Math 435 Number Theory I

Problem Set 11

1) Which of the following numbers are quadratic residues mod 1200?

a) 619 b) 841 c) 937

2) Use the method of descent from the proof of Theorem 10.1 to write 1973 as the sum of two squares. Start from the fact that $259^2 \equiv -1 \pmod{1973}$.

3) Suppose p is prime and $p = a^2 + 5b^2$ where $a, b \in \mathbb{Z}$. Prove that $p = 5$ or $p \equiv 1$ or $9 \pmod{20}$.

4) (5pt Bonus) Let $f(X) \in \mathbb{Z}[X]$. Suppose $f(a) \equiv 0 \pmod{p^j}$, $p^t | f'(a)$, $p^{t+1} \not| f'(a)$ and $j \geq 2t + 1$. Prove that there is k such that if $b = a + p^{j-t}k$ then $f(b) \equiv 0 \pmod{p^{j+1}}$.