Homework 5 : Due Wednesday, March 3

Problem 1: Suppose that p is prime, that $a, b \in \mathbb{Z}$, and that $p \nmid a$. Show that

$$\sum_{k=0}^{p-1} \left(\frac{ak+b}{p} \right) = 0$$

Problem 2: Suppose that p is an odd prime and that $n \mid (p-1)$. Show that the set of n^{th} powers forms a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $\frac{p-1}{n}$.

Problem 3: Let p be an odd prime.
a. Show that a primitive root modulo p must be a quadratic nonresidue modulo p.
b. Show that every quadratic nonresidue modulo p is a primitive root modulo p if and only if $p = 2^n + 1$ for some $n \in \mathbb{N}^+$. Such primes are called *Fermat primes* and in fact any such prime must be of the form $2^{2^k}+1$.

Problem 4: Consider the polynomial $f(x) = x^6 + x^4 - 4x^2 - 4$. Show that f has a root modulo every prime, but f has no integer roots.
Hint: Begin by factoring $f(x) = (x^2 + 1)(x^4 - 4)$.

Problem 5: Suppose that p is an odd prime.
a. Show that if $p \equiv_4 1$, then the product of the quadratic residues in the set $\{1, 2, \ldots, p-1\}$ is congruent to -1 modulo p.
b. Show that if $p \equiv_4 3$, then the product of the quadratic residues in the set $\{1, 2, \ldots, p-1\}$ is congruent to 1 modulo p.

Problem 6: Suppose that $p > 3$ is prime. Prove that the sum of the quadratic residues in the set $\{1, 2, \ldots, p-1\}$ is congruent to 0 modulo p. What is the sum equal to when $p = 3$?