

To find a such that

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

p - odd prime.

Let n - quadratic non-residue.

$$p-1 = 2^\alpha \cdot 8 \quad (\beta \rightarrow \text{odd})$$

$$\text{Let } b = n^8 \pmod{p}$$

$$g_1 = a^{\frac{8+1}{2}} \pmod{p}$$

Claim: $\frac{g_1^2}{a}$ is $2^{\alpha-1}$ -th root of unity.

$$\text{In fact, } (g_1^2 \cdot a^{-1})^{2^{\alpha-1}} = (a^{\frac{8+1}{2} \cdot a^{-1}})^{2^{\alpha-1}}$$

$$= a^{\frac{8 \cdot 2^{\alpha-1}}{2}}$$

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

$$= a$$

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

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

Claim: b is primitive 2^α -th

root of unity.

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

$$b^{2^{\alpha}} = n^{8 \cdot 2^{\alpha}} = n^{p-1} = 1 \quad (\text{F.L.T.})$$

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 a primitive $2^{\alpha-1}$ -th root of 1.

$\Rightarrow b$ is a square (residue)

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

$$\text{But } \left(\frac{b}{p}\right) = \left(\frac{n^8}{p}\right) = \left(\frac{n}{p}\right)^8 = (-1)^8 = -1, \text{ as } 8 \text{ is odd.}$$

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

Let $j = j_0 + 2^1 j_1 + 2^2 j_2 + \dots + 2^{\alpha-2} j_{\alpha-2}$.

(binary representation of j).

Where each j_1, j_2, \dots 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, \dots

1. Compute $(a^2/a)^{2^{\alpha-2}} = \pm 1$

$$\left(\frac{a^2}{a} \right)^{2^{\alpha-2}} = \left(\frac{a^2}{a} \right)^{2^{\alpha-2}} = \pm 1$$

If it is $\{+1\}$, take $j_0 = 0$
 $\{-1\}$, take $j_0 = 1$.

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

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

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

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

Taking square root,

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

$$= \begin{cases} +1 \\ -1. \end{cases}$$

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

$$\Rightarrow \left[\frac{\left(b^{j_0} + 2^{j_1} + \dots + 2^k j_k \right)^2}{a} \right]^2 = 1$$

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

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

i.e., $\frac{(b^{j_\alpha})^2}{a} = 1$

$$\Rightarrow x = b^{j_\alpha} \quad \text{and} \quad \underline{\underline{x^2 \equiv a \pmod{p}}}$$

Ex:- Find square root of 302
 $\pmod{p=2081}$

$$p = 2081, \quad a = 302$$

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

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

$$\therefore b+n=3.$$

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

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

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

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

$$\alpha^4 \equiv 578$$

$$\alpha^8 \equiv 1124$$

$$\alpha^{16} \equiv 209$$

$$\alpha^{32} \equiv 2061$$

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

$$b = n^{65} = 888$$

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

$$3^4 = 81$$

$$3^8 \equiv 318$$

$$3^{16} \equiv 1236$$

$$3^{32} \equiv 242$$

$$3^{64} \equiv 296$$

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

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

$$\Rightarrow j = j_0 + 2^{j_1} + 2^{j_2} + 2^{j_3} \quad (\because \alpha = 5)$$

To find j_0

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

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

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

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

$$\boxed{\begin{aligned}(102)^2 &\equiv -1 \\(102)^4 &= +1 \\(102)^8 &= +1.\end{aligned}}$$

$$\therefore \left[\left(b^{\frac{3}{2}} g \right)^2 a^{-1} \right]^2 = \left[(203)^2 \times 820 \right]^{\frac{\alpha-3}{2}} \\= (102)^4 = \underline{\underline{+1}}$$

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

$$\left[\left(b^{\frac{3}{2}} + 2j_1 g \right)^2 a^{-1} \right]^2 = (102)^2 = -1.$$

$$\therefore \underline{\underline{j_2 = 1}}$$

$$\therefore \left[\left(b^{\frac{3}{2}} + 2j_1 + \frac{2}{2} j_2 g \right)^2 a^{-1} \right]^2$$

$$= (f^4 g)^2 \cdot a^{-1}$$
$$= [(888)^4 \cdot 203]^2 \cdot 820$$

$$= [1134 \times 203]^2 \cdot 820 = \textcircled{1}$$

$$(888)^2 \equiv -155$$

$$(888)^4 \equiv 1134$$

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

$$= \underline{\underline{1292}}$$

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

$$\underline{\underline{1292}}$$

Ex:- Find a square root of
 $a = 186 \pmod{p} = 401$.

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

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

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

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

$$\therefore \underline{n=3}$$

$$b = n^{\beta} = 3^{25} \\ = \underline{\underline{268}}$$

(Repeated squaring)

$$\begin{aligned} 3^2 &= 9 \\ 3^4 &= 81 \\ 3^8 &\equiv 145 \\ 3^{16} &\equiv 173 \\ 3^{25} &= 3^{16+8+1} \\ &= 173 \times 145 \times 3 \\ &= \underline{\underline{268}} \end{aligned}$$

$$r = a^{\frac{s+1}{2}} = (186)^{13} \\ = \underline{\underline{103}}$$

(Repeated squaring)

$$\left| \begin{array}{l} 186^2 = 110 \\ 186^4 = 70 \\ 186^8 = 88 \\ 186^{13} = 88 \times 70 \times 186 \\ = \underline{\underline{103}} \end{array} \right.$$

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

$$\text{Now, } \frac{g_1^2}{a} = (103)^2 \times 235 = \underline{\underline{98}}$$

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

To find j_0

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

$$98^2 = 381$$

$$98^4 = 400 \equiv -1$$

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

$$\begin{aligned}
 \Rightarrow (\ell^{j_0} g)^2 \cdot a^{-1} &= (g \ell)^2 \cdot a^{-1} \\
 &= [268 \times 103]^2 \times 235 \\
 &= (336)^2 \times 235 \\
 &= 400 \\
 &\equiv -1
 \end{aligned}$$

$$[(\ell^{j_0} g)^2 \cdot a^{-1}]^2 = (-1)^2 = +1$$

$$\Rightarrow j_1 = 0$$

$$\begin{aligned}
 \Rightarrow [(\ell^{j_0+2j_1} g)^2 \cdot a^{-1}]^2 &= [(268 \times 103)^2 \times 235] \\
 &= 400 \\
 &\equiv -1
 \end{aligned}$$

$$\therefore j_2 = 1$$

$$\therefore j = 1 + 2 \times 0 + \frac{2}{2} \times 1 = 5$$

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

$$= 147 \times 103$$

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

$$(268)^2 \equiv 45$$

$$(268)^4 \equiv 20$$

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

$$\equiv \underline{\underline{147}}$$

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

② Find sq. root of 567 mod 809.

Definition :-

$[x]$ = the largest integer less than or equal to x

$[x]$ = unique integer such that-

$$x-1 < [x] \leq x$$

Ex:- $[\sqrt{2}] = 1$, $[\sqrt{3}] = 2$, $[-\frac{3}{2}] = -2$, $[-\pi] = -4$
 $[\frac{3}{2}] = 1$, $[\pi] = 3.$

Note:- $x = [x] + \theta$, $0 \leq \theta < 1$

Properties:- ① $[x+n] = [x] + n$ (x -real
n-integ.)

Proof:- $x-1 < [x] \leq x$

$$\Rightarrow x-1+n < [x]+n \leq x+n \longrightarrow ①$$

Also, $x+n-1 < [x+n] \leq x+n$. $\longrightarrow ②$

$$\Rightarrow x+n < [x+n]+1 \longrightarrow ③$$

From ① and ③,

$$[x]+n < [x+n]+1 \longrightarrow ④$$

From ②, $[x+n]-1 \leq x+n-1$

$$\Rightarrow [x]+n < [x+n] \longrightarrow ⑤$$

From ④ and ⑤,

$$[x+n]-1 < [x]+n < [x+n]+1$$

$$\Rightarrow -1 < [x] + n - ([x+n]) < 1$$

$$\therefore [x] + n - [x+n] = 0$$

$$\Rightarrow \underline{\underline{[x+n]}} = \underline{\underline{[x] + n}}$$

② $[x] + [-x] = 0$ or -1 ,
according as x is an integer
or not.

If x is an integer,
 $[x] = x$ and $[-x] = -x$
 $\therefore [x] + [-x] = 0$.

If x is not an integer,
 $x = [x] + \theta \quad 0 < \theta < 1$
 $-x = [-x] + \theta' \quad 0 < \theta' < 1$.

Adding, $0 = [x] + [-x] + \theta + \theta'$

But $0 < \theta + \theta' < 2$ and

$$\theta + \theta' = -([x] + [-x])$$

$$\therefore 0 < -(\lceil x \rceil + \lceil -x \rceil) < 2$$

$$\Rightarrow -2 < \lceil x \rceil + \lceil -x \rceil < 0$$

$$\Rightarrow \lceil x \rceil + \lceil -x \rceil = -1$$

③ $\lceil x \rceil + \lceil y \rceil \leq \lceil x+y \rceil$

If x and y integers,

$$\lceil x \rceil + \lceil y \rceil = x + y = \lceil x+y \rceil$$

If one of x and y is an integer, say y is integer, then

$$\lceil x \rceil + \lceil y \rceil = \lceil x \rceil + y$$

Already $\lceil x+y \rceil = \lceil x \rceil + y$ (if y is integer)

$$\therefore \lceil x+y \rceil = \lceil x \rceil + \lceil y \rceil$$

If both x and y are not integers, then,

$$x-1 < \lceil x \rceil < x \quad \& \quad y-1 < \lceil y \rceil < y$$

$$\therefore [x] + [y] < x + y$$

$$\Rightarrow [x] + [y] - 1 < x + y - 1 \rightarrow ①$$

Also, $x + y - 1 < [x+y] \leq x + y \rightarrow ②$

From ① and ②,

$$[x] + [y] - 1 < [x+y] \rightarrow ③$$

$$\Rightarrow [x] + y < [x+y]$$

④ If $x > 0, y > 0$, then $[xy] \leq [x][y]$

Let $x = [x] + \theta, 0 \leq \theta < 1$

$$y = [y] + \theta', 0 \leq \theta' < 1.$$

$$[xy] = [(x) + \theta)([y] + \theta')]$$

$$= [[x][y] + \theta[y] + \theta'[x] + \theta\theta']$$

$$= [x][y] + [\theta[y] + \theta'[x] + \theta\theta']$$

$$\Rightarrow [xy] \geq [x][y]$$

(5) $\left[\frac{x}{n} \right] = \left[\frac{\lfloor x \rfloor}{n} \right]$, for any
+ve integer n .

$$\text{Let } \frac{x}{n} = \left[\frac{x}{n} \right] + \theta, \quad 0 \leq \theta < 1$$

$$\therefore x = \left[\frac{x}{n} \right] \cdot n + \theta n$$

$$\Rightarrow \lfloor x \rfloor = \left[\left[\frac{x}{n} \right] \cdot n + \theta n \right]$$

$$= \left[\frac{x}{n} \right] \cdot n + \lfloor \theta n \rfloor$$

($\because \left[\frac{x}{n} \right] \cdot n$ is an integer)

$$\therefore \frac{\lfloor x \rfloor}{n} = \left[\frac{x}{n} \right] + \frac{\lfloor \theta n \rfloor}{n} \rightarrow ①$$

$$\text{But } 0 \leq \theta < 1 \Rightarrow 0 \leq \theta n < n$$

$$\Rightarrow 0 \leq \lfloor \theta n \rfloor \leq \theta n < n$$

$$\Rightarrow 0 \leq \frac{\lfloor \theta n \rfloor}{n} < 1$$

$$\Rightarrow \frac{\lfloor \theta n \rfloor}{n} = 0 \Rightarrow \underline{\underline{\left[\frac{x}{n} \right] = \frac{\lfloor x \rfloor}{n}}}$$

$$⑥ [x] + [y] + [x+y] \leq [2x] + [2y]$$

$$\text{Let } x = [x] + \theta, \quad 0 \leq \theta < 1$$

$$y = [y] + \theta', \quad 0 \leq \theta' < 1$$

$$x+y = [x] + [y] + \theta + \theta'$$

$$[x+y] = [x] + [y] + [\theta + \theta']$$

$$= [x] + [y] + [\theta + \theta'] \rightarrow ①$$

Case (i) $0 \leq \theta < 0.5, \quad 0 \leq \theta' < 0.5$

$$0 \leq \theta + \theta' < 1 \Rightarrow [\theta + \theta'] = 0$$

$$\therefore ① \Rightarrow [x+y] = [x] + [y]$$

$$[x] + [y] + [x+y] = 2[x] + 2[y]$$

$$\text{But} - 2[x] = 2x - 2\theta$$

$$\text{or} \quad 2x = 2[x] + 2\theta$$

$$\Rightarrow [2x] = [2[x] + 2\theta]$$

$$= 2[x] + [2\theta]$$

$$0 \leq \theta < 0.5 \Rightarrow 0 \leq 2\theta < 1$$

$$\therefore [2\theta] = 0$$

$$\therefore 2[x] = 2[x]$$

Similarly, $\underline{2[y] = 2[y]}$

$$\therefore [x] + [y] + [x+y] = 2[x] + 2[y] \\ = [2x] + [2y]$$

Case (ii) $0 \leq \theta < 0.5, 0.5 \leq \theta' < 1.$

$$\Rightarrow 0 < \theta + \theta' < 1.5$$

$$\Rightarrow 0 \leq [\theta + \theta'] \leq 1$$

$$\therefore \text{From } ①, [x+y] \leq [x] + [y] + 1$$

$$\therefore [x] + [y] + [x+y] \leq 2[x] + 2[y] + 1$$

→ (2)

But $2[x] = 2x - 2\theta$

$$\Rightarrow 2x = 2[x] + 2\theta$$

$$[2x] =$$

Ex:- Find the highest power
of 5 dividing 1000!

$$\left[\frac{1000}{5} \right] + \left[\frac{1000}{5^2} \right] + \left[\frac{1000}{5^3} \right] + \left[\frac{1000}{5^4} \right]$$

$$= 200 + 40 + 8 + 1 = \underline{249}$$

5^{249} divides 1000! &

5^{250} won't divide.

(Hw) Find the highest power of
7 dividing 2000!

Ex:- For an integer $n \geq 0$,

$$\left[\frac{n}{2} \right] - \left[-\frac{n}{2} \right] = ?$$

If n is even, then $n = 2k$

and $\left[\frac{n}{2} \right] = \left[k \right] = k$

$$\left. \begin{aligned} \left[-\frac{n}{2} \right] &= \left[-k \right] = -k \end{aligned} \right\}$$

$$\Rightarrow \left[\frac{n}{2} \right] - \left[-\frac{n}{2} \right] = k - (-k) = 2k = n$$

If n is odd, $n = 2k + 1$

$$\Rightarrow \left[\frac{n}{2} \right] = \left[\frac{2k+1}{2} \right] = \left[k + \frac{1}{2} \right] = k$$

$$\text{and } \left[-\frac{n}{2} \right] = \left[-\frac{2k+1}{2} \right] = \left[-k - \frac{1}{2} \right] \\ = \left[-(k + \frac{1}{2}) \right]$$

$$= - (k + 1)$$

$$\therefore \left[\frac{n}{2} \right] - \left[-\frac{n}{2} \right] = k + (k + 1)$$

$$= 2k + 1 = n$$
