Homework 5 (Section 4.3)

#28(e) $\left(\frac{2817}{4177}\right) = \left(\frac{3^2 \cdot 313}{4177}\right)$ since $2817 = 3^2 \cdot 313$

$= \left(\frac{3^2}{4177}\right)\left(\frac{313}{4177}\right)$ (Prop. 4.5(c))

$= \left(\frac{313}{4177}\right)$ (Prop. 4.5(a))

$= \left(\frac{4177}{313}\right)$ (by LQR since 313, 4177 prime & $4177 = 4 \cdot 1044 + 1 \equiv 1 \pmod 4$)

$= \left(\frac{108}{313}\right)$ (since $13 \cdot 313 + 108 = 4177$ and $4177 \equiv 108 \pmod{313}$)

$= \left(\frac{2^2 \cdot 3^3}{313}\right)$ since $108 = 2^2 \cdot 3^3$

$= \left(\frac{2^2}{313}\right)\left(\frac{3^3}{313}\right)$

$= \left(\frac{3}{313}\right)^3$

$= \left(\frac{3}{313}\right)$ (since $(\pm 1)^3 = (\pm 1)$)

$= \left(\frac{313}{3}\right)$ (by LQR since $313 = 4 \cdot 78 + 1 \equiv 1 \pmod 4$)

$= \left(\frac{1}{3}\right)$ (since $313 = 3 \cdot 104 + 1 \equiv 1 \pmod 3$)

$= 1.$

28(f)

$$\left(\frac{2819}{4177}\right) = \left(\frac{4177}{2819}\right)$$ (by LQR since 2819, 4177 prime & $4177 \equiv 1 \pmod 4$)

$$= \left(\frac{1358}{2819}\right)$$ (since $4177 = 2819 + 1358 \equiv 1358 \pmod{2819}$)

$$= \left(\frac{2 \cdot 7 \cdot 97}{2819}\right)$$

$$= \left(\frac{2}{2819}\right)\left(\frac{7}{2819}\right)\left(\frac{97}{2819}\right).$$

$\left(\frac{2}{2819}\right) = -1$ since $2819 = 352 \cdot 8 + 3 \equiv 3 \pmod 8$.

$\left(\frac{7}{2819}\right) = -\left(\frac{2819}{7}\right)$ by LQR since $2819 \equiv 7 \equiv 3 \pmod 4$.

$= -\left(\frac{5}{7}\right)$ since $2819 = 402 \cdot 7 + 5 \equiv 5 \pmod 7$

$= -\left(\frac{-2}{7}\right)$ since $5 \equiv -2 \pmod 7$

$= -\left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) = \left(\frac{2}{7}\right)$ since $7 \equiv 3 \pmod 4$

$= 1$ since $7 \equiv 7 \pmod 8$.

$\left(\frac{97}{2819}\right) = \left(\frac{2819}{97}\right)$ (by LQR since 97 is also prime, $97 \equiv 1 \pmod 4$.)

$= \left(\frac{6}{97}\right)$ since $2819 = 29 \cdot 97 + 6 \equiv 6 \pmod{97}$.

$= \left(\frac{2}{97}\right)\left(\frac{3}{97}\right) = \left(\frac{3}{97}\right)$ since $97 \equiv 1 \pmod 8$

(p3)

$$\left(\frac{97}{2819}\right) = \left(\frac{3}{97}\right) = \left(\frac{97}{3}\right) \qquad \text{by LQR since } 97 \equiv 1 \pmod 4$$

$$= \left(\frac{1}{3}\right) \qquad \text{since } 97 \equiv 1 \pmod 3$$

$$= 1.$$

So

$$\left(\frac{2819}{4177}\right) = \left(\frac{2}{2819}\right)\left(\frac{7}{2819}\right)\left(\frac{97}{2819}\right) = (-1)(1)(1) = -1.$$

#30

Let p, q be ~~distinct~~ odd primes s.t.

$$p = 4q + 1.$$

Then clearly $p \neq q$ & $p \nmid q$ so that $\left(\frac{q}{p}\right)$ is defined.

Since $p \equiv 1 \pmod 4$,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \qquad \text{by LQR}$$

$$= \left(\frac{4q+1}{q}\right)$$

$$= \left(\frac{1}{q}\right) \qquad \text{since } 4q+1 \equiv 1 \pmod q$$

$$= 1.$$

#34 Assume p, q are odd primes, $p = q + 4a$, $a \neq 0$, & $a \in \mathbb{Z}$.

Since $a \neq 0$, $p \neq q$ & it follows that $p \nmid q$ & $q \nmid p$ so that $\left(\frac{q}{p}\right)$, $\left(\frac{p}{q}\right)$ are defined.

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) \quad \text{since } q + 4a \equiv 4a \pmod{q}$$

$$= \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right) \quad \text{since } 4 = 2^2.$$

By LQR

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

since then $q \equiv p \equiv 3 \pmod 4$.

& $\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right)$

$$\left(\frac{a}{q}\right) = \left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right)$$

$$= \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \quad \text{since } p \equiv q \pmod 4$$

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

$$= \left(\frac{p+4a}{p}\right) \quad (\text{since } -q = 4a - p)$$

$$= \left(\frac{4a}{p}\right) \quad \text{since } -p + 4q \equiv 4a \pmod p$$

$$= \left(\frac{4}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right) \quad \text{since } 4 = 2^2.$$

Here $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$.

#36(a) Let p be any odd prime $p \neq 5$.

x	$x^2 \pmod 5$
± 1	1
± 2	4

So $1, 4$ are q.r. $(\bmod 5)$ & $2, 3$ are q.n.r. $(\bmod 5)$.

Since $5 \equiv 1 \pmod 4$,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \quad \text{by LQR}$$

$$= 1 \quad \text{if } p \equiv 1 \text{ or } 4 \pmod 5$$

Hence 5 is q.r. mod p iff p is a prime congruent to 1 or 4 $(\bmod 5)$.

#36 (c). Let p be any odd prime $p \neq 7$.

x	$x^2 \pmod 7$
± 1	1
± 2	4
± 3	$9 \equiv 2$.

The q.r. mod 7 are $1, 2, 4$

The q.n.r. mod 7 are $3, 5, 6$

$$\left(\frac{2}{7}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 2, 4 \pmod 7 \\ -1 & \text{if } p \equiv 3, 5, 6 \pmod 7 \end{cases}$$

(p6)

By the LQR (since $7 \equiv 3 \pmod 4$)

$$\left(\frac{7}{p}\right) = \begin{cases} \left(\frac{p}{7}\right) & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{7}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Hence $\left(\frac{\pm 1}{p}\right) = +1$ if $p \equiv 1 \pmod 4$ & $p \equiv 1, 2$ or $4 \pmod 7$

OR $p \equiv 3 \pmod 4$ & $p \equiv 3, 5, 6 \pmod 7$.

We use CRT to solve

$$(*) \begin{cases} x \equiv b_1 \pmod 4 \\ x \equiv b_2 \pmod 7 \end{cases}$$

$M = 28$, $M_1 = 7$, $M_2 = 4$.

$M_1 x_1 = 7x_1 \equiv 1 \pmod 4$ & take $x_1 = -1$.

$M_2 x_2 = 4x_2 \equiv 1 \pmod 7$ & take $x_2 = 2$.

So sol to $(*)$ is

$$x \equiv M_1 b_1 x_1 + M_2 b_2 x_2 = -7b_1 + 8b_2 \pmod{28}.$$

We consider $(b_1, b_2) = (1,1), (1,2), (1,4), (-1,3), (-1,5), (-1,6)$.

$x \equiv 1, 9, 25, 31, 47, 55 \pmod{28}$

$\equiv 1, 9, 25, 3, 19, 27 \pmod{28}$

i.e. $x \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$.

#37

(a) $105 = 3 \cdot 5 \cdot 7$

Then

$$\left(\frac{-77}{105}\right) = \left(\frac{-77}{3}\right)\left(\frac{-77}{5}\right)\left(\frac{-77}{7}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{1}{5}\right)\left(\frac{5}{7}\right)$$

$$= (-1)(1)(-1) = 1$$

$133 = (7)(19)$.

$$\left(\frac{87}{133}\right) = \left(\frac{87}{7}\right)\left(\frac{87}{19}\right)$$

$$= \left(\frac{3}{7}\right)\left(\frac{11}{19}\right)$$

$$= -\left(\frac{11}{19}\right)$$

$$= -\left(\frac{-8}{19}\right) \quad \text{since } 11 \equiv -8 \ (19)$$

$$= -\left(\frac{-1}{19}\right)\left(\frac{2}{19}\right)^3$$

$$= (-1)(-1)\left(-1\right)^3 \quad \text{since } 19 \equiv 3 \ (\text{mod } 4),\ 19 \equiv 3 \ (\text{mod } 8)$$

$$= -1$$

$129 = 3 \cdot 43$. So

$$\left(\frac{91}{129}\right) = \left(\frac{91}{3}\right)\left(\frac{91}{43}\right)$$
$$= \left(\frac{1}{3}\right)\left(\frac{5}{43}\right)$$
$$= \left(\frac{5}{43}\right)$$
$$= \left(\frac{43}{5}\right) \quad \text{(by LQR since } 5 \equiv 1 \pmod 4\text{)}$$
$$= \left(\frac{3}{5}\right) = -1.$$

(b) Suppose n is a positive odd integer, $n > 1$ & $n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ is a prime factorization, $a \in \mathbb{Z}$ & $(a, n) = 1$. Suppose a is q.r. mod n. So $x^2 \equiv a \pmod n$ for some $x \in \mathbb{Z}$. So $n \mid (x^2 - a)$ & $p_j \mid (x^2 - a)$ for each j. So for each j $x^2 \equiv a \pmod{p_j}$ and $\left(\frac{a}{p_j}\right) = 1$.

Hence $\left(\frac{a}{n}\right) = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{b_j} = \prod_{j=1}^{r} 1^{b_j} = 1.$

We show converse does not hold.

Let $a = 2$, $n = 9$. Then

$$\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = 1.$$

But 2 q.n.r. mod 9 since if $x^2 \equiv 2 \pmod 9$, $x \in \mathbb{Z}$

then $x^2 \equiv 2 \pmod 3$ which is impossible.