# 1 本題の証明

**命題 1.** 求める $r, c$ は

$$(BC - AC)(-BC + AB + AC)^{M-2},$$
$$(BC - AB)(-BC + AB + AC)^{M-2}$$

をそれぞれ $M$ で割った余りである。

**証明.** $M = 10^9 + 7$ とおく。$(r, c), (r, c+1), (r+1, c)$ にたどり着く方法の個数をそれぞれ $A', B', C'$ とおくと，$A', B', C'$ を $M$ で割った余りがそれぞれ $A, B, C$ である。

マス $(x, y)$ にたどり着く方法の個数は ${}_{x+y}\mathrm{C}_y$ であるから，$A', B', C'$ は次のように表せる：

$$\begin{cases} A' = {}_{r+c}\mathrm{C}_r = {}_{r+c}\mathrm{C}_c \\ B' = {}_{r+c+1}\mathrm{C}_{c+1} \\ C' = {}_{r+c+1}\mathrm{C}_{r+1} \end{cases}$$

**[1]** $r \geq 1$ **かつ** $c \geq 1$ **のとき**

一般に，$n \geq 2,\ k \geq 1$ のとき

$$k \times {}_n\mathrm{C}_k = n \times {}_{n-1}\mathrm{C}_{k-1}$$

が成り立つから，$A', B', C'$ に関して次が成り立つ：

$$\begin{cases} (r+1)\ C' = (r+c+1)\ A' \\ (c+1)\ B' = (r+c+1)\ A' \end{cases}$$

$1 \leq A' < B',\ 1 \leq A' < C'$ に注意してこれを解くと，

$$\begin{cases} r = \dfrac{B'C' - A'C'}{-B'C' + A'B' + A'C'} \\ c = \dfrac{B'C' - A'B'}{-B'C' + A'B' + A'C'} \end{cases} \tag{1}$$

である。

題意により $r, c$ は $M$ より小さい非負整数なので，$r, c$ は (1) の右辺を $M$ で割った余りに一致する。

ここで,

$$
\begin{aligned}
S &= B'C' - A'C' \\
T &= B'C' - A'B' \\
U &= -B'C' + A'B' + A'C' \\
s &= BC - AC \\
t &= BC - AB \\
u &= -BC + AB + AC
\end{aligned}
$$

とおく。

$M$ と $U$ が互いに素ではないと仮定すると，$M$ が素数であるこであることから $U$ は $M$ で割り切れる。すると $r, c$ が整数であることから，$S, T$ も $M$ で割り切れるので，$A'$ は $M$ で割り切れる。ところが題意により $0 \leq r+c < 2\times 99999999 < M$ なので，補題 1 により $A'$ は $M$ で割り切れず，矛盾が生じる。したがって，$M$ と $U$ は互いに素である。よって，$M$ と $u$ も互いに素である。

$M$ は素数なので，補題 2 により法 $M$ に関する $U, u$ のモジュラ逆数 $U', u'$ $(0 \leq U' < M,\ 0 \leq u' < M)$ が唯一つ存在する。$r, c$ が整数ゆえに $S, T$ がそれぞれ $U$ の倍数であることに注意すれば，次が成り立つ：

$$
\begin{aligned}
r &\equiv SU' \quad \bmod M \qquad (\because \text{補題 } 3) \\
&\equiv su' \quad \bmod M \qquad (\because \text{補題 } 4) \\
c &\equiv TU' \quad \bmod M \qquad (\because \text{補題 } 3) \\
&\equiv tu' \quad \bmod M \qquad (\because \text{補題 } 4)
\end{aligned}
$$

このことと定理 1 から，

$$u' \equiv u^{M-2} \mod M$$

なので，$r, c$ は $su^{M-2},\ tu^{M-2}$ をそれぞれ $M$ で割った余りである。したがって，命題 1 が成り立つ。

**[2]** $r = 0$ **または** $c = 0$ **のとき**

$A' = 1,\ B' = c+1,\ C' = r+1$ であるから，(1) が成り立つ。したがって，[1] と同様の議論により命題 1 が成り立つ。 □

## 2　二項係数に関する証明

**補題 1.** $M$ を素数とする。任意の整数 $n, r$ $(n \geq 1,\ 0 \leq r \leq n)$ に対して，$n < M$ ならば，${}_n\mathrm{C}_r$ は $M$ で割り切れない。

**証明.**

$$ {}_n\mathrm{C}_r = \frac{n!}{(n-r)!r!} $$

なので，${}_n\mathrm{C}_r$ が $M$ で割り切れるならば $n!$ が $M$ で割り切れなければならないが，$n < M$ かつ $M$ は素数なので $n!$ は $M$ で割り切れない。したがって ${}_n\mathrm{C}_r$ は $M$ で割り切れない。 □

# 3　モジュラ逆数の性質に関する証明

**補題 2.** $M$ を素数，$x$ を $M$ と互いに素な整数とすると，法 $M$ に関する $x$ のモジュラ逆数 $x'$ が $0 \leq x' < M$ の範囲に唯一つ存在する。

**証明.** $x^n$ ($n$ は自然数; $1 \leq n \leq M$) を $M$ で割った余りをそれぞれ $a_n$ とおくと，

$$ \begin{aligned} x &\equiv a_1 \mod M \\ x^2 &\equiv a_2 \mod M \\ &\vdots \\ x^M &\equiv a_M \mod M \end{aligned} $$

となる。任意の整数を $M$ で割った余りは $0$ から $M-1$ までの $M$ 通りであるから，鳩の巣原理により，$a_1$ から $a_M$ のうちで少なくとも一組の重複がある。そのような組のひとつを $a_i$，$a_j$ $(1 \leq i < j \leq M)$ とおくと，

$$ x^j - x^i \equiv 0 \mod M $$

であるから，

$$ x \cdot x^{j-i-1} \equiv 1 \mod M $$

が成り立つ。したがって，$x^{j-i-1}$ は法 $M$ に関する $x$ のモジュラ逆数のひとつであるから，モジュラ逆数の存在が示された。

ここで，$x', x''$ $(1 \leq x' < M,\ 1 \leq x'' < M)$ を $x$ のモジュラ逆数とすると，

$$ \begin{aligned} x \cdot x' &\equiv 1 \mod M \\ x \cdot x'' &\equiv 1 \mod M \end{aligned} $$

より，

$$ x(x' - x'') \equiv 0 \mod M $$

であるから，

$$ x' \equiv x'' \mod M $$

が成り立ち，$1 \leq x' < M,\ 1 \leq x'' < M$ により $x' = x''$ である。したがって，モジュラ逆数の一意性が示された。 □

**補題 3.** 任意の整数 $x, y$ に対して，法 $M$ に関する $y$ のモジュラ逆数 $y'$ が存在するならば，

$$\frac{xy}{y} \equiv xyy' \mod M$$

が成り立つ。

**証明.** 与式の左辺は $x$ と等しく，右辺は $M$ を法として $x$ と合同であるから，与式が成り立つ。 □

**補題 4.** $M$ を素数とする。任意の整数 $x, y$ の法 $M$ に関するモジュラ逆数が存在しそれぞれ $x', y'$ であるとき，

$$x \equiv y \mod M \quad\Longrightarrow\quad x' \equiv y' \mod M$$

が成り立つ。

**証明.** モジュラ逆数の性質により

$$xx' \equiv yy' \mod M$$

が成り立つ。$M$ が素数であることと，モジュラ逆数が存在することから，$M$ と $x$，$M$ と $y$ はそれぞれ互いに素である。よって，辺々を $x, y$ で割って

$$x' \equiv y' \mod M$$

が成り立つ。 □

# 4　フェルマーの小定理の証明

整数 $m$ $(\geq 2)$ に対して

$$d_m = \gcd({}_m\mathrm{C}_1, {}_m\mathrm{C}_2,\ \ldots\ , {}_m\mathrm{C}_{m-1})$$

と定義する。

**補題 5.** $m$ が素数ならば $d_m = m$ が成り立つ。

**証明.** 一般に，$m \geq 2,\ k \geq 1$ のとき

$$k \times {}_m\mathrm{C}_k = m \times {}_{m-1}\mathrm{C}_{k-1}$$

が成り立つ。このことと，$1 \leq k \leq m-1$ のとき $m$ と $k$ は互いに素であることから，任意の $k$ $(1 \leq k \leq m-1)$ に対して ${}_m\mathrm{C}_k$ は $m$ で割り切れる。

また，${}_m\mathrm{C}_1 = m$ で $m$ は素数なので $d_m = 1$ または $d_m = m$ が必要である。

したがって，$d_m = m$ である。 □

**補題 6.** 任意の自然数 $k$ に対して，$k^m - k$ は $d_m$ で割り切れる。

**証明.** 自然数 $n$ に関する条件「$n^m - n$ は $d_m$ で割り切れる」を $P(n)$ とおく。

$n = 1$ のとき，$n^m - n$ すなわち 0 は $d_m$ $(\geq 1)$ で割り切れるから，$P(1)$ が成り立つ。

ある $n = k$ $(\geq 1)$ に対して $P(k)$ が成り立つと仮定すると

$$k^m - k \equiv 0 \mod d_m \tag{2}$$

が成り立つが，このとき

$$\begin{aligned}
(k+1)^m - (k+1) &= \sum_{j=0}^{m} {}_m\mathrm{C}_j k^j - (k+1) \\
&= \sum_{j=1}^{m-1} {}_m\mathrm{C}_j k^j + k^m - k \\
&\equiv k^m - k && \mod d_m \\
&\equiv 0 && \mod d_m \quad (\because (2))
\end{aligned}$$

なので，$P(k+1)$ も成り立つ。

以上より，補題 6 が成り立つ。 □

フェルマーの小定理

**定理 1.** $p$ が素数のとき，任意の自然数 $k$ に対して $k^{p-1} \equiv 1 \mod p$ が成り立つ。

**証明.** 補題 5, 6 より，$p$ が素数のとき，$p$ と互いに素な任意の自然数 $k$ に対して

$$k^p \equiv k \mod p$$

が成り立つ。$k$ と $p$ は互いに素であるから，両辺を $k$ で割ることができ，

$$k^{p-1} \equiv 1 \mod p$$

が成り立つ。 □