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 $x = b^j q$ 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 $2^{\alpha-1}$, 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

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

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.

Definition :-

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

$[x]$ = unique integer such that

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

Ex :- $[\sqrt{2}] = 1$, $[1/3] = 0$, $[-3/2] = -2$, $[-\pi] = -4$, $[\pi] = 3$, $[3/2] = 1$

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

Properties :- ① $[x+n] = [x] + n$ (x - real, n - integer)

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

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

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

$\Rightarrow x + n < [x+n] + 1$ ⟶ ③

From ① and ③,

$$[x] + n < [x+n] + 1 \longrightarrow ④$$

From ②, $[x+n] - 1 \leq x + n - 1$

From ①, $x + n - 1 < [x] + n$ ⟶ ⑤

From ④ and ⑤,

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

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

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

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

(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 <u>not</u> 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

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

$\therefore\ 0 < -([x] + [-x]) < 2$

$\Rightarrow -2 < [x] + [-x] < 0$

$\Rightarrow [x] + [-x] = -1$

(3) $[x] + [y] \leq [x+y]$

If x and y integers,

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

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

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

Already $[x+y] = [x] + y$ (if y is integer)

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

If both x and y are not integers, then,

$x - 1 < [x] < x$ & $y - 1 < [y] < y$

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

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

Also, $x+y-1 < [x+y] \leq x+y \longrightarrow (2)$

From (1) and (2),

$[x]+[y]-1 < [x+y] \longrightarrow (3)$

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

---

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

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

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

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

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

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

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

Note:- (Division Algorithm)

Given integers a and $b>0$, there exists a unique integer r with $0 \le r < b$, satisfying $a = \left[\frac{a}{b}\right] b + r$.

In fact, $\frac{a}{b} - 1 < \left[\frac{a}{b}\right] \le \frac{a}{b}$

$$\Rightarrow \left[\frac{a}{b}\right] b \le a \Rightarrow a - \left[\frac{a}{b}\right] b \ge 0.$$

Also, $\left(\frac{a}{b} - 1\right) b < \left[\frac{a}{b}\right] b$

$$\Rightarrow a - b < \left[\frac{a}{b}\right] b$$

$$\Rightarrow a - \left[\frac{a}{b}\right] b < b.$$

$\therefore$ Taking $r = a - \left[\frac{a}{b}\right] b$, we get $0 \le r < b$

r is unique, as $r = a - \left[\frac{a}{b}\right] b$.

Theorem:- If n is a positive integer, and p is a prime number, then the highest power of p that divides $n!$ is $\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$

Proof:- n can be written as,

$$n = \left[\frac{n}{p}\right] p + r, \quad 0 \le r < p. \text{ (uniquely)}.$$

$\Rightarrow$ the integers $\le n$, which are divisible by p are $p, 2p, 3p, \ldots, \left[\frac{n}{p}\right] p$.

$\Rightarrow$ there are exactly $\left[\frac{n}{p}\right]$ integers $\leq n$, which are divisible by p.

Hence, for any k, $k=1,2,3,\ldots,n$, the integers $\leq n$, which are divisible by p^k are

$p^k, 2p^k, 3p^k, \ldots, \left[\frac{n}{p^k}\right]p^k$

$\therefore$ The total number of times p divides $n!$ is $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$

Note:- $\left[\frac{n}{p^k}\right]=0$, for $p^k>n$.

Remark:- $n! = \prod_{p\leq n} p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]}$

Ex:- For $n=11$, $(11)! = 1\times2\times3\times4\times5\times6\times7\times8\times9\times10\times11$

$= 2^8 \times 3^4 \times 5^2 \times 7 \times 11$

For instance, $\sum_{k=1}^{\infty}\left[\frac{11}{2^k}\right] = \left[\frac{11}{2}\right]+\left[\frac{11}{2^2}\right]+\left[\frac{11}{2^3}\right]+0\cdots\cdots$

$= 5+2+1 = 8$

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

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

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

$\therefore$ 5^{249} divides 1000! & 5^{250} won't divide.

(HW) Find the highest power of 7 dividing 2,000!

Ex:- How many zero's 1000! terminates with ?

$$\sum_{K=1}^{\infty} \left[\frac{1000}{5^K}\right] = \left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right]$$

$$= 200 + 40 + 8 + 1$$

$$= \underline{249}$$

The number of zeros 1000! ending with is number of pairs of (2×5).

Highest power of 2 dividing 1000! is more than 249. $\left(\because \sum_{k=1}^{\infty} \left[\frac{1000}{2^k}\right] > 249\right)$

$\therefore$ 1000! ends with 249 zero's.

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

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

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

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

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

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

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

$$= -(k+1)$$

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

$$= 2k+1 = n$$

Ex:- Prove that $\binom{n}{r}$ is an integer, if n and r are both positive integers.

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}$$

We know that $[a+b] \geq [a]+[b]$, for any real numbers a and b.

$$n = r + (n-r)$$

$$\Rightarrow \frac{n}{p^k} = \frac{r}{p^k} + \frac{n-r}{p^k}$$, for any prime p and $k = 1, 2, 3, \ldots\ldots$

$$\Rightarrow \left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{n-r}{p^k}\right]$$

$$\Rightarrow \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] \geq \sum_{k=1}^{\infty}\left[\frac{r}{p^k}\right] + \sum_{k=1}^{\infty}\left[\frac{n-r}{p^k}\right]$$

Then LHS = highest power of p dividing $n!$

RHS = highest power of p dividing $r!\,(n-r)!$

$\Rightarrow r!\,(n-r)!$ divides $n!$

$\Rightarrow \binom{n}{r}$ is an integer.

Ex:- For a positive integer, the product of any r consecutive integers is divisible by $r!$

Proof:- The product of r consecutive integers can be written as,

$$n(n-1)\cdots\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

$$= \left[\frac{n!}{r!\,(n-r)!}\right] r!$$

$$= \binom{n}{r} \cdot r!$$

$\Rightarrow r!$ divides $n(n-1)\cdots(n-r+1)$

($\because \binom{n}{r}$ is an integer).