

※その他、証明すべき命題

$$qM'_1 \equiv 1 \pmod{p} \Rightarrow qM'_1 \equiv 1 + ap \pmod{pq} \quad (a = 0, 1, 2, \dots, q-1) \quad \text{の証明}$$

∴

$$qM'_1 \equiv 1 \pmod{p} \text{ の時}$$

$$qM'_1 = 1 + ap \quad (a \text{ はある整数})$$

この時、 M'_1 は $0 \sim p-1$ までのいずれかの整数と合同であるため

$$M'_1 \equiv 0 \pmod{p} \text{ 又は}$$

$$M'_1 \equiv 1 \pmod{p} \text{ 又は}$$

∴

$$M'_1 \equiv p-1 \pmod{p} \text{ とおけ}$$

この時

$$M'_1 = 0 + k_0 p$$

$$M'_1 = 1 + k_1 p$$

∴

$$M'_1 = p-1 + k_{p-1} p$$

であり、 M'_1 は $qM'_1 \equiv 1 \pmod{p}$ を満たすある任意の値であるため

$k_0 \sim k_{p-1}$ を 0 と定めてしまえば、 M'_1 は $0, 1, \dots, p-1$ のどれかの値と等しい。

この時 $0 \leq qM'_1 \leq q(p-1)$ であり

従って $0 \leq qM'_1 \leq pq - q < pq$

故に $0 \leq 1 + qp < pq$

又、上記より

$$-1 \leq ap < pq - 1$$

$$-\frac{1}{p} \leq a < \frac{pq}{p} - \frac{1}{p}$$

$$-\frac{1}{p} \leq a < q - \frac{1}{p}$$

この時 a は整数より

$$0 \leq a < q - 1$$

従って、この時

$$qM'_1 = 1 + ap \text{ は}$$

$$qM'_1 \equiv 1 + ap \pmod{pq} \quad (a = 0, 1, 2, \dots, q - 1)$$

と表せる。

以上より、上記の命題が成立する。

$g_q^\gamma \equiv a \pmod{q}$ と置く時

$$g_q^\gamma \pmod{q} \equiv -1 \quad \Leftrightarrow \quad \gamma = \frac{q-1}{2} \text{ の証明}$$

$$1. \quad g_q^\gamma \equiv -1 \pmod{q} \Rightarrow \gamma = \frac{q-1}{2}$$

$\therefore$

$g_q^\gamma \equiv -1 \pmod{q}$ の時

フェルマーの小定理より

q が素数で g_q は q で割り切れない事から

$$g_q^{q-1} \equiv 1 \pmod{q} \text{ ---①}$$

この時

$$g_q^{q-1} - 1 \equiv 0 \pmod{q} \text{ であることより}$$

$$\left(g_q^{\frac{q-1}{2}} - 1\right) \left(g_q^{\frac{q-1}{2}} + 1\right) \equiv 0 \pmod{q}$$

また、この時

$$g_q^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q} \text{ と } g_q^{\frac{q-1}{2}} + 1 \equiv 0 \pmod{q} \text{ は同時には成立しない。 ---※ (補足あり)}$$

従って、

$$\left(g_q^{\frac{q-1}{2}} - 1\right) \left(g_q^{\frac{q-1}{2}} + 1\right) \equiv 0 \pmod{q} \text{ が成り立つためには}$$

$$g_q^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q} \text{ か } g_q^{\frac{q-1}{2}} + 1 \equiv 0 \pmod{q} \text{ のどちらか一方が}$$

成り立つ必要がある。

ここで仮に、 $g_q^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q}$ が成り立つと仮定すると

$$g_q^{\frac{q-1}{2}} \equiv 1 \pmod{q} \text{ ---②}$$

この時 ① , ②より

$$g_q^{q-1} \equiv g_q^{\frac{q-1}{2}} \pmod{q}$$

この時 g_q は原始根より

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

$$\therefore 2q-2 = q-1$$

$$\therefore q = 1$$

この時 q は素数より矛盾。

$$\therefore g_q^{\frac{q-1}{2}} \equiv -1 \pmod{q} \text{ である。}$$

この時 $g_q^\gamma \equiv -1 \pmod{q}$ より

$$g_q^{\frac{q-1}{2}} \equiv g_q^\gamma \pmod{q}$$

この時 g_q は原始根より

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

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

以上より

$$g_q^\gamma \equiv -1 \pmod{q} \Rightarrow \gamma = \frac{q-1}{2}$$

II. $g_q^\gamma \equiv a \pmod{q}$ と置く時

$$\gamma = \frac{q-1}{2} \Rightarrow g_q^\gamma \equiv -1 \pmod{q}$$

$\therefore$

$g_q^\gamma \equiv a \pmod{q}$ である時

$\gamma = \frac{q-1}{2}$ ③ である事から

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

$$\left(g_q^{\frac{q-1}{2}}\right)^2 \equiv a^2 \pmod{q}$$

$$g_q^{q-1} \equiv a^2 \pmod{q}$$

この時、 g_q 法 q に関する原始根であるため
 g_q は q では割り切れない。

$\therefore$ フェルマーの小定理より

$$g_q^{q-1} \equiv 1 \pmod{q}$$

この時

$$1 \equiv a^2 \pmod{q}$$

$$\therefore a^2 \equiv 1 \pmod{q}$$

$$\therefore a \equiv -1; 1 \pmod{q}$$

$$\therefore a = -1 + qs_1 \quad \text{or} \quad 1 + qs_2$$

仮に $a = 1 + qs_2$ と置くと

$$g_q^{\frac{q-1}{2}} \equiv 1 + qs_2 \pmod{q}$$

$$\therefore g_q^{\frac{q-1}{2}} \equiv 1 \pmod{q}$$

この時

$$g_q^{q-1} \equiv 1 \pmod{q}$$

$$\therefore g_q^{q-1} \equiv g_q^{\frac{q-1}{2}} \pmod{q}$$

この時 g_q は原始根より

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

$$\therefore 2q-2 = q-1$$

$$\therefore q = 1$$

従って、 q は素数である事より矛盾。

$$\therefore a = -1 + qs_1$$

$$\therefore g_q^{\frac{q-1}{2}} \equiv -1 \pmod{q}$$

この時 ③より

$$\gamma = \frac{q-1}{2} \text{ である事から}$$

$$g_q^\gamma \equiv -1 \pmod{q}$$

以上より

$$g_q^\gamma \equiv a \pmod{q} \text{ と置く時}$$

$$\gamma = \frac{q-1}{2} \Rightarrow g_q^\gamma \equiv -1 \pmod{q}$$

従って I, II より

$$g_q^\gamma \equiv a \pmod{q} \text{ と置く時}$$

$$-1 \equiv g_q^\gamma \pmod{q} \Leftrightarrow \gamma = \frac{q-1}{2}$$

「 $g_q^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q}$ と $g_q^{\frac{q-1}{2}} + 1 \equiv 0 \pmod{q}$ は同時には成立しない」

事の証明

∵

$g_q^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q}$ と $g_q^{\frac{q-1}{2}} + 1 \equiv 0 \pmod{q}$ が同時に成立すると仮定する。

この時、双方の合同式の差をとっても成立する事から

$$\left(g_q^{\frac{q-1}{2}} - 1\right) - \left(g_q^{\frac{q-1}{2}} + 1\right) \equiv 0 \pmod{q}$$

$$\therefore -1 - 1 \equiv 0 \pmod{q}$$

$$\therefore -2 \equiv 0 \pmod{q}$$

$$\therefore 2 \equiv 0 \pmod{q}$$

$$\therefore 2 = qs$$

この時 2 は q の倍数より

$$(2, q) = q$$

しかし、 $(2, q) = 1$ である事より矛盾。

従って

$g_q^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q}$ と $g_q^{\frac{q-1}{2}} + 1 \equiv 0 \pmod{q}$ は同時には成立しない。

以上より、上記の命題が成立する。