11 p を素数とする．

（1） $1 \leqq k < p$ を満たす自然数 k について，二項係数 ${}_pC_k$ は p の倍数であることを証明せよ．

（2） すべての自然数 n について，$n^p - n$ は p の倍数であることを証明せよ．　（24　信州大・前期）

11 数学B【数学的帰納法】標準

《フェルマーの小定理（B15）☆》

▶解答◀ （1） ${}_pC_k = \dfrac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$

p は素数で $k, k-1, \cdots, 1$ は p より小さいから p は約分されないで残る．したがって ${}_pC_k$ は p の倍数である．

（2） $f(n) = n^p - n$ とおく．

$$\begin{aligned} f(n+1) &= (n+1)^p - (n+1) \\ &= 1 + {}_pC_1 n + \cdots + {}_pC_{p-1} n^{p-1} + n^p - n - 1 \\ &= {}_pC_1 n + \cdots + {}_pC_{p-1} n^{p-1} + f(n) \end{aligned}$$

${}_pC_1$ から ${}_pC_{p-1}$ まではすべて p の倍数であるから，$f(n+1)$ を p で割った余りと $f(n)$ を p で割った余りは等しく，$f(n)$ を p で割った余りは自然数 n の値によらず一定である．$f(1) = 1 - 1 = 0$ は p の倍数であるから，$f(n)$ は常に p の倍数である．よって証明された．

注意 【帰納法の形式で書く】

私は高校生のときから上のように書いていた．世間で，どうして帰納法で書くのか，不思議でしかたがない．形式上，帰納法で書くと次のようになる．

$f(1) = 0$ は p の倍数である．$n = 1$ のとき成り立つ．$n = m$ で成り立つとする．$f(m)$ は p の倍数である．

$$\begin{aligned} f(m+1) &= (m+1)^p - (m+1) \\ &= 1 + \sum_{k=1}^{p-1} {}_pC_k m^k + m^p - (m+1) \\ &= \sum_{k=1}^{p-1} {}_pC_k m^k + f(m) \end{aligned}$$

${}_pC_k$ と $f(m)$ は p の倍数であるから，$f(m+1)$ は p の倍数である．$n = m+1$ でも成り立つから数学的帰納法により証明された．

注意 【フェルマーの小定理】

p が素数で n と p が互いに素のとき

$$n^{p-1} \equiv 1 \pmod{p}$$

が成り立つ．これをフェルマーの小定理という．