1　本題の証明

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. $M=1000000007$ 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。

$x\geq 1,\ y\geq 1$ のときマス (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] $A\geq 2$ **のとき**

$A\geq 2$ ならば $A'\geq 2$ なので，$r\geq 1,\ c\geq 1$ である。

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，

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

であるから，r,c は一意的に定まる。

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，

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

とおく。M が素数なので，補題 1 により法 M に関する U, u の逆元 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：

$$\begin{aligned} r &\equiv SU' \mod M \quad (\because \text{補題 } 2) \\ &\equiv su' \mod M \quad (\because \text{補題 } 3) \\ c &\equiv TU' \mod M \quad (\because \text{補題 } 2) \\ &\equiv tu' \mod M \quad (\because \text{補題 } 3) \end{aligned}$$

このことと定理 1 により，

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

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。

[2] $A = 0$ または $A = 1$ のとき

TODO □

2　逆元の性質に関する証明

補題 1. M が素数のとき，任意の整数 x に対して，法 M に関する x の逆元 x' が $0 \leq x' < M$ の範囲に唯一つ存在する。

証明. □

補題 2. 任意の整数 x, y に対して，法 M に関する y の逆元 y' が存在するならば，

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

が成り立つ。

証明. □

補題 3. 任意の整数 x, y の法 M に関する逆元をそれぞれ x', y' とおくと

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

が成り立つ。

証明. □

3　フェルマーの小定理の証明

整数 m (≥ 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 4. 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 5. 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 (≥ 1) で割り切れるから，$P(1)$ が成り立つ。

ある $n = k$ (≥ 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

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

なので，$P(k+1)$ も成り立つ。

以上より，補題 5 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 4, 補題 5 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。 □