PMATH 340 Number Theory, Exercises for Chapter 4 (Quadratic Residues)

1: Determine whether $10 \in Q_{37}$ in each of the following four ways.

(a) For each $k \in P = \{1, 2, \cdots, 18\}$, find $k^2 \bmod 37$ and hence determine Q_{37}.

(b) For each $k \in P$, find $10^k \bmod 37$, and hence determine $\left(\frac{10}{37}\right)$ using Euler's Criterion.

(c) For each $k \in P$, find $10k$, determine $|10P \cap N|$, then find $\left(\frac{10}{37}\right)$ using Gauss' Lemma.

(d) Use Quadratic Reciprocity to calculate $\left(\frac{10}{37}\right)$.

2: (a) Find $\left(\frac{19}{53}\right)$.

(b) Find $\left(\frac{71}{127}\right)$.

(c) Find $\left(\frac{649}{967}\right)$.

3: (a) Determine whether $569 \in Q_{2600}$.

(b) Determine whether 84168 is a square (a quadratic residue) modulo 75924.

4: (a) Find all of the primes p with $2 < p < 100$ such that $\left(\frac{11}{p}\right) = 1$.

(b) Find all of the primes p with $2 < p < 100$ such that $\left(\frac{-10}{p}\right) = 1$.

5: Let p be an odd prime, let $a, b, c \in \mathbf{Z}_p$ with $a \neq 0$, and let $d = b^2 - 4ac \in \mathbf{Z}_p$. Show that when $d = 0$ the quadratic equation $ax^2 + bx + c = 0$ has exactly one solution $x \in \mathbf{Z}_p$, and when $d \neq 0$ so $d \in U_p$, if $d \notin Q_p$ then $ax^2 + bx + c = 0$ has no solution $x \in \mathbf{Z}_p$, and if $d \in Q_p$ then $ax^2 + bx + c = 0$ has exactly 2 distinct solutions $x \in \mathbf{Z}_p$.