

平方剰余の相互法則

$p = 4m_1 + 3$ $q = 4m_2 + 3$ の時

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$$

この時、 $1 = 1$ を生成する素数のペアを探したければ

i. $\left(\frac{q}{p}\right) = 1$ かつ $\left(\frac{p}{q}\right) = -1$ のペアを探すか

ii. $\left(\frac{q}{p}\right) = -1$ かつ $\left(\frac{p}{q}\right) = 1$ のペアを探す。

この時、 $1 = -1$ を生成する素数のペアを探したければ

iii. $\left(\frac{q}{p}\right) = 1$ かつ $\left(\frac{p}{q}\right) = 1$ のペアを探すか

iv. $\left(\frac{q}{p}\right) = -1$ かつ $\left(\frac{p}{q}\right) = -1$ のペアを探す。

◎ $1 = 1$ を生成する素数のペアを探す時

【 i である場合】

$$\begin{aligned}\left(\frac{q}{p}\right) = 1 &\Leftrightarrow q^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow \text{ind } q \equiv 0, 2, 4, 6, 8, \dots, p-3 \pmod{p-1} \\ &\Leftrightarrow q \equiv g_p^{2A_1} \pmod{p} \quad (2A_1 = 0, 2, 4, 6, 8, \dots, p-3)\end{aligned}$$

かつ

$$\begin{aligned}\left(\frac{p}{q}\right) = -1 &\Leftrightarrow p^{\frac{q-1}{2}} \equiv -1 \pmod{q} \Leftrightarrow \text{ind } p \equiv 1, 3, 5, 7, 9, \dots, q-2 \pmod{q-1} \\ &\Leftrightarrow p \equiv g_q^{2B_1+1} \pmod{q} \quad (2B_1+1 = 1, 3, 5, 7, 9, \dots, q-2)\end{aligned}$$

【 ii である場合】

$$\begin{aligned}\left(\frac{q}{p}\right) = -1 &\Leftrightarrow q^{\frac{p-1}{2}} \equiv -1 \pmod{p} \Leftrightarrow \text{ind } q \equiv 1, 3, 5, 7, 9, \dots, p-2 \pmod{p-1} \\ &\Leftrightarrow q \equiv g_p^{2A_2+1} \pmod{p} \quad (2A_2+1 = 1, 3, 5, 7, 9, \dots, p-2)\end{aligned}$$

かつ

$$\begin{aligned}\left(\frac{p}{q}\right) = 1 &\Leftrightarrow p^{\frac{q-1}{2}} \equiv 1 \pmod{q} \Leftrightarrow \text{ind } p \equiv 0, 2, 4, 6, 8, \dots, q-3 \pmod{q-1} \\ &\Leftrightarrow p \equiv g_q^{2B_2} \pmod{q} \quad (2B_2 = 0, 2, 4, 6, 8, \dots, q-3)\end{aligned}$$

◎ $1 = -1$ を生成する素数のペアを探す時

【iiiである場合】

$$\begin{aligned} \left(\frac{q}{p}\right) = 1 &\Leftrightarrow q^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow \text{ind } q \equiv 0, 2, 4, 6, 8, \dots, p-3 \pmod{p-1} \\ &\Leftrightarrow q \equiv g_p^{2A'_1} \pmod{p} \quad (2A'_1 = 0, 2, 4, 6, 8, \dots, p-3) \end{aligned}$$

かつ

$$\begin{aligned} \left(\frac{p}{q}\right) = 1 &\Leftrightarrow p^{\frac{q-1}{2}} \equiv 1 \pmod{q} \Leftrightarrow \text{ind } p \equiv 0, 2, 4, 6, 8, \dots, q-3 \pmod{q-1} \\ &\Leftrightarrow p \equiv g_q^{2B'_1} \pmod{q} \quad (2B'_1 = 0, 2, 4, 6, 8, \dots, q-3) \end{aligned}$$

【ivである場合】

$$\begin{aligned} \left(\frac{q}{p}\right) = -1 &\Leftrightarrow q^{\frac{p-1}{2}} \equiv -1 \pmod{p} \Leftrightarrow \text{ind } q \equiv 1, 3, 5, 7, 9, \dots, p-2 \pmod{p-1} \\ &\Leftrightarrow q \equiv g_p^{2A'_2+1} \pmod{p} \quad (2A'_2 + 1 = 1, 3, 5, 7, 9, \dots, p-2) \end{aligned}$$

かつ

$$\begin{aligned} \left(\frac{p}{q}\right) = -1 &\Leftrightarrow p^{\frac{q-1}{2}} \equiv -1 \pmod{q} \Leftrightarrow \text{ind } p \equiv 1, 3, 5, 7, 9, \dots, q-2 \pmod{q-1} \\ &\Leftrightarrow p \equiv g_q^{2B'_2+1} \pmod{q} \quad (2B'_2 + 1 = 1, 3, 5, 7, 9, \dots, q-2) \end{aligned}$$

【 i である場合】

$$\begin{aligned}
 (g_p, q) = 1 \quad \text{かつ} \quad (g_q, p) = 1 \quad \text{である時} \\
 q \equiv g_p^{2A_1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B_1+1} \pmod{q} \\
 \Leftrightarrow g_p^{2A_1}p + g_q^{2B_1+1}q \equiv g_p^{2A_1}g_q^{2B_1+1} \pmod{pq} \quad \text{の証明}
 \end{aligned}$$

$$\begin{aligned}
 \text{I.} \quad (g_p, q) = 1 \quad \text{かつ} \quad (g_q, p) = 1 \quad \text{である時} \\
 q \equiv g_p^{2A_1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B_1+1} \pmod{q} \\
 \Rightarrow g_p^{2A_1}p + g_q^{2B_1+1}q \equiv g_p^{2A_1}g_q^{2B_1+1} \pmod{pq}
 \end{aligned}$$

∴

$$q \equiv g_p^{2A_1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B_1+1} \pmod{q} \quad \text{である時}$$

$$p + q \equiv g_p^{2A_1} \pmod{p} \quad \text{かつ} \quad p + q \equiv g_q^{2B_1+1} \pmod{q} \quad \text{—※— であるから}$$

$M_s M'_s$ を条件

$$m_1 = p, \quad M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, \quad M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$a_0 = M_1 M'_1 g_p^{2A_1} + M_2 M'_2 g_q^{2B_1+1}$$

とする。

この時、連立合同式※を満足する a の値の全体は合同式

$$a \equiv a_0 \pmod{pq} \quad (a = p + q)$$

$$a \equiv M_1 M'_1 g_p^{2A_1} + M_2 M'_2 g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p + q \equiv M_1 M'_1 g_p^{2A_1} + M_2 M'_2 g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p + q \equiv q M'_1 g_p^{2A_1} + p M'_2 g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p + q \equiv (1 + ap) g_p^{2A_1} + (1 + bq) g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_1} + ap g_p^{2A_1} + g_q^{2B_1+1} + bq g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_1} + a g_p^{2A_1} p + g_q^{2B_1+1} + b g_q^{2B_1+1} q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_1} + (aq + np)p + g_q^{2B_1+1} + (bp + mq)q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_1} + apq + np^2 + g_q^{2B_1+1} + bpq + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_1} + np^2 + g_q^{2B_1+1} + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv np^2 + mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{pq}$$

この時上記の命題は

$$p + q \equiv np^2 + mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{p} \text{ ---①}$$

かつ

$$p + q \equiv np^2 + mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{q} \text{ ---②}$$

と同値である。

① の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{p}$$

$$q \equiv mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{p}$$

$$g_p^{2A_1} \equiv mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{p}$$

$$g_p^{2A_1} \equiv mqq + g_p^{2A_1} + g_q^{2B_1+1} \pmod{p}$$

$$0 \equiv mg_p^{2A_1}q + g_q^{2B_1+1} \pmod{p}$$

$$mg_p^{2A_1}q + g_q^{2B_1+1} \equiv 0 \pmod{p}$$

$$mg_p^{2A_1}q \equiv -g_q^{2B_1+1} \pmod{p}$$

$$mg_p^{2A_1}q^2 \equiv -g_q^{2B_1+1}q \pmod{pq} \text{ ---①'}$$

② の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{q}$$

$$p \equiv np^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{q}$$

$$p \equiv npp + g_p^{2A_1} + g_q^{2B_1+1} \pmod{q}$$

$$g_q^{2B_1+1} \equiv ng_q^{2B_1+1}p + g_p^{2A_1} + g_q^{2B_1+1} \pmod{q}$$

$$0 \equiv ng_q^{2B_1+1}p + g_p^{2A_1} \pmod{q}$$

$$ng_q^{2B_1+1}p + g_p^{2A_1} \equiv 0 \pmod{q}$$

$$ng_q^{2B_1+1}p \equiv -g_p^{2A_1} \pmod{q}$$

$$ng_q^{2B_1+1}p^2 \equiv -g_p^{2A_1}p \pmod{pq} \text{ ---②'}$$

また、 $p + q \equiv np^2 + mq^2 + g_p^{2A_1} + g_q^{2B_1+1} \pmod{pq}$ である時

$g_p^{2A_1}g_q^{2B_1+1}$ を両辺に掛けて

$$g_p^{2A_1}g_q^{2B_1+1}(p + q) \equiv g_p^{2A_1}g_q^{2B_1+1}(np^2 + mq^2 + g_p^{2A_1} + g_q^{2B_1+1}) \pmod{pq}$$

$$\begin{aligned} & g_p^{2A_1}g_q^{2B_1+1}p + g_p^{2A_1}g_q^{2B_1+1}q \\ & \equiv g_p^{2A_1}g_q^{2B_1+1}np^2 + g_p^{2A_1}g_q^{2B_1+1}mq^2 + g_p^{2A_1}g_q^{2B_1+1}g_p^{2A_1} + g_p^{2A_1}g_q^{2B_1+1}g_q^{2B_1+1} \pmod{pq} \end{aligned}$$

$$\begin{aligned}
& g_p^{2A_1} g_q^{2B_1+1} p + g_p^{2A_1} g_q^{2B_1+1} q \\
& \equiv g_p^{2A_1} (g_q^{2B_1+1} n p^2) + g_q^{2B_1+1} (g_p^{2A_1} m q^2) + g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}
\end{aligned}$$

この時 ①' ②' より

$$\begin{aligned}
& g_p^{2A_1} g_q^{2B_1+1} p + g_p^{2A_1} g_q^{2B_1+1} q \\
& \equiv g_p^{2A_1} (-g_p^{2A_1} p) + g_q^{2B_1+1} (-g_q^{2B_1+1} q) + g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A_1} g_q^{2B_1+1} p + g_p^{2A_1} g_q^{2B_1+1} q + g_p^{2A_1} (g_p^{2A_1} p) + g_q^{2B_1+1} (g_q^{2B_1+1} q) \\
& \equiv g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}
\end{aligned}$$

$$g_p^{2A_1} g_q^{2B_1+1} p + g_p^{2A_1} g_q^{2B_1+1} q + g_p^{4A_1} p + g_q^{4B_1+2} q \equiv g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}$$

$$g_p^{4A_1} p + g_p^{2A_1} g_q^{2B_1+1} p + g_p^{2A_1} g_q^{2B_1+1} q + g_q^{4B_1+2} q \equiv g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}$$

$$g_p^{2A_1} (g_p^{2A_1} + g_q^{2B_1+1}) p + g_q^{2B_1+1} (g_p^{2A_1} + g_q^{2B_1+1}) q \equiv g_p^{2A_1} g_q^{2B_1+1} (g_p^{2A_1} + g_q^{2B_1+1}) \pmod{pq}$$

____※₁

又、 $q \equiv g_p^{2A_1} \pmod{p}$ かつ $p \equiv g_q^{2B_1+1} \pmod{q}$ である時
 $-q \equiv -g_p^{2A_1} \pmod{p}$ かつ $p \equiv g_q^{2B_1+1} \pmod{q}$

$p - q \equiv -g_p^{2A_1} \pmod{p}$ かつ $p - q \equiv g_q^{2B_1+1} \pmod{q}$ であるから

$M_s M'_s$ を条件

$$m_1 = p, M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$b_0 = -M_1 M'_1 g_p^{2A_1} + M_2 M'_2 g_q^{2B_1+1}$$

とする。

この時、連立合同式※を満足する b の値の全体は合同式

$$b \equiv b_0 \pmod{pq} \quad (b = p - q)$$

$$b \equiv -M_1 M'_1 g_p^{2A_1} + M_2 M'_2 g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p - q \equiv -M_1 M'_1 g_p^{2A_1} + M_2 M'_2 g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p - q \equiv -q M'_1 g_p^{2A_1} + p M'_2 g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p - q \equiv -(1 + ap) g_p^{2A_1} + (1 + bq) g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_1} - ap g_p^{2A_1} + g_q^{2B_1+1} + bq g_q^{2B_1+1} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_1} - a g_p^{2A_1} p + g_q^{2B_1+1} + b g_q^{2B_1+1} q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_1} - (aq + np) p + g_q^{2B_1+1} + (bp + mq) q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_1} - apq - np^2 + g_q^{2B_1+1} + bpq + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_1} - np^2 + g_q^{2B_1+1} + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -np^2 + mq^2 - g_p^{2A_1} + g_q^{2B_1+1} \pmod{pq}$$

また、 $p - q \equiv -np^2 + mq^2 - g_p^{2A_1} + g_q^{2B_1+1} \pmod{pq}$ である時

$g_p^{2A_1} g_q^{2B_1+1}$ を両辺に掛けて

$$g_p^{2A_1} g_q^{2B_1+1} (p - q) \equiv g_p^{2A_1} g_q^{2B_1+1} (-np^2 + mq^2 - g_p^{2A_1} + g_q^{2B_1+1}) \pmod{pq}$$

$$g_p^{2A_1} g_q^{2B_1+1} p - g_p^{2A_1} g_q^{2B_1+1} q$$

$$\equiv -g_p^{2A_1} g_q^{2B_1+1} np^2 + g_p^{2A_1} g_q^{2B_1+1} mq^2 - g_p^{2A_1} g_q^{2B_1+1} g_p^{2A_1} + g_p^{2A_1} g_q^{2B_1+1} g_q^{2B_1+1} \pmod{pq}$$

$$g_p^{2A_1} g_q^{2B_1+1} p - g_p^{2A_1} g_q^{2B_1+1} q$$

$$\equiv -g_p^{2A_1} (g_q^{2B_1+1} np^2) + g_q^{2B_1+1} (g_p^{2A_1} mq^2) - g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}$$

この時 ①' ②' より

$$\begin{aligned} & g_p^{2A_1} g_q^{2B_1+1} p - g_p^{2A_1} g_q^{2B_1+1} q \\ & \equiv -g_p^{2A_1} (-g_p^{2A_1} p) + g_q^{2B_1+1} (-g_q^{2B_1+1} q) - g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_1} g_q^{2B_1+1} p - g_p^{2A_1} g_q^{2B_1+1} q - g_p^{2A_1} (g_p^{2A_1} p) + g_q^{2B_1+1} (g_q^{2B_1+1} q) \\ & \equiv -g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq} \end{aligned}$$

$$g_p^{2A_1} g_q^{2B_1+1} p - g_p^{2A_1} g_q^{2B_1+1} q - g_p^{4A_1} p + g_q^{4B_1+2} q \equiv -g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}$$

$$-g_p^{4A_1} p + g_p^{2A_1} g_q^{2B_1+1} p - g_p^{2A_1} g_q^{2B_1+1} q + g_q^{4B_1+2} q \equiv -g_p^{4A_1} g_q^{2B_1+1} + g_p^{2A_1} g_q^{4B_1+2} \pmod{pq}$$

$$g_p^{2A_1} (g_q^{2B_1+1} - g_p^{2A_1}) p + g_q^{2B_1+1} (g_q^{2B_1+1} - g_p^{2A_1}) q \equiv g_p^{2A_1} g_q^{2B_1+1} (g_q^{2B_1+1} - g_p^{2A_1}) \pmod{pq}$$

$$-g_p^{2A_1} (g_p^{2A_1} - g_q^{2B_1+1}) p - g_q^{2B_1+1} (g_p^{2A_1} - g_q^{2B_1+1}) q \equiv -g_p^{2A_1} g_q^{2B_1+1} (g_p^{2A_1} - g_q^{2B_1+1}) \pmod{pq}$$

$$g_p^{2A_1} (g_p^{2A_1} - g_q^{2B_1+1}) p + g_q^{2B_1+1} (g_p^{2A_1} - g_q^{2B_1+1}) q \equiv g_p^{2A_1} g_q^{2B_1+1} (g_p^{2A_1} - g_q^{2B_1+1}) \pmod{pq}$$

____ $\times_2$

この時 $\times_1 + \times_2$ より

$$\begin{aligned} g_p^{2A_1}(g_p^{2A_1} + g_q^{2B_1+1})p + g_q^{2B_1+1}(g_p^{2A_1} + g_q^{2B_1+1})q \\ + g_p^{2A_1}(g_p^{2A_1} - g_q^{2B_1+1})p + g_q^{2B_1+1}(g_p^{2A_1} - g_q^{2B_1+1})q \\ \equiv g_p^{2A_1}g_q^{2B_1+1}(g_p^{2A_1} + g_q^{2B_1+1}) + g_p^{2A_1}g_q^{2B_1+1}(g_p^{2A_1} - g_q^{2B_1+1}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} g_p^{2A_1}(g_p^{2A_1} + g_q^{2B_1+1})p + g_p^{2A_1}(g_p^{2A_1} - g_q^{2B_1+1})p \\ + g_q^{2B_1+1}(g_p^{2A_1} + g_q^{2B_1+1})q + g_q^{2B_1+1}(g_p^{2A_1} - g_q^{2B_1+1})q \\ \equiv g_p^{2A_1}g_q^{2B_1+1}(g_p^{2A_1} + g_q^{2B_1+1}) + g_p^{2A_1}g_q^{2B_1+1}(g_p^{2A_1} - g_q^{2B_1+1}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} g_p^{2A_1}(g_p^{2A_1} + g_q^{2B_1+1} + g_p^{2A_1} - g_q^{2B_1+1})p + g_q^{2B_1+1}(g_p^{2A_1} + g_q^{2B_1+1} + g_p^{2A_1} - g_q^{2B_1+1})q \\ \equiv g_p^{2A_1}g_q^{2B_1+1}(g_p^{2A_1} + g_q^{2B_1+1} + g_p^{2A_1} - g_q^{2B_1+1}) \pmod{pq} \\ g_p^{2A_1}(g_p^{2A_1} + g_p^{2A_1})p + g_q^{2B_1+1}(g_p^{2A_1} + g_p^{2A_1})q \equiv g_p^{2A_1}g_q^{2B_1+1}(g_p^{2A_1} + g_p^{2A_1}) \pmod{pq} \end{aligned}$$

$$g_p^{2A_1}p \times 2g_p^{2A_1} + g_q^{2B_1+1}q \times 2g_p^{2A_1} \equiv g_p^{2A_1}g_q^{2B_1+1} \times 2g_p^{2A_1} \pmod{pq}$$

この時 $(2, pq) = 1$ より両辺を 2 で割って

$$g_p^{2A_1}p \times g_p^{2A_1} + g_q^{2B_1+1}q \times g_p^{2A_1} \equiv g_p^{2A_1}g_q^{2B_1+1} \times g_p^{2A_1} \pmod{pq}$$

$$\therefore g_p^{4A_1}p + g_q^{2B_1+1}g_p^{2A_1}q \equiv g_p^{4A_1}g_q^{2B_1+1} \pmod{pq}$$

この時 $(g_p, p) = 1$ $(g_p, q) = 1$ より $(g_p, pq) = 1$

$$\therefore (g_p^{2A_1}, pq) = 1$$

従って両辺を $g_p^{2A_1}$ で割って

$$g_p^{2A_1}p + g_q^{2B_1+1}q \equiv g_p^{2A_1}g_q^{2B_1+1} \pmod{pq}$$

II. $(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$g_p^{2A_1} p + g_q^{2B_1+1} q \equiv g_p^{2A_1} g_q^{2B_1+1} \pmod{pq}$$

$$\Rightarrow q \equiv g_p^{2A_1} \pmod{p} \text{ かつ } p \equiv g_q^{2B_1+1} \pmod{q}$$

$\therefore$

$$g_p^{2A_1} p + g_q^{2B_1+1} q \equiv g_p^{2A_1} g_q^{2B_1+1} \pmod{pq} \text{ の時}$$

上記の方程式は

$$g_p^{2A_1} p + g_q^{2B_1+1} q \equiv g_p^{2A_1} g_q^{2B_1+1} \pmod{p}$$

かつ

$$g_p^{2A_1} p + g_q^{2B_1+1} q \equiv g_p^{2A_1} g_q^{2B_1+1} \pmod{q}$$

と同値である。

又、上記の方程式は

$$g_q^{2B_1} q \equiv g_p^{2A_1} g_q^{2B_1+1} \pmod{p}$$

かつ

$$g_p^{2A_1} p \equiv g_p^{2A_1} g_q^{2B_1+1} \pmod{q} \text{ ---}\star_1$$

と同値である。

この時 $(g_q, p) = 1$ より $(g_q^{2B_1+1}, p) = 1$

又、 $(g_p, q) = 1$ より $(g_p^{2A_1}, q) = 1$

従って、上記の方程式の両辺を $g_q^{2B_1+1}$, $g_p^{2A_1}$ でそれぞれ割って

$$q \equiv g_p^{2A_1} \pmod{p}$$

かつ

$$p \equiv g_q^{2B_1+1} \pmod{q} \text{ ---}\star_2$$

この時、 $\star_2$ の方程式のそれぞれに $g_q^{2B_1+1}$, $g_p^{2A_1}$ を掛け合わせると

$\star_1$ の方程式へと戻するため $\star_1$ の方程式と $\star_2$ の方程式は同値である。

以上より、上記の命題が成立する。

【ii である場合】

$(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$q \equiv g_p^{2A_2+1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B_2} \pmod{q}$$

$$\Leftrightarrow g_p^{2A_2+1}p + g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{pq} \quad \text{の証明}$$

I. $(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$q \equiv g_p^{2A_2+1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B_2} \pmod{q}$$

$$\Rightarrow g_p^{2A_2+1}p + g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{pq}$$

$\therefore$

$q \equiv g_p^{2A_2+1} \pmod{p}$ かつ $p \equiv g_q^{2B_2} \pmod{q}$ である時

$p + q \equiv g_p^{2A_2+1} \pmod{p}$ かつ $p + q \equiv g_q^{2B_2} \pmod{q}$ —※— であるから

$M_s M'_s$ を条件

$$m_1 = p, M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$a_0 = M_1 M'_1 g_p^{2A_2+1} + M_2 M'_2 g_q^{2B_2}$$

とする。

この時、連立合同式※を満足する a の値の全体は合同式

$$a \equiv a_0 \pmod{pq} \quad (a = p + q)$$

$$a \equiv M_1 M'_1 g_p^{2A_2+1} + M_2 M'_2 g_q^{2B_2} \pmod{pq}$$

$$\therefore p + q \equiv M_1 M'_1 g_p^{2A_2+1} + M_2 M'_2 g_q^{2B_2} \pmod{pq}$$

$$\therefore p + q \equiv q M'_1 g_p^{2A_2+1} + p M'_2 g_q^{2B_2} \pmod{pq}$$

$$\therefore p + q \equiv (1 + ap) g_p^{2A_2+1} + (1 + bq) g_q^{2B_2} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_2+1} + ap g_p^{2A_2+1} + g_q^{2B_2} + bq g_q^{2B_2} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_2+1} + a g_p^{2A_2+1} p + g_q^{2B_2} + b g_q^{2B_2} q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_2+1} + (aq + np) p + g_q^{2B_2} + (bp + mq) q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_2+1} + apq + np^2 + g_q^{2B_2} + bpq + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A_2+1} + np^2 + g_q^{2B_2} + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv np^2 + mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{pq}$$

この時上記の命題は

$$p + q \equiv np^2 + mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{p} \text{ ---③}$$

かつ

$$p + q \equiv np^2 + mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{q} \text{ ---④}$$

と同値である。

③ の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{p}$$

$$q \equiv mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{p}$$

$$g_p^{2A_2+1} \equiv mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{p}$$

$$g_p^{2A_2+1} \equiv mqq + g_p^{2A_2+1} + g_q^{2B_2} \pmod{p}$$

$$0 \equiv mg_p^{2A_2+1}q + g_q^{2B_2} \pmod{p}$$

$$mg_p^{2A_2+1}q + g_q^{2B_2} \equiv 0 \pmod{p}$$

$$mg_p^{2A_2+1}q \equiv -g_q^{2B_2} \pmod{p}$$

$$mg_p^{2A_2+1}q^2 \equiv -g_q^{2B_2}q \pmod{pq} \text{ ---③'}$$

④ の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{q}$$

$$p \equiv np^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{q}$$

$$g_q^{2B_2} \equiv npp + g_p^{2A_2+1} + g_q^{2B_2} \pmod{q}$$

$$g_q^{2B_2} \equiv ng_q^{2B_2}p + g_p^{2A_2+1} + g_q^{2B_2} \pmod{q}$$

$$0 \equiv ng_q^{2B_2}p + g_p^{2A_2+1} \pmod{q}$$

$$ng_q^{2B_2}p + g_p^{2A_2+1} \equiv 0 \pmod{q}$$

$$ng_q^{2B_2}p \equiv -g_p^{2A_2+1} \pmod{q}$$

$$ng_q^{2B_2}p^2 \equiv -g_p^{2A_2+1}p \pmod{pq} \text{ ---④'}$$

また、 $p + q \equiv np^2 + mq^2 + g_p^{2A_2+1} + g_q^{2B_2} \pmod{pq}$ である時

$g_p^{2A_2+1}g_q^{2B_2}$ を両辺に掛けて

$$g_p^{2A_2+1}g_q^{2B_2}(p + q) \equiv g_p^{2A_2+1}g_q^{2B_2}(np^2 + mq^2 + g_p^{2A_2+1} + g_q^{2B_2}) \pmod{pq}$$

$$\begin{aligned}
& g_p^{2A_2+1} g_q^{2B_2} p + g_p^{2A_2+1} g_q^{2B_2} q \\
& \equiv g_p^{2A_2+1} g_q^{2B_2} n p^2 + g_p^{2A_2+1} g_q^{2B_2} m q^2 + g_p^{2A_2+1} g_q^{2B_2} g_p^{2A_2+1} \\
& \quad + g_p^{2A_2+1} g_q^{2B_2} g_q^{2B_2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A_2+1} g_q^{2B_2} p + g_p^{2A_2+1} g_q^{2B_2} q \\
& \equiv g_p^{2A_2+1} (g_q^{2B_2} n p^2) + g_q^{2B_2} (g_p^{2A_2+1} m q^2) + g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq}
\end{aligned}$$

この時 ③' ④' より

$$\begin{aligned}
& g_p^{2A_2+1} g_q^{2B_2} p + g_p^{2A_2+1} g_q^{2B_2} q \\
& \equiv g_p^{2A_2+1} (-g_p^{2A_2+1} p) + g_q^{2B_2} (-g_q^{2B_2} q) + g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A_2+1} g_q^{2B_2} p + g_p^{2A_2+1} g_q^{2B_2} q + g_p^{2A_2+1} (g_p^{2A_2+1} p) + g_q^{2B_2} (g_q^{2B_2} q) \\
& \equiv g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A_2+1} g_q^{2B_2} p + g_p^{2A_2+1} g_q^{2B_2} q + g_p^{4A_2+2} p + g_q^{4B_2} q \\
& \equiv g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{4A_2+2} p + g_p^{2A_2+1} g_q^{2B_2} p + g_p^{2A_2+1} g_q^{2B_2} q + g_q^{4B_2} q \\
& \equiv g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A_2+1} (g_p^{2A_2+1} + g_q^{2B_2}) p + g_q^{2B_2} (g_p^{2A_2+1} + g_q^{2B_2}) q \\
& \equiv g_p^{2A_2+1} g_q^{2B_2} (g_p^{2A_2+1} + g_q^{2B_2}) \pmod{pq} \text{ --- } \times_3
\end{aligned}$$

又、 $q \equiv g_p^{2A_2+1} \pmod{p}$ かつ $p \equiv g_q^{2B_2} \pmod{q}$ である時
 $-q \equiv -g_p^{2A_2+1} \pmod{p}$ かつ $p \equiv g_q^{2B_2} \pmod{q}$

$p - q \equiv -g_p^{2A_2+1} \pmod{p}$ かつ $p - q \equiv g_q^{2B_2} \pmod{q}$ 〓 であるから

$M_s M'_s$ を条件

$$m_1 = p, M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$b_0 = -M_1 M'_1 g_p^{2A_2+1} + M_2 M'_2 g_q^{2B_2}$$

とする。

この時、連立合同式〓を満足する b の値の全体は合同式

$$b \equiv b_0 \pmod{pq} \quad (b = p - q)$$

$$b \equiv -M_1 M'_1 g_p^{2A_2+1} + M_2 M'_2 g_q^{2B_2} \pmod{pq}$$

$$\therefore p - q \equiv -M_1 M'_1 g_p^{2A_2+1} + M_2 M'_2 g_q^{2B_2} \pmod{pq}$$

$$\therefore p - q \equiv -q M'_1 g_p^{2A_2+1} + p M'_2 g_q^{2B_2} \pmod{pq}$$

$$\therefore p - q \equiv -(1 + ap) g_p^{2A_2+1} + (1 + bq) g_q^{2B_2} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_2+1} - ap g_p^{2A_2+1} + g_q^{2B_2} + bq g_q^{2B_2} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_2+1} - a g_p^{2A_2+1} p + g_q^{2B_2} + b g_q^{2B_2} q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_2+1} - (aq + np) p + g_q^{2B_2} + (bp + mq) q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_2+1} - apq - np^2 + g_q^{2B_2} + bpq + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A_2+1} - np^2 + g_q^{2B_2} + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -np^2 + mq^2 - g_p^{2A_2+1} + g_q^{2B_2} \pmod{pq}$$

また、 $p - q \equiv -np^2 + mq^2 - g_p^{2A_2+1} + g_q^{2B_2} \pmod{pq}$ である時

$g_p^{2A_2+1} g_q^{2B_2}$ を両辺に掛けて

$$g_p^{2A_2+1} g_q^{2B_2} (p - q) \equiv g_p^{2A_2+1} g_q^{2B_2} (-np^2 + mq^2 - g_p^{2A_2+1} + g_q^{2B_2}) \pmod{pq}$$

$$g_p^{2A_2+1} g_q^{2B_2} p - g_p^{2A_2+1} g_q^{2B_2} q$$

$$\equiv -g_p^{2A_2+1} g_q^{2B_2} np^2 + g_p^{2A_2+1} g_q^{2B_2} mq^2 - g_p^{2A_2+1} g_q^{2B_2} g_p^{2A_2+1} + g_p^{2A_2+1} g_q^{2B_2} g_q^{2B_2} \pmod{pq}$$

$$g_p^{2A_2+1} g_q^{2B_2} p - g_p^{2A_2+1} g_q^{2B_2} q$$

$$\equiv -g_p^{2A_2+1} (g_q^{2B_2} np^2) + g_q^{2B_2} (g_p^{2A_2+1} mq^2) - g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq}$$

この時 ③' ④' より

$$\begin{aligned} & g_p^{2A_2+1} g_q^{2B_2} p - g_p^{2A_2+1} g_q^{2B_2} q \\ & \equiv -g_p^{2A_2+1} (-g_p^{2A_2+1} p) + g_q^{2B_2} (-g_q^{2B_2} q) - g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_2+1} g_q^{2B_2+1} p - g_p^{2A_2+1} g_q^{2B_2} q - g_p^{2A_2+1} (g_p^{2A_2+1} p) + g_q^{2B_2} (g_q^{2B_2} q) \\ & \equiv -g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_2+1} g_q^{2B_2} p - g_p^{2A_2+1} g_q^{2B_2} q - g_p^{4A_2+2} p + g_q^{4B_2} q \\ & \equiv -g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq} \end{aligned}$$

$$\begin{aligned} & -g_p^{4A_2+2} p + g_p^{2A_2+1} g_q^{2B_2} p - g_p^{2A_2+1} g_q^{2B_2} q + g_q^{4B_2} q \\ & \equiv -g_p^{4A_2+2} g_q^{2B_2} + g_p^{2A_2+1} g_q^{4B_2} \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_2+1} (g_q^{2B_2} - g_p^{2A_2+1}) p + g_q^{2B_2} (g_q^{2B_2} - g_p^{2A_2+1}) q \\ & \equiv g_p^{2A_2+1} g_q^{2B_2} (g_q^{2B_2} - g_p^{2A_2+1}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} & -g_p^{2A_2+1} (g_p^{2A_2+1} - g_q^{2B_2}) p - g_q^{2B_2} (g_p^{2A_2+1} - g_q^{2B_2}) q \\ & \equiv -g_p^{2A_2+1} g_q^{2B_2+1} (g_p^{2A_2+1} - g_q^{2B_2}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_2+1} (g_p^{2A_2+1} - g_q^{2B_2}) p + g_q^{2B_2} (g_p^{2A_2+1} - g_q^{2B_2}) q \\ & \equiv g_p^{2A_2+1} g_q^{2B_2} (g_p^{2A_2+1} - g_q^{2B_2}) \pmod{pq} \end{aligned}$$

____※₄

この時 $\times_3 + \times_4$ より

$$\begin{aligned} & g_p^{2A_2+1}(g_p^{2A_2+1} + g_q^{2B_2})p + g_q^{2B_2}(g_p^{2A_2+1} + g_q^{2B_2})q \\ & \quad + g_p^{2A_2+1}(g_p^{2A_2+1} - g_q^{2B_2})p + g_q^{2B_2}(g_p^{2A_2+1} - g_q^{2B_2})q \\ & \equiv g_p^{2A_2+1}g_q^{2B_2}(g_p^{2A_2+1} + g_q^{2B_2}) + g_p^{2A_2+1}g_q^{2B_2}(g_p^{2A_2+1} - g_q^{2B_2}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_2+1}(g_p^{2A_2+1} + g_q^{2B_2})p + g_p^{2A_2+1}(g_p^{2A_2+1} - g_q^{2B_2})p \\ & \quad + g_q^{2B_2}(g_p^{2A_2+1} + g_q^{2B_2})q + g_q^{2B_2}(g_p^{2A_2+1} - g_q^{2B_2})q \\ & \equiv g_p^{2A_2+1}g_q^{2B_2}(g_p^{2A_2+1} + g_q^{2B_2}) + g_p^{2A_2+1}g_q^{2B_2}(g_p^{2A_2+1} - g_q^{2B_2}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_2+1}(g_p^{2A_2+1} + g_q^{2B_2} + g_p^{2A_2+1} - g_q^{2B_2})p + g_q^{2B_2}(g_p^{2A_2+1} + g_q^{2B_2} + g_p^{2A_2+1} - g_q^{2B_2})q \\ & \equiv g_p^{2A_2+1}g_q^{2B_2}(g_p^{2A_2+1} + g_q^{2B_2} + g_p^{2A_2+1} - g_q^{2B_2}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A_2+1}(g_p^{2A_2+1} + g_p^{2A_2+1})p + g_q^{2B_2}(g_p^{2A_2+1} + g_p^{2A_2+1})q \\ & \equiv g_p^{2A_2+1}g_q^{2B_2}(g_p^{2A_2+1} + g_p^{2A_2+1}) \pmod{pq} \end{aligned}$$

$$g_p^{2A_2+1}p \times 2g_p^{2A_2+1} + g_q^{2B_2}q \times 2g_p^{2A_2+1} \equiv g_p^{2A_2+1}g_q^{2B_2} \times 2g_p^{2A_2+1} \pmod{pq}$$

この時 $(2, pq) = 1$ より両辺を 2 で割って

$$g_p^{2A_2+1}p \times g_p^{2A_2+1} + g_q^{2B_2}q \times g_p^{2A_2+1} \equiv g_p^{2A_2+1}g_q^{2B_2} \times g_p^{2A_2+1} \pmod{pq}$$

$$\therefore g_p^{4A_2+2}p + g_q^{2B_2}g_p^{2A_2+1}q \equiv g_p^{4A_2+2}g_q^{2B_2} \pmod{pq}$$

この時 $(g_p, p) = 1$ $(g_p, q) = 1$ より $(g_p, pq) = 1$

$$\therefore (g_p^{2A_2+1}, pq) = 1$$

従って両辺を $g_p^{2A_2'+1}$ で割って

$$g_p^{2A_2+1}p + g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{pq}$$

II. $(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$g_p^{2A_2+1}p + g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{pq}$$

$$\Rightarrow q \equiv g_p^{2A_2+1} \pmod{p} \text{ かつ } p \equiv g_q^{2B_2} \pmod{q}$$

$\therefore$

$$g_p^{2A_2+1}p + g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{pq} \text{ の時}$$

上記の方程式は

$$g_p^{2A_2+1}p + g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{p}$$

かつ

$$g_p^{2A_2+1}p + g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{q}$$

と同値である。

又、上記の方程式は

$$g_q^{2B_2}q \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{p}$$

かつ

$$g_p^{2A_2+1}p \equiv g_p^{2A_2+1}g_q^{2B_2} \pmod{q} \text{ ---}\star_3$$

と同値である。

この時 $(g_q, p) = 1$ より $(g_q^{2B_2}, p) = 1$

又、 $(g_p, q) = 1$ より $(g_p^{2A_2+1}, q) = 1$

従って、上記の方程式の両辺を $g_q^{2B_2}$, $g_p^{2A_2+1}$ でそれぞれ割って

$$q \equiv g_p^{2A_2+1} \pmod{p}$$

かつ

$$p \equiv g_q^{2B_2} \pmod{q} \text{ ---}\star_4$$

この時、 $\star_4$ の方程式のそれぞれに $g_q^{2B_2'+1}$, $g_p^{2A_2'+1}$ を掛け合わせると

$\star_3$ の方程式へと戻るため $\star_3$ の方程式と $\star_4$ の方程式は同値である。

以上より、上記の命題が成立する。

【iiiである場合】

$$\begin{aligned}
 (g_p, q) = 1 \quad \text{かつ} \quad (g_q, p) = 1 \quad \text{である時} \\
 q \equiv g_p^{2A'_1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B'_1} \pmod{q} \\
 \Leftrightarrow g_p^{2A'_1}p + g_q^{2B'_1}q \equiv g_p^{2A'_1}g_q^{2B'_1} \pmod{pq} \quad \text{の証明}
 \end{aligned}$$

$$\begin{aligned}
 \text{I.} \quad (g_p, q) = 1 \quad \text{かつ} \quad (g_q, p) = 1 \quad \text{である時} \\
 q \equiv g_p^{2A'_1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B'_1} \pmod{q} \\
 \Rightarrow g_p^{2A'_1}p + g_q^{2B'_1}q \equiv g_p^{2A'_1}g_q^{2B'_1} \pmod{pq}
 \end{aligned}$$

∴

$$q \equiv g_p^{2A'_1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B'_1} \pmod{q} \quad \text{である時}$$

$$p + q \equiv g_p^{2A'_1} \pmod{p} \quad \text{かつ} \quad p + q \equiv g_q^{2B'_1} \pmod{q} \quad \text{---※ であるから}$$

$M_s M'_s$ を条件

$$m_1 = p, \quad M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, \quad M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$a_0 = M_1 M'_1 g_p^{2A'_1} + M_2 M'_2 g_q^{2B'_1}$$

とする。

この時、連立合同式※を満足する a の値の全体は合同式

$$a \equiv a_0 \pmod{pq} \quad (a = p + q)$$

$$a \equiv M_1 M'_1 g_p^{2A'_1} + M_2 M'_2 g_q^{2B'_1} \pmod{pq}$$

$$\therefore p + q \equiv M_1 M'_1 g_p^{2A'_1} + M_2 M'_2 g_q^{2B'_1} \pmod{pq}$$

$$\therefore p + q \equiv q M'_1 g_p^{2A'_1} + p M'_2 g_q^{2B'_1} \pmod{pq}$$

$$\therefore p + q \equiv (1 + ap) g_p^{2A'_1} + (1 + bq) g_q^{2B'_1} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_1} + ap g_p^{2A'_1} + g_q^{2B'_1} + bq g_q^{2B'_1} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_1} + a g_p^{2A'_1} p + g_q^{2B'_1} + b g_q^{2B'_1} q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_1} + (aq + np)p + g_q^{2B'_1} + (bp + mq)q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_1} + apq + np^2 + g_q^{2B'_1} + bpq + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_1} + np^2 + g_q^{2B'_1} + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv np^2 + mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{pq}$$

この時上記の命題は

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{p} \text{ ---⑤}$$

かつ

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{q} \text{ ---⑥}$$

と同値である。

⑤ の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{p}$$

$$q \equiv mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{p}$$

$$g_p^{2A'_1} \equiv mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{p}$$

$$g_p^{2A'_1} \equiv mqq + g_p^{2A'_1} + g_q^{2B'_1} \pmod{p}$$

$$0 \equiv mg_p^{2A'_1}q + g_q^{2B'_1} \pmod{p}$$

$$mg_p^{2A'_1}q + g_q^{2B'_1} \equiv 0 \pmod{p}$$

$$mg_p^{2A'_1}q \equiv -g_q^{2B'_1} \pmod{p}$$

$$mg_p^{2A'_1}q^2 \equiv -g_q^{2B'_1}q \pmod{pq} \text{ ---⑤'}$$

⑥ の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{q}$$

$$p \equiv np^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{q}$$

$$p \equiv npp + g_p^{2A'_1} + g_q^{2B'_1} \pmod{q}$$

$$g_q^{2B'_1} \equiv ng_q^{2B'_1}p + g_p^{2A'_1} + g_q^{2B'_1} \pmod{q}$$

$$0 \equiv ng_q^{2B'_1}p + g_p^{2A'_1} \pmod{q}$$

$$ng_q^{2B'_1}p + g_p^{2A'_1} \equiv 0 \pmod{q}$$

$$ng_q^{2B'_1}p \equiv -g_p^{2A'_1} \pmod{q}$$

$$ng_q^{2B'_1}p^2 \equiv -g_p^{2A'_1}p \pmod{pq} \text{ ---⑥'}$$

また、 $p + q \equiv np^2 + mq^2 + g_p^{2A'_1} + g_q^{2B'_1} \pmod{pq}$ である時

$g_p^{2A'_1}g_q^{2B'_1}$ を両辺に掛けて

$$g_p^{2A'_1}g_q^{2B'_1}(p + q) \equiv g_p^{2A'_1}g_q^{2B'_1}(np^2 + mq^2 + g_p^{2A'_1} + g_q^{2B'_1}) \pmod{pq}$$

$$\begin{aligned} g_p^{2A'_1}g_q^{2B'_1}p + g_p^{2A'_1}g_q^{2B'_1}q \\ \equiv g_p^{2A'_1}g_q^{2B'_1}np^2 + g_p^{2A'_1}g_q^{2B'_1}mq^2 + g_p^{2A'_1}g_q^{2B'_1}g_p^{2A'_1} + g_p^{2A'_1}g_q^{2B'_1}g_q^{2B'_1} \pmod{pq} \end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_1} g_q^{2B'_1} p + g_p^{2A'_1} g_q^{2B'_1} q \\
& \equiv g_p^{2A'_1} (g_q^{2B'_1} n p^2) + g_q^{2B'_1} (g_p^{2A'_1} m q^2) + g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}
\end{aligned}$$

この時 ⑤' ⑥' より

$$\begin{aligned}
& g_p^{2A'_1} g_q^{2B'_1} p + g_p^{2A'_1} g_q^{2B'_1} q \\
& \equiv g_p^{2A'_1} (-g_p^{2A'_1} p) + g_q^{2B'_1} (-g_q^{2B'_1} q) + g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_1} g_q^{2B'_1} p + g_p^{2A'_1} g_q^{2B'_1} q + g_p^{2A'_1} (g_p^{2A'_1} p) + g_q^{2B'_1} (g_q^{2B'_1} q) \\
& \equiv g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}
\end{aligned}$$

$$g_p^{2A'_1} g_q^{2B'_1} p + g_p^{2A'_1} g_q^{2B'_1} q + g_p^{4A'_1} p + g_q^{4B'_1} q \equiv g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}$$

$$g_p^{4A'_1} p + g_p^{2A'_1} g_q^{2B'_1} p + g_p^{2A'_1} g_q^{2B'_1} q + g_q^{4B'_1} q \equiv g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}$$

$$g_p^{2A'_1} (g_p^{2A'_1} + g_q^{2B'_1}) p + g_q^{2B'_1} (g_p^{2A'_1} + g_q^{2B'_1}) q \equiv g_p^{2A'_1} g_q^{2B'_1} (g_p^{2A'_1} + g_q^{2B'_1}) \pmod{pq} \text{ ---}\ast_1$$

又、 $q \equiv g_p^{2A'_1} \pmod{p}$ かつ $p \equiv g_q^{2B'_1} \pmod{q}$ である時
 $-q \equiv -g_p^{2A'_1} \pmod{p}$ かつ $p \equiv g_q^{2B'_1} \pmod{q}$

$p - q \equiv -g_p^{2A'_1} \pmod{p}$ かつ $p - q \equiv g_q^{2B'_1} \pmod{q}$ であるから

$M_s M'_s$ を条件

$$m_1 = p, M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$b_0 = -M_1 M'_1 g_p^{2A'_1} + M_2 M'_2 g_q^{2B'_1}$$

とする。

この時、連立合同式※を満足する b の値の全体は合同式

$$b \equiv b_0 \pmod{pq} \quad (b = p - q)$$

$$b \equiv -M_1 M'_1 g_p^{2A'_1} + M_2 M'_2 g_q^{2B'_1} \pmod{pq}$$

$$\therefore p - q \equiv -M_1 M'_1 g_p^{2A'_1} + M_2 M'_2 g_q^{2B'_1} \pmod{pq}$$

$$\therefore p - q \equiv -q M'_1 g_p^{2A'_1} + p M'_2 g_q^{2B'_1} \pmod{pq}$$

$$\therefore p - q \equiv -(1 + ap) g_p^{2A'_1} + (1 + bq) g_q^{2B'_1} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_1} - ap g_p^{2A'_1} + g_q^{2B'_1} + bq g_q^{2B'_1} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_1} - a g_p^{2A'_1} p + g_q^{2B'_1} + b g_q^{2B'_1} q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_1} - (aq + np) p + g_q^{2B'_1} + (bp + mq) q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_1} - apq - np^2 + g_q^{2B'_1} + bpq + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_1} - np^2 + g_q^{2B'_1} + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -np^2 + mq^2 - g_p^{2A'_1} + g_q^{2B'_1} \pmod{pq}$$

また、 $p - q \equiv -np^2 + mq^2 - g_p^{2A'_1} + g_q^{2B'_1} \pmod{pq}$ である時

$g_p^{2A'_1} g_q^{2B'_1}$ を両辺に掛けて

$$g_p^{2A'_1} g_q^{2B'_1} (p - q) \equiv g_p^{2A'_1} g_q^{2B'_1} (-np^2 + mq^2 - g_p^{2A'_1} + g_q^{2B'_1}) \pmod{pq}$$

$$g_p^{2A'_1} g_q^{2B'_1} p - g_p^{2A'_1} g_q^{2B'_1} q$$

$$\equiv -g_p^{2A'_1} g_q^{2B'_1} np^2 + g_p^{2A'_1} g_q^{2B'_1} mq^2 - g_p^{2A'_1} g_q^{2B'_1} g_p^{2A'_1} + g_p^{2A'_1} g_q^{2B'_1} g_q^{2B'_1} \pmod{pq}$$

$$g_p^{2A'_1} g_q^{2B'_1} p - g_p^{2A'_1} g_q^{2B'_1} q$$

$$\equiv -g_p^{2A'_1} (g_q^{2B'_1} np^2) + g_q^{2B'_1} (g_p^{2A'_1} mq^2) - g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}$$

この時 ⑤' ⑥' より

$$\begin{aligned} & g_p^{2A'_1} g_q^{2B'_1} p - g_p^{2A'_1} g_q^{2B'_1} q \\ & \equiv -g_p^{2A'_1} (-g_p^{2A'_1} p) + g_q^{2B'_1} (-g_q^{2B'_1} q) - g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A'_1} g_q^{2B'_1} p - g_p^{2A'_1} g_q^{2B'_1} q - g_p^{2A'_1} (g_p^{2A'_1} p) + g_q^{2B'_1} (g_q^{2B'_1} q) \\ & \equiv -g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq} \end{aligned}$$

$$g_p^{2A'_1} g_q^{2B'_1} p - g_p^{2A'_1} g_q^{2B'_1} q - g_p^{4A'_1} p + g_q^{4B'_1} q \equiv -g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}$$

$$-g_p^{4A'_1} p + g_p^{2A'_1} g_q^{2B'_1} p - g_p^{2A'_1} g_q^{2B'_1} q + g_q^{4B'_1} q \equiv -g_p^{4A'_1} g_q^{2B'_1} + g_p^{2A'_1} g_q^{4B'_1} \pmod{pq}$$

$$g_p^{2A'_1} (g_q^{2B'_1} - g_p^{2A'_1}) p + g_q^{2B'_1} (g_q^{2B'_1} - g_p^{2A'_1}) q \equiv g_p^{2A'_1} g_q^{2B'_1} (g_q^{2B'_1} - g_p^{2A'_1}) \pmod{pq}$$

$$-g_p^{2A'_1} (g_p^{2A'_1} - g_q^{2B'_1}) p - g_q^{2B'_1} (g_p^{2A'_1} - g_q^{2B'_1}) q \equiv -g_p^{2A'_1} g_q^{2B'_1} (g_p^{2A'_1} - g_q^{2B'_1}) \pmod{pq}$$

$$g_p^{2A'_1} (g_p^{2A'_1} - g_q^{2B'_1}) p + g_q^{2B'_1} (g_p^{2A'_1} - g_q^{2B'_1}) q \equiv g_p^{2A'_1} g_q^{2B'_1} (g_p^{2A'_1} - g_q^{2B'_1}) \pmod{pq}$$

____※₂

この時 $\times_1 + \times_2$ より

$$\begin{aligned} & g_p^{2A'_1}(g_p^{2A'_1} + g_q^{2B'_1})p + g_q^{2B'_1}(g_p^{2A'_1} + g_q^{2B'_1})q \\ & \quad + g_p^{2A'_1}(g_p^{2A'_1} - g_q^{2B'_1})p + g_q^{2B'_1}(g_p^{2A'_1} - g_q^{2B'_1})q \\ & \equiv g_p^{2A'_1}g_q^{2B'_1}(g_p^{2A'_1} + g_q^{2B'_1}) + g_p^{2A'_1}g_q^{2B'_1}(g_p^{2A'_1} - g_q^{2B'_1}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A'_1}(g_p^{2A'_1} + g_q^{2B'_1})p + g_p^{2A'_1}(g_p^{2A'_1} - g_q^{2B'_1})p \\ & \quad + g_q^{2B'_1}(g_p^{2A'_1} + g_q^{2B'_1})q + g_q^{2B'_1}(g_p^{2A'_1} - g_q^{2B'_1})q \\ & \equiv g_p^{2A'_1}g_q^{2B'_1}(g_p^{2A'_1} + g_q^{2B'_1}) + g_p^{2A'_1}g_q^{2B'_1}(g_p^{2A'_1} - g_q^{2B'_1}) \pmod{pq} \end{aligned}$$

$$\begin{aligned} & g_p^{2A'_1}(g_p^{2A'_1} + g_q^{2B'_1} + g_p^{2A'_1} - g_q^{2B'_1})p + g_q^{2B'_1}(g_p^{2A'_1} + g_q^{2B'_1} + g_p^{2A'_1} - g_q^{2B'_1})q \\ & \equiv g_p^{2A'_1}g_q^{2B'_1}(g_p^{2A'_1} + g_q^{2B'_1} + g_p^{2A'_1} - g_q^{2B'_1}) \pmod{pq} \end{aligned}$$

$$g_p^{2A'_1}(g_p^{2A'_1} + g_p^{2A'_1})p + g_q^{2B'_1}(g_p^{2A'_1} + g_p^{2A'_1})q \equiv g_p^{2A'_1}g_q^{2B'_1}(g_p^{2A'_1} + g_p^{2A'_1}) \pmod{pq}$$

$$g_p^{2A'_1}p \times 2g_p^{2A'_1} + g_q^{2B'_1}q \times 2g_p^{2A'_1} \equiv g_p^{2A'_1}g_q^{2B'_1} \times 2g_p^{2A'_1} \pmod{pq}$$

この時 $(2, pq) = 1$ より両辺を 2 で割って

$$g_p^{2A'_1}p \times g_p^{2A'_1} + g_q^{2B'_1}q \times g_p^{2A'_1} \equiv g_p^{2A'_1}g_q^{2B'_1} \times g_p^{2A'_1} \pmod{pq}$$

$$\therefore g_p^{4A'_1}p + g_q^{2B'_1}g_p^{2A'_1}q \equiv g_p^{4A'_1}g_q^{2B'_1} \pmod{pq}$$

この時 $(g_p, p) = 1$ $(g_p, q) = 1$ より $(g_p, pq) = 1$

$$\therefore (g_p^{2A'_1}, pq) = 1$$

従って両辺を $g_p^{2A'_1}$ で割って

$$g_p^{2A'_1}p + g_q^{2B'_1}q \equiv g_p^{2A'_1}g_q^{2B'_1} \pmod{pq}$$

II. $(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$\begin{aligned} g_p^{2A'_1} p + g_q^{2B'_1} q &\equiv g_p^{2A'_1} g_q^{2B'_1} \pmod{pq} \\ &\Rightarrow q \equiv g_p^{2A'_1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B'_1} \pmod{q} \end{aligned}$$

$\therefore$

$g_p^{2A'_1} p + g_q^{2B'_1} q \equiv g_p^{2A'_1} g_q^{2B'_1} \pmod{pq}$ の時

上記の方程式は

$$g_p^{2A'_1} p + g_q^{2B'_1} q \equiv g_p^{2A'_1} g_q^{2B'_1} \pmod{p}$$

かつ

$$g_p^{2A'_1} p + g_q^{2B'_1} q \equiv g_p^{2A'_1} g_q^{2B'_1} \pmod{q}$$

と同値である。

又、上記の方程式は

$$g_q^{2B'_1} q \equiv g_p^{2A'_1} g_q^{2B'_1} \pmod{p}$$

かつ

$$g_p^{2A'_1} p \equiv g_p^{2A'_1} g_q^{2B'_1} \pmod{q} \text{ --- } \star_1$$

と同値である。

この時 $(g_q, p) = 1$ より $(g_q^{2B'_1}, p) = 1$

又、 $(g_p, q) = 1$ より $(g_p^{2A'_1}, q) = 1$

従って、上記の方程式の両辺を $g_q^{2B'_1}$, $g_p^{2A'_1}$ でそれぞれ割って

$$q \equiv g_p^{2A'_1} \pmod{p}$$

かつ

$$p \equiv g_q^{2B'_1} \pmod{q} \text{ --- } \star_2$$

この時、 $\star_2$ の方程式のそれぞれに $g_q^{2B'_1}$, $g_p^{2A'_1}$ を掛け合わせると
 $\star_1$ の方程式へと戻るため $\star_1$ の方程式と $\star_2$ の方程式は同値である。

以上より、上記の命題が成立する。

【ivである場合】

$(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$q \equiv g_p^{2A'_2+1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B'_2+1} \pmod{q}$$

$$\Leftrightarrow g_p^{2A'_2+1}p + g_q^{2B'_2+1}q \equiv g_p^{2A'_2+1}g_q^{2B'_2+1} \pmod{pq} \quad \text{の証明}$$

I. $(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$q \equiv g_p^{2A'_2+1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B'_2+1} \pmod{q}$$

$$\Rightarrow g_p^{2A'_2+1}p + g_q^{2B'_2+1}q \equiv g_p^{2A'_2+1}g_q^{2B'_2+1} \pmod{pq}$$

$\therefore$

$q \equiv g_p^{2A'_2+1} \pmod{p}$ かつ $p \equiv g_q^{2B'_2+1} \pmod{q}$ である時

$p + q \equiv g_p^{2A'_2+1} \pmod{p}$ かつ $p + q \equiv g_q^{2B'_2+1} \pmod{q}$ —※ であるから

$M_s M'_s$ を条件

$$m_1 = p, M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$a_0 = M_1 M'_1 g_p^{2A'_2+1} + M_2 M'_2 g_q^{2B'_2+1}$$

とする。

この時、連立合同式※を満足する a の値の全体は合同式

$$a \equiv a_0 \pmod{pq} \quad (a = p + q)$$

$$a \equiv M_1 M'_1 g_p^{2A'_2+1} + M_2 M'_2 g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p + q \equiv M_1 M'_1 g_p^{2A'_2+1} + M_2 M'_2 g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p + q \equiv q M'_1 g_p^{2A'_2+1} + p M'_2 g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p + q \equiv (1 + ap) g_p^{2A'_2+1} + (1 + bq) g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_2+1} + ap g_p^{2A'_2+1} + g_q^{2B'_2+1} + bq g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_2+1} + a g_p^{2A'_2+1} p + g_q^{2B'_2+1} + b g_q^{2B'_2+1} q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_2+1} + (aq + np)p + g_q^{2B'_2+1} + (bp + mq)q \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_2+1} + apq + np^2 + g_q^{2B'_2+1} + bpq + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv g_p^{2A'_2+1} + np^2 + g_q^{2B'_2+1} + mq^2 \pmod{pq}$$

$$\therefore p + q \equiv np^2 + mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{pq}$$

この時上記の命題は

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{p} \text{ ---⑦}$$

かつ

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{q} \text{ ---⑧}$$

と同値である。

⑦ の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{p}$$

$$q \equiv mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{p}$$

$$g_p^{2A'_2+1} \equiv mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{p}$$

$$g_p^{2A'_2+1} \equiv mqq + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{p}$$

$$0 \equiv mg_p^{2A'_2+1}q + g_q^{2B'_2+1} \pmod{p}$$

$$mg_p^{2A'_2+1}q + g_q^{2B'_2+1} \equiv 0 \pmod{p}$$

$$mg_p^{2A'_2+1}q \equiv -g_q^{2B'_2+1} \pmod{p}$$

$$mg_p^{2A'_2+1}q^2 \equiv -g_q^{2B'_2+1}q \pmod{pq} \text{ ---⑦'}$$

⑧ の時

$$p + q \equiv np^2 + mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{q}$$

$$p \equiv np^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{q}$$

$$g_q^{2B'_2+1} \equiv npp + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{q}$$

$$g_q^{2B'_2+1} \equiv ng_q^{2B'_2+1}p + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{q}$$

$$0 \equiv ng_q^{2B'_2+1}p + g_p^{2A'_2+1} \pmod{q}$$

$$ng_q^{2B'_2+1}p + g_p^{2A'_2+1} \equiv 0 \pmod{q}$$

$$ng_q^{2B'_2+1}p \equiv -g_p^{2A'_2+1} \pmod{q}$$

$$ng_q^{2B'_2+1}p^2 \equiv -g_p^{2A'_2+1}p \pmod{pq} \text{ ---⑧'}$$

また、 $p + q \equiv np^2 + mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{pq}$ である時

$g_p^{2A'_2+1}g_q^{2B'_2+1}$ を両辺に掛けて

$$g_p^{2A'_2+1}g_q^{2B'_2+1}(p + q) \equiv g_p^{2A'_2+1}g_q^{2B'_2+1}(np^2 + mq^2 + g_p^{2A'_2+1} + g_q^{2B'_2+1}) \pmod{pq}$$

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p + g_p^{2A'_2+1} g_q^{2B'_2+1} q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} np^2 + g_p^{2A'_2+1} g_q^{2B'_2+1} mq^2 + g_p^{2A'_2+1} g_q^{2B'_2+1} g_p^{2A'_2+1} \\
& \quad + g_p^{2A'_2+1} g_q^{2B'_2+1} g_q^{2B'_2+1} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p + g_p^{2A'_2+1} g_q^{2B'_2+1} q \\
& \equiv g_p^{2A'_2+1} (g_q^{2B'_2+1} np^2) + g_q^{2B'_2+1} (g_p^{2A'_2+1} mq^2) + g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

この時 ⑦' ⑧' より

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p + g_p^{2A'_2+1} g_q^{2B'_2+1} q \\
& \equiv g_p^{2A'_2+1} (-g_p^{2A'_2+1} p) + g_q^{2B'_2+1} (-g_q^{2B'_2+1} q) + g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p + g_p^{2A'_2+1} g_q^{2B'_2+1} q + g_p^{2A'_2+1} (g_p^{2A'_2+1} p) + g_q^{2B'_2+1} (g_q^{2B'_2+1} q) \\
& \equiv g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p + g_p^{2A'_2+1} g_q^{2B'_2+1} q + g_p^{4A'_2+2} p + g_q^{4B'_2+2} q \\
& \equiv g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{4A'_2+2} p + g_p^{2A'_2+1} g_q^{2B'_2+1} p + g_p^{2A'_2+1} g_q^{2B'_2+1} q + g_q^{4B'_2+2} q \\
& \equiv g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} (g_p^{2A'_2+1} + g_q^{2B'_2+1}) p + g_q^{2B'_2+1} (g_p^{2A'_2+1} + g_q^{2B'_2+1}) q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} + g_q^{2B'_2+1}) \pmod{pq} \text{ ---}\textcircled{\times}_3
\end{aligned}$$

又、 $q \equiv g_p^{2A'_2+1} \pmod{p}$ かつ $p \equiv g_q^{2B'_2+1} \pmod{q}$ である時

$$-q \equiv -g_p^{2A'_2+1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2B'_2+1} \pmod{q}$$

$p - q \equiv -g_p^{2A'_2+1} \pmod{p}$ かつ $p - q \equiv g_q^{2B'_2+1} \pmod{q}$ であるから

$M_s M'_s$ を条件

$$m_1 = p, M_1 = q$$

$$pq = M_s m_s$$

$$M_1 M'_1 \equiv q M'_1 \equiv 1 \pmod{p}$$

$$(m_1 = p, m_2 = q)$$

$$m_2 = q, M_2 = p$$

$$M_s M'_s \equiv 1 \pmod{m_s}$$

$$M_2 M'_2 \equiv p M'_2 \equiv 1 \pmod{q}$$

によって定められる数とし

$$b_0 = -M_1 M'_1 g_p^{2A'_2+1} + M_2 M'_2 g_q^{2B'_2+1}$$

とする。

この時、連立合同式※を満足する b の値の全体は合同式

$$b \equiv b_0 \pmod{pq} \quad (b = p - q)$$

$$b \equiv -M_1 M'_1 g_p^{2A'_2+1} + M_2 M'_2 g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p - q \equiv -M_1 M'_1 g_p^{2A'_2+1} + M_2 M'_2 g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p - q \equiv -q M'_1 g_p^{2A'_2+1} + p M'_2 g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p - q \equiv -(1 + ap) g_p^{2A'_2+1} + (1 + bq) g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_2+1} - ap g_p^{2A'_2+1} + g_q^{2B'_2+1} + bq g_q^{2B'_2+1} \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_2+1} - a g_p^{2A'_2+1} p + g_q^{2B'_2+1} + b g_q^{2B'_2+1} q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_2+1} - (aq + np) p + g_q^{2B'_2+1} + (bp + mq) q \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_2+1} - apq - np^2 + g_q^{2B'_2+1} + bpq + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -g_p^{2A'_2+1} - np^2 + g_q^{2B'_2+1} + mq^2 \pmod{pq}$$

$$\therefore p - q \equiv -np^2 + mq^2 - g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{pq}$$

また、 $p - q \equiv -np^2 + mq^2 - g_p^{2A'_2+1} + g_q^{2B'_2+1} \pmod{pq}$ である時

$g_p^{2A'_2+1} g_q^{2B'_2+1}$ を両辺に掛けて

$$g_p^{2A'_2+1} g_q^{2B'_2+1} (p - q) \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (-np^2 + mq^2 - g_p^{2A'_2+1} + g_q^{2B'_2+1}) \pmod{pq}$$

$$\begin{aligned} & g_p^{2A'_2+1} g_q^{2B'_2+1} p - g_p^{2A'_2+1} g_q^{2B'_2+1} q \\ & \equiv -g_p^{2A'_2+1} g_q^{2B'_2+1} np^2 + g_p^{2A'_2+1} g_q^{2B'_2+1} mq^2 - g_p^{2A'_2+1} g_q^{2B'_2+1} g_p^{2A'_2+1} \\ & \quad + g_p^{2A'_2+1} g_q^{2B'_2+1} g_q^{2B'_2+1} \pmod{pq} \end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p - g_p^{2A'_2+1} g_q^{2B'_2+1} q \\
& \equiv -g_p^{2A'_2+1} (g_q^{2B'_2+1} np^2) + g_q^{2B'_2+1} (g_p^{2A'_2+1} mq^2) - g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

この時 ⑦' ⑧' より

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p - g_p^{2A'_2+1} g_q^{2B'_2+1} q \\
& \equiv -g_p^{2A'_2+1} (-g_p^{2A'_2+1} p) + g_q^{2B'_2+1} (-g_q^{2B'_2+1} q) - g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p - g_p^{2A'_2+1} g_q^{2B'_2+1} q - g_p^{2A'_2+1} (g_p^{2A'_2+1} p) + g_q^{2B'_2+1} (g_q^{2B'_2+1} q) \\
& \equiv -g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} g_q^{2B'_2+1} p - g_p^{2A'_2+1} g_q^{2B'_2+1} q - g_p^{4A'_2+2} p + g_q^{4B'_2+2} q \\
& \equiv -g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& -g_p^{4A'_2+2} p + g_p^{2A'_2+1} g_q^{2B'_2+1} p - g_p^{2A'_2+1} g_q^{2B'_2+1} q + g_q^{4B'_2+2} q \\
& \equiv -g_p^{4A'_2+2} g_q^{2B'_2+1} + g_p^{2A'_2+1} g_q^{4B'_2+2} \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} (g_q^{2B'_2+1} - g_p^{2A'_2+1}) p + g_q^{2B'_2+1} (g_q^{2B'_2+1} - g_p^{2A'_2+1}) q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (g_q^{2B'_2+1} - g_p^{2A'_2+1}) \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& -g_p^{2A'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) p - g_q^{2B'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) q \\
& \equiv -g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) p + g_q^{2B'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) \pmod{pq}
\end{aligned}$$

この時 $\times_3 + \times_4$ より

$$\begin{aligned}
& g_p^{2A'_2+1}(g_p^{2A'_2+1} + g_q^{2B'_2+1})p + g_q^{2B'_2+1}(g_p^{2A'_2+1} + g_q^{2B'_2+1})q \\
& \quad + g_p^{2A'_2+1}(g_p^{2A'_2+1} - g_q^{2B'_2+1})p + g_q^{2B'_2+1}(g_p^{2A'_2+1} - g_q^{2B'_2+1})q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} + g_q^{2B'_2+1}) + g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1}(g_p^{2A'_2+1} + g_q^{2B'_2+1})p + g_p^{2A'_2+1}(g_p^{2A'_2+1} - g_q^{2B'_2+1})p \\
& \quad + g_q^{2B'_2+1}(g_p^{2A'_2+1} + g_q^{2B'_2+1})q + g_q^{2B'_2+1}(g_p^{2A'_2+1} - g_q^{2B'_2+1})q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} + g_q^{2B'_2+1}) + g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} - g_q^{2B'_2+1}) \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1}(g_p^{2A'_2+1} + g_q^{2B'_2+1} + g_p^{2A'_2+1} - g_q^{2B'_2+1})p + g_q^{2B'_2+1}(g_p^{2A'_2+1} + g_q^{2B'_2+1} + g_p^{2A'_2+1} - g_q^{2B'_2+1})q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} + g_q^{2B'_2+1} + g_p^{2A'_2+1} - g_q^{2B'_2+1}) \pmod{pq}
\end{aligned}$$

$$\begin{aligned}
& g_p^{2A'_2+1}(g_p^{2A'_2+1} + g_p^{2A'_2+1})p + g_q^{2B'_2+1}(g_p^{2A'_2+1} + g_p^{2A'_2+1})q \\
& \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} (g_p^{2A'_2+1} + g_p^{2A'_2+1}) \pmod{pq}
\end{aligned}$$

$$g_p^{2A'_2+1} p \times 2g_p^{2A'_2+1} + g_q^{2B'_2+1} q \times 2g_p^{2A'_2+1} \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \times 2g_p^{2A'_2+1} \pmod{pq}$$

この時 $(2, pq) = 1$ より両辺を 2 で割って

$$g_p^{2A'_2+1} p \times g_p^{2A'_2+1} + g_q^{2B'_2+1} q \times g_p^{2A'_2+1} \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \times g_p^{2A'_2+1} \pmod{pq}$$

$$\therefore g_p^{4A'_2+2} p + g_q^{2B'_2+1} g_p^{2A'_2+1} q \equiv g_p^{4A'_2+2} g_q^{2B'_2+1} \pmod{pq}$$

この時 $(g_p, p) = 1$ $(g_p, q) = 1$ より $(g_p, pq) = 1$

$$\therefore (g_p^{2A'_2+1}, pq) = 1$$

従って両辺を $g_p^{2A'_2+1}$ で割って

$$g_p^{2A'_2+1} p + g_q^{2B'_2+1} q \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \pmod{pq}$$

II. $(g_p, q) = 1$ かつ $(g_q, p) = 1$ である時

$$g_p^{2A'_2+1} p + g_q^{2B'_2+1} q \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \pmod{pq}$$

$$\Rightarrow q \equiv g_p^{2A'_2+1} \pmod{p} \text{ かつ } p \equiv g_q^{2B'_2+1} \pmod{q}$$

$\therefore$

$$g_p^{2A'_2+1} p + g_q^{2B'_2+1} q \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \pmod{pq} \text{ の時}$$

上記の方程式は

$$g_p^{2A'_2+1} p + g_q^{2B'_2+1} q \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \pmod{p}$$

かつ

$$g_p^{2A'_2+1} p + g_q^{2B'_2+1} q \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \pmod{q}$$

と同値である。

又、上記の方程式は

$$g_q^{2B'_2+1} q \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \pmod{p}$$

かつ

$$g_p^{2A'_2+1} p \equiv g_p^{2A'_2+1} g_q^{2B'_2+1} \pmod{q} \text{ ——} \star_3$$

と同値である。

$$\text{この時 } (g_q, p) = 1 \text{ より } (g_q^{2B'_2+1}, p) = 1$$

$$\text{又、} (g_p, q) = 1 \text{ より } (g_p^{2A'_2+1}, q) = 1$$

従って、上記の方程式の両辺を $g_q^{2B'_2+1}$, $g_p^{2A'_2+1}$ でそれぞれ割って

$$q \equiv g_p^{2A'_2+1} \pmod{p}$$

かつ

$$p \equiv g_q^{2B'_2+1} \pmod{q} \text{ ——} \star_4$$

この時、 $\star_4$ の方程式のそれぞれに $g_q^{2B'_2+1}$, $g_p^{2A'_2+1}$ を掛け合わせると $\star_3$ の方程式へと戻るため $\star_3$ の方程式と $\star_4$ の方程式は同値である。

以上より、上記の命題が成立する。