原始根をもつ条件

扱う文字は全て整数とする.

定義 1 関数 $\lambda(m)$ を次のように定義する.[*1]

$$\lambda(1)=1,\lambda(2)=1,\lambda(4)=2,$$

つまり $0\leq k\leq 2$ のとき

$$\lambda(2^k)=\phi(2^k)$$

$k\geq 3$ のとき

$$\lambda(2^k)=2^{k-2}=\frac{\phi(2^k)}{2}$$

p を奇素数とすると，$h\geq 1$ のとき

$$\lambda(p^h)=\phi(p^h)=(p-1)\cdot p^{h-1}$$

p_n を奇素数とすると，$k\geq 0, h_m\geq 1$ のとき

$$\lambda(2^k{p_1}^{h_1}{p_2}^{h_2}{p_3}^{h_3}\cdots{p_t}^{h_t})=\mathrm{lcm}(\lambda(2^k),\lambda({p_1}^{h_1}),\lambda({p_2}^{h_2}),\lambda({p_3}^{h_3}),\cdots,\lambda({p_t}^{h_t}))$$

補題 1 任意の奇数 a について $a^n\equiv 1 \pmod{2^k, k\geq 1}$ が成り立つ条件は $\lambda(2^k)|n$ である.

[証明略]

補題 2 $m=m_1m_2m_3\cdots m_t$ のとき

$$x\equiv 1 \pmod m$$

は

$$\begin{cases} x\equiv 1 \pmod{m_1} \\ x\equiv 1 \pmod{m_2} \\ x\equiv 1 \pmod{m_3} \\ \cdots\cdots\cdots\cdots \\ x\equiv 1 \pmod{m_t} \end{cases}$$

と同値である.

[証明略] ほぼ自明

定理 1 $(m,a)=1$ である任意の a について

$$a^n\equiv 1 \pmod m$$

が成り立つための必要十分条件は

$$\lambda(m)|n$$

である.

[*1] この関数をカーマイケル関数あるいはカーマイケルの λ 関数と呼ぶ

[証明]$(m,a)=1$ である任意の a について

$$a^n \equiv 1 \pmod{m}$$

であるとき，$m = 2^k {p_1}^{h_1} {p_2}^{h_2} {p_3}^{h_3} \cdots {p_t}^{h_t}$ とすると，

$$\begin{aligned}
a^n &\equiv 1 \pmod{2^k} \\
a^n &\equiv 1 \pmod{{p_1}^{h_1}} \\
a^n &\equiv 1 \pmod{{p_2}^{h_2}} \\
a^n &\equiv 1 \pmod{{p_3}^{h_3}} \\
&\cdots\cdots\cdots\cdots \\
a^n &\equiv 1 \pmod{{p_t}^{h_t}}
\end{aligned}$$

つまり，

$$\lambda(2^k)|n, \lambda({p_1}^{h_1})|n, \lambda({p_2}^{h_2})|n, \lambda({p_3}^{h_3})|n, \cdots, \lambda({p_t}^{h_t})|n$$

$$\therefore \lambda(m)|n$$

逆に

$$\lambda(m)|n$$

であるとき，

$$\lambda(2^k)|n, \lambda({p_1}^{h_1})|n, \lambda({p_2}^{h_2})|n, \lambda({p_3}^{h_3})|n, \cdots, \lambda({p_t}^{h_t})|n$$

よって

$$\begin{aligned}
a^n &\equiv 1 \pmod{2^k} \\
a^n &\equiv 1 \pmod{{p_1}^{h_1}} \\
a^n &\equiv 1 \pmod{{p_2}^{h_2}} \\
a^n &\equiv 1 \pmod{{p_3}^{h_3}} \\
&\cdots\cdots\cdots\cdots \\
a^n &\equiv 1 \pmod{{p_t}^{h_t}}
\end{aligned}$$

がそれぞれの法と互いに素である任意の a について成り立つ．そのなかで m と互いに素である a を任意に選べばこれらの合同式を全て満たし，その場合，補題 2 より，

$$a^n \equiv 1 \pmod{m}$$

を満たす． [証明おわり]

定理 2 m を法とする原始根が存在する必要十分条件は

$$m = 2, 4, p^h, 2p^h$$

のどれかであることである．ただし p は奇素数である．

[証明] 定理 1 より m が原始根をもつ条件は

$$\phi(m) = \lambda(m), m \neq 1$$

つまり,

$$(\lambda(2^k), \lambda({p_1}^{h_1}), \lambda({p_2}^{h_2}), \lambda({p_3}^{h_3}), \cdots, \lambda({p_t}^{h_t})) = 1, 0 \leq k \leq 2, m \neq 1$$

$\lambda({p_1}^{h_1}), \lambda({p_2}^{h_2}), \lambda({p_3}^{h_3}), \cdots, \lambda({p_t}^{h_t})$ は全て約数 2 をもつので，奇素数 (の冪) は複数個あってはならない．また $\lambda(4) = 2$ であるので，奇素数と 4 の積も原始根をもたない．のこりは

$$m = 2, 4, p^h, 2p^h$$

が全てである．　[証明おわり]