

(3) (a)  $\mu = \#$  neg. residues among  $\{7, \underline{14}, 4, \underline{11}, 1, 8, \underline{15}, 6\}$   
 (Notice that I mark residues  $\geq \frac{17-1}{2} = 8$ )

$= \underline{\underline{3}}$

On the other hand,  $\left(\frac{7}{17}\right) \stackrel{RL}{\equiv} \left(\frac{17}{7}\right) (-1)^{\frac{6 \cdot 16}{4}} = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1 = (-1)^3$ , as expected.

(b) For  $l \in \{1, \dots, \frac{p-1}{2}\}$ , define  $\mu_a(l)$  and  $p_l$  as follows:

$la \equiv (-1)^{\mu_a(l)} p_l \pmod{p}$ , where  $p_l \in \{1, \dots, \frac{p-1}{2}\}$  and  $\mu_a(l) \in \{0, 1\}$

(It's easy to check  $\mu_a(l)$  and  $p_l$  are both well-defined)

By definition,  $\mu = \sum_{l=1}^{\frac{p-1}{2}} \mu_a(l)$ , therefore  $b/c \{p_l\}_{l=1}^{\frac{p-1}{2}} = \{1, 2, \dots, \frac{p-1}{2}\}$

$\prod_{l=1}^{\frac{p-1}{2}} (la) \equiv \prod_{l=1}^{\frac{p-1}{2}} (-1)^{\mu_a(l)} p_l = (-1)^\mu \prod_{l=1}^{\frac{p-1}{2}} p_l \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! \pmod{p} \quad (*)$

But also,  $\prod_{l=1}^{\frac{p-1}{2}} (la) = a^{\frac{p-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} l = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p} \quad (**)$

Comparing (\*) and (\*\*), we prove the claim. □

(c)  $\left(\frac{2}{p}\right) = \#$  of neg. residues in  $S$ , where  $S = \{2r \mid r=1, 2, \dots, \frac{p-1}{2}\}$   
 $= \# \{2r \in S \mid 2r > \frac{p-1}{2}\} \xrightarrow{\text{define}} N$

Consider the following two cases:

(i)  $p \equiv 1, 5 \pmod{8}$ . Then  $N = \{2r \mid 2r > \frac{p-1}{2}\} = \{2r \mid r > \frac{p-1}{4}\} = \{2 \cdot (\frac{p-1}{4} + 1), \dots, 2 \cdot (\frac{p-1}{2})\}$   
 therefore  $\#N = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4} \xrightarrow{\text{odd } p \equiv 5 \pmod{8}} \frac{p-1}{4}$   
 $\xrightarrow{\text{even } p \equiv 1 \pmod{8}} \frac{p-1}{4}$ , so  $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{8} \\ -1 & p \equiv 5 \pmod{8} \end{cases}$

(ii)  $p \equiv 3, 7 \pmod{8}$ . Then  $N = \{2r \mid 2r > \frac{p-1}{2}\} = \{2 \cdot (\frac{p+1}{4}), \dots, 2 \cdot (\frac{p-1}{2})\}$ , so  
 $\#N = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p-3}{4} + 1 \xrightarrow{\text{odd } p \equiv 3 \pmod{8}} \frac{p-3}{4} + 1$   
 $\xrightarrow{\text{even } p \equiv 7 \pmod{8}} \frac{p-3}{4} + 1$ , so  $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 7 \pmod{8} \\ -1 & p \equiv 3 \pmod{8} \end{cases}$

Hence  $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$