

※その他、証明すべき命題（その2）

a, b を互いに素である奇素数と置く。この時

$$\begin{aligned} ind\ a \equiv 0, 2, 4, 6, 8, \dots, b-3 \pmod{b-1} \\ \Rightarrow \frac{b-1}{2} ind\ a \equiv 0 \pmod{b-1} \end{aligned}$$

∴

$ind\ a \equiv 0, 2, 4, 6, 8, \dots, b-3 \pmod{b-1}$ の時

$2A = 0, 2, 4, 6, 8, \dots, b-3$ と置くと

$$ind\ a \equiv 2A \pmod{b-1}$$

この時

$$ind\ a = 2A + (b-1)s \quad (s \text{ はある整数})$$

∴

$$\begin{aligned} \frac{b-1}{2} ind\ a &\equiv \frac{b-1}{2} \times \{2A + (b-1)s\} \pmod{b-1} \\ &\equiv \frac{b-1}{2} \cdot 2A + \frac{b-1}{2} \cdot (b-1)s \pmod{b-1} \\ &\equiv (b-1)A + \frac{b-1}{2} (b-1)s \pmod{b-1} \end{aligned}$$

この時 $\frac{b-1}{2}$ は整数より、 $m_1 = \frac{b-1}{2}$ と置けば

$$\frac{b-1}{2} ind\ a \equiv (b-1)A + m_1(b-1)s \pmod{b-1}$$

$$\frac{b-1}{2} ind\ a \equiv (b-1)(A + m_1s) \pmod{b-1}$$

∴

$$\frac{b-1}{2} ind\ a \equiv 0 \pmod{b-1}$$

以上より上記の命題が成立する。

a, b を互いに素である奇素数と置く。この時

$$\frac{b-1}{2} \text{ind } a \equiv 0 \pmod{b-1} \quad \Leftrightarrow \quad a^{\frac{b-1}{2}} \equiv 1 \pmod{b}$$

$$\text{I. } \frac{b-1}{2} \text{ind } a \equiv 0 \pmod{b-1} \quad \Rightarrow \quad a^{\frac{b-1}{2}} \equiv 1 \pmod{b}$$

$\therefore$

$$\frac{b-1}{2} \text{ind } a \equiv 0 \pmod{b-1} \text{ の時}$$

$$\frac{b-1}{2} \text{ind } a \equiv \text{ind } a^{\frac{b-1}{2}} \pmod{b-1} \text{ より}$$

$$\text{ind } a^{\frac{b-1}{2}} \equiv 0 \pmod{b-1} \text{ ---①}$$

また、 $\gamma_1 = 0$ ---② と置き

$$\gamma_1 = \text{ind } L \text{ ---③ とすると}$$

$$L \equiv g_b^{\gamma_1} \pmod{b} \text{ と置ける。}$$

この時、②より

$$L \equiv g_b^0 \pmod{b}$$

$$\therefore L \equiv 1 \pmod{b}$$

$$\therefore L = 1 + bt \quad (t \text{はある整数}) \text{ ---④}$$

④を ③に代入して

$$\gamma_1 = \text{ind } (1 + bt) \text{ ---⑤}$$

また、②より

$$0 = \text{ind } (1 + bt) \text{ ---⑥}$$

従って、⑥を ①に代入して

$$\text{ind } a^{\frac{b-1}{2}} \equiv \text{ind } (1 + bt) \pmod{b-1} \quad \text{---⑦}$$

また、この時

$$\gamma_2 = \text{ind } a^{\frac{b-1}{2}} \quad \text{---⑧} \quad \text{と置け}$$

$$\therefore a^{\frac{b-1}{2}} \equiv g_b^{\gamma_2} \pmod{b}$$

$$\therefore g_b^{\gamma_2} \equiv a^{\frac{b-1}{2}} \pmod{b} \quad \text{---⑨}$$

また、⑤より

$$\gamma_1 = \text{ind } (1 + bt) \quad \text{であるため}$$

$$(1 + bt) \equiv g_b^{\gamma_1} \pmod{b}$$

$$\therefore g_b^{\gamma_1} \equiv (1 + bt) \pmod{b} \quad \text{---⑩}$$

この時、⑦に ⑤ , ⑧を代入して

$$\gamma_2 \equiv \gamma_1 \pmod{b-1}$$

$$\therefore \gamma_1 \equiv \gamma_2 \pmod{b-1}$$

$$\therefore \gamma_1 \equiv \gamma_2 \pmod{c}$$

この時、 g_b は原始根ゆえ、法 b に関してべき数 c に属する。

$$\therefore g_b^{\gamma_1} \equiv g_b^{\gamma_2} \pmod{b} \quad \text{---⑪}$$

従って、⑨ , ⑩を ⑪に代入して、

$$\therefore (1 + bt) \equiv a^{\frac{b-1}{2}} \pmod{b}$$

$$\therefore a^{\frac{b-1}{2}} \equiv (1 + bt) \pmod{b}$$

$$\therefore a^{\frac{b-1}{2}} \equiv 1 + bt \pmod{b}$$

$$\therefore a^{\frac{b-1}{2}} \equiv 1 \pmod{b}$$

以上より上記の命題が成立する。

$$\text{II. } a^{\frac{b-1}{2}} \equiv 1 \pmod{b} \Rightarrow \frac{b-1}{2} \text{ ind } a \equiv 0 \pmod{b-1}$$

$\therefore$

$$a^{\frac{b-1}{2}} \equiv 1 \pmod{b} \text{ の時}$$

$$g_b^0 = 1 \text{ と置け}$$

$$g_b^0 \equiv 1 \pmod{b} \text{ である事から}$$

$$a^{\frac{b-1}{2}} \equiv g_b^0 \pmod{b}$$

この時 $0 = \text{ind } a^{\frac{b-1}{2}}$ であり、

$$\therefore 0 \equiv \text{ind } a^{\frac{b-1}{2}} \pmod{b-1}$$

また $\text{ind } a^{\frac{b-1}{2}} \equiv \frac{b-1}{2} \text{ ind } a \pmod{b-1}$ である事から

$$0 \equiv \frac{b-1}{2} \text{ ind } a \pmod{b-1}$$

$$\therefore \frac{b-1}{2} \text{ ind } a \equiv 0 \pmod{b-1}$$

以上より上記の命題が成立する。

従って I. II. より

a, b を互いに素である奇素数と置く。この時

$$\frac{b-1}{2} \text{ ind } a \equiv 0 \pmod{b-1} \quad \Leftrightarrow \quad a^{\frac{b-1}{2}} \equiv 1 \pmod{b}$$

が成立する。

a, b を互いに素である奇素数と置く。この時

$$\text{ind } a \equiv 1, 3, 5, 7, 9, \dots, b-2 \pmod{b-1}$$

$$\Rightarrow \frac{b-1}{2} \text{ind } a \equiv \text{ind } b-1 \pmod{b-1}$$

$\therefore$

$$\text{ind } a \equiv 1, 3, 5, 7, 9, \dots, b-2 \pmod{b-1} \text{ の時}$$

$$2B+1 = 1, 3, 5, 7, 9, \dots, b-2 \text{ と置くと}$$

$$\text{ind } a \equiv 2B+1 \pmod{b-1}$$

この時

$$\text{ind } a = 2B+1 + (b-1)u \quad (u \text{はある整数})$$

$\therefore$

$$(\text{左辺}) = \frac{b-1}{2} \text{ind } a \text{ ---① と置くと}$$

$$(\text{左辺}) \equiv \frac{b-1}{2} \text{ind } a \pmod{b-1}$$

$$\equiv \frac{b-1}{2} \times \{2B+1 + (b-1)u\} \pmod{b-1}$$

$$\equiv \frac{b-1}{2} \cdot (2B+1) + \frac{b-1}{2} \cdot (b-1)u \pmod{b-1}$$

$$\equiv \frac{b-1}{2} \cdot (2B+1) \pmod{b-1}$$

$$\equiv (b-1)B + \frac{b-1}{2} \pmod{b-1}$$

$$\equiv \frac{b-1}{2} \pmod{b-1}$$

$\therefore$

$$(\text{左辺}) \equiv \frac{b-1}{2} \pmod{b-1} \text{ ---※}_1$$

また、(右辺) = $\text{ind } b - 1$ __② と置く時

$$\gamma_3 = \text{ind } b - 1 \text{ __③}$$

$$b - 1 \equiv g_b^{\gamma_3} \pmod{b}$$

$$\therefore -1 \equiv g_b^{\gamma_3} \pmod{b}$$

この時、 $g_b^{\gamma_3} \equiv -1 \pmod{b}$ より

$$\gamma_3 = \frac{b-1}{2} \text{ __④}$$

従って、この時 ③に ④を代入して

$$\frac{b-1}{2} = \text{ind } b - 1$$

$$\therefore \text{ind } b - 1 = \frac{b-1}{2} \text{ __⑤}$$

従って、⑤を ②に代入して

$$(\text{右辺}) = \frac{b-1}{2}$$

$$(\text{右辺}) \equiv \frac{b-1}{2} \pmod{b-1} \text{ __※}_2$$

この時、※₁ , ※₂ より

$$(\text{左辺}) \equiv (\text{右辺}) \pmod{b-1}$$

この時、① , ②より

$$\frac{b-1}{2} \text{ind } a \equiv \text{ind } b - 1 \pmod{b-1}$$

以上より上記の命題が成立する。

a, b を互いに素である奇素数と置く。この時

$$\frac{b-1}{2} \text{ind } a \equiv \text{ind } b-1 \pmod{b-1} \quad \Leftrightarrow \quad a^{\frac{b-1}{2}} \equiv -1 \pmod{b}$$

$$\text{I. } \frac{b-1}{2} \text{ind } a \equiv \text{ind } b-1 \pmod{b-1} \quad \Rightarrow \quad a^{\frac{b-1}{2}} \equiv -1 \pmod{b}$$

$\therefore$

$$\frac{b-1}{2} \text{ind } a \equiv \text{ind } b-1 \pmod{b-1} \text{ の時}$$

$$\frac{b-1}{2} \text{ind } a \equiv \text{ind } a^{\frac{b-1}{2}} \pmod{b-1} \quad \text{より}$$

$$\text{ind } a^{\frac{b-1}{2}} \equiv \text{ind } b-1 \pmod{b-1} \quad \text{---①}$$

$$\text{また、} \gamma_4 = \text{ind } a^{\frac{b-1}{2}} \quad \text{---②} \quad \text{と置くと}$$

$$a^{\frac{b-1}{2}} \equiv g_b^{\gamma_4} \pmod{b}$$

$$g_b^{\gamma_4} \equiv a^{\frac{b-1}{2}} \pmod{b} \quad \text{---③}$$

$$\text{また } \gamma_5 = \text{ind } b-1 \quad \text{---④} \quad \text{と置くと}$$

$$b-1 \equiv g_b^{\gamma_5} \pmod{b}$$

$$g_b^{\gamma_5} \equiv b-1 \pmod{b} \quad \text{---⑤}$$

この時、①に ②と ④を代入して

$$\gamma_4 \equiv \gamma_5 \pmod{b-1}$$

$$\therefore \gamma_4 \equiv \gamma_5 \pmod{c}$$

この時、 g_b は原始根ゆえ、法 b に関してべき数 c に属する。

$$g_b^{\gamma_4} \equiv g_b^{\gamma_5} \pmod{b} \quad \text{---⑥}$$

この時、③と ⑤を ⑥に代入すると

$$a^{\frac{b-1}{2}} \equiv b-1 \pmod{b}$$

$$\therefore a^{\frac{b-1}{2}} \equiv -1 \pmod{b}$$

以上より、上記の命題が成立する。

$$\text{II. } a^{\frac{b-1}{2}} \equiv -1 \pmod{b} \quad \Rightarrow \quad \frac{b-1}{2} \text{ ind } a \equiv \text{ind } b - 1 \pmod{b-1}$$

$\therefore$

$$a^{\frac{b-1}{2}} \equiv -1 \pmod{b} \quad \text{---①} \quad \text{の時}$$

$$g_b^{\gamma_6} \equiv -1 \pmod{b} \quad \text{と置くと}$$

$$\gamma_6 = \frac{b-1}{2}$$

$$g_b^{\frac{b-1}{2}} \equiv -1 \pmod{b} \quad \text{---②}$$

この時

$$g_b^{\frac{b-1}{2}} \equiv b-1 \pmod{b}$$

$$\therefore \frac{b-1}{2} = \text{ind } b - 1$$

$$\therefore \frac{b-1}{2} \equiv \text{ind } b - 1 \pmod{b-1} \text{ ---③}$$

また、②を ①に代入して

$$a^{\frac{b-1}{2}} \equiv g_b^{\frac{b-1}{2}} \pmod{b}$$

$$\therefore \frac{b-1}{2} = \text{ind } a^{\frac{b-1}{2}}$$

$$\therefore \frac{b-1}{2} \equiv \text{ind } a^{\frac{b-1}{2}} \pmod{b-1} \text{ ---④}$$

この時、③に ④を代入して

$$\text{ind } a^{\frac{b-1}{2}} \equiv \text{ind } b - 1 \pmod{b-1}$$

$$\text{また、} \text{ind } a^{\frac{b-1}{2}} \equiv \frac{b-1}{2} \text{ind } a \pmod{b-1} \text{ より}$$

$$\frac{b-1}{2} \text{ind } a \equiv \text{ind } b - 1 \pmod{b-1}$$

以上より、上記の命題が成立する。

従って I . II . より

a, b を互いに素である奇素数と置く。この時

$$\frac{b-1}{2} \text{ind } a \equiv \text{ind } b - 1 \pmod{b-1} \quad \Leftrightarrow \quad a^{\frac{b-1}{2}} \equiv -1 \pmod{b}$$

が成立する。