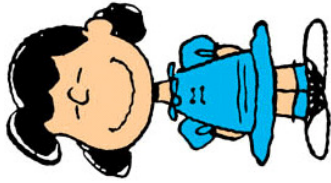


$$v = s^2$$



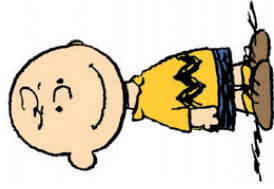
$$\beta \stackrel{\leftarrow u}{\leftarrow} \{0, 1\}$$

Halt if $\gamma \notin \mathbb{Z}_n^*$

$$\gamma^2 = r^2 s^2 \beta \stackrel{?}{=} \alpha v^\beta$$

$$\begin{array}{c} \xrightarrow{\alpha = r^2} \\ \xrightarrow{\beta} \\ \xrightarrow{\gamma = r s^\beta} \end{array}$$

$$s \in \mathbb{Z}_n^*$$



$$r \stackrel{\leftarrow u}{\leftarrow} \mathbb{Z}_n^*$$