PMATH 340 Number Theory, Assignment 3 Due: Mon Mar 25, 11:00 pm

1: Make a table showing some of the values of k^2, 3^k, $(-4)^k$ and $-4k$ modulo 31 for $1 \leq k \leq 15$, and then determine whether $-4 \in Q_{31}$ using each of the following 5 methods:

(a) From the list of values k^2 mod 31, determine whether $-4 \in Q_{31}$ using Definition 4.2.

(b) From the list of values 3^k mod 31, determine whether $-4 \in Q_{31}$ using Note 4.8.

(c) From the list of values $(-4)^k$ mod 31, determine whether $-4 \in Q_{31}$ using Theorem 4.11 (Euler's Criterion).

(d) From the list of values $-4k$ mod 31, determine whether $-4 \in Q_{31}$ using Theorem 4.12 (Gauss' Lemma).

(e) Determine whether $-4 \in Q_{31}$ using Theorem 4.9 (The Multiplicative Property) and Theorem 4.14.

2: (a) Determine whether $23 \in Q_{61}$.

(b) Determine whether $47 \in Q_{1111}$.

(c) Determine whether $413 \in Q_{739}$.

3: (a) Determine the number of quadratic residues in U_{400} (that is find $|Q_{400}|$).

(b) Determine the number of quadratic residues in $\mathbb{Z}_{400}$ (that is find $|S_{400}|$).

(c) Let $n = 10^6$. Find the number of solutions to $(x-1)(x-5) = 0$ in $\mathbb{Z}_n$.

4: (a) Prove that for all primes $p > 3$ we have $-3 \in Q_p \iff p = 1 \bmod 6$.

(b) Find a set $S \subseteq U_{24}$ such that for all primes $p > 3$ we have $6 \in Q_p \iff p \in S \bmod 24$.

(c) Find a set $S \subseteq U_{28}$ such that for all primes $p > 7$ we have $7 \in Q_p \iff p \in S \bmod 28$.