NOTE ON A CONGRUENCE INVOLVING PRODUCTS OF BINOMIAL COEFFICIENTS

Ping Xu
Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
pingxu_nju@yahoo.com.cn

Hao Pan
Department of Mathematics, Shanghai Jiaotong University, Shanghai 200240, People's Republic of China
haopan79@yahoo.com.cn

Received: 6/30/06, Revised: 1/4/07, Accepted: 1/18/07, Published: 1/31/07

Abstract

We prove that for integers $n, m \geqslant 2$ with $(n, 2m) = 1$,

$$(-1)^{\frac{\phi(n)(m-1)}{2}} \prod_{k=1}^{m-1} \prod_{d|n} \binom{d-1}{\lfloor dk/m \rfloor}^{\mu(n/d)} \equiv m(m^{\phi(n)} - 1) + 1 \pmod{n^2},$$

where $\phi(n)$ is the Euler totient function. This generalizes a result of Granville.

The Main Result

As early as 1895, Morley [4] proved a beautiful congruence as follows:

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

where $p \geqslant 5$ is a prime. In [2], Granville extended the result of Morley and showed that

$$(-1)^{\frac{(p-1)(m-1)}{2}} \prod_{k=1}^{m-1} \binom{p-1}{\lfloor pk/m \rfloor} \equiv m^p - m + 1 \pmod{p^2} \tag{2}$$

for any prime $p \geqslant 3$ and $m \geqslant 2$, where $\lfloor x \rfloor$ denotes the greatest integer not exceeding x. For further extensions of Granville's result, the reader may refer to [6]. A q-analogue of (2) has been established in [5].

With the help of a generalization of Lehmer's congruence, Cai [1] proved that

$$(-1)^{\phi(n)/2} \prod_{d|n} \binom{d-1}{(d-1)/2}^{\mu(n/d)} \equiv 4^{\phi(n)} \begin{cases} \pmod{n^3} & \text{if } 3 \nmid n, \\ \pmod{n^3/3} & \text{if } 3 \mid n, \end{cases} \tag{3}$$

for any odd positive integer n, where $\phi(n)$ is the Euler totient function. Inspired by Cai's result, in this note we generalize Granville's congruence (2) to arbitrary integers $n, m \geqslant 2$ with $(n, 2m) = 1$.

Theorem 1. *For any integers $n, m \geqslant 2$ with $(n, 2m) = 1$, we have*

$$(-1)^{\frac{\phi(n)(m-1)}{2}} \prod_{k=1}^{m-1} \prod_{d|n} \binom{d-1}{\lfloor dk/m \rfloor}^{\mu(n/d)} \equiv m(m^{\phi(n)}-1)+1 \pmod{n^2}.$$

First, we require a lemma on the quotients of Euler.

Lemma 2. *Let n be a positive integer and a be an integer with $(a, n) = 1$. Then*

$$\frac{a^{\phi(n)}-1}{n} \equiv \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \frac{1}{aj} \left\lfloor \frac{aj}{n} \right\rfloor \pmod{n}. \tag{4}$$

Proof. Let $1 \leqslant r_j \leqslant n$ be the least non-negative residue of aj modulo n for every $j \in \mathbb{Z}$. It is easy to see the set $\{r_j : 1 \leqslant j \leqslant n, (j,n) = 1\}$ coincides with $\{j : 1 \leqslant j \leqslant n, (j,n) = 1\}$, since if $j_1 \not\equiv j_2 \pmod{n}$ then $r_{j_1} \neq r_{j_2}$. Hence

$$\begin{aligned} a^{\phi(n)} &= \prod_{\substack{j=1\\(j,n)=1}}^{n} \frac{aj}{j} = \prod_{\substack{j=1\\(j,n)=1}}^{n} \frac{\lfloor aj/n \rfloor n + r_j}{j} = \prod_{\substack{j=1\\(j,n)=1}}^{n} \frac{r_j}{j}\left(1 + \frac{\lfloor aj/n \rfloor n}{r_j}\right) \\ &= \prod_{\substack{j=1\\(j,n)=1}}^{n} \left(1 + \frac{\lfloor aj/n \rfloor n}{r_j}\right) \equiv 1 + n \sum_{\substack{j=1\\(j,n)=1}}^{n} \frac{1}{r_j}\left\lfloor \frac{aj}{n} \right\rfloor \pmod{n^2} \\ &\equiv 1 + n \sum_{\substack{j=1\\(j,n)=1}}^{n} \frac{1}{aj}\left\lfloor \frac{aj}{n} \right\rfloor \pmod{n^2}. \end{aligned}$$

□

Remark. When n is a prime, the result of Lemma 2 was first discovered by Lerch [3].

Proof of Theorem 1. Let $P_d = \prod_{k=1}^{m-1} \binom{d-1}{\lfloor dk/m \rfloor}$ and $Q_d = \prod_{k=1}^{m-1} \prod_{\substack{j=1\\(j,d)=1}}^{\lfloor dk/m \rfloor} \left(\frac{d}{j} - 1\right)$. Then $P_n = \prod_{k=1}^{m-1} \prod_{j=1}^{\lfloor nk/m \rfloor} \left(\frac{n}{j} - 1\right) = \prod_{k=1}^{m-1} \prod_{d|n} \prod_{\substack{j=1\\(n,j)=d}}^{\lfloor nk/m \rfloor} \left(\frac{n}{j} - 1\right) = \prod_{d|n} Q_{n/d} = \prod_{d|n} Q_d$. By using the inverse formula for the Möbius function, $Q_n = \prod_{d|n} P_d^{\mu(n/d)} = \prod_{d|n} \prod_{k=1}^{m-1} \binom{d-1}{\lfloor dk/m \rfloor}^{\mu(n/d)}$. On the other hand, define $N = \sum_{k=1}^{m-1} |\{j : 1 \leqslant j \leqslant \lfloor nk/m \rfloor, (j,n) = 1\}|$ and apply Lemma 2 to get

$$\begin{aligned}(-1)^N Q_n = & \prod_{k=1}^{m-1} \prod_{\substack{j=1\\(j,n)=1}}^{\lfloor nk/m \rfloor} \left(1 - \frac{n}{j}\right) \equiv 1 - n \sum_{k=1}^{m-1} \sum_{\substack{j=1\\(j,n)=1}}^{\lfloor nk/m \rfloor} \frac{1}{j} \pmod{n^2} \\ = & 1 - n \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \frac{1}{j} \sum_{k=\lfloor mj/n \rfloor + 1}^{m-1} 1 = 1 - n \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \frac{m - 1 - \lfloor mj/n \rfloor}{j} \\ = & 1 - n(m-1) \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \frac{1}{j} + nm \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \frac{\lfloor mj/n \rfloor}{mj} \\ \equiv & m(m^{\phi(n)} - 1) + 1 \pmod{n^2},\end{aligned}$$

where the last congruence follows from

$$\sum_{\substack{j=1\\(j,n)=1}}^{n-1} \frac{1}{j} = \frac{1}{2} \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \left(\frac{1}{j} + \frac{1}{n-j}\right) = \frac{n}{2} \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \frac{1}{j(n-j)} \equiv 0 \pmod{n}.$$

Finally,

$$\begin{aligned}N = & \sum_{k=1}^{m-1} \sum_{\substack{j=1\\(j,n)=1}}^{\lfloor nk/m \rfloor} 1 = \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \sum_{k=\lfloor mj/n \rfloor + 1}^{m-1} 1 = \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \left(m - 1 - \left\lfloor \frac{mj}{n} \right\rfloor\right) \\ = & (m-1)\phi(n) - \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \left(\frac{mj}{n} - \left\{\frac{mj}{n}\right\}\right) \\ = & (m-1)\phi(n) - \sum_{\substack{j=1\\(j,n)=1}}^{n-1} \left(\frac{mj}{n} - \frac{j}{n}\right) = \frac{\phi(n)(m-1)}{2},\end{aligned}$$

where $\{x\} = x - \lfloor x \rfloor$. □

Acknowledgment. We are grateful to the anonymous referee for his/her valuable suggestions on this paper. We also thank our advisor, Professor Zhi-Wei Sun, for his helpful comments.

References

[1] Tianxin Cai, *A congruence involving the quotients of Euler and its applications (I)*, Acta Arith., **103**(2002).

[2] A. Granville, *Arithmetic Properties of Binomial Coefficients I: Binomial coefficients modulo prime powers*, in Organic mathematics (Burnady,BC,1995), CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253-276.

[3] M. Lerch, *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Math. Ann., **60**(1905),471-490.

[4] F. Morley, *Note on the congruence* $2^{4n} \equiv (-1)^n (2n)!/(n!)^2$, *where* $2n+1$ *is a prime*, Annals of Math., **9**(1895), 168-170.

[5] H. Pan, *A q-analogue of Lehmer's congruence*, preprint, arXiv:math.NT/0507511.

[6] Z.-W. Sun, *Products of binomial coefficients modulo* p^2, Acta Arith., **97**(2001), 87-98.