Homework 6 : Due Wednesday, March 9

**Problem 1:** Let $K$ be a finite field with $|K| = p^n$. Define a function $\sigma: K \to K$ by letting $\sigma(a) = a^p$.

a. Show that $\sigma$ is an automorphism of $K$ (it is called the Frobenius automorphism).

b. Show that $\sigma$ has order $n$, i.e. that $\sigma^n = id_K$ and $\sigma^m \neq id_K$ for all $m < n$.

c. Show that $n \mid \varphi(p^n - 1)$ for every prime $p$ and $n \in \mathbb{N}^+$.  
*Hint for c:* Think about the multiplicative group $K \setminus \{0\}$.

**Problem 2:** Show that $x^{p^n} - x \in \mathbb{Z}/p\mathbb{Z}[x]$ equals the product of all monic irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ over all degrees $d \mid n$. For example, over $\mathbb{Z}/2\mathbb{Z}$, we have

$$x^8 - x = x^8 + x = x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

where the factors on the right are all of the monic irreducible polynomials of degree either 1 or 3.

**Problem 3:** Let $K = \mathbb{Z}/3\mathbb{Z}$. Notice that $x^3 + 2x + 1$ and $x^3 + 2x + 2$ are irreducible in $K[x]$. Let

$$F = K[x]/\langle x^3 + 2x + 1 \rangle \quad E = K[x]/\langle x^3 + 2x + 2 \rangle$$

We know that $F$ and $E$ are both fields of order 27 and hence must be isomorphic. Writing $u = \overline{x}$ in $F$, we have $F = \{ a + bu + cu^2 : a, b, c \in K \}$. Also, writing $w = \overline{x}$ in $E$, we have $E = \{ a + bw + cw^2 : a, b, c \in K \}$. Describe an explicit isomorphism $\varphi: F \to E$. That is, give a formula for $\varphi(a + bu + cu^2)$.

**Problem 4:** Let $K$ be a field with 25 elements.

a. Show that $K$ has an element $u$ such that $u^2 = 3$.

b. Show that $K = \mathbb{Z}/5\mathbb{Z}(u)$.

c. Show that $u + 1$ is a generator of $K \setminus \{0\}$.
*Hint for c:* You can greatly minimize the computations with a bit of theory.

**Problem 5:**

a. Show that $8 \mid (k^2 - 1)$ for every odd $k \in \mathbb{N}^+$.

b. Show that $x^4 + 1$ splits in $\mathbb{F}_{p^2}$ for every prime $p$.

c. Show that $x^4 + 1$ is reducible in $\mathbb{Z}/p\mathbb{Z}[x]$ for every prime $p$. (*Note:* It is irreducible in $\mathbb{Q}[x]$).