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である場合の証明】

$\left(\frac{q}{p}\right)=1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv 1\,(mod\ p)$　の証明

Ⅰ．　$\left(\frac{q}{p}\right)=1 \quad \Rightarrow \quad q^{\frac{p-1}{2}} \equiv 1\,(mod\ p)$

$\because$

$\left(\frac{q}{p}\right)=1$ の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$1 \equiv q^{\frac{p-1}{2}}\ (mod\ p)$

$\therefore\ q^{\frac{p-1}{2}} \equiv 1\,(mod\ p)$

Ⅱ．　$q^{\frac{p-1}{2}} \equiv 1\,(mod\ p) \quad \Rightarrow \quad \left(\frac{q}{p}\right)=1$

$\because$

$q^{\frac{p-1}{2}} \equiv 1\,(mod\ p)$ の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$\left(\frac{q}{p}\right) \equiv 1\ (mod\ p)$

$\therefore\ \left(\frac{q}{p}\right)=1+pe_1$　　（e_1は整数）

この時

$\left(\frac{q}{p}\right)$ は１か－１である。

$\therefore\ \left(\frac{q}{p}\right)=-1$ と仮定すると

$-1=1+pe_1$

$\therefore\ -2=pe_1$

$\therefore\ 2=p(-e_1)$

$\therefore$ ２は p の倍数

$\therefore \quad (2, p) = p$

しかし p は奇素数より矛盾。

$\therefore \left(\frac{q}{p}\right) = 1$

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

$\left(\frac{q}{p}\right) = 1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$

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

Ⅰ．　$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$　　$\Rightarrow$　$ind\ q \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots,p-3\ (mod\ p-1)$

$\because$

$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ ＿①　の時

$\left(\frac{p-1}{2}\ ,\ \varphi(p)\right) = \left(\frac{p-1}{2}\ ,\ p-1\right)$

$= \frac{p-1}{2}$

であるから、①の合同式が解けるのは $ind\ 1$ が $\frac{p-1}{2}$ の倍数である場合、かつ、
その場合に限る。

実際、合同式①は
$\frac{p-1}{2}\ ind\ q\ \equiv ind\ 1\ (mod\ p-1)$
と同値である。

この時
$ind\ 1 = \eta_1$ と置くと
$1 \equiv g_p^{\eta_1}\ (mod\ p)$
$\therefore\ \eta_1 = 0$
$\therefore\ ind\ 1 = 0$ より

$\frac{p-1}{2}\ ind\ q\ \equiv 0\ (mod\ p-1)$＿②

この時 $\frac{p-1}{2}$ は p の値が $4m_1+1\ ,4m_1+3$ のどちらであったとしても整数である。

又、$\left(\frac{p-1}{2}\ ,p-1\right) = \left(\frac{p-1}{2}\ ,2\left(\frac{p-1}{2}\right)\right)$

$= \frac{p-1}{2}\ (\ 1\ ,2\ )$
$= \frac{P-1}{2}$

であり、0 は $\frac{p-1}{2}$ の倍数である。
従って、②の合同式は $\frac{p-1}{2}$ 個の解を持つ。

両辺と法を $\frac{p-1}{2}$ で割ると
$ind\ q\ \equiv 0\ (mod\ 2\ )$

$\therefore \quad ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, 0 + 2\left(\frac{p-1}{2} - 1\right) \quad (mod\ p-1)$

$\therefore \quad ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3 \quad (mod\ p-1)$

Ⅱ. $ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3\ (mod\ p-1) \quad \Rightarrow \quad q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$

$\because$

$ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3\ (mod\ p-1)$ の時
これらの値は、合同式 $\frac{p-1}{2}\ ind\ q \equiv 0\ (mod\ p-1)$の解である。

従って、
$ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3\ (mod\ p-1)$ の時
$\frac{p-1}{2}\ ind\ q \equiv 0\ (mod\ p-1)$ は成り立つ。

又、$\frac{p-1}{2}\ ind\ q \equiv 0\ (mod\ p-1)$ は

$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1) \quad \Leftrightarrow \quad q \equiv g_p^{2C_1}\ (mod\ p)$ の証明

$(\ 2C_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ )$

Ⅰ． $ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1) \quad \Rightarrow \quad q \equiv g_p^{2C_1}\ (mod\ p)$

$(\ 2C_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ )$

$\because$

$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1)$ の時

$2C_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3$ と置くと

$ind\ q \equiv 2C_1\ (mod\ p-1)$

この時、$ind\ q = \eta_2$ と置くと

$q \equiv g_p^{\eta_2}\ (mod\ p)$

又、 $\eta_2 \equiv 2C_1\ (mod\ p-1)$より

$\eta_2 = 2C_1 + (p-1)\ e_2$ （e_2は整数）

$\therefore \quad q \equiv g_p^{\eta_2}(mod\ p)$

$\equiv g_p^{2C_1+(p-1)e_2}\ (mod\ p)$

この時 g_pは法 pの原始根より

g_pは pで割り切れない。

従って、フェルマーの小定理より

$g_p^{p-1} \equiv 1\ (mod\ p)$

$\therefore \quad q \equiv g_p^{2C_1}\left(g_p^{p-1}\right)^{e_2}\ (mod\ p)$

$\equiv g_p^{2C_1}\left(\ 1\ \right)^{e_2}\ (mod\ p)$

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

Ⅱ．　$q \equiv g_p^{2C_1} \ (mod\ p)$　　⇒　$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\cdots\cdots,p-3\ (mod\ p-1)$

$(\ 2C_1 = 0\,,2\,,4\,,6\,,8\,,\cdots\cdots,p-3\ )$

$\because$

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

$2C_1 = ind\ q$

又、$2C_1 \equiv 2C_1 \ (mod\ p-1)$

$\therefore$　$ind\ q \equiv 2C_1 \ (mod\ p-1)$

$\therefore$　$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\cdots\cdots,p-3\ (mod\ p-1)$

従ってⅠ,Ⅱより

$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\cdots\cdots,p-3\ (mod\ p-1)$　⇔　$q \equiv g_p^{2C_1} \ (mod\ p)$

$(\ 2C_1 = 0\,,2\,,4\,,6\,,8\,,\cdots\cdots,p-3\ )$

$\left(\frac{p}{q}\right)=1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$ の証明

Ⅰ. $\left(\frac{p}{q}\right)=1 \quad \Rightarrow \quad p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$

$\because$

$\left(\frac{p}{q}\right)=1$ の時

$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}}\ (mod\ q)$ より

$1 \equiv p^{\frac{q-1}{2}}\ (mod\ q)$

$\therefore\ p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$

Ⅱ. $p^{\frac{q-1}{2}} \equiv 1\ (mod\ q) \quad \Rightarrow \quad \left(\frac{p}{q}\right)=1$

$\because$

$p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$ の時

$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}}\ (mod\ q)$ より

$\left(\frac{p}{q}\right) \equiv -1\ (mod\ q)$

$\therefore\ \left(\frac{p}{q}\right)=1+qf_1$ （f_1は整数）

この時

$\left(\frac{p}{q}\right)$ は 1 か－ 1 である。

$\therefore\ \left(\frac{p}{q}\right)=1$ と仮定すると

$-1=1+qf_1$

$\therefore\ -2=qf_1$

$\therefore\ 2=q(-f_1)$

$\therefore$ 2 は q の倍数

$\therefore\ \ (2,q)=q$

しかし q は奇素数より矛盾。

$\therefore \left(\frac{p}{q}\right) = 1$

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

$\left(\frac{p}{q}\right) = 1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv 1 \ (mod\ q)$

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

Ⅰ． $p^{\frac{q-1}{2}} \equiv 1\ (mod\ q) \quad \Rightarrow \quad ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$

$\because$

$p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$ _③ の時

$\left(\frac{q-1}{2}\ ,\ \varphi(q)\right) = \left(\frac{q-1}{2}\ ,\ q-1\right)$

$= \frac{q-1}{2}$

であるから、③の合同式が解けるのは $ind\ 1$ が $\frac{q-1}{2}$ の倍数である場合、かつ、
その場合に限る。

実際、合同式③は
$\frac{q-1}{2}\ ind\ p\ \equiv ind\ 1\ (mod\ q-1)$
と同値である。

この時
$ind\ 1 = \theta_1$ と置くと
$1 \equiv g_q^{\theta_1}\ (mod\ q)$
$\therefore\ \theta_1\ = 0$
$\therefore\ ind\ 1 = 0$ より

$\frac{q-1}{2}\ ind\ p\ \equiv 0\ (mod\ q-1)$__④

この時 $\frac{q-1}{2}$ は q の値が $4m_2+1\,,4m_2+3$ のどちらであったとしても整数である。

又、$\left(\frac{q-1}{2}\,,q-1\right) = \left(\frac{q-1}{2}\,,2\left(\frac{q-1}{2}\right)\right)$

$= \frac{q-1}{2}\,(\,1\,,2\,)$

$= \frac{q-1}{2}$

であり、0 は $\frac{q-1}{2}$ の倍数である。
従って、④の合同式は $\frac{q-1}{2}$ 個の解を持つ。

両辺と法を $\frac{q-1}{2}$ で割ると
$ind\ p\ \equiv 0\ (mod\ 2\,)$

$\therefore \quad ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, 0 + 2\left(\frac{q-1}{2} - 1\right) \quad (mod\ q-1)$

$\therefore \quad ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3 \quad (mod\ q-1)$

Ⅱ. $\quad ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3\ (mod\ q-1) \quad \Rightarrow \quad p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$

$\because$

$ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3\ (mod\ q-1)$ の時
これらの値は、合同式 $\frac{q-1}{2}\ ind\, p \equiv 0\ (mod\ q-1)$の解である。

従って、
$ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3\ (mod\ q-1)$ の時
$\frac{q-1}{2}\ ind\, p \equiv 0\ (mod\ q-1)$ は成り立つ。

又、$\frac{q-1}{2}\ ind\, p \equiv 0\ (mod\ q-1)$ は

$p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ q-1) \quad \Leftrightarrow \quad p \equiv g_q^{2D_1}\ (mod\ q)$　　の証明

$(\ 2D_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ )$

Ⅰ．　$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ q-1) \quad \Rightarrow \quad p \equiv g_q^{2D_1}\ (mod\ q)$

$(\ 2D_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ )$

$\because$

$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$ の時

$2D_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3$ と置くと

$ind\ p \equiv 2D_1\ (mod\ q-1)$

この時、$ind\ p = \theta_2$ と置くと

$p \equiv g_q^{\theta_2}\ (mod\ q)$

又、 $\theta_2 \equiv 2D_1\ (mod\ q-1)$より

$\theta_2 = 2D_1 + (q-1)\,f_2$　　（f_2は整数）

$\therefore \quad p \equiv g_q^{\theta_2}(mod\ q)$

$\equiv g_q^{2D_1+(q-1)f_2}\ (mod\ q)$

この時 g_qは法 qの原始根より

g_qは qで割り切れない。

従って、フェルマーの小定理より

$g_q^{q-1} \equiv 1\ (mod\ q)$

$\therefore \quad p \equiv g_q^{2D_1}\left(g_q^{q-1}\right)^{f_2}\ (mod\ q)$

$\equiv g_p^{2D_1}\left(1\right)^{f_2}\ (mod\ q)$

$\equiv g_q^{2D_1}\ (mod\ q)$

Ⅱ．　$p \equiv g_q^{2D_1} \ (mod\ q)$　　⇒　　$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$

$(\ 2D_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ )$

∵

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

$2D_1 = ind\ p$

又、$2D_1 \equiv 2D_1 \ (mod\ q-1)$

∴　$ind\ p \equiv 2D_1 \ (mod\ q-1)$

∴　$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$

従ってⅠ,Ⅱより

$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$　⇔　$p \equiv g_q^{2D_1} \ (mod\ q)$

$(\ 2D_1 = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ )$

【ii である場合の証明】

$\left(\frac{q}{p}\right) = -1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の証明

Ⅰ. $\left(\frac{q}{p}\right) = -1 \quad \Rightarrow \quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

$\because$

$\left(\frac{q}{p}\right) = -1$の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$-1 \equiv q^{\frac{p-1}{2}}\ (mod\ p)$

$\therefore\ q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

Ⅱ. $q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Rightarrow \quad \left(\frac{q}{p}\right) = -1$

$\because$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$\left(\frac{q}{p}\right) \equiv -1 \quad (mod\ p)$

$\therefore\ \left(\frac{q}{p}\right) = -1 + pg_1$ （g_1は整数）

この時

$\left(\frac{q}{p}\right)$ は 1 か－ 1 である。

$\therefore\ \left(\frac{q}{p}\right) = 1$ と仮定すると

$1 = -1 + pg_1$

$\therefore\ 2 = pg_1$

$\therefore$ 2 は p の倍数

$\therefore\ (2, p) = p$

しかし p は奇素数より矛盾。

$\therefore \left(\frac{q}{p}\right) = -1$

以上より上記の命題が成立する。

従ってⅠ, Ⅱより

$\left(\frac{q}{p}\right) = -1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Leftrightarrow \quad ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\dots\dots,p-2\ (mod\ p-1)$ の証明

Ⅰ． $q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Rightarrow \quad ind\ p \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\dots\dots,p-2\ (mod\ q-1)$

$\because$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の時

$q^{\frac{p-1}{2}} \equiv p-1\ (mod\ p)$ ＿⑤

$\left(\frac{p-1}{2}\ ,\ \varphi(p)\right) = \left(\frac{p-1}{2}\ ,\ p-1\right)$

$= \frac{q-1}{2}$

であるから、⑤の合同式が解けるのは $ind\ p-1$ が $\frac{p-1}{2}$ の倍数である場合、かつ、その場合に限る。

実際、合同式⑤は

$\frac{p-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$

と同値である。

この時

$ind\ p-1=\iota_1$ と置くと

$p-1 \equiv g_p^{\iota_1}\ (mod\ p)$

この時 $\iota_1 = \frac{p-1}{2}$ より

$ind\ p-1 = \frac{p-1}{2}$

＿＿※補足参照

$\therefore \quad \frac{p-1}{2}\ ind\ q\ \equiv \frac{p-1}{2}\ (mod\ p-1)$＿⑥

この時 $\frac{p-1}{2}$ は p の値が $4m_1+1\ ,4m_1+3$ のどちらであったとしても整数である。

又、$\left(\frac{p-1}{2}\ ,p-1\right) = \left(\frac{p-1}{2}\ ,2\left(\frac{p-1}{2}\right)\right)$

$= \frac{p-1}{2}\ (\ 1\ ,2\ )$

$= \frac{p-1}{2}$

であり、$\frac{p-1}{2}$ は $\frac{p-1}{2}$ の倍数である。

従って、⑥の合同式は $\frac{p-1}{2}$ 個の解を持つ。

両辺と法を $\frac{p-1}{2}$ で割ると

$ind\ q\ \equiv 1\ (mod\ 2\ )$

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

$\therefore\quad ind\ q\ \equiv 1\ ,\ 3\ ,5\ ,7\ ,9\ ,\ldots\ldots\ ,\ p-2\quad (\ mod\ p-1\ )$

Ⅱ.　$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)\quad \Rightarrow\quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

$\because$

$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)$ の時

これらの値は、合同式 $\frac{q-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$の解である。

従って、

$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)$ の時

$\frac{p-1}{2}\ ind\ q\ \equiv\ ind\ p-1(mod\ p-1)$ は成り立つ。

又、$\frac{p-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$ は

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

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

$(\ 2C_2+1 = 1,3,5,7,9,\ldots\ldots,p-2\ )$

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

$(\ 2C_2+1 = 1,3,5,7,9,\ldots\ldots,p-2\ )$

$\because$

$ind\ q \equiv 1,3,5,7,9,\ldots\ldots,p-2\ (mod\ p-1)$ の時

$2C_2+1 = 1,3,5,7,9,\ldots\ldots,p-2$ と置くと

$ind\ q \equiv 2C_2+1\ (mod\ p-1)$

この時、$ind\ q = \iota_2$ と置くと

$q \equiv g_p^{\iota_2}\ (mod\ p)$

又、 $\iota_2 \equiv 2C_2+1\ (mod\ p-1)$より

$\iota_2 = 2C_2+1+(p-1)\ g_2$　　（g_2は整数）

$\therefore \quad q \equiv g_p^{\iota_2}(mod\ p)$

$\equiv g_p^{2C_2+1+(p-1)g_2}\ (mod\ p)$

この時 g_pは法 pの原始根より

g_pは pで割り切れない。

従って、フェルマーの小定理より

$g_p^{p-1} \equiv 1\ (mod\ p)$

$\therefore \quad q \equiv g_p^{2C_2+1}\left(g_p^{p-1}\right)^{g_2}\ (mod\ p)$

$\equiv g_p^{2C_2+1}\left(1\right)^{g_2}\ (mod\ p)$

$\equiv g_p^{2c_2+1}\ (mod\ p)$

Ⅱ．　$q \equiv g_p^{2C_2+1} \ (mod\ p)$　　⇒　$ind\ q \equiv 1\,,3\,,5\,,7\,,9\,,\cdots\cdots,p-2\ (mod\ p-1)$

$(\ 2C_2+1=1\,,3\,,5\,,7\,,9\,,\cdots\cdots,p-2\,)$

$\because$

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

$2C_2+1=ind\ q$

又、$2C_2+1 \equiv 2C_2+1(mod\ p-1)$

$\therefore$　$ind\ q \equiv 2C_2+1(mod\ p-1)$

$\therefore$　$ind\ q \equiv 1\,,3\,,5\,,7\,,9\,,\cdots\cdots,p-2\ (mod\ p-1)$

従ってⅠ,Ⅱより

$ind\ q \equiv 1\,,3\,,5\,,7\,,9\,,\cdots\cdots,p-2\ (mod\ p-1)$　⇔　$q \equiv g_p^{2C_2+1} \ (mod\ p)$

$(\ 2C_2+1=1\,,3\,,5\,,7\,,9\,,\cdots\cdots,p-2\,)$

$\left(\frac{q}{p}\right) = -1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の証明

Ⅰ. $\left(\frac{q}{p}\right) = -1 \quad \Rightarrow \quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

$\because$

$\left(\frac{q}{p}\right) = -1$の時

$\left(\frac{q}{p}\right) \equiv\ q^{\frac{p-1}{2}}\ (mod\ p)$ より

$-1 \equiv\ q^{\frac{p-1}{2}}\ (mod\ p)$

$\therefore\ q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

Ⅱ. $q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Rightarrow \quad \left(\frac{q}{p}\right) = -1$

$\because$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の時

$\left(\frac{q}{p}\right) \equiv\ q^{\frac{p-1}{2}}\ (mod\ p)$ より

$\left(\frac{q}{p}\right) \equiv -1 \quad (mod\ p)$

$\therefore\ \left(\frac{q}{p}\right) = -1 + ph_1$ （h_1は整数）

この時

$\left(\frac{q}{p}\right)$ は 1 か－ 1 である。

$\therefore\ \left(\frac{q}{p}\right) = 1$ と仮定すると

$1 = -1 + ph_1$

$\therefore\ 2 = ph_1$

$\therefore$ 2 は p の倍数

$\therefore\ (2, p) = p$

しかし p は奇素数より矛盾。

$\therefore\ \left(\frac{q}{p}\right) = -1$

以上より上記の命題が成立する。

従ってⅠ, Ⅱより

$$\left(\frac{q}{p}\right) = -1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Leftrightarrow \quad ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\dots\dots,p-2\ (mod\ p-1)$ の証明

Ⅰ． $q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Rightarrow \quad ind\ p \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\dots\dots,p-2\ (mod\ q-1)$

$\because$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の時

$q^{\frac{p-1}{2}} \equiv p-1\ (mod\ p)$ ＿⑦

$\left(\frac{p-1}{2}\ ,\ \varphi(p)\right) = \left(\frac{p-1}{2}\ ,\ p-1\right)$

$= \frac{q-1}{2}$

であるから、⑦の合同式が解けるのは $ind\ p-1$ が $\frac{p-1}{2}$ の倍数である場合、かつ、その場合に限る。

実際、合同式⑦は

$\frac{p-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$

と同値である。

この時

$ind\ q-1=\kappa_1$ と置くと

$p-1 \equiv g_p^{\kappa_1}\ (mod\ p)$

この時 $\kappa_1 = \frac{p-1}{2}$ より

$ind\ p-1 = \frac{p-1}{2}$

＿＿※補足参照

$\therefore \quad \frac{p-1}{2}\ ind\ q\ \equiv \frac{p-1}{2}\ (mod\ p-1)$＿⑧

この時 $\frac{p-1}{2}$ は p の値が $4m_1+1\ ,4m_1+3$ のどちらであったとしても整数である。

又、$\left(\frac{p-1}{2}\ ,p-1\right) = \left(\frac{p-1}{2}\ ,2\left(\frac{p-1}{2}\right)\right)$

$= \frac{p-1}{2}\ (\ 1\ ,2\ )$

$= \frac{p-1}{2}$

であり、$\frac{p-1}{2}$ は $\frac{p-1}{2}$ の倍数である。

従って、⑧の合同式は $\frac{p-1}{2}$ 個の解を持つ。

両辺と法を $\frac{p-1}{2}$ で割ると

$ind\ q\ \equiv 1\ (mod\ 2\ )$

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

$\therefore\quad ind\ q\ \equiv 1\ ,\ 3\ ,5\ ,7\ ,9\ ,\ldots\ldots\ ,\ p-2\quad (\ mod\ p-1\ )$

Ⅱ.　$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)\quad \Rightarrow\quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

$\because$

$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)$ の時

これらの値は、合同式 $\frac{q-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$の解である。

従って、

$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)$ の時

$\frac{p-1}{2}\ ind\ q\ \equiv\ ind\ p-1(mod\ p-1)$ は成り立つ。

又、$\frac{p-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$ は

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

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

$(\ 2D_2+1 = 1,3,5,7,9,\ldots\ldots,p-2\ )$

Ⅰ. $ind\ q \equiv 1,3,5,7,9,\ldots\ldots,p-2\ (mod\ p-1) \quad \Rightarrow \quad q \equiv g_p^{2D_2+1}\ (mod\ p)$

$(\ 2D_2+1 = 1,3,5,7,9,\ldots\ldots,p-2\ )$

$\because$

$ind\ q \equiv 1,3,5,7,9,\ldots\ldots,p-2\ (mod\ p-1)$ の時

$2D_2+1 = 1,3,5,7,9,\ldots\ldots,p-2$ と置くと

$ind\ q \equiv 2D_2+1\ (mod\ p-1)$

この時、$ind\ q = \kappa_2$ と置くと

$q \equiv g_p^{\kappa_2}\ (mod\ p)$

又、 $\kappa_2 \equiv 2D_2+1\ (mod\ p-1)$より

$\kappa_2 = 2D_2+1+(p-1)\ h_2$ （h_2は整数）

$\therefore \quad q \equiv g_p^{\kappa_2}(mod\ p)$

$\equiv g_p^{2D_2+1+(p-1)h_2}\ (mod\ p)$

この時 g_pは法 pの原始根より

g_pは pで割り切れない。

従って、フェルマーの小定理より

$g_p^{p-1} \equiv 1\ (mod\ p)$

$\therefore \quad q \equiv g_p^{2D_2+1}\left(g_p^{p-1}\right)^{h_2}\ (mod\ p)$

$\equiv g_p^{2D_2+1}\left(1\right)^{h_2}\ (mod\ p)$

$\equiv g_p^{2D_2+1}\ (mod\ p)$

Ⅱ．　$q \equiv g_p^{2D_2+1} \ (mod\ p)$　　⇒　$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\cdots\cdots,p-2\ (mod\ p-1)$

$(\ 2D_2+1=1\ ,3\ ,5\ ,7\ ,9\ ,\cdots\cdots,p-2\ )$

$\because$

$q \equiv g_p^{2D_2+1} \ (mod\ p)$（$2D_2+1=1\ ,3\ ,5\ ,7\ ,9\ ,\cdots\cdots,p-2$）の時

$2D_2+1=ind\ q$

又、$2D_2+1 \equiv 2D_2+1(mod\ p-1)$

$\therefore$　$ind\ q \equiv 2D_2+1(mod\ p-1)$

$\therefore$　$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\cdots\cdots,p-2\ (mod\ p-1)$

従ってⅠ,Ⅱより

$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\cdots\cdots,p-2\ (mod\ p-1)$　⇔　$q \equiv g_p^{2D_2+1} \ (mod\ p)$

$(\ 2D_2+1=1\ ,3\ ,5\ ,7\ ,9\ ,\cdots\cdots,p-2\ )$

【ⅲである場合の証明】

$\left(\frac{q}{p}\right)=1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$　の証明

Ⅰ．　$\left(\frac{q}{p}\right)=1 \quad \Rightarrow \quad q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$

$\because$

$\left(\frac{q}{p}\right)=1$ の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$1 \equiv q^{\frac{p-1}{2}}\ (mod\ p)$

$\therefore\ q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$

Ⅱ．　$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p) \quad \Rightarrow \quad \left(\frac{q}{p}\right)=1$

$\because$

$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$\left(\frac{q}{p}\right) \equiv 1\ (mod\ p)$

$\therefore\ \left(\frac{q}{p}\right)=1+ps_1$　　（s_1は整数）

この時

$\left(\frac{q}{p}\right)$ は 1 か－ 1 である。

$\therefore\ \left(\frac{q}{p}\right)=-1$ と仮定すると

$-1=1+ps_1$

$\therefore\ -2=ps_1$

$\therefore\ 2=p(-s_1)$

$\therefore$ 2 は p の倍数

$\therefore \quad (2, p) = p$

しかし p は奇素数より矛盾。

$\therefore \left(\frac{q}{p}\right) = 1$

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

$\left(\frac{q}{p}\right) = 1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$

$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$　　⇔　$ind\ q \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots,p-3\ (mod\ p-1)$　の証明

Ⅰ．　$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$　　⇒　$ind\ q \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots,p-3\ (mod\ p-1)$

∵

$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ __①　の時

$\left(\frac{p-1}{2}\ ,\ \varphi(p)\right) = \left(\frac{p-1}{2}\ ,\ p-1\right)$

$= \frac{p-1}{2}$

であるから、①の合同式が解けるのは $ind\ 1$ が $\frac{p-1}{2}$ の倍数である場合、かつ、
その場合に限る。

実際、合同式①は
$\frac{p-1}{2}\ ind\ q\ \equiv ind\ 1\ (mod\ p-1)$
と同値である。

この時
$ind\ 1 = \eta_1'$ と置くと
$1 \equiv g_p^{\eta_1'}\ (mod\ p)$
$\therefore\ \eta_1' = 0$
$\therefore\ ind\ 1 = 0$ より

$\frac{p-1}{2}\ ind\ q\ \equiv 0\ (mod\ p-1)$__②

この時 $\frac{p-1}{2}$ は p の値が $4m_1+1\ ,4m_1+3$ のどちらであったとしても整数である。

又、$\left(\frac{p-1}{2}\ ,p-1\right) = \left(\frac{p-1}{2}\ ,2\left(\frac{p-1}{2}\right)\right)$

$= \frac{p-1}{2}\ (1\ ,2\ )$

$= \frac{P-1}{2}$

であり、0 は $\frac{p-1}{2}$ の倍数である。
従って、②の合同式は $\frac{p-1}{2}$ 個の解を持つ。

両辺と法を $\frac{p-1}{2}$ で割ると
$ind\ q\ \equiv 0\ (mod\ 2\ )$

$\therefore \quad ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, 0 + 2\left(\frac{p-1}{2} - 1\right) \quad (mod\ p-1)$

$\therefore \quad ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3 \quad (mod\ p-1)$

Ⅱ. $ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3\ (mod\ p-1) \quad \Rightarrow \quad q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$

$\because$

$ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3\ (mod\ p-1)$ の時
これらの値は、合同式 $\frac{p-1}{2}\ ind\ q \equiv 0\ (mod\ p-1)$の解である。

従って、
$ind\ q \equiv 0, 2, 4, 6, 8, \cdots\cdots, p-3\ (mod\ p-1)$ の時
$\frac{p-1}{2}\ ind\ q \equiv 0\ (mod\ p-1)$ は成り立つ。

又、$\frac{p-1}{2}\ ind\ q \equiv 0\ (mod\ p-1)$ は

$q^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1) \quad \Leftrightarrow \quad q \equiv g_p^{2C_1'}\ (mod\ p)$ の証明

$(\ 2C_1' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ )$

Ⅰ． $ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1) \quad \Rightarrow \quad q \equiv g_p^{2C_1'}\ (mod\ p)$

$(\ 2C_1' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ )$

$\because$

$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1)$ の時

$2C_1' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3$ と置くと

$ind\ q \equiv 2C_1'\ (mod\ p-1)$

この時、$ind\ q = \eta_2'$ と置くと

$q \equiv g_p^{\eta_2'}\ (mod\ p)$

又、 $\eta_2' \equiv 2C_1'\ (mod\ p-1)$より

$\eta_2' = 2C_1' + (p-1)\ s_2$ （s_2は整数）

$\therefore \quad q \equiv g_p^{\eta_2'}(mod\ p)$

$\equiv g_p^{2c_1'+(p-1)s_2}\ (mod\ p)$

この時 g_pは法 pの原始根より

g_pは pで割り切れない。

従って、フェルマーの小定理より

$g_p^{p-1} \equiv 1\ (mod\ p)$

$\therefore \quad q \equiv g_p^{2c_1'}\left(g_p^{p-1}\right)^{s_2}\ (mod\ p)$

$\equiv g_p^{2c_1'}\left(\ 1\ \right)^{s_2}\ (mod\ p)$

$\equiv g_p^{2c_1'}\ (mod\ p)$

Ⅱ．　$q \equiv g_p^{2C_1'} \ (mod\ p)$　　⇒　$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1)$

$(\ 2C_1' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ )$

$\because$

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

$2C_1' = ind\ q$

又、$2C_1' \equiv 2C_1' \ (mod\ p-1)$

$\therefore$　$ind\ q \equiv 2C_1' \ (mod\ p-1)$

$\therefore$　$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1)$

従ってⅠ,Ⅱより

$ind\ q \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ (mod\ p-1)$　⇔　$q \equiv g_p^{2C_1'} \ (mod\ p)$

$(\ 2C_1' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,p-3\ )$

$\left(\frac{p}{q}\right) = -1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv -1\ (mod\ q)$ の証明

Ⅰ. $\left(\frac{p}{q}\right) = -1 \quad \Rightarrow \quad p^{\frac{q-1}{2}} \equiv -1\ (mod\ q)$

$\because$

$\left(\frac{p}{q}\right) = -1$ の時

$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}}\ (mod\ q)$ より

$-1 \equiv p^{\frac{q-1}{2}}\ (mod\ q)$

$\therefore\ p^{\frac{q-1}{2}} \equiv -1\ (mod\ q)$

Ⅱ. $p^{\frac{q-1}{2}} \equiv -1\ (mod\ q) \quad \Rightarrow \quad \left(\frac{p}{q}\right) = -1$

$\because$

$p^{\frac{q-1}{2}} \equiv -1\ (mod\ q)$ の時

$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}}\ (mod\ q)$ より

$\left(\frac{p}{q}\right) \equiv -1\ (mod\ q)$

$\therefore\ \left(\frac{p}{q}\right) = -1 + qt_1$ （t_1は整数）

この時

$\left(\frac{p}{q}\right)$ は 1 か－ 1 である。

$\therefore\ \left(\frac{p}{q}\right) = 1$ と仮定すると

$1 = -1 + qt_1$

$\therefore\ 2 = qt_1$

$\therefore$ 2 は q の倍数

$\therefore\ \ (2, q) = q$

しかし q は奇素数より矛盾。

$\therefore\ \left(\frac{p}{q}\right) = -1$

以上より上記の命題が成立する。

従ってⅠ, Ⅱより

$$\left(\frac{p}{q}\right) = -1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv -1 \,(mod\ q)$$

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

Ⅰ． $p^{\frac{q-1}{2}} \equiv -1\ (mod\ q) \quad \Rightarrow \quad ind\ p \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots,p-2\ (mod\ q-1)$

$\because$

$p^{\frac{q-1}{2}} \equiv -1\ (mod\ q)$ の時

$p^{\frac{q-1}{2}} \equiv q-1\ (mod\ q)$ ＿③

$\left(\frac{q-1}{2}\ ,\ \varphi(q)\right) = \left(\frac{q-1}{2}\ ,\ q-1\right)$

$= \frac{q-1}{2}$

であるから、③の合同式が解けるのは $ind\ q-1$ が $\frac{q-1}{2}$ の倍数である場合、かつ、その場合に限る。

実際、合同式③は

$\frac{q-1}{2}\ ind\ p\ \equiv ind\ q-1\ (mod\ q-1)$

と同値である。

この時

$ind\ q-1=\theta_1'$ と置くと

$q-1 \equiv g_q^{\theta_1'}\ (mod\ q)$

この時 $\theta_1' = \frac{q-1}{2}$ より

$ind\ q-1 = \frac{q-1}{2}$

＿＿※補足参照

$\therefore \quad \frac{q-1}{2}\ ind\ p\ \equiv \frac{q-1}{2}\ (mod\ q-1)$＿④

この時 $\frac{q-1}{2}$ は q の値が $4m_2+1\ ,4m_2+3$ のどちらであったとしても整数である。

又、$\left(\frac{q-1}{2}\ ,q-1\right) = \left(\frac{q-1}{2}\ ,2\left(\frac{q-1}{2}\right)\right)$

$= \frac{q-1}{2}\ (\ 1\ ,2\ )$

$= \frac{q-1}{2}$

であり、$\frac{q-1}{2}$ は $\frac{q-1}{2}$ の倍数である。

従って、④の合同式は $\frac{q-1}{2}$ 個の解を持つ。

両辺と法を $\frac{p-1}{2}$ で割ると

$ind\,p \equiv 1\,(mod\,2)$

$\therefore \quad ind\,p \equiv 1,\ 3,5,7,9,\cdots\cdots,\ 1+2\left(\frac{q-1}{2}-1\right) \quad (mod\,q-1)$

$\therefore \quad ind\,p \equiv 1,\ 3,5,7,9,\cdots\cdots,\ q-2 \quad (mod\,q-1)$

Ⅱ. $\quad ind\,p \equiv 1,3,5,7,9,\cdots\cdots,q-2\,(mod\,q-1) \quad \Rightarrow \quad p^{\frac{q-1}{2}} \equiv -1\,(mod\,q)$

$\because$

$ind\,p \equiv 1,3,5,7,9,\cdots\cdots,q-2\,(mod\,q-1)$ の時

これらの値は、合同式 $\frac{q-1}{2}\,ind\,p \equiv ind\,q-1\,(mod\,q-1)$の解である。

従って、

$ind\,p \equiv 1,3,5,7,9,\cdots\cdots,q-2\,(mod\,q-1)$ の時

$\frac{q-1}{2}\,ind\,p \equiv ind\,q-1(mod\,p-1)$ は成り立つ。

又、$\frac{q-1}{2}\,ind\,p \equiv ind\,q-1\,(mod\,q-1)$ は

$p^{\frac{q-1}{2}} \equiv -1\,(mod\,q)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

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

$(\ 2D_1'+1 = 1,3,5,7,9,\ldots\ldots,q-2\ )$

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

$(\ 2D_1'+1 = 1,3,5,7,9,\ldots\ldots,q-2\ )$

$\because$

$ind\ p \equiv 1,3,5,7,9,\ldots\ldots,q-2\ (mod\ q-1)$ の時

$2D_1'+1 = 1,3,5,7,9,\ldots\ldots,q-2$ と置くと

$ind\ p \equiv 2D_1'+1\ (mod\ q-1)$

この時、$ind\ p = \theta_2'$ と置くと

$p \equiv g_q^{\theta_2'}\ (mod\ q)$

又、 $\theta_2' \equiv 2D_1'+1\ (mod\ q-1)$より

$\theta_2' = 2D_1'+1+(q-1)\ t_2$　　（t_2は整数）

$\therefore \quad p \equiv g_q^{\theta_2'}(mod\ q)$

$\equiv g_q^{2D_1'+1+(q-1)t_2}\ (mod\ q)$

この時 g_qは法 qの原始根より

g_qは qで割り切れない。

従って、フェルマーの小定理より

$g_q^{q-1} \equiv 1\ (mod\ q)$

$\therefore \quad p \equiv g_q^{2D_1'+1}\left(g_q^{q-1}\right)^{t_2}\ (mod\ q)$

$\equiv g_p^{2D_1'+1}\left(1\right)^{t_2}\ (mod\ q)$

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

Ⅱ．　$p \equiv g_q^{2D_1'+1} \ (mod\ q)$　　⇒　　$ind\ p \equiv 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\ (mod\ q-1)$

$(\ 2D_1'+1 = 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\ )$

$\because$

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

$2D_1'+1 = ind\ p$

又、$2D_1'+1 \equiv 2D_1'+1\ (mod\ q-1)$

$\therefore$　$ind\ p \equiv 2D_1'+1\ (mod\ q-1)$

$\therefore$　$ind\ p \equiv 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\ (mod\ q-1)$

従ってⅠ,Ⅱより

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

$(\ 2D_1'+1 = 1\,,3\,,5\,,7\,,9\,,\ldots\ldots,q-2\ )$

【ivである場合の証明】

$\left(\frac{q}{p}\right) = -1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の証明

Ⅰ. $\left(\frac{q}{p}\right) = -1 \quad \Rightarrow \quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

$\because$

$\left(\frac{q}{p}\right) = -1$の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$-1 \equiv q^{\frac{p-1}{2}}\ (mod\ p)$

$\therefore\ q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

Ⅱ. $q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Rightarrow \quad \left(\frac{q}{p}\right) = -1$

$\because$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の時

$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ (mod\ p)$ より

$\left(\frac{q}{p}\right) \equiv -1 \quad (mod\ p)$

$\therefore\ \left(\frac{q}{p}\right) = -1 + pu_1$ （u_1は整数）

この時

$\left(\frac{q}{p}\right)$ は 1 か－ 1 である。

$\therefore\ \left(\frac{q}{p}\right) = 1$ と仮定すると

$1 = -1 + pu_1$

$\therefore\ 2 = pu_1$

$\therefore$ 2 は p の倍数

$\therefore\ (2, p) = p$

しかし p は奇素数より矛盾。

$\therefore \left(\frac{q}{p}\right) = -1$

以上より上記の命題が成立する。

従ってⅠ, Ⅱより

$\left(\frac{q}{p}\right) = -1 \quad \Leftrightarrow \quad q^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Leftrightarrow \quad ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\dots\dots,p-2\ (mod\ p-1)$ の証明

Ⅰ． $q^{\frac{p-1}{2}} \equiv -1\ (mod\ p) \quad \Rightarrow \quad ind\ p \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\dots\dots,p-2\ (mod\ q-1)$

$\because$

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ の時

$q^{\frac{p-1}{2}} \equiv p-1\ (mod\ p)$ ＿⑤

$\left(\frac{p-1}{2}\ ,\ \varphi(p)\right) = \left(\frac{p-1}{2}\ ,\ p-1\right)$

$= \frac{q-1}{2}$

であるから、⑤の合同式が解けるのは $ind\ p-1$ が $\frac{p-1}{2}$ の倍数である場合、かつ、その場合に限る。

実際、合同式⑤は

$\frac{p-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$

と同値である。

この時

$ind\ p-1 = \iota'_1$ と置くと

$p-1 \equiv g_p^{\iota'_1}\ (mod\ p)$

この時 $\iota'_1 = \frac{p-1}{2}$ より

$ind\ p-1 = \frac{p-1}{2}$

＿＿※補足参照

$\therefore \quad \frac{p-1}{2}\ ind\ q\ \equiv \frac{p-1}{2}\ (mod\ p-1)$＿⑥

この時 $\frac{p-1}{2}$ は p の値が $4m_1+1\ ,4m_1+3$ のどちらであったとしても整数である。

又、$\left(\frac{p-1}{2}\ ,p-1\right) = \left(\frac{p-1}{2}\ ,2\left(\frac{p-1}{2}\right)\right)$

$= \frac{p-1}{2}\ (\ 1\ ,2\ )$

$= \frac{p-1}{2}$

であり、$\frac{p-1}{2}$ は $\frac{p-1}{2}$ の倍数である。

従って、⑥の合同式は $\frac{p-1}{2}$ 個の解を持つ。

両辺と法を $\frac{p-1}{2}$ で割ると

$ind\ q\ \equiv 1\ (mod\ 2\ )$

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

$\therefore\quad ind\ q\ \equiv 1\ ,\ 3\ ,5\ ,7\ ,9\ ,\ldots\ldots\ ,\ p-2\quad (\ mod\ p-1\ )$

Ⅱ.　$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)\quad \Rightarrow\quad q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$

$\because$

$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)$ の時

これらの値は、合同式 $\frac{q-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$の解である。

従って、

$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots, p-2\ (mod\ p-1)$ の時

$\frac{p-1}{2}\ ind\ q\ \equiv\ ind\ p-1(mod\ p-1)$ は成り立つ。

又、$\frac{p-1}{2}\ ind\ q\ \equiv ind\ p-1\ (mod\ p-1)$ は

$q^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

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

$(\ 2C_2'+1 = 1,3,5,7,9,\ldots\ldots,p-2\ )$

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

$(\ 2C_2'+1 = 1,3,5,7,9,\ldots\ldots,p-2\ )$

$\because$

$ind\ q \equiv 1,3,5,7,9,\ldots\ldots,p-2\ (mod\ p-1)$ の時

$2C_2'+1 = 1,3,5,7,9,\ldots\ldots,p-2$ と置くと

$ind\ q \equiv 2C_2'+1\ (mod\ p-1)$

この時、$ind\ q = \iota_2'$ と置くと

$q \equiv g_p^{\iota_2'}\ (mod\ p)$

又、 $\iota_2' \equiv 2C_2'+1\ (mod\ p-1)$より

$\iota_2' = 2C_2'+1+(p-1)\ u_2$　　（u_2は整数）

$\therefore \quad q \equiv g_p^{\iota_2'}(mod\ p)$

$\equiv g_p^{2c_2'+1+(p-1)u_2}\ (mod\ p)$

この時 g_pは法 pの原始根より

g_pは pで割り切れない。

従って、フェルマーの小定理より

$g_p^{p-1} \equiv 1\ (mod\ p)$

$\therefore \quad q \equiv g_p^{2c_2'+1}\left(g_p^{p-1}\right)^{u_2}\ (mod\ p)$

$\equiv g_p^{2c_2'+1}\left(1\right)^{u_2}\ (mod\ p)$

$\equiv g_p^{2c_2'+1}\ (mod\ p)$

Ⅱ．　$q \equiv g_p^{2C_2'+1} \ (mod\ p)$　　⇒　$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots,p-2\ (mod\ p-1)$

$(\ 2C_2'+1=1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots,p-2\ )$

$\because$

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

$2C_2'+1 = ind\ q$

又、$2C_2'+1 \equiv 2C_2'+1(mod\ p-1)$

$\therefore$　$ind\ q \equiv 2C_2'+1(mod\ p-1)$

$\therefore$　$ind\ q \equiv 1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots,p-2\ (mod\ p-1)$

従ってⅠ,Ⅱより

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

$(\ 2C_2'+1=1\ ,3\ ,5\ ,7\ ,9\ ,\ldots\ldots,p-2\ )$

$\left(\frac{p}{q}\right)=1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv 1\,(mod\ q)$　の証明

Ⅰ．　$\left(\frac{p}{q}\right)=1 \quad \Rightarrow \quad p^{\frac{q-1}{2}} \equiv 1\,(mod\ q)$

$\because$

$\left(\frac{p}{q}\right)=1$ の時

$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}}(mod\ q)$ より

$1 \equiv p^{\frac{q-1}{2}}\ (mod\ q)$

$\therefore\ p^{\frac{q-1}{2}} \equiv 1\,(mod\ q)$

Ⅱ．　$p^{\frac{q-1}{2}} \equiv 1\,(mod\ q) \quad \Rightarrow \quad \left(\frac{p}{q}\right)=1$

$\because$

$p^{\frac{q-1}{2}} \equiv 1\,(mod\ q)$ の時

$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}}\ (mod\ q)$ より

$\left(\frac{p}{q}\right) \equiv 1\ (mod\ q)$

$\therefore\ \left(\frac{p}{q}\right)=1+qv_1$　　（v_1は整数）

この時

$\left(\frac{p}{q}\right)$ は 1 か－ 1 である。

$\therefore\ \left(\frac{p}{q}\right)=-1$ と仮定すると

$-1=1+qv_1$

$\therefore\ -2=qv_1$

$\therefore\ 2=q(-v_1)$

$\therefore$ 2 は q の倍数

$\therefore\ \ (2,q)=q$

しかし q は奇素数より矛盾。

$\therefore \left(\frac{p}{q}\right) = 1$

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

$\left(\frac{p}{q}\right) = 1 \quad \Leftrightarrow \quad p^{\frac{q-1}{2}} \equiv 1 \ (mod\ q)$

$p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$　　⇔　$ind\ p \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots,q-3\ (mod\ q-1)$　の証明

Ⅰ．　$p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$　　⇒　$ind\ p \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots,q-3\ (mod\ q-1)$

∵

$p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$ __⑦　の時

$\left(\frac{q-1}{2}\ ,\ \varphi(q)\right) = \left(\frac{q-1}{2}\ ,\ q-1\right)$

$= \frac{q-1}{2}$

であるから、⑦の合同式が解けるのは $ind\ 1$ が $\frac{q-1}{2}$ の倍数である場合、かつ、
その場合に限る。

実際、合同式⑦は
$\frac{q-1}{2}\ ind\ p\ \equiv ind\ 1\ (mod\ q-1)$
と同値である。

この時
$ind\ 1 = \kappa_1'$と置くと
$1 \equiv g_q^{\kappa_1'}\ (mod\ q)$
$\therefore\ \kappa_1' = 0$
$\therefore\ ind\ 1 = 0$ より

$\frac{q-1}{2}\ ind\ p\ \equiv 0\ (mod\ q-1)$__⑧

この時 $\frac{q-1}{2}$ は q の値が $4m_2+1\ ,4m_2+3$ のどちらであったとしても整数である。

又、$\left(\frac{q-1}{2}\ ,q-1\right) = \left(\frac{q-1}{2}\ ,2\left(\frac{q-1}{2}\right)\right)$

$= \frac{q-1}{2}\ (\ 1\ ,2\ )$
$= \frac{q-1}{2}$

であり、0 は $\frac{q-1}{2}$ の倍数である。
従って、⑧の合同式は $\frac{q-1}{2}$ 個の解を持つ。

両辺と法を $\frac{q-1}{2}$ で割ると
$ind\ p\ \equiv 0\ (mod\ 2\ )$

$\therefore \quad ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, 0 + 2\left(\frac{q-1}{2} - 1\right) \quad (mod\ q-1)$

$\therefore \quad ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3 \quad (mod\ q-1)$

Ⅱ. $\quad ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3\ (mod\ q-1) \quad \Rightarrow \quad p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$

$\because$

$ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3\ (mod\ q-1)$ の時
これらの値は、合同式 $\frac{q-1}{2}\ ind\, p \equiv 0\ (mod\ q-1)$の解である。

従って、
$ind\, p \equiv 0, 2, 4, 6, 8, \cdots\cdots, q-3\ (mod\ q-1)$ の時
$\frac{q-1}{2}\ ind\, p \equiv 0\ (mod\ q-1)$ は成り立つ。

又、$\frac{q-1}{2}\ ind\, p \equiv 0\ (mod\ q-1)$ は

$p^{\frac{q-1}{2}} \equiv 1\ (mod\ q)$ と同値である。

以上より上記の命題が成立する。

従ってⅠ,Ⅱより

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

$ind\ p \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots, q-3\ (mod\ q-1) \quad \Leftrightarrow \quad p \equiv g_q^{2D_2'}\ (mod\ q)$ の証明

$(\ 2D_2' = 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots, q-3\ )$

Ⅰ. $ind\ p \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots, p-3\ (mod\ q-1) \quad \Rightarrow \quad p \equiv g_q^{2D_2'}\ (mod\ q)$

$(\ 2D_2' = 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots, q-3\ )$

$\because$

$ind\ p \equiv 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots, q-3\ (mod\ q-1)$ の時

$2D_2' = 0\ ,2\ ,4\ ,6\ ,8\ ,\ldots\ldots, q-3$ と置くと

$ind\ p \equiv 2D_2'\ (mod\ q-1)$

この時、$ind\ p = \kappa_2'$ と置くと

$p \equiv g_q^{\kappa_2'}\ (mod\ q)$

又、 $\kappa_2' \equiv 2D_2'\ (mod\ q-1)$より

$\kappa_2' = 2D_2' + (q-1)\ v_2$ （v_2は整数）

$\therefore \quad p \equiv g_p^{\kappa_2'}\ (mod\ q)$

$\equiv g_q^{2D_2'+(q-1)v_2}\ (mod\ q)$

この時 g_qは法 qの原始根より

g_qは qで割り切れない。

従って、フェルマーの小定理より

$g_q^{q-1} \equiv 1\ (mod\ q)$

$\therefore \quad p \equiv g_q^{2D_2'}\left(g_q^{q-1}\right)^{v_2}\ (mod\ q)$

$\equiv g_q^{2D_2'}\left(\ 1\ \right)^{v_2}\ (mod\ q)$

$\equiv g_q^{2D_2'}\ (mod\ q)$

Ⅱ．　$p \equiv g_q^{2D_2'} \ (mod\ q)$　　⇒　$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$

$(\ 2D_2' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\,)$

$\because$

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

$2D_2' = ind\ p$

又、$2D_2' \equiv 2D_2' \ (mod\ q-1)$

$\therefore$　$ind\ p \equiv 2D_2' (mod\ q-1)$

$\therefore$　$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$

従ってⅠ,Ⅱより

$ind\ p \equiv 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\ (mod\ q-1)$　⇔　$p \equiv g_q^{2D_2'} \ (mod\ q)$

$(\ 2D_2' = 0\,,2\,,4\,,6\,,8\,,\ldots\ldots,q-3\,)$