Homework #8. Due Wednesday, March 27th

Reading:

1. For this homework assignment: Chapter 7. Make sure to read 7.2, 7.5 and 7.6 (in class we did not discuss 7.5, 7.6 and most of 7.2).

2. For the next two classes: Chapter 8.

Problems:

1. Let p be an odd prime. Prove that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$.

2. Let p be an odd prime, and consider a congruence $ax^2+bx+c \equiv 0 \mod p$ where $p \nmid a$. Prove the number of (mod p) solutions to this congruence is equal to $1+\left(\frac{b^2-4ac}{p}\right)$.

3. Compute the Legendre symbols $\left(\frac{331}{113}\right)$ and $\left(\frac{319}{107}\right)$.

4. Let $a, b, c \in \mathbb{Z}$. Prove that for any prime p, the congruence $(x^2-ab)(x^2-ac)(x^2-bc) \equiv 0 \mod p$ has a solution.

5. 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).

6. 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)

7. 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}.

8. Let p be an odd prime.

(a) Prove that $\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \mod p$ (we used this congruence in the proof of quadratic reciprocity in class). **Hint:** write each expression as a product of $p-1$ elements and show that after suitable reordering of factors, the i^{th} factor on the left is congruent mod p to the i^{th} factor on the right, for each i.

(b) Use (a) and Wilson's theorem to prove that if $p \equiv 3 \mod 4$, then $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \mod p$. Bonus: when is it plus and when is it minus?

9. Exercise 7.20 from the book.

10. Exercise 7.21 from the book.