PMATH 340 **Assignment 3, due March 3**

1. Let $f(x) = 5x^6 + 7x^4 + 8x^3 + 9x + 10, g(x) = 4x^3 + 5x^2 + 2x + 1 \in F_{11}[x]$. Find polynomials $q(x), r(x) \in F_{11}[x]$ such that $f(x) = q(x)g(x) + r(x)$, where $\deg(r(x)) < \deg(g(x))$ or else $r(x)$ is the zero polynomial.

2. Let p be a odd prime of the form $p = 2^m + 1$, for some positive integer m. Let g be a primitive root mod p with $1 \leq g \leq p$. How many such g are there? Justify your answer.

3. a) Find the orders mod 17 of all $1 \leq a \leq 16$. b) How many of these a are primitive roots mod 17? List them. c) List the quadratic residues mod 17.

4. Show that 2^k has no primitive roots if $k > 2$. Note: a is said to be a primitive root mod m if it has order equal to $\phi(m)$. When considering this problem, you can restrict yourself to $\gcd(a, 2^k) = 1$, namely a odd, since even a cannot have finite order mod 2^k. hint: show, if $k > 2$, that $a^{\phi(2^k)/2} \equiv 1$ mod 2^k for all odd $1 \leq a < 2^k$.

5. Let p be prime and congruent to 1 mod 4. i) How many $1 \leq a < p$ are there of order 4? ii) Use part i to show that there exist integers x such that $x^2 \equiv -1 \mod p$. While there are a variety of proofs to ii, to get credit for ii your proof should rely on i.

6. Let p be an odd prime. Show that the product of two primitive roots mod p is not a primitive root mod p.