Algebra Homework 3

Due by the *start* of class on Wednesday Oct. 14

The problems with the asterisks $*$ might need material from Wednesday's (or next Wednesday's) class.

Problem 1: In $\mathbb{Z}_3[x]$, show that $x^4 + x$ and $x^2 + x$ determine the same function (that is, $f(a) = g(a)$ for all $a \in \mathbb{Z}_3$). In high school, you might have conflated the concept of a polynomial with the concept of the function $\mathbb{R} \to \mathbb{R}$ it defines. This problem should teach you not to conflate these concepts for polynomials with more exotic coefficients.

Problem 2: Let $f(x) = x^2 + 3x + 2 \in \mathbb{Z}_6[x]$. Show that there are four elements $a \in \mathbb{Z}_6$ such that $f(a) = 0$.

Problem 3: Let $f = 5x^4 + 3x^3 + 1$ and $g = 3x^2 + 2x + 1$ be elements of $\mathbb{Z}_7[x]$. Apply polynomial long division to find polynomials q, r such that $f = qg + r$ and $\deg(r) < \deg(g)$.

Problem 4: You are a Chinese general and your army has just come back from battle. You want to count the survivors, but this would take hours: you can tell that are somewhere between 10,000 and 15,000 of them! Instead, you tell them to form groups of 15. There are three soldiers left over. Then you tell them to form groups of 16. Again, there are three soldiers left over. Finally, you tell them to form groups of 17. Again, there are three soldiers left over. Use the chinese remainder theorem to calculate the exact number of survivors. (Hint: there is one "obvious" integer k such that $[k] = [3]$ in $\mathbb{Z}_{15}, \mathbb{Z}_{16}$, and $\mathbb{Z}_{17}$, but it is not between 10,000 and 15,000).

Problem 5: Let R be the set of real numbers that can be expressed in the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$.

1. Show that R is a subring of $\mathbb{R}$ and that it is a field.
2. Show that $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is isomorphic to R.
3. Prove (or disprove) that $\langle x^2 - 2\rangle$ is a maximal ideal in $\mathbb{Q}[x]$.
4. Prove (or disprove) that $\langle x^2 - 2\rangle$ is a maximal ideal in $\mathbb{R}[x]$.

Problem 6*:

1. Let $f \in \mathbb{Z}_p[x]$, where p is a prime. If f is irreducible and $\deg(f) = n$, then prove that $\mathbb{Z}_p[x]/\langle f\rangle$ is a field with p^n elements.
2. Find a field with 9 elements. Find a field with 25 elements. (hint: For the field with nine elements, it might help to write down all the squares in $\mathbb{Z}_3$ – that is, the elements of the set $\{x^2 \mid x \in \mathbb{Z}_3\}$. Does this help you determine which of the polynomials of the form $x^2 + a$, for $a \in \mathbb{Z}_3$ are irreducible?)

Problem 7*: Write $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ as a product of irreducible elements in $\mathbb{Z}_2[x]$.

Problem 8*: Let F be a finite field (i.e. a field with finitely many elements).

1. Prove that there is a nonzero polynomial p such that $p(a) = 0$ for *all* elements $a \in F$.
2. Prove that there is an irreducible polynomial in $F[x]$ of degree > 1. (hint: Does $p + 1 \in F[x]$ have any roots? Does it have linear factors?)
3. Prove that for every finite field F, there is a finite field E with more elements than F that contains F as a subring.