189-235A: Basic Algebra I
Assignment 3

Due: Monday, October 29

1. Perform the division algorithm for dividing $f(x) = 3x^4 - 2x^3 + 6x^2 - x + 2$ by $g(x) = x^2 + x + 1$ in $\mathbf{Q}[x]$. (I.e., find polynomials $q(x)$ and $r(x)$ with $\deg(r) < \deg(g)$ satisfying $f = gq + r$.

2. Same question as 1, with $f(x) = x^5 - x + 1$ and $g(x) = x^2 + x + 1$ in $\mathbf{Z}/2\mathbf{Z}[x]$.

3. Let $f : \mathbf{Z}[x] \to \mathbf{Z}$ be the function which to any polynomial $p(x) = a_0 + a_1 x + \cdots + a_d x^d$ associates its constant term a_0: $f(p) = a_0$. Show that f is a homomorphism of rings, i.e., it satisfies $f(p_1 + p_2) = f(p_1) + f(p_2)$ and $f(p_1 p_2) = f(p_1) f(p_2)$.

4. Find the gcd of $x^4 + 3x^3 - 2x + 4$ and $x^2 + 1$ in $\mathbf{Z}/5\mathbf{Z}[x]$ using the Euclidean algorithm.

5. List all the monic irreducible polynomials of degree 3 in $\mathbf{Z}/2\mathbf{Z}[x]$.

6. If p is an odd prime of the form $1 + 4m$, use Wilson's Theorem to show that $a = (2m)!$ is a root in $\mathbf{Z}/p\mathbf{Z}$ of the polynomial $x^2 + 1$ in $\mathbf{Z}/p\mathbf{Z}[x]$. Show that there is no such root when p is a prime of the form $3 + 4m$.

7. Make a list of all the primes $p \leq 50$ for which the polynomial $x^2 + x + 1$ has a root in $\mathbf{Z}/p\mathbf{Z}[x]$, and those primes for which it remains irreducible. Can you detect a pattern, similar to the one in problem 6?

8. Find a polynomial of degree 2 in $\mathbf{Z}/6\mathbf{Z}[x]$ that has four roots in $\mathbf{Z}/6\mathbf{Z}$. Why does this not contradict the theorem shown in class that a polynomial in $F[x]$ of degree d has at most d roots?

9. Exercise (2), parts (a), (c), (e) and (f) on page 65 of Eyal Goren's notes.

10. Let p be a prime and let F denote the field $\mathbf{Z}/p\mathbf{Z}$ with p elements.

(a) Show that the polynomial $x^p - x$ factors into p distinct linear factors in $F[x]$.

(b) Let $g(x)$ be a polynomial in $F[x]$. Show that $\gcd(x^p - x, g(x))$ is a polynomial whose degree is equal to the number of distinct roots of $g(x)$ in F.

(c) Use (b) to describe a realistic algorithm for computing the number of roots of a polynomial $g(x)$ in F. (By realistic, we mean that a computer could perform the calculation in a matter of seconds, for p a prime of around 20 or 30 digits and g a polynomial of degree 10 or so.)