To find a such that $x^2 \equiv a \pmod{p}$, when $\left(\frac{a}{p}\right) = 1$

p - odd prime.

Let n - quadratic non-residue

$p - 1 = 2^{\alpha} \cdot s \quad (s \to \text{odd})$

Let $b = n^s \bmod p$

$$r = a^{\frac{s+1}{2}} \bmod p$$

Claim:- $\frac{r^2}{a}$ is $2^{\alpha-1}$-th root of unity.

Infact, $\left(r^2 \cdot a^{-1}\right)^{2^{\alpha-1}} = \left(a^{s+1} \cdot a^{-1}\right)^{2^{\alpha-1}}$

$$= a^{s \cdot 2^{\alpha-1}}$$

$$= a^{\frac{p-1}{2}}$$

$$= \left(\frac{a}{p}\right) \bmod p$$

$$= 1 \quad \text{(claim holds)}$$

Claim:- b is primitive 2^{α}-th root of unity.

(i.e., 2^α-th roots of unity are powers of b.)

$$b^{2^\alpha} = n^{s \cdot 2^\alpha} = n^{p-1} = 1 \quad \text{(F.L.T.)}$$

If b is not primitive 2^α-th root of unity, there is a $j < 2^\alpha$ such that $b^j = 1$ and $j \mid 2^\alpha$. (j-even)

$\Rightarrow$ b is an even power of primitive 2^α-th root of 1.

$\Rightarrow$ b is a square (residue)

$\Rightarrow \left(\frac{b}{p}\right) = 1.$

But $\left(\frac{b}{p}\right) = \left(\frac{n^s}{p}\right) = \left(\frac{n}{p}\right)^s = (-1)^s$

$= -1$, as s is odd.

To find j, $0 \le j < 2^\alpha$, such that $x = b^j a$ and $x^2 \equiv a \pmod p$.

Let $j = j_0 + 2j_1 + 2^2 j_2 + \cdots + 2^{\alpha-2} j_{\alpha-2}$.

(binary representation of j).

Where each $j_1, j_2, \ldots$ is 0 or 1.

Note that $j < 2^{\alpha-1}$ We can modify j by $2^{\alpha-i}$, to get another Sq. root. ($\because b^{2^{\alpha-1}} = -1$)

To find $j_0, j_1, j_2, \ldots$

1, Compute $\left(a^2/a\right)^{2^{\alpha-2}} = +1$ or -1

$\left(\because \left[\left(a^2/a\right)^{2^{\alpha-2}}\right]^2 = \left(a^2/a\right)^{2^{\alpha-1}} = +1\right)$

If it is $\begin{cases} +1, & \text{take } j_0 = 0 \\ -1, & \text{take } j_0 = 1. \end{cases}$

i.e., take $j_0 = 0$ or 1, such that

$$\left(b^{j_0} g^2 / a\right)^{2^{\alpha-2}} = +1.$$

(2) Suppose we find $j_0, j_1, \cdots, j_{k-1}$ such that

$$\left[\frac{\left(b^{j_0 + 2j_1 + \cdots + 2^{k-1} j_{k-1}} g\right)^2}{a}\right]^{2^{\alpha-k-1}} = 1.$$

Taking square root,

$$\left[\frac{\left(b^{j_0 + 2j_1 + \cdots + 2^{k-1} j_{k-1}} g\right)^2}{a}\right]^{2^{\alpha-k-2}} = \begin{cases} +1 \\ -1 \end{cases}.$$

Take $j_k = \begin{cases} 0 \\ 1 \end{cases}$, respectively.

$$\Rightarrow \left[\frac{\left(b^{j_0} + 2j_1 + \cdots + 2^k j_k\, r\right)^2}{a}\right]^{2^{\alpha-k-2}} = 1$$

When $k = \alpha - 2$, we get

$$\left[\frac{\left(b^{j_0} + 2j_1 + \cdots + 2^{\alpha-2} j_{\alpha-2}\, r\right)^2}{a}\right]^{2^{\alpha-(\alpha-2)-2}} = 1$$

i.e., $$\frac{\left(b^j r\right)^2}{a} = 1$$

$\Rightarrow x = b^j r$ and $\underline{x^2 \equiv a \pmod p}$

Ex:- Find square root of 302 mod $p = 2081$.

$p = 2081$, $a = 302$

$\left(\frac{2}{p}\right) = +1$ $(\because 2081 \equiv 1 \pmod 8)$

$\left(\frac{3}{p}\right) = \left(\frac{3}{2081}\right) = \left(\frac{2081}{3}\right) = \left(\frac{2}{3}\right) = -1.$

$\therefore$ Let $n = 3.$

$p - 1 = 2080 = 2^5 \times 65$

$\Rightarrow \alpha = 5, \quad s = 65.$

$q = a^{\frac{s+1}{2}} = a^{33} = (302)^{33}.$

$a^2 \equiv 1721 \equiv -360 \pmod{2081}$

$a^4 \equiv 578$

$a^8 \equiv 1124$

$a^{16} \equiv 209$

$a^{32} \equiv 2061$

$q = a^{33} = 2061 \times 302 \equiv \underline{203} \pmod{2081}$

$q = 203$

$n: a^{33} = 2061 \times 302 \equiv \underline{203} \pmod{2081}$

$b = n^{65} = 888$

$(\because \quad 3^2 = 9$

$3^4 = 81$

$3^8 \equiv 318$

$3^{16} \equiv 1236$

$3^{32} \equiv 242$

$3^{64} \equiv 296$

$3^{65} \equiv 296 \times 3 \equiv \underline{888} \pmod{2081}$

$j = j_0 + 2j_1 + \cdots + 2^{\alpha-2} j_{\alpha-2}$

$\Rightarrow j = j_0 + 2j_1 + 2^2 j_2 + 2^3 j_3$

$(\because \alpha = 5)$

To find j_0

$$(x^2 a^{-1})^{2^3} = \left[(203)^2 \times 820\right]^8$$

$a^{-1} = 820$ (by Euclidean Algorithm)

$$\therefore \left[x^2 a^{-1}\right]^{2^3} = (102)^8 = +1$$

$$\therefore \underline{j_0 = 0}$$

$$(102)^2 \equiv -1$$
$$(102)^4 = +1$$
$$(102)^8 = +1.$$

$$\therefore \left[(e^{j_0} x)^2 a^{-1}\right]^{2^{\alpha-3}} = \left[(203)^2 \times 820\right]^{\frac{2}{2}}$$

$$= (102)^4 = \underline{\underline{+1}}$$

$$\therefore \underline{\underline{j_1 = 0}}$$

$$\left[(e^{j_0 + 2j_1} x)^2 \cdot a^{-1}\right]^2 = (102)^2 = -1.$$

$$\therefore j_2 = 1$$

$$\therefore \left[(e^{j_0 + 2j_1 + \frac{2}{2} j_2} x)^2 a^{-1}\right]^{2^0}$$

$$= (b^4 y)^2 \cdot a^{-1}$$

$$= \left[(888)^4 \cdot 203\right]^2 \cdot 820$$

$$= \left[1134 \times 203\right]^2 \cdot 820 = 1$$

$(888)^2 \equiv -155$

$(888)^4 \equiv 1134$

$\therefore \quad x = 1134 \times 203$

$= \underline{1292}$

$\therefore$ Sq. root of $302 \pmod{2081}$ is

$\underline{1292}$

Ex:- Find a square root of $a = 186$ modulo $p = 401$.

$p - 1 = 400 = 2^4 \cdot 25$

$\therefore \alpha = 4$ and $s = 25$.

$\left(\frac{2}{p}\right) = \left(\frac{2}{401}\right) = 1$ $(\because 401 \equiv 1 \pmod 8)$

$\left(\frac{3}{p}\right) = \left(\frac{3}{401}\right) = \left(\frac{401}{3}\right) = \left(\frac{2}{3}\right) = -1.$

$\therefore \underline{n = 3}$

$b = n^s = 3^{25}$

$= \underline{268}$

(Repeated squaring)

$3^2 = 9$

$3^4 = 81$

$3^8 \equiv 145$

$3^{16} \equiv 173$

$3^{25} = 3^{16+8+1}$

$= 173 \times 145 \times 3$

$\equiv \underline{268}$

$$r \equiv a^{\frac{s+1}{2}} = (186)^{13}$$

$$= \underline{\underline{103}}$$

(Repeated squaring)

$186^2 = 110$

$186^4 = 70$

$186^8 = 88$

$186^{13} = 88 \times 70 \times 186$

$= 103$

$a^{-1} = 235$ (Euclidean Algorithm)

Now, $\frac{r^2}{a} = (103)^2 \times 235 = \underline{\underline{98}}$

$j = j_0 + 2j_1 + 2^2 j_2$

To find j_0

$$\left[r^2 \cdot a^{-1}\right]^{2^2} = (98)^4 = \underline{\underline{-1}}$$

$98^2 = 381$

$98^4 = 400 \equiv -1$

$\Rightarrow \underline{\underline{j_0 = 1}}$

$$\Rightarrow \left(b^{j_0} n\right)^2 \cdot a^{-1} = (b n)^2 \cdot a^{-1}$$

$$= [268 \times 103]^2 \times 235$$

$$= (336)^2 \times 235$$

$$= 400$$

$$\equiv \underline{-1}$$

$$\left[\left(b^{j_0} n\right)^2 \cdot a^{-1}\right]^2 = (-1)^2 = +1$$

$$\Rightarrow j_1 = 0$$

$$\Rightarrow \left[\left(b^{j_0 + 2j_1} n\right)^2 a^{-1}\right]^{2^0} = \left[(268 \times 103)^2 \times 235\right]$$

$$= 400$$

$$\equiv -1$$

$$\therefore j_2 = 1$$

$$\therefore j = 1 + 2 \times 0 + 2^2 \times 1 = 5$$

$\therefore x = e^5 \times 9 = (268)^5 \times 103$

$= 147 \times 103$

$\equiv \underline{304}$ (Ans.)

$(268)^2 \equiv 45$

$(268)^4 \equiv 20$

$(268)^5 \equiv 20 \times 268$

$\equiv \underline{147}$

(HW) (1) Find sq. root of 432 modulo 673.

(2) Find sq. root of 567 mod 809.