PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 85, Number 2, June 1982

CAUCHY-TYPE CONGRUENCES FOR BINOMIAL COEFFICIENTS

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

ABSTRACT. In 1840 Cauchy [2] showed that for a prime $p = ef + 1$, $e = 20$,

$$\binom{10f}{f} \equiv \pm\binom{10f}{3f} \pmod{p},$$

and it was not until 1965 that Whiteman [6] succeeded in removing the sign ambiguity in this congruence.

In this paper we show how the Davenport-Hasse relation [3] in the form given by Yamamoto [8] can be used to resolve the sign ambiguity in other Cauchy-type congruences. Details are given just for $e = 8, 12$, and 20.

1. Introduction. Throughout this note e denotes a composite integer and p denotes a prime congruent to 1 modulo e, say, $p = ef + 1$.

For $p = 20f + 1$ the congruence

$$\binom{10f}{f} \equiv \pm\binom{10f}{3f} \pmod{p} \tag{1.1}$$

was established by L'Augustin Cauchy [2] in 1840. It was not until 125 years later that Whiteman [6] succeeded in removing the ambiguity in the sign in (1.1) by proving the following theorem.

THEOREM 1 (WHITEMAN). *Let* $p = 20f + 1 = a^2 + b^2$, $a \equiv 1 \pmod 4$. *Then*

$$\binom{10f}{f} \equiv \begin{cases} \binom{10f}{3f} \pmod{p}, & \text{if } b \equiv 0 \pmod 5, \\ -\binom{10f}{3f} \pmod{p}, & \text{if } a \equiv 0 \pmod 5. \end{cases} \tag{1.2}$$

The purpose of this note is to show how the Davenport-Hasse relation [3] in the form given by Yamamoto [8] can be used to resolve the sign ambiguity in other congruences similar to (1.1).

For $e = 8, 12$, and 20 and $p = ef + 1$, we determine the sign ambiguity in all congruences of the type

$$\binom{rf}{sf} \equiv \pm\binom{r'f}{s'f} \pmod{p}, \qquad 1 \le s < r \le e - 1, \quad 1 \le s' < r' \le e - 1, \tag{1.3}$$

excluding only those which can be deduced directly from the elementary properties of binomial coefficients.

Received by the editors December 4, 1980 and, in revised form, August 30, 1981.

1980 *Mathematics Subject Classification.* Primary 10A10; Secondary 10A99, 10C05.

Key words and phrases. Davenport-Hasse relation, sign ambiguities in Cauchy-type congruences, binomial coefficients (mod p).

[1]Research supported by Natural Sciences and Engineering Research Council Canada Grant A-7233.

0002-9939/82/0000-0035/$03.50

2. Preliminaries. Let $\xi_m = e^{2\pi i/m}$ and for $x \not\equiv 0 \pmod p$ define the index of x with respect to a primitive root g, written $\operatorname{ind}_g(x)$, to be the unique integer b such that $x \equiv g^b \pmod p$, $0 \le b \le p-2$. It follows from the Davenport-Hasse relation [3] that

$$\xi_m^{\operatorname{ind} g(n)} = \frac{G_e(n)\prod_{j=1}^{n-1} G_e(mj)}{\prod_{j=0}^{n-1} G_e(mj+1)}, \tag{2.1}$$

where $G_e(r)$ denotes the Gauss sum of order e defined for $e \nmid r$ and for a character $\chi_e \pmod p$ of order e by

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

Applying the work of Yamamoto [8, pp. 488–489] to (2.1) we obtain

$$n^{(p-1)/m} \equiv \frac{nf!\prod_{j=1}^{n-1}(mjf)!}{\prod_{j=0}^{n-1}(mj+1)f!} \pmod p. \tag{2.2}$$

In addition we require three elementary results. A simple modification of Wilson's theorem yields

$$sf!tf! \equiv (-1)^{sf-1} \equiv (-1)^{tf-1} \pmod p, \tag{2.3}$$

where s and t are positive integers with $s+t=e$. Making use of (2.3) and the elementary fact that $\binom{a}{b} = \binom{a}{a-b}$ it is straightforward to verify that for $1 \le s < r \le e-1$ we have

$$\begin{aligned}\binom{rf}{sf} &\equiv \binom{rf}{(r-s)f} \equiv (-1)^{(r+s)f}\binom{(e-s)f}{(e-r)f} \\ &\equiv (-1)^{(r+s)f}\binom{(e-s)f}{(r-s)f} \equiv (-1)^{sf}\binom{(e-r+s)f}{(e-r)f} \\ &\equiv (-1)^{sf}\binom{(e-r+s)f}{sf} \pmod p.\end{aligned} \tag{2.4}$$

Finally, (2.3) yields the following result. For integers g, h, and k satisfying $1 \le h < g \le e-1$, $1 \le h < k \le e-1$, $e-k > g-h$, we have

$$\binom{gf}{hf}\binom{(e-g)f}{(k-h)f} \equiv (-1)^{(g+k)f}\binom{kf}{hf}\binom{(e-k)f}{(g-h)f} \pmod p. \tag{2.5}$$

3. Congruences analogous to that of Cauchy. The following lemmas are easy consequences of (2.2).

LEMMA 3.1. *If $p = 2mf+1$ is prime then we have*

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

LEMMA 3.2. *If* $p = 3mf + 1$ *is prime then we have*

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

LEMMA 3.3. *If* $p = 5mf + 1$ *is prime then we have*

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

Taking $m = 4$ in Lemma 3.3 and applying (2.3) and (2.4) we have for $p = 20f + 1$,

$$\begin{aligned} 5^{(p-1)/4} &\equiv \frac{\binom{6f}{f}\binom{11f}{6f}}{\binom{8f}{3f}\binom{13f}{8f}} \equiv (-1)^f \frac{\binom{19f}{14f}\binom{14f}{5f}}{\binom{17f}{5f}\binom{15f}{8f}} \equiv (-1)^f \frac{19f!5f!12f!14f!7f!8f!}{5f!14f!17f!5f!9f!15f!} \\ &\equiv \frac{\binom{19f}{9f}\binom{10f}{f}}{\binom{17f}{7f}\binom{10f}{3f}} \pmod{p}, \end{aligned}$$

establishing Theorem 1 in view of the well-known criterion for 5 to be a fourth power modulo p, see, e.g., [5].

The following two theorems, which do not appear in Whiteman's papers [6, 7], may be established by arguments analogous to those in the above proof of Theorem 1. They are, as we now show, also simple consequences of (2.4), (2.5), and Theorem 1.

THEOREM 2. *Let* $p = 20f + 1 = a^2 + b^2$, $a \equiv 1 \pmod 4$. *Then*

$$\binom{7f}{f} \equiv \binom{9f}{3f} \quad \text{or} \quad -\binom{9f}{3f} \pmod{p}$$

according as $b \equiv 0 \pmod 5$ *or* $a \equiv 0 \pmod 5$.

PROOF. Using (2.5) with $g = 11$, $h = 10$, $k = 13$, we have

$$\binom{11f}{f}\binom{9f}{3f} \equiv \binom{13f}{10f}0\binom{7f}{f} \pmod{p}.$$

Appealing to (2.4) gives

$$\binom{10f}{f}\binom{9f}{3f} \equiv \binom{10f}{3f}\binom{7f}{f} \pmod{p},$$

from which Theorem 2 follows immediately in view of Theorem 1.

THEOREM 3. *Let* $p = 20f + 1 = a^2 + b^2$, $a \equiv 1 \pmod 4$. *Then*

$$\binom{3f}{f} \equiv \binom{9f}{2f} \quad \text{or} \quad -\binom{9f}{2f} \pmod{p}$$

according as $b \equiv 0 \pmod 5$ *or* $a \equiv 0 \pmod 5$.

PROOF. Taking $g = 17$, $h = 10$, $k = 11$ in (2.5) we have

$$\binom{17f}{10f}\binom{3f}{f} \equiv \binom{11f}{10f}\binom{9f}{7f} \pmod{p}.$$

Appealing to (2.4) gives

$$\binom{10f}{3f}\binom{3f}{f} \equiv \binom{10f}{f}\binom{9f}{2f} \pmod{p},$$

and again the theorem follows from Theorem 1.

The final two theorems illustrate the ideas used above in the cases $e = 8$ and 12. Using Lemma 3.1 with $m = 4$, (2.4), (2.5), and the well-known result of Gauss that $2^{(p-1)/4} \equiv (-1)^{b/4} \pmod{p}$ for primes p satisfying

$$p = 8f + 1 = a^2 + b^2, \quad a \equiv 1 \pmod{4},\ b \equiv 0 \pmod{4}, \tag{3.1}$$

we obtain

THEOREM 4. *Let p be a prime satisfying* (3.1). *Then*

$$\binom{2f}{f} \equiv (-1)^{f+b/4}\binom{4f}{f} \pmod{p}, \tag{3.2}$$

$$\binom{3f}{f} \equiv (-1)^{f+b/4}\binom{4f}{2f} \pmod{p}, \tag{3.3}$$

and

$$\binom{2f}{f} \equiv (-1)^{f}\binom{5f}{2f} \pmod{p}. \tag{3.4}$$

Similarly, using Lemma 3.2 with $m = 4$ and the result for 3 to be a fourth power (mod p), see, e.g., [5], we have the following theorem.

THEOREM 5. *Let p be a prime satisfying*

$$p = 12f + 1 = a^2 + b^2,\ a \equiv 1 \pmod{4},\ b \equiv 0 \pmod{2}.$$

We have

$$\binom{6f}{f} \equiv \binom{6f}{3f} \quad \text{or} \quad -\binom{6f}{3f} \pmod{p}, \tag{3.5}$$

and

$$\binom{3f}{f} \equiv \binom{5f}{2f} \quad \text{or} \quad -\binom{5f}{2f} \pmod{p} \tag{3.6}$$

according as $b \equiv 0 \pmod{3}$ or $a \equiv 0 \pmod{3}$.

Moreover, we have

$$\binom{4f}{f} \equiv (-1)^{f}\binom{7f}{3f} \pmod{p}, \qquad \binom{5f}{f} \equiv \binom{8f}{4f} \pmod{p}. \tag{3.7}$$

Congruence (3.5) in Theorem 5 is an immediate consequence of Lemma 3.2 with $m = 4$. Congruence (3.6) follows from (2.4), (2.5), and (3.5). To prove (3.7) we take $m = 3$ in Lemma 3.1 so that, using (2.4), we have

$$2^{(p-1)/3} \equiv \frac{\binom{4f}{2f}}{\binom{8f}{2f}} \equiv \frac{\binom{4f}{2f}}{\binom{6f}{2f}} \pmod{p}. \tag{3.8}$$

Next, taking $m = 6$ in Lemma 3.1 and using (2.4) and (2.5) we get

$$2^{(p-1)/6} \equiv \frac{\binom{2f}{f}}{\binom{7f}{f}} \equiv (-1)^f \frac{\binom{5f}{f}}{\binom{10f}{4f}} \equiv (-1)^f \frac{\binom{5f}{f}}{\binom{6f}{2f}} \pmod{p}. \tag{3.9}$$

Multiplying (3.8) and (3.9) together we obtain

$$2^{(p-1)/2} \equiv (-1)^f \equiv (-1)^f \frac{\binom{5f}{f}\binom{4f}{2f}}{\binom{6f}{2f}\binom{6f}{2f}} \pmod{p}. \tag{3.10}$$

Appealing to (2.5) with $g = 4$, $h = 2$, $k = 6$, we have

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

so that from (3.10),

$$\binom{5f}{f} \equiv \binom{8f}{4f} \pmod{p}. \tag{3.11}$$

Finally, using (2.5) with $g = 7$, $h = 3$, $k = 4$, we have

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

completing the proof of (3.7).

f	p	a	b	$\binom{6f}{f}$	$\binom{6f}{3f}$	$\binom{3f}{f}$	$\binom{5f}{2f}$	$\binom{4f}{f}$	$\binom{7f}{3f}$	$\binom{5f}{f}$	$\binom{8f}{4f}$
1	13	−3	2	6	7	3	10	4	9	5	5
3	37	1	6	2	2	10	10	35	2	11	11
5	61	5	6	10	10	14	14	10	51	60	60
6	73	−3	8	6	67	22	51	57	57	66	66
8	97	9	4	79	18	17	80	8	8	78	78

ACKNOWLEDGEMENT. The authors wish to express their thanks to Mr. Lee-Jeff Bell for computing a number of binomial coefficients (mod p).

REFERENCES

1. B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory **11** (1979), 349–398.
2. A. Cauchy, *Mémoire sur la théorie des nombres*, Mém. Institut de France **17** (1840), 249–278 (Ouevres completés (1) **3** (1911), 5–83).
3. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182.
4. C. F. Gauss, *Theoria residuorum biquadraticorum*, Werke, vol. 2, p. 90.

5. E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.
6. A. L. Whiteman, *Theorems on Brewer and Jacobsthal sums.* I, Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc., Providence, R.I., 1965, pp. 44–55.
7. ——, *Theorems on Brewer and Jacobsthal sums.* II, Michigan Math. J. **12** (1965), 65–80.
8. K. Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combin. Theory Ser. A **1** (1966), 476–489.

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