Homework 5

Question 1 =>

(a) $a = 78$ $p = 103$

$a = 78 = 2 \cdot 3 \cdot 13$ $\left(\frac{78}{103}\right) = \left(\frac{2}{103}\right) \cdot \left(\frac{3}{103}\right) \cdot \left(\frac{13}{103}\right) =$

$103 \equiv 7 \pmod 8$

$$= (1) \cdot \left(\frac{3}{103}\right) \cdot \left(\frac{13}{103}\right) =$$

$3 \equiv 3 \pmod 4$
$13 \equiv 1 \pmod 4$
$103 \equiv 3 \pmod 4$

$$= -\left(\frac{103}{3}\right) \cdot \left(\frac{103}{13}\right) = -\left(\frac{1}{3}\right) \cdot \left(\frac{12}{13}\right)$$

$$= -(1) \cdot \left(\frac{-1}{13}\right) = -1 \cdot 1 = \boxed{-1}$$

Therefore, 78 is not a square mod 13.

(b) Skip because p is not prime

(c) $a = 12345678901234567890$ $p = 1010101010101010101073$
notice we can reduce $a \pmod p$.

$a_1 = a \pmod p = 224466880022446681 7$
$a_1 = 191 \cdot 4971737 \cdot 2363800151$

$$\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right) = \left(\frac{191}{p}\right) \cdot \left(\frac{4971737}{p}\right) \cdot \left(\frac{2363800151}{p}\right) =$$

$p \equiv 1 \pmod 4$

$$= \left(\frac{p}{191}\right) \cdot \left(\frac{p}{4971737}\right) \cdot \left(\frac{p}{2363800151}\right)$$

$$= \left(\frac{133}{191}\right) \cdot \left(\frac{4839649}{4971737}\right) \cdot \left(\frac{562684460}{2363800151}\right)$$

we can write

$133 = 19 \cdot 7$

$56268460 = 2^2 \cdot 5 \cdot 2813423$ so we have:

$$\left(\frac{19}{191}\right) \cdot \left(\frac{7}{191}\right) \cdot \left(\frac{4839649}{4971737}\right) \cdot \left(\frac{2}{23638001S1}\right)^2 \cdot \left(\frac{5}{23638001S1}\right)$$

$$\cdot \left(\frac{2813423}{23638001S1}\right)$$

$19 \equiv 3 \pmod 4$ so $-\left(\frac{191}{19}\right)$ and $^{-}\left(\frac{7}{191}\right)$

$7 \equiv 3 \pmod 4$

$191 \equiv 3 \pmod 4$

$4971737 \equiv 1 \pmod 4$ so $\left(\frac{4971737}{4839649}\right)$

$2363800151 \equiv 7 \pmod 8$ so $(1)^2$

$2363800151 \equiv 3 \pmod 4$ so $\left(\frac{2363800151}{5}\right)$ and

$5 \equiv 1 \pmod 4$

$2813423 \equiv 3 \pmod 4$ $-\left(\frac{2363800151}{2813423}\right)$

combining these we get:

$$-\left(\frac{191}{19}\right) \cdot -\left(\frac{191}{7}\right) \cdot \left(\frac{4971737}{4839649}\right) \cdot \cancel{(1)^2} \cdot \left(\frac{2363800151}{5}\right)$$

$$\cdot -\left(\frac{2363800151}{2813423}\right) =$$

$$= \left(\frac{-1}{19}\right) \cdot -\left(\frac{2}{7}\right) \cdot \left(\frac{132088}{4839649}\right) \cdot \left(\frac{1}{5}\right) \cdot -\left(\frac{524831}{2813423}\right) =$$

$$= (-1) \cdot -(1) \cdot \left(\frac{132088}{4839649}\right) \cdot \cancel{(1)} \cdot -\left(\frac{524831}{2813423}\right)$$

$$= \cancel{(1)} \cdot \left(\frac{132088}{4839649}\right) \cdot \left(\frac{-524831}{2813423}\right)$$

$$= \left(\frac{132088}{4839649}\right) \cdot -\left(\frac{524831}{2813423}\right)$$

now, we can write

$132088 = 2^3 \cdot 11 \cdot 19 \cdot 79$

$$= \left(\frac{2}{4839649}\right)^3 \cdot \left(\frac{11}{4839649}\right) \cdot \left(\frac{19}{4839649}\right) \cdot \left(\frac{79}{4839649}\right) \cdot \left(\frac{-524831}{2813423}\right)$$

$4839649 \equiv 1 \pmod 8$ $\quad 524831 \equiv 3 \pmod 4$

$4839649 \equiv 1 \pmod 4$ $\quad 2813423 \equiv 3 \pmod 4$ $\quad$ so:

$$= \cancel{(1)}^3 \cdot \left(\frac{4839649}{11}\right) \cdot \left(\frac{4839649}{19}\right) \cdot \left(\frac{4839649}{79}\right) \cdot -\left(\frac{-2813423}{524831}\right)$$

$$= \left(\frac{1}{11}\right) \cdot \left(\frac{7}{19}\right) \cdot \left(\frac{30}{79}\right) \cdot \left(\frac{189268}{524831}\right) = \cancel{(1)} \cdot \left(\frac{7}{19}\right) \cdot \left(\frac{30}{79}\right) \cdot \left(\frac{189268}{524831}\right)$$

$7 \equiv 3 \pmod 4$ $\quad 30 = 2 \cdot 5 \cdot 3$ $\quad 524831 \equiv 7 \pmod 8$

$19 \equiv 3 \pmod 4$ $\quad 189268 = 2^2 \cdot 47317$

$$= -\left(\frac{19}{7}\right) \cdot \left(\frac{2}{79}\right) \cdot \left(\frac{3}{79}\right) \cdot \left(\frac{5}{79}\right) \cdot \left(\frac{2}{524831}\right)^2 \cdot \left(\frac{47317}{524831}\right)$$

$79 \equiv 7 \pmod 8$ $\quad 3 \equiv 3 \pmod 4$ $\quad 47317 \equiv 1 \pmod 4$

$79 \equiv 3 \pmod 4$ $\quad 5 \equiv 1 \pmod 4$

$$= -\left(\frac{5}{7}\right) \cdot \cancel{(1)} \cdot -\left(\frac{79}{3}\right) \cdot \left(\frac{79}{5}\right) \cdot \cancel{(1)}^2 \cdot \left(\frac{524831}{47317}\right)$$

$$-\left(\frac{5}{7}\right)\cdot -\left(\frac{79}{3}\right)\cdot\left(\frac{79}{5}\right)\cdot\left(\frac{524831}{47317}\right) =$$

$$= -\left(\frac{5}{7}\right)\cdot -\left(\frac{1}{3}\right)\cdot\left(\frac{-1}{5}\right)\cdot\left(\frac{4344}{47317}\right) =$$

$7 \equiv 3 \pmod 4$ $\quad$ $4344 = 2^3 \cdot 3 \cdot 181$

$5 \equiv 1 \pmod 4$ $\quad$ $47317 \equiv 5 \pmod 8$

$$= -\left(\frac{7}{5}\right)\cdot -(1)\cdot \cancel{(1)} \cdot \left(\frac{2}{47317}\right)^3 \cdot \left(\frac{3}{47317}\right)\cdot\left(\frac{181}{47317}\right)$$

$$= -\left(\frac{2}{5}\right)\cdot(-1)\cdot(-1)^3 \cdot \left(\frac{3}{47317}\right)\cdot\left(\frac{181}{47317}\right)$$

$$= \cancel{-(-1)\cdot(-1)\cdot(-1)} \cdot \left(\frac{3}{47317}\right)\cdot\left(\frac{181}{47317}\right) =$$

$47317 \equiv 1 \pmod 8$

$$= \left(\frac{47317}{3}\right)\cdot\left(\frac{47317}{181}\right)$$

$$= \left(\frac{1}{3}\right)\cdot\left(\frac{76}{181}\right) = \cancel{(1)}\cdot\left(\frac{76}{181}\right) =$$

$76 = 2^2 \cdot 19$

$181 \equiv 1 \pmod 4$

$181 \equiv 5 \pmod 8$

$$= \left(\frac{2}{181}\right)^2 \cdot \left(\frac{19}{181}\right) = \cancel{(-1)}^2 \cdot \left(\frac{19}{181}\right) =$$

$$= \left(\frac{181}{19}\right) = \left(\frac{10}{19}\right) =$$

$19 \equiv 3 \pmod 8$

$19 \equiv 3 \pmod 4$

$5 \equiv 1 \pmod 4$

$$= \left(\frac{2}{19}\right)\cdot\left(\frac{5}{19}\right) = (-1)\cdot\left(\frac{19}{5}\right)$$

$$= (-1)\cdot\left(\frac{-1}{5}\right) = (-1)\cdot(1)$$

$$\boxed{= -1}$$

Thus a is not a square mod p.