Complete Solutions to Exercise 7.4

1. In each case we use the corollary:

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

(a) We are asked to see if $x^2\equiv 12\pmod{89}$ is solvable. This means we need to determine the Legendre symbol $\left(\frac{12}{89}\right)$. We know that $12=2^2\times 3$ so

$$\left(\frac{12}{89}\right)=\underbrace{\left(\frac{2^2}{89}\right)}_{=1 \text{ because } 2^2 \text{ is a quadratic residue}}\times\left(\frac{3}{89}\right)=1\times\left(\frac{3}{89}\right)=\left(\frac{3}{89}\right)\qquad(\dagger)$$

Since $89\equiv 1\pmod 4$ so by using (7.17) on the right-hand side of (†) we have

$$\left(\frac{3}{89}\right)=\left(\frac{89}{3}\right)=\left(\frac{2}{3}\right)\quad\left[\text{Because } 89\equiv 2\pmod 3\right].$$

Applying the test for residue 2, Proposition (7.15):

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

To $\left(\frac{2}{3}\right)$ with $3\equiv 3\pmod 8$ gives $\left(\frac{2}{3}\right)=-1$. By (†) and this result we have

$$\left(\frac{12}{89}\right)=\left(\frac{3}{89}\right)=\left(\frac{2}{3}\right)=-1.$$

Since $\left(\frac{12}{89}\right)=-1$ so 12 is a quadratic non-residue of 89 which implies that $x^2\equiv 12\pmod{89}$ is unsolvable.

(b) We need to test whether $x^2\equiv 40\pmod{101}$ is solvable. This means we must find the Legendre symbol $\left(\frac{40}{101}\right)$. The prime decomposition of 40 is $40=8\times 5=2^3\times 5$:

$$\left(\frac{40}{101}\right)=\left(\frac{2^3\times 5}{101}\right)=\left(\frac{2^3}{101}\right)\times\left(\frac{5}{101}\right)$$
$$=\underbrace{\left(\frac{2^2}{101}\right)}_{=1}\times\left(\frac{2}{101}\right)\times\left(\frac{5}{101}\right)$$
$$=\left(\frac{2}{101}\right)\times\left(\frac{5}{101}\right) \qquad (\dagger)$$

We use our normal test for residue 2, 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 $p=101\equiv 5\equiv -3\pmod 8$ so $\left(\frac{2}{101}\right)=-1$. Evaluating the other term in (†):

$$\left(\frac{5}{101}\right)\underset{\text{Because } 5\equiv 1\pmod 4}{=}\left(\frac{101}{5}\right)\underset{\text{Because } 101\equiv 1\pmod 5}{=}\left(\frac{1}{5}\right)=1.$$

[Remember 1 is a quadratic residue of any odd prime p.]

Substituting $\left(\frac{2}{101}\right)=-1$ and $\left(\frac{1}{5}\right)=1$ into (†) gives

$$\left(\frac{40}{101}\right)=\left(\frac{2}{101}\right)\times\left(\frac{5}{101}\right)=(-1)\times(1)=-1.$$

Hence 40 is a quadratic non – residue of 101 so $x^2\equiv 40\pmod{101}$ *cannot* be solved.

(c) We are given the quadratic congruence $x^2\equiv 36\pmod{1223}$ and since $36=6^2$ so $x\equiv 6\pmod{1223}$. Therefore $x^2\equiv 36\pmod{1223}$ is solvable.

(d) We have to find whether $x^2\equiv 89\pmod{197}$ is solvable. This means we need to calculate the Legendre symbol $\left(\frac{89}{197}\right)$. Since $89\equiv 1\pmod 4$ so by (7.17) we have

$$\left(\frac{89}{197}\right)=\left(\frac{197}{89}\right)=\left(\frac{19}{89}\right) \qquad \left[\text{Because } 197\equiv 19\left(\text{mod } 89\right)\right]$$
$$=\left(\frac{89}{19}\right) \qquad \left[\text{Because } 89\equiv 1\left(\text{mod } 4\right) \text{ so applying (7.17)}\right]$$
$$=\left(\frac{13}{19}\right) \qquad \left[\text{Because } 89\equiv 13\left(\text{mod } 19\right)\right]$$
$$=\left(\frac{19}{13}\right) \qquad \left[\text{Because } 13\equiv 1\left(\text{mod } 4\right) \text{ so applying (7.17)}\right]$$
$$=\left(\frac{6}{13}\right) \qquad \left[\text{Because } 19\equiv 6\left(\text{mod } 13\right)\right]$$
$$=\left(\frac{2}{13}\right)\times\left(\frac{3}{13}\right) \qquad \left[\text{Because } 6=2\times 3\right]$$

So far we have

$$\left(\frac{89}{197}\right)=\left(\frac{2}{13}\right)\times\left(\frac{3}{13}\right) \qquad (\ddagger)$$

The residue 2 is tested by using Proposition (7.15):

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

Since $13\equiv 5\equiv -3\left(\text{mod } 8\right)$ so using this proposition we have $\left(\frac{2}{13}\right)=-1$.

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

$$\left(\frac{3}{13}\right)=\left(\frac{13}{3}\right) \qquad \left[\text{Because } 13\equiv 1\left(\text{mod } 4\right) \text{ so applying (7.17)}\right]$$
$$=\left(\frac{1}{3}\right)=1 \qquad \left[\text{Because } 13\equiv 1\left(\text{mod } 3\right)\right]$$

Putting these $\left(\frac{2}{13}\right)=-1$ and $\left(\frac{3}{13}\right)=1$ into (‡) gives

$$\left(\frac{89}{197}\right)=\left(\frac{2}{13}\right)\times\left(\frac{3}{13}\right)=-1\times 1=-1.$$

Since $\left(\frac{89}{197}\right)=-1$ so $x^2\equiv 89\left(\text{mod } 197\right)$ is *not* solvable.

(e) We need to test whether $x^2\equiv 197\left(\text{mod } 89\right)$ is solvable. We have to find $\left(\frac{197}{89}\right)$.

Since $89\equiv 1\left(\text{mod } 4\right)$ so by (7.17) we have $\left(\frac{197}{89}\right)=\left(\frac{89}{197}\right)$.

This was evaluated in part (d) and we had $\left(\frac{89}{197}\right) = -1 = \left(\frac{197}{89}\right)$. Hence $x^2 \equiv 197 \pmod{89}$ is unsolvable.

2. We need to find $(-1)^{\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)}$ for (i) $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$ and (ii) $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$.

(i) We are given that $p \equiv 1 \pmod 4$, $q \equiv 3 \pmod 4$ so there are integers k and m such that

$$p = 4k+1 \text{ and } q = 4m+3$$

Substituting these into the index $\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)$ gives

$$\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right) = \left(\frac{4k+1-1}{2}\right)\times\left(\frac{4m+3-1}{2}\right)$$
$$= 2k\times(2m+1) \qquad [\text{Even Number}]$$

So $(-1)^{\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)} = (-1)^{2k\times(2m+1)} = 1$.

(ii) Similarly, for $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$ by interchanging p and q we have $(-1)^{\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)} = 1$.

3. We need to show that:

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

Proof.

We have by the Law of Quadratic Reciprocity:

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

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

We found in Example 17 and question 2 above that if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ then $\left(\frac{p}{q}\right)\times\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)} = 1$ and if $p \equiv q \equiv 3 \pmod 4$ then

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

This is our required result.

■

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

Proof.

To prove this we use the following corollary:

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

If our given $p\equiv 1 \pmod 4$ then by this corollary we have

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right).$$

If $p\equiv 3 \pmod 4$ then by this corollary, we have

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

This proves our required result.

■

5. (i) We are required to prove that for prime $p>3$ we have

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

Proof.

Since $-3=-1\times 3$ so

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\times\left(\frac{3}{p}\right) \qquad (\dagger)$$

By (7.11) we have

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

By result of question 11(i) of Exercise 7.3 we have

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

We use these two results and (†).

Consider the two cases (i) $p\equiv 1 \pmod 6$ and (ii) $p\equiv 5 \pmod 6$.

Case (i)

Let $p\equiv 1 \pmod 6$ then there is a positive integer such that $p=6k+1$. Now either k is even or odd. Let us first take k to be even then $k=2m$ where m is a positive integer. Substituting this into $p=6k+1$ gives

$$p=6(2m)+1=12m+1=4(3m)+1.$$

Hence $p\equiv 1 \pmod{12}$ and $p\equiv 1 \pmod 4$ so using the above results and (†):

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

Now let us take k to be odd so $k=2n+1$ where n is a positive integer. Putting this into $p=6k+1$ gives

$$p=6(2n+1)+1=12n+7=4(3n+1)+3.$$

Therefore $p\equiv 7 \pmod{12}$ and $p\equiv 3 \pmod 4$ so again using the above results with (†):

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

In both cases (k is odd and even) we have $\left(\frac{-3}{p}\right)=1$ if $p\equiv 1 \pmod 6$. This proves the first part of the result.

Case (ii)

Let $p\equiv 5 \pmod 6$ then there is a positive integer k such that $p=6k+5$. Now either k is even or odd. Let us first take k to be even then $k=2m$ where m is a positive integer. Substituting this into $p=6k+5$ gives

$$p=6(2m)+5=12m+5=4(3m+1)+1.$$

Hence $p\equiv 5 \pmod{12}$ and $p\equiv 1 \pmod 4$ so using the above results and (†):

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

Now let us take k to be odd so $k = 2n+1$ where n is a positive integer. Putting this into $p = 6k+5$ gives

$$p = 6\big(2n+1\big)+5 = 12n+11 = 4\big(3n+2\big)+3\,.$$

Therefore $p \equiv 11 \pmod{12}$ and $p \equiv 3 \pmod{4}$ so again using the above results with (†):

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\times\left(\frac{3}{p}\right) = \big(-1\big)\times 1 = -1\,.$$

In both cases (k is odd and even) we have $\left(\dfrac{-3}{p}\right) = -1$ if $p \equiv 5\big(\mathrm{mod}\ 6\big)$. This proves the second part of the result.

Therefore, we have $\left(\dfrac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$. This is our required result.

■

(ii) We use the result of part (i) to factorize each of the integers in this part.

(a) We are asked to find the prime factorization of $104^2 + 3 = 10\,819$. Since our integer is of the form n^2+3 so the odd prime factors p of this 104^2+3 must satisfy $p \equiv 1\big(\mathrm{mod}\ 6\big)$. The first few primes are 7, 13, 19, 31, 37, 43, ---. Dividing $10\,819$ by each of these we find that

$$10\,819 = 31\times 349\,.$$

We have $\left\lfloor\sqrt{349}\right\rfloor = 18$ and none of the primes in the above list below 18 go into 349, so 349 is prime. Hence $10\,819 = 31\times 349$.

(b) We need to find the prime factorization of $236^2 + 3 = 55\,699$. Let p be a prime factor of 236^2+3 then $p \equiv 1\big(\mathrm{mod}\ 6\big)$ and the primes of this form are 7, 13, 19, 31, 37, 43, 61, 67, 73 --- and we find that

$$\frac{55\,699}{73} = 763 \;\Rightarrow\; 55\,699 = 73\times 763\,.$$

We just need to factorize 763 but let us first see which primes we need to test. We have $\left\lfloor\sqrt{763}\right\rfloor = 27$ and there are *no* primes in the above list which are below 27 and go into 763. *How do we know this?*

Because if there was a smaller prime then it would also be a factor of 55 699 and the first prime to be a factor of 55 699 is 73. Therefore 763 is prime and $55\,699 = 73\times 763$.

(c) We are asked to factorize $362^2+3=131\,047$. Let p be a prime factor of this number then $p\equiv 1\pmod 6$. The first of these is 7 and we find that

$$\frac{131\,047}{7}=18\,721.$$

From this we have $\left\lfloor\sqrt{18\,721}\right\rfloor=136$. We need to now try prime factors which satisfy $p\equiv 1\pmod 6$ and first few are 7, 13, 19, 31, 37, 43, 61, 67, 73, 79 and 97 which is a factor of 18 721 because $18\,721=97\times 193$. Now 193 is prime so the prime factorization of $131\,047=7\times 97\times 193$.

6. We are required to prove that prime factors of the integer n^2-n+1 are of the form $6k+1$.

Proof.

Let p be an arbitrary prime factor of the given integer n^2-n+1. We have

$$n^2-n+1\equiv 0\pmod p.$$

By using the given hint in the question consider the integer

$$(2n-1)^2=4n^2-4n+1=4(n^2-n+1)-3.$$

Using the first result we have

$$(2n-1)^2\equiv 4\underbrace{(n^2-n+1)}_{\equiv 0\pmod p}-3\equiv 0-3\equiv -3\pmod p \qquad (*)$$

Let $x=2n-1$ and substituting this into (*) yields

$$x^2\equiv -3\pmod p$$

This is a quadratic congruence. Hence we need to find for which primes p is the Legendre symbol $\left(\frac{-3}{p}\right)=1$ because when the Legendre symbol is equal to 1 we have a quadratic residue.

By the result of the previous question:

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

Hence the prime p must be of the form $p\equiv 1\pmod 6$ so $p=6k+1$ for some positive integer k.

■

7. We are asked to prove that there are infinitely many primes of the form $8k-1$.

Proof.

We use the given hint and suppose there are *finitely* many primes of the form $8k-1$ which we can denote as $p_1, p_2, \cdots, p_k$. Let $n = p_1 \times p_2 \times \cdots \times p_k$ and consider the integer $N = (4n)^2 - 2$. Clearly N is composite because 2 is factor of N. Let p be a prime factor greater than 2 (or an odd prime) of N. Then

$$N \equiv (4n)^2 - 2 \equiv 0 \pmod{p}.$$

Let $x = 4n$ then we have

$$N \equiv x^2 - 2 \equiv 0 \pmod{p} \quad \Rightarrow \quad x^2 \equiv 2 \pmod{p}$$

This $x^2 \equiv 2 \pmod{p}$ and is solvable because $x = 4n$ so $\left(\frac{2}{p}\right) = 1$. By question 3(i) of Exercises 7.3:

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

we have $p \equiv \pm 1 \pmod{8}$, which implies that

$$p = 8k+1 \text{ or } p = 8k-1.$$

If *all* the prime factors greater than 2 of N are of the form $8k+1$ then the product of this is also of the form $8m+1$ (this can be shown by induction) but this is impossible because $N = (4n)^2 - 2$. Hence N must have a prime factor of the form $p = 8k-1$. Clearly this $p = 8k-1$ is *not one* in the above list $p_1, p_2, \cdots, p_k$. *Why not?*

If it is then $p \mid n$ so $p \mid (4n)^2$ and $p \mid N$ and since $N = (4n)^2 - 2$ so

$$p \mid 2.$$

This is impossible because p is an odd prime.

Hence there are infinitely many primes of the form $8k-1$.

■

8. We need to find the given sum $\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{k \times p}{q} \right\rfloor + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{k \times q}{p} \right\rfloor$ for the primes $p = 17$ and $q = 13$. Substituting these $p = 17$ and $q = 13$ into $\frac{p-1}{2}$ and $\frac{q-1}{2}$ respectively gives

$$\frac{p-1}{2}=\frac{17-1}{2}=8 \text{ and } \frac{q-1}{2}=\frac{13-1}{2}=6\,.$$

Evaluating the sum separately:

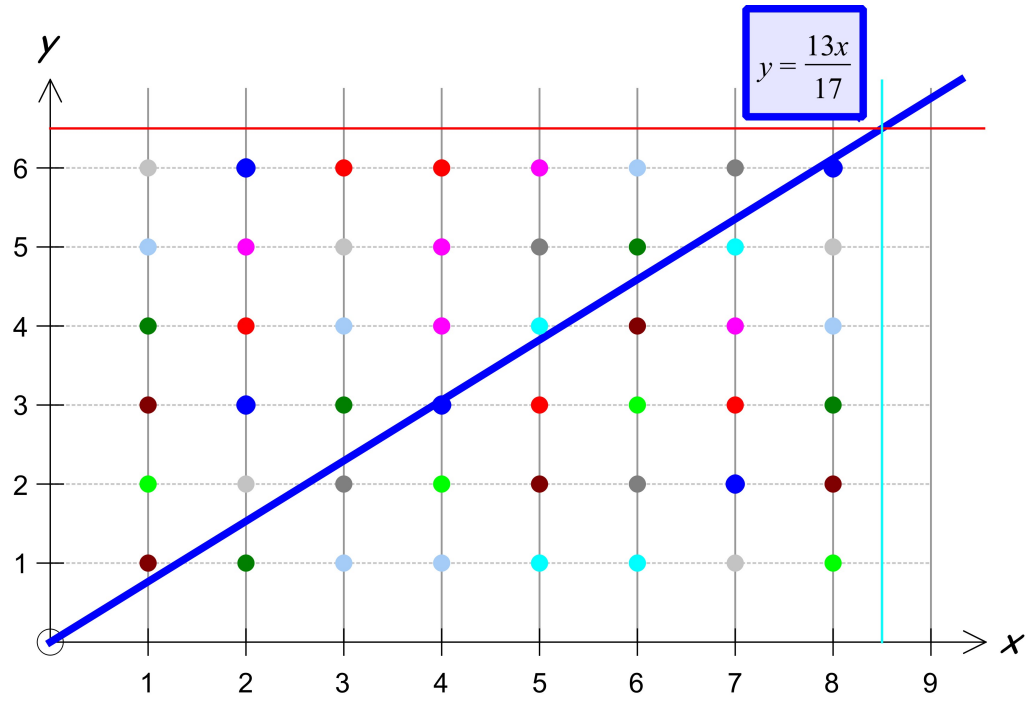
$$\begin{aligned}\sum_{k=1}^{6}\left\lfloor\frac{k\times 17}{13}\right\rfloor &= \left\lfloor\frac{1\times 17}{13}\right\rfloor+\left\lfloor\frac{2\times 17}{13}\right\rfloor+\left\lfloor\frac{3\times 17}{13}\right\rfloor+\left\lfloor\frac{4\times 17}{13}\right\rfloor+\left\lfloor\frac{5\times 17}{13}\right\rfloor+\left\lfloor\frac{6\times 17}{13}\right\rfloor\\ &=\left\lfloor\frac{17}{13}\right\rfloor+\left\lfloor\frac{34}{13}\right\rfloor+\left\lfloor\frac{51}{13}\right\rfloor+\left\lfloor\frac{68}{13}\right\rfloor+\left\lfloor\frac{85}{13}\right\rfloor+\left\lfloor\frac{102}{13}\right\rfloor\\ &=1+2+3+5+6+7=24\end{aligned}$$

$$\begin{aligned}\sum_{k=1}^{8}\left\lfloor\frac{k\times 13}{17}\right\rfloor &= \left\lfloor\frac{1\times 13}{17}\right\rfloor+\left\lfloor\frac{2\times 13}{17}\right\rfloor+\left\lfloor\frac{3\times 13}{17}\right\rfloor+\left\lfloor\frac{4\times 13}{17}\right\rfloor+\left\lfloor\frac{5\times 13}{17}\right\rfloor+\left\lfloor\frac{6\times 13}{17}\right\rfloor+\left\lfloor\frac{7\times 13}{17}\right\rfloor+\left\lfloor\frac{8\times 13}{17}\right\rfloor\\ &=\left\lfloor\frac{13}{17}\right\rfloor+\left\lfloor\frac{26}{17}\right\rfloor+\left\lfloor\frac{39}{17}\right\rfloor+\left\lfloor\frac{52}{17}\right\rfloor+\left\lfloor\frac{65}{17}\right\rfloor+\left\lfloor\frac{78}{17}\right\rfloor+\left\lfloor\frac{91}{17}\right\rfloor+\left\lfloor\frac{104}{17}\right\rfloor\\ &=0+1+2+3+3+4+5+6=24\end{aligned}$$

Adding both these summations gives

$$\sum_{k=1}^{6}\left\lfloor\frac{k\times 17}{13}\right\rfloor+\sum_{k=1}^{8}\left\lfloor\frac{k\times 13}{17}\right\rfloor=24+24=48$$

Drawing the graph gives:



The number of lattice points shown in this graph is $6\times 8=48$ which is given by the above sum.

9. (See Example 17.) Consider the two different cases:

(a) $p\equiv 1\pmod 4$ or $q\equiv 1\pmod 4$.

(b) Both $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$.

Case (a)

Let $p \equiv 1 \pmod 4$ then there exists a positive integer k such that $p = 4k+1$.

Putting this into the index of Law of Quadratic Reciprocity $\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)$ we have

$$\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right) = \left(\frac{4k+1-1}{2}\right)\times\left(\frac{q-1}{2}\right) = 2k\times\left(\frac{q-1}{2}\right) \qquad \left[\text{Even because } q \text{ is odd}\right]$$

$$\left(\frac{p}{q}\right)\times\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right)} = (-1)^{2k\times\left(\frac{q-1}{2}\right)} = 1 \qquad \left[\text{Because index is even}\right]$$

Since $\left(\frac{p}{q}\right)\times\left(\frac{q}{p}\right) = 1$ so $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$ or $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$. Either way $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

We can present the same argument with $q \equiv 1 \pmod 4$.

Case (b)

Let $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$ then there are positive integers k and m such that

$$p = 4k+3 \text{ and } q = 4m+3.$$

Substituting this into the index of the Law of Quadratic Reciprocity yields

$$\left(\frac{p-1}{2}\right)\times\left(\frac{q-1}{2}\right) = \left(\frac{4k+3-1}{2}\right)\times\left(\frac{4m+3-1}{2}\right)$$

$$= \left(\frac{4k+2}{2}\right)\times\left(\frac{4m+2}{2}\right) = (2k+1)\times(2m+1) \qquad \left[\text{Odd number}\right]$$

Therefore $\left(\frac{p}{q}\right)\times\left(\frac{q}{p}\right) = (-1)^{(2k+1)(2m+1)} = -1$ because $(2k+1)(2m+1)$ is odd.

We have $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{q}{p}\right) = -1$ or $\left(\frac{p}{q}\right) = -1$ and $\left(\frac{q}{p}\right) = 1$. Hence $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

This completes our proof.

■

10. We need to prove that $\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \equiv g \pmod 2$ where $p \not| a$ and g be the number of negative residues defined in Gauss's Lemma.

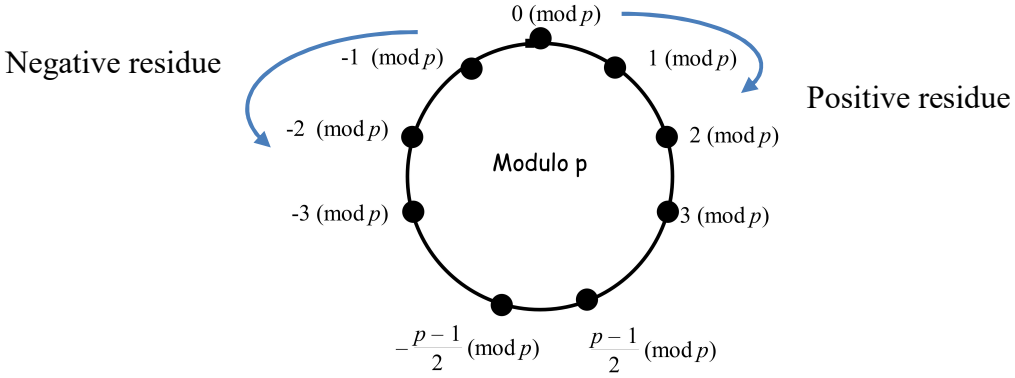
Proof.

Let S be the set of the product of k and a where $k = 1,\ 2,\ 3,\ \cdots,\ \frac{p-1}{2}$:

$$S = \left\{ a,\ 2a,\ 3a,\ \ 4a,\ \cdots,\ \left(\frac{p-1}{2}\right)a \right\}.$$

The integer g is defined as the number of negative residues in this list, these are the ones which are greater than $\frac{p-1}{2}$.

We can write each of these ka as a residue of modulo p which lies between $-\left(\frac{p-1}{2}\right)$ and $\left(\frac{p-1}{2}\right)$. We can illustrate this on a modulo p clock:



Denoting each of these residues by r_k, that is

$$ka \equiv r_k \pmod p.$$

If r_k is *positive* then ka is one of the least positive residues in the set

$$T = \left\{ 1,\ 2,\ 3,\ \ 4,\ \cdots,\ \left(\frac{p-1}{2}\right) \right\}$$

We need to consider the floor function $\left\lfloor \frac{ka}{p} \right\rfloor$. So dividing these integers in the set T by p and then evaluating the floor function gives

$$T' = \left\{ \left\lfloor \frac{1}{p} \right\rfloor,\ \left\lfloor \frac{2}{p} \right\rfloor,\ \left\lfloor \frac{3}{p} \right\rfloor,\ \left\lfloor \frac{4}{p} \right\rfloor,\ \cdots,\ \left\lfloor \frac{p-1}{2p} \right\rfloor \right\} = \left\{ 0,\ 0,\ 0,\ 0,\ \cdots,\ 0 \right\}$$

If r_k is *negative,* then ka is one of the negative residues in the set

$$U=\left\{-1,\ -2,\ -3,\ \ -4,\ \cdots,\ -\left(\frac{p-1}{2}\right)\right\}$$

Similarly finding the floor function $\left\lfloor\frac{ka}{p}\right\rfloor$ gives

$$U'=\left\{\left\lfloor-\frac{1}{p}\right\rfloor,\ \left\lfloor-\frac{2}{p}\right\rfloor,\ \left\lfloor-\frac{3}{p}\right\rfloor,\ \ \left\lfloor-\frac{4}{p}\right\rfloor,\ \cdots,\ \left\lfloor-\frac{p-1}{2p}\right\rfloor\right\}=\left\{-1,\ -1,\ -1,-1,\ \cdots,\ -1\right\}$$

Evaluating the sum $\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ka}{p}\right\rfloor$ gives

$$\begin{aligned}\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ka}{p}\right\rfloor&=\left\lfloor\frac{a}{p}\right\rfloor+\left\lfloor\frac{2a}{p}\right\rfloor+\left\lfloor\frac{3a}{p}\right\rfloor+\cdots+\left\lfloor\left(\frac{p-1}{2}\right)\frac{a}{p}\right\rfloor\\&\equiv 0+0+\underbrace{\left(-1-1-\cdots-1\right)}_{g=\text{Number of negative residues}}+0\cdots+0\\&\equiv -g\ \left(\text{mod }p\right)\end{aligned}$$

Taking modulo 2 we have

$$\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ka}{p}\right\rfloor\equiv -g\equiv g\ \left(\text{mod }2\right)$$

This is our required result.

■

11. Substituting $p=13$ and $a=16$ into $\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{ka}{p}\right\rfloor$ gives

$$\begin{aligned}\sum_{k=1}^{6}\left\lfloor\frac{16k}{p}\right\rfloor&=\left\lfloor\frac{16}{13}\right\rfloor+\left\lfloor\frac{32}{13}\right\rfloor+\left\lfloor\frac{48}{13}\right\rfloor+\left\lfloor\frac{64}{13}\right\rfloor+\left\lfloor\frac{80}{13}\right\rfloor+\left\lfloor\frac{96}{13}\right\rfloor\\&=1+2+3+4+6+7=23\end{aligned}$$

We have $ka=16,\ 32,\ 48,\ 64,\ 80,\ 96$, Writing these integers as residues between -6 and 6 of modulo 13 gives

$$ka\equiv 16\equiv 3,\ \ 32\equiv 6,\ \ 48\equiv -4,\ \ 64\equiv -1,\ \ 80\equiv 2,\ 96\equiv 5\ \left(\text{mod }13\right)$$

Hence $g=2$. We have $23\not\equiv 2\left(\text{mod }2\right)$. *Why doesn't Lemma (7.20) work in this case?*

Because $a=16$ but in the Lemma it states that let 'a also be odd'.

12. We need to prove that *odd* prime divisors of the integer n^2+1 are of the form $4k+1$.

Proof.

Let p be an odd prime divisor of n^2+1, that is

$$n^2+1 \equiv 0 \pmod{p} \text{ implies that } n^2 \equiv -1 \pmod{p}.$$

By question 6 of Exercises 7.1:

-1 is a QR of an odd prime $p \Leftrightarrow p \equiv 1 \pmod{4}$.

The quadratic congruence $n^2 \equiv -1 \pmod{p}$ has solutions so $p \equiv 1 \pmod{4}$ which implies that $p = 4k+1$.

■

13. We need to prove that there are an infinite number of primes of the form $3m+1$.

Proof.

Suppose there are a finite number of primes of the form $3m+1$ which we can write in a list as

$$p_1,\ p_2,\ p_3,\ \cdots,\ p_n$$

Consider the integer

$$N = \left(3 \times p_1 \times p_2 \times p_3 \times \cdots \times p_n\right)^2 + 3.$$

N is composite because 3 is a factor of N. This implies that we must have a prime factor, $p > 3$ say of N. By using modular arithmetic we have

$$\left(3 \times p_1 \times p_2 \times p_3 \times \cdots \times p_n\right)^2 + 3 \equiv 0 \pmod{p} \quad \Rightarrow \quad \left(3 \times p_1 \times p_2 \times p_3 \times \cdots \times p_n\right)^2 \equiv -3 \pmod{p}$$

Let $3 \times p_1 \times p_2 \times p_3 \times \cdots \times p_n = x$ then the above can be written as

$$x^2 \equiv -3 \pmod{p}.$$

This is a quadratic congruence. We know it has solutions because $x = 3 \times p_1 \times p_2 \cdots \times p_n$ so it is solvable. By the result of question 5:

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

We have $p \equiv 1 \pmod{6}$ so $p = 6k+1$. Writing this as a factor of 3 gives

$$p = 3(2k)+1$$

We have $p = 3(2k)+1$ which is of the form $3m+1$ and is a prime factor of N, that is $p \mid N$. Since p is of the form $3m+1$ so it must be one in the above finite list

$$p_1,\ p_2,\ p_3,\ \cdots,\ p_n.$$

From this we have $p \mid \left(3 \times p_1 \times p_2 \times p_3 \times \cdots \times p_n\right)^2$.

Since

$$N = \left(3 \times p_1 \times p_2 \times p_3 \times \cdots \times p_n\right)^2 + 3$$

And $p \mid N$ and $p \mid \left(3 \times p_1 \times p_2 \times p_3 \times \cdots \times p_n\right)^2$ so $p \mid 3$ this is impossible because $p > 3$. We have a contradiction so there are an infinite number of primes of the form $3m + 1$.

14. (a) We are required to find x in $25^{997} \equiv x \pmod{1993}$ given that 1993 is prime. Using 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 $a = 25 = 5^2$ so clearly 5 is a quadratic residue of 1993 so by (7.5) we have

$$25^{\frac{1993-1}{2}} \equiv 25^{996} \equiv 1 \pmod{1993}$$

Multiplying both sides of this result $25^{996} \equiv 1 \pmod{1993}$ by 25 yields

$$25 \times 25^{996} \equiv 25^{997} \equiv 25 \pmod{1993}$$

Hence $x \equiv 25 \pmod{1993}$.

(b) We are asked to find the least positive residue x in $26^{997} \equiv x \pmod{1993}$. The prime decomposition of 26 is 2×13. We need to check that if 2 and 13 are quadratic residues of 1993 because

$$\left(\frac{26}{1993}\right) = \left(\frac{2}{1993}\right) \times \left(\frac{13}{1993}\right) \qquad (*)$$

For 2 we use (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 $1993 \equiv 1 \pmod{8}$ so $\left(\frac{2}{1993}\right) = 1$ which implies that 2 is a quadratic residue of 1993.

We need to find the other Legendre symbol $\left(\frac{13}{1993}\right)$. Since $13 \equiv 1 \pmod{4}$ so by

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

We have

$$\left(\frac{13}{1993}\right)=\left(\frac{1993}{13}\right)=\left(\frac{4}{13}\right) \qquad \left[\text{Because } 1993\equiv 4\pmod{13}\right]$$
$$=\left(\frac{2^2}{13}\right)=1 \qquad \left[\text{Because } 2^2 \text{ is a quadratic residue}\right]$$

Substituting these into (*) yields

$$\left(\frac{26}{1993}\right)=\left(\frac{2}{1993}\right)\times\left(\frac{13}{1993}\right)=1\times 1=1.$$

Hence 26 is a quadratic residue of 1993 so by Euler's Criterion

$$26^{\frac{1993-1}{2}}\equiv 26^{996}\equiv 1\pmod{1993}.$$

Therefore $26^{997}\equiv 26\pmod{1993}$ or $x\equiv 26\pmod{1993}$.

15. We are required to prove that if $p=8k+1$ then $p\left|\left(2^{\frac{p-1}{2}}-1\right)\right.$.

Proof.

We are given $p=8k+1$ therefore $p\equiv 1\pmod 8$. By

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

We have $\left(\frac{2}{p}\right)=1$ which implies that 2 is a quadratic residue of p. By Euler's Criterion (7.5):

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

Using this criterion with $a=2$ we have

$$2^{\frac{p-1}{2}}\equiv 1\pmod p \;\Rightarrow\; 2^{\frac{p-1}{2}}-1\equiv 0\pmod p.$$

Since $2^{\frac{p-1}{2}}-1\equiv 0\pmod p$ so we conclude that $p\left|\left(2^{\frac{p-1}{2}}-1\right)\right.$. This completes our proof.

■

16. We are asked to show that $\left(\frac{2a}{p}\right)=\left(\frac{a}{p}\right)$ provided $p\equiv 1\left(\text{mod } 4\right)$.

Proof.

Factorizing $2a=2\times a$ so

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

We are given that $p\equiv 1\left(\text{mod } 4\right)$ therefore by (7.15):

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

This implies that if $p\equiv 1\left(\text{mod } 8\right)$ which in turn implies that $p=8k+1=4\left(2k\right)+1$ then

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

Substituting this into (‡) gives $\left(\frac{2a}{p}\right)=\left(\frac{2}{p}\right)\times\left(\frac{a}{p}\right)=1\times\left(\frac{a}{p}\right)=\left(\frac{a}{p}\right)$.

This completes our proof.

■

17. We need to show that if $p\equiv 1\left(\text{mod } 4\right)$ then $\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)=0$.

Proof.

We need to show that $\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)=\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-1}{2p}\right)=0$.

From question 7(a) of the Exercise 7.1 we have the following result:

If a is a quadratic residue then $p-a$ is a quadratic residue $\Leftrightarrow p\equiv 1\left(\text{mod } 4\right)$.

Consider the set

$$S=\left\{\underbrace{1,\ 2,\ 3,\ \cdots,\ \frac{p-1}{2}}_{\text{First half of the least positive residues modulo } p},\quad \underbrace{\frac{p+1}{2},\ \cdots,\ p-3,\ p-2,\ p-1}_{\text{Last half of the least positive residues modulo } p}\right\}$$

The above result claims that if 1 is a quadratic residue then so is $p-1$ and if 2 is a quadratic residue so is $p-2$ and so on.

This implies that the quadratic residues in the above list are symmetrical. By Proposition (7.4):

There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues of p.

Since the list in S is symmetrical so half the residues in the first half, that is

$$\underbrace{1,\ 2,\ 3,\ \cdots,\ \frac{p-1}{2}}_{\text{First half of the least positive residues modulo } p},$$

must be quadratic residues and half of these must be quadratic non-residues. By the definition of the Legendre symbol (7.7):

$$\left(\frac{a}{p}\right)=\begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic non-residue of } p \end{cases}$$

Therefore

$$\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)=\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\cdots+\left(\frac{p-1}{2p}\right)=0$$

This is our required result.

■

18. We are given the following table:

Prime p	3	7	11	13	17	19	23	29	31
$\left(5/p\right)$	-1	-1	1	-1	-1	1	-1	1	1

Prediction is

$$\left(\frac{5}{p}\right)=\begin{cases} 1 & \text{if } p\equiv\pm1\left(\text{mod } 5\right) \\ -1 & \text{if } p\equiv\pm2\left(\text{mod } 5\right) \end{cases}$$

We need to prove this.

Proof.

We need to consider the four different cases:

(i) $p\equiv 1\left(\text{mod } 5\right)$ (ii) $p\equiv -1\left(\text{mod } 5\right)$

(iii) $p\equiv 2\left(\text{mod } 5\right)$ (iv) $p\equiv -2\left(\text{mod } 5\right)$

In each case we use the popular corollary:

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

Since $5\equiv 1\left(\text{mod } 4\right)$ we have $\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$.

Case (i):

Applying this to $p \equiv 1 \pmod 5$:

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

Case (ii):

This time $p \equiv -1 \pmod 5$ so

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) \qquad \left[\text{Because } p \equiv -1 \pmod 5\right]$$

Using

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

We have $\left(\frac{5}{p}\right) = \left(\frac{-1}{5}\right) = 1$ because $5 \equiv 1 \pmod 4$.

Case (iii):

We consider the case $p \equiv 2 \pmod 5$:

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

Applying the following to $\left(2/5\right)$:

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

In view of $5 \equiv -3 \pmod 8$ we have

$$\left(\frac{5}{p}\right) = \left(\frac{2}{5}\right) = -1\,.$$

Case (iv):

This time we have $p \equiv -2 \pmod 5$ so

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

Therefore

$$\left(\frac{5}{p}\right) = \left(\frac{-2}{5}\right) = \underbrace{\left(\frac{-1}{5}\right)}_{=1 \text{ by (7.11)}} \times \underbrace{\left(\frac{2}{5}\right)}_{=-1 \text{ by (7.15)}} = 1 \times (-1) = -1$$

We have considered all four cases and shown our predicted formula.

■

To factorize each of the given integers we need to use our predicted formula:

$$\left(\frac{5}{p}\right)=\begin{cases}1 & \text{if } p\equiv\pm1\pmod 5\\ -1 & \text{if } p\equiv\pm2\pmod 5\end{cases}$$

(a) We are asked to factorize $104^2-5=10\,811$. Let p be a prime factor of 10 811 therefore p satisfies $p\equiv\pm1\pmod 5$. The first couple of primes of this format are 11, 19 and we find that $10\,811=19\times569$. Also $\left\lfloor\sqrt{569}\right\rfloor=23$ so we only need to test if 19 goes into 569 but it doesn't so 569 is prime. Hence $10\,811=19\times569$.

(b) Like part (a) we must find the prime factorization of

$$504^2-5=254\,011$$

Let p be a prime factor of this number then $p\equiv\pm1\pmod 5$ and testing primes of this format 11, 19, 29, 31, 41, ---. Clearly 11 is *not* a factor because adding the digits of 254 011 gives $1-1+0-4+5-2=-1$ and $11\not|\,(-1)$. Trying 19 we have

$$254011=19\times13\,369$$

Also $\left\lfloor\sqrt{13\,369}\right\rfloor=115$ so we need to test primes up to 115. Again 11 *cannot* be a factor as it is not a factor of the original number. We find that 19 is also *not* a factor. The next prime after 19 of the format $p\equiv\pm1\pmod 5$ is 29 and

$$13\,369=29\times461$$

Also 461 is prime because we have tested primes up to 29 and $\left\lfloor\sqrt{461}\right\rfloor=21$. Hence $254011=19\times29\times461$.

19. We need to prove:

$$\left(\frac{7}{p}\right)=1 \quad \text{if } p\equiv\pm1,\ \pm3,\ \pm9\pmod{28}$$

Proof.

Arguing along similar lines to solution of previous question we have the following cases:

$p\equiv1\pmod{28}$:

Since $p \equiv 1 \pmod{28}$ so $p = 28k+1 = 7(4k)+1 = 4(7k)+1$ which implies that $p \equiv 1 \pmod 7$ and $p \equiv 1 \pmod 4$. Applying (7.17) we have

$$\left(\frac{7}{p}\right) \underset{\text{By (7.17)}}{\equiv} \left(\frac{p}{7}\right) \underset{\text{Because } p \equiv 1 \pmod 7}{\equiv} \left(\frac{1}{7}\right) = 1.$$

$p \equiv -1 \pmod{28}$:

Since $p \equiv -1 \pmod{28}$ so $p = 28k-1 = 7(4k)-1$ which implies that $p \equiv -1 \pmod 7$ and $p \equiv -1 \equiv 3 \pmod 4$:

$$\left(\frac{7}{p}\right) \underset{\text{By (7.17)}}{\equiv} -\left(\frac{p}{7}\right) \underset{\text{Because } p \equiv -1 \pmod 7}{\equiv} -\left(\frac{-1}{7}\right) \qquad (\dagger)$$

Now we use the test for residue -1 which is

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

As $7 \equiv 3 \pmod 4$ so applying (7.11) gives $\left(-1/7\right) = -1$. Substituting this into (†) yields

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

$p \equiv 3 \pmod{28}$:

In view of $p \equiv 3 \pmod{28}$ so $p = 28k+3 = 7(4k)+3 = 4(7k)+3$ which implies that $p \equiv 3 \pmod 7$ and $p \equiv 3 \pmod 4$. Applying (7.17) we have

$$\left(\frac{7}{p}\right) \underset{\text{By (7.17)}}{\equiv} -\left(\frac{p}{7}\right) \underset{\text{Because } p \equiv 3 \pmod 7}{\equiv} -\left(\frac{3}{7}\right)$$

$$\underset{\text{by (7.17)}}{\equiv} --\left(\frac{7}{3}\right) = +\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1 \quad \left[\text{Because } 7 \equiv 1 \pmod 3\right]$$

$p \equiv -3 \pmod{28}$:

In view of $p \equiv -3 \pmod{28}$ so $p = 28k-3 = 7(4k)-3 = 4(7k)-3$ which implies that $p \equiv -3 \pmod 7$ and $p \equiv -3 \equiv 1 \pmod 4$. Applying (7.17) we have

$$\left(\frac{7}{p}\right) \underset{\text{By (7.17)}}{\equiv} \left(\frac{p}{7}\right) \underset{\text{Because } p \equiv -3 \pmod 7}{\equiv} \left(\frac{-3}{7}\right) = \left(\frac{-1}{7}\right) \times \left(\frac{3}{7}\right) \qquad (*)$$

Evaluating each of the Legendre symbols on the right - hand side of (*).

As $7 \equiv 3 \pmod 4$ so by applying

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

we have $\left(-1/7\right) = -1$. Evaluating the second Legendre symbol in (*):

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

Substituting $\left(\frac{-1}{7}\right) = -1$ and $\left(\frac{3}{7}\right) = -1$ into (*) gives

$$\left(\frac{7}{p}\right) = \left(\frac{-1}{7}\right) \times \left(\frac{3}{7}\right) = \left(-1\right) \times \left(-1\right) = 1.$$

$p \equiv 9 \pmod{28}$:

In view of $p \equiv 9 \pmod{28}$ so $p = 28k + 9 = 7\left(4k+1\right) + 2 = 4\left(7k+2\right) + 1$ which implies that $p \equiv 2 \pmod 7$ and $p \equiv 1 \pmod 4$. Applying (7.17) we have

$$\left(\frac{7}{p}\right) \underbrace{=}_{\text{By (7.17)}} \left(\frac{p}{7}\right) \underbrace{=}_{\text{Because } p \equiv 2 \pmod 7} \left(\frac{2}{7}\right)$$

Using the test for residue 2 which is (7.15):

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

As $7 \equiv -1 \pmod 8$ so by applying this (7.15) we have

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

$p \equiv -9 \pmod{28}$:

Since $p \equiv -9 \pmod{28}$ so $p = 28k - 9 = 7\left(4k-1\right) - 2 = 4\left(7k-2\right) - 1$ which implies that $p \equiv -2 \pmod 7$ and $p \equiv -1 \equiv 3 \pmod 4$. Applying (7.17) we have

$$\left(\frac{7}{p}\right) \underbrace{=}_{\text{By (7.17)}} -\left(\frac{p}{7}\right) \underbrace{=}_{\text{Because } p \equiv -2 \pmod 7} -\left(\frac{-2}{7}\right) = -\left(\frac{-1}{7}\right) \times \left(\frac{2}{7}\right) \qquad (\ddagger)$$

From the previous case we have $\left(\frac{2}{7}\right) = 1$ and from the penultimate case we have $\left(\frac{-1}{7}\right) = -1$. Putting these into the above calculation (‡) yields

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

Hence, we have proven that 7 is a quadratic residue of the primes p which satisfy the congruence:

$$p \equiv \pm 1,\ \pm 3,\ \pm 9 \left(\text{mod } 28\right).$$

■

(a) We are asked to find the prime factorization of $120^2 - 7 = 14\,393$. Using the result of the above theory we have the prime factor must be of the form $p \equiv \pm 1,\ \pm 3,\ \pm 9 \left(\text{mod } 28\right)$. The first few primes of this format are 3, 19, 29, 31, 37 and 37 is a factor of 14 393 because $14\,393 = 37 \times 389$. Also 389 is prime because if it has a prime factor it would be less than 19 and the only factors below 19 of the given format is 3 and 19 and none of these are factors of 389 because they were *not* factors of 14 393. Hence $14\,393 = 37 \times 389$.

(b) Similarly, we have to factorize $354^2 - 7 = 125\,309$. Let p be a factor of this number. Then $p \equiv \pm 1,\ \pm 3,\ \pm 9 \left(\text{mod } 28\right)$. The first few are 3, 19, 29, 31, 37, --- . By trialling these primes we find that $125\,309 = 29 \times 4321$. We need to find the prime factors of 4321. First $\left\lfloor \sqrt{4321} \right\rfloor = 65$. There is no point trailing 3 and 19 as these *not* factors of 125 309 so they *cannot* be factors of 4321. The next prime is 29 and we have $4321 = 29 \times 149$ and 149 is prime. Therefore, the prime factorization of $354^2 - 7 = 125\,309$ is $125\,309 = 29^2 \times 149$

20. We need to show that one of the prime factors of $x^2 + 3$ is of the form $12n + 7$.

Proof.

Let $p > 3$ be a prime factor of $x^2 + 3$. We have

$$x^2 + 3 \equiv 0 \left(\text{mod } p\right) \text{ implies } x^2 \equiv -3 \left(\text{mod } p\right).$$

We have a quadratic congruence $x^2 \equiv -3 \left(\text{mod } p\right)$. We need to show that -3 is a quadratic residue for a prime p of the form $12n + 7$. This implies that $p \equiv 7 \left(\text{mod } 12\right)$.

Using Legendre symbols we have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\times\left(\frac{3}{p}\right) \qquad (\dagger)$$

By (7.11)

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

From this $p\equiv 7\pmod{12}$ we have $p=12k+7=4(3k+1)+3$. Therefore

$$p\equiv 3\pmod 4$$

By (7.11)

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

By result of question 11 of Exercise 7.3 we have

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

$\left(\frac{3}{p}\right)=-1$ because $p\equiv 7\pmod{12}$.

Putting these two results $\left(\frac{-1}{p}\right)=-1$ and $\left(\frac{3}{p}\right)=-1$ into (†) gives

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

Hence -3 is a quadratic residue of a prime $p\equiv 7\pmod{12}$ which implies it is of the form $12n+7$. As we have a solution to the quadratic congruence $x^2+3\equiv 0\pmod p$ so a prime factor of x^2+3 is of the form $12n+7$. This completes our proof.

■

21. We are asked to prove that there are infinite number of primes of the form $3n-1$.

Proof.

Suppose there are a finite number of primes of the form $3n-1$ and they are all

$$p_1,\ p_2,\ \cdots,\ p_n \qquad (*)$$

Consider the number $N=(3\times p_1\times p_2\times\cdots\times p_n)^2-3$. Clearly 3 is a factor of N. Let $p>3$ be another prime factor of N and $x=3\times p_1\times p_2\times\cdots\times p_n$ then

$$N=x^2-3\equiv 0\pmod p.$$

This quadratic congruence $x^2 \equiv 3 \pmod{p}$ has solutions so 3 is a quadratic residue of p. By question 11(ii) of Exercise 7.1 we have

$$3 \text{ is a QR of } p \Leftrightarrow p \equiv 1, 11 \pmod{12}.$$

This implies that $p \equiv 1$ or $11 \pmod{12}$. If $p \equiv 1 \pmod{12}$ then $p = 12k+1$ but if all the prime factors of N are of this form $p = 12k+1$ then N must also be of this form (you can show by induction that this is indeed the case) but it is not because

$$N = \left(3 \times p_1 \times p_2 \times \cdots \times p_n\right)^2 - 3.$$

So one of the factors must be of the form $p \equiv 11 \pmod{12}$ which implies

$$p = 12k + 11 = 3\left(4\left[k+1\right]\right) - 1.$$

Hence p is of the form $3n-1$. Since p is a prime factor of N so $p \mid N$. In view of p being of the form $3n-1$ it must be one of the primes in the above list (*). So

$$p \mid x \quad \text{implies} \quad p \mid x^2.$$

Since $p \mid N$ and $p \mid x^2$ so from $N = \left(3 \times p_1 \times p_2 \times \cdots \times p_n\right)^2 - 3$ we must have

$$p \mid 3.$$

This is impossible because $p > 3$. We have a contradiction so there are an infinite number of primes of the form $3n-1$.

■