyclotomy higher congruences, and Waring's problem I, II*, Amer. J. Math. 57 (1935), 463–474.

[3] R. Hudson and K. S. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. 281 (1984), 431–505.

[4] T. Ishikawa, *On the number of zeros of diagonal forms*, Math. Comp. 64 (1995), 841–854.

[5] P. A. Leonard and K. S. Williams, *The cyclotomy numbers of order seven*, Proc. Amer. Math. Soc. 51 (1975), 295–300.

[6] A. R. Rajwade, *Some congruences in algebraic integers and rational integers*, Indian J. Pure Appl. Math. 7 (1976), 431–435.

[7] K. M. Yeung, *On congruences for binomial coefficients*, J. Number Theory 33 (1989), 1–17.

Department of Mathematics
Osaka Institute of Technology
Omiya, Asahi-ku, Osaka 535-8585, Japan
E-mail: ishikawa@ge.oit.ac.jp

Received on 28.2.2005 (4945)