# 平方剰余の相互法則

$p = 4m_1 + 3 \qquad q = 4m_2 + 1$

$p = 4m_1 + 1 \qquad q = 4m_2 + 3$

$p = 4m_1 + 1 \qquad q = 4m_2 + 1$　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】

$$\left(\frac{q}{p}\right)=1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv 1\,(mod\ p) \quad \Leftrightarrow \quad ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\,(mod\ p-1)$$

$$\Leftrightarrow \quad q \equiv g_p^{2C_1}\,(mod\ p)\ (\,2C_1=0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\,)$$

かつ

$$\left(\frac{p}{q}\right)=1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv 1\,(mod\ q) \quad \Leftrightarrow \quad ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\,(mod\ q-1)$$

$$\Leftrightarrow \quad p \equiv g_q^{2D_1}\,(mod\ q)\ (\,2D_1=0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\,)$$

【ⅱである場合】

$$\left(\frac{q}{p}\right)=-1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1\,(mod\ p) \quad \Leftrightarrow \quad ind\ q \equiv 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,p-2\,(mod\ p-1)$$

$$\Leftrightarrow \quad q \equiv g_p^{2C_2+1}\ (mod\ p)\ (\,2C_2+1=1\,,3\,,5\,,7\,,9\,,\ldots\ldots,p-2\,)$$

かつ

$$\left(\frac{p}{q}\right)=-1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv -1\,(mod\ q) \quad \Leftrightarrow \quad ind\ p \equiv 1,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\,(mod\ q-1)$$

$$\Leftrightarrow \quad p \equiv g_q^{2D_2+1}\,(mod\ q)\ (\,2D_2+1=1\,,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\,)$$

◎ $1=-1$を生成する素数のペアを探す時

【iii である場合】

$$\left(\frac{q}{p}\right)=1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv 1\,(mod\ p) \quad \Leftrightarrow \quad ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\,(mod\ p-1)$$

$$\Leftrightarrow \quad q \equiv g_p^{2C_1'}\,(mod\ p)\ (\ 2C_1' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ )$$

かつ

$$\left(\frac{p}{q}\right)=-1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv -1\,(mod\ q) \quad \Leftrightarrow \quad ind\ p \equiv 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\,(mod\ q-1)$$

$$\Leftrightarrow \quad p \equiv g_q^{2D_1'+1}\,(mod\ q)\ (\ 2D_1'+1 = 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\ )$$

【iv である場合】

$$\left(\frac{q}{p}\right)=-1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1\,(mod\ p) \quad \Leftrightarrow \quad ind\ q \equiv 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,p-2\,(mod\ p-1)$$

$$\Leftrightarrow \quad q \equiv g_p^{2C_2'+1}\ (mod\ p)\ (\ 2C_2'+1 = 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,p-2\ )$$

かつ

$$\left(\frac{p}{q}\right)=1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv 1\,(mod\ q) \quad \Leftrightarrow \quad ind\ p \equiv 0,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\,(mod\ q-1)$$

$$\Leftrightarrow \quad p \equiv g_q^{2D_2'}\,(mod\ q)\ (\ 2D_2' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ )$$

【ｉである場合】

$(g_p, q) = 1$　かつ　$(g_q, p) = 1$　である時

$q \equiv g_p^{2C_1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1} \ (mod\ q)$

$\Leftrightarrow$　$g_p^{2C_1} p + g_q^{2D_1} q \equiv g_p^{2C_1} g_q^{2D_1} \ \ (mod\ pq)$　の証明

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

$q \equiv g_p^{2C_1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1} \ (mod\ q)$

$\Rightarrow$　$g_p^{2C_1} p + g_q^{2D_1} q \equiv g_p^{2C_1} g_q^{2D_1} \ \ (mod\ pq)$

$\because$

$q \equiv g_p^{2C_1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1} \ (mod\ q)$　である時

$p + q \equiv g_p^{2C_1} \ (mod\ p)$　かつ　$p + q \equiv g_q^{2D_1} \ (mod\ q)$ __※ であるから

$M_s M_s'$ を条件

$pq = M_s m_s$

$(m_1 = p, m_2 = q)$

$M_s M_s' \equiv 1 \ (mod\ m_s)$

$m_1 = p$ ， $M_1 = q$

$M_1 M_1' \equiv q M_1' \equiv 1 \ \ (mod\ p)$

$m_2 = q$ ， $M_2 = p$

$M_2 M_2' \equiv p M_2' \equiv 1 \ \ (mod\ q)$

によって定められる数とし
$a_0 = M_1 M_1' g_p^{2C_1} + M_2 M_2' g_q^{2D_1}$
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

$a \equiv a_0 \ \ (mod\ pq) \qquad (a = p + q)$

$$a \equiv M_1 M_1' g_p^{2C_1} + M_2 M_2' g_q^{2D_1} \pmod{pq}$$

$$\therefore \quad p+q \equiv M_1 M_1' g_p^{2C_1} + M_2 M_2' g_q^{2D_1} \pmod{pq}$$

$$\therefore \quad p+q \equiv qM_1' g_p^{2C_1} + pM_2' g_q^{2D_1} \pmod{pq}$$

$$\therefore \quad p+q \equiv (1+ap) g_p^{2C_1} + (1+bq) g_q^{2D_1} \pmod{pq}$$

$$\therefore \quad p+q \equiv g_p^{2C_1} + apg_p^{2C_1} + g_q^{2D_1} + bqg_q^{2D_1} \pmod{pq}$$

$$\therefore \quad p+q \equiv g_p^{2C_1} + ag_p^{2C_1} p + g_q^{2D_1} + bg_q^{2D_1} q \pmod{pq}$$

$$\therefore \quad p+q \equiv g_p^{2C_1} + (aq+np)p + g_q^{2D_1} + (bp+mq)q \pmod{pq}$$

$$\therefore \quad p+q \equiv g_p^{2C_1} + apq + np^2 + g_q^{2D_1} + bpq + mq^2 \pmod{pq}$$

$$\therefore \quad p+q \equiv g_p^{2C_1} + np^2 + g_q^{2D_1} + mq^2 \pmod{pq}$$

$$\therefore \quad p+q \equiv np^2 + mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{pq}$$

この時上記の命題は

$$p+q \equiv np^2 + mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{p} \quad \text{__①}$$

かつ

$$p+q \equiv np^2 + mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{q} \quad \text{__②}$$

と同値である。

① の時

$$p+q \equiv np^2 + mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{p}$$

$$q \equiv mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{p}$$

$$g_p^{2C_1} \equiv mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{p}$$

$g_p^{2C_1} \equiv mqq + g_p^{2C_1} + g_q^{2D_1} \pmod{p}$

$0 \equiv mg_p^{2C_1}q + g_q^{2D_1} \pmod{p}$

$mg_p^{2C_1}q + g_q^{2D_1} \equiv 0 \pmod{p}$

$mg_p^{2C_1}q \equiv -g_q^{2D_1} \pmod{p}$

$mg_p^{2C_1}q^2 \equiv -g_q^{2D_1}q \pmod{pq}$ __①'

② の時

$p + q \equiv np^2 + mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{q}$

$p \equiv np^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{q}$

$p \equiv npp + g_p^{2C_1} + g_q^{2D_1} \pmod{q}$

$g_q^{2D_1} \equiv ng_q^{2D_1}p + g_p^{2C_1} + g_q^{2D_1} \pmod{q}$

$0 \equiv ng_q^{2D_1}p + g_p^{2C_1} \pmod{q}$

$ng_q^{2D_1}p + g_p^{2C_1} \equiv 0 \pmod{q}$

$ng_q^{2D_1}p \equiv -g_p^{2C_1} \pmod{q}$

$ng_q^{2D_1}p^2 \equiv -g_p^{2C_1}p \pmod{pq}$ __②'

また、$p + q \equiv np^2 + mq^2 + g_p^{2C_1} + g_q^{2D_1} \pmod{pq}$ である時

$g_p^{2C_1}g_q^{2D_1}$ を両辺に掛けて

$g_p^{2C_1}g_q^{2D_1}(p + q) \equiv g_p^{2C_1}g_q^{2D_1}(np^2 + mq^2 + g_p^{2C_1} + g_q^{2D_1}) \pmod{pq}$

$g_p^{2C_1}g_q^{2D_1}p + g_p^{2C_1}g_q^{2D_1}q$

$\equiv g_p^{2C_1}g_q^{2D_1}np^2 + g_p^{2C_1}g_q^{2D_1}mq^2 + g_p^{2C_1}g_q^{2D_1}g_p^{2C_1} + g_p^{2C_1}g_q^{2D_1}g_q^{2D_1} \pmod{pq}$

$$g_p^{2C_1} g_q^{2D_1} p + g_p^{2C_1} g_q^{2D_1} q$$

$$\equiv g_p^{2C_1}(g_q^{2D_1} np^2) + g_q^{2D_1}(g_p^{2C_1} mq^2) + g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \quad (mod\ pq)$$

この時 ①' ②'より

$$g_p^{2C_1} g_q^{2D_1} p + g_p^{2C_1} g_q^{2D_1} q$$

$$\equiv g_p^{2C_1}(-g_p^{2C_1} p) + g_q^{2D_1}(-g_q^{2D_1} q) + g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \quad (mod\ pq)$$

$$g_p^{2C_1} g_q^{2D_1} p + g_p^{2C_1} g_q^{2D_1} q + g_p^{2C_1}(g_p^{2C_1} p) + g_q^{2D_1}(g_q^{2D_1} q)$$

$$\equiv g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \quad (mod\ pq)$$

$$g_p^{2C_1} g_q^{2D_1} p + g_p^{2C_1} g_q^{2D_1} q + g_p^{4C_1} p + g_q^{4D_1} q \equiv g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \quad (mod\ pq)$$

$$g_p^{4C_1} p + g_p^{2C_1} g_q^{2D_1} p + g_p^{2C_1} g_q^{2D_1} q + g_q^{4D_1} q \equiv g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \quad (mod\ pq)$$

$$g_p^{2C_1}(g_p^{2C_1} + g_q^{2D_1}) p + g_q^{2D_1}(g_p^{2C_1} + g_q^{2D_1}) q \equiv g_p^{2C_1} g_q^{2D_1}\left(g_p^{2C_1} + g_q^{2D_1}\right) \quad (mod\ pq) \quad \text{___※}_1$$

又、$q \equiv g_p^{2C_1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1} \ (mod\ q)$　である時

$-q \equiv -g_p^{2C_1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1} \ (mod\ q)$

$p - q \equiv -g_p^{2C_1} \ (mod\ p)$　かつ　$p - q \equiv g_q^{2D_1} \ (mod\ q)$ __※ であるから

$M_s M_s'$ を条件

$pq = M_s m_s$

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

$M_s M_s' \equiv 1 \ (mod\ m_s)$

$m_1 = p\ ,\ M_1 = q$

$M_1 M_1' \equiv q M_1' \equiv 1 \quad (mod\ p)$

$m_2 = q\ ,\ M_2 = p$

$M_2 M_2' \equiv p M_2' \equiv 1 \quad (mod\ q)$

によって定められる数とし
$b_0 = -M_1 M_1' g_p^{2C_1} + M_2 M_2' g_q^{2D_1}$
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

$b \equiv b_0 \quad (mod\ pq) \qquad (b = p - q)$

$b \equiv -M_1 M_1' g_p^{2C_1} + M_2 M_2' g_q^{2D_1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -M_1 M_1' g_p^{2C_1} + M_2 M_2' g_q^{2D_1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -q M_1' g_p^{2C_1} + p M_2' g_q^{2D_1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -(1 + ap) g_p^{2C_1} + (1 + bq) g_q^{2D_1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -g_p^{2C_1} - apg_p^{2C_1} + g_q^{2D_1} + bqg_q^{2D_1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -g_p^{2C_1} - ag_p^{2C_1} p + g_q^{2D_1} + bg_q^{2D_1} q \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -g_p^{2C_1} - (aq + np)p + g_q^{2D_1} + (bp + mq)q \quad (mod\ pq)$

$$\therefore \quad p-q \equiv -g_p^{2C_1} - apq - np^2 + g_q^{2D_1} + bpq + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -g_p^{2C_1} - np^2 + g_q^{2D_1} + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -np^2 + mq^2 - g_p^{2C_1} + g_q^{2D_1} \pmod{pq}$$

また、$p-q \equiv -np^2 + mq^2 - g_p^{2C_1} + g_q^{2D_1} \pmod{pq}$ である時

$g_p^{2C_1} g_q^{2D_1}$ を両辺に掛けて

$$g_p^{2C_1} g_q^{2D_1}(p-q) \equiv g_p^{2C_1} g_q^{2D_1}(-np^2 + mq^2 - g_p^{2C_1} + g_q^{2D_1}) \pmod{pq}$$

$$g_p^{2C_1} g_q^{2D_1} p - g_p^{2C_1} g_q^{2D_1} q$$

$$\equiv -g_p^{2C_1} g_q^{2D_1} np^2 + g_p^{2C_1} g_q^{2D_1} mq^2 - g_p^{2C_1} g_q^{2D_1} g_p^{2C_1} + g_p^{2C_1} g_q^{2D_1} g_q^{2D_1} \pmod{pq}$$

$$g_p^{2C_1} g_q^{2D_1} p - g_p^{2C_1} g_q^{2D_1} q$$

$$\equiv -g_p^{2C_1}\left(g_q^{2D_1} np^2\right) + g_q^{2D_1}\left(g_p^{2C_1} mq^2\right) - g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \pmod{pq}$$

この時 ①' ②'より

$$g_p^{2C_1} g_q^{2D_1} p - g_p^{2C_1} g_q^{2D_1} q$$

$$\equiv -g_p^{2C_1}\left(-g_p^{2C_1} p\right) + g_q^{2D_1}\left(-g_q^{2D_1} q\right) - g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \pmod{pq}$$

$$g_p^{2C_1} g_q^{2D_1} p - g_p^{2C_1} g_q^{2D_1} q - g_p^{2C_1}(g_p^{2C_1} p) + g_q^{2D_1}(g_q^{2D_1} q)$$

$$\equiv -g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \pmod{pq}$$

$$g_p^{2C_1} g_q^{2D_1} p - g_p^{2C_1} g_q^{2D_1} q - g_p^{4C_1} p + g_q^{4D_1} q \equiv -g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \pmod{pq}$$

$$-g_p^{4C_1} p + g_p^{2C_1} g_q^{2D_1} p - g_p^{2C_1} g_q^{2D_1} q + g_q^{4D_1} q \equiv -g_p^{4C_1} g_q^{2D_1} + g_p^{2C_1} g_q^{4D_1} \pmod{pq}$$

$$g_p^{2C_1}(g_q^{2D_1} - g_p^{2C_1})p + g_q^{2D_1}(g_q^{2D_1} - g_p^{2C_1})q \equiv g_p^{2C_1} g_q^{2D_1}\left(g_q^{2D_1} - g_p^{2C_1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1}(g_p^{2C_1} - g_q^{2D_1})p - g_q^{2D_1}(g_p^{2C_1} - g_q^{2D_1})q \equiv -g_p^{2C_1} g_q^{2D_1}\left(g_p^{2C_1} - g_q^{2D_1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1}(g_p^{2C_1} - g_q^{2D_1})p + g_q^{2D_1}(g_p^{2C_1} - g_q^{2D_1})q \equiv g_p^{2C_1} g_q^{2D_1}\left(g_p^{2C_1} - g_q^{2D_1}\right) \quad (mod\ pq)$$

___※$_2$

この時 ※$_1$＋※$_2$ より

$$g_p^{2C_1}(g_p^{2C_1}+g_q^{2D_1})p+g_q^{2D_1}(g_p^{2C_1}+g_q^{2D_1})q$$
$$+g_p^{2C_1}(g_p^{2C_1}-g_q^{2D_1})p+g_q^{2D_1}(g_p^{2C_1}-g_q^{2D_1})q$$
$$\equiv g_p^{2C_1}g_q^{2D_1}\left(g_p^{2C_1}+g_q^{2D_1}\right)+g_p^{2C_1}g_q^{2D_1}\left(g_p^{2C_1}-g_q^{2D_1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1}(g_p^{2C_1}+g_q^{2D_1})p+g_p^{2C_1}(g_p^{2C_1}-g_q^{2D_1})p$$
$$+g_q^{2D_1}(g_p^{2C_1}+g_q^{2D_1})q+g_q^{2D_1}(g_p^{2C_1}-g_q^{2D_1})q$$
$$\equiv g_p^{2C_1}g_q^{2D_1}\left(g_p^{2C_1}+g_q^{2D_1}\right)+g_p^{2C_1}g_q^{2D_1}\left(g_p^{2C_1}-g_q^{2D_1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1}(g_p^{2C_1}+g_q^{2D_1}+g_p^{2C_1}-g_q^{2D_1})p+g_q^{2D_1}(g_p^{2C_1}+g_q^{2D_1}+g_p^{2C_1}-g_q^{2D_1})q$$
$$\equiv g_p^{2C_1}g_q^{2D_1}\left(g_p^{2C_1}+g_q^{2D_1}+g_p^{2C_1}-g_q^{2D_1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1}(g_p^{2C_1}+g_p^{2C_1})p+g_q^{2D_1}(g_p^{2C_1}+g_p^{2C_1})q \equiv g_p^{2C_1}g_q^{2D_1}\left(g_p^{2C_1}+g_p^{2C_1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1}p\times 2g_p^{2C_1}+g_q^{2D_1}q\times 2g_p^{2C_1}\equiv g_p^{2C_1}g_q^{2D_1}\times 2g_p^{2C_1} \quad (mod\ pq)$$

この時 $(2,pq)=1$ より両辺を 2 で割って

$$g_p^{2C_1}p\times g_p^{2C_1}+g_q^{2D_1}q\times g_p^{2C_1}\equiv g_p^{2C_1}g_q^{2D_1}\times g_p^{2C_1} \quad (mod\ pq)$$

$$\therefore\ g_p^{4C_1}p+g_q^{2D_1}g_p^{2C_1}q\equiv g_p^{4C_1}g_q^{2D_1} \quad (mod\ pq)$$

この時 $\left(g_p,p\right)=1 \quad \left(g_p,q\right)=1$ より $\left(g_p,pq\right)=1$

$$\therefore\ \left(g_p^{2C_1},pq\right)=1$$

従って両辺を $g_p^{2C_1}$ で割って

$$g_p^{2C_1}p+g_q^{2D_1}q\equiv g_p^{2C_1}g_q^{2D_1} \quad (mod\ pq)$$

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

$$g_p^{2C_1} p + g_q^{2D_1} q \equiv g_p^{2C_1} g_q^{2D_1} \quad (mod\ pq)$$

$$\Rightarrow \quad q \equiv g_p^{2C_1}\ (mod\ p) \quad かつ \quad p \equiv g_q^{2D_1}\ (mod\ q)$$

∵

$g_p^{2C_1} p + g_q^{2D_1} q \equiv g_p^{2C_1} g_q^{2D_1} \quad (mod\ pq)$　の時

上記の方程式は

$g_p^{2C_1} p + g_q^{2D_1} q \equiv g_p^{2C_1} g_q^{2D_1} \quad (mod\ p)$

かつ

$g_p^{2C_1} p + g_q^{2D_1} q \equiv g_p^{2C_1} g_q^{2D_1} \quad (mod\ q)$

と同値である。

又、上記の方程式は

$g_q^{2D_1} q \equiv g_p^{2C_1} g_q^{2D_1} \quad (mod\ p)$

かつ

$g_p^{2C_1} p \equiv g_p^{2C_1} g_q^{2D_1} \quad (mod\ q)$ ＿＿＿☆$_1$

と同値である。

この時 $(g_q, p) = 1$　より　$(g_q^{2D_1}, p) = 1$

又、$(g_p, q) = 1$　より　$(g_p^{2C_1}, q) = 1$

従って、上記の方程式の両辺を $g_q^{2D_1}$，$g_p^{2C_1}$ でそれぞれ割って

$q \equiv g_p^{2C_1} \quad (mod\ p)$

かつ

$p \equiv g_q^{2D_1} \quad (mod\ q)$ ＿＿＿☆$_2$

この時、☆$_2$の方程式のそれぞれに $g_q^{2D_1}$，$g_p^{2C_1}$ を掛け合わせると
☆$_1$の方程式へと戻るため☆$_1$の方程式と☆$_2$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

$q \equiv g_p^{2C_2+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2+1} \ (mod\ q)$

$\Leftrightarrow \quad g_p^{2C_2+1} p + g_q^{2D_2+1} q \equiv g_p^{2C_2+1} g_q^{2D_2+1} \quad (mod\ pq)$　の証明

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

$q \equiv g_p^{2C_2+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2+1} \ (mod\ q)$

$\Rightarrow \quad g_p^{2C_2+1} p + g_q^{2D_2+1} q \equiv g_p^{2C_2+1} g_q^{2D_2+1} \quad (mod\ pq)$

$\because$

$q \equiv g_p^{2C_2+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2+1} \ (mod\ q)$　である時

$p + q \equiv g_p^{2C_2+1} \ (mod\ p)$　かつ　$p + q \equiv g_q^{2D_2+1} \ (mod\ q)$ __※ であるから

$M_s M_s'$ を条件

$pq = M_s m_s$

$(m_1 = p, m_2 = q)$

$M_s M_s' \equiv 1 \ (mod\ m_s)$

$m_1 = p \ , \ M_1 = q$

$M_1 M_1' \equiv q M_1' \equiv 1 \quad (mod\ p)$

$m_2 = q \ , \ M_2 = p$

$M_2 M_2' \equiv p M_2' \equiv 1 \quad (mod\ q)$

によって定められる数とし
$a_0 = M_1 M_1' g_p^{2C_2+1} + M_2 M_2' g_q^{2D_2+1}$
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

$a \equiv a_0 \quad (mod\ pq) \qquad (a = p + q)$

$$a \equiv M_1 M_1' g_p^{2C_2+1} + M_2 M_2' g_q^{2D_2+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv M_1 M_1' g_p^{2C_2+1} + M_2 M_2' g_q^{2D_2+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv qM_1' g_p^{2C_2+1} + pM_2' g_q^{2D_2+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv (1+ap) g_p^{2C_2+1} + (1+bq) g_q^{2D_2+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_2+1} + apg_p^{2C_2+1} + g_q^{2D_2+1} + bqg_q^{2D_2+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_2+1} + ag_p^{2C_2+1} p + g_q^{2D_2+1} + bg_q^{2D_2+1} q \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_2+1} + (aq+np)p + g_q^{2D_2+1} + (bp+mq)q \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_2+1} + apq + np^2 + g_q^{2D_2+1} + bpq + mq^2 \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_2+1} + np^2 + g_q^{2D_2+1} + mq^2 \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv np^2 + mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ pq)$$

この時上記の命題は

$$p+q \equiv np^2 + mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ p) \quad \text{__③}$$

かつ

$$p+q \equiv np^2 + mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ q) \quad \text{__④}$$

と同値である。

③ の時

$$p+q \equiv np^2 + mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ p)$$

$$q \equiv mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ p)$$

$$g_p^{2C_2+1} \equiv mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ p)$$

$$g_p^{2C_2+1} \equiv mqq + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ p)$$

$$0 \equiv mg_p^{2C_2+1}q + g_q^{2D_2+1} \quad (mod\ p)$$

$$mg_p^{2C_2+1}q + g_q^{2D_2+1} \equiv 0 \quad (mod\ p)$$

$$mg_p^{2C_2+1}q \equiv -g_q^{2D_2+1} \quad (mod\ p)$$

$$mg_p^{2C_2+1}q^2 \equiv -g_q^{2D_2+1}q \quad (mod\ pq) \quad \text{__③'}$$

④　の時

$$p + q \equiv np^2 + mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ q)$$

$$p \equiv np^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ q)$$

$$p \equiv npp + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ q)$$

$$g_q^{2D_2+1} \equiv ng_q^{2D_2+1}p + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ q)$$

$$0 \equiv ng_q^{2D_2+1}p + g_p^{2C_2+1} \quad (mod\ q)$$

$$ng_q^{2D_2+1}p + g_p^{2C_2+1} \equiv 0 \quad (mod\ q)$$

$$ng_q^{2D_2+1}p \equiv -g_p^{2C_2+1} \quad (mod\ q)$$

$$ng_q^{2D_2+1}p^2 \equiv -g_p^{2C_2+1}p \quad (mod\ pq) \quad \text{__④'}$$

また、$p + q \equiv np^2 + mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1} \quad (mod\ pq)$ である時

$g_p^{2C_2+1}g_q^{2D_2+1}$を両辺に掛けて

$$g_p^{2C_2+1}g_q^{2D_2+1}(p + q) \equiv g_p^{2C_2+1}g_q^{2D_2+1}(np^2 + mq^2 + g_p^{2C_2+1} + g_q^{2D_2+1}) \quad (mod\ pq)$$

$$g_p^{2C_2+1}g_q^{2D_2+1}p + g_p^{2C_2+1}g_q^{2D_2+1}q$$
$$\equiv g_p^{2C_2+1}g_q^{2D_2+1}np^2 + g_p^{2C_2+1}g_q^{2D_2+1}mq^2 + g_p^{2C_2+1}g_q^{2D_2+1}g_p^{2C_2+1}$$
$$+ g_p^{2C_2+1}g_q^{2D_2+1}g_q^{2D_2+1} \quad (mod\ pq)$$

$$g_p^{2C_2+1}g_q^{2D_2+1}p + g_p^{2C_2+1}g_q^{2D_2+1}q$$
$$\equiv g_p^{2C_2+1}(g_q^{2D_2+1}np^2) + g_q^{2D_2+1}(g_p^{2C_2+1}mq^2) + g_p^{4C_2+2}g_q^{2D_2+1} + g_p^{2C_2+1}g_q^{4D_2+2} \quad (mod\ pq)$$

この時 ③' ④'より
$$g_p^{2C_2+1}g_q^{2D_2+1}p + g_p^{2C_2+1}g_q^{2D_2+1}q$$
$$\equiv g_p^{2C_2+1}(-g_p^{2C_2+1}p) + g_q^{2D_2+1}(-g_q^{2D_2+1}q) + g_p^{4C_2+2}g_q^{2D_2+1} + g_p^{2C_2+1}g_q^{4D_2+2} \quad (mod\ pq)$$

$$g_p^{2C_2+1}g_q^{2D_2+1}p + g_p^{2C_2+1}g_q^{2D_2+1}q + g_p^{2C_2+1}(g_p^{2C_2+1}p) + g_q^{2D_2+1}(g_q^{2D_2+1}q)$$
$$\equiv g_p^{4C_2+2}g_q^{2D_2+1} + g_p^{2C_2+1}g_q^{4D_2+2} \quad (mod\ pq)$$

$$g_p^{2C_2+1}g_q^{2D_2+1}p + g_p^{2C_2+1}g_q^{2D_2+1}q + g_p^{4C_2+2}p + g_q^{4D_2+2}q$$
$$\equiv g_p^{4C_2+2}g_q^{2D_2+1} + g_p^{2C_2+1}g_q^{4D_2+2} \quad (mod\ pq)$$

$$g_p^{4C_2+2}p + g_p^{2C_2+1}g_q^{2D_2+1}p + g_p^{2C_2+1}g_q^{2D_2+1}q + g_q^{4D_2+2}q$$
$$\equiv g_p^{4C_2+2}g_q^{2D_2+1} + g_p^{2C_2+1}g_q^{4D_2+2} \quad (mod\ pq)$$

$$g_p^{2C_2+1}\left(g_p^{2C_2+1} + g_q^{2D_2+1}\right)p + g_q^{2D_2+1}\left(g_p^{2C_2+1} + g_q^{2D_2+1}\right)q$$
$$\equiv g_p^{2C_2+1}g_q^{2D_2+1}\left(g_p^{2C_2+1} + g_q^{2D_2+1}\right)(mod\ pq) \quad \text{\_\_\_※3}$$

又、$q \equiv g_p^{2C_2+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2+1} (mod\ q)$　である時

$-q \equiv -g_p^{2C_2+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2+1} \ (mod\ q)$

$p - q \equiv -g_p^{2C_2+1} \ (mod\ p)$　かつ　$p - q \equiv g_q^{2D_2+1} \ (mod\ q)$ __※ であるから

$M_s M_s'$ を条件

$pq = M_s m_s$

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

$M_s M_s' \equiv 1 \ (mod\ m_s)$

$m_1 = p\ ,\ M_1 = q$

$M_1 M_1' \equiv q M_1' \equiv 1 \quad (mod\ p)$

$m_2 = q\ ,\ M_2 = p$

$M_2 M_2' \equiv p M_2' \equiv 1 \quad (mod\ q)$

によって定められる数とし
$b_0 = -M_1 M_1' g_p^{2C_2+1} + M_2 M_2' g_q^{2D_2+1}$
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

$b \equiv b_0 \quad (mod\ pq) \qquad (b = p - q)$

$b \equiv -M_1 M_1' g_p^{2C_2+1} + M_2 M_2' g_q^{2D_2+1} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -M_1 M_1' g_p^{2C_2+1} + M_2 M_2' g_q^{2D_2+1} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -q M_1' g_p^{2C_2+1} + p M_2' g_q^{2D_2+1} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -(1 + ap) g_p^{2C_2+1} + (1 + bq) g_q^{2D_2+1} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -g_p^{2C_2+1} - apg_p^{2C_2+1} + g_q^{2D_2+1} + bqg_q^{2D_2+1} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -g_p^{2C_2+1} - ag_p^{2C_2+1} p + g_q^{2D_2+1} + bg_q^{2D_2+1} q \quad (mod\ pq)$

$\therefore \quad p - q \equiv -g_p^{2C_2+1} - (aq + np)p + g_q^{2D_2+1} + (bp + mq)q \quad (mod\ pq)$

$$\therefore \quad p-q \equiv -g_p^{2C_2+1} - apq - np^2 + g_q^{2D_2+1} + bpq + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -g_p^{2C_2+1} - np^2 + g_q^{2D_2+1} + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -np^2 + mq^2 - g_p^{2C_2+1} + g_q^{2D_2+1} \pmod{pq}$$

また、$p-q \equiv -np^2 + mq^2 - g_p^{2C_2+1} + g_q^{2D_2+1} \pmod{pq}$ である時

$g_p^{2C_2+1} g_q^{2D_2+1}$ を両辺に掛けて

$$g_p^{2C_2+1} g_q^{2D_2+1}(p-q) \equiv g_p^{2C_2+1} g_q^{2D_2+1}(-np^2 + mq^2 - g_p^{2C_2+1} + g_q^{2D_2+1}) \pmod{pq}$$

$$g_p^{2C_2+1} g_q^{2D_2+1} p - g_p^{2C_2+1} g_q^{2D_2+1} q$$
$$\equiv -g_p^{2C_2+1} g_q^{2D_2+1} np^2 + g_p^{2C_2+1} g_q^{2D_2+1} mq^2 - g_p^{2C_2+1} g_q^{2D_2+1} g_p^{2C_2+1}$$
$$+ g_p^{2C_2+1} g_q^{2D_2+1} g_q^{2D_2+1} \pmod{pq}$$

$$g_p^{2C_2+1} g_q^{2D_2+1} p - g_p^{2C_2+1} g_q^{2D_2+1} q$$
$$\equiv -g_p^{2C_2+1} \left(g_q^{2D_2+1} np^2\right) + g_q^{2D_2+1} \left(g_p^{2C_2+1} mq^2\right) - g_p^{4C_2+2} g_q^{2D_2+1} + g_p^{2C_2+1} g_q^{4D_2+2} \pmod{pq}$$

この時 ③' ④'より

$$g_p^{2C_2+1} g_q^{2D_2+1} p - g_p^{2C_2+1} g_q^{2D_2+1} q$$
$$\equiv -g_p^{2C_2+1} \left(-g_p^{2C_2+1} p\right) + g_q^{2D_2+1} \left(-g_q^{2D_2+1} q\right) - g_p^{4C_2+2} g_q^{2D_2+1} + g_p^{2C_2+1} g_q^{4D_2+2} \pmod{pq}$$

$$g_p^{2C_2+1} g_q^{2D_2+1} p - g_p^{2C_2+1} g_q^{2D_2+1} q - g_p^{2C_2+1} \left(g_p^{2C_2+1} p\right) + g_q^{2D_2+1} \left(g_q^{2D_2+1} q\right)$$
$$\equiv -g_p^{4C_2+2} g_q^{2D_2+1} + g_p^{2C_2+1} g_q^{4D_2+2} \pmod{pq}$$

$$g_p^{2C_2+1} g_q^{2D_2+1} p - g_p^{2C_2+1} g_q^{2D_2+1} q - g_p^{4C_2+2} p + g_q^{4D_2+2} q$$
$$\equiv -g_p^{4C_2+2} g_q^{2D_2+1} + g_p^{2C_2+1} g_q^{4D_2+2} \pmod{pq}$$

$$-g_p^{4C_2+2} p + g_p^{2C_2+1} g_q^{2D_2+1} p - g_p^{2C_2+1} g_q^{2D_2+1} q + g_q^{4D_2+2} q$$

$$\equiv -g_p^{4C_2+1} g_q^{2D_2+1} + g_p^{2C_2+1} g_q^{4D_2+2} \quad (mod\ pq)$$

$$g_p^{2C_2+1}\left(g_q^{2D_2+1} - g_p^{2C_2+1}\right)p + g_q^{2D_2+1}\left(g_q^{2D_2+1} - g_p^{2C_2+1}\right)q$$

$$\equiv g_p^{2C_2+1} g_q^{2D_2+1}\left(g_q^{2D_2+1} - g_p^{2C_2+1}\right) \quad (mod\ pq)$$

$$-g_p^{2C_2+1}\left(g_p^{2C_2+1} - g_q^{2D_2+1}\right)p - g_q^{2D_2+1}\left(g_p^{2C_2+1} - g_q^{2D_2+1}\right)q$$

$$\equiv -g_p^{2C_2+1} g_q^{2D_2+1}\left(g_p^{2C_2+1} - g_q^{2D_2+1}\right) \quad (mod\ pq)$$

$$g_p^{2C_2+1}\left(g_p^{2C_2+1} - g_q^{2D_2+1}\right)p + g_q^{2D_2+1}\left(g_p^{2C_2+1} - g_q^{2D_2+1}\right)q$$

$$\equiv g_p^{2C_2+1} g_q^{2D_2+1}\left(g_p^{2C_2+1} - g_q^{2D_2+1}\right) \quad (mod\ pq)$$

___※4

この時 ※$_3$＋※$_4$ より

$$g_p^{2C_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1})p+g_q^{2D_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1})q$$
$$+g_p^{2C_2+1}(g_p^{2C_2+1}-g_q^{2D_2+1})p+g_q^{2D_2+1}(g_p^{2C_2+1}-g_q^{2D_2+1})q$$
$$\equiv g_p^{2C_2+1}g_q^{2D_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1})+g_p^{2C_2+1}g_q^{2D_2+1}(g_p^{2C_2+1}-g_q^{2D_2+1}) \quad (mod\ pq)$$

$$g_p^{2C_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1})p+g_p^{2C_2+1}(g_p^{2C_2+1}-g_q^{2D_2+1})p$$
$$+g_q^{2D_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1})q+g_q^{2D_2+1}(g_p^{2C_2+1}-g_q^{2D_2+1})q$$
$$\equiv g_p^{2C_2+1}g_q^{2D_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1})+g_p^{2C_2+1}g_q^{2D_2+1}(g_p^{2C_2+1}-g_q^{2D_2+1}) \quad (mod\ pq)$$

$$g_p^{2C_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1}+g_p^{2C_2+1}-g_q^{2D_2+1})p+g_q^{2D_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1}+g_p^{2C_2+1}-g_q^{2D_2+1})$$
$$\equiv g_p^{2C_2+1}g_q^{2D_2+1}(g_p^{2C_2+1}+g_q^{2D_2+1}+g_p^{2C_2+1}-g_q^{2D_2+1}) \quad (mod\ pq)$$

$$g_p^{2C_2+1}(g_p^{2C_2+1}+g_p^{2C_2+1})p+g_q^{2D_2+1}(g_p^{2C_2+1}+g_p^{2C_2+1})$$
$$\equiv g_p^{2C_2+1}g_q^{2D_2+1}(g_p^{2C_2+1}+g_p^{2C_2+1}) \quad (mod\ pq)$$

$$g_p^{2C_2+1}p\times 2g_p^{2C_2+1}+g_q^{2D_2+1}q\times 2g_p^{2C_2+1}\equiv g_p^{2C_2+1}g_q^{2D_2+1}\times 2g_p^{2C_2+1} \quad (mod\ pq)$$

この時 $(2,pq)=1$ より両辺を 2 で割って

$$g_p^{2C_2+1}p\times g_p^{2C_2+1}+g_q^{2D_2+1}q\times g_p^{2C_2+1}\equiv g_p^{2C_2+1}g_q^{2D_2+1}\times g_p^{2C_2+1} \quad (mod\ pq)$$

$$\therefore g_p^{4C_2+2}p+g_q^{2D_2+1}g_p^{2C_2+1}q\equiv g_p^{4C_2+2}g_q^{2D_2+1} \quad (mod\ pq)$$

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

$\therefore\ (g_p^{2C_2+1},pq)=1$

従って両辺を $g_p^{2C_2+1}$ で割って

$$g_p^{2C_2+1}p+g_q^{2D_2+1}q\equiv g_p^{2C_2+1}g_q^{2D_2+1} \quad (mod\ pq)$$

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

$$g_p^{2C_2+1} p + g_q^{2D_2+1} q \equiv g_p^{2C_2+1} g_q^{2D_2+1} \pmod{pq}$$

$$\Rightarrow \quad q \equiv g_p^{2C_2+1} \pmod{p} \quad \text{かつ} \quad p \equiv g_q^{2D_2+1} \pmod{q}$$

∵

$g_p^{2C_2+1} p + g_q^{2D_2+1} q \equiv g_p^{2C_2+1} g_q^{2D_2+1} \pmod{pq}$　の時

上記の方程式は

$$g_p^{2C_2+1} p + g_q^{2D_2+1} q \equiv g_p^{2C_2+1} g_q^{2D_2+1} \pmod{p}$$

かつ

$$g_p^{2C_2+1} p + g_q^{2D_2+1} q \equiv g_p^{2C_2+1} g_q^{2D_2+1} \pmod{q}$$

と同値である。

又、上記の方程式は

$$g_q^{2D_2+1} q \equiv g_p^{2C_2+1} g_q^{2D_2+1} \pmod{p}$$

かつ

$$g_p^{2C_2+1} p \equiv g_p^{2C_2+1} g_q^{2D_2+1} \pmod{q} \quad \text{____☆}_3$$

と同値である。

この時 $(g_q, p) = 1$　より　$(g_q^{2D_2+1}, p) = 1$

又、$(g_p, q) = 1$　より　$(g_p^{2C_2+1}, q) = 1$

従って、上記の方程式の両辺を $g_q^{2D_2+1}$, $g_p^{2C_2+1}$ でそれぞれ割って

$$q \equiv g_p^{2C_2+1} \pmod{p}$$

かつ

$$p \equiv g_q^{2D_2+1} \pmod{q} \quad \text{____☆}_4$$

この時、☆$_4$の方程式のそれぞれに $g_q^{2D_2+1}$，$g_p^{2C_2+1}$ を掛け合わせると
☆$_3$の方程式へと戻るため☆$_3$の方程式と☆$_4$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】

$(g_p, q) = 1$　かつ　$(g_q, p) = 1$　である時

$q \equiv g_p^{2C_1'} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1'+1} \ (mod\ q)$

$\Leftrightarrow \quad g_p^{2C_1'} p + g_q^{2D_1'+1} q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ pq)$　の証明

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

$q \equiv g_p^{2C_1'} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1'+1} \ (mod\ q)$

$\Rightarrow \quad g_p^{2C_1'} p + g_q^{2D_1'+1} q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ pq)$

$\because$

$q \equiv g_p^{2C_1'} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1'+1} \ (mod\ q)$　である時

$p + q \equiv g_p^{2C_1'} \ (mod\ p)$　かつ　$p + q \equiv g_q^{2D_1'+1} \ (mod\ q)$ __※ であるから

$M_s M_s'$ を条件

$pq = M_s m_s$

$(m_1 = p, m_2 = q)$

$M_s M_s' \equiv 1 \ (mod\ m_s)$

$m_1 = p \ , \ M_1 = q$

$M_1 M_1' \equiv q M_1' \equiv 1 \quad (mod\ p)$

$m_2 = q \ , \ M_2 = p$

$M_2 M_2' \equiv p M_2' \equiv 1 \quad (mod\ q)$

によって定められる数とし

$a_0 = M_1 M_1' g_p^{2C_1'} + M_2 M_2' g_q^{2D_1'+1}$

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

$a \equiv a_0 \quad (mod\ pq) \qquad (a = p + q)$

$$a \equiv M_1 M_1' g_p^{2C_1'} + M_2 M_2' g_q^{2D_1'+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv M_1 M_1' g_p^{2C_1'} + M_2 M_2' g_q^{2D_1'+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv qM_1' g_p^{2C_1'} + pM_2' g_q^{2D_1'+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv (1+ap) g_p^{2C_1'} + (1+bq) g_q^{2D_1'+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_1'} + apg_p^{2C_1'} + g_q^{2D_1'+1} + bqg_q^{2D_1'+1} \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_1'} + ag_p^{2C_1'} p + g_q^{2D_1'+1} + bg_q^{2D_1'+1} q \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_1'} + (aq+np)p + g_q^{2D_1'+1} + (bp+mq)q \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_1'} + apq + np^2 + g_q^{2D_1'+1} + bpq + mq^2 \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv g_p^{2C_1'} + np^2 + g_q^{2D_1'+1} + mq^2 \quad (mod\ pq)$$

$$\therefore \quad p+q \equiv np^2 + mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ pq)$$

この時上記の命題は

$$p+q \equiv np^2 + mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ p) \quad \text{⑤}$$

かつ

$$p+q \equiv np^2 + mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ q) \quad \text{⑥}$$

と同値である。

⑤ の時

$$p+q \equiv np^2 + mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ p)$$

$$q \equiv mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ p)$$

$$g_p^{2C_1'} \equiv mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ p)$$

$g_p^{2C_1'} \equiv mqq + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ p)$

$0 \equiv mg_p^{2C_1'}q + g_q^{2D_1'+1} \quad (mod\ p)$

$mg_p^{2C_1'}q + g_q^{2D_1'+1} \equiv 0 \quad (mod\ p)$

$mg_p^{2C_1'}q \equiv -g_q^{2D_1'+1} \quad (mod\ p)$

$mg_p^{2C_1'}q^2 \equiv -g_q^{2D_1'+1}q \quad (mod\ pq)$ __⑤'

⑥ の時

$p + q \equiv np^2 + mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ q)$

$p \equiv np^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ q)$

$p \equiv npp + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ q)$

$g_q^{2D_1'+1} \equiv ng_q^{2D_1'+1}p + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ q)$

$0 \equiv ng_q^{2D_1'+1}p + g_p^{2C_1'} \quad (mod\ q)$

$ng_q^{2D_1'+1}p + g_p^{2C_1'} \equiv 0 \quad (mod\ q)$

$ng_q^{2D_1'+1}p \equiv -g_p^{2C_1'} \quad (mod\ q)$

$ng_q^{2D_1'+1}p^2 \equiv -g_p^{2C_1'}p \quad (mod\ pq)$ __⑥'

また、$p + q \equiv np^2 + mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1} \quad (mod\ pq)$ である時

$g_p^{2C_1'}g_q^{2D_1'+1}$ を両辺に掛けて

$g_p^{2C_1'}g_q^{2D_1'+1}(p + q) \equiv g_p^{2C_1'}g_q^{2D_1'+1}(np^2 + mq^2 + g_p^{2C_1'} + g_q^{2D_1'+1}) \quad (mod\ pq)$

$g_p^{2C_1'}g_q^{2D_1'+1}p + g_p^{2C_1'}g_q^{2D_1'+1}q$

$$\equiv g_p^{2C_1'} g_q^{2D_1'+1} np^2 + g_p^{2C_1'} g_q^{2D_1'+1} mq^2 + g_p^{2C_1'} g_q^{2D_1'+1} g_p^{2C_1'} + g_p^{2C_1'} g_q^{2D_1'+1} g_q^{2D_1'+1} \quad (mod\ pq)$$

$$g_p^{2C_1'} g_q^{2D_1'+1} p + g_p^{2C_1'} g_q^{2D_1'+1} q$$

$$\equiv g_p^{2C_1'} (g_q^{2D_1'+1} np^2) + g_q^{2D_1'+1} (g_p^{2C_1'} mq^2) + g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \quad (mod\ pq)$$

この時 ⑤' ⑥'より

$$g_p^{2C_1'} g_q^{2D_1'+1} p + g_p^{2C_1'} g_q^{2D_1'+1} q$$

$$\equiv g_p^{2C_1'} (-g_p^{2C_1'} p) + g_q^{2D_1'+1} (-g_q^{2D_1'+1} q) + g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \quad (mod\ pq)$$

$$g_p^{2C_1'} g_q^{2D_1'+1} p + g_p^{2C_1'} g_q^{2D_1'+1} q + g_p^{2C_1'} (g_p^{2C_1'} p) + g_q^{2D_1'+1} (g_q^{2D_1'+1} q)$$

$$\equiv g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \quad (mod\ pq)$$

$$g_p^{2C_1'} g_q^{2D_1'+1} p + g_p^{2C_1'} g_q^{2D_1'+1} q + g_p^{4C_1'} p + g_q^{4D_1'+2} q \equiv g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \quad (mod\ pq)$$

$$g_p^{4C_1'} p + g_p^{2C_1'} g_q^{2D_1'+1} p + g_p^{2C_1'} g_q^{2D_1'+1} q + g_q^{4D_1'+2} q \equiv g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \quad (mod\ pq)$$

$$g_p^{2C_1'} (g_p^{2C_1'} + g_q^{2D_1'+1}) p + g_q^{2D_1'+1} (g_p^{2C_1'} + g_q^{2D_1'+1}) q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \left( g_p^{2C_1'} + g_q^{2D_1'+1} \right) \quad (mod\ pq)$$

___※1

又、$q \equiv g_p^{2C_1'} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1'+1} \ (mod\ q)$　である時

$-q \equiv -g_p^{2C_1'} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_1'+1} \ (mod\ q)$

$p - q \equiv -g_p^{2C_1'} \ (mod\ p)$　かつ　$p - q \equiv g_q^{2D_1'+1} \ (mod\ q)$ __※ であるから

$M_s M_s'$ を条件　　$m_1 = p \ ,\ M_1 = q$

$pq = M_s m_s$　　$M_1 M_1' \equiv q M_1' \equiv 1 \quad (mod\ p)$

$(m_1 = p\ , m_2 = q)$　　$m_2 = q \ ,\ M_2 = p$

$M_s M_s' \equiv 1\ (mod\ m_s)$　　$M_2 M_2' \equiv p M_2' \equiv 1 \quad (mod\ q)$

によって定められる数とし
$b_0 = -M_1 M_1' g_p^{2C_1'} + M_2 M_2' g_q^{2D_1'+1}$
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

$b \equiv b_0 \quad (mod\ pq) \qquad (b = p - q)$

$b \equiv -M_1 M_1' g_p^{2C_1'} + M_2 M_2' g_q^{2D_1'+1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -M_1 M_1' g_p^{2C_1'} + M_2 M_2' g_q^{2D_1'+1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -q M_1' g_p^{2C_1'} + p M_2' g_q^{2D_1'+1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -(1 + ap) g_p^{2C_1'} + (1 + bq) g_q^{2D_1'+1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -g_p^{2C_1'} - apg_p^{2C_1'} + g_q^{2D_1'+1} + bqg_q^{2D_1'+1} \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -g_p^{2C_1'} - ag_p^{2C_1'} p + g_q^{2D_1'+1} + bg_q^{2D_1'+1} q \quad (mod\ pq)$

$\therefore \qquad p - q \equiv -g_p^{2C_1'} - (aq + np)p + g_q^{2D_1'+1} + (bp + mq)q \quad (mod\ pq)$

$$\therefore \quad p-q \equiv -g_p^{2C_1'} - apq - np^2 + g_q^{2D_1'+1} + bpq + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -g_p^{2C_1'} - np^2 + g_q^{2D_1'+1} + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -np^2 + mq^2 - g_p^{2C_1'} + g_q^{2D_1'+1} \pmod{pq}$$

また、$p-q \equiv -np^2 + mq^2 - g_p^{2C_1'} + g_q^{2D_1'+1} \pmod{pq}$ である時

$g_p^{2C_1'} g_q^{2D_1'+1}$ を両辺に掛けて

$$g_p^{2C_1'} g_q^{2D_1'+1}(p-q) \equiv g_p^{2C_1'} g_q^{2D_1'+1}(-np^2 + mq^2 - g_p^{2C_1'} + g_q^{2D_1'+1}) \pmod{pq}$$

$$g_p^{2C_1'} g_q^{2D_1'+1} p - g_p^{2C_1'} g_q^{2D_1'+1} q$$
$$\equiv -g_p^{2C_1'} g_q^{2D_1'+1} np^2 + g_p^{2C_1'} g_q^{2D_1'+1} mq^2 - g_p^{2C_1'} g_q^{2D_1'+1} g_p^{2C_1'} + g_p^{2C_1'} g_q^{2D_1'+1} g_q^{2D_1'+1} \pmod{pq}$$

$$g_p^{2C_1'} g_q^{2D_1'+1} p - g_p^{2C_1'} g_q^{2D_1'+1} q$$
$$\equiv -g_p^{2C_1'} \left(g_q^{2D_1'+1} np^2\right) + g_q^{2D_1'+1} \left(g_p^{2C_1'} mq^2\right) - g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \pmod{pq}$$

この時 ⑤' ⑥'より

$$g_p^{2C_1'} g_q^{2D_1'+1} p - g_p^{2C_1'} g_q^{2D_1'+1} q$$
$$\equiv -g_p^{2C_1'} \left(-g_p^{2C_1'} p\right) + g_q^{2D_1'+1} \left(-g_q^{2D_1'+1} q\right) - g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \pmod{pq}$$

$$g_p^{2C_1'} g_q^{2D_1'+1} p - g_p^{2C_1'} g_q^{2D_1'+1} q - g_p^{2C_1'} (g_p^{2C_1'} p) + g_q^{2D_1'+1} (g_q^{2D_1'+1} q)$$
$$\equiv -g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \pmod{pq}$$

$$g_p^{2C_1'} g_q^{2D_1'+1} p - g_p^{2C_1'} g_q^{2D_1'+1} q - g_p^{4C_1'} p + g_q^{4D_1'+2} q \equiv -g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \pmod{pq}$$

$$-g_p^{4C_1'} p + g_p^{2C_1'} g_q^{2D_1'+1} p - g_p^{2C_1'} g_q^{2D_1'+1} q + g_q^{4D_1'+2} q \equiv -g_p^{4C_1'} g_q^{2D_1'+1} + g_p^{2C_1'} g_q^{4D_1'+2} \pmod{pq}$$

$$g_p^{2C_1'}(g_q^{2D_1'+1} - g_p^{2C_1'})p + g_q^{2D_1'+1}(g_q^{2D_1'+1} - g_p^{2C_1'})q \equiv g_p^{2C_1'} g_q^{2D_1'+1}\left(g_q^{2D_1'+1} - g_p^{2C_1'}\right) \quad (mod\ pq)$$

$$-g_p^{2C_1'}(g_p^{2C_1'} - g_q^{2D_1'+1})p - g_q^{2D_1'+1}(g_p^{2C_1'} - g_q^{2D_1'+1})q \equiv -g_p^{2C_1'} g_q^{2D_1'+1}\left(g_p^{2C_1'} - g_q^{2D_1'+1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1'}(g_p^{2C_1'} - g_q^{2D_1'+1})p + g_q^{2D_1'+1}(g_p^{2C_1'} - g_q^{2D_1'+1})q \equiv g_p^{2C_1'} g_q^{2D_1'+1}\left(g_p^{2C_1'} - g_q^{2D_1'+1}\right) \quad (mod\ pq)$$

___※$_2$

この時 ※$_1$＋※$_2$ より

$$g_p^{2C_1'}(g_p^{2C_1'}+g_q^{2D_1'+1})p+g_q^{2D_1'+1}(g_p^{2C_1'}+g_q^{2D_1'+1})q$$
$$+g_p^{2C_1'}(g_p^{2C_1'}-g_q^{2D_1'+1})p+g_q^{2D_1'+1}(g_p^{2C_1'}-g_q^{2D_1'+1})q$$
$$\equiv g_p^{2C_1'}g_q^{2D_1'+1}\left(g_p^{2C_1'}+g_q^{2D_1'+1}\right)+g_p^{2C_1'}g_q^{2D_1'+1}\left(g_p^{2C_1'}-g_q^{2D_1'+1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1'}(g_p^{2C_1'}+g_q^{2D_1'+1})p+g_p^{2C_1'}(g_p^{2C_1'}-g_q^{2D_1'+1})p$$
$$+g_q^{2D_1'+1}(g_p^{2C_1'}+g_q^{2D_1'+1})q+g_q^{2D_1'+1}(g_p^{2C_1'}-g_q^{2D_1'+1})q$$
$$\equiv g_p^{2C_1'}g_q^{2D_1'+1}\left(g_p^{2C_1'}+g_q^{2D_1'+1}\right)+g_p^{2C_1'}g_q^{2D_1'+1}\left(g_p^{2C_1'}-g_q^{2D_1'+1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1'}(g_p^{2C_1'}+g_q^{2D_1'+1}+g_p^{2C_1'}-g_q^{2D_1'+1})p+g_q^{2D_1'+1}(g_p^{2C_1'}+g_q^{2D_1'+1}+g_p^{2C_1'}-g_q^{2D_1'+1})q$$
$$\equiv g_p^{2C_1'}g_q^{2D_1'+1}\left(g_p^{2C_1'}+g_q^{2D_1'+1}+g_p^{2C_1'}-g_q^{2D_1'+1}\right) \quad (mod\ pq)$$

$$g_p^{2C_1'}(g_p^{2C_1'}+g_p^{2C_1'})p+g_q^{2D_1'+1}(g_p^{2C_1'}+g_p^{2C_1'})q\equiv g_p^{2C_1'}g_q^{2D_1'+1}\left(g_p^{2C_1'}+g_p^{2C_1'}\right) \quad (mod\ pq)$$

$$g_p^{2C_1'}p\times 2g_p^{2C_1'}+g_q^{2D_1'+1}q\times 2g_p^{2C_1'}\equiv g_p^{2C_1'}g_q^{2D_1'+1}\times 2g_p^{2C_1'} \quad (mod\ pq)$$

この時 $(2,pq)=1$ より両辺を 2 で割って

$$g_p^{2C_1'}p\times g_p^{2C_1'}+g_q^{2D_1'+1}q\times g_p^{2C_1'}\equiv g_p^{2C_1'}g_q^{2D_1'+1}\times g_p^{2C_1'} \quad (mod\ pq)$$

$$\therefore\ g_p^{4C_1'}p+g_q^{2D_1'+1}g_p^{2C_1'}q\equiv g_p^{4C_1'}g_q^{2D_1'+1} \quad (mod\ pq)$$

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

$$\therefore\ \left(g_p^{2c_1'},pq\right)=1$$

従って両辺を $g_p^{2c_1'}$ で割って

$$g_p^{2C_1'}p+g_q^{2D_1'+1}q\equiv g_p^{2C_1'}g_q^{2D_1'+1} \quad (mod\ pq)$$

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

$$g_p^{2C_1'} p + g_q^{2D_1'+1} q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ pq)$$

$$\Rightarrow \quad q \equiv g_p^{2C_1'}\ (mod\ p) \quad \text{かつ} \quad p \equiv g_q^{2D_1'+1}\ (mod\ q)$$

∵

$g_p^{2C_1'} p + g_q^{2D_1'+1} q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ pq)$ の時

上記の方程式は

$$g_p^{2C_1'} p + g_q^{2D_1'+1} q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ p)$$

かつ

$$g_p^{2C_1'} p + g_q^{2D_1'+1} q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ q)$$

と同値である。

又、上記の方程式は

$$g_q^{2D_1'+1} q \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ p)$$

かつ

$g_p^{2C_1'} p \equiv g_p^{2C_1'} g_q^{2D_1'+1} \quad (mod\ q)$ ＿＿＿☆$_1$

と同値である。

この時 $(g_q, p) = 1$ より $\left(g_q^{2D_1'+1}, p\right) = 1$

又、$(g_p, q) = 1$ より $\left(g_p^{2C_1'}, q\right) = 1$

従って、上記の方程式の両辺を $g_q^{2D_1'+1}$, $g_p^{2C_1'}$ でそれぞれ割って

$$q \equiv g_p^{2C_1'} \quad (mod\ p)$$

かつ

$$p \equiv g_q^{2D_1'+1} \pmod{q} \quad \text{____☆}_2$$

この時、☆$_2$の方程式のそれぞれに $g_q^{2D_1'+1}$，$g_p^{2C_1'}$ を掛け合わせると

☆$_1$の方程式へと戻るため☆$_1$の方程式と☆$_2$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

$q \equiv g_p^{2C_2'+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2'} \ (mod\ q)$

$\Leftrightarrow \quad g_p^{2C_2'+1} p + g_q^{2D_2'} q \equiv g_p^{2C_2'+1} g_q^{2D_2'} \quad (mod\ pq)$　の証明

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

$q \equiv g_p^{2C_2'+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2'} \ (mod\ q)$

$\Rightarrow \quad g_p^{2C_2'+1} p + g_q^{2D_2'} q \equiv g_p^{2C_2'+1} g_q^{2D_2'} \quad (mod\ pq)$

∵

$q \equiv g_p^{2C_2'+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2'} \ (mod\ q)$　である時

$p + q \equiv g_p^{2C_2'+1} \ (mod\ p)$　かつ　$p + q \equiv g_q^{2D_2'} \ (mod\ q)$ __※ であるから

$M_s M_s'$ を条件

$pq = M_s m_s$

$(m_1 = p, m_2 = q)$

$M_s M_s' \equiv 1 \ (mod\ m_s)$

$m_1 = p \ , \ M_1 = q$

$M_1 M_1' \equiv q M_1' \equiv 1 \quad (mod\ p)$

$m_2 = q \ , \ M_2 = p$

$M_2 M_2' \equiv p M_2' \equiv 1 \quad (mod\ q)$

によって定められる数とし

$a_0 = M_1 M_1' g_p^{2C_2'+1} + M_2 M_2' g_q^{2D_2'}$

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

$a \equiv a_0 \quad (mod\ pq) \qquad (a = p + q)$

$$a \equiv M_1 M_1' g_p^{2C_2'+1} + M_2 M_2' g_q^{2D_2'} \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv M_1 M_1' g_p^{2C_2'+1} + M_2 M_2' g_q^{2D_2'} \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv qM_1' g_p^{2C_2'+1} + pM_2' g_q^{2D_2'} \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv (1+ap) g_p^{2C_2'+1} + (1+bq) g_q^{2D_2'} \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv g_p^{2C_2'+1} + apg_p^{2C_2'+1} + g_q^{2D_2'} + bqg_q^{2D_2'} \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv g_p^{2C_2'+1} + ag_p^{2C_2'+1} p + g_q^{2D_2'} + bg_q^{2D_2'} q \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv g_p^{2C_2'+1} + (aq+np)p + g_q^{2D_2'} + (bp+mq)q \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv g_p^{2C_2'+1} + apq + np^2 + g_q^{2D_2'} + bpq + mq^2 \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv g_p^{2C_2'+1} + np^2 + g_q^{2D_2'} + mq^2 \quad (mod\ pq)$$

$$\therefore \qquad p+q \equiv np^2 + mq^2 + g_p^{2C_1'+1} + g_q^{2D_2'} \quad (mod\ pq)$$

この時上記の命題は

$$p+q \equiv np^2 + mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \quad (mod\ p) \quad \text{⑦}$$

かつ

$$p+q \equiv np^2 + mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \quad (mod\ q) \quad \text{⑧}$$

と同値である。

⑦ の時

$$p+q \equiv np^2 + mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \quad (mod\ p)$$

$$q \equiv mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \quad (mod\ p)$$

$$g_p^{2C_2'+1} \equiv mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \quad (mod\ p)$$

$g_p^{2C_2'+1} \equiv mqq + g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{p}$

$0 \equiv mg_p^{2C_2'+1}q + g_q^{2D_2'} \pmod{p}$

$mg_p^{2C_2'+1}q + g_q^{2D_2'} \equiv 0 \pmod{p}$

$mg_p^{2C_2'+1}q \equiv -g_q^{2D_2'} \pmod{p}$

$mg_p^{2C_2'+1}q^2 \equiv -g_q^{2D_2'}q \pmod{pq}$ __⑦'

⑧ の時

$p + q \equiv np^2 + mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{q}$

$p \equiv np^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{q}$

$p \equiv npp + g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{q}$

$g_q^{2D_2'} \equiv ng_q^{2D_2'}p + g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{q}$

$0 \equiv ng_q^{2D_2'}p + g_p^{2C_2'+1} \pmod{q}$

$ng_q^{2D_2'}p + g_p^{2C_2'+1} \equiv 0 \pmod{q}$

$ng_q^{2D_2'}p \equiv -g_p^{2C_2'+1} \pmod{q}$

$ng_q^{2D_2'}p^2 \equiv -g_p^{2C_2'+1}p \pmod{pq}$ __⑧'

また、$p + q \equiv np^2 + mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{pq}$ である時

$g_p^{2C_2'+1}g_q^{2D_2'}$を両辺に掛けて

$$g_p^{2C_2'+1}g_q^{2D_2'}(p + q) \equiv g_p^{2C_2'+1}g_q^{2D_2'}(np^2 + mq^2 + g_p^{2C_2'+1} + g_q^{2D_2'}) \pmod{pq}$$

$$g_p^{2C_2'+1}g_q^{2D_2'}p + g_p^{2C_2'+1}g_q^{2D_2'}q$$

$$\equiv g_p^{2C_2'+1}g_q^{2D_2'}np^2 + g_p^{2C_2'+1}g_q^{2D_2'}mq^2 + g_p^{2C_2'+1}g_q^{2D_2'}g_p^{2C_2'+1} + g_p^{2C_2'+1}g_q^{2D_2'}g_q^{2D_2'} \quad (mod\ pq)$$

$$g_p^{2C_2'+1}g_q^{2D_2'}p + g_p^{2C_2'+1}g_q^{2D_2'}q$$

$$\equiv g_p^{2C_2'+1}(g_q^{2D_2'}np^2) + g_q^{2D_2'}(g_p^{2C_1'+1}mq^2) + g_p^{4C_2'+2}g_q^{2D_2'} + g_p^{2C_2'+1}g_q^{4D_2'} \quad (mod\ pq)$$

この時 ⑦' ⑧'より

$$g_p^{2C_2'+1}g_q^{2D_2'}p + g_p^{2C_2'+1}g_q^{2D_2'}q$$

$$\equiv g_p^{2C_2'+1}(-g_p^{2C_2'+1}p) + g_q^{2D_2'}(-g_q^{2D_2'}q) + g_p^{4C_2'+2}g_q^{2D_2'} + g_p^{2C_2'+1}g_q^{4D_2'} \quad (mod\ pq)$$

$$g_p^{2C_2'+1}g_q^{2D_2'}p + g_p^{2C_2'+1}g_q^{2D_2'}q + g_p^{2C_2'+1}(g_p^{2C_2'+1}p) + g_q^{2D_2'}(g_q^{2D_2'}q)$$

$$\equiv g_p^{4C_2'+2}g_q^{2D_2'} + g_p^{2C_2'+1}g_q^{4D_2'} \quad (mod\ pq)$$

$$g_p^{2C_2'+1}g_q^{2D_2'}p + g_p^{2C_2'+1}g_q^{2D_2'}q + g_p^{4C_2'+2}p + g_q^{4D_2'}q \equiv g_p^{4C_2'+2}g_q^{2D_2'} + g_p^{2C_2'+1}g_q^{4D_2'}(mod\ pq)$$

$$g_p^{4C_2'+2}p + g_p^{2C_2'+1}g_q^{2D_2'}p + g_p^{2C_2'+1}g_q^{2D_2'}q + g_q^{4D_2'}q \equiv g_p^{4C_2'+2}g_q^{2D_2'} + g_p^{2C_2'+1}g_q^{4D_2'} \quad (mod\ pq)$$

$$g_p^{2C_2'+1}(g_p^{2C_2'+1} + g_q^{2D_2'})p + g_q^{2D_2'}(g_p^{2C_2'+1} + g_q^{2D_2'})q \equiv g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1} + g_q^{2D_2'}\right)(mod\ pq)$$

___※3

又、$q \equiv g_p^{2C_2'+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2'} (mod\ q)$　である時

$-q \equiv -g_p^{2C_2'+1} \ (mod\ p)$　かつ　$p \equiv g_q^{2D_2'} \ (mod\ q)$

$p - q \equiv -g_p^{2C_2'+1} \ (mod\ p)$　かつ　$p - q \equiv g_q^{2D_2'} \ (mod\ q)$ ＿※ であるから

$M_s M_s'$ を条件

$pq = M_s m_s$

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

$M_s M_s' \equiv 1 \ (mod\ m_s)$

$m_1 = p\ ,\ M_1 = q$

$M_1 M_1' \equiv q M_1' \equiv 1 \quad (mod\ p)$

$m_2 = q\ ,\ M_2 = p$

$M_2 M_2' \equiv p M_2' \equiv 1 \quad (mod\ q)$

によって定められる数とし
$b_0 = -M_1 M_1' g_p^{2C_2'+1} + M_2 M_2' g_q^{2D_2'}$
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

$b \equiv b_0 \quad (mod\ pq) \qquad (b = p - q)$

$b \equiv -M_1 M_1' g_p^{2C_2'+1} + M_2 M_2' g_q^{2D_2'} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -M_1 M_1' g_p^{2C_2'+1} + M_2 M_2' g_q^{2D_2'} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -q M_1' g_p^{2C_2'+1} + p M_2' g_q^{2D_2'} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -(1 + ap) g_p^{2C_2'+1} + (1 + bq) g_q^{2D_2'} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -g_p^{2C_2'+1} - apg_p^{2C_2'+1} + g_q^{2D_2'} + bqg_q^{2D_2'} \quad (mod\ pq)$

$\therefore \quad p - q \equiv -g_p^{2C_2'+1} - ag_p^{2C_2'+1} p + g_q^{2D_2'} + bg_q^{2D_2'} q \quad (mod\ pq)$

$\therefore \quad p - q \equiv -g_p^{2C_2'+1} - (aq + np)p + g_q^{2D_2'} + (bp + mq)q \quad (mod\ pq)$

$$\therefore \quad p-q \equiv -g_p^{2C_2'+1} - apq - np^2 + g_q^{2D_2'} + bpq + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -g_p^{2C_2'+1} - np^2 + g_q^{2D_2'} + mq^2 \pmod{pq}$$

$$\therefore \quad p-q \equiv -np^2 + mq^2 - g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{pq}$$

また、$p-q \equiv -np^2 + mq^2 - g_p^{2C_2'+1} + g_q^{2D_2'} \pmod{pq}$ である時

$g_p^{2C_2'+1} g_q^{2D_2'}$ を両辺に掛けて

$$g_p^{2C_2'+1} g_q^{2D_2'}(p-q) \equiv g_p^{2C_2'+1} g_q^{2D_2'}(-np^2 + mq^2 - g_p^{2C_2'+1} + g_q^{2D_2'}) \pmod{pq}$$

$$g_p^{2C_2'+1} g_q^{2D_2'} p - g_p^{2C_2'+1} g_q^{2D_2'} q$$
$$\equiv -g_p^{2C_2'+1} g_q^{2D_2'} np^2 + g_p^{2C_2'+1} g_q^{2D_2'} mq^2 - g_p^{2C_2'+1} g_q^{2D_2'} g_p^{2C_2'+1} + g_p^{2C_2'+1} g_q^{2D_2'} g_q^{2D_2'} \pmod{pq}$$

$$g_p^{2C_2'+1} g_q^{2D_2'} p - g_p^{2C_2'+1} g_q^{2D_2'} q$$
$$\equiv -g_p^{2C_2'+1} \left(g_q^{2D_2'} np^2\right) + g_q^{2D_2'} \left(g_p^{2C_2'+1} mq^2\right) - g_p^{4C_2'+2} g_q^{2D_2'} + g_p^{2C_2'+1} g_q^{4D_2'} \pmod{pq}$$

この時 ⑦' ⑧'より

$$g_p^{2C_2'+1} g_q^{2D_2'} p - g_p^{2C_2'+1} g_q^{2D_2'} q$$
$$\equiv -g_p^{2C_2'+1} \left(-g_p^{2C_2'+1} p\right) + g_q^{2D_2'} \left(-g_q^{2D_2'} q\right) - g_p^{4C_2'+2} g_q^{2D_2'} + g_p^{2C_2'+1} g_q^{4D_2'} \pmod{pq}$$

$$g_p^{2C_2'+1} g_q^{2D_2'} p - g_p^{2C_2'+1} g_q^{2D_2'} q - g_p^{2C_2'+1} \left(g_p^{2C_2'+1} p\right) + g_q^{2D_2'} \left(g_q^{2D_2'} q\right)$$
$$\equiv -g_p^{4C_2'+2} g_q^{2D_2'} + g_p^{2C_2'+1} g_q^{4D_2'} \pmod{pq}$$

$$g_p^{2C_2'+1} g_q^{2D_2'} p - g_p^{2C_2'+1} g_q^{2D_2'} q - g_p^{4C_2'+2} p + g_q^{4D_2'} q \equiv -g_p^{4C_2'+2} g_q^{2D_2'} + g_p^{2C_2'+1} g_q^{4D_2'} \pmod{pq}$$

$$-g_p^{4C_2'+2} p + g_p^{2C_2'+1} g_q^{2D_2'} p - g_p^{2C_2'+1} g_q^{2D_2'} q + g_q^{4D_2'} q \equiv -g_p^{4C_2'+2} g_q^{2D_2'} + g_p^{2C_2'+1} g_q^{4D_2'} \pmod{pq}$$

$$g_p^{2C_2'+1}\left(g_q^{2D_2'}-g_p^{2C_2'+1}\right)p+g_q^{2D_2'}\left(g_q^{2D_2'}-g_p^{2C_2'+1}\right)q\equiv g_p^{2C_2'+1}g_q^{2D_2'}\left(g_q^{2D_2'}-g_p^{2C_2'+1}\right)\quad(mod\ pq)$$

$$-g_p^{2C_2'+1}(g_p^{2C_2'+1}-g_q^{2D_2'})p-g_q^{2D_2'}(g_p^{2C_2'+1}-g_q^{2D_2'})q\equiv -g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}-g_q^{2D_2'}\right)\quad(mod\ pq)$$

$$g_p^{2C_2'+1}(g_p^{2C_2'+1}-g_q^{2D_2'})p+g_q^{2D_2'}(g_p^{2C_2'+1}-g_q^{2D_2'})q\equiv g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}-g_q^{2D_2'}\right)\quad(mod\ pq)$$

____※$_4$

この時 ※$_3$＋※$_4$ より

$$g_p^{2C_2'+1}(g_p^{2C_2'+1}+g_q^{2D_2'})p+g_q^{2D_2'}(g_p^{2C_2'+1}+g_q^{2D_2'})q$$
$$+g_p^{2C_2'+1}(g_p^{2C_2'+1}-g_q^{2D_2'})p+g_q^{2D_2'}(g_p^{2C_2'+1}-g_q^{2D_2'})q$$
$$\equiv g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}+g_q^{2D_2'}\right)+g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}-g_q^{2D_2'}\right) \quad (mod\ pq)$$

$$g_p^{2C_2'+1}(g_p^{2C_2'+1}+g_q^{2D_2'})p+g_p^{2C_2'+1}(g_p^{2C_2'+1}-g_q^{2D_2'})p$$
$$+g_q^{2D_2'}(g_p^{2C_2'+1}+g_q^{2D_2'})q+g_q^{2D_2'}(g_p^{2C_2'+1}-g_q^{2D_2'})q$$
$$\equiv g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}+g_q^{2D_2'}\right)+g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}-g_q^{2D_2'}\right) \quad (mod\ pq)$$

$$g_p^{2C_2'+1}(g_p^{2C_2'+1}+g_q^{2D_2'}+g_p^{2C_2'+1}-g_q^{2D_2'})p+g_q^{2D_2'}\left(g_p^{2C_2'+1}+g_q^{2D_2'}+g_p^{2C_2'+1}-g_q^{2D_2'}\right)$$
$$\equiv g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}+g_q^{2D_2'}+g_p^{2C_2'+1}-g_q^{2D_2'}\right) \quad (mod\ pq)$$

$$g_p^{2C_2'+1}\left(g_p^{2C_2'+1}+g_p^{2C_2'+1}\right)p+g_q^{2D_2'}\left(g_p^{2C_2'+1}+g_p^{2C_2'+1}\right)$$
$$\equiv g_p^{2C_2'+1}g_q^{2D_2'}\left(g_p^{2C_2'+1}+g_p^{2C_2'+1}\right) \quad (mod\ pq)$$

$$g_p^{2C_2'+1}p\times 2g_p^{2C_2'+1}+g_q^{2D_2'}q\times 2g_p^{2C_2'+1}\equiv g_p^{2C_2'+1}g_q^{2D_2'}\times 2g_p^{2C_2'+1} \quad (mod\ pq)$$

この時 $(2,pq)=1$ より両辺を 2 で割って

$$g_p^{2C_2'+1}p\times g_p^{2C_2'+1}+g_q^{2D_2'}q\times g_p^{2C_2'+1}\equiv g_p^{2C_2'+1}g_q^{2D_2'}\times g_p^{2C_2'+1} \quad (mod\ pq)$$

$$\therefore g_p^{4C_2'+2}p+g_q^{2D_2'}g_p^{2C_2'+1}q\equiv g_p^{4C_2'+2}g_q^{2D_2'} \quad (mod\ pq)$$

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

$$\therefore \left(g_p^{2C_2'+1},pq\right)=1$$

従って両辺を $g_p^{2c_2'+1}$ で割って

$$g_p^{2C_2'+1}p + g_q^{2D_2'}q \equiv g_p^{2C_2'+1}g_q^{2D_2'} \quad (mod\ pq)$$

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

$$g_p^{2C_2'+1} p + g_q^{2D_2'} q \equiv g_p^{2C_2'+1} g_q^{2D_2'} \quad (mod\ pq)$$

$$\Rightarrow \quad q \equiv g_p^{2C_2'+1}\ (mod\ p) \quad \text{かつ} \quad p \equiv g_q^{2D_2'}\ (mod\ q)$$

∵

$g_p^{2C_2'+1} p + g_q^{2D_2'} q \equiv g_p^{2C_2'+1} g_q^{2D_2'}$　$(mod\ pq)$　の時

上記の方程式は

$$g_p^{2C_2'+1} p + g_q^{2D_2'} q \equiv g_p^{2C_2'+1} g_q^{2D_2'} \quad (mod\ p)$$

かつ

$$g_p^{2C_2'+1} p + g_q^{2D_2'} q \equiv g_p^{2C_2'+1} g_q^{2D_2'} \quad (mod\ q)$$

と同値である。

又、上記の方程式は

$$g_q^{2D_2'} q \equiv g_p^{2C_2'+1} g_q^{2D_2'} \quad (mod\ p)$$

かつ

$$g_p^{2C_2'+1} p \equiv g_p^{2C_2'+1} g_q^{2D_2'} \quad (mod\ q) \quad \text{\_\_\_\_☆}_3$$

と同値である。

この時 $(g_q, p) = 1$　より　$\left(g_q^{2D_2'}, p\right) = 1$

又、$(g_p, q) = 1$　より　$\left(g_p^{2C_2'+1}, q\right) = 1$

従って、上記の方程式の両辺を $g_q^{2D_2'}$, $g_p^{2C_2'+1}$ でそれぞれ割って

$$q \equiv g_p^{2C_2'+1} \quad (mod\ p)$$

かつ

$p \equiv g_q^{2D_2'} \pmod{q}$ ＿＿＿☆$_4$

この時、☆$_4$の方程式のそれぞれに $g_q^{2D_2'}$，$g_p^{2C_2'+1}$ を掛け合わせると

☆$_3$の方程式へと戻るため☆$_3$の方程式と☆$_4$の方程式は同値である。

以上より、上記の命題が成立する。