X_1: Demonstrate that if $p \equiv 1 \bmod 4$, then $r \equiv a^{\frac{p+1}{4}}$ will generate two square roots {r, $-r$ }. We will validate this by squaring both sides and discover that r equals the square root of a.

$$Let\ a = u^2$$

$$r \equiv a^{\frac{p+1}{4}} = (u^2)^{\frac{p+1}{4}} = u^{\frac{p+1}{2}} = [(u^2)(u^{p-1})]^{\frac{1}{2}}$$

$$Since\ u^{p-1} \equiv 1\ mod\ p$$

$$r = (u^2)^{\frac{1}{2}}$$

$$r \equiv a^{\frac{1}{2}}$$

X_2: Demonstrate that if $p \equiv 5 \bmod 8$, $r = a^{\frac{p+3}{8}}\ mod\ p$ will generate two square roots of a, {r, $-r$ } when $1 \equiv a^{\frac{p-1}{4}}\ mod\ p$. If $p-1 \equiv a^{\frac{p-1}{4}}\ mod\ p$, then $r = (2a)(4a)^{\frac{p-5}{8}}\ mod\ p$ will generate two square roots of a, {r, -r}. We will validate the first part:

$$Let\ a = u^2$$

$$r = (u^2)^{\frac{p+3}{8}} = u^{\frac{p+3}{4}} = (u^{\frac{p-1}{4}})(u) = u$$

We then validate the second part:

<< I will attempt this and send in a later email, I need to get to work >>