Complete Solutions to Exercise 7.2

1. In each case we the properties of Proposition (7.9):

(a) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

(c) $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) = \left(\frac{a \times b}{p}\right)$.

(a) We need to establish that the square root of $35 \pmod{31}$ exists. We have

$$35 \equiv 4 \pmod{31}.$$

By Proposition (7.9) part (a):

We have $\left(\frac{35}{31}\right) = \left(\frac{4}{31}\right)$. Note that $4 = 2^2$ so using part (b) of (7.9):

$$\left(\frac{35}{31}\right) = \left(\frac{4}{31}\right) = \left(\frac{2^2}{31}\right) = 1.$$

Since the Legendre symbol $\left(\frac{35}{31}\right) = 1$ so 35 is a quadratic residue of 31.

(b) Similarly, for the integer 71 we have

$$71 \equiv 9 \pmod{31}.$$

Therefore, by part (a) of (7.9) we have $\left(\frac{71}{31}\right) = \left(\frac{9}{31}\right)$. Again $9 = 3^2$ so by part (b) of (7.9):

$$\left(\frac{71}{31}\right) = \left(\frac{9}{31}\right) = \left(\frac{3^2}{31}\right) = 1.$$

The Legendre symbol $\left(\frac{71}{31}\right) = 1$ therefore 71 is a quadratic residue of 31.

(c) Arguing along the same lines we have

$$56 \equiv 25 \pmod{31}.$$

Evaluating the Legendre symbol gives

$$\left(\frac{56}{31}\right) = \left(\frac{25}{31}\right) = \left(\frac{5^2}{31}\right) = 1.$$

Hence 56 is a quadratic residue of 31.

(d) We have $94 \equiv 1 \pmod{31}$. Applying the above Proposition (7.9) to show that 94 is a quadratic residue of 31:

$$\left(\frac{94}{31}\right) = \left(\frac{1}{31}\right) = \left(\frac{1^2}{31}\right) = 1 .$$

Hence 94 is a quadratic residue of 31.

(e) We have $47 \equiv 16 \pmod{31}$. Therefore

$$\left(\frac{47}{31}\right) = \left(\frac{16}{31}\right) = \left(\frac{4^2}{31}\right) = 1 .$$

Since the Legendre symbol $\left(\frac{47}{31}\right) = 1$ so 47 is a quadratic residue.

2. (a) We need to test whether the square root of $46 \pmod{47}$ exists. Note that $46 \equiv -1 \pmod{47}$; so we test whether -1 is a quadratic residue of 47. Also our prime 47 satisfies $47 \equiv 3 \pmod{4}$ so by Proposition (7.11):

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

we have

$$\left(\frac{46}{47}\right) = \left(\frac{-1}{47}\right) = -1 \quad \text{because } 47 \equiv 3 \pmod{4}.$$

Since the Legendre symbol $\left(\frac{46}{47}\right) = -1$ so 46 is a quadratic *non* – residue of 47.

(b) We have $95 \equiv 1 \pmod{47}$ therefore

$$\left(\frac{95}{47}\right) = \left(\frac{1}{47}\right) .$$

By Proposition (7.10):

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

So $\left(\frac{95}{47}\right) = \left(\frac{1}{47}\right) = 1$ which means that 95 is a quadratic residue of 47.

(c) We have $90 \equiv 43 \equiv -4 \pmod{47}$. We can write -4 as $-4 = -1 \times 2^2$. Applying the properties of the Legendre symbol we have

$$\left(\frac{90}{47}\right)=\left(\frac{-4}{47}\right)=\left(\frac{-1\times 2^2}{47}\right)=\left(\frac{-1}{47}\right)\times\left(\frac{2^2}{47}\right)\quad(\ddagger)$$

Since $47\equiv 3\pmod 4$ so $\left(\frac{-1}{47}\right)=-1$ and by applying (7.9) part (b):

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

we have $\left(\frac{2^2}{47}\right)=1$. Substituting $\left(\frac{-1}{47}\right)=-1$ and $\left(\frac{2^2}{47}\right)=1$ into $(\ddagger)$ gives

$$\left(\frac{90}{47}\right)=\left(\frac{-1}{47}\right)\times\left(\frac{2^2}{47}\right)=-1\times 1=-1\,.$$

Since the Legendre symbol $\left(\frac{90}{47}\right)=-1$ so 90 is a quadratic *non* – residue of 47.

(d) We need to find whether the square root of $58\pmod{47}$ exists. Well

$$58\equiv 11\pmod{47}.$$

We could use Euler's criterion but that would mean we need to evaluate

$$11^{\frac{47-1}{2}}\equiv 11^{23}\equiv ?\pmod{47}.$$

Is there an easier to find whether 58 is a quadratic residue of 47?

Yes, because $58\equiv 11\equiv -36\pmod{47}$ and

$$-36=-1\times 6^2\,.$$

Therefore, we have

$$\left(\frac{58}{47}\right)=\left(\frac{-36}{47}\right)=\left(\frac{-1\times 6^2}{47}\right)=\left(\frac{-1}{47}\right)\times\left(\frac{6^2}{47}\right)=(-1)\times 1=-1\,.$$

Hence 58 is a quadratic *non* – residue of modulo 47.

(e) We need to find whether 90×58 is a quadratic residue of 47. By the solutions to parts (c) and (d) we have

$$\left(\frac{90\times 58}{47}\right)=\left(\frac{90}{47}\right)\times\left(\frac{58}{47}\right)=\underbrace{(-1)}_{\text{by part (c)}}\times\underbrace{(-1)}_{\text{by part (d)}}=1$$

Hence 90×58 is a quadratic residue of modulo 47. Note that 90 and 58 are quadratic non – residues but 90×58 is a quadratic residue of 47.

3. (a) Clearly 5 is a factor of $18^2+1=325$. We have $\frac{325}{5}=65=5\times 13$ so

$$325=5\times 5\times 13=5^2\times 13$$

(b) Factorizing this integer $30^2+1=901$ is more challenging. Since it is a quadratic of the form x^2+1 so the (odd) primes p must satisfy $p\equiv 1\left(\text{mod } 4\right)$.

Clearly 5 is not a factor of 901 but what about 13?

$$\frac{901}{13}=69.31\,.$$

Therefore 13 is *not* prime factor of 901. Let's trial 17:

$$\frac{901}{17}=53\,.$$

Hence 17 is a factor of 901 and 53 is prime so

$$901=17\times 53\,.$$

(c) Clearly $10=2\times 5$ is a factor of $53^2+1=2810$. We have

$$2810=2\times 5\times 281\,.$$

We need to find the factors of 281. The simplest way to find the prime factors p of 281 is to first check that 281 is prime or composite. You can show by Corollary (2.10) that 281 is prime.

Hence $2810=2\times 5\times 281$.

(d) We are asked to factorize $60^2+1=3601$. Since this is an integer which conforms to x^2+1 so it must have prime factors p such that $p\equiv 1\left(\text{mod } 4\right)$.

No point trying 5. So, we trial 13:

$$\frac{3601}{13}=277\,.$$

Now 277 is either composite or prime. By Corollary (2.10) we only need to examine the odd primes below $\left\lfloor\sqrt{277}\right\rfloor=16$. So, we examine prime p which satisfy $p\equiv 1\left(\text{mod } 4\right)$ and below 16. We only need to try 13 again:

$$\frac{277}{13}=21.31\left(2\text{ dp}\right).$$

Since 13 is not a factor of 277 so 277 is prime. Therefore

$$3601=13\times 277\,.$$

(e) We need to factorize $24^2+1=577$. Since $\left\lfloor\sqrt{24^2+1}\right\rfloor=\left\lfloor 577\right\rfloor=24$ so we only need to examine the odd primes p of the form $p\equiv 1\left(\text{mod } 4\right)$ below 24.

We know 5 is *not* a factor of 577. Only need to try 13 and 17:

$$\frac{577}{13}=44.38,\qquad \frac{577}{17}=33.94\,.$$

Since 13 and 17 are not factors of 577 so 577 is prime.

(f) We need to factorize $104^2+1=10\,817$. The primes p must satisfy $p\equiv 1\pmod 4$. Clearly 5 is not a factor of this 10 817. The next few primes of the format $p\equiv 1\pmod 4$ are 13, 17, 29 and if we divide 10 817 by each of these we find that $\dfrac{10\,817}{29}=373$. Therefore 29 is a factor and

$$10\,817=29\times 373.$$

Need to test the primality of 373. Using Corollary (2.10) we find that

$$\left\lfloor\sqrt{373}\right\rfloor=\lfloor 19.31..\rfloor=19.$$

Clearly 373 is prime because we have tried primes larger than 19 and they did not go into 10 817 so cannot be factors of 373. Hence $10\,817=29\times 373$.

(g) We are asked to factorize $302^2+1=91\,205$. Clearly 5 is factor:

$$\frac{91\,205}{5}=18\,241.$$

The prime factor p of 18 241 must be of the form $p\equiv 1\pmod 4$. Trialling 13 and 17 we find that

$$\frac{18\,241}{13}=1403.154...,\quad \frac{18\,241}{17}=1073$$

So, 17 is a factor of 18 241 and 91 205. Testing 1073 for primality gives

$$\left\lfloor\sqrt{1073}\right\rfloor=32.$$

Testing whether 17 and 29 are factors of 1073 we have

$$\frac{1073}{17}=63.118...,\quad \frac{1073}{29}=37.$$

Therefore $1073=29\times 37$ which implies $18\,241=17\times 1073=17\times 29\times 37$. Hence $302^2+1=91\,205=5\times 17\times 29\times 37$.

(h) We need to factorize $1014^2+1=1028\,197$. As before we only need to examine primes p of the form $p\equiv 1\pmod 4$. We trail 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, … and we find that

$$\frac{1028\,197}{109}=9433.$$

Evaluating $\left\lfloor\sqrt{9433}\right\rfloor=97$ and since the first prime into 1 028 197 was 109 so none of the earlier primes can go into 9433 because if they did then they would be factors of 1 028 197. Hence 9433 is prime and we have

$$1014^2+1=1028\,197=109\times 9433\,.$$

4. *Proof.*

   Using the Legendre symbol we have

   Let $x\equiv a^n \pmod p$ then squaring gives $x^2\equiv a^{2n}\pmod p$. Hence a^{2n} is a quadratic residue of prime p. This completes our proof.

   ■

5. We need to prove $\left(\frac{a_1}{p}\right)\times\left(\frac{a_2}{p}\right)\times\cdots\times\left(\frac{a_n}{p}\right)=\left(\frac{a_1\times a_2\times a_3\times\cdots\times a_n}{p}\right)$. *How?*

   Use mathematical induction.

   Proof.

   By Proposition (7.9) part (c):

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

   We have the base case $\left(\frac{a_1}{p}\right)\times\left(\frac{a_2}{p}\right)=\left(\frac{a_1\times a_2}{p}\right)$.

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

   $$\left(\frac{a_1}{p}\right)\times\left(\frac{a_2}{p}\right)\times\cdots\times\left(\frac{a_k}{p}\right)=\left(\frac{a\times a_2\times a_3\times\cdots\times a_k}{p}\right)\qquad(*)$$

   We need to prove this for the case $n=k+1$:

   $$\left(\frac{a_1}{p}\right)\times\left(\frac{a_2}{p}\right)\times\cdots\times\left(\frac{a_k}{p}\right)\times\left(\frac{a_{k+1}}{p}\right)=\underbrace{\left(\frac{a\times a_2\times a_3\times\cdots\times a_k}{p}\right)}_{\text{by }(*)}\times\left(\frac{a_{k+1}}{p}\right)$$
   $$=\left(\frac{a\times a_2\times a_3\times\cdots\times a_k\times a_{k+1}}{p}\right)\qquad\text{[By the base case]}$$

   Hence by mathematical induction we have our result.

   ■

6. We need to prove that $\left(\frac{a}{p}\right)=\left(\frac{p_1}{p}\right)^{k_1}\times\left(\frac{p_2}{p}\right)^{k_2}\times\cdots\times\left(\frac{p_n}{p}\right)^{k_n}$.

   Proof.

   We are given that $a=p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_n^{k_n}$ so by the result of the previous question we have

$$\left(\frac{a}{p}\right)=\left(\frac{p_1^{k_1}\times p_2^{k_2}\times\cdots\times p_n^{k_n}}{p}\right)=\left(\frac{p_1^{k_1}}{p}\right)\times\left(\frac{p_2^{k_2}}{p}\right)\times\cdots\times\left(\frac{p_n^{k_n}}{p}\right)$$
$$\underbrace{=}_{\substack{\text{by result of}\\ \text{previous question}}}\left(\frac{p_1}{p}\right)^{k_1}\times\left(\frac{p_2}{p}\right)^{k_2}\times\cdots\times\left(\frac{p_n}{p}\right)^{k_n}$$

This is our required result.

■

7. We are required to prove that if $p\equiv 1\pmod 4$ then $a^{\frac{p-1}{2}}$, where $\gcd(a,\ p)=1$, is a quadratic residue of p.

Proof.

We are given that $p\equiv 1\pmod 4$ so $p=4k+1$ for some integer k. Consider the residue $a^{\frac{p-1}{2}}$:

$$a^{\frac{p-1}{2}}=a^{\frac{4k+1-1}{2}}=a^{2k}.$$

By the result of question 4 we have a^{2k} is a quadratic residue of p so $a^{\frac{p-1}{2}}$ is a quadratic residue of p.

■

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

Proof.

By Proposition (7.8):

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\pmod p$$

We have $\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\pmod p$. We are given that p is an odd prime so $p\geq 3$ which implies that

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\pmod p.$$

$(-1)^{\frac{p-1}{2}}$ can only take values of 1 or -1 so $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

■

9. (i) We are asked to show that if $p\mid(x^2+1)$ then $p\equiv 1\pmod 4$.

Proof.

From the definition of congruence, we have

$$p \mid \left(x^2+1\right) \;\Leftrightarrow\; x^2+1 \equiv 0 \left(\text{mod } p\right) \;\Leftrightarrow\; x^2 \equiv -1 \left(\text{mod } p\right)$$

Hence $x^2 \equiv -1 \left(\text{mod } p\right)$ has solutions because we are given $p \mid \left(x^2+1\right)$ so $p \equiv 1 \left(\text{mod } 4\right)$. *Why?*

Because by question 6 of Exercises 7.1:

-1 is a quadratic residue of an odd prime $p \Leftrightarrow p \equiv 1 \left(\text{mod } 4\right)$.

we have -1 is a QR implies that $p \equiv 1 \left(\text{mod } 4\right)$.

This completes our proof.

■

(ii) We need to prove there are an infinite number of primes of the form $4n+1$.

Proof.

Assume there are only a finite number of primes $p_1, p_2, \cdots, p_m$ of the form $4n+1$. Consider the number

$$N = \left(2 \times p_1 \times p_2 \times \cdots \times p_m\right)^2 + 1.$$

Let p be a prime factor of N. By part (i) we have $p \equiv 1 \left(\text{mod } 4\right)$. Since $p \mid N$ so $p \neq p_1, p_2, \cdots, p_m$ because if p was equal to one of these then $p \mid 1$.

Hence p is *not* amongst the finite list of primes $p_1, p_2, \cdots, p_m$ and $p \equiv 1 \left(\text{mod } 4\right)$ therefore $p = 4n+1$ which implies there are infinite number of primes of the form $4n+1$.

■

10. We need to prove that $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

Proof.

By Proposition (7.9) part (c):

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

We have $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b^2}{p}\right)$. By Proposition (7.9) part (b):

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

We have $\left(\frac{b^2}{p}\right) = 1$. Substituting this $\left(\frac{b^2}{p}\right) = 1$ into the above $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b^2}{p}\right)$ yields

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

This completes our proof.

■

11. We are required to prove that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$. *How do we prove this?*

We use Proposition (7.4):

> Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues of p.

Proof.

By the above proposition we have exactly $\frac{p-1}{2}$ quadratic residues which means for these residues we have $\left(\frac{a}{p}\right) = 1$ and for the remaining $\frac{p-1}{2}$ residues we have $\left(\frac{a}{p}\right) = -1$. Hence

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

This is our required result.

■

12. (a) We need to prove r^{2n} is a quadratic residue of p.

Proof.

The quadratic congruence

$$x^2 \equiv r^{2n} \left(\text{mod } p\right)$$

has a solution because $x \equiv r^n \left(\text{mod } p\right)$ satisfies this congruence. Hence r^{2n} is a quadratic residue of p.

■

(b) We need to prove r^{2n+1} is a quadratic *non* - residue of p.

Proof.

Consider the quadratic congruence

$$x^2 \equiv r^{2n+1} \pmod{p}$$

Taking the ind_r of both sides of this equation which converts into linear form:

$$2 \times \text{ind}_r(x) \equiv (2n+1) \times \underbrace{\text{ind}_r(r)}_{=1} \equiv (2n+1) \pmod{p-1}.$$

The $\gcd(2, \quad p-1) = 2$ but $2 \nmid (2n+1)$ which implies this congruence

$$2 \times \text{ind}_r(x) \equiv (2n+1) \pmod{p-1}.$$

has *no* solutions, so r^{2n+1} is a quadratic *non* - residue of p.

■

(c) Half the residues are quadratic residues and half are quadratic non-residues of modulo p.

Proof.

By the Primitive Root Theorem (6.22):

> Every prime p has a primitive root.

we have a primitive root r modulo p.

The reduced residue system modulo p is given by $\{1, 2, \cdots, p-1\}$ and each of these can be expressed as $r^k \equiv a \pmod{p}$ where $a \in \{1, 2, \cdots, p-1\}$. The even powers such as r^{2m} in this list satisfy the quadratic congruence

$$x^2 \equiv r^{2m} \equiv (r^m)^2 \pmod{p}.$$

By Proposition (3.14) (b):

$$a^2 \equiv b^2 \pmod{p} \Leftrightarrow a \equiv \pm b \pmod{p}$$

We have $x \equiv \pm r^m \pmod{p}$ so these are the quadratic residues of p. There are $\frac{p-1}{2}$ residues in $\{1, 2, \cdots, p-1\}$ which have base r with an even index.

Hence there are $\frac{p-1}{2}$ quadratic residues of p.

Additionally, there are $\frac{p-1}{2}$ residues in $\{1, 2, \cdots, p-1\}$ which have *no* solutions to the quadratic residues $x^2 \equiv a \pmod{p}$ where $a \in \{1, 2, \cdots, p-1\}$ so there are $\frac{p-1}{2}$ quadratic non – residues of p. This completes our proof.

■

13. We need to find the quadratic residues of 17. We are given that 3 is a primitive root of 17 so we need to find the even powers of 3. *Why?*

By the result of the previous question part (a) we showed that r^{2n} is a quadratic residue of prime p.

$$\begin{aligned}
3^2 &\equiv 9 \pmod{17} \\
3^4 &\equiv \left(3^2\right)^2 \equiv 9^2 \equiv 81 \equiv -4 \equiv 13 \pmod{17} \qquad (*) \\
3^6 &\equiv 3^4 \times 3^2 \equiv -4 \times 9 \equiv -36 \equiv -2 \equiv 15 \pmod{17} \\
3^8 &\equiv \left(3^4\right)^2 \equiv \left(-4\right)^2 \equiv 16 \equiv -1 \pmod{17} \\
3^{10} &\equiv 3^8 \times 3^2 \equiv \left(-1\right) \times 9 \equiv -9 \equiv 8 \pmod{17} \\
3^{12} &\equiv \left(3^6\right)^2 \equiv \left(-2\right)^2 \equiv 4 \pmod{17} \\
3^{14} &\equiv 3^8 \times 3^6 \equiv \left(-1\right) \times \left(-2\right) \equiv 2 \pmod{17} \\
3^{16} &\equiv \left(3^8\right)^2 \equiv \left(-1\right)^2 \equiv 1 \pmod{17}
\end{aligned}$$

The quadratic residues of 17 are 1, 2, 4, 8, 9, 13, 15 and 16.

To find the square roots of $13 \pmod{17}$ we need to solve the quadratic

$$x^2 \equiv 13 \pmod{17}$$

By the above we have that 3 is a primitive root of 17 so taking indices to the base 3 which converts the quadratic into linear form we have

$$2 \times \operatorname{ind}_3(x) \equiv \operatorname{ind}_3(13) \pmod{16}$$

By (*) we have $\operatorname{ind}_3(13) = 4$. Substituting this into the above yields

$$2 \times \operatorname{ind}_3(x) \equiv 4 \pmod{16} \;\Rightarrow\; \operatorname{ind}_3(x) \equiv 2 \pmod{8}.$$

Hence the square roots of $13 \pmod{17}$ are

$$x \equiv \pm 3^2 \equiv \pm 9 \equiv 9, \; -9 \equiv 9, \; 8 \pmod{17}.$$

14. We are given that 2 is a primitive root of 101 and we need to solve the quadratic $x^2 \equiv 14 \pmod{101}$. Taking indices to the base 2 to convert the quadratic into linear form gives

$$2 \times \operatorname{ind}_2(x) \equiv \operatorname{ind}_2(14) \pmod{100} \qquad (\dagger)$$

We must find what power of 2 gives 14 modulo 101. Computing powers of 2:

$$2^7 \equiv 128 \equiv 27 \pmod{101}$$

$$2^8 \equiv 27 \times 2 \equiv 54 \pmod{101}$$

$$2^9 \equiv 54 \times 2 \equiv 108 \equiv 7 \pmod{101}$$

$$2^{10} \equiv 7 \times 2 \equiv 14 \pmod{101}$$

From the last result we have $\text{ind}_2(14) = 10$ and substituting this into (†) gives

$$2 \times \text{ind}_2(x) \equiv 10 \pmod{100} \;\Rightarrow\; \text{ind}_2(x) \equiv 5 \pmod{50}.$$

Therefore, the square roots of $14 \pmod{101}$ are given by

$$x \equiv \pm 2^5 \equiv \pm 32 \equiv 32, \; -32 \equiv 32, \; 69 \pmod{101}.$$