Problem sheet 6 Solutions

Problem 1

(a) It follows from Euler's lemma $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(b) By (a), -1 is quadratic nonresidue if and only if $(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, i.e. $p \equiv 1 \pmod{4}$.

Problem 2

By the law of quadratic reciprocity, we have

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}.$$

Note that $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \pmod{3}$ and $\left(\frac{p}{3}\right) = -1$ if $p \equiv -1 \pmod{3}$. It follows that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

Problem 3

$$\begin{aligned}\left(\frac{107}{1009}\right) &= (-1)^{\frac{(107-1)(1009-1)}{4}}\left(\frac{1009}{107}\right) = \left(\frac{46}{107}\right) = \left(\frac{2}{107}\right)\left(\frac{23}{107}\right)\\ &= (-1)^{\frac{107^2-1}{8}}(-1)^{\frac{(23-1)(107-1)}{4}}\left(\frac{107}{23}\right) = \left(\frac{-8}{23}\right) = -\left(\frac{2}{23}\right)^3\\ &= -(-1)^{\frac{23^2-1}{8}} = -1,\end{aligned}$$

$$\begin{aligned}\left(\frac{21}{101}\right) &= \left(\frac{3}{101}\right)\left(\frac{7}{101}\right)\\ &= (-1)^{\frac{(3-1)(101-1)}{4}}\left(\frac{101}{3}\right)(-1)^{\frac{(7-1)(101-1)}{4}}\left(\frac{101}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{7}\right)\\ &= (-1)\cdot(-1)^{\frac{(3-1)(7-1)}{4}}\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1,\end{aligned}$$

$$\left(\frac{377}{233}\right) = \left(\frac{144}{233}\right) = \left(\frac{12}{233}\right)^2 = 1,$$

$$\begin{aligned}\left(\frac{-104}{131}\right) &= \left(\frac{27}{131}\right) = \left(\frac{3}{131}\right)^3 = \left(\frac{3}{131}\right)\\ &= (-1)^{\frac{(3-1)(131-1)}{4}}\left(\frac{131}{3}\right) = -\left(\frac{2}{3}\right) = -1.\end{aligned}$$

Problem 4

Observe that $2^{2k} - 1 = (2^k + 1)(2^k - 1)$ and $2^k + 1, 2^k - 1 > 1$ for $k > 1$. It follows that if $p = 2^n - 1$ is a prime, then n is odd. We also note that $2^n - 1 \equiv 1 \pmod 3$ for n odd and $2^n - 1 \equiv 3 \pmod 4$ for $n > 2$. Hence by the law of quadratic reciprocity, we have

$$\left(\frac{3}{p}\right) = (-1)^{\frac{(3-1)(p-1)}{4}} \left(\frac{p}{3}\right) = (-1)\left(\frac{1}{3}\right) = -1.$$

Problem 5

It suffices to show that $\left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) = -1$. Since $\left(\frac{-1}{p}\right) = -1$ for $p \equiv 3 \pmod 4$, we have

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

Problem 6

Note that the cardinality of $\{1^2, 2^2 \cdots, (p-1)^2\}$ is $\frac{p-1}{2}$. It implies that the number of quadratic residues and non-residues are both $\frac{p-1}{2}$, hence

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