$\binom{N}{p} \equiv \left[\frac{N}{p}\right] \pmod{p}$;二項係数の或る数論的性質

中嶋眞澄
Masumi NAKAJIMA
Department of Economics
International University of Kagoshima
Kagoshima 891-0197, JAPAN
e-mail: nakajima@eco.iuk.ac.jp

概 要

Abstract

We prove here that $\binom{N}{p} \equiv \left[\frac{N}{p}\right] \pmod{p}$ *if* p *is prime.*

Key words ; binomial coefficients.

Mathematics Subject Classification ; 05A10.

次の定理を証明する。

定理

pが素数ならば、 $\binom{N}{p} \equiv \left[\frac{N}{p}\right] \pmod{p}$.

この定理を証明する為に以下の幾つかの補題を証明する。

補題1

$$1 \leq r \leq p-1,\ p\text{が素数ならば,}\ \binom{p}{r} \equiv 0 \pmod{p}$$

証明

$\binom{p}{r} = \dfrac{p(p-1)\cdots(p-r+1)}{r!}$で$1 \leq r \leq p-1$であるから分母の$r!$の素因数は全て素数$p$より小さく，分子の$p$を約す事はなく$p$は残るので$\binom{p}{r}$は$p$の倍数である。□

補題2

$N-m \geq r \geq m \geq 0$のとき，

$$\binom{N}{r} = \sum_{k=0}^{m} \binom{m}{k}\binom{N-m}{r-k} = \binom{N-m}{r} + \binom{N-m}{r-m} + \sum_{k=1}^{m-1} \binom{m}{k}\binom{N-m}{r-k}.$$

証明

再帰公式：$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$を順次$m$回，$\binom{N}{r}$に適用する。□

素数pを三つの場合：$N \geq p > \frac{N}{2}$，$1 < p < \frac{N}{2}$，$N = 2p$に分けて考える。

補題3

$$N \geq p > \frac{N}{2},\ p\text{が素数ならば,}\ \binom{N}{p} \equiv 1 \pmod{p}.$$

証明

$N = p$のとき，$\binom{N}{p} = \binom{p}{p} = 1 = \left[\dfrac{p}{p}\right] = \left[\dfrac{N}{p}\right] \pmod{p}$となり，結論を満たす。

補題2で$1 \leq r = m = N-p$とすると，補題2の条件を満たし$\binom{N-m}{r-m} = 1$であるので，

$$\binom{N}{p} = \binom{N}{N-p} = \binom{N}{r} =$$
$$= \binom{N-m}{r} + \binom{N-m}{r-m} + \sum_{k=1}^{m-1} \binom{m}{k}\binom{N-m}{r-k}$$
$$= \binom{p}{r} + \binom{p}{0} + \sum_{k=1}^{N-p-1} \binom{N-p}{k}\binom{p}{r-k}$$
$$= \binom{p}{r} + 1 + \sum_{k=1}^{N-p-1} \binom{N-p}{k}\binom{p}{N-p-k}$$
$$\equiv 1 \pmod{p}. \quad \square$$

補題 4

$p < \dfrac{N}{2}$, pが素数ならば, $\displaystyle\binom{N}{p} \equiv \binom{N-p}{p} + 1 \pmod{p}$.

証明

補題 2 で $r = m = p$ とすると，補題 2 の条件を満たし

$$\binom{N}{p} = \binom{N}{r} =$$
$$= \binom{N-m}{r} + \binom{N-m}{r-m} + \sum_{k=1}^{m-1} \binom{m}{k}\binom{N-m}{r-k}$$
$$= \binom{N-p}{p} + \binom{N-p}{p-p} + \sum_{k=1}^{p-1} \binom{p}{k}\binom{N-p}{p-k}$$
$$= \binom{N-p}{p} + 1 + \sum_{k=1}^{p-1} \binom{p}{k}\binom{N-p}{p-k}$$
$$\equiv \binom{N-p}{p} + 1 \pmod{p}. \quad \square$$

補題 5

pが素数ならば, $\displaystyle\binom{2p}{p} \equiv 2 \pmod{p}$.

証明

補題 2 で $p = m = r$, $N = 2p$ とすると，

$$
\begin{aligned}
&\binom{2p}{p} = \binom{N}{r} = \\
&= \binom{N-m}{r} + \binom{N-m}{r-m} + \sum_{k=1}^{m-1} \binom{m}{k}\binom{N-m}{r-k} \\
&= \binom{2p-p}{p} + \binom{2p-p}{p-p} + \sum_{k=1}^{p-1} \binom{p}{k}\binom{2p-p}{p-k} \\
&= \binom{p}{p} + \binom{p}{0} + \sum_{k=1}^{p-1} \binom{p}{k}\binom{p}{p-k} \\
&= 1 + 1 + \sum_{k=1}^{p-1} \binom{p}{k}\binom{p}{p-k} \\
&\equiv 2 \pmod{p}. \qquad \square
\end{aligned}
$$

定理の証明　補題3，4，5を使って順次1を追い出せば良い。□

注 この定理の逆は不成立。

- N が素数でないとき，$\binom{N}{N} = 1 = \left[\frac{N}{N}\right] \pmod{N}$
- $N-1$ が素数でないとき，

$$N = \binom{N}{N-1} \equiv \left[\frac{N}{N-1}\right] = 1 \pmod{N-1}$$

参考文献

[1] 北村泰一 Kitamura,T.『数論入門 (改訂版)』*Introduction to Number Theory,* (in Japanese), revised ed., 槇書店 Maki-Shoten, 1986(1965 1st ed.), (v+160)pp..

[2] 和田秀男 Wada,H.『数の世界-整数論への道』*The World of Numbers – A Way to Number Theory,* (in Japanese), 岩波書店 Iwanami-Shoten, 1981, (xii+254)pp..

[3] 草場公邦 Kusaba,T.『整数論』*Number Theory,* (in Japanese), 日本放送協会 NHK, 1974, (0+230)pp..

[4] 酒井孝一 Sakai,K.『整数論講義』*Lectures on Number Theory,* (in Japanese), 宝文館 Houbun-Kan, 1976, (v+323)pp..

[5] Vinogradov,I.M., 三瓶与右衛門, 山中健訳:『整数論入門』共立出版, 1959, (iii+202)pp.. *Introduction to Number Theory* (Japanese translation), Kyouritsu-Shuppan, Tokyo.

(received 31 May 2021.)