m を正の整数とする．2 つの整数 $a,\ b$ について，a を m で割った余りと b を m で割った余りが等しいとき，a と b は m を法として合同であるといい $a \equiv b \pmod{m}$ と表す．p を素数，n を正の整数として，以下の問いに答えよ．

(1) k は p より小さな正の整数とする．${}_p\mathrm{C}_k k!$ を p で割った余りを求めよ．また，${}_p\mathrm{C}_k$ を p で割った余りを求めよ．

(2) $(n+1)^p \equiv n^p + 1 \pmod{p}$ であることを示せ．ここで，二項定理

$$(a+b)^k = \sum_{l=0}^{k} {}_k\mathrm{C}_l a^l b^{k-l}$$

を証明なしに用いてよい．ただし，$a,\ b$ は実数である．

(3) $n^p \equiv n \pmod{p}$ を数学的帰納法により証明せよ．

(4) 2020^{2017} を 2017 で割った余りを求めよ．ただし，2017 は素数である．

(17 公立はこだて未来大 シス情 4)

【答】

(1) 0，0

(2) 略

(3) 略

(4) 3

【解答】

(1) $1 \leqq k < p$ のとき

$${}_p\mathrm{C}_k k! = \frac{n!}{(n-k)!k!} \cdot k! = p \times (p-1)(p-2)\cdots(p-k+1)$$

${}_p\mathrm{C}_k k!$ は p の倍数であるから，${}_p\mathrm{C}_k k!$ を p で割った余りは $\mathbf{0}$ である． ……(答)

また，p は素数なので，$k,\ k-1,\ k-2,\ \cdots,\ 2,\ 1$ はいずれも p と互いに素であり，$k!$ は p の倍数ではない．${}_p\mathrm{C}_k \times k!$ は p の倍数であるから，${}_p\mathrm{C}_k$ は p の倍数である．

よって，${}_p\mathrm{C}_k$ を p で割った余りは $\mathbf{0}$ である． ……(答)

- ${}_p\mathrm{C}_k$ は整数である．また

$${}_p\mathrm{C}_k = \frac{n!}{(n-k)!k!} = p \times \frac{(p-1)(p-2)\cdots(p-k+1)}{k!}$$

とみれば，${}_p\mathrm{C}_k k!$ が p の倍数であることを示さなくても，【解答】と同じ議論により，${}_p\mathrm{C}_k$ は p の倍数であることが示される．

(2) 二項定理を用いると

$$(n+1)^p = \sum_{k=0}^{p} {}_p\mathrm{C}_k n^k \cdot 1^{p-k} = 1 + n^p + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k n^k$$

であるが，(1) より ${}_p\mathrm{C}_k\ (k = 1,\ 2,\ \cdots,\ p-1)$ は p の倍数であるから，$\displaystyle\sum_{k=1}^{p-1} {}_p\mathrm{C}_k n^k$ は p の倍数である．したがって，$(n+1)^p$ を p で割った余りは $n^p + 1$ を p で割った余りに等しい．すなわち

$$(n+1)^p \equiv n^p + 1 \pmod{p}$$

である． ……(証明終わり)

(3) $$n^p \equiv n \pmod{p} \qquad \cdots\cdots (*)$$

(i) $n=1$ のとき

$$(\text{左辺}) = 1^p = 1, \quad (\text{右辺}) = 1$$

であるから，n^p も n も p で割った余りはともに 1 であり，$(*)$ は成り立つ．

(ii) $n=m$ (m は正の整数) のときの成立を仮定すると

$$\begin{aligned}(m+1)^p &\equiv m^p+1 \pmod{p} \quad (\because\ (2))\\ &\equiv m+1 \pmod{p} \quad (\because\ \text{帰納法の仮定})\\ \therefore\quad (m+1)^p &\equiv m+1 \pmod{p}\end{aligned}$$

であり，$(*)$ は $n=m+1$ のときも成り立つ．

以上 (i)，(ii) より，すべての正の整数 n に対して $(*)$ は成り立つ．　　……(証明終わり)

(4) 2017 は素数であるから，(3) の結果を用いると

$$2020^{2017} \equiv 2020 \pmod{2017}$$

である．これより，2020 を 2017 で割った余りは，2020 を 2017 で割った余りに等しく

$$2020 = 2017 \times 1 + 3$$

であるから，2020^{2017} を 2017 で割った余りは **3** である．　　……(答)

- (3) の「p が素数のとき

$$n^p \equiv n \pmod{p} \qquad \cdots\cdots (*)$$

が成り立つ」はフェルマーの小定理と呼ばれている．

n が p と互いに素なとき，すなわち，$n \not\equiv 0 \pmod{p}$ のときは

$$n^{p-1} \equiv 1 \pmod{p} \qquad \cdots\cdots (**)$$

でもある．n が p と互いに素なとき，$(*)$ と $(**)$ は同値である．

$(**)$ の証明をしておこう．

n が p と互いに素なとき，$n,\ 2n,\ 3n,\ \cdots,\ (p-1)n$ は p と互いに素であり，p で割った余りはどれも異なる．すなわち，$n,\ 2n,\ 3n,\ \cdots,\ (p-1)n$ は全体において一つずつ $1,\ 2,\ 3,\ \cdots,\ p-1$ と p を法として合同となる．これらをすべて掛けると

$$\begin{aligned}n \cdot 2n \cdot 3n \cdot \cdots \cdot (p-1)n &\equiv (p-1)! \pmod{p}\\ n^{p-1}(p-1)! &\equiv (p-1)! \pmod{p}\end{aligned}$$

$(p-1)!$ は p と互いに素であるから

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

である．