Homework #7. Due Thursday, March 27th

Reading:

1. For this homework assignment: Chapter 7.

2. For the next two classes: Also Chapter 7.

Problems:

0. Read the proof of quadratic reciprocity available at
`http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=4932268`
This is the proof I will present in class (though using slightly different language)

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 reduced 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. The goal of this problem is to use Legendre symbols to prove that there are infinitely many primes of the form $8n+3, 8n+5$ and $8n+7$. The fact that there are infinitely primes of the from $8n+1$ is a special case of Exercise 7.20 from the book (which thereby completes the proof of Dirichlet's theorem for $b = 8$).

The following facts are (very) relevant for this problem:
(i) If p is an odd prime, the Legendre symbol $\left(\frac{2}{p}\right)$ is equal to 1 if $p \equiv 1$ or 7 mod 8 and is -1 if $p \equiv 3$ or 5 mod 8;
(ii) $x^2 \equiv 1 \mod 8$ for any odd x.

(a) Prove that there are infinitely many primes of the form $8n + 5$. **Hint:** Assume there are only finitely many such primes $p_1, \ldots, p_k$, let $m = 4(p_1 \ldots p_k)^2 + 1$ and show that m has a prime factor of the form $8n+5$. This is essentially a combination of the methods used to prove that there are infinitely many primes of the form $4n+3$ and infinitely many primes of the form $4n+1$, discussed in class.

(b) Now prove that there are infinitely many primes of the form $8n+7$. **Hint:** Use a trick similar to (a) and (i) and (ii) above.

(c) Finally prove that there are infinitely many primes of the form $8n+3$. **Hint:** First find an integer $m \in \mathbb{Z}$ such that for any odd prime p we have $\left(\frac{m}{p}\right) = 1 \iff p \equiv 1$ or $3 \bmod 8$.

6. Let p be an odd prime.

(a) Prove that $\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \mod p$ (this congruence will be used 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 (very hard): when is it plus and when is it minus?