MATH 152: PROBLEM SET 5

Due October 27

1. Divide the residue classes 1, 2, $\dots$, $p-1 \pmod p$ (p an odd prime) into two nonempty sets $\mathcal{S}_1$ and $\mathcal{S}_2$ such that the product of two residue classes from the same set is always in $\mathcal{S}_1$, while the product of an element from $\mathcal{S}_1$ and an element from $\mathcal{S}_2$ always lies in $\mathcal{S}_2$. Prove that $\mathcal{S}_1$ is the set of quadratic residues, and $\mathcal{S}_2$ the set of quadratic nonresidues.

2. Suppose $p \ge 7$ is prime. Show that there exists at least one number n in the interval $1 \le n \le 9$ such that $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) = 1$.

3. Let p be an odd prime and put $S(a,p) = \sum_{n=1}^{p} \left(\frac{n(n+a)}{p}\right)$. Prove that $S(0,p) = p-1$ and that $\sum_{a=1}^{p} S(a,p) = 0$.

4. Keep the notations of problem 3, and show that if $(a,p)=1$ then $S(a,p) = S(1,p)$. (Hint: multiply $n(n+1)$ by a^2.) Using problem 3, conclude that $S(a,p) = -1$ if $(a,p)=1$.

5. Let p_1, $\dots$, p_r be primes of the form $1 \pmod 4$ and consider $(2p_1 \cdot p_2 \cdot \dots \cdot p_r)^2 + 1$. Using this observation and your knowledge of what numbers are sums of two squares, show why there are infinitely many primes $\equiv 1 \pmod 4$.

6. In class we discussed Dirichlet's theorem which shows that for any irrational θ there are infinitely many rational approximations a/q with $(a,q)=1$ and $|\theta - a/q| \le 1/q^2$. In fact, this can be strengthened a little, and there exist infinitely many approximations with $|\theta - a/q| \le 1/(\sqrt{5}q^2)$. This exercise will show that Dirichlet's theorem cannot be strengthened any further.

Let c be any real number strictly below $1/\sqrt{5}$. Let ϕ denote the Golden Ratio $(1+\sqrt{5})/2$ which is the positive solution to $(f(x) =) x^2 - x - 1 = 0$. Prove that there are only finitely many rational numbers a/q with $(a,q)=1$ that satisfy $|\phi - a/q| \le c/q^2$.

Hint: What is a lower bound for $|f(a/q)|$? Then consider $|f(\phi) - f(a/q)|$ ....