MATH 152 Problem set 5 solutions

1. To make it clearer what the problem is asking to prove: any $\mathcal{S}_1$ and $\mathcal{S}_2$ with the properties as described in the problem are the set of quadratic residue and the set of quadratic nonresidues, respectively.

Fix a primitive element $g \pmod p$. Then $g \in \mathcal{S}_2$, since otherwise $g^2 \in \mathcal{S}_1$, $g^3 \in \mathcal{S}_1$, $\ldots$, and thus $\mathcal{S}_1 = \{1, 2, \ldots, p-1\}$ and $\mathcal{S}_2 = \phi$; but we assumed that both $\mathcal{S}_i$'s are nonzero, a contradiction. Furthermore, $g^2 \in \mathcal{S}_1$ because it is a multiple of elements in $\mathcal{S}_2$. This implies that all the even powers of g are contained in $\mathcal{S}_1$, and this in turn implies that all the odd powers of g are contained in $\mathcal{S}_2$, since every odd power of g is g times an even power of g. This completes the proof.

2. $(\frac{1}{p}) = (\frac{4}{p}) = (\frac{9}{p}) = 1$ for all p. Therefore if $(\frac{2}{p}) = 1$ or $(\frac{5}{p}) = 1$, we're done. If neither holds, then $(\frac{10}{p}) = 1$, and we're done.

3. $S(0,p) = \sum_{n=1}^{p} (\frac{n^2}{p}) = p - 1$, since $(\frac{n^2}{p})$ is equal to 1 if $n \not\equiv 0 \pmod p$ and is zero otherwise.

Next,

$$\begin{aligned}\sum_{a=1}^{p} S(a,p) &= \sum_{a=1}^{p}\sum_{n=1}^{p}\Big(\frac{n}{p}\Big)\Big(\frac{n+a}{p}\Big)\\ &= \sum_{n=1}^{p}\sum_{a=1}^{p}\Big(\frac{n}{p}\Big)\Big(\frac{n+a}{p}\Big)\\ &= \sum_{n=1}^{p}\Big(\frac{n}{p}\Big)\sum_{a=1}^{p}\Big(\frac{n+a}{p}\Big)\\ &= 0\end{aligned}$$

because $\sum_{a=1}^{p}(\frac{n+a}{p}) = 0$.

4. By definition $S(a,p) = \sum_{n=1}^{p}(\frac{n^2+na}{p})$. Using the change of variable $n = ma$, we obtain $S(a,p) = \sum_{m=1}^{p}(\frac{m^2a^2+ma^2}{p}) = \sum_{m=1}^{p}(\frac{m^2+m}{p}) = S(1,p)$.

By this and the results of the previous problem, $(p-1)S(1,p) + (p-1) = 0$. This immediately implies $S(1,p) = -1$.

5. Suppose $p_1, \dots, p_r$ are all the 1 mod 4 primes there are, and consider $(2p_1 \dots p_r)^2 + 1$. This is divisible only by primes 1 mod 3. Therefore, by what we know about a sum of two squares, $(2p_1 \dots p_r)^2 + 1$ is a square of an integer, say x^2. But then this implies $1 = x^2 - (2p_1 \dots p_r)^2 = (x + 2p_1 \dots p_r)(x - 2p_1 \dots p_r)$, an impossibility.

6. Fix $\varepsilon > 0$. Then from the Taylor expansion of f around ϕ, i.e.

$$f(x) = \sqrt{5}(x - \phi) + (x - \phi)^2,$$

it follows that $|f(x)| < (\sqrt{5}+\varepsilon)|x-\phi|$ whenever $|x-\phi| < \varepsilon$. (One may think $c = (\sqrt{5}+\varepsilon)^{-1}$.)

Now if $q \in \mathbb{Z}$ has an absolute value strictly greater than $1/2\varepsilon$, then there exists $a \in \mathbb{Z}$ such that $|a/q - \phi| < \varepsilon$. Without loss of generality, pick a that minimizes $|a/q - \phi|$. Substituting $x = a/q$ in the previous inequality above,

$$(\sqrt{5} + \varepsilon)|a/q - \phi| > |(a/q)^2 - a/q - 1| = |a^2 - aq - q^2|/q^2 \geq 1/q^2.$$

Therefore,

$$|a/q - \phi| > (\sqrt{5} + \varepsilon)^{-1}/q^2.$$

Since a minimizes the left side, for all $b \in \mathbb{Z}$ we have

$$|b/q - \phi| > (\sqrt{5} + \varepsilon)^{-1}/q^2.$$

Next suppose $q \in \mathbb{Z}$ has an absolute value less than or equal to $1/2\varepsilon$. There are only finitely many such q's, so we are done if we show that for each q there are only finitely many integers a such that $|a/q - \phi| \leq (\sqrt{5} + \varepsilon)^{-1}/q^2$. But this is plain obvious.