Complete Solutions to Exercise 7.5

1. (i) As 3 and 7 are prime numbers so $(3/7)$ is a Legendre symbol:

$$\left(\frac{3}{7}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1 \qquad \left[\text{Because } 7\equiv 1\pmod 3\right]$$

(ii) We need to work out $\left(\frac{3}{49}\right)$. The prime decomposition of $49=7^2$ so we have

$$\left(\frac{3}{49}\right)=\left(\frac{3}{7^2}\right)=\left(\frac{3}{7}\right)\times\left(\frac{3}{7}\right)$$

By part (i) we have $\left(\frac{3}{7}\right)=-1$ so $\left(\frac{3}{49}\right)=\left(\frac{3}{7}\right)\times\left(\frac{3}{7}\right)=-1\times(-1)=1$.

Note that although $(3/49)=1$ but there are *no* solutions to $x^2\equiv 3\pmod{49}$ because by part (i) we have $x^2\equiv 3\pmod 7$ has *no* solutions.

2. (a) We need to find $\left(\frac{26}{27}\right)$. Firstly note that $26\equiv -1\pmod{27}$ and $27=3^3$ therefore

$$\left(\frac{26}{27}\right)=\left(\frac{-1}{3^3}\right)=\left(\frac{-1}{3}\right)^3 \qquad (\ddagger)$$

Now we use the test for -1 modulo p where p is a prime:

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

In our case we have $p=3\equiv 3\pmod 4$ so by using this result $\left(\frac{-1}{3}\right)=-1$. Substituting this into (‡) gives

$$\left(\frac{26}{27}\right)=(-1)^3=-1$$

(b) Writing the prime decomposition of the integers in the Jacobi symbol $\left(\frac{12}{115}\right)$ is

$$12=2^2\times 3 \text{ and } 115=5\times 23$$

We have

$$\left(\frac{12}{115}\right)=\left(\frac{2^2\times 3}{115}\right)=\underbrace{\left(\frac{2^2}{115}\right)}_{=1}\times\left(\frac{3}{115}\right)=\left(\frac{3}{115}\right)$$

Using $115=5\times 23$ we have

$$\left(\frac{3}{115}\right)=\left(\frac{3}{5\times 23}\right)=\left(\frac{3}{5}\right)\times\left(\frac{3}{23}\right) \qquad (*)$$

Now on the right hand side we have Legendre symbols so we can use LQR and its corollary to evaluate $\left(\frac{3}{5}\right)$ and $\left(\frac{3}{23}\right)$:

$$\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right) \qquad \left[\text{Because } 5\equiv 2 \pmod 3\right]$$

Similarly for the other term on the right hand side of (*) we have

$$\left(\frac{3}{23}\right)=-\left(\frac{23}{3}\right)=-\left(\frac{2}{3}\right) \qquad \left[\text{Because } 23\equiv 2 \pmod 3\right]$$

We need to evaluate the Jacobi symbol $(2/3)$ in each case. *How?*By applying

$$\text{(7.15)} \qquad \left(\frac{2}{p}\right)=\begin{cases} 1 & \text{if } p\equiv \pm 1 \pmod 8 \\ -1 & \text{if } p\equiv \pm 3 \pmod 8 \end{cases}$$

With $p=3\equiv 3 \pmod 4$ we have $\left(\frac{2}{3}\right)=-1$. Substituting this into (*) gives

$$\left(\frac{3}{115}\right)=\left(\frac{3}{5}\right)\times\left(\frac{3}{23}\right)=\left(\frac{2}{3}\right)\times\left[-\left(\frac{2}{3}\right)\right]=-1\times\left[-(-1)\right]=-1$$

(c) We need to evaluate $\left(\frac{128}{1001}\right)$. The prime factorization of both these numbers is:

$$128=2^7 \text{ and } 1001=7\times 11\times 13$$

Therefore

$$\left(\frac{128}{1001}\right)=\left(\frac{2^7}{7\times 11\times 13}\right)=\left(\frac{2^7}{7}\right)\times\left(\frac{2^7}{11}\right)\times\left(\frac{2^7}{13}\right)$$

Applying Proposition (7.22) part (c):

$$\left(\frac{a\times b}{n}\right)=\left(\frac{a}{n}\right)\times\left(\frac{b}{n}\right)$$

To the above calculation yields

$$\left(\frac{128}{1001}\right)=\left(\frac{2}{7}\right)^7\times\left(\frac{2}{11}\right)^7\times\left(\frac{2}{13}\right)^7 \qquad (\dagger)$$

Again using the test for residue 2 modulo *p* where *p* is prime:

$$\text{(7.15)} \qquad \left(\frac{2}{p}\right)=\begin{cases} 1 & \text{if } p\equiv \pm 1 \pmod 8 \\ -1 & \text{if } p\equiv \pm 3 \pmod 8 \end{cases}$$

For each of the cases in (†) we have

$$\left(\frac{2}{7}\right)^7 \underbrace{\equiv}_{\text{because } 7\equiv -1 \pmod 8} 1^7=1,\quad \left(\frac{2}{11}\right)^7 \underbrace{\equiv}_{\text{because } 11\equiv 3 \pmod 8} (-1)^7=-1 \text{ and } \left(\frac{2}{13}\right)^7 \underbrace{\equiv}_{\text{because } 13\equiv -3 \pmod 8} (-1)^7=-1$$

Putting these into (†) gives

$$\left(\frac{128}{1001}\right)=1\times(-1)\times(-1)=1$$

Since we have two Legendre symbols equal to -1 so 128 is a quadratic non – residue of 1001.

(d) Using the given factorization we have

$$\left(\frac{72}{5183}\right)=\left(\frac{72}{71\times 73}\right)=\left(\frac{72}{71}\right)\times\left(\frac{72}{73}\right)$$

Since $72\equiv 1 \pmod{71}$ and $72\equiv -1 \pmod{73}$ we can use (7.22) part (a):

$$a \equiv b \pmod{n} \text{ implies } \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

$$\left(\frac{72}{5183}\right) = \left(\frac{72}{71}\right) \times \left(\frac{72}{73}\right) = \left(\frac{1}{71}\right) \times \left(\frac{-1}{73}\right) \qquad (*)$$

Clearly $(1/71) = 1$ because 1 is a quadratic residue. For the residue -1 we use

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

In view of $p = 73 \equiv 1 \pmod{4}$ we have $\left(\frac{-1}{73}\right) = 1$. Putting $\left(\frac{1}{71}\right) = \left(\frac{-1}{73}\right) = 1$ into (*) gives

$$\left(\frac{72}{5183}\right) = \left(\frac{1}{71}\right) \times \left(\frac{-1}{73}\right) = 1 \times 1 = 1$$

3. Since both the integers in the Jacobi symbol in this question are odd and relatively prime we can use Corollary (7.26) :

(7.26) $$\left(\frac{m}{n}\right) = \begin{cases} (n/m) & \text{if } m \equiv 1 \pmod{4} \text{ or } n \equiv 1 \pmod{4} \\ -(n/m) & \text{if } m \equiv n \equiv 3 \pmod{4} \end{cases}$$

(a) We are given the Jacobi symbol $\left(\frac{11}{211}\right)$.

By Corollary (7.26) with $11 \equiv 211 \equiv 3 \pmod{4}$ we have

$$\left(\frac{11}{211}\right) = -\left(\frac{211}{11}\right)$$

Using modular arithmetic $211 \equiv 2 \pmod{11}$ so by (7.22) part (a):

$$a \equiv b \pmod{n} \text{ implies } \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

We have

$$\left(\frac{11}{211}\right) = -\left(\frac{211}{11}\right) = -\left(\frac{2}{11}\right) \qquad (\ddagger)$$

As $p = 11 \equiv 3 \pmod{8}$ so by

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

We have $\left(\frac{2}{11}\right) = -1$. Substituting this into (‡) yields

$$\left(\frac{11}{211}\right) = -\left(\frac{2}{11}\right) = -(-1) = 1$$

Hence $\left(\frac{11}{211}\right) = 1$.

(b) We need to evaluate $\left(\frac{17}{135}\right)$. With $m = 17 \equiv 1 \pmod{4}$ we have by Corollary (7.26);

$$\left(\frac{17}{135}\right)=\left(\frac{135}{17}\right)$$

As $135\equiv 16\,(\text{mod}\,17)$ therefore by (7.22) part (a):

$$a\equiv b\,(\text{mod}\,n)\ \text{ implies }\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$$

We have $\left(\frac{17}{135}\right)=\left(\frac{135}{17}\right)\underbrace{\equiv}_{\text{because }135\equiv 16\,(\text{mod}\,17)}\left(\frac{16}{17}\right)=\left(\frac{4^2}{17}\right)$. By (7.22) part (c):

$$\left(a^2/n\right)=1$$

Hence $\left(\frac{17}{135}\right)=\left(\frac{4^2}{17}\right)=1$.

(c) We are asked to evaluate the Jacobi symbol $\left(\frac{231}{1025}\right)$. Both of these are composite odd integers so we can use Corollary:

$$(7.26)\qquad \left(\frac{m}{n}\right)=\begin{cases}(n/m) & \text{if } m\equiv 1\,(\text{mod}\ 4)\ \text{ or } n\equiv 1\,(\text{mod}\ 4)\\ -(n/m) & \text{if } m\equiv n\equiv 3\,(\text{mod}\ 4)\end{cases}$$

With $m=1025\equiv 1\,(\text{mod}\ 4)$

$$\left(\frac{231}{1025}\right)=\left(\frac{1025}{231}\right)$$

Since $1025\equiv 101\,(\text{mod}\ 231)$ so by (7.22) part (a):

$$a\equiv b\,(\text{mod}\,n)\ \text{ implies }\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$$

We have

$$\left(\frac{231}{1025}\right)=\left(\frac{1025}{231}\right)=\left(\frac{101}{231}\right)\qquad (\dagger)$$

Using Corollary (7.26) again with $101\equiv 1\,(\text{mod}\ 4)$

$$\left(\frac{101}{231}\right)=\left(\frac{231}{101}\right)$$

Using modular arithmetic we have $231\equiv 29\,(\text{mod}\,101)$. By (7.22) part (a) again:

$$\left(\frac{231}{101}\right)=\left(\frac{29}{101}\right)\underbrace{=}_{\substack{\text{by (7.17)}\\ \text{as 101 and 29 are prime}}}\left(\frac{101}{29}\right)=\left(\frac{14}{29}\right)\qquad \left[\text{Because } 101\equiv 14\,(\text{mod } 29)\right]$$

Since 14 is even so we cannot use the above corollary.
Factorizing $14=2\times 7$ therefore

$$\left(\frac{14}{29}\right)=\left(\frac{2\times 7}{29}\right)=\left(\frac{2}{29}\right)\times\left(\frac{7}{29}\right)\qquad (*)$$

By now you must know the formula for testing 2 modulo *p*:

$$(7.15)\qquad \left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv \pm 1\,(\text{mod}\,8)\\ -1 & \text{if } p\equiv \pm 3\,(\text{mod}\,8)\end{cases}$$

Our prime is $p = 29 \equiv 5 \equiv -3 \pmod 8$ so by this formula $\left(\frac{2}{29}\right) = -1$.

Working out the last Legendre symbol on the right hand side of (*)

$$\left(\frac{7}{29}\right) = \left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1$$

Substituting these into (*) yields $\left(\frac{14}{29}\right) = (-1) \times 1 = -1$. By (†) and (*) we have

$$\left(\frac{231}{1025}\right) = \left(\frac{14}{29}\right) = -1$$

(d) We need to evaluate $\left(\frac{333}{403}\right)$. Using Corollary:

(7.26) $$\left(\frac{m}{n}\right) = \begin{cases} (n/m) & \text{if } m \equiv 1 \pmod 4 \text{ or } n \equiv 1 \pmod 4 \\ -(n/m) & \text{if } m \equiv n \equiv 3 \pmod 4 \end{cases}$$

With $n = 333 \equiv 1 \pmod 4$ we have

$$\left(\frac{333}{403}\right) = \left(\frac{403}{333}\right)$$

We have $403 \equiv 70 \pmod{333}$ so by (7.22) part (a):

$$a \equiv b \pmod n \text{ implies } \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

We have $\left(\frac{403}{333}\right) = \left(\frac{70}{333}\right)$. Factorizing these numbers $70 = 2 \times 5 \times 7$ and $333 = 3^2 \times 37$.

By applying the Jacobi symbol definition (7.21):

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \times \left(\frac{a}{p_2}\right)^{k_2} \times \cdots \times \left(\frac{a}{p_m}\right)^{k_m}$$

We have

$$\left(\frac{70}{333}\right) = \left(\frac{2 \times 5 \times 7}{3^2 \times 37}\right) = \left(\frac{2 \times 5 \times 7}{3}\right)^2 \times \left(\frac{2 \times 5 \times 7}{37}\right) \qquad (*)$$

Clearly $\left(\frac{2 \times 5 \times 7}{3}\right)^2 = 1$. Only need to evaluate $\left(\frac{2 \times 5 \times 7}{37}\right)$. By (7.22) part (c):

$$\left(\frac{a \times b}{n}\right) = \left(\frac{a}{n}\right) \times \left(\frac{b}{n}\right)$$

We have

$$\left(\frac{2 \times 5 \times 7}{37}\right) = \left(\frac{2}{37}\right) \times \left(\frac{5}{37}\right) \times \left(\frac{7}{37}\right) \qquad (‡)$$

The right hand side of (‡) are all Legendre symbols. We need to evaluate each of these. By

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

With prime $p = 37 \equiv 5 \equiv -3 \left(\text{mod } 8\right)$ we have

$$\left(\frac{2}{37}\right) = -1$$

Working out the middle Legendre symbol on the right hand side of (‡):

$$\left(\frac{5}{37}\right) \underbrace{\equiv}_{\text{By (7.17)}} \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) \qquad \left[\text{Because } 37 \equiv 2 \left(\text{mod } 5\right)\right]$$

$$= -1 \qquad \left[\text{Because } p = 5 \equiv 5 \equiv -3 \left(\text{mod } 8\right)\right]$$

Evaluating the last Legendre symbol on the right hand side of (‡):

$$\left(\frac{7}{37}\right) \underbrace{\equiv}_{\text{By (7.17)}} \left(\frac{37}{7}\right) = \left(\frac{2}{7}\right) \qquad \left[\text{Because } 37 \equiv 2 \left(\text{mod } 7\right)\right]$$

$$= 1 \qquad \left[\text{Because } p = 7 \equiv 7 \equiv -1 \left(\text{mod } 8\right)\right]$$

Substituting all these evaluations into (‡) gives

$$\left(\frac{2 \times 5 \times 7}{37}\right) = \left(-1\right) \times \left(-1\right) \times 1 = 1$$

Hence $\left(\frac{333}{403}\right) = 1$.

4. We are asked to prove $\left(\frac{a^k}{n}\right) = \left(\frac{a}{n}\right)^k$ where k is a positive integer. *How?*

Use mathematical induction.

Proof.

For the base case $k = 2$ we need to show $\left(\frac{a^2}{n}\right) = \left(\frac{a}{n}\right)^2$. Applying (7.22) part (c):

$$\boxed{\left(\frac{a \times b}{n}\right) = \left(\frac{a}{n}\right) \times \left(\frac{b}{n}\right)}$$

With $a = a$ and $b = a$ we have our base case

$$\left(\frac{a^2}{n}\right) = \left(\frac{a}{n}\right) \times \left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^2$$

Assume the result is true for $m = k$:

$$\left(\frac{a^m}{n}\right) = \left(\frac{a}{n}\right)^m \qquad (*)$$

We are required to prove that $\left(\frac{a^{m+1}}{n}\right) = \left(\frac{a}{n}\right)^{m+1}$. Consider the left hand side of this

$$\left(\frac{a^{m+1}}{n}\right) = \left(\frac{a^m \times a}{n}\right) = \left(\frac{a^m}{n}\right) \times \left(\frac{a}{n}\right) \qquad \left[\text{By } \left(7.22\right) \text{ part } \left(\text{c}\right)\right]$$

$$= \underbrace{\left(\frac{a}{n}\right)^m}_{\text{by } (*)} \times \left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^{m+1}$$

By mathematical induction we have our result.

■

5. We are asked to prove Corollary (7.26):

$$\left(\frac{m}{n}\right)=\begin{cases}(n/m) & \text{if } m\equiv 1\pmod 4 \text{ or } n\equiv 1\pmod 4\\ -(n/m) & \text{if } m\equiv n\equiv 3\pmod 4\end{cases}$$

Proof.
We consider the two different cases.
<u>Case 1</u>:

First we prove that if $m\equiv 1\pmod 4$ or $n\equiv 1\pmod 4$ then $\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)$.

Without loss of generality assume $m\equiv 1\pmod 4$. There is a positive integer k such that $m=4k+1$. We are going to use GLQR (7.25) which means we need to evaluate the index $\left(\frac{m-1}{2}\right)$. Substituting $m=4k+1$ into this gives

$$\left(\frac{m-1}{2}\right)=\left(\frac{4k+1-1}{2}\right)=2k$$

By GLQR

(7.25) $$\left(\frac{n}{m}\right)\times\left(\frac{m}{n}\right)=(-1)^{\left(\frac{n-1}{2}\right)\times\left(\frac{m-1}{2}\right)}$$

We have $\left(\frac{n}{m}\right)\times\left(\frac{m}{n}\right)=(-1)^{\left(\frac{n-1}{2}\right)\times 2k}=1$ because we have an even index. Recall $\left(\frac{m}{n}\right)$ and $\left(\frac{n}{m}\right)$ are Jacobi symbols so they are ±1. We have

$$\left(\frac{n}{m}\right)\times\left(\frac{m}{n}\right)=1 \text{ implies } \left(\frac{n}{m}\right)=\left(\frac{m}{n}\right)=1 \text{ or } \left(\frac{n}{m}\right)=\left(\frac{m}{n}\right)=-1$$

Either case we have our required result.
<u>Case 2</u>:

Similarly we prove the case for $m\equiv n\equiv 3\pmod 4$. There are positive integers k and k' such that $n=4k+3,\ m=4k'+3$. Substituting these into indices of GLQR:

$$\frac{n-1}{2}=\frac{4k+3-1}{2}=2k+1 \text{ and } \frac{m-1}{2}=\frac{4k'+3-1}{2}=2k'+1$$

By GLQR (7.25) we have

$$\left(\frac{n}{m}\right)\times\left(\frac{m}{n}\right)=(-1)^{\left(\frac{n-1}{2}\right)\times\left(\frac{m-1}{2}\right)}=(-1)^{(2k+1)(2k'+1)}=-1 \qquad [\text{Because odd index}]$$

Therefore $\left(\frac{n}{m}\right)\times\left(\frac{m}{n}\right)=-1$. Arguing along the lines of the first case we have

$$\left(\frac{n}{m}\right)=1 \text{ and } \left(\frac{m}{n}\right)=-1 \text{ or } \left(\frac{n}{m}\right)=-1 \text{ and } \left(\frac{m}{n}\right)=1$$

Hence $\left(\frac{m}{n}\right)=-\left(\frac{n}{m}\right)$.

This completes both cases.

■

6. (a) We need to prove that $\left(\frac{-1}{n}\right)=\begin{cases} 1 & \text{if } n\equiv 1\pmod 4 \\ -1 & \text{if } n\equiv 3\pmod 4 \end{cases}$.

Proof.
By Proposition (7.24) part (a):

$$\boxed{\left(\frac{-1}{n}\right)=(-1)^{\frac{1}{2}(n-1)}}$$

For the case $n\equiv 1\pmod 4$ there is a positive integer *k* such that

$$n=4k+1$$

Substituting this into the index of (7.24) part (a) we have

$$\frac{1}{2}(n-1)=\frac{1}{2}(4k+1-1)=2k$$

Putting this into $\left(\frac{-1}{n}\right)=(-1)^{\frac{1}{2}(n-1)}$ yields

$$\left(\frac{-1}{n}\right)=(-1)^{2k}=1 \qquad [\text{Because we have an even index}]$$

Similarly for the case $n\equiv 3\pmod 4$ there is a positive integer *m* such that

$$n=4m+3$$

Hence

$$\left(\frac{-1}{n}\right)=(-1)^{\frac{1}{2}(n-1)}=(-1)^{\frac{1}{2}(4m+3-1)}=(-1)^{\frac{1}{2}(4m+2)}=(-1)^{2m+1}=-1 \qquad [\text{Odd index}]$$

This completes our proof for this part.

■

(b) For part (b) we have to prove $\left(\frac{2}{n}\right)=\begin{cases} 1 & \text{if } n\equiv \pm 1\pmod 8 \\ -1 & \text{if } n\equiv \pm 3\pmod 8 \end{cases}$.

Proof.
To prove this result we use Proposition (7.24) part (b):

$$\boxed{\left(\frac{2}{n}\right)=(-1)^{\frac{1}{8}(n^2-1)}}$$

We consider the index of -1;

$$\frac{1}{8}(n^2-1)=\frac{1}{8}(n-1)(n+1) \qquad (*)$$

<u>Case 1</u>

If $n\equiv 1\pmod 8$ then there is a positive integer *k* such that

$$n=8k+1$$

Putting this into (*) yields

$$\frac{1}{8}(n-1)(n+1)=\frac{1}{8}(8k+1-1)(8k+1+1)=k(8k+2)=2k(4k+1) \qquad [\text{Even}]$$

Therefore $\left(\frac{2}{n}\right)=(-1)^{\frac{1}{8}(n^2-1)}=1$.

<u>Case 2</u>

Similarly if $n \equiv -1 \pmod 8$ we have an even index so $\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} = 1$.

Case 3

If $n \equiv 3 \pmod 8$ then there is a positive integer *m* such that

$$n = 8m + 3$$

Putting this into (*) yields

$$\begin{aligned} \frac{1}{8}(n-1)(n+1) &= \frac{1}{8}(8m+3-1)(8m+3+1) \\ &= \frac{1}{8}(8m+2)(8m+4) \\ &= \frac{1}{8}\left([8m]^2 + 48m + 8\right) = 8m^2 + 6m + 1 = 2\left(m^2 + 3m\right) + 1 \qquad [\text{Odd}] \end{aligned}$$

Therefore $\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} = -1$.

Case 4

If $n \equiv -3 \pmod 8$ we have an odd index so $\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} = -1$.

We have shown for all four cases the required result.

■

7. (i) We are asked to show that $(n-a)^2 \equiv a^2 \pmod n$.

Proof.

Expanding the left hand side gives

$$(n-a)^2 \equiv n^2 - 2an + a^2 \equiv 0 + 0 + a^2 \equiv a^2 \pmod n \qquad \left[\text{Because } n^2 \text{ and } 2an \text{ are multiples of } n\right]$$

Hence we have our required result.

■

(ii) We need to find the quadratic residues of 35. By the result of part (i) we only need to calculate the first half of the residues, $\frac{35-1}{2} = 17$;

$$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 9,\ 4^2 \equiv 16,\ 5^2 \equiv 25,\ 6^2 \equiv 1,\ 7^2 \equiv 49 \equiv 14,\ 8^2 \equiv 64 \equiv 29,\ 9^2 \equiv 81 \equiv 11,$$
$$10^2 \equiv 30,\ 11^2 \equiv 1,\ 12^2 \equiv 4,\ 13^2 \equiv 169 \equiv 29,\ 14^2 \equiv 21,\ 15^2 \equiv 15,\ 16^2 \equiv 11,\ 17^2 \equiv 9 \pmod{35}$$

The quadratic residues of 35 are

1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30

8. We are asked to prove $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \times \left(\frac{a}{n}\right)$.

Proof.

Let $m = \prod_{j=1}^{r} p_j^{\alpha_j}$ and $n = \prod_{i=1}^{s} q_i^{\beta_i}$ be the prime decompositions of *m* and *n*. By the Jacobi symbol definition (7.21) we have

$$\left(\frac{a}{mn}\right)=\prod_{j=1}^{r}\left(\frac{a}{p_j}\right)^{\sim_j}\times\prod_{i=1}^{s}\left(\frac{a}{q_i}\right)^{\;_i}$$

$$=\left(\frac{a}{m}\right)\times\left(\frac{a}{n}\right)$$

This is our required result.

■

9. We need to show $\left(\frac{a}{p^{2m}}\right)=1$.

Proof.

We have

$$\left(\frac{a}{p^{2m}}\right)=\left(\frac{a}{p}\right)^{2m}=(\pm1)^{2m}=1$$

Hence we have our result.

■

10. (a) We are asked to show that $\left(\frac{a-1}{2}\right)+\left(\frac{b-1}{2}\right)\equiv\left(\frac{ab-1}{2}\right)(\text{mod } 2)$.

Proof.

We are given that *a* and *b* are odd so there are integers *m* and *n* such that

$$a=2m+1 \text{ and } b=2n+1$$

Evaluating the left hand side of the given congruence

$$\left(\frac{a-1}{2}\right)+\left(\frac{b-1}{2}\right)\equiv\left(\frac{2m+1-1}{2}\right)+\left(\frac{2n+1-1}{2}\right)\equiv m+n\,(\text{mod } 2)$$

Evaluating the right hand side of the given congruence

$$\left(\frac{ab-1}{2}\right)\equiv\left(\frac{(2m+1)(2n+1)-1}{2}\right)\equiv\frac{4mn+2m+2n+1-1}{2}$$

$$\equiv 2mn+m+n\equiv m+n\,(\text{mod } 2)$$

Hence we have our given result.

■

(b) We need to prove that $\left(\frac{a^2-1}{8}\right)+\left(\frac{b^2-1}{8}\right)\equiv\left(\frac{[ab]^2-1}{8}\right)(\text{mod } 2)$.

Proof.

As for part (a) let $a=2m+1$ and $b=2n+1$ where *m* and *n* are integers. Examining the left hand side of the given congruence

$$\left(\frac{a^2-1}{8}\right)+\left(\frac{b^2-1}{8}\right)\equiv\left(\frac{(2m+1)^2-1}{8}\right)+\left(\frac{(2n+1)^2-1}{8}\right)$$

$$\equiv\frac{4m^2+4m}{8}+\frac{4n^2+4n}{8}\equiv\frac{4m^2+4m+4n^2+4n}{8}\,(\text{mod } 8)$$

Working out the right hand side of the given congruence

$$\begin{aligned}
\frac{[ab]^2-1}{8} &\equiv \frac{[(2m+1)(2n+1)]^2-1}{8} \\
&\equiv \frac{(2m+1)^2(2n+1)^2-1}{8} \\
&\equiv \frac{(4m^2+4m+1)(4n^2+4n+1)-1}{8} \\
&\equiv \frac{16m^2n^2+16m^2n+4m^2+16mn^2+16mn+4m+4n^2+4n+1-1}{8} \\
&\equiv \frac{16\left[m^2n^2+m^2n+mn^2+mn\right]}{8}+\frac{4m^2+4m+4n^2+4n}{8} \\
&\equiv \underbrace{2\left[m^2n^2+m^2n+mn^2+mn\right]}_{\equiv 0 \pmod 2 \text{ because it is a multiple of 2}}+\frac{4m^2+4m+4n^2+4n}{8} \equiv \frac{4m^2+4m+4n^2+4n}{8} \pmod 2
\end{aligned}$$

Hence we have our required result.

■

11. (a) We are required to prove $\sum_{j=1}^{m} k_j \times \frac{(p_j-1)}{2} \equiv \frac{n-1}{2} \pmod 2$ where $n=\prod_{j=1}^{m} p_j^{k_j}$.

Proof.

Expanding the left hand side of the given congruence:

$$\sum_{j=1}^{m} k_j \times \frac{(p_j-1)}{2} = \left[k_1 \times \frac{(p_1-1)}{2}\right]+\left[k_2 \times \frac{(p_2-1)}{2}\right]+\cdots+\left[k_m \times \frac{(p_m-1)}{2}\right] \qquad (‡)$$

Writing the first term on the right hand side of (‡) as an addition:

$$k_1 \times \frac{(p_1-1)}{2} = \underbrace{\frac{(p_1-1)}{2}+\frac{(p_1-1)}{2}+\cdots+\frac{(p_1-1)}{2}}_{k_1 \text{ copies}} \qquad (*)$$

By the result of the previous question:

$$\boxed{\left(\frac{a-1}{2}\right)+\left(\frac{b-1}{2}\right) \equiv \left(\frac{ab-1}{2}\right) \pmod 2}$$

Applying this to (*) yields

$$k_1 \times \frac{(p_1-1)}{2} = \underbrace{\frac{(p_1-1)}{2}+\frac{(p_1-1)}{2}+\cdots+\frac{(p_1-1)}{2}}_{k_1 \text{ copies}} \equiv \frac{p_1^{k_1}-1}{2} \pmod 2$$

Similarly we have

$$k_j \times \frac{(p_j-1)}{2} \equiv \frac{p_j^{k_j}-1}{2} \pmod 2 \text{ for } j=2,\ 3,\ \cdots,\ m$$

Putting each of these into (‡) gives

$$\begin{aligned}
\sum_{j=1}^{m} k_j \times \frac{(p_j-1)}{2} &\equiv \left[\frac{p_1^{k_1}-1}{2}\right]+\left[\frac{p_2^{k_2}-1}{2}\right]+\cdots+\left[\frac{p_m^{k_m}-1}{2}\right] \\
&\equiv \left[\frac{p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}-1}{2}\right] \equiv \left[\frac{n-1}{2}\right] \pmod 2 \quad \left[\text{Because } n=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}\right]
\end{aligned}$$

We have our required result.

■

(b) We are asked to prove $\sum_{j=1}^{m} k_j \times \frac{\left(p_j{}^2-1\right)}{8} \equiv \frac{n^2-1}{8} \pmod{2}$. The proof of this result is very similar to part (a).

Proof.

Expanding the left hand side of the given congruence:

$$\sum_{j=1}^{m} k_j \times \frac{\left(p_j{}^2-1\right)}{8} = \left[k_1 \times \frac{\left(p_1{}^2-1\right)}{8}\right] + \left[k_2 \times \frac{\left(p_2{}^2-1\right)}{8}\right] + \cdots + \left[k_m \times \frac{\left(p_m{}^2-1\right)}{8}\right] \qquad (\ddagger)$$

Writing the first term on the right hand side of (‡) as an addition:

$$k_1 \times \frac{\left(p_1{}^2-1\right)}{8} = \underbrace{\frac{\left(p_1{}^2-1\right)}{8} + \frac{\left(p_1{}^2-1\right)}{8} + \cdots + \frac{\left(p_1{}^2-1\right)}{8}}_{k_1 \text{ copies}} \qquad (*)$$

By the result of the previous question part (b):

$$\left(\frac{a^2-1}{8}\right) + \left(\frac{b^2-1}{8}\right) \equiv \left(\frac{[ab]^2-1}{8}\right) \pmod{2}$$

Applying this to (*) yields

$$k_1 \times \frac{\left(p_1-1\right)}{8} = \underbrace{\frac{\left(p_1{}^2-1\right)}{8} + \frac{\left(p_1{}^2-1\right)}{8} + \cdots + \frac{\left(p_1{}^2-1\right)}{8}}_{k_1 \text{ copies}} \equiv \frac{\left(p_1{}^{k_1}\right)^2-1}{8} \pmod{2}$$

Similarly we have

$$k_j \times \frac{\left(p_j-1\right)}{8} \equiv \frac{\left(p_j{}^{k_j}\right)^2-1}{8} \pmod{2} \text{ for } j = 2,\ 3,\ \cdots,\ m$$

Putting each of these into (‡) gives

$$\begin{aligned} \sum_{j=1}^{m} k_j \times \frac{\left(p_j{}^2-1\right)}{8} &= \left[k_1 \times \frac{\left(p_1{}^2-1\right)}{8}\right] + \left[k_2 \times \frac{\left(p_2{}^2-1\right)}{8}\right] + \cdots + \left[k_m \times \frac{\left(p_m{}^2-1\right)}{8}\right] \\ &\equiv \frac{\left(\left(p_1{}^{k_1}\right)^2-1\right)}{8} + \frac{\left(\left(p_2{}^{k_2}\right)^2-1\right)}{8} + \cdots + \frac{\left(\left(p_m{}^{k_m}\right)^2-1\right)}{8} \\ &\equiv \frac{\left(p_1{}^{k_1} p_2{}^{k_2} \cdots p_m{}^{k_m}\right)^2-1}{8} \equiv \frac{n^2-1}{2} \pmod{2} \end{aligned}$$

We have our required result.

■

12. We need to prove $\left(\frac{2}{n}\right) = (-1)^{\frac{1}{8}\left(n^2-1\right)}$. *How?*

We use the result of Lemma (7.23) part (b):

$$\sum_{j=1}^{m} k_j \times \frac{\left(p_j{}^2-1\right)}{8} \equiv \frac{n^2-1}{8} \pmod{2}$$

Also Corollary (7.18):

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

Proof.

Let the prime decomposition of $n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_m^{k_m}$. Then

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right)^{k_1} \times \left(\frac{2}{p_2}\right)^{k_2} \times \left(\frac{2}{p_3}\right)^{k_3} \times \cdots \times \left(\frac{2}{p_m}\right)^{k_m} \qquad \left[\text{By the Jacobi definition (7.21)}\right]$$

$$= \left[(-1)^{\frac{p_1^2-1}{8}}\right]^{k_1} \times \left[(-1)^{\frac{p_2^2-1}{8}}\right]^{k_2} \times \cdots \times \left[(-1)^{\frac{p_m^2-1}{8}}\right]^{k_m} \qquad \left[\text{By Corollary (7.18)} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}\right]$$

$$= (-1)^{k_1\left(\frac{p_1^2-1}{8}\right)} \times (-1)^{k_2\left(\frac{p_2^2-1}{8}\right)} \times \cdots \times (-1)^{k_m\left(\frac{p_m^2-1}{8}\right)} \qquad \left[\text{By rules of indices} \quad \left(a^x\right)^y = a^{xy}\right]$$

$$= (-1)^{k_1\left(\frac{p_1^2-1}{8}\right) + k_2\left(\frac{p_2^2-1}{8}\right) + \cdots + k_m\left(\frac{p_m^2-1}{8}\right)} \qquad \left[\text{By rules of indices} \quad a^x a^y = a^{x+y} \quad \text{with} \quad a = (-1)\right]$$

$$= (-1)^{\sum_{j=1}^{m} k_j\left(\frac{p_j^2-1}{8}\right)} = (-1)^{\frac{1}{8}\left(n^2-1\right)} \qquad \left[\text{By (7.23) (b)} \sum_{j=1}^{m} k_j \times \frac{\left(p_j^2-1\right)}{8} \equiv \frac{n^2-1}{8} \pmod 2\right]$$

Hence we have our result.

■

13. You are asked to show the following needed result in question 5:

$$\left(\frac{b^x}{k}\right) = \left(\frac{b}{k}\right)^x \qquad (**)$$

We use this result in the proof of GLQR (7.25).

Proof

Writing the prime decomposition of m and n in compact form:

$$m = q_1^{k_1} \times q_2^{k_2} \times \cdots \times q_r^{k_r} = \prod_{i=1}^{r} q_i^{k_i} \quad \text{and} \quad n = p_1^{\lambda_1} \times p_2^{\lambda_2} \times \cdots \times p_s^{\lambda_s} = \prod_{j=1}^{s} p_j^{\lambda_j}$$

Using this notation we have

$$\left(\frac{m}{n}\right) = \prod_{j=1}^{s} \left(\frac{m}{p_j}\right)^{\lambda_j} \qquad \left[\text{By definition (7.21)} \quad \left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \times \left(\frac{a}{p_2}\right)^{k_2} \times \cdots \times \left(\frac{a}{p_m}\right)^{k_m}\right]$$

$$= \prod_{j=1}^{s} \left(\frac{q_1^{k_1} \times q_2^{k_2} \times \cdots \times q_r^{k_r}}{p_j}\right)^{\lambda_j} \qquad \left[\text{Because } m = q_1^{k_1} \times q_2^{k_2} \times \cdots \times q_r^{k_r}\right]$$

$$= \prod_{j=1}^{s} \left[\left(\frac{q_1^{k_1}}{p_j}\right) \times \left(\frac{q_2^{k_2}}{p_j}\right) \times \cdots \times \left(\frac{q_r^{k_r}}{p_j}\right)\right]^{\lambda_j} \qquad \left[\text{Because} \quad \left(\frac{a \times b}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)\right]$$

$$= \prod_{j=1}^{s} \left[\left(\frac{q_1}{p_j}\right)^{k_1} \times \left(\frac{q_2}{p_j}\right)^{k_2} \times \cdots \times \left(\frac{q_r}{p_j}\right)^{k_r}\right]^{\lambda_j} \qquad \left[\text{By } (**)\right]$$

$$= \prod_{j=1}^{s} \left[\prod_{i=1}^{r} \left(\frac{q_i}{p_j}\right)^{k_i}\right]^{\lambda_j} = \prod_{j=1}^{s} \left[\prod_{i=1}^{r} \left(\frac{q_i}{p_j}\right)^{k_i \times \lambda_j}\right] \qquad \left[\text{Using rules of indices} \quad \left(a^x\right)^y = a^{x \times y}\right]$$

Similarly we have the result the other way round:

$$\left(\frac{n}{m}\right)=\prod_{i=1}^{r}\left[\prod_{j=1}^{s}\left(\frac{p_j}{q_i}\right)^{\lambda_j\times k_i}\right]$$

Multiplying these two derivations $\left(\frac{m}{n}\right)=\prod_{j=1}^{s}\left[\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)^{\lambda_j\times k_i}\right]$ and $\left(\frac{n}{m}\right)=\prod_{i=1}^{r}\left[\prod_{j=1}^{s}\left(\frac{p_j}{q_i}\right)^{\lambda_j\times k_i}\right]$ and remembering that multiplication is commutative we have

$$\left(\frac{m}{n}\right)\times\left(\frac{n}{m}\right)=\prod_{j=1}^{s}\left[\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)^{\lambda_j\times k_i}\right]\times\prod_{i=1}^{r}\left[\prod_{j=1}^{s}\left(\frac{p_j}{q_i}\right)^{\lambda_j\times k_i}\right]$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(\frac{q_i}{p_j}\right)^{\lambda_j\times k_i}\left(\frac{p_j}{q_i}\right)^{\lambda_j\times k_i}\right]\qquad\left[\text{Because multiplication is commutative }\ xy=yx\right]$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right)\right]^{\lambda_j\times k_i}\qquad\left[\text{Because }\ x^m y^m=\left[xy\right]^m\ \text{ with } x=\left(\frac{q_i}{p_j}\right)\ \text{ and }\ y=\left(\frac{p_j}{q_i}\right)\right]$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(-1\right)^{\left(\frac{p_j-1}{2}\right)\times\left(\frac{q_i-1}{2}\right)}\right]^{\lambda_j\times k_i}\qquad\left[\text{By (7.16)}\ \left(\frac{p}{q}\right)\times\left(\frac{q}{p}\right)=\left(-1\right)^{\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)}\right]$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(-1\right)^{\left(\lambda_j\times k_i\right)\left[\left(\frac{p_j-1}{2}\right)\times\left(\frac{q_i-1}{2}\right)\right]}\right]\qquad\left[\text{By rules of indices }\left(x^m\right)^n=x^{mn}\ \text{ with }\ x=\left(-1\right)\right]$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(-1\right)^{\lambda_j\left(\frac{p_j-1}{2}\right)\times k_i\left(\frac{q_i-1}{2}\right)}\right]\qquad\left[\text{Rearranging the index multiplication}\right]$$

So that we don't get lost in the notation, let

$x_i=k_i\left(\frac{q_i-1}{2}\right)$ and $y_j=\lambda_j\left(\frac{p_j-1}{2}\right)$. Then from the last line we have

$$
\begin{aligned}
\prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(-1\right)^{\lambda_j\left(\frac{p_j-1}{2}\right)\times k_i\left(\frac{q_i-1}{2}\right)}\right] &= \prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(-1\right)^{y_j\times x_i}\right] && \left[\text{Substituting from above}\right]\\
&= \prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(-1\right)^{x_i}\right]^{y_j} && \left[\text{By rules of indices } a^{m\times n}=\left(a^m\right)^n\right]\\
&= \prod_{j=1}^{s}\left[\left(-1\right)^{x_1}\left(-1\right)^{x_2}\cdots\left(-1\right)^{x_r}\right]^{y_j} && \left[\text{Expanding } \prod_{i=1}^{r}\right]\\
&= \prod_{j=1}^{s}\left[\left(-1\right)^{\left(x_1+x_2+\cdots+x_r\right)}\right]^{y_j} && \left[\begin{array}{l}\text{By the rules of}\\ \text{indices } a^m a^n=a^{m+n}\end{array}\right]\\
&= \prod_{j=1}^{s}\left[\left(-1\right)^{\sum_{i=1}^{r} x_i}\right]^{y_j} && (\dagger)
\end{aligned}
$$

Let $b=\sum_{i=1}^{r} x_i$ and substituting this into (†) gives

$$
\begin{aligned}
\prod_{j=1}^{s}\left[\left(-1\right)^{\sum_{i=1}^{r} x_i}\right]^{y_j} = \prod_{j=1}^{s}\left[\left(-1\right)^{b}\right]^{y_j} &= \left[\left(-1\right)^{b}\right]^{y_1}\times\left[\left(-1\right)^{b}\right]^{y_2}\times\cdots\times\left[\left(-1\right)^{b}\right]^{y_s} && \left[\text{Expanding } \prod_{j=1}^{s}\right]\\
&= \left[\left(-1\right)^{b}\right]^{y_1+y_2+\cdots+y_s} && \left[\begin{array}{l}\text{Using the rules of indices}\\ a^m\times a^n=a^{m+n} \quad \text{with} \quad a=\left(-1\right)^b\end{array}\right]\\
&= \left[\left(-1\right)^{b}\right]^{\sum_{j=1}^{s} y_j} && \left[\begin{array}{l}\text{Replacing with the sigma notation}\\ \text{for sum}\end{array}\right]\\
&= \left(-1\right)^{b\times\sum_{j=1}^{s} y_j} && \left[\text{Using the rules of indices } \left(a^m\right)^n=a^{m\times n}\right]
\end{aligned}
$$

Replacing back $b=\sum_{i=1}^{r} x_i$ in the above calculation yields

$$\prod_{j=1}^{s}\prod_{i=1}^{r}\left[(-1)^{\lambda_j\left(\frac{p_j-1}{2}\right)\times k_i\left(\frac{q_i-1}{2}\right)}\right] = (-1)^{\left(\sum_{i=1}^{r} x_i\right)\times\left(\sum_{j=1}^{s} y_j\right)}$$

$$= (-1)^{\left(\sum_{i=1}^{r} k_i\left(\frac{q_i-1}{2}\right)\right)\times\left(\sum_{j=1}^{s}\lambda_j\left(\frac{p_j-1}{2}\right)\right)} \quad \left[\begin{array}{l}\text{Replacing from above} \\ x_i = k_i\left(\dfrac{q_i-1}{2}\right) \text{ and } y_j = \lambda_j\left(\dfrac{p_j-1}{2}\right)\end{array}\right]$$

$$= (-1)^{\left(\frac{m-1}{2}\right)\times\left(\frac{n-1}{2}\right)} \quad \left[\begin{array}{l}\text{By (7.23) (a) } \displaystyle\sum_{i=1}^{r} k_i\left(\frac{q_i-1}{2}\right) \equiv \frac{m-1}{2} \pmod 2 \\ \text{and } \displaystyle\sum_{j=1}^{s}\lambda_j\left(\frac{p_j-1}{2}\right) \equiv \frac{n-1}{2} \pmod 2\end{array}\right]$$

Hence we have $\left(\frac{m}{n}\right)\times\left(\frac{n}{m}\right) = (-1)^{\left(\frac{m-1}{2}\right)\times\left(\frac{n-1}{2}\right)}$. This completes our proof.

■