ELEMENTARY NUMBER THEORY

HOMEWORK 5

These are problems I will be going through next Tuesday. Solve as many as you can, but at least four.

(1) Use Gauss's Lemma to prove that $(\frac{-2}{p}) = +1$ or -1 according as $p \equiv 1, 3 \bmod 8$ or $p \equiv 5, 7 \bmod 8$.

(2) Show that $\sum_{a=1}^{p-1} (\frac{a}{p}) = 0$.

(3) Let $p = a^2 + 4b^2$ be a prime. Show that $(\frac{a}{p}) = +1$.

(4) Show that, for Fermat primes $p = F_n = 2^{2^n} + 1$, we have $\phi(p-1) = \frac{p-1}{2}$. Conclude that every quadratic nonresidue mod p is a primitive root mod p.

(5) Show that 3 is a primitive root modulo p for every for every Fermat prime F_n with $n > 0$.

(6) Let $n = 4m^2 + 3$, where m is an integer not divisible by 3. Show that there exists a prime $p \mid n$ with $p \equiv 7 \bmod 12$.

(7) Show that there are infinitely many primes $p \equiv 7 \bmod 12$.