#A42 INTEGERS 11 (2011)

ON THE CONDITIONED BINOMIAL COEFFICIENTS

Liqun Tao
School of Mathematical Sciences, Luoyang Normal University, Luoyang, China
lqtao@lynu.edu.cn

Received: 12/24/10, Revised: 5/11/11, Accepted: 5/16/11, Published: 6/27/11

Abstract

We answer a question on the conditioned binomial coefficients raised in and article of Barlotti and Pannone, thus giving an alternative proof of an extension of Frobenius' generalization of Sylow's theorem.

1. Introduction

In [2], Barlotti and Pannone proved the following extension of Sylow's theorem [6]:

Theorem 1. *Let G be a finite group of order n, p a prime dividing n, H a subgroup of G of order p^h. Then for any positive integer $k > h$ such that $p^k \mid n$, the cardinality of the set of all the p-subgroups of G of order p^k containing H is congruent to one modulo p.*

In the special case $h = 0$, this result was first proved by Frobenius [3], and rediscovered by Krull [4].

The proof in [2] is given by considering the collection of all the subsets of G having cardinality p^k and containing exactly p^{k-h} right cosets of H.

It is worth pointing out that the above result was also proved independently by Spiegel [5] using Möbius inversion methods developed in Weisner's paper [7].

As suggested and finally raised as a question in [2], one should be able to show the result by considering the family of the subsets of G having order p^k and containing at least one right coset of H.

This leads to the following:

Definition 2 ([2]). Let a, b, c be positive integers such that $a \geq b \geq c$ and $c \mid a$. Let A be a set of cardinality a partitioned into subsets all of cardinality c. The conditioned binomial coefficient determined by a, b and c, denoted by

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

is defined to be the number of subsets of A of cardinality b containing at least one component of the partition.

The aim of this paper is to answer the question raised in [2], which asks to prove the following:

Theorem 3. *Let a, b, c be positive integers such that $c \mid b$ and $b \mid a$. Then*

(1) $\frac{a}{b}$ *divides* $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$.

(2) *If b is a power of a prime p, then* $\begin{pmatrix} a \\ b \\ c \end{pmatrix} / \frac{a}{b} \equiv 1 \pmod{p}$.

Remark 4. If $c = 1$, the conditioned binomial coefficient determined by a, b and c is just $\binom{a}{b}$. Then Theorem 3 follows from Lemmas 5 and 6 in the next section.

Our method of proof of the main result is to express the conditioned binomial coefficient explicitly as a combination of usual binomials and then consider the divisibility and congruence of these binomials (see (1) below). The method we use is very elementary.

We refer the reader to [1] (Chapters 2 and 6), or other standard algebra textbooks for terminology and notations used in the paper.

2. Proof of the Main Result

We will need the following two results. The first one can be verified directly; the second one is shown in [4], but we still give a proof here for the reader's convenience.

Lemma 5. *Let a, b be positive integers such that b divides a. Then $\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1}$.*

Lemma 6. *Let p be a prime, s a positive integer, and g a positive integer divisible by p^s. Then*

$$\binom{g-1}{p^s-1} \equiv 1 \pmod{p}.$$

Proof. We prove the result by induction on s, the exponent of p. For $s = 1$, since $p \mid g$, we have $g - i \equiv p - i \pmod{p}$ for $1 \le i < p$, and hence $(g-1)(g-2)\cdots(g-(p-1)) \equiv (p-1)(p-2)\cdots 1 \pmod{p}$. As $(p-1)(p-2)\cdots 1$ is prime to p, we get $\binom{g-1}{p-1} = \frac{(g-1)(g-2)\cdots(g-(p-1))}{(p-1)(p-2)\cdots 1} \equiv 1 \pmod{p}$.

Suppose that the result holds for exponents less than s. By straightforward computation we obtain the equality

$$\binom{g-1}{p^s-1} = \binom{\frac{g}{p}-1}{p^{s-1}-1} \prod_{j=0}^{p^{s-1}-1} \prod_{i=1}^{p-1} \frac{g-(jp+i)}{p^s-(jp+i)}.$$

Then the result follows by the induction hypothesis and the above argument for the case $s = 1$. □

Proof of Theorem 3. Let A be a set of cardinality a partitioned into subsets all of cardinality c. The number of subsets of A of cardinality b containing no component of the partition is

$$\sum_{\substack{0\le n_i<c\\ n_1+n_2+\cdots+n_{\frac{a}{c}}=b}} \binom{c}{n_1}\binom{c}{n_2}\cdots\binom{c}{n_{\frac{a}{c}}},$$

which is the coefficient of the term x^b in $((1+x)^c-x^c)^{\frac{a}{c}}$. The coefficient equals

$$\sum_{r=0}^{\frac{b}{c}}\binom{\frac{a}{c}}{r}\binom{(\frac{a}{c}-r)c}{b-rc}(-1)^r.$$

Then

$$\left(\begin{array}{c} a\\ b\\ c\end{array}\right)=\binom{a}{b}-\sum_{r=0}^{\frac{b}{c}}\binom{\frac{a}{c}}{r}\binom{(\frac{a}{c}-r)c}{b-rc}(-1)^r=\sum_{r=1}^{\frac{b}{c}}(-1)^{r-1}A_r, \tag{1}$$

where $A_r=\binom{\frac{a}{c}}{r}\binom{(\frac{a}{c}-r)c}{b-rc}$.

For $1\le r\le\frac{b}{c}$, by Lemma 5, we have $A_r=\frac{\frac{a}{c}}{r}\binom{\frac{a}{c}-1}{r-1}\binom{(\frac{a}{c}-r)c}{b-rc}$, hence $\frac{a}{c}\mid rA_r$. On the other hand, by Lemma 5 again, we have

$$\begin{aligned} A_r &= \binom{\frac{a}{c}}{\frac{a}{c}-r}\binom{(\frac{a}{c}-r)c}{b-rc}\\ &= \frac{\frac{a}{c}}{\frac{a}{c}-r}\binom{\frac{a}{c}-1}{\frac{a}{c}-r-1}\frac{(\frac{a}{c}-r)c}{b-rc}\binom{(\frac{a}{c}-r)c-1}{b-rc-1}\\ &= \frac{\frac{a}{c}}{\frac{b}{c}-r}\binom{\frac{a}{c}-1}{\frac{a}{c}-r-1}\binom{(\frac{a}{c}-r)c-1}{b-rc-1}. \end{aligned}$$

Thus, $\frac{a}{c}\mid(\frac{b}{c}-r)A_r$. Therefore we have that $\frac{\frac{a}{c}}{(\frac{b}{c}-r,r)}=\frac{\frac{a}{c}}{(\frac{b}{c},r)}$ divides A_r. *A fortiori*, $\frac{\frac{a}{c}}{\frac{b}{c}}=\frac{a}{b}$ divides A_r.

So we obtain

$$\frac{a}{b}\mid\left(\begin{array}{c} a\\ b\\ c\end{array}\right).$$

This completes the proof of the first part of the theorem.

For the second part, in view of Remark 4, we may assume that $a=mp^h, b=p^k, c=p^h$ are positive integers, where p is a prime and $k>h\ge 1$.

From (1), we have

$$\begin{pmatrix} mp^h \\ p^k \\ p^h \end{pmatrix} = \binom{mp^h}{p^k} - \sum_{r=0}^{p^{k-h}} (-1)^r B_r,$$

where $B_r = \binom{m}{r}\binom{(m-r)p^h}{p^k - rp^h}$, and for $1 \le r < p^{k-h}$, $\frac{m}{(p^{k-h},r)}$ divides B_r. Hence $\frac{m}{p^{k-h-1}}$ divides B_r, which implies that $B_r / \frac{mp^h}{p^k} \equiv 0 \pmod{p}$, for $1 \le r < p^{k-h}$.

By Lemmas 5 and 6,

$$\binom{mp^h}{p^k} = \frac{mp^h}{p^k}\binom{mp^h - 1}{p^k - 1},$$

hence,

$$\binom{mp^h}{p^k} \Big/ \frac{mp^h}{p^k} \equiv 1 \pmod{p}.$$

By the same argument,

$$\binom{m}{p^{k-h}} \Big/ \frac{mp^h}{p^k} \equiv 1 \pmod{p}.$$

Thus whether p is an odd prime or not, we have

$$\frac{B_0 + B_{p^{k-h}}(-1)^{p^{k-h}}}{\frac{mp^h}{p^k}} \equiv 0 \pmod{p}.$$

Putting the above facts together, we get

$$\begin{pmatrix} mp^h \\ p^k \\ p^h \end{pmatrix} \Big/ \frac{mp^h}{p^k} \equiv 1 \pmod{p}.$$

□

Remark. As mentioned at the beginning of the paper, we may prove Theorem 1 by considering $F'_H(p^k)$, the family of the subsets of G having order p^k and containing at least one right coset of H. Let $S_H(p^k)$ be the set of all the p-subgroups of G of order p^k containing H. Consider the right-multiplication action of G on $F'_H(p^k)$. Then $F'_H(p^k)$ is partitioned as a union of orbits:

$$F'_H(p^k) = \bigcup_{i=1}^{l} \mathcal{O}_{U_i}.$$

Note that $|Stab(U_i)|$ divides $|U_i| = p^k$, and $|Stab(U_i)| = p^k$ if and only if $\mathcal{O}_{U_i}$ contains a (unique) subgroup K of order p^k, and hence consists of right cosets of K. Since K contains some right coset of H, actually $K \supset H$. Thus we have

$$|F'_H(p^k)| = \sum_{i=1}^{l} \frac{|G|}{|Stab(U_i)|} = \frac{|G|}{p^k}(|S_H(p^k)| + \text{multiple of } p).$$

Applying Theorem 3 to the case $a = |G| = mp^h, b = p^k, c = |H| = p^h$, we obtain

$$|F'_H(p^k)|/\tfrac{mp^h}{p^k} = \begin{pmatrix} mp^h \\ p^k \\ p^h \end{pmatrix} /\tfrac{mp^h}{p^k} \equiv 1 \,(\mathrm{mod}\ p).$$

Thus

$$S_H(p^k) \equiv 1 \,(\mathrm{mod}\ p)$$

as desired.

Acknowledgement. This work is partially supported by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry and Research Seed Fund of Luoyang Normal University for Provincial or Ministry level project. The author is very grateful to the referee for helpful comments and suggestions.

References

[1] M. Artin, Algebra, Prentice-Hall, 1991.

[2] M. Barlotti and V. Pannone, Sylow's theorem and the arithmetic of binomial coefficients, *Note di Matematica* **22** (2003), 83-87.

[3] G. Frobenius, Verallgemeinerung des Sylowschen Satze, *Berliner Sitz*, (1895), 981-993.

[4] W. Krull, Über die p-Untergruppen, *Archiv der Math*, **12** (1961), 1-6.

[5] E. Spiegel, Another Look at Sylow's Third Theorem, *Math. Mag* **77** (2004), 227-232.

[6] M. L. Sylow, Théoremès sur les groupes de substitutions, *Math. Ann.* **5** (1872), 584-594.

[7] L. Weisner, Some properties of prime power groups, *Trans. Amer. Math. Soc.* **38** (1935), 485-492.