Solutions to Exercise Sheet 4

Solution 4.1. *Computation of the Legendre symbol.*

(1) We factor 474 into primes as $474 = 2 \times 3 \times 79$. Hence $(\frac{474}{733}) = (\frac{2}{733})(\frac{3}{733})(\frac{79}{733})$. We have $(\frac{2}{733}) = -1$ since $733 \equiv 5 \pmod 8$. We use quadratic reciprocity to compute the other two factors. Notice that $733 \equiv 1 \pmod 4$, therefore $(\frac{3}{733}) = (\frac{733}{3}) = (\frac{1}{3}) = 1$. For the same reason we have $(\frac{79}{733}) = (\frac{733}{79}) = (\frac{22}{79}) = (\frac{2}{79})(\frac{11}{79})$. Since $79 \equiv -1 \pmod 8$ we have $(\frac{2}{79}) = 1$. Since $11 \equiv 79 \equiv 3 \pmod 8$, by quadratic reciprocity we get $(\frac{11}{79}) = -(\frac{79}{11}) = -(\frac{2}{11}) = 1$, where the last equality is due to $11 \equiv 3 \pmod 8$. Hence we have $(\frac{79}{733}) = 1$. It follows that $(\frac{474}{733}) = (-1) \times 1 \times 1 = -1$.

(2) The computation is always easier if we use Jacobi symbols. We just need to remember pulling out -1 and 2 from the numerators.

In this problem we have $(\frac{-113}{997}) = (\frac{-1}{997})(\frac{113}{997})$. The first factor $(\frac{-1}{997}) = 1$ since $997 \equiv 1 \pmod 4$. The second factor $(\frac{113}{997}) = (\frac{997}{113})$ by quadratic reciprocity since $113 \equiv 1 \pmod 4$ (or $997 \equiv 1 \pmod 4$). Then $(\frac{997}{113}) = (\frac{93}{113}) = (\frac{113}{93}) = (\frac{20}{93}) = (\frac{4}{93})(\frac{5}{93}) = (\frac{5}{93}) = (\frac{93}{5}) = (\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1$, where the second, sixth and eighth equalities are consequences of quadratic reciprocity since $113 \equiv 1 \pmod 4$ and $5 \equiv 1 \pmod 4$. Finally we conclude $(\frac{-113}{997}) = -1$.

(3) For this one we have $(\frac{514}{1093}) = (\frac{2}{1093})(\frac{257}{1093})$. Since $1093 \equiv 5 \pmod 8$ we get $(\frac{2}{1093}) = -1$. Realising $257 \equiv 1 \pmod 4$ and using quadratic reciprocity, we have $(\frac{257}{1093}) = (\frac{1093}{257}) = (\frac{65}{257}) = (\frac{257}{65}) = (\frac{62}{65})$. At this point we can of course factor 62 and do the computation as usual. But there is a shortcut. We write $(\frac{62}{65}) = (\frac{-3}{65}) = (\frac{-1}{65})(\frac{3}{65})$. Since $65 \equiv 1 \pmod 4$, we have $(\frac{-1}{65}) = 1$, and by quadratic reciprocity $(\frac{3}{65}) = (\frac{65}{3}) = (\frac{2}{3}) = -1$. Finally we conclude that $(\frac{514}{1093}) = (-1) \times (-1) = 1$.

Solution 4.2. *Primes for which a given number is a quadratic residue.*

(1) To find all the odd primes p for which 5 is a quadratic residue, we need to compute $(\frac{5}{p})$ for any odd prime $p \neq 5$ (because p has to be coprime with 5 for being a quadratic residue). Since $5 \equiv 1 \pmod 4$, $(\frac{5}{p}) = (\frac{p}{5})$. By direct computation we know that $(\frac{1}{5}) = (\frac{4}{5}) = 1$, $(\frac{2}{5}) = -1$ and $(\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1$. Hence

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

In other words, 5 is a quadratic residue modulo an odd prime p iff $p \equiv \pm 1 \pmod 5$.

(2) Let p be an odd prime and $p \neq 3$ (because p has to be coprime with -3). We compute $(\frac{-3}{p})$. We know $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p})$. The first factor $(\frac{-1}{p}) = 1$ if $p \equiv 1 \pmod 4$ and -1 if $p \equiv 3 \pmod 4$. We apply quadratic reciprocity for the second

factor; i.e. $(\frac{3}{p}) = (\frac{p}{3})$ if $p \equiv 1 \pmod 4$ and $-(\frac{p}{3})$ if $p \equiv 3 \pmod 4$. No matter whether $p \equiv 1$ or $3 \pmod 4$, we always have $(\frac{-3}{p}) = (\frac{p}{3})$. Since $(\frac{1}{3}) = 1$ and $(\frac{2}{3}) = -1$, we have

$$\Big(\frac{-3}{p}\Big) = \begin{cases} 1 & \text{if } \ p \equiv 1 \pmod 3 \\ -1 & \text{if } \ p \equiv 2 \pmod 3. \end{cases}$$

In other words, -3 is a quadratic residue modulo an odd prime p iff $p \equiv 1 \pmod 3$.

Solution 4.3. *Properties of Jacobi symbols.*

(1) Let $b = p_1 p_2 \cdots p_m$ be its prime factorisation, where $p_1, p_2, \cdots, p_m$ are not necessarily distinct. Since a is a quadratic residue modulo b, there exists some integer $x \in \mathbb{Z}$, such that $x^2 \equiv a \pmod b$. It follows that $x^2 \equiv a \pmod{p_i}$ for each $i = 1, 2, \cdots, m$. Since $\mathrm{hcf}(a, b) = 1$, we know $p_i \nmid a$, therefore a is a quadratic residue modulo p_i for each $i = 1, 2, \cdots, m$. By Definition 4.2, $(\frac{a}{p_i}) = 1$ for each i, hence by Definition 4.9, we have $(\frac{a}{b}) = (\frac{a}{p_1})(\frac{a}{p_2}) \cdots (\frac{a}{p_m}) = 1$.

(2) Let $b = p_1 p_2 \cdots p_m$ be its prime factorisation, where $p_1, p_2, \cdots, p_m$ are not necessarily distinct primes. By Definition 4.9 and Proposition 4.4 (2) we have

$$\Big(\frac{a_1 a_2}{b}\Big) = \Big(\frac{a_1 a_2}{p_1}\Big) \cdots \Big(\frac{a_1 a_2}{p_m}\Big) = \Big(\frac{a_1}{p_1}\Big)\Big(\frac{a_2}{p_1}\Big) \cdots \Big(\frac{a_1}{p_m}\Big)\Big(\frac{a_2}{p_m}\Big)$$
$$\Big(\frac{a_1}{b}\Big)\Big(\frac{a_2}{b}\Big) = \Big(\frac{a_1}{p_1}\Big) \cdots \Big(\frac{a_1}{p_m}\Big) \cdot \Big(\frac{a_2}{p_1}\Big) \cdots \Big(\frac{a_2}{p_m}\Big).$$

The right-hand sides of the above two equations are products of the same factors (although in different orders), Hence they are equal. It follows that the left-hand sides of these two equations are also equal.

Solution 4.4. *Quadratic residues and the Legendre symbol.*

(1) We do it in the most naive way. We could try to compute the square of all integers from 1 to 12 to get all quadratic residues modulo 13. In fact we only need to compute the first six of them, because for every $k \in \mathbb{Z}$, $1 \leqslant k \leqslant 6$, we have $13 - k \equiv -k \pmod{13}$, hence $(13-k)^2 \equiv k^2 \pmod{13}$. In other words, the square of any integer between 7 and 12 would not produce any new congruence class. The squares of $1, 2, 3, 4, 5, 6$ are $1, 4, 9, 16, 25, 36$, which reduce to $1, 4, 9, 3, 12, 10$ modulo 13. So a is a quadratic residue modulo 13 iff $a \equiv 1, 3, 4, 9, 10$ or $12 \pmod{13}$, and a quadratic non-residue modulo 13 iff $a \equiv 2, 5, 6, 7, 8$ or $11 \pmod{13}$.

(2) Recall that a solution to such a congruence equation is a congruence class modulo p. There are three cases. If $p \mid a$, then the congruence equation becomes $x^2 \equiv 0 \pmod p$. It follows that $p \mid x$ and $x \equiv 0 \pmod p$ is the only solution to the equation. In this case we do have $(\frac{a}{p}) + 1 = 1$ which is the number of solutions.

If a is a quadratic residue modulo p, then there exists some $x_0 \in \mathbb{Z}$ such that $x_0^2 \equiv a \pmod{p}$. Since $p \nmid a$, we also have $p \nmid x_0$. We claim that the congruence $x^2 \equiv a \pmod{p}$ has two solutions, which are given by $x \equiv x_0 \pmod{p}$ and $x \equiv -x_0 \pmod{p}$. Obviously both are solutions to the congruence equation. They must be distinct. Indeed, if they were the same solution, then $x_0 \equiv -x_0 \pmod{p}$, hence $2x_0 \equiv 0 \pmod{p}$. Since p is an odd prime, this implies $p \mid x_0$. Contradiction. Therefore we have found two solutions to the congruence equation $x^2 \equiv a \pmod{p}$. We can interpret this congruence as an equation $x^2 = \overline{a}$ in $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a field by Proposition 2.9, this equation has at most two solutions by Lemma 3.3. Hence we have found all solutions. In this case, $(\frac{a}{p}) + 1 = 2$ which is indeed the number of solutions.

If a is a quadratic non-residue modulo p, then there is no solution to the congruence $x^2 \equiv a \pmod{p}$. And we do have $(\frac{a}{p}) + 1 = 0$ in this case. We proved our result in all three possible cases.

(3) We consider the congruence equations $x^2 \equiv a \pmod{p}$ for $a = 0, 1, \cdots, p-1$. There are p equations in total. The sum of numbers of solutions to these p equations is given by $\sum_{a=0}^{p-1}((\frac{a}{p}) + 1)$.

On the other hand, every congruence class modulo p is precisely a solution to one of these equations. (In other words, for every $0 \leqslant x_0 \leqslant p-1$, the congruence class $x \equiv x_0 \pmod{p}$ is a solution to the unique congruence equation $x^2 \equiv a \pmod{p}$ for a being the residue of x_0^2 modulo p.) Therefore the sum of numbers of solutions to all p congruence equations is p.

It follows that $\sum_{a=0}^{p-1}((\frac{a}{p}) + 1) = p$. The left-hand side is $\sum_{a=0}^{p-1}(\frac{a}{p}) + p$, hence we conclude that $\sum_{a=0}^{p-1}(\frac{a}{p}) = 0$.

(4) We look at the left-hand side of the equation $\sum_{a=0}^{p-1}(\frac{a}{p}) = 0$. For $a = 0$, we have $(\frac{a}{p}) = 0$. For all other values of a, $(\frac{a}{p}) = \pm 1$. Since they add up to 0, there should be the same number of 1's and -1's. In other words, in the set $\{1, 2, \cdots, p-1\}$, there are the same number of quadratic residues and non-residues.

The answer to part (1) is consistent with this conclusion, because among all positive integers less than 13, we found 6 quadratic residues modulo 13 and 6 quadratic non-residues.