Complete Solutions to Exercises 7.3

1. In each case we use the formula:

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

(a) We need to evaluate the Legendre symbol $\left(\frac{12}{71}\right)$. The number 12 is composite, that is $12=4\times 3=2^2\times 3$ so

$$\left(\frac{12}{71}\right)=\left(\frac{2^2\times 3}{71}\right)=\underbrace{\left(\frac{2^2}{71}\right)}_{\substack{=1 \text{ because we}\\ \text{have 2 squared}}}\times\left(\frac{3}{71}\right)=\left(\frac{3}{71}\right)$$

Since $71\equiv 3 \pmod 4$ and $3\equiv 3 \pmod 4$ so by the above formula (7.17):

$$\left(\frac{3}{71}\right)=-\left(\frac{71}{3}\right)=-\left(\frac{2}{3}\right)=-\left(\frac{-1}{3}\right) \quad \left[\text{because } 2\equiv -1 \pmod 3\right]$$

By Proposition (7.11):

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

Our prime $p=3$ so we have $3\equiv 3 \pmod 4$ therefore -1 is a quadratic non-residue. Hence $\left(\frac{-1}{3}\right)=-1$. Substituting this into the above gives

$$\left(\frac{12}{71}\right)=\left(\frac{3}{71}\right)=-\left(\frac{-1}{3}\right)=-(-1)=1$$

(b) This time we need to evaluate the Legendre symbol $\left(\frac{15}{101}\right)$. Since $15=5\times 3$ we have

$$\left(\frac{15}{101}\right)=\left(\frac{5}{101}\right)\left(\frac{3}{101}\right) \qquad (*)$$

Since $101\equiv 1 \pmod 4$ so applying formula (7.17) we have

$$\left(\frac{5}{101}\right)=\left(\frac{101}{5}\right)=\left(\frac{1}{5}\right)=1 \quad \left[\text{Because 1 is a quadratic residue}\right]$$

Similarly we have

$$\left(\frac{3}{101}\right)=\left(\frac{101}{3}\right)=\left(\frac{2}{3}\right)=\left(\frac{-1}{3}\right)=-1 \qquad \left[\begin{array}{l}\text{Because } 101\equiv 2\pmod 3 \text{ and } 3\equiv 3\pmod 4\\ \text{so } -1 \text{ is a quadratic non-residue}\end{array}\right]$$

Putting these $\left(\frac{5}{101}\right)=1$ and $\left(\frac{3}{101}\right)=-1$ into (*) gives

$$\left(\frac{15}{101}\right)=\left(\frac{5}{101}\right)\times\left(\frac{3}{101}\right)=1\times(-1)=-1.$$

(c) Similarly evaluating the Legendre symbol $\left(\frac{28}{163}\right)$:

$$\left(\frac{28}{163}\right)=\left(\frac{7\times 4}{163}\right)=\left(\frac{7}{163}\right)\times\left(\frac{4}{163}\right)=\left(\frac{7}{163}\right)\times\underbrace{\left(\frac{2^2}{163}\right)}_{\substack{=1 \text{ because we}\\ \text{have a square, } 2^2}}=\left(\frac{7}{163}\right) \qquad (\dagger)$$

How do we find $\left(\frac{7}{163}\right)$*?*

Use the above formula (7.17). Since $163\equiv 7\equiv 3\pmod 4$ we have

$$\left(\frac{7}{163}\right)=-\left(\frac{163}{7}\right)=-\left(\frac{2}{7}\right) \qquad \left[\text{Because } 163\equiv 2\pmod 7\right]$$

Using Proposition (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 $p=7\equiv -1\pmod 8$ so

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

Substituting $\left(\frac{7}{163}\right)=-\left(\frac{2}{7}\right)=-1$ into $(\dagger)$ gives

$$\left(\frac{28}{163}\right)=\left(\frac{7}{163}\right)=-1$$

(d) We need to evaluate $\left(\frac{75}{541}\right)$. Since $75=3\times 25$ so

$$\left(\frac{75}{541}\right)=\left(\frac{3}{541}\right)\left(\frac{25}{541}\right)=\left(\frac{3}{541}\right)\underbrace{\left(\frac{5^2}{541}\right)}_{=1}=\left(\frac{3}{541}\right).$$

Note that 541 is congruent to 1 modulo 4 so by formula (7.17) we have

$$\left(\frac{3}{541}\right)=\left(\frac{541}{3}\right)\underbrace{\equiv}_{541\equiv 1\pmod 3}\left(\frac{1}{3}\right)=1.$$

Hence $\left(\frac{75}{541}\right)=1.$

(e) This Legendre symbol $\left(\frac{360}{1223}\right)$ is more difficult to evaluate than the previous ones. First note that $360=2^3\times 3^2\times 5$ so we have

$$\left(\frac{360}{1223}\right)=\left(\frac{2^3\times 3^2\times 5}{1223}\right)=\left(\frac{2^3}{1223}\right)\left(\frac{3^2}{1223}\right)\left(\frac{5}{1223}\right)$$
$$=\underbrace{\left(\frac{2^2}{1223}\right)}_{=1}\left(\frac{2}{1223}\right)\underbrace{\left(\frac{3^2}{1223}\right)}_{=1}\left(\frac{5}{1223}\right)=\left(\frac{2}{1223}\right)\left(\frac{5}{1223}\right)$$

To evaluate $\left(\frac{2}{1223}\right)$ we use Proposition (7.15):

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

Since $p=1223\equiv 7\equiv -1\pmod 8$ so $\left(\frac{2}{1223}\right)=1$. Evaluating $\left(\frac{5}{1223}\right)$ by using formula (7.17) we have

$$\left(\frac{5}{1223}\right)=\left(\frac{1223}{5}\right)\qquad\left[\text{Because } 5\equiv 1\pmod 4\right]$$
$$=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1\qquad\left[\text{By (7.15) with } p=3\equiv 3\pmod 8\right]$$

Substituting $\left(\frac{2}{1223}\right)=1$ and $\left(\frac{5}{1223}\right)=-1$ into $\left(\frac{360}{1223}\right)=\left(\frac{2}{1223}\right)\left(\frac{5}{1223}\right)$ gives

$$\left(\frac{360}{1223}\right)=\left(\frac{2}{1223}\right)\left(\frac{5}{1223}\right)=1\times(-1)=-1.$$

(f) This time we need to evaluate $\left(\frac{115}{1987}\right)$. The number 115 is composite because $115=5\times 23$. We have

$$\left(\frac{115}{1987}\right)=\left(\frac{5}{1987}\right)\times\left(\frac{23}{1987}\right)\quad(*)$$

We have $5\equiv 1\pmod 4$ so by formula (7.17):

$$\left(\frac{5}{1987}\right)=\left(\frac{1987}{5}\right)=\left(\frac{2}{5}\right)\qquad\left[\text{Because } 1987\equiv 2\pmod 5\right]$$

The prime $p = 5 \equiv -3 \pmod 8$ so by Proposition (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 $\left(\frac{2}{5}\right) = -1$. Evaluating the other Legendre symbol in (*):

$$\left(\frac{23}{1987}\right) = -\left(\frac{1987}{23}\right) \qquad \left[\text{Because } 1987 \equiv 23 \equiv 3 \pmod 4\right]$$

$$= -\left(\frac{9}{23}\right) \qquad \left[\text{Because } 1987 \equiv 9 \pmod{23}\right]$$

$$= -\left(\frac{3^2}{23}\right) = -1 \quad \left[\text{Because we have } 3^2\right]$$

Substituting $\left(\frac{2}{5}\right) = -1$ and $\left(\frac{23}{1987}\right) = -1$ into (*) gives

$$\left(\frac{115}{1987}\right) = \left(\frac{5}{1987}\right)\left(\frac{23}{1987}\right) = (-1)(-1) = 1.$$

(g) We are required to evaluate $\left(\frac{700}{3571}\right)$. Writing the factors of 700 we have

$$700 = 2^2 \times 5^2 \times 7.$$

Therefore

$$\left(\frac{700}{3571}\right) = \left(\frac{2^2}{3571}\right)\left(\frac{5^2}{3571}\right)\left(\frac{7}{3571}\right) = 1 \times 1 \times \left(\frac{7}{3571}\right) = \left(\frac{7}{3571}\right)$$

Both $3571 \equiv 7 \equiv 3 \pmod 4$. So using formula (7.17) we have

$$\left(\frac{7}{3571}\right) = -\left(\frac{3571}{7}\right) = -\left(\frac{1}{7}\right) = -1 \qquad \left[\text{Because } 3571 \equiv 1 \pmod 7\right]$$

Hence $\left(\frac{700}{3571}\right) = \left(\frac{7}{3571}\right) = -1$.

(h) We need to evaluate $\left(\frac{703}{4409}\right)$. By hint we have $703 = 19 \times 37$.

Using this to find the given Legendre symbol:

$$\left(\frac{703}{4409}\right) = \left(\frac{19 \times 37}{4409}\right) = \left(\frac{19}{4409}\right) \times \left(\frac{37}{4409}\right) \qquad (*)$$

Evaluating each of the Legendre symbols on the right-hand side:

$$\left(\frac{19}{4409}\right)=\left(\frac{4409}{19}\right) \qquad \left[\text{Because } 4409\equiv 1 \pmod 4\right]$$
$$=\left(\frac{1}{19}\right)=1 \qquad \left[\text{Because } 4409\equiv 1 \pmod{19}\right]$$

Finding the other Legendre symbol:

$$\left(\frac{37}{4409}\right)=\left(\frac{4409}{37}\right) \qquad \left[\text{Because } 4409\equiv 1 \pmod 4\right]$$
$$=\left(\frac{6}{37}\right) \qquad \left[\text{Because } 4409\equiv 6 \pmod{37}\right]$$

Since $6=2\times 3$ we have

$$\left(\frac{6}{37}\right)=\left(\frac{2\times 3}{37}\right)$$
$$=\left(\frac{2}{37}\right)\times\left(\frac{3}{37}\right) \qquad (\dagger)$$

The prime $p=37\equiv 5\equiv -3 \pmod 8$ so by Proposition (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 $\left(\frac{2}{37}\right)=-1$.

Evaluating $\left(\frac{3}{37}\right)$ gives

$$\left(\frac{3}{37}\right)=\left(\frac{37}{3}\right) \qquad \left[\text{Because } 37\equiv 1 \pmod 4\right]$$
$$=\left(\frac{1}{3}\right)=1 \qquad \left[\text{Because } 37\equiv 1 \pmod 3\right]$$

Substituting $\left(\frac{2}{37}\right)=-1$ and $\left(\frac{3}{37}\right)=1$ into (†) gives

$$\left(\frac{6}{37}\right)=\left(\frac{2}{37}\right)\times\left(\frac{3}{37}\right)=-1\times 1=-1.$$

Hence $\left(\frac{37}{4409}\right)=\left(\frac{6}{37}\right)=-1$. Substituting $\left(\frac{19}{4409}\right)=1$ and $\left(\frac{37}{4409}\right)=-1$ into (*) gives

$$\left(\frac{703}{4409}\right)=\left(\frac{19}{4409}\right)\times\left(\frac{37}{4409}\right)=1\times(-1)=-1.$$

2. (a) We need to test whether 14 is a quadratic residue of 131. This means we need to evaluate the Legendre symbol $\left(\frac{14}{131}\right)$. Since $14 = 2\times 7$ we have

$$\left(\frac{14}{131}\right) = \left(\frac{2\times 7}{131}\right) = \left(\frac{2}{131}\right)\times\left(\frac{7}{131}\right) \qquad (*)$$

The prime $p = 131 \equiv 3 \pmod 8$ so by Proposition (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 $\left(\frac{2}{131}\right) = -1$. Evaluating the other Legendre symbol on the right - hand side of (*):

$$\begin{aligned} \left(\frac{7}{131}\right) &= -\left(\frac{131}{7}\right) && \left[\text{Because } 131 \equiv 7 \equiv 3 \pmod 4\right] \\ &= -\left(\frac{5}{7}\right) && \left[\text{Because } 131 \equiv 5 \pmod 7\right] \\ &= -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) && \left[\text{Because } 7 \equiv 2 \pmod 5\right] \end{aligned}$$

We need to find the Legendre symbol $\left(\frac{2}{5}\right)$. Since $p = 5 \equiv -3 \pmod 8$ so by the above Proposition (7.15) we have $\left(\frac{2}{5}\right) = -1$. Substituting this into the above derivation gives

$$\left(\frac{7}{131}\right) = -\left(\frac{2}{5}\right) = -(-1) = 1.$$

Substituting $\left(\frac{2}{131}\right) = -1$ and $\left(\frac{7}{131}\right) = 1$ into (*) gives

$$\left(\frac{14}{131}\right) = \left(\frac{2}{131}\right)\times\left(\frac{7}{131}\right) = (-1)\times 1 = -1.$$

Hence 14 is a quadratic non-residue of 131.

(b) This time we need to test whether 12 is a quadratic residue of 131:

$$\left(\frac{12}{131}\right) = \left(\frac{2^2\times 3}{131}\right) = \left(\frac{2^2}{131}\right)\times\left(\frac{3}{131}\right) = 1\times\left(\frac{3}{131}\right) = \left(\frac{3}{131}\right) \qquad (*)$$

Since $131 \equiv 3 \pmod 4$ so by formula (7.17):

$$\left(\frac{3}{131}\right) = -\left(\frac{131}{3}\right) = -\left(\frac{2}{3}\right) = -\left(\frac{-1}{3}\right) \qquad \left[\text{Because } 2 \equiv -1 \pmod 3\right]$$

By Proposition (7.11):

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

We have prime $p=3\equiv 3\left(\text{mod } 4\right)$ so

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

Therefore $\left(\frac{3}{131}\right)=-\left(\frac{-1}{3}\right)=-\left(-1\right)=1$. Putting this into (*) gives

$$\left(\frac{12}{131}\right)=\left(\frac{3}{131}\right)=1$$

Therefore 12 is a quadratic residue of 131.

(c) This time we need to find whether 15 is a quadratic residue of 131. This means we need to evaluate the Legendre symbol $\left(\frac{15}{131}\right)$:

$$\left(\frac{15}{131}\right)=\left(\frac{5}{131}\right)\times\left(\frac{3}{131}\right) \qquad (\dagger)$$

Since $5\equiv 1\left(\text{mod } 4\right)$ so we have

$$\left(\frac{5}{131}\right)=\left(\frac{131}{5}\right)=\left(\frac{1}{5}\right)=1 \qquad \left[\text{Because } 131\equiv 1\left(\text{mod } 5\right)\right]$$

The other Legendre symbol, $\left(\frac{3}{131}\right)$, on the right hand side of $(\dagger)$, we evaluated in part (b):

$$\left(\frac{3}{131}\right)=1$$

Substituting $\left(\frac{5}{131}\right)=1$ and $\left(\frac{3}{131}\right)=1$ into $(\dagger)$ gives

$$\left(\frac{15}{131}\right)=\left(\frac{5}{131}\right)\times\left(\frac{3}{131}\right)=1\times 1=1.$$

Hence 15 is a quadratic residue of 131.

(d) We need to test whether 65 is a quadratic residue of 131. Since $65=5\times 13$, the Legendre symbol $\left(\frac{65}{131}\right)$ is

$$\left(\frac{65}{131}\right)=\left(\frac{5\times 13}{131}\right)=\left(\frac{5}{131}\right)\times\left(\frac{13}{131}\right) \qquad (*)$$

The Legendre symbol $\left(\frac{5}{131}\right)$ we evaluated in part (c):

$$\left(\frac{5}{131}\right)=1$$

We need to work out $\left(\frac{13}{131}\right)$. Since $13\equiv 1\pmod 4$ so

$$\left(\frac{13}{131}\right)=\left(\frac{131}{13}\right)=\left(\frac{1}{13}\right)=1 \qquad \left[\text{Because } 131\equiv 1\pmod{13}\right]$$

Substituting $\left(\frac{5}{131}\right)=1$ and $\left(\frac{13}{131}\right)=1$ into (*) gives

$$\left(\frac{65}{131}\right)=\left(\frac{5}{131}\right)\times\left(\frac{13}{131}\right)=1\times 1=1.$$

Hence 65 is a quadratic residue of 131.

3. (i) We need to show 2 is a quadratic residue of prime $p \Leftrightarrow p\equiv\pm 1\pmod 8$.

Proof.

$(\Leftarrow)$. If $p\equiv\pm 1\pmod 8$ then by Proposition (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 the Legendre symbol $\left(\frac{2}{p}\right)=1$ so 2 is a QR of p.

$(\Rightarrow)$. Assume 2 is a QR of p that is $\left(\frac{2}{p}\right)=1$. Required to prove that $p\equiv\pm 1\pmod 8$. By Corollary (7.18):

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}} \text{ where } p \text{ is an odd prime.}$$

We are assuming $\left(\frac{2}{p}\right)=1$ therefore $\frac{p^2-1}{8}$ is even. Remember p is an odd prime so $p\equiv\pm 1\pmod 8$ or $p\equiv\pm 3\pmod 8$. From $p\equiv\pm 1\pmod 8$ we have $p=8k\pm 1$ where k is an integer. We obtain

$$\frac{p^2-1}{8}=\frac{(8k\pm 1)^2-1}{8}=\frac{64k^2\pm 16k+1-1}{8}=\frac{16k(4k+1)}{8}=2k(4k+1).$$

We have $\dfrac{p^2-1}{8} = 2k\left(4k+1\right)$ is even so $p \equiv \pm 1 \left(\text{mod } 8\right)$.

If $p \equiv 3\left(\text{mod } 8\right)$ then the index $\dfrac{p^2-1}{8}$ is even.

■

(ii) (a) We are asked to factorize $18^2 - 2 = 322$. This is an even number so 2 is a factor of this 322:

$$322 = 2 \times 161 .$$

We need to find the factors of 161. By Corollary (2.10) of chapter 2:

> If $n > 1$ is composite, then it has a prime divisor p such that $p \le \left\lfloor \sqrt{n} \right\rfloor$.

Let p be a prime factor of 161 then by this corollary we have

$$p \le \left\lfloor \sqrt{161} \right\rfloor = 12 .$$

Since $18^2 - 2 = 322$ so by part (i), the prime p must satisfy $p \equiv \pm 1 \left(\text{mod } 8\right)$. The only prime less than 12 which satisfies this congruence is 7 and:

$$\frac{161}{7} = 23 .$$

Therefore $161 = 7 \times 23$ and from above we have

$$322 = 2 \times 161 = 2 \times 7 \times 23 .$$

(b) This time we have to factorize $23^2 - 2 = 527$. Let p be the prime factor of 527 then by the above Corollary (2.10) we have

$$p \le \left\lfloor 527 \right\rfloor = 22 .$$

Additionally, p must also conform to $p \equiv \pm 1 \left(\text{mod } 8\right)$. The primes below 22 which satisfy this congruence are 7 and 17. Let us check 7 first:

$$\frac{527}{7} = 75.29 \left(\text{2dp}\right).$$

Clearly 7 is not a factor of 527. Now we try 17:

$$\frac{527}{17} = 31 .$$

Hence 17 is a factor of 527 and as 31 is prime so 31 is the other prime factor of 527. Note that $31 \equiv -1 \left(\text{mod } 8\right)$. We have

$$527 = 17 \times 31 .$$

(c) We need to factorize $51^2 - 2 = 2599$. Remember the prime factor p of 2599 must satisfy $p \equiv \pm 1 \left(\text{mod } 8\right)$ because we are given $51^2 - 2 = 2599$. We only need

to test the primes below 50 because the floor function of $\sqrt{51^2-2}=\sqrt{2599}$ is less than 51 so it is 50. Hence, we only trial

$$7,\ 17,\ 23,\ 31,\ 41 \text{ and } 47$$

We need to test these primes:

$$\frac{2599}{7}=371.29\ (2\text{dp})$$

$$\frac{2599}{17}=152.88\ (2\text{dp})$$

$$\frac{2599}{23}=113$$

So 23 is a prime factor of 2599. Also 113 must be prime because $\left\lfloor\sqrt{113}\right\rfloor=10$ and we have already tested the prime 7 which is the only one below 10 and satisfies the above congruence. Hence $2599=23\times113$.

(d) We are required to factorize $27^2-2=727$. Let p be a prime factor of 727 then the prime factors p must satisfy $p\equiv\pm1\ (\text{mod } 8)$. The only prime factors are 7, 17 and 23 below 27:

$$\frac{727}{7}=103.86,\quad \frac{727}{17}=42.76 \quad \text{and} \quad \frac{727}{23}=31.61.$$

Since *none* of these primes are factors so 727 is prime.

(e) We are to factorize $105^2-2=11\,023$. The prime factors p of this are of the form $p\equiv\pm1(\text{mod } 8)$. We trial 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, … as factors of 11 023 and we find that 73 is a factor and $\dfrac{11\,023}{73}=151$. Now 151 is a prime.

Why?

Because $\left\lfloor\sqrt{151}\right\rfloor=12$ and the only prime below 12 which satisfy $\pm1(\text{mod } 8)$ is 7 and as 7 does *not* go into 11 023 so 7 *cannot* be a factor of 151. Therefore

$$11\,023=73\times151$$

(f) We are asked to factorize $47^2-2=2207$. Let p be a prime factor of $47^2-2=2207$ then p must be one of 7, 17, 23, 31, 41 if 2207 is composite. We don't need to go any further because we are given 47^2-2 and the square root of this is going to be less than 47. None of these primes 7, 17, 23, 31, 41 go into 2207 therefore 2207 is prime.

(g) We need to factorize $195^2 - 2 = 38\ 023$. We only need to test prime factors p which are of the form $p \equiv \pm 1 \pmod 8$ and below 195. Testing the first few primes of this type 7, 17, 23, 31, 41, 47,... we find that

$$38\ 023 = 47 \times 809$$

We now need to test the primality of 809. We have $\left\lfloor \sqrt{809} \right\rfloor = 28$ and there are *no* primes in the above list below 28 which go into 809 because if they did, that prime would also go into 38 023. Hence $38\ 023 = 47 \times 809$.

4. We need to prove that if p is an odd prime and $p \nmid a$ then

$$a,\ 2a,\ 3a,\ \cdots,\ \frac{p-1}{2}a \not\equiv 0 \pmod p$$

How do we prove this?

Using contradiction.

Proof.

Suppose $ka \equiv 0 \pmod p$ for an arbitrary k where $k \in \left\{1,\ 2,\ 3,\ \cdots,\ \frac{p-1}{2}\right\}$. From $ka \equiv 0 \pmod p$ we have $p \mid ka$ and because we are given that $p \nmid a$ so $\gcd(p,\ a) = 1$.

Applying Euclid's Lemma (1.13):

> If $x \mid yz$ with $\gcd(x,\ y) = 1$ then $x \mid z$.

To $p \mid ka$ gives $p \mid k$. This *cannot* be the case because $k \in \left\{1,\ 2,\ 3,\ \cdots,\ \frac{p-1}{2}\right\}$.

We have a contradiction so $ka \not\equiv 0 \pmod p$.

■

5. We are required to prove that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ where p is an odd prime.

Proof.

How do we prove this?

By using Proposition (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 consider the two cases $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 3 \pmod 8$ because we are given that p is an odd prime.

Case I:

Take $p \equiv \pm 1 \pmod 8$ then $p = 8k \pm 1$ where k is a positive integer. Then

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k + 1 - 1}{8}$$
$$= \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k = 2k(4k \pm 1)$$

This $\frac{p^2-1}{8} = 2k(4k+1)$ implies that $\frac{p^2-1}{8}$ is even, so if $p \equiv \pm 1 \pmod 8$ then by the above proposition (7.15) we have $(-1)^{\frac{p^2-1}{8}} = 1 = \left(\frac{2}{p}\right)$.

Case II:

Take $p \equiv \pm 3 \pmod 8$ then $p = 8k \pm 3$ where k is a positive integer. Then

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 9 - 1}{8}$$
$$= \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1 = 2k(4k \pm 3) + 1$$

This $\frac{p^2-1}{8} = 2k(4k \pm 3) + 1$ implies that $\frac{p^2-1}{8}$ is odd, so if $p \equiv \pm 3 \pmod 8$ then by (7.15) we have $(-1)^{\frac{p^2-1}{8}} = -1 = \left(\frac{2}{p}\right)$.

This completes our proof.

■

6. We need to show $1223 \mid (2^{611} - 1)$.

Proof.

Euler's Criterion (7.5) is:

$$a \text{ is a quadratic residue of } p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Note that if we let $p = 1223$ then $\frac{p-1}{2} = \frac{1223-1}{2} = 611$. If we can show that 2 is a quadratic residue of 1223 then by Euler's Criterion we will have

$$2^{\frac{1223-1}{2}} \equiv 2^{611} \equiv 1 \pmod{1223} \qquad (*)$$

How do we show 2 is a quadratic residue of 1223?

By Proposition (7.15):

$$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm1\pmod 8\\ -1 & \text{if } p\equiv\pm3\pmod 8\end{cases}$$

We have $1223\equiv 7\equiv -1\pmod 8$ so by (7.15)

$$\left(\frac{2}{1223}\right)=1.$$

Hence 2 is a quadratic residue of 1223 so by (*) we have

$$2^{611}\equiv 1\pmod{1223}.$$

Therefore $1223\mid\left(2^{611}-1\right)$.

7. We need to determine x such that $2^{271}\equiv x\pmod{541}$. *How?*

Well we are given that 541 is a prime so we can test whether 2 is a quadratic residue of 541. *How?*

By using (7.15):

$$\left(\frac{2}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm1\pmod 8\\ -1 & \text{if } p\equiv\pm3\pmod 8\end{cases}$$

$541\equiv 5\equiv -3\pmod 8$ so by (7.15) we have 2 is a quadratic *non* – residue of 541, therefore by Euler's Criterion

$$2^{\frac{p-1}{2}}\equiv 2^{270}\equiv -1\pmod{541}.$$

Multiplying this by 2 gives

$$2\times 2^{270}\equiv 2^{271}\equiv 2\times(-1)\equiv -2\equiv 539\pmod{541}.$$

We have $2^{271}\equiv 539\pmod{541}$ which gives $x\equiv 539\pmod{541}$.

8. (a) We need to find $25^{995}\equiv x\pmod{1987}$. Since $25=5^2$ so it is a quadratic residue of 1987 so we have

$$25^{\frac{1987-1}{2}}\equiv 25^{993}\equiv 1\pmod{1987}\qquad (*)$$

Therefore

$$25^{995}\equiv 25^2\times\underbrace{25^{993}}_{\equiv 1 \text{ by } (*)}\equiv 25^2\times 1\equiv 625\times 1\equiv 625\pmod{1987}.$$

(b) We are asked to find $26^{995} \equiv x \pmod{1987}$.

Since $26 = 2 \times 13$ so we check if 26 is a quadratic residue of 1987. Using Legendre symbols, we have

$$\left(\frac{26}{1987}\right) = \left(\frac{2}{1987}\right) \times \left(\frac{13}{1987}\right) \qquad (\dagger)$$

Note that $1987 \equiv 3 \pmod{8}$ 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 $\left(\frac{2}{1987}\right) = -1$.

Need to test $\left(\frac{13}{1987}\right)$ for quadratic residue:

$$\left(\frac{13}{1987}\right) = \left(\frac{1987}{13}\right) = \left(\frac{11}{13}\right) \quad \left[\text{Because } 1987 \equiv 11 \pmod{13}\right]$$
$$= \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) \quad \left[\text{Because } 13 \equiv 2 \pmod{11}\right]$$

Since $11 \equiv 3 \pmod{8}$ so by the above (7.15):

$$\left(\frac{13}{1987}\right) = \left(\frac{2}{11}\right) = -1.$$

Substituting $\left(\frac{2}{1987}\right) = -1$ and $\left(\frac{13}{1987}\right) = -1$ into (†) gives

$$\left(\frac{26}{1987}\right) = \left(\frac{2}{1987}\right) \times \left(\frac{13}{1987}\right) = (-1) \times (-1) = 1.$$

This means that 26 is a quadratic residue of 1987 so

$$26^{\frac{1987-1}{2}} \equiv 26^{993} \equiv 1 \pmod{1987} \qquad (\ddagger)$$

However, we need to find $26^{995} \equiv x \pmod{1987}$ so multiplying both sides of (‡) by 26^2 we have

$$26^{995} \equiv 26^2 \times 26^{993} \equiv 26^2 \times 1 \equiv 676 \pmod{1987}.$$

9. (i) We are required to prove that

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

Proof.

We have

$$\left(\frac{-2}{p}\right)=\left(\frac{-1\times 2}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{2}{p}\right) \qquad (\ddagger)$$

Using (7.11):

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

By (7.15):

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

Consider the four cases:

Case I:

Let $p\equiv 1 \pmod 8$ then $p\equiv 1\pmod 4$ so by applying (7.11) and (7.15) on (‡):

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{2}{p}\right)=1\times 1=1.$$

Case II:

Let $p\equiv 3\pmod 8$ then $p\equiv 3\pmod 4$ so by applying (7.11) and (7.15) on (‡):

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{2}{p}\right)=-1\times(-1)=1.$$

Case III:

Let $p\equiv -1 \pmod 8$ then $p\equiv 3\pmod 4$ so by applying (7.11) and (7.15) on (‡):

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{2}{p}\right)=-1\times 1=-1.$$

Case IV:

Let $p\equiv -3\pmod 8$ then $p\equiv 1\pmod 4$ so by applying (7.11) and (7.15) on (‡):

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{2}{p}\right)=1\times(-1)=-1.$$

Combining all four cases together we have

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

This completes our proof.

■

(ii) We are asked to show that if the odd prime p satisfies $p \mid \left(x^2+2\right)$ then $p \equiv 1, 3 \pmod 8$.

Proof.

We are given that $p \mid \left(x^2+2\right)$ so in modular arithmetic we have

$$x^2+2 \equiv 0 \pmod p \Rightarrow x^2 \equiv -2 \pmod p.$$

Therefore -2 is a QR of prime p. We have

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right) \times \left(\frac{-1}{p}\right) = 1.$$

This implies that $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = 1$ or $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = -1$. By combining (7.11) and (7.15):

$$(7.11)\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases} \quad (7.15) \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

We obtain $p \equiv 1, 3 \pmod 8$.

(a) We need to factorize $18^2+2 = 326$. Clearly 2 is a factor because we have an even number so $18^2+2 = 326 = 2 \times 163$.

By part (i) we know the prime factors p of 163 satisfy $p \equiv 1$ or $3 \pmod 8$. There are only two primes 3 and 11 below 12 because $\left\lfloor \sqrt{163} \right\rfloor = 12$ which satisfy $p \equiv 1, 3 \pmod 8$ and 3, 11 do not go into 163. Therefore 163 is prime. Thus $18^2+2 = 2 \times 163$.

(b) We are asked to factorize $23^2+2 = 531$. By part (i) we have the only prime factors p of 23^2+2 are the ones which satisfy $p \equiv 1, 3 \pmod 8$. The only ones below 23 are 3, 11, 17, 19. Testing 3 and 11 as factors is easy as we have done this many times before. Since $5+3+1 = 9$ so actually 9 is factor of 531 and $531 = 9 \times 59$ and 59 is prime. We have $531 = 3^2 \times 59$.

(c) We need to find the prime decomposition of $51^2+2 = 2603$. The prime factors p of $51^2+2 = 2603$ satisfy $p \equiv 1, 3 \pmod 8$. We only need to trial the primes below 51 of this type; they are 3, 11, 17, 19, 41 and 43. Clearly 3 and 11 are *not* factors of 2603. Testing the remaining primes in the list gives

$$\frac{2603}{17} = 153.12\big(2\text{dp}\big)\ ,\ \frac{2603}{19} = 137$$

We have $2603 = 19 \times 137$.

(d) We are asked to find the prime factors of $27^2 + 2 = 731$. By the result of part (i) any prime factors p of $27^2 + 2$ must satisfy $p \equiv 1, 3\big(\text{mod } 8\big)$. The only ones below 27 are 3, 11, 17 and 19. Using the normal tests for 3 and 11, we find these are *not* factors of 731. Testing the next prime factor, 17, gives

$$731 = 17 \times 43 \text{ and } 43 \text{ is prime.}$$

Thus, we have $731 = 17 \times 43$.

(e) We need to find the prime factors of $105^2 + 2 = 11\,027$. The prime factors p of $105^2 + 2$ must satisfy $p \equiv 1, 3\big(\text{mod } 8\big)$. The first few below 105 are 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89 and 97.

Clearly 3 and 11 are *not* factors of 11 207. Testing the remaining primes, we find that none of them are factors of 11 207 so 11 207 is prime.

(f) Similarly, we find the prime factors of $47^2 + 2 = 2211$. Clearly 3 is a factor of 2211 as $2 + 2 + 1 + 1 = 6$ and $3 \mid 6$. Also 11 is factor because $1 - 1 + 2 - 2 = 0$ and $11 \mid 0$. We have $2211 = 3 \times 11 \times 67$ and 67 is prime so we have our prime factorization.

(g) The obvious prime factor of $195^2 + 2 = 38\,027$ is 11 because $7 - 2 + 0 - 8 + 3 = 0$ and $11 \mid 0$. Hence we have $38027 = 11 \times 3457$ and any prime factors of 3457 which must be less than or equal to $\left\lfloor \sqrt{3457} \right\rfloor = 58$. Recall the prime factors p of 3457 must be of the type $p \equiv 1, 3\big(\text{mod } 8\big)$. Clearly 3 and 11 are not factors of 3457. We need to test 17, 19, 41 and 43:

$$\frac{3457}{17} = 203.35\big(2\text{dp}\big),\ \frac{3457}{19} = 181.95\big(2\text{dp}\big),\ \frac{3457}{41} = 84.32\big(2\text{dp}\big), \frac{3457}{43} = 80.40\big(2\text{dp}\big)$$

Hence 3457 is prime so $38027 = 11 \times 3457$.

10. (a) We need to find $\left(\frac{3}{13}\right)$ by using Gauss's Lemma:

We find the product of 3 and the $\frac{p-1}{2} = \frac{13-1}{2} = 6$ least positive residues. That is

$$S = \big\{3\big(1\big),\ 3\big(2\big),\ 3\big(3\big),\ 3\big(4\big), 3\big(5\big),\ 3\big(6\big)\big\} = \big\{3,\ 6,\ 9,\ 12,\ 15,\ 18\big\}.$$

The break off point between positive and negative residues occurs at 6.

We have the following for the prime 13:

$$S=\{3,\ 6,\ 9,\ 12,\ 15,\ 18\}=\{3,\ 6,\ \underbrace{-4,\ -1}_{\text{There are 2 negative residues}},\ 2,\ 5\}\ (\text{mod } 13)$$

Since we have 2 negative residues so by Gauss's Lemma we have

$$\left(\frac{3}{13}\right)=(-1)^2=1.$$

Therefore 3 is a quadratic residue of 13.

(b)We need to find $\left(\frac{3}{17}\right)$ by using Gauss's Lemma:

We find the product of 3 and the $\frac{p-1}{2}=\frac{17-1}{2}=8$ least positive residues. We have

$$S=\{3(1),\ 3(2),\ 3(3),\ 3(4),\ 3(5),\ 3(6),\ 3(7),\ 3(8)\}=\{3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24\}$$

The break off point between positive and negative residues is 8.

We have the following for the prime 17:

$$S=\{3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24\}=\{3,\ 6,\ \underbrace{-8,\ -5,\ -2}_{\text{There are 3 negative residues}},\ 1,\ 4,\ 7\}\ (\text{mod } 17)$$

Since we have 3 negative residues so by Gauss's Lemma we have

$$\left(\frac{3}{17}\right)=(-1)^3=-1.$$

Therefore 3 is a quadratic *non* - residue of 17.

(c) We need to find $\left(\frac{3}{19}\right)$ by using Gauss's Lemma:

We find the product of 3 and the $\frac{p-1}{2}=\frac{19-1}{2}=9$ least positive residues. We have the following for the prime modulo 19:

$$S=\{3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27\}\equiv\{3,\ 6,\ 9,\ \underbrace{-7,\ -4,\ -1}_{\text{There are 3 negative residues}},\ 2,\ 5,\ 8\}$$

Since we have 3 negative residues so by Gauss's Lemma:

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

Therefore 3 is a quadratic *non* - residue of 19.

(d)We need to find $\left(\frac{3}{23}\right)$ by using Gauss's Lemma:

We find the product of 3 and the $\frac{p-1}{2}=\frac{23-1}{2}=11$ least positive residues. We have the following for the prime modulo 23:

$$S=\{3,6,9,12,15,18,21,24,27,30,33\}\equiv\{3,6,9,\underbrace{-11,\ -8,\ -5,\ -2}_{\text{There are 4 negative residues}},1,4,7,10\}$$

Since we have 4 negative residues so by Gauss's Lemma:

$$\left(\frac{3}{23}\right)=(-1)^4=1.$$

Therefore 3 is a quadratic residue of 23.

11. (i) We are required to prove that $\left(\frac{3}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \text{ or } 11 \pmod{12}\\ -1 & \text{if } p\equiv 5 \text{ or } 7 \pmod{12}\end{cases}$.

Proof.

If $p\equiv 1\pmod{12}$ then $p=12k+1$ where k is an integer. We have

$$\left(\frac{3}{p}\right)=\left(\frac{3}{12k+1}\right)\underbrace{=}_{\text{because } 12k+1\equiv 1\pmod 4}\left(\frac{12k+1}{3}\right)\underbrace{=}_{12k+1\equiv 1\pmod 3}\left(\frac{1}{3}\right)=1 \qquad (*)$$

Similarly, for $p\equiv 11\equiv -1\pmod{12}$ implies $p=12k-1$ and

$$\left(\frac{3}{p}\right)=\left(\frac{3}{12k-1}\right)\underbrace{=}_{\text{because } 12k-1\equiv 3\pmod 4}-\left(\frac{12k-1}{3}\right)\underbrace{=}_{12k-1\equiv -1\pmod 3}-\left(\frac{-1}{3}\right)\underbrace{=}_{\text{because } 3\equiv 3\pmod 4}-(-1)=1 \qquad (**)$$

Very similar to these you can show that when $p\equiv 5 \text{ or } 7\pmod{12}$ that $\left(\frac{3}{p}\right)=-1$.

This completes our proof.

■

(ii) We are asked to show that that 3 is a quadratic residue $\Leftrightarrow$ $p\equiv 1,11\pmod{12}$.

Proof.

$(\Leftarrow)$. From part (i) we have if $p\equiv 1,11\pmod{12}$ then $\left(\frac{3}{p}\right)=1$ which implies that 3 is a quadratic residue of p.

$(\Rightarrow)$. Now we assume that $\left(\frac{3}{p}\right)=1$ and by (*) and (**) of part (i) we have $p\equiv\pm 1\equiv 1,11\pmod{12}$.

■

(iii) (a) We need to find the prime factors of $62^2 - 3 = 3841$. By part (i) we have the prime factors p of $62^2 - 3 = 3841$ must be of the form $p \equiv 1, 11 \pmod{12}$. The primes of form $p \equiv 1, 11 \pmod{12}$ below 62 are 11, 13, 23, 37, 47, 59 and 61. Clearly 11 is *not* factor of 3841. Dividing 3841 by each of remaining primes until we get a whole number gives $3841 = 23 \times 167$. Now 167 is prime because $\left\lfloor \sqrt{167} \right\rfloor = 12$ and the only prime of form $p \equiv 1, 11 \pmod{12}$ and 11 is *not* a factor of 167. Hence $3841 = 23 \times 167$.

(b) We are asked to find the prime factors p of $104^2 - 3 = 10\,813$. They must satisfy $p \equiv 1, 11 \pmod{12}$. Clearly 11 is a factor because $3 - 1 + 8 - 0 + 1 = 11$ and $11 \mid 11$. We have $10\,813 = 11 \times 983$. Now $\left\lfloor \sqrt{983} \right\rfloor = 31$ so the only primes p which are of the form $p \equiv 1, 11 \pmod{12}$ below 31 are 11, 13 and 23. We can test that 11 is *not* a factor of 983 so we only need to test 13 and 23:

$$\frac{983}{13} = 75.62 \text{(2dp)}, \quad \frac{983}{23} = 42.74 \text{(2dp)}$$

Therefore 983 is prime and $10\,813 = 11 \times 983$.

(c) The prime factors p of $200^2 - 3 = 39\,997$ must satisfy $p \equiv 1, 11 \pmod{12}$. Clearly 11 is *not* a factor because $7 - 9 + 9 - 9 + 3 = 1$ and $11 \nmid 1$. The next few primes of this format are 13, 23, 37, 47, 59, 61, … . We trial these primes and find:

$$39\,997 = 23 \times 1739.$$

Next, we find the prime factors of 1739 and again they must of the form $p \equiv 1, 11 \pmod{12}$. We know 13, 23 does *not* go into 1739 so the next prime is 37:

$$1739 = 37 \times 47$$

We have our prime factorization $200^2 - 3 = 39\,997 = 23 \times 37 \times 47$.

(d) We need to find the prime factors of $364^2 - 3 = 132\,493$. By part (i) we know the prime factors p satisfy $p \equiv 1, 11 \pmod{12}$. Clearly 11 is *not* a factor of 132 493. The next few primes of this format $p \equiv 1, 11 \pmod{12}$ are 13, 23, 37, 47, 59, 61, 71, 73, … . Dividing 132 493 by each of these gives

$$\frac{132\ 493}{13} = 10\ 191.77\big(2\text{dp}\big),\ \frac{132\ 493}{23} = 5706.57\big(2\text{dp}\big),\ \frac{132\ 493}{37} = 3580.89\big(2\text{dp}\big),$$
$$\frac{132\ 493}{47} = 2819$$

Therefore $132\ 493 = 47 \times 2819$. Just need to factorize 2819. One prime factor of 2819 is less than or equal to $\left\lfloor \sqrt{2819} \right\rfloor = 53$. We know 13, 23 and 37 do *not* go into 2819 otherwise they would have been factors of 132 493. Just need to check whether 47 goes into 2819 but it doesn't so 2819 is prime and $132\ 493 = 47 \times 2819$.

(e) We are asked to factorize $568^2 - 3 = 322\ 621$. Let p be a prime factor of $322\ 621$ then by part (i) p satisfies $p \equiv 1, 11 \big(\text{mod } 12\big)$. The first few primes of this format are 13, 23, 37, 47, 59, 61, 71, 73,... . Dividing 322 621 by each of these until we get an integer as an answer:

$$\frac{322\ 621}{13} = 24\ 817 \ \Rightarrow\ 322\ 621 = 13 \times 24\ 817$$

Now we find the factors of 24 817:

$$\frac{24\ 817}{13} = 1909 \ \Rightarrow\ 24\ 817 = 13 \times 1909$$

Now finding the factors of 1909:

$$\frac{1909}{13} = 146.85\big(2\text{dp}\big),\ \frac{1909}{23} = 83$$

Therefore $1909 = 23 \times 83$ where both 23 and 83 and prime. So our prime factorization of $322\ 621 = 13 \times 24\ 817 = 13^2 \times 23 \times 83$.

12. (a) We are asked to show that $x^2 \equiv 3 \big(\text{mod } F_n\big)$ where the Fermat prime $F_n = 2^{2^n} + 1$ has *no* solutions for $n = 1, 2, 3, 4$. *How do we show this?*

By using the result of the last question part (i):

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \ \big(\text{mod } 12\big) \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \ \big(\text{mod } 12\big) \end{cases}$$

We have the following:

When $n = 1$ we have $F_1 = 2^{2^1} + 1 = 5 \equiv 5 \big(\text{mod } 12\big)$ so by the above result we have 3 is a quadratic non-residue of 5.

When $n=2$ we have $F_2 = 2^{2^2}+1 = 17 \equiv 5 \pmod{12}$ so by the above result we have 3 is a quadratic non-residue of 17.

When $n=3$ we have $F_3 = 2^{2^3}+1 = 257 \equiv 5 \pmod{12}$ so by the above result we have 3 is a quadratic non-residue of 257.

When $n=4$ we have $F_4 = 2^{2^4}+1 = 65\,537 \equiv 5 \pmod{12}$ so by the above result we have 3 is a quadratic non-residue of 65 537.

(b) We need to prove $F_n = 2^{2^n}+1 \equiv 5 \pmod{12}$. We use proof by induction.

For $n=1$ we have from part (a) $F_1 = 2^{2^1}+1 = 5 \equiv 5 \pmod{12}$.

Assume the result is true for $n=k$ that is

$$F_k = 2^{2^k}+1 \equiv 5 \pmod{12} \qquad (*)$$

Consider $n=k+1$. We need to show that

$$F_{k+1} = 2^{2^{k+1}}+1 \equiv 5 \pmod{12}$$

Examining the indices of the left – hand side yields

$$\begin{aligned} F_{k+1} = 2^{2^{k+1}}+1 &= 2^{\left(2^{k+1}\right)}+1 \\ &= 2^{\left(2^k \times 2\right)}+1 \\ &= 2^{2^k}2^2+1 \\ &= 4\left(2^{2^k}\right)+1 = 4\left(2^{2^k}+1\right)-3 = 4\underbrace{\left(12k+5\right)}_{\text{by (*)}}-3 = 48k+17 \equiv 5 \pmod{12} \end{aligned}$$

Hence by mathematical induction we have our result $F_n = 2^{2^n}+1 \equiv 5 \pmod{12}$.

13. Proposition (4.19) claims the following:

> If $p = 2n+1$ is prime, then we have the following:
> (a) If $p \equiv \pm 1 \pmod{8}$ then $p \mid \left(2^n - 1\right)$.
> (b) If $p \equiv \pm 3 \pmod{8}$ then $p \mid \left(2^n + 1\right)$.

Proof.

We just provide a proof of part (a). Part (b) is very similar.

We are required to prove that $2^n \equiv 1 \pmod{p}$.

Using Proposition (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 2 is a quadratic residue of $p \;\Leftrightarrow\; p \equiv \pm 1 \pmod{8}$.

By Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

With $a = 2$ we have 2 is a quadratic residue of $p \;\Leftrightarrow\; 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Re-arranging the given prime $p = 2n + 1$ to $\frac{p-1}{2} = n$. Substituting this $\frac{p-1}{2} = n$ into the above gives

$$2^{\frac{p-1}{2}} \equiv 2^n \equiv 1 \pmod{p}.$$

This completes our proof. ■

14. Proposition (4.24) claims the following:

Let q be an odd prime. Any prime factor p of the composite $2^q - 1$ satisfies $p \equiv \pm 1 \pmod{8}$.

Proof.

Let p be a prime factor of $2^q - 1$. By the definition of congruence we have

$$2^q \equiv 1 \pmod{p} \qquad (*)$$

By Proposition (4.23):

Any prime factor p of $2^q - 1$ is of the form $2kq + 1$.

We have $p = 2kq + 1$. Re-arranging this we have

$$\frac{p-1}{2} = qk \qquad (**)$$

Taking the congruence in (*) to the power k gives

$$\left(2^q\right)^k \equiv 2^{qk} \equiv 1^k \equiv 1 \pmod{p}$$

Substituting $qk = \frac{p-1}{2}$ from (**) into the above congruence $2^{qk} \equiv 1 \pmod{p}$ yields

$$2^{qk} \equiv 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

By applying Euler's Criterion (7.5):

$$a \text{ is a quadratic residue of } p \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

We have $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ gives us that 2 is a quadratic residue of p. Writing this in Legendre symbol means we have $\left(\frac{2}{p}\right) = 1$.

By result of question 3(i):

2 is a quadratic residue of prime $p \Leftrightarrow p \equiv \pm 1 \pmod{8}$.

Hence $p \equiv \pm 1 \pmod{8}$. This completes our proof.

■

15. We are asked to find the first primitive root of modulo 223. We are given that 223 is prime so $\phi(223) = 223 - 1 = 222$. The prime factorization of 222 is

$$222 = 2 \times 3 \times 37,$$

and the factors of 222 are 1, 2, 3, 37, 74, 111 and 222.

We only need to test 74 and 111 as the index since all the others are factors of 111 apart from 2 which is easily checked.

If r is a primitive root of modulo 223 then we need to show that $r^{74} \not\equiv 1 \pmod{223}$ and $r^{111} \not\equiv 1 \pmod{223}$. Note that if $p = 223$ then

$$\frac{223-1}{2} = \frac{223-1}{2} = 111.$$

We trial $r = 2$ and test $2^{111} \equiv x \pmod{223}$. This is given by Euler's criterion because:

$$a \text{ is a quadratic residue of } p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Hence, we test the Legendre symbol $\left(\frac{2}{223}\right)$. Since $223 \equiv 7 \equiv -1 \pmod{8}$ so 2 is a quadratic residue of 223 because

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

Therefore $2^{111} \equiv 1 \pmod{223}$ so 2 cannot be a primitive root of modulo 223. We don't need to test whether $2^{74} \equiv 1 \pmod{223}$ because 2 cannot be a primitive root of 223.

Next, we trial $r = 3$ and evaluate the Legendre symbol $\left(\frac{3}{223}\right)$.

$$\left(\frac{3}{223}\right) \underbrace{=}_{\text{Because } 223\equiv 3\left(\text{mod } 4\right)} -\left(\frac{223}{3}\right) \underbrace{=}_{\text{Because } 223\equiv 1\left(\text{mod } 3\right)} -\left(\frac{1}{3}\right) = -1.$$

Therefore 3 is a quadratic non - residue which implies that 3 could be a primitive root of 223 because $3^{111} \equiv -1 \not\equiv 1\left(\text{mod } 223\right)$. We also need to show that $3^{74} \not\equiv 1\left(\text{mod } 223\right)$ because if $3^{74} \equiv 1\left(\text{mod } 223\right)$ then 3 *cannot* be a primitive root of 223. Computing simpler powers of 3 gives

$$3^5 \equiv 243 \equiv 20\left(\text{mod } 223\right)$$

$$3^{10} \equiv \left(3^5\right)^2 \equiv 20^2 \equiv 400 \equiv 177 \equiv -46\left(\text{mod } 223\right)$$

$$3^{11} \equiv -46 \times 3 \equiv -138\left(\text{mod } 223\right)$$

$$3^{12} \equiv -138 \times 3 \equiv -414 \equiv 32\left(\text{mod } 223\right) \quad (*)$$

Using these to evaluate $3^{74} \equiv x\left(\text{mod } 223\right)$:

$$\begin{aligned} 3^{74} &\equiv \left(3^{12}\right)^6 \times 3^2 \equiv \left(32\right)^6 \times 9 \\ &\equiv \left(32^3\right)^2 \times 9 \equiv 32\ 768^2 \times 9 \\ &\equiv 210^2 \times 9 \equiv \left(-13\right)^2 \times 9 \equiv 169 \times 9 \equiv 1521 \equiv 183 \not\equiv 1\left(\text{mod } 223\right) \end{aligned}$$

Since $3^{74} \equiv 183 \not\equiv 1\left(\text{mod } 223\right)$ so 3 is a primitive root of 223.

We need to use this primitive root 3 to find the square root of $32\left(\text{mod } 223\right)$ which implies that we need to solve $x^2 \equiv 32\left(\text{mod } 223\right)$. Taking index to the base 3 of this yields

$$\text{ind}_3\left(x^2\right) \equiv \text{ind}_3\left(32\right)\left(\text{mod } 222\right) \qquad (\dagger)$$

By the above calculations (*) we have

$$3^{12} \equiv 32\left(\text{mod } 223\right) \text{ which implies } \text{ind}_3\left(32\right) = 12.$$

Substituting this $\text{ind}_3\left(32\right) = 12$ into (†) and using the rules of indices of Chapter 6 we have

$$\begin{aligned} \text{ind}_3\left(x^2\right) &\equiv 12\left(\text{mod } 222\right) \\ 2 \times \text{ind}_3\left(x\right) &\equiv 12\left(\text{mod } 222\right) \quad \left[\text{Linear Form}\right] \end{aligned}$$

The $\gcd\left(2,\ \ 222\right) = 2$ and $2 \mid 12$ so we have two incongruent solutions. Dividing the last congruence by 2 yields

$$\text{ind}_3\left(x\right) \equiv 6\left(\text{mod } 111\right) \ \Rightarrow\ \text{ind}_3\left(x\right) \equiv 6,\ \ 6 + 111 \equiv 6,\ \ 117\left(\text{mod } 222\right).$$

Therefore $x \equiv 3^6,\ 3^{117} \Big(\text{mod } 223\Big)$. We don't need to evaluate $3^{117} \Big(\text{mod } 223\Big)$ because the square roots of $32 \Big(\text{mod } 223\Big)$ are given by

$$x \equiv \pm 3^6 \equiv \pm 729 \equiv \pm 60 \equiv 60,\ -60 \equiv 60,\ 163 \Big(\text{mod } 223\Big).$$

The square roots of $32 \Big(\text{mod } 223\Big)$ are $60,\ 163 \Big(\text{mod } 223\Big)$.