MATH 152: PROBLEM SET 4

Due October 20

1. Let $p \equiv 7 \pmod{40}$ be such that $p-1=2q$ for a prime q. Prove that 10 is a quadratic non-residue $\pmod{p}$. Prove that 10 is a primitive root $\pmod{p}$.

2. Given a square-free number n (that is, n is not divisible by the square of any prime), we stated in class that the primes p for which n is a quadratic residue $\pmod{p}$ may be described as those primes lying in certain residue classes $\pmod{4n}$. Prove this. It may help you to start with an example like $n=15$ and build a proof.

3. Let p be an odd prime such that every quadratic non-residue $\pmod{p}$ is a primitive root $\pmod{p}$.

(i) Show that p is of the form 2^k+1 for some positive integer k.

(ii) Now show that p is of the form $2^{2^n}+1$ for a non-negative integer n.

(iii) Conversely if p is of the form $2^{2^n}+1$ then show that every quadratic non-residue is a primitive root.

4. Explain what this sentence means: "In the 7-adics, the square root of 2 equals $\ldots 213$." Your explanation should make as much sense as $\sqrt{2}=1.414\ldots$.

5. The unit disc $\{x \in \mathbb{Q} : \ |x|<1\}$ has as its unique center the point 0. Consider now the p-adic unit disc $\{x \in \mathbb{Q} : \ |x|_p<1\}$. Show that every point in this disc is at the center of the disc.

6. Let p be an odd prime and consider the congruence $x^2+10x-10 \equiv 0 \pmod{p}$.

(a) Find a number n such that the above congruence has two solutions if and only if n is a quadratic residue $\pmod{p}$.

(b) Describe the odd primes p such that n is a quadratic residue $\pmod{p}$, where n is the number from part (a).