$g^k \pmod p$

$p = 2\tilde{p} + 1$ $\quad p, \tilde{p}$ - prime numbers

$g \in \mathbb{F}_p^*$ $\quad |\mathbb{F}_p^*| = p - 1 = 2\tilde{p}$

$g^k = g^{k \pmod{p-1}} \pmod p$

$\operatorname{ord} g \mid p - 1$

Let g' is a generator of $\mathbb{F}_p^*$

$g = (g')^k \pmod p$

$g^k = ((g')^k)^k \pmod p = (g')^{k \cdot k} \pmod p$

$= (g')^{k \cdot k \pmod{p-1}} \pmod p =$

$= ((g')^k)^{k \pmod{p-1}} \pmod p$

$= g^{k \pmod{p-1}} \pmod p$

$g^0, g^1, \dots, g^{p-2}, g^{p-1} = 1$

$\| \qquad\qquad\qquad\qquad\qquad\qquad\quad \| \pmod{p-1}$

$1 \qquad\qquad\qquad\qquad\qquad\qquad\quad 1$

$$g^k = g^{k \pmod{p-1}} \pmod{p}$$

CRT:

$M = m_1 \cdot m_2 \cdots m_k$, $\gcd(m_i, m_j) = 1$ if $i \neq j$

$$a = x \pmod{M} \iff \begin{cases} a \equiv x_1 \pmod{m_1} \\ a \equiv x_2 \pmod{m_2} \\ \vdots \\ a \equiv x_k \pmod{m_k} \end{cases}$$

$$x \rightleftarrows (x_1, \ldots, x_k)$$

$p - 1 = 2 \cdot \tilde{p}$

$$g^k \pmod{p-1} = g^{\begin{cases} 0 \pmod 2 \\ k \pmod{\tilde{p}} \end{cases}} \pmod{p}$$

$\mathbb{F}_p^* \cong \langle (2) \rangle \times \langle (\tilde{p}) \rangle$

$g^k g^\ell = g^{k+\ell} \pmod{p}$

$g = g'^{\ell} \pmod{p}$ $\quad \langle g' \rangle = \mathbb{F}_p^*$

$$g^2 \pmod{p} = (g')^{2\ell} \pmod{p} = (g')^{\begin{cases} 2\ell \pmod 2 \\ 2\ell \pmod{\tilde{p}} \end{cases}} \pmod{p}$$

$$= g^{\begin{cases} 0 \pmod 2 \\ 2\ell \pmod{\tilde{p}} \end{cases}} \pmod{p}$$

if $\ell = 0 \Rightarrow g^2 \pmod{p} = 1$

if $\ell \neq 0 \Rightarrow g^2 \pmod{p} \neq 1$

of course

$\begin{cases} \ell = 0 \pmod{\tilde{p}} \\ \ell \neq 0 \pmod{\tilde{p}} \end{cases}$

correspondingly

Let $l \neq 0 \pmod{\tilde{p}}$:

Let t be the order of $\tilde{g} = g^2 \pmod{p}$.

So t is the smallest positive integer that:

$$\tilde{g}^1, \tilde{g}^2, \ldots, \underbrace{\tilde{g}^t \pmod{p}}_{=1}$$

$$\tilde{g}^t = (g^2)^t = (g^l)^{2lt} \pmod{p} =$$

$$= (g^l)^{\begin{cases} 2lt \pmod 2 \\ 2lt \pmod{\tilde{p}} \end{cases}} = (g^l)^{\begin{cases} 0 \pmod 2 \\ 2lt \pmod{\tilde{p}} \end{cases}} = 1 \pmod{p}$$

$$(g^l)^{\begin{cases} 0 \pmod 2 \\ 0 \pmod{\tilde{p}} \end{cases}}$$

That is:

$$\begin{cases} 0 \equiv 0 \pmod 2 \\ 2lt \equiv 0 \pmod{\tilde{p}} \end{cases}$$

$$\Downarrow$$

$$2lt \equiv 0 \pmod{\tilde{p}} \qquad \gcd(2l, \tilde{p}) = 1$$

because $\tilde{p}$ - prime and $2, l > 0$,

hence

$$2lt \equiv 0 \pmod{\tilde{p}} \quad / \cdot (2l)^{-1}$$

$$(*) \quad t \equiv 0 \pmod{\tilde{p}}$$

the smallest positive t satisfying the condition $(*)$ is $t = \tilde{p}$.