Homework #7. Due Wednesday, March 20th

Nothing is due in writing this week, but you should do Problems 1 and 2 as a preparation for next week's classes (this is especially relevant for the class on Wednesday). Also, Problems 3-6 below will likely appear in the next assignment, perhaps in a slightly modified form.

1. Read Chapter 7 as well as the proof of quadratic reciprocity available at `http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=4932268`

2. Review the definition of quotient groups. Then solve the following problem: let p be an odd prime, let $G = U_p$ and $H = \{\pm[1]_p\}$. Clearly, H is a subgroup of G, which is automatically normal (since G is abelian), so we can consider the quotient group G/H. Prove that each of the following sets S contains precisely one element from every left coset gH, and thus we can identify G/H with $\{sH : s \in S\}$ as sets:

(i) $S = \{[1], [2], \ldots, [\frac{p-1}{2}]\} = \{[x] : 1 \leq x \leq \frac{p-1}{2}\}$

(ii) $S = \{[1], [3], [5], \ldots, [p-2]\} = \{[2x-1] : 1 \leq x \leq \frac{p-1}{2}\}$

3. Let $p > 3$ be a prime. Compute the Legendre symbol $\left(\frac{3}{p}\right)$ in two different ways:

(i) using quadratic reciprocity

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

4. Let p be a prime (no restrictions this time). Find the number of mod p solutions to the congruence $x^2 + x + 1 \equiv 0 \mod p$.

5. 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.

6.

(a) Let n be an odd integer. Prove that the number of quadratic residues modulo n is equal to $\frac{\phi(n)}{2^k}$ where k is the number of distinct prime divisors of n.

(b) Find all quadratic residues modulo 105 by doing a few computations as possible.