$2p^h$ を法とする原始根

扱う文字は全て整数とする．p は奇素数とする．

定理 1 r が p^h の奇数の原始根である場合，これは $2p^h$ の原始根である．偶数の原始根である場合，$r+p^h$ は $2p^h$ の原始根である．

[証明] p^h を法とする場合 r に対応する指数を n とすると，

$$r^n = 1 + kp^h$$

r が奇数の場合，右辺も奇数であるから kp^h は偶数．よって k も偶数であり

$$r^n \equiv 1 \pmod{2p^h}$$

また

$$r^m \neq 1 + kp^h (m < n)$$

であるから $2p^h$ を法とする場合 r に対応する指数は n である．したがって r は $2p^h$ の原始根である．

r が偶数の場合 k は奇数となり，

$$r^n \equiv 1 + p^h \pmod{2p^h}$$

$$\begin{aligned}(r+p^h)^n &= r^n + nr^{n-1}p^h + \cdots + p^{hn} \\ &= 1 + kp^h + nr^{n-1}p^h + \cdots + p^{hn} \\ &= 1 + k'p^h\end{aligned}$$

k' は偶数であるので，

$$(r+p^h)^n \equiv 1 \pmod{2p^h}$$

やはりこの $r+p^h$ は n より小さい指数には対応しえないので $2p^h$ の原始根である．　[証明おわり]