In this Lecture, we study: let p be an odd prime,

$$\left(\frac{2}{p}\right) = ?$$

By Euler's creterion, we have:

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

Therefore, we just need to investigate $2^{\frac{p-1}{2}} \pmod{p}$.

We look at two examples and then try to generalize it.

Example I: $p = 13$. Set $P = \frac{p-1}{2} = 6$.

We look at all even integers between 0 and 13.

$$2 \quad 4 \quad 6 \quad 8 \quad 10 \quad 12. \qquad (6 \text{ numbers})$$

- $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 = 2(1) \cdot 2(2) \cdot 2(3) \cdot 2(4) \cdot 2(5) \cdot 2(6)$
$$= 2^6 \cdot (1)(2)(3)(4)(5)(6)$$
$$= 2^6 \cdot 6!$$

- $2 \cdot 4 \cdot \underset{\Delta}{6} \cdot 8 \cdot 10 \cdot 12 \equiv 2 \cdot 4 \cdot 6 \; (8-13)(10-13)(12-13) \pmod{13}$
$$\equiv 2 \cdot 4 \cdot 6 \cdot (-5)(-3)(-1) \pmod{13}$$
$$\equiv (-1)^3 \cdot 6!$$

$$\Rightarrow \quad 2^6 \cdot 6! \equiv (-1)^3 \cdot 6! \pmod{13}$$

$$\Rightarrow \quad 2^6 \equiv -1 \pmod{13} \quad \Rightarrow \quad \left(\frac{2}{13}\right) = -1$$

Example II. $p = 17$ $\qquad \underline{P} = \frac{17-1}{2} = 8$

We look at all even integers between 0 and 17.

$$2 \quad 4 \quad 6 \quad 8 \quad 10 \quad 12 \quad 14 \quad 16 \quad (8 \text{ numbers})$$

- $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 = 2(1) \cdot 2(2) \cdot 2(3) \cdot 2(4) \cdot 2(5) \cdot 2(6) \cdot 2(7) \cdot 2(8)$
$$= 2^8 \cdot 8!$$
- $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 \equiv 2 \cdot 4 \cdot 6 \cdot 8 \cdot (10-17)(12-17)(14-17)(16-17) \pmod{17}$
$$\equiv 2 \cdot 4 \cdot 6 \cdot 8 \cdot (-7)(-5)(-3)(-1) \pmod{17}$$
$$\equiv (-1)^4 \cdot 8! \pmod{17}$$

$$\Rightarrow \quad 2^8 \cdot 8! \equiv (-1)^4 \cdot 8! \pmod{17}$$

$$\Rightarrow \quad 2^8 \equiv 1 \pmod{17} \qquad \left(\frac{2}{17}\right) = 1.$$

We consider a general p, set $P = \frac{p-1}{2}$.

- $2 \cdot 4 \cdot 6 \cdots (p-1) = 2(1) \cdot 2(2) \cdot 2(3) \cdots 2 \cdot \left(\frac{p-1}{2}\right)$

$$= 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!$$

- $2 \cdot 4 \cdot 6 \cdots (p-1) = 2 \cdot 4 \cdot 6 \cdots \frac{p-1}{2} \cdot \frac{p+3}{2} \; \frac{p+7}{2} \cdots (p-1)$

$$\equiv 2 \cdot 4 \cdot 6 \cdots \frac{p-1}{2} \cdot \left(\frac{p+3}{2} - p\right)\left(\frac{p+7}{2} - p\right) \cdots (p-1-p) \pmod p$$

$$\equiv 2 \cdot 4 \cdot 6 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-3}{2}\right)\left(-\frac{p-7}{2}\right) \cdot (-1) \pmod p$$

$$\equiv (-1)^{*} \cdot \left(\frac{p-1}{2}\right)! \pmod p$$

$(*)$ = number of integers in the list

$$2, 4, 6, 8, \cdots p-1$$

that are larger than $\frac{p-1}{2}$.

$$\Rightarrow \quad 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^{*} \cdot \left(\frac{p-1}{2}\right)! \pmod p$$

$$\Rightarrow \quad 2^{\frac{p-1}{2}} \equiv (-1)^{*} \pmod p \quad \Rightarrow \quad \left(\frac{2}{p}\right) = (-1)^{*}$$

Theorem 21.4 (Quadratic Reciprocity, Part II)

Let p be an odd prime.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Proof: We need to consider 4 cases. Here we only do

$p \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$

Case: $p \equiv 1 \pmod 8$ $\quad p = 8k+1. \quad P = \frac{p-1}{2} = 4k.$

$2, 4, 6, \cdots 4k, 4k+2, \cdots 8k$ (4k numbers)

We need to count how many numbers are $> P = 4k$

That is, $4k+2, 4k+4, \cdots 8k.$

There are $2k$ numbers in total and hence

$$2^{p-1} = 2^{4k} \equiv (-1)^{2k} \pmod p$$
$$\equiv 1 \pmod p$$

$$\Rightarrow \left(\frac{2}{p}\right) = 1$$

Case: $p \equiv 5 \pmod 8$ $\quad p = 8k+5 \quad P = \frac{p-1}{2} = 4k+2.$

We look at

$$2, 4, 6, \cdots 4k+2, \underbrace{4k+4, 4k+6, \cdots 8k+4}_{2k+1 \text{ numbers.}}$$

Therefore, $2^{p-1} = 2^{P} \equiv (-1)^{2k+1} \pmod p$

$$\equiv -1 \pmod p$$

$$\Rightarrow \left(\frac{2}{p}\right) = -1$$

Remark: In the proof of the theorem, the key observation is:

$$2^{\frac{p-1}{2}} \equiv (-1)^{\#} \pmod p$$

where $\#$ = number of integers in the list

$$2, 4, 6, 8, \cdots p-1$$

that are larger than $\frac{p-1}{2}$.

Here is another way to interpret $2, 4, 6, 8, \cdots p-1$:

$$2 \cdot 1, \ 2 \cdot 2, \ 2 \cdot 3, \ \cdots \ 2 \cdot \frac{p-1}{2}.$$

Later, when we consider $\left(\frac{a}{p}\right)$, we will look at:

$$a \cdot 1, \ a \cdot 2, \ a \cdot 3, \ \cdots \ a \cdot \frac{p-1}{2}.$$