Lecture 2

Example: $\left(\frac{35}{41}\right) = ?$

$$\left(\frac{35}{41}\right) \overset{2)}{=} \left(\frac{5}{41}\right)\left(\frac{7}{41}\right) = \left(\frac{41}{5}\right) \times \left(\frac{41}{7}\right)$$

[As $\left(\frac{41}{5}\right)\left(\frac{5}{41}\right) = (-1)^{\frac{(5-1)(41-1)}{4}} = 1$

$\left(\frac{41}{7}\right)\left(\frac{7}{41}\right) = (-1)^{\frac{(7-1)(41-1)}{4}} = 1$] 4)

$$= \left(\frac{1}{5}\right)\left(\frac{-1}{7}\right) = 1 \times (-1)^{\frac{7-1}{2}} = -1$$

1)

Lemma: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof: Try out! (Non-examinable)

Corollary: $p \neq 3$. Then

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \bmod 12 \\ -1 & \text{if } p \equiv \pm 5 \bmod 12 \end{cases}$$

Pf: $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right)$

$\overset{2}{\underset{4}{}}$) $(-1)^{\frac{(3-1)(p-1)}{4}} = (-1)^{\frac{p-1}{2}}$

Thus $\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \bmod 4 \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv -1 \bmod 4 \end{cases}$

But $\left(\frac{p}{3}\right) \overset{2}{\underset{1}{}} \begin{cases} 1, & \text{if } p \equiv 1 \bmod 3 \\ -1, & \text{if } p \equiv -1 \bmod 3 \end{cases}$

As 1 is quad. res. mod 3 but
-1 is quad non-res mod 3.

Combining, we obtain,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 \\ -1 \\ -1 \\ 1 \end{cases} \quad \begin{matrix} \textcircled{1} \\ \textcircled{2} \end{matrix} \quad \begin{matrix} \textcircled{a} \\ \textcircled{a} \end{matrix} \quad \begin{matrix} p \equiv 1 \bmod 4,\ p \equiv 1 \bmod 3 \\ p \equiv 1 \bmod 4,\ p \equiv -1 \bmod 3 \\ p \equiv -1 \bmod 4,\ p \equiv 1 \bmod 3 \\ p \equiv -1 \bmod 4,\ p \equiv -1 \bmod 3 \end{matrix}$$

① $p \equiv \pm 1 \bmod 3$ & $p \equiv \pm 1 \bmod 4 \iff p \equiv \pm 1 \bmod 12$

② $p \equiv \pm 1 \bmod 3$ & $p \equiv \mp 1 \bmod 4 \iff p \equiv \pm 5 \bmod 12$

Using the Chinese remainder theorem.

[Because $4 + (-1)3 = 1$

$x \equiv 4 \times 1 \times 1 + (-1) \times 3 \times (-1) \equiv 7 \bmod 12$

$\equiv 4 \times 1 \times (-1) + (-1) \times 3 \times 1 \equiv -7 \bmod 12$]

Proof of theorem 2)

Let z be a primitive root mod p.

We know from the proof of the last prop that $\exists \ 0 \le i, j \le p-2$ s.t.

$$a \equiv z^i \bmod p.$$
$$b \equiv z^j \bmod p.$$

Recall that $\left(\frac{z^i}{p}\right) = \begin{cases} +1 & \text{if } i \text{ even} \\ -1 & \text{if } i \text{ odd} \end{cases}$

$\Rightarrow \left(\frac{z^i}{p}\right) = (-1)^i$. Similarly, $\left(\frac{z^j}{p}\right) = (-1)^j$

$\Rightarrow \left(\frac{ab}{p}\right) \overset{1)}{=} \left(\frac{z^{i+j}}{p}\right) = (-1)^{i+j} = (-1)^i (-1)^j$

$= \left(\frac{z^i}{p}\right)\left(\frac{z^j}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3) Note that $\left(\underbrace{z^{\frac{p-1}{2}}}_{\| \ x}\right)^2 \equiv 1 \bmod p$ (z is a prim. root $\Uparrow$)

Thus $p \mid x^2 - 1 = (x+1)(x-1)$. But $p \nmid x-1$ (same reason)

So $p \mid x+1 \Rightarrow x \equiv -1 \bmod p$

$$\Rightarrow \left(\frac{-1}{p}\right) = \left(\frac{x}{p}\right) = \left(\frac{z^{\frac{p-1}{2}}}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Euler's criterion: $p \nmid a \Rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$

Proof: Let z be a primitive root mod p & $a \equiv z^j \bmod p$.

Thus $\left(\frac{a}{p}\right) = \left(\frac{z^j}{p}\right) = (-1)^j$.

But $a^{\frac{p-1}{2}} \equiv z^{j\frac{p-1}{2}} \bmod p$

On the other hand, as $z^{p-1} \equiv 1 \bmod p$ & z is a primitive root

$$p \mid \left(z^{\frac{p-1}{2}} - 1\right)\left(z^{\frac{p-1}{2}} + 1\right)$$

$$\Rightarrow z^{\frac{p-1}{2}} \equiv -1 \bmod p$$

$$\Rightarrow z^{j\frac{p-1}{2}} \equiv (-1)^j \bmod p.$$

Rmk: Calculating $\left(\frac{a}{p}\right)$ only helps to determine whether $x^2 \equiv a \bmod p$ solvable.

Solving $x^2 \equiv a \bmod b$

Lemma: 1) Let $b \equiv 3 \bmod 4$. If $\left(\frac{a}{b}\right) = 1$ then $z = a^{\frac{b+1}{4}}$ is a sol^n of

$$x^2 \equiv a \bmod b$$

2) Let $b \equiv 1 \bmod 4$. If $\left(\frac{a}{b}\right) = -1$ then $z = a^{\frac{b-1}{4}}$ is a sol^n of

$$x^2 \equiv -1 \bmod b$$

Pf: 1) $\left(a^{\frac{b+1}{4}}\right)^2 = a^{\frac{b+1}{2}}$

$$= a \cdot a^{\frac{b-1}{2}} \equiv a\left(\frac{a}{b}\right) \bmod b$$

↑ Euler's Criterion

$$\equiv a \bmod b.$$

2) $\left(a^{\frac{b-1}{4}}\right)^2 = a^{\frac{b-1}{2}} \equiv \left(\frac{a}{b}\right) \bmod b.$

↑ Euler's criterion

$$= -1.$$

Exercise: Find $\left(\frac{39}{31}\right)$.

$$\left(\frac{39}{31}\right) = \left(\frac{8}{31}\right) = \left(\frac{2}{31}\right)^3$$

$$= (-1)^{\frac{31^2-1}{8}\times 3} = (-1)^{\frac{30^2+60}{8}}$$

$$= (-1)^{\frac{960}{8}} = (-1)^{120} = 1$$

Exercise: Solve $x^2 \equiv -1 \mod 29$

As $29 \equiv 1 \mod 4$

$x = a^{\frac{29-1}{4}} = a^7$ is a sol^n

where $\left(\frac{a}{29}\right) = -1$

$a = 1$: won't work

$a = 2$: $\left(\frac{2}{29}\right) = (-1)^{\frac{29^2-1}{8}} = (-1)^{\frac{28\cdot 30}{8}}$

$= (-1)^{7\cdot 15} = -1$

So $2^7 \mod 29 = 12 \mod 29$.

is a sol^n.

Exercise:

1) Find a solution of

$$x^2 \equiv -1 \mod 229$$

2) Find $\left(\frac{38}{43}\right)$

3) Prove that $\forall\, n > 3$, $\varphi(n)$ is even.

4) Show that $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) = 0$

Hint: Find number of $x \in \mathbb{Z}/p\mathbb{Z}$ s.t $\left(\frac{x}{p}\right) = 1$

5) Show that $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

where $p \nmid ab$.

6) (*) Hard! Show that $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = -1$