Homework #8. Due Thursday, April 3rd

Reading:

1. For this homework assignment: Chapter 7.
2. For the next two classes: Chapter 9.

Problems:

1. Let $p > 3$ be a prime. Prove that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \mod 12 \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \mod 12 \end{cases}$$

in two different ways:

(i) using quadratic reciprocity

(ii) directly using Gauss lemma (similarly to the way we computed $\left(\frac{2}{p}\right)$ in class).

2. Let q be an odd primes, and set $N = q$ if $q \equiv 1 \mod 4$ and $N = 4q$ if $q \equiv 3 \mod 4$. Prove that if p is an odd prime different from q, then the Legendre symbol $\left(\frac{q}{p}\right)$ is completely determined by the congruence class of p mod N. In other words, prove that there exist integers $a_1, \ldots, a_t$ and $b_1, \ldots, b_s$ depending only on q such that

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv a_1, \ldots, \text{ or } a_t \mod N \\ -1 & \text{if } p \equiv b_1, \ldots, \text{ or } b_s \mod N \end{cases}$$

Before doing problems 3 and 4 make sure to read sections 7.2, 7.5 and 7.6 which were not discussed in class.

3. Let p be an odd prime, let $a \in \mathbb{Z}$ be coprime to p, and let $k \geq 1$ be an integer. Use the lifting method to prove that a is a quadratic residue mod $p^k \iff a$ is a quadratic residue mod p. Note that a completely different (group-theoretic) proof of this fact is given in the book (Theorem 7.13)

4. Let Q_n be the group of quadratic residues mod n (in this problem we think of quadratic residues as elements of U_n, not as integers, which is the convention that the book uses).

(a) Let n be an odd integer. Prove that $|Q_n| = \frac{\phi(n)}{2^k}$ where k is the number of distinct prime divisors of n.

(b) Prove that Q_{105} is a cyclic group of order 6.

(c) Find a generator for Q_{105}.

5. Exercise 7.20 from the book.
6. Exercise 7.21 from the book.