Czechoslovak Mathematical Journal

Jung-Jo Lee

Corrigendum to “Congruences for certain binomial sums”

Czechoslovak Mathematical Journal, Vol. 63 (2013), No. 2, 573–575

Persistent URL: http://dml.cz/dmlcz/143334

Czechoslovak Mathematical Journal, 63 (138) (2013), 573–575

CORRIGENDUM TO "CONGRUENCES FOR CERTAIN BINOMIAL SUMS"

JUNG-JO LEE, Seoul

(Received April 21, 2013)

Abstract. Theorem 1 of J.-J. Lee, Congruences for certain binomial sums. Czech. Math. J. 63 (2013), 65–71, is incorrect as it stands. We correct this here. The final result is changed, but the essential idea of above mentioned paper remains valid.

Keywords: central binomial coefficient, Legendre polynomial

MSC 2010: 05A10, 11B65

The following is a correction of Theorem 1 of [2].

Theorem 1. *Let p be a prime such that $p \geqslant 5$. Let $n = p^r - 1$ or $2p^r - 1$ with $r \geqslant 1$ an integer. Then*

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{2k}{k} \equiv \begin{cases} 1 \pmod p, & \text{if } p \equiv 1 \pmod 3; \\ (-1)^r \pmod p, & \text{if } p \equiv -1 \pmod 3. \end{cases}$$

The error occurs in Lemma 2 of the paper, and the following is a replacement to it.

Lemma 2. *Let $r \geqslant 1$ be a natural number, and p a prime number. Then*

$$\binom{p^r - 1}{k} \equiv (-1)^k \pmod p \quad \text{and} \quad \binom{2p^r - 1}{k} \equiv (-1)^k \pmod p. \tag{1}$$

P r o o f. We will prove the second case, and the first case can be proved similarly.

This research was suppported by NRF grant No. 2012-005700, Republic of Korea.

Let us write $2p^r - 1$ in base p, that is,

$$2p^r - 1 = p^r + (p-1)p^{r-1} + (p-1)p^{r-2} + \ldots + (p-1).$$

Also, write $k = k_0 + k_1 p + k_2 p + \ldots + k_d p^d$ in base p, where $d \leqslant r$.

Then the Lucas theorem (see [1]) tells us that

$$\binom{2p^r - 1}{k} \equiv \binom{p-1}{k_0} \cdots \binom{p-1}{k_d} \binom{p-1}{0} \cdots \binom{p-1}{0} \binom{1}{0} \pmod p. \tag{2}$$

Now, for any integer $m \leqslant p - 1$, observe that

$$\binom{p-1}{m} = \frac{(p-1)!}{m!(p-m-1)!} = \frac{\{(p-1)\ldots(p-m)\}(p-m-1)!}{m!(p-m-1)!} \equiv (-1)^m \pmod p.$$

Using this, we can simplify Formula (2) as

$$\binom{2p^r - 1}{k} \equiv (-1)^{k_0} \ldots (-1)^{k_d} = (-1)^{k_0 + \ldots + k_d} = (-1)^k \pmod p, \tag{3}$$

where the last equality is because $k_0 + \ldots + k_d \equiv k \pmod 2$. Notice that since p is an odd prime, $p \equiv 1 \pmod 2$. This proves the second case.

For the first case, write $p^r - 1$ in base p, that is,

$$p^r - 1 = (p-1)p^{r-1} + (p-1)p^{r-2} + \ldots + (p-1),$$

and the result follows in a similar way. □

Corresponding to this Lemma, we need to replace Formula (3.1) of [2], which is $\binom{rp^2-1}{k} = (-1)^k + p^2 f(k)$, by $\binom{p^r-1}{k} = (-1)^k + pf(k)$ or $\binom{2p^r-1}{k} = (-1)^k + pf(k)$, where $f\colon \mathbb{N} \to \mathbb{N}$ is a function defined on the set of natural numbers $\mathbb{N}$ (including 0).

To prove Theorem 1, we replace $rp^2 - 1$ in [2] by either $p^r - 1$ or $2p^r - 1$. Most of the calculations remain valid without any changes. However, Lemma 6 of [2] needs a slight modification in its statement as follows. It explains why the statement of our main theorem changes as given in Theorem 1.

Lemma 3. *Let p be a prime such that $p \geqslant 5$. Let $n = p^r - 1$ or $2p^r - 1$ with $r \geqslant 1$ an integer. Let*

$$S = (-\mathrm{i})^n \exp\Big(n \cdot \frac{5\pi}{6}\mathrm{i}\Big) \sum_{k=0}^{n} \exp\Big(\frac{4k\pi}{3}\mathrm{i}\Big).$$

Then $S = 1$ if $p \equiv 1 \pmod 3$, and $S = (-1)^r$ if $p \equiv -1 \pmod 3$.

Proof. Notice that in Lemma 6 of [2], S was defined as

$$S = (-\mathrm{i})^{rp^2-1} \exp\Big((rp^2 - 1) \cdot \frac{5\pi}{6}\mathrm{i}\Big) \sum_{k=0}^{rp^2-1} \exp\Big(\frac{4k\pi}{3}\mathrm{i}\Big).$$

The proof is also obtained by replacing $rp^2 - 1$ by either $p^r - 1$ or $2p^r - 1$. Only the final statement is changed according to the evaluations of trigonometric functions. In both cases of $n = p^r - 1$ and $2p^r - 1$, it follows that $S = 1$ if $p^r \equiv 1 \pmod 3$, and $S = -1$ if $p^r \equiv -1 \pmod 3$. Equivalently, $S = 1$ if $p \equiv 1 \pmod 3$, and $S = (-1)^r$ if $p \equiv -1 \pmod 3$. $\square$

Now, all the rest of the proofs in [2] are valid and we get the proof of Theorem 1.

Acknowledgement. I would like to express my gratitude to Professor David Callan for pointing out the error of my paper as soon as it was published on-line, and providing me useful comments.

References

[1] *A. Granville*: Arithmetic properties of binomial coefficients. I. Binomial Coefficients Modulo Prime Powers (J. Borwein et al., ed.). Organic mathematics. Proceedings of the workshop, Simon Fraser University, Burnaby, Canada, 1995, AMS, Providence, RI, 1997, pp. 253–276.

[2] *J.-J. Lee*: Congruences for certain binomial sums. Czech. Math. J. *63* (2013), 65–71.

Author's address: Jung-Jo Lee, Seoul National University, Seoul 151-742, South Korea, e-mail: jungjolee@gmail.com.