189-235A: Basic Algebra I
Assignment 3

Due: Monday, October 21

1. Perform the Euclidean algorithm to find the gcd of $f(x) = x^4 + 3x^3 + 16x^2 + 33x + 55$ and $g(x) = x^3 + x^2 - x - 10$ in the polynomial ring $\mathbf{Q}[x]$. Write this greatest common divisor as a linear combination of $f(x)$ and $g(x)$ with coefficients in $\mathbf{Q}[x]$.

2. Same question as 1, with $f(x) = x^6 + x^4 + x + 1$ and $g(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ in $\mathbf{Z}/2\mathbf{Z}[x]$.

3. List all the irreducible polynomials of degree 4 in $\mathbf{Z}/2\mathbf{Z}[x]$.

4. 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 $\mathbf{Z}/p\mathbf{Z}[x]$.

5. In class, we showed that a polynomial of degree d with coefficients in a field F has at most d roots. Show that this statement ceases to be true when F is replaced by an arbitrary ring, such as the ring $\mathbf{Z}/n\mathbf{Z}$ of residue classes modulo n with n a composite integer.

6. Let d be a fixed integer. Let $n = pq \in \mathbf{Z}$ be an integer which is a product of two distinct primes, p and q, and let $f \in \mathbf{Z}/n\mathbf{Z}[x]$ be a monic polynomial with coefficients in $\mathbf{Z}/n\mathbf{Z}$ of degree d. Give a "best possible" general upper bound (as a function of d) for the number of distinct roots that such a polynomial could have over $\mathbf{Z}/n\mathbf{Z}$, and show with an example that your estimate is indeed best possible. (I.e., describe a judicious choice of f having the maximal number of distinct roots.)

7. Write down the powers of x in the ring $\mathbf{Z}/2\mathbf{Z}[x]/(x^3 + x + 1)$ and show that every non-zero element in this ring can be expressed as a power of x.

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

9. Use the result of question 8 to show that the polynomial $x^2 + 1$ has no roots in $\mathbf{Z}/p\mathbf{Z}$ when p is a prime of the form $3 + 4m$. (Note how this result compares with what you've found in Problem 4.)

10. Use the result of question 8 to describe a realistic algorithm for computing the number of roots of a polynomial $g(x)$ in $F = \mathbf{Z}/p\mathbf{Z}$. (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.)