# 二項係数の合同関係

宮川　幸隆

平成19年12月31日

## 1　序文

本稿の目的は，二項係数の或る合同関係の証明です．本稿で考察するパスカル三角形の第1段の数の配列は1,1;　第2段の数の配列は1,2,1;　…;　一般に，　第$n$段の数の配列は

$$1,\left(\begin{array}{c} n \\ 1 \end{array}\right),\left(\begin{array}{c} n \\ 2 \end{array}\right),\cdots,\left(\begin{array}{c} n \\ n-1 \end{array}\right),1$$

であるとします．

筆者は，　上述のパスカル三角形で色々と実験している内に，　次の定理1.1を帰納的に発見しました．その定理は有理素数$p$に関するものですが，　$p=2$のときの証明は，　最後の詰めが詰め切らないまま本講演に臨む結果となりました．

実は，　$p$が奇素数のときに限定すれば，　筆者の証明法でも完全であり，　筆者は，　それ（$p$を奇素数のときに限定したもの）を日本評論社の「数学セミナー」誌に2006年の暮れに投稿したのですが，　何の音沙汰も無いままに数ヶ月が過ぎました．　そこで，　切手を貼った返信用封筒を「数学セミナー」編集部に二回も送って問い合わせをしたのですが，　更には，　2007年の3月には日本評論社まで出向いて「数学セミナー」編集部員に面会を申し出たのですが全員が春の学会に出掛けていると言うことで編集部員に会うことも叶いませんでした．　それにも拘わらず完全に無視されたまま今日に至って居ります．　誠に不誠実極まりない対応という他はありません．

それに引き換え，　本講演においては，　講演後に次の定理1.1について御存知かどうかをお尋ねしましたところ，　法政大学の斎藤正顕さんから、Internat. J. Math. and Math. Sci. VOL 11 No. 4 (1988) 743-750にあるNEVILLE ROBBINSのSOME CONGRUENSE PROPERTIES OF BINOMIAL COEFFICIENTS AND LINEAR SECOND ORDER RECURRENCESの中のTHEOREM 2.1. が関連があるのではないかとの御指摘を受けることが出来ました．　更には，　この「数学史シンポジウム」の世話人の一人であられる長岡一昭氏から次の定理1.1の完璧な証明を郵送して頂きました．

上述の論文「SOME CONGRUENSE PROPERTIES OF BINOMIAL COEFFICIENTS AND LINEAR SECOND ORDER RECURRENCES」は，　後ほど，　参考文献として掲げますが，　その中のTHEOREM 2.1. が本稿の主定理であるところの定理1.1を証明している訳では決して無いのです．　本稿の主定理であるところの定理1.1は，　あくまでも長岡一昭氏が証明された，　後述の補助定理2.2に拠って証明されるのです．

私事で恐縮ですが，　長岡一昭氏は私の学部・修士時代の先輩であり，　当時も色々と御指導頂いたのですが，　今回もまた御指導頂いた訳でして，　法政大学の斎藤正顕さんから御指摘を頂きましたことと併せて，　今回の「数学史シンポジウム」で講演させて頂いて本当に良かったと思って居ります．　本稿の目的は，次の定理1.1と，　その長岡一昭氏に拠る証明の紹介です:

**定理 1.1**　$p$を素数，　$k$を2以上の自然数とし，　$l$を$k$以上の自然数とする．
パスカル三角形の第$p^{l-1}$段の二項係数の配列は，

$$1,\binom{p^{l-1}}{1},\binom{p^{l-1}}{2},\cdots,\binom{p^{l-1}}{p^{l-1}-1},1$$

であり，　第$p^l$段の二項係数の配列は，

$$1,\binom{p^l}{1},\binom{p^l}{2},\cdots,\binom{p^l}{p-1},$$

$$\binom{p^l}{p},\binom{p^l}{p+1},\binom{p^l}{p+2},\cdots,\binom{p^l}{2p-1},$$

$$\binom{p^l}{2p},\binom{p^l}{2p+1},\binom{p^l}{2p+2},\cdots,\binom{p^l}{3p-1},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$\binom{p^l}{(p^{l-1}-1)p},\binom{p^l}{(p^{l-1}-1)p+1},\cdots,\binom{p^l}{p^l-1},\ 1$$

であるが，

$$\binom{p^{l-1}}{1}\equiv\binom{p^l}{p}\pmod{p^k}$$

$$\binom{p^{l-1}}{2}\equiv\binom{p^l}{2p}\pmod{p^k},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$\binom{p^{l-1}}{p^{l-1}-1}\equiv\binom{p^l}{(p^{l-1}-1)p}\pmod{p^k},$$

$$\binom{p^l}{1}\equiv\binom{p^l}{2}\equiv\cdots\equiv\binom{p^l}{p-1}\equiv 0\pmod{p^k},$$

$$\binom{p^l}{p+1}\equiv\binom{p^l}{p+2}\equiv\cdots\equiv\binom{p^l}{2p-1}\equiv 0\pmod{p^k},$$

$$\binom{p^l}{2p+1}\equiv\binom{p^l}{2p+2}\equiv\cdots\equiv\binom{p^l}{3p-1}\equiv 0\pmod{p^k},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$\binom{p^l}{(p^{l-1}-1)p+1}\equiv\cdots\equiv\binom{p^l}{p^l-1}\equiv 0\pmod{p^k}$$

が成り立つ．

これだけでは，何のことか解りにくいと思いますので具体例で説明しますと，

本稿で考察したパスカル三角形の，

例えば，第2段の二項係数の，一番左からど真ん中までの各数を4で割ったときの余りを列挙すると

1，2であり，

第4段の二項係数の，一番左からど真ん中までの各数を4で割ったときの余りを列挙すると

1，0，2，

第8段の二項係数の，一番左からど真ん中までの各数を4で割ったときの余りを列挙すると

1，0，0，0，2，

第16段の二項係数の，一番左からど真ん中までの各数を4で割ったときの余りを列挙すると

1，0，0，0，0，0，0，0，2，

第32段の二項係数の，一番左からど真ん中までの各数を4で割ったときの余りを列挙すると

1，0，0，0，0，0，0，0，0，0，0，0，0，0，0，0，2であって，

また，例えば，第4段の二項係数の，一番左からど真ん中までの各数を8で割ったときの余りを列挙すると

1，4，6であり，

第8段の二項係数の，一番左からど真ん中までの各数を8で割ったときの余りを列挙すると

1，0，4，0，6，

第16段の二項係数の，一番左からど真ん中までの各数を8で割ったときの余りを列挙すると

1，0，0，0，4，0，0，0，6，

第32段の二項係数の，一番左からど真ん中までの各数を8で割ったときの余りを列挙すると

1，0，0，0，0，0，0，0，4，0，0，0，0，0，0，0，6であって，

また，例えば，第3段の二項係数の，一番左からど真ん中までの各数を9で割ったときの余りを列挙すると

1，3であり，

第9段の二項係数の，一番左からど真ん中までの各数を9で割ったときの余りを列挙すると

1，0，0，3，0，

第27段の二項係数の，一番左からど真ん中までの各数を9で割ったときの余りを列挙すると

1，0，0，0，0，0，0，0，0，3，0，0，0，0であって，

また，例えば，第8段の二項係数の，一番左からど真ん中までの各数を16で割ったときの余りを列挙すると

1，8，12，8，6であり，

第16段の二項係数の，一番左からど真ん中までの各数を16で割ったときの余りを列挙すると

1，0，8，0，12，0，8，0，6，

第32段の二項係数の，一番左からど真ん中までの各数を16で割ったときの余りを列挙すると

1，0，0，0，8，0，0，0，12，0，0，0，8，0，0，0，6であって，

また，例えば，第5段の二項係数の，一番左からど真ん中までの各数を25で割ったときの余りを列挙すると

1，5，10であり，

第25段の二項係数の，一番左からど真ん中までの各数を25で割ったときの余りを列挙すると

1，0，0，0，0，5，0，0，0，0，10，0，0であって，

また，例えば，第9段の二項係数の，一番左からど真ん中までの各数を27で割ったときの余りを列挙すると

1, 9, 9, 3, 18であり，

第27段の二項係数の，一番左からど真ん中までの各数を27で割ったときの余りを列挙すると

1, 0, 0, 9, 0, 0, 9, 0, 0, 3, 0, 0, 18, 0であって，

また，例えば，第16段の二項係数の，一番左からど真ん中までの各数を32で割ったときの余りを列挙すると

1, 16, 24, 16, 28, 16, 8, 16, 6であり，

第32段の二項係数の，一番左からど真ん中までの各数を32で割ったときの余りを列挙すると

1, 0, 16, 0, 24, 0, 16, 0, 28, 0, 16, 0, 8, 0, 16, 0, 6です.

## 2 証明

（後半部）先ず，次の補助定理を示します：

**補助定理 2.1** $n$, $a$を自然数とするとき，$0 < a < n$かつ$(n, a) = 1$ならば，

$$\left( \begin{array}{c} n \\ a \end{array} \right) \equiv 0 \pmod{n}$$

が成り立つ.

証明] 先ず，

$$\left( \begin{array}{c} n \\ a \end{array} \right) = \frac{n}{a} \left( \begin{array}{c} n-1 \\ a-1 \end{array} \right)$$

であり，

$$\left( \begin{array}{c} n \\ a \end{array} \right)$$

も

$$\left( \begin{array}{c} n-1 \\ a-1 \end{array} \right)$$

も自然数です．そして，$a = p_1^{e_1} \cdots p_r^{e_r}$を$a$の素因数分解とするとき，$(n, a) = 1$から，$p_1^{e_1}, \cdots, p_r^{e_r}$は全て自然数

$$\left( \begin{array}{c} n-1 \\ a-1 \end{array} \right)$$

の約数です．よって，

$$\frac{1}{a} \left( \begin{array}{c} n-1 \\ a-1 \end{array} \right)$$

は自然数であり，この補助定理の成立が解ります.

q.e.d.

この補助定理で，$n = p^l$とすれば，定理の後半部の成立がわかります.

（前半部）

前述の Internat. J. Math. and Math. Sci. VOL 11 No. 4 (1988) 743-750 にある NEVILLE ROBBINS の SOME CONGRUENSE PROPERTIES OF BINOMIAL COEFFICIENTS AND LINEAR SECOND ORDER RECURRENCES の中の THEOREM 2.1. を証明する時に使われる Lemma 2.1 とは，次の様なものです.

**Lemma 2.1** $p$ を素数，$a$，$b$ を自然数とし，$n$，$m$ を整数とするとき，$0 \leq m \leq n$ かつ $0 < b < ap^{n-m}$ かつ $p$ が $ab$ を割り切らないならば，

$$\left( \begin{array}{c} ap^n \\ bp^m \end{array} \right) \equiv (-1)^{b(p^m-1)} \left( \begin{array}{c} ap^{n-m} \\ b \end{array} \right) \pmod{p^n}$$

が成り立つ.

この Lemma で，$a = m = 1$ とすると，

**Lemma 2.2** $p$ を素数，$b$，$n$ を自然数とするとき，$0 < b < p^{n-1}$ かつ $p$ が $b$ を割り切らないならば，

$$\left( \begin{array}{c} p^n \\ bp \end{array} \right) \equiv (-1)^{b(p-1)} \left( \begin{array}{c} p^{n-1} \\ b \end{array} \right) \pmod{p^n}$$

が成り立つ.

というものになりますが，長岡一昭氏は，この Lemma 2.2 よりも更に強力な次の補助定理を証明されました：

**補助定理 2.2** $p$ を素数，$b$，$n$ を自然数とするとき，$0 < b < p^{n-1}$ ならば，

$$\left( \begin{array}{c} p^n \\ bp \end{array} \right) \equiv (-1)^{b(p-1)} \left( \begin{array}{c} p^{n-1} \\ b \end{array} \right) \pmod{p^n}$$

が成り立つ.

証明] 先ず，自然数 $m$，$a$ が $(m,a) = 1$ を満たすとき，$ax \equiv 1 \pmod{m}$ を満たす自然数 $x(0 < x < m)$ を $a^{-1}$ と書くことにします．このとき，$a|c$ ならば，

$$\frac{c}{a} \equiv ca^{-1} \pmod{m}$$

が成り立ちます．次に，

$a$ 個の異なるものから $r$ 個を選んで並べて得られる順列の総数を $[a;r]$ と表すことにし，$r$ 個の連続した整数の積

$$a(a+1)\cdots(a+r-1)$$

を $(a;r)$ と表すことにします．さて，$0 < b < p^{n-1}$ とし，

$$\left( \begin{array}{c} p^n \\ bp \end{array} \right) = \frac{p^n[p^n-1;p-1]}{(1;p-1)p} \frac{(p^n-p)[p^n-(p+1);p-1]}{(p+1;p-1)2p} \cdots \frac{(p^n-(b-1)p)[p^n-((b-1)p+1);p-1]}{((b-1)p+1;p-1)bp}$$

$$= \left( \begin{array}{c} p^{n-1} \\ b \end{array} \right) \frac{[p^n-1;p-1]}{(1;p-1)} \frac{[p^n-(p+1);p-1]}{(p+1;p-1)} \cdots \frac{[p^n-((b-1)p+1);p-1]}{((b-1)p+1;p-1)}$$

であることに注意しましょう.

ここで, $0 \leq c \leq b-1$ なる整数 $c$ に対して,

$$[p^n-(cp+1);p-1]=(p^n-(cp+1))(p^n-(cp+2))\cdots(p^n-(cp+p-1))$$

$$\equiv(-1)^{p-1}(cp+1)(cp+2)\cdots(cp+p-1)=(-1)^{(p-1)}(cp+1;p-1) \pmod{p^n}$$

であり, $(p^n,(1;p-1)(p+1;p-1)\cdots((b-1)p+1;p-1))=1$ であって,
$(1;p-1)(p+1;p-1)\cdots((b-1)p+1;p-1)$ は

$$\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right)[p^n-1;p-1][p^n-(p+1);p-1]\cdots[p^n-((b-1)p+1);p-1]$$

の約数であるから,

$$\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right)\frac{[p^n-1;p-1]}{(1;p-1)}\frac{[p^n-(p+1);p-1]}{(p+1;p-1)}\cdots\frac{[p^n-((b-1)p+1);p-1]}{((b-1)p+1;p-1)}$$

$$\equiv\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right)[p^n-1;p-1][p^n-(p+1);p-1]\cdots[p^n-((b-1)p+1);p-1]$$
$$\times((1;p-1)(p+1;p-1)\cdots((b-1)p+1;p-1))^{-1}$$

$$\equiv\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right)(-1)^{b(p-1)}(1;p-1)(p+1;p-1)\cdots((b-1)p+1;p-1)$$
$$\times((1;p-1)(p+1;p-1)\cdots((b-1)p+1;p-1))^{-1}$$

$$\equiv\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right)(-1)^{b(p-1)} \pmod{p^n},$$

すなわち,

$$\left(\begin{array}{c} p^n \\ bp \end{array}\right)\equiv(-1)^{b(p-1)}\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right) \pmod{p^n}$$

が成り立って, 補助定理 2.2 は示されました.

q.e.d.

この補助定理 2.2 から, $p$ が奇数の場合と $p=2$ で $b$ が偶数の場合は定理 1.1 の（前半部）が示されました. また, $p=2$ で $b$ が奇数の場合は, 補助定理 2.1 から,

$$\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right)\equiv 0 \pmod{p^{n-1}}$$

が成り立ちますから,

$$\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right)\equiv-\left(\begin{array}{c} p^{n-1} \\ b \end{array}\right) \pmod{p^n},$$

したがって, この場合も定理 1.1 の（前半部）が示されました.

定理 1.1 の証明終り

## 3 参考文献


NEVILLE ROBBINS,

SOME CONGRUENSE PROPERTIES OF BINOMIAL COEFFICIENTS AND LINEAR SECOND ORDER RECURRENCES,

Internat. J. Math. and Math. Sci. VOL 11 No. 4 (1988) 743-750