# 二項定理と合同式

**命題.** $p$ を素数とする．このとき，次が成り立つ．

$$(a+b)^p \equiv a^p + b^p \mod p$$

整数 $m, n$ $(m \geq n \geq 0)$ に対して，二項係数を

$$\binom{m}{n} = {}_mC_n = \frac{m!}{(m-n)!n!}$$

で表す．二項係数は整数である[1] 命題の証明のために補題を用意する．

**補題.** $p$ を素数とする．$k = 1, \cdots, p-1$ に対して，整数 $\binom{p}{k}$ は，$p$ の倍数である．

証明. 定義から，$\binom{p}{k} = \frac{p!}{(p-k)!k!}$ である．$p!$ は $p$ で割れるので，$(p-k)!$ と $k!$ が $p$ で割れないことを示せばよい．$p$ は素数なので，$p$ より小さい全ての自然数 $n$ に対して，$n!$ は，$p$ を約数に持たない．よって，$1 \leqq k \leqq p-1$ という仮定から，$p-k < p$，$k < p$ であり，$(p-k)!$ と $k!$ は，$p$ で割れない． □

補題を用いて，命題を証明する．

命題の証明. 二項定理[2]から，

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

と展開できる．上の補題から，右辺の和の $k = 1, \cdots, p-1$ の部分の項は $p$ の倍数であるため，

$$\sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = \binom{p}{0} a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + \binom{p}{p} b^n \equiv a^p + b^p \ (\mod p)$$

となり，結果が従う． □

上の命題は次のように一般化できる．

**命題.** $p$ を素数とする．このとき，次が成り立つ．

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \mod p$$

証明. 多項定理[3]から，左辺の展開式における $a_1^{r_1} a_2^{r_2} \cdots a_n^{r_n}$, $p = r_1 + \cdots + r_n$ の項の係数は，

$$\frac{p!}{r_1! r_2! \cdots r_n!}$$

である．上の補題と同様の考察により，$r_i = p$ を満たす $i$ を持たない項の係数は $p$ の倍数である．よって，それらの項は全て $p$ を法として 0 と合同であり，結果の合同式が得られる． □

---

[1] コンビネーション ${}_mC_n$ の定義（$m$ 個から $n$ 個を選ぶ組み合わせの数）から明らかである．

[2] https://gleamath.com/binomial-thm/

[3] https://gleamath.com/multinomial-thm/