Math 567: Introduction to Coding Theory

Homework 2: Due Wednesday, February 13

Problem 1.1. Let q be an integer with $q \geq 2$ and m, n be integers. Show that $q^m - 1 \mid q^n - 1$ if and only if $m \mid n$.

Problem 1.2. Let F be a field of characteristic p. Show that $p\gamma = 0$ for all $\gamma \in F$.

Problem 1.3. Let F be a finite field and $\#I(F, d)$ denote the number of monic irreducible polynomials in $F[x]$ of degree d. Compute $\#I(F, d)$ for $F = \mathbb{Z}/(p)$ for each prime $p = 2, 3, 5$ and each $d = 1, 2, 3, 4, 5, 6$.

Problem 1.4. Let F be a finite field with q elements and $f \in F[x]$ have degree d. Show that f is irreducible if and only if $f(x)$ divides $x^{q^d} - x$ and the (monic) gcd of $f(x)$ and $x^{q^j} - x$ is 1 for each $j < d$ with $j \mid d$.

Problem 1.5. Show that if q is an integer at least 2, then

$$\frac{q^d}{d} - \frac{2q^{d/2}}{d} \sim \frac{q^d}{d} \qquad \text{as d} \to \infty,$$

where we say that $f(d) \sim g(d)$ if $\lim_{d\to\infty} f(d)/g(d) = 1$.

Problem 1.6. Show that the additive group of a finite field is cyclic if and only if the field has a prime number of elements.

Problem 1.7. Suppose that p is a prime, $d \geq 1$ and K is a field with p^d elements. In class we showed that every element of K is a root of $x^{p^d} - x$. Show that if $j \mid d$ then set F of roots in K of $x^{p^j} - x$ is a subfield of K with p^j elements.

Problem 1.8. Let F be a finite field. Show that every function $f : F \to F$ is a polynomial.