二項係数のある性質

松 坂 和 夫

§1 mod 2 によるパスカルの三角形

この小文では二項係数についての二三の簡単な性質を述べる．これらはいわば“数学のこぼれ話”のようなささやかな話に過ぎない．また，内容の一部には，数年前数学セミナー誌上に問題として提出したものもある．しかし，まだまとまった形では書いていないし，今までの書物には見当らない性質もあるように思われるので，ここに一応まとめて記録しておきたいと思う．

問題の出発点はパスカルの三角形の mod 2 による構成である．すなわち，通常のように各行の両端にはいつも 1 をおいてパスカルの三角形を作るのであるが，1 つの行から次の行に移るときに

$$0+0=1+1=0,\quad 1+0=0+1=0$$

という演算を用いるのである．

n=1……1　1
n=2……1　0　1
n=3……1　1　1　1
n=4……1　0　0　0　1
n=5……1　1　0　0　1　1
n=6……1　0　1　0　1　0　1
n=7……1　1　1　1　1　1　1　1
n=8……1　0　0　0　0　0　0　0　1
⋮　　⋮

この図式はいうまでもなく二項係数 $\binom{n}{r}$ の奇偶を 2 つの数字によって区別するものにほかならない．すなわち，普通のパスカルの三角形において $\binom{n}{r}$ が奇数であるところには 1，偶数であるところには

0 が書かれているわけである.

ところで上の図式にみられるように, $n=3$ や $n=7$ に対応する行では 1 だけが並んでいる. このように 1 だけが並ぶ行はどのような n に対応しているかということをまず問題にしよう. いいかえれば, $\binom{n}{r}$ $(0\leqq r\leqq n)$ がすべて奇数であるような整数 $n\geqq 1$ は何か, という問題である.

n のかわりにその次の行を考えれば, 明らかに上の問題は, 両端以外はすべて 0 であるような行を求めること, すなわち $\binom{n}{r}$ $(0<r<n)$ がすべて偶数であるような整数 $n\geqq 1$ を求めることと同じである.

これについて次の定理が成り立つ.

定理 1 $\binom{n}{r}$ $(0<r<n)$ がすべて偶数であるためには, $n=2^k(k\geqq 1)$ であることが必要十分である.

(証明) 標数 2 の体, たとえば素体 $\boldsymbol{Z}/(2)$ を考える. x を不定元とすれば, $\binom{n}{r}$ $(0<r<n)$ がすべて偶数であることは, この体 $\boldsymbol{Z}/(2)$ において (正確にはこの体の上の多項式環において)

$$(1)\qquad (x+1)^n=x^n+1$$

が成り立つことにほかならない.

$n=2^k$ ならば, 標数 2 の体における基本的な演算公式によってたしかに (1) が成り立つ.

また $n\neq 2^k$ ならば, $n=2^k l$, $l>1$, l は奇数, と書くことができ,

$$\begin{aligned}(x+1)^n&=[(x+1)^{2^k}]^l=(x^{2^k}+1)^l\\&=x^{2^k l}+lx^{2^k(l-1)}+\cdots\cdots+1\end{aligned}$$

となる. ここで l は奇数であるから, $x^{2^k(l-1)}$ の係数は ($\boldsymbol{Z}/(2)$ において) 1 に等しい. よってこの場合は (1) は成り立たない. (証明終)

系 $\binom{n}{r}$ $(0\leqq r\leqq n)$ がすべて奇数であるためには, $n=2^k-1(k\geqq 1)$ であることが必要十分である.

定理 1 の証明に用いたのは, 標数 2 の体においては

$$(2)\qquad (x+1)^{2^k}=x^{2^k}+1$$

が成り立つという代数学で周知の定理である. しかし, 考えてみれば, 定理 1 はほとんどこの定理と同等の内容をもつものであって, 実質的

には単に後者をいいかえただけに過ぎない．けれども，通常の代数学の書物では，(2) は基本的公式として書かれているが，それを定理1のような形に述べかえてあることは少ないので，定理1（あるいはその系）のような表現は一見みあたらしく思われるのである．（ヴィノグラドフの整数論入門では第1章の問題 12 に上の定理1がのっている．しかし，その解答に用いられている帰納法はかなり難解で，普通 (2) を証明するときに用いられる帰納法のようには簡明ではない．）

§2　特殊行の再現問題

定理1およびその系から次のことがわかる．

まず 2^k 個の1を最上段に並べておき，それから出発して mod 2 でパスカルの三角形を作る．そのとき 2^k 回目にふたたび 2^{k+1} 個の1だけが並ぶ行が得られる．

あるいは，両端だけが1で他が全部0である 2^k+1 個の数を最上段として mod 2 でパスカルの三角形を作れば，2^k 回目にふたたび両端だけが1で他が全部0であるような $2^{k+1}+1$ 個の数の行が得られる．

今，簡単のため，両端だけが1で他が全部0であるような行を“特殊行”とよぶことにしよう．上にいったように 2^k+1 個の数から成る特殊行から出発してパスカルの三角形を作った場合には適当な回数の後にふたたび特殊行が現われるが，$n\neq 2^k$ の場合にも，$n+1$ 個の数から成る特殊行から出発してパスカルの三角形を作ったときに，ふたたび特殊行が現われることがあるであろうか．その答は否定的である．

定理 2　$n+1$ $(n\geqq 1)$ 個の数から成る特殊行から出発して mod 2 でパスカルの三角形を作るとき，ふたたび特殊行が現われるためには，$n=2^k$ であることが必要十分である．

（証明）　定理の条件が十分であることは上に述べた．

必要であることは次のようにして証明される．今，n が定理に述べたような性質をもつとする．すなわち，$n+1$ 個の数から成る特殊行から出発して作ったパスカルの三角形にふたたび特殊行が現われるとする．このことは，$\mathbf{Z}/(2)$ における多項式の演算で考えれば，ある整

数 $m\geqq 1$ が存在して

$$(3)\qquad (x^n+1)(x+1)^m=x^{n+m}+1$$

が成り立つ，ということを意味している．ここで，$m=2^k l$, l は奇数，とおけば，

$$(x+1)^m=(x^{2^k}+1)^l$$

であるから，(3) の左辺は

$$(x^n+1)(x^{2^k l}+lx^{2^k(l-1)}+\cdots\cdots)$$
$$=x^{n+m}+lx^{n+2^k(l-1)}+[\text{次数}<n+2^k(l-1)\ \text{の項}]$$
$$+x^{2^k l}+[\text{次数}<2^k l\ \text{の項}]$$

となる．これが x^{n+m} と定数項1以外の項を含まないのであるから，$x^{n+2^k(l-1)}$ の項と $x^{2^k l}$ の項とは消し合わなければならない．したがって $n+2^k(l-1)=2^k l$，すなわち $n=2^k$ となる．(証明終)

はじめにもことわっておいたが，かつて数学セミナーに問題として提出したことがあるといったのは上の定理1および定理2である．(筆者は都立大学の石田信君とともにこれを同誌の“エレガントな解答を求む”欄にのせたのであった．) そのとき寄せられた解答のうちには $\mathbf{Z}/(2)$ における演算の利用を意図したものもあったが，たいていは他のもっと複雑な方法によるもので，$\mathbf{Z}/(2)$ における演算を考えたものにも上記のような簡単な証明はなかったようである．

上では $\mathbf{Z}/(2)$ における演算を用いた．$\mathbf{Z}/(2)$ のかわりに，一般に $\mathbf{Z}/(p)$ (p は素数) を考え，そこにおける公式 $(x+1)^{p^k}=x^{p^k}+1$ を用いれば，上とほとんど同様にして次の定理が得られる．

定理 3　$\binom{n}{r}$ $(0<r<n)$ がすべて素数 p で割り切れるためには，$n=p^k(k\geqq 1)$ であることが必要十分である．

定理 4　$n+1(n\geqq 1)$ 個の数から成る特殊行から出発して mod p でパスカルの三角形を作るとき，ふたたび特殊行が現われるためには，$n=p^k$ であることが必要十分である．

§3　二三の一般化

上の定理 1～4 の証明に用いたのは，$\mathbf{Z}/(p)$ における基本的な演算

公式

$$(x+1)^{p^k}=x^{p^k}+1$$

であった．この単純な原理を応用して，上記定理3の二三の拡張を考えることができる．

定理 5　p を素数とし，$n=2p^k(k\geqq 0)$ とする．そのとき，$0<r<n$ に対し，

$$r\neq\frac{n}{2} \quad \text{ならば} \quad \binom{n}{r}\equiv 0(\mathrm{mod}\ p),$$

$$r=\frac{n}{2} \quad \text{ならば} \quad \binom{n}{r}\equiv 2(\mathrm{mod}\ p)$$

である．($p=2$ の場合にはこの定理は定理1の中に含まれている.)

(証明)　等式

$$(x+1)^2=x^2+2x+1$$

の x に x^{p^k} を代入すれば

$$(x^{p^k}+1)^2=x^{2p^k}+2x^{p^k}+1$$

$\mathbf{Z}/(p)$ において左辺は $[(x+1)^{p^k}]^2$ に等しいから，

$$(x+1)^n=x^n+2x^{n/2}+1.$$

これより上の結論が得られる．(証明終)

同様に，等式

$$(x+1)^3=x^3+3x^2+3x+1$$

の x に x^{p^k} を代入して，mod p で計算すれば，次の定理が得られる．

定理 6　p を素数とし，$n=3p^k(k\geqq 0)$ とする．そのとき，$0<r<n$ に対し，

$$r\neq\frac{n}{3},\ \frac{2n}{3} \quad \text{ならば} \quad \binom{n}{r}\equiv 0(\mathrm{mod}\ p),$$

$$r=\frac{n}{3},\ \frac{2n}{3} \quad \text{ならば} \quad \binom{n}{r}\equiv 3(\mathrm{mod}\ p)$$

である．

次の定理は定理5および定理6をさらに一般な形にしたものである．

定理 7　p を素数，$m\geqq 1$，$k\geqq 0$ とする．そのとき，$0\leqq r\leqq p^k m$ に

対し，$r\not\equiv 0 \pmod{p^k}$ である場合には

$$\binom{p^k m}{r} \equiv 0 \pmod{p},$$

$r=p^k s (0\leqq s\leqq m)$ である場合には

$$\binom{p^k m}{r} = \binom{p^k m}{p^k s} \equiv \binom{m}{s} \pmod{p}$$

が成り立つ．

（証明）　二項展開式

$$(x+1)^m = \sum_{s=0}^{m} \binom{m}{s} x^s$$

の x のところに x^{p^k} を代入し，mod p で計算すれば

$$(x+1)^{p^k m} = \sum_{s=0}^{m} \binom{m}{s} x^{p^k s}$$

これより結論が得られる．（証明終）

定理 7 において，特に $1\leqq m<p$ とすれば，$\binom{m}{s}$ は p では割り切れないから，

$$\binom{p^k m}{r} \equiv 0 \pmod{p}$$

であるための必要十分条件は $r\not\equiv 0 \pmod{p^k}$ となる．$\binom{n}{r}$ が p で割り切れるかどうかをみるための一般的な条件は §5 に与えるであろう．

§4　二項係数 $\binom{n}{r}$ の奇偶の判定

ふたたび出発点にもどって，mod 2 によるパスカルの三角形について考える．

この三角形の各行の 1 の個数を調べてみると，次頁の図のように 2, 2, 4, 2, 4, 4, 8, 2, ……となる．すなわち，n の小さい値に対しては，各行に現われる 1 の個数はいつも 2 のべきとなっている．このことが一般に成り立たないか，すなわち任意の n に対して，$\binom{n}{r}$ $(0\leqq r\leqq n)$ のうちの奇数の個数はつねに 2 のべきであるという結論が得られ

ないか，という問題はちょっとした興味をひくであろう．この事実は実際に成り立つのであって，その証明は $\binom{n}{r}$ の奇偶を判定する一般的な条件から直ちに得られる．そして，$\binom{n}{r}$ の奇偶の判定条件は整数の二進法展開を考えることから容易に与えられるのである．

$n=1$ …… 1　1 …… 2
$n=2$ …… 1　0　1 …… 2
$n=3$ …… 1　1　1　1 …… 4
$n=4$ …… 1　0　0　0　1 …… 2
$n=5$ …… 1　1　0　0　1　1 …… 4
$n=6$ …… 1　0　1　0　1　0　1 …… 4
$n=7$ …… 1　1　1　1　1　1　1　1 …… 8
$n=8$ …… 1　0　0　0　0　0　0　0　1 …… 2
⋮　　⋮　　⋮

n を整数 $\geqq 1$ とする．n を二進法で表示すれば

$$n=2^{\alpha_1}+2^{\alpha_2}+\cdots\cdots+2^{\alpha_t},$$
$$0\leqq\alpha_1<\alpha_2<\cdots\cdots<\alpha_t$$

の形に一意的に表わされる．このとき，n の展開に現われる指数の集合 $\{\alpha_1, \alpha_2, \cdots\cdots, \alpha_t\}$ を $I(n)$ と書くことにしよう．また便宜上，$I(0)$ は空集合と約束しておく．

そこで，整数 $m, n\geqq 0$ に対し，$I(m)\supset I(n)$ であるとき

$$m\overset{*}{\geqq}n$$

として順序関係 $\overset{*}{\geqq}$ を定義する．（実際にこれは負でない整数全体の集合における順序であって，0がこの順序による最小元である．）

このように順序 $\overset{*}{\geqq}$ を定義すると，次の定理が成り立つのである．

定理 8　$n\geqq 1$, $0\leqq r\leqq n$ とするとき，$\binom{n}{r}$ が奇数であるための必要十分条件は，$n\overset{*}{\geqq}r$ であることである．

（証明）　上のように $I(n)=\{\alpha_1, \alpha_2, \cdots\cdots, \alpha_t\}$，すなわち

$$n=2^{\alpha_1}+2^{\alpha_2}+\cdots\cdots+2^{\alpha_t}$$

とし，$\mathbf{Z}/(2)$ で $(x+1)^n$ を計算すれば

$$(x+1)^n=(x+1)^{2^{\alpha_1}}(x+1)^{2^{\alpha_2}}\cdots\cdots(x+1)^{2^{\alpha_t}}$$

$$=(x^{2^{\alpha_1}}+1)(x^{2^{\alpha_2}}+1)\cdots\cdots(x^{2^{\alpha_t}}+1)$$

この右辺を展開すると，明らかに，2^{α_i} のうちのいくつかの和（空の和も含む）であるような r を指数とする項 x^r，またそのような項のみが現われる．したがって

$$(x+1)^n=\sum_{r;\ I(r)\subset I(n)}x^r=\sum_{r;\ r\overset{*}{\leqq}n}x^r$$

われわれの命題はこの式から明らかである．（証明終）

定理8は特別の場合として定理1およびその系を包含していることに注意しておこう．実際，$n=2^k$ $(k\geqq 1)$ すなわち $I(n)=\{k\}$ である場合には，$n\overset{*}{\geqq}r$ であるような r は n と0しかない．逆に $n\overset{*}{\geqq}r$ であるような r が n と0のほかにないならば，明らかに n は $n=2^k$ の形でなければならない．したがって定理1が成り立つ．定理1の系についても同様である．

今，n を整数 $\geqq 1$ とし，$I(n)$ の元の個数を t とする．その場合，$n\overset{*}{\geqq}r$ すなわち $I(n)\supset I(r)$ であるような r の個数は，$I(n)$ の部分集合全部の個数にほかならないから 2^t である．ゆえに定理8から次の系が得られる．

系　任意の整数 $n\geqq 1$ に対して，$\binom{n}{r}$ $(0\leqq r\leqq n)$ が奇数であるような r の個数は2のべきである．すなわち，$I(n)$ の元の個数を t とすれば 2^t に等しい．

たとえば，$n=500$ を二進法で展開すれば

$$n=2^2+2^4+2^5+2^6+2^7+2^8$$

したがって，$\binom{500}{r}$ $(0\leqq r\leqq 500)$ のうちの奇数の個数は $2^6=64$ である．

上の定理8および系は，少なくとも，あまり一般的に知られている事実ではないようである．もちろん，このような命題自身にたいした意味があるわけではないけれども，その証明が上のように mod 2 の計算と二進法の簡単な応用として得られるところに，幾分の興味が感じられるように思う．

§5 $\binom{n}{r} \equiv 0 \pmod{p}$ の判定

前節では $\binom{n}{r}$ の奇偶を判定するための条件を与えた．このとき整数の二進展開を用いたが，これを p 進展開におきかえることによって，$\binom{n}{r}$ が素数 p で割り切れるための判定条件を与えることができる．

p を1つの与えられた素数とする．そのとき，任意の整数 $n \geqq 0$ は

$$n=\sum_{i=0}^{\infty} a_i p^i, \quad 0 \leqq a_i < p$$

の形に一意的に表わされる．（もちろんこの和は有限和である．）r をもう1つの整数 $\geqq 0$ とし，

$$r=\sum_{i=0}^{\infty} b_i p^i, \quad 0 \leqq b_i < p$$

とする．このとき，すべての $i=0, 1, 2, \cdots\cdots$ に対し $a_i \geqq b_i$ が成り立つことをもって，$n \overset{*}{\geqq}_{(p)} r$ と定義する．もちろん $\overset{*}{\geqq}_{(p)}$ も負でない整数全体の集合における1つの順序関係である．（前節の $\overset{*}{\geqq}$ は $\overset{*}{\geqq}_{(2)}$ にほかならない．）

そうすれば，定理8の一般化として，次の定理が得られる．

定理 9　$n \geqq 1$, $0 \leqq r \leqq n$ とするとき，

$$n \overset{*}{\geqq}_{(p)} r \quad \text{ならば} \quad \binom{n}{r} \not\equiv 0 \pmod{p},$$

$$n \overset{*}{\geqq}_{(p)} r \quad \text{でなければ} \quad \binom{n}{r} \equiv 0 \pmod{p}$$

である．

（証明）　n の p 進展開を

$$n=\mu_1 p^{\alpha_1}+\cdots\cdots+\mu_t p^{\alpha_t}$$
$$0 \leqq \alpha_1 < \cdots < \alpha_t, \quad 0 < \mu_i < p \ (i=1, \cdots, t)$$

とする．そのとき mod p で計算すれば

$$(x+1)^n=(x+1)^{p^{\alpha_1}\mu_1}\cdots\cdots(x+1)^{p^{\alpha_t}\mu_t}$$
$$=(x^{p^{\alpha_1}}+1)^{\mu_1}\cdots\cdots(x^{p^{\alpha_t}}+1)^{\mu_t}$$

二項定理を用いて，さらにこの右辺を展開すれば

$$\left(\sum_{\nu_1=0}^{\mu_1}\binom{\mu_1}{\nu_1}x^{p^{\alpha_1}\nu_1}\right)\cdots\cdots\left(\sum_{\nu_t=0}^{\mu_t}\binom{\mu_t}{\nu_t}x^{p^{\alpha_t}\nu_t}\right)$$

$$=\sum_{\nu_1=0}^{\mu_1}\cdots\sum_{\nu_t=0}^{\mu_t}\binom{\mu_1}{\nu_1}\cdots\binom{\mu_t}{\nu_t}x^{\nu_1 p^{\alpha_1}+\cdots\cdots+\nu_t p^{\alpha_t}}$$

となる．（この右辺の和の中に同じ指数の項は重複しては現われない．）したがって

$$(x+1)^n=\sum_{\nu_1=0}^{\mu_1}\cdots\sum_{\nu_t=0}^{\mu_t}\binom{\mu_1}{\nu_1}\cdots\binom{\mu_t}{\nu_t}x^{\nu_1 p^{\alpha_1}+\cdots\cdots+\nu_t p^{\alpha_t}}$$

ここで $0\leqq\nu_i<\mu_i<p$ であるから$\binom{\mu_t}{\nu_t}\not\equiv 0(\mathrm{mod}\ p)$，したがって

$$\binom{\mu_1}{\nu_1}\cdots\binom{\mu_t}{\nu_t}\not\equiv 0(\mathrm{mod}\ p)$$

すなわち，$(x+1)^n$ の $\mathbf{Z}/(p)$ における展開式において，0 でない係数で現われる項は $n\overset{*}{\geqq}_{(p)}r$ であるような項 x^r またそのような項だけに限る．このことからわれわれの命題が得られる．（証明終）

上の定理 9 が特別の場合として定理 3 を含むことも，定理 8 が定理 1 を含むのと同様である．実際，$n\overset{*}{\geqq}_{(p)}r$ であるような r が n と 0 だけに限るのは，明らかに n が $n=p^k$ の形であることと同値であるからである．

この場合と対照的に，すべての $\binom{n}{r}$ $(0\leqq r\leqq n)$ が p と互に素であるための条件を考えてみよう．定理 9 によれば，それはすべての $0\leqq r\leqq n$ について $n\overset{*}{\geqq}_{(p)}r$ が成り立つことを意味するが，そのためには，n の p 進展開が

$$n=(p-1)+(p-1)p+\cdots+(p-1)p^{k-1}+\mu p^k\quad(0\leqq\mu<p)$$

の形になっていることが明らかに必要十分である．（ここで $k\geqq 0$ であるが，$\mu=0$ の場合には $k\geqq 1$ である．）上の n の式を計算して，記号を改めれば，次の系が得られる．

系　整数 $n\geqq 1$ に対し，$\binom{n}{r}$ $(0\leqq r\leqq n)$ がすべて p と互に素であるためには，n が $n=\lambda p^k-1$ $(0<\lambda<p,\ k\geqq 0$；ただし $\lambda=1$ のときには $k\geqq 1)$ の形であることが必要十分である．

この系は定理 1 の系の一般化である．

なお一般には，n の p 進展開が

$$n=\sum_{i=0}^{\infty}a_ip^i,\quad 0\leqq a_i<p$$

の形であるとき，$n\overset{*}{\geqq}_{(p)}r$ であるような r は，明らかに

$$\prod_{i=0}^{\infty}(a_i+1)$$

個存在する．定理9によれば，これが$\binom{n}{r}$ $(0\leqq r\leqq n)$ のうちで p と互に素であるものの個数に等しい．特に $p=2$ の場合には，すべての a_i が0または1に等しいので，たまたま定理8の系のような印象的な形をとるわけである．

1972 年2月