Solutions to Exercise Sheet 5

Solution 5.1. *Evaluating Legendre symbols by Gauss' lemma.*

- For $(\frac{5}{7})$, since $p = 7$ and $r = 3$, we need to consider the least residues of 5, 10 and 15, which are -2, 3 and 1. There is only one negative least residue, hence $(\frac{5}{7}) = -1$.

  For $(\frac{3}{11})$, since $p = 11$ and $r = 5$, we consider the least residues of 3, 6, 9, 12 and 15, which are 3, -5, -2, 1 and 4. There are two negative least residues, hence $(\frac{3}{11}) = 1$.

  For $(\frac{6}{13})$, since $p = 13$ and $r = 6$, we consider the least residue of 6, 12, 18, 24, 30 and 36, which are 6, -1, 5, -2, 4 and -3. There are three negative ones, hence $(\frac{6}{13}) = -1$.
- We consider $(\frac{-1}{p})$. Let $r = \frac{p-1}{2}$. We need to look at the least residues of $-1, -2, \cdots, -r$. But they are already least residues themselves. Since there are r of them, by Gauss' Lemma, we get $(\frac{-1}{p}) = (-1)^r = (-1)^{\frac{p-1}{2}}$.

  Now we consider $(\frac{2}{p})$. Let $r = \frac{p-1}{2}$. We look at the least residues of $2, 4, \cdots, 2r$. We deal with four cases $p \equiv 1, 3, 5$ or $7 \pmod 8$ separately. If $p \equiv 1 \pmod 8$, then we can assume $p = 8m+1$ for some $m \geqslant 0$, and $r = 4m$. The number $2k$ has positive least residue for $1 \leqslant k \leqslant 2m$ and negative least residue for $2m+1 \leqslant k \leqslant 4m$. Hence by Gauss' Lemma, $(\frac{2}{p}) = (-1)^{2m} = 1$. If $p \equiv 3 \pmod 8$, then we write $p = 8m+3$, and $r = 4m+1$. The number $2k$ has positive least residue for $1 \leqslant k \leqslant 2m$ and negative least residue for $2m+1 \leqslant k \leqslant 4m+1$. Hence $(\frac{2}{p}) = (-1)^{2m+1} = -1$. If $p \equiv 5 \pmod 8$, then we write $p = 8m+5$ and $r = 4m+2$. The number $2k$ has positive least residue for $1 \leqslant k \leqslant 2m+1$ and negative least residue for $2m+2 \leqslant k \leqslant 4m+2$, hence $(\frac{2}{p}) = (-1)^{2m+1} = -1$. If $p \equiv 7 \pmod 8$, then we write $p = 8m+7$ and $r = 4m+3$. The number $2k$ has positive least residue for $1 \leqslant k \leqslant 2m+1$ and negative least residue for $2m+2 \leqslant k \leqslant 4m+3$, hence $(\frac{2}{p}) = (-1)^{2m+2} = 1$. In summary, we have $(\frac{2}{p}) = 1$ if $p \equiv 1$ or $7 \pmod 8$ and -1 if $p \equiv 3$ or $5 \pmod 8$.
- Since $a = -1$, for any $1 \leqslant l \leqslant \frac{p-1}{2}$, $-1 < \frac{la}{p} < 0$, hence $[\frac{la}{p}] = -1$. Then $t = \sum_{l=1}^{\frac{p-1}{2}} [\frac{la}{p}] = \sum_{l=1}^{\frac{p-1}{2}} -1 = -\frac{p-1}{2}$. By Lemma 5.2, $(\frac{-1}{p}) = (-1)^t = (-1)^{-\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$, where the last equality is due to the fact that n and $-n$ always have the same parity (both odd or both even) for any integer n. Or equivalently, $(\frac{-1}{p}) = 1$ if $p \equiv 1 \pmod 4$ and -1 if $p \equiv -1 \pmod 4$.

Solution 5.2. *Special cases of Dirichlet's theorem.*

(1) Assume there are only finitely many primes congruent to -1 modulo 6, say, $S = \{p_1, p_2, \cdots, p_n\}$. Then we consider $N = 6p_1p_2\cdots p_n - 1 > 1$. It is clear that $p_i \nmid N$

for each $p_i \in S$, hence $p \notin S$ for each prime factor p of N. It follows that $p \not\equiv 5 \pmod 6$. Moreover, p must be odd since N is odd, so $p \not\equiv 0, 2$ or $4 \pmod 6$. Furthermore, the only prime congruent to 3 modulo 6 is 3. However $3 \nmid N$, hence $p \not\equiv 3 \pmod 6$. Therefore the only possibility is $p \equiv 1 \pmod 6$. It follows that N is a product of primes congruent to 1 modulo 6, hence $N \equiv 1 \pmod 6$, which contradicts the formula of N, from which we can see $N \equiv 5 \pmod 6$. It follows that there are infinitely many primes congruent to -1 modulo 6.

(2) Assume there are only finitely many primes congruent to -1 modulo 8, say, $T = \{q_1, q_2, \cdots, q_m\}$. Then we consider $M = (4q_1q_2\cdots q_m)^2 - 2 > 1$. Since each $q_j \in T$ is an odd prime, $q_j \nmid 2$, hence $q_j \nmid M$. If follows that if q is an odd prime factor of M, then $q \notin T$, hence $q \not\equiv -1 \pmod 8$. On the other hand, $q \mid M$ implies that 2 is a quadratic residue modulo q, hence $q \equiv 1$ or $-1 \pmod 8$. It follows that $q \equiv 1 \pmod 8$. In other words, every odd prime factor of M is congruent to 1 modulo 8. If we write $M = 2(8q_1^2q_2^2\cdots q_m^2 - 1)$, then the second factor $8q_1^2q_2^2\cdots q_m^2 - 1$ must be a product of primes congruent to 1 modulo 8, which is itself congruent to 1 modulo 8. Contradiction. This contradiction shows that there are infinitely many primes congruent to -1 modulo 8.

Solution 5.3. *Quadratic residues for powers of odd primes.*

(1) Since a is a quadratic residue modulo p^{e+1}, there exists some $x \in \mathbb{Z}$, such that $x^2 \equiv a \pmod{p^{e+1}}$. Equivalently, $x^2 - a$ is a multiple of p^{e+1}, which implies $x^2 - a$ is a multiple of p^e. Or equivalently, $x^2 \equiv a \pmod{p^e}$. Since $p \nmid a$, we have $\operatorname{hcf}(a, p^e) = 1$. We conclude that a is a quadratic residue modulo p^e.

(2) Since a is a quadratic residue modulo p^e, we have $x^2 \equiv a \pmod{p^e}$ for some $x \in \mathbb{Z}$. Equivalently, we can write $x^2 = a + bp^e$ for some $b \in \mathbb{Z}$. Set $y = x + cp^e$ for some $c \in \mathbb{Z}$, then we consider $y^2 - a$. We have $y^2 - a = (x + cp^e)^2 - a = x^2 - a + 2xcp^e + c^2p^{2e} = (b + 2xc)p^e + c^2p^{2e}$.

Now we claim that we can choose c such that $b + 2xc$ is a multiple of p. Indeed, since $p \nmid a$, we have $p \nmid x$, hence $\operatorname{hcf}(2x, p) = 1$. It follows by Proposition 2.5 that the congruence equation $2xz \equiv -b \pmod p$ (think of it as an equation of z) has a solution for z. Let $z = c$ be such a solution, then $2xc + b$ is a multiple of p, hence $(b + 2xc)p^e$ is a multiple of p^{e+1}. On the other hand c^2p^{2e} is also a multiple of p^{e+1} because $2e \geqslant e + 1$. It follows that $y^2 - a$ is a multiple of p^{e+1}, or equivalently, $y^2 \equiv a \pmod{p^{e+1}}$. Since $p \nmid a$, we have $\operatorname{hcf}(a, p^{e+1}) = 1$. Therefore a is a quadratic residue modulo p^{e+1}.

(3) By parts (1) and (2), a is a quadratic residue modulo p^e iff a is a quadratic residue modulo p^{e+1}. Using this result inductively, we can conclude that a is a quadratic

residue modulo p^e for any positive integer e iff p is a quadratic residue modulo p, which is equivalent to $(\frac{a}{p}) = 1$.

Solution 5.4. *Fermat's two-square problem.*

(1) Since $p \equiv 1 \pmod 4$, -1 is a quadratic residue modulo p. In other words, $x^2 \equiv -1 \pmod p$ has a solution. Let $x = s$ be one such solution, then $s^2 + 1$ is a multiple of p. We can then write $s^2 + 1 = pt$, where $s, t \in \mathbb{Z}$. It follows that p divides $s^2 + 1 = (s + i)(s - i)$ in $\mathbb{Z}[i]$. If p could divide $s + i$ in $\mathbb{Z}[i]$, then we can write $s + i = p(x + yi)$ for some $x, y \in \mathbb{Z}$. It follows that $py = 1$. Contradiction. Therfore p does not divide $s + i$. Similar one can show that p does not divide $s - i$. Hence p is not a prime, because p divides the product of $s + i$ and $s - i$ but neither of the factors.

(2) We know from Exercise 1.4 (2) that $\mathbb{Z}[i]$ is a Euclidean domain, hence a PID. By Proposition 1.9 (2), every irreducible element in $\mathbb{Z}[i]$ is a prime. By part (1), p is not a prime in $\mathbb{Z}[i]$ hence is not irreducible. It follows that we can write $p = \alpha\beta$, such that α and β are non-units. We apply Exercise 1.4 (1) and get $\nu(p) = \nu(\alpha)\nu(\beta)$. By the formula of the valuation ν, the left-hand side is p^2. By Exercise 1.4 (4), neither of the factor on the right-hand side is 1. Therefore the only possibility is $\nu(\alpha) = \nu(\beta) = p$. Let $\alpha = a + bi$ for some $a, b \in \mathbb{Z}$. Then $\nu(\alpha) = a^2 + b^2 = p$.

(3) We show that $a^2 \equiv 0$ or $1 \pmod 4$ for every $a \in \mathbb{Z}$. Indeed, if a is even, say $a = 2k$ for some $k \in \mathbb{Z}$, then $a^2 = 4k^2 \equiv 0 \pmod 4$. If a is odd, say $a = 2k + 1$ for some $k \in \mathbb{Z}$, then $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$. The same is true for b^2. We consider all the combinations and conclude that $a^2 + b^2 \equiv 0$ or 1 or $2 \pmod 4$. By assumption $p \equiv 3 \pmod 4$, hence $p = a^2 + b^2$ is never possible.