Math 567: Introduction to Coding Theory

Homework 1: Due Wednesday, January 23

Problem 1.1. Show that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field.

Problem 1.2. Let F be a finite field and $a, b \in F$. Show that if $ab = 0$ then $a = 0$ or $b = 0$.

Problem 1.3. Show that if p is a prime number then

$$(p-1)! \equiv -1 \pmod{p}.$$

Problem 1.4. Let $F = \mathbb{Z}/(2)$ and define $M = x^2 + 1$ and $N = x^2 + x + 1$ in $F[x]$. Each of the systems $F[x]/(M)$ and $F[x]/(N)$ has four elements. Write out the full 4×4 multiplication table for each system. Are either of these systems a field?

Let F be a field. One of the benefits of working with the polynomial ring $F[x]$ is that it is a *Euclidean domain*. What this means is that it has the following division-with-remainder property:

Theorem 1.5. Let F be a field and $A, B \in F[x]$ with $B \neq 0$. Then there exist $Q, R \in F[x]$ with

$$A = QB + R \qquad \textit{with } R = 0 \textit{ or } \deg R < \deg B.$$

Problem 1.6. Let F be a field. Use Theorem 1.5 to show that if $f \in F[x]$ and $\alpha \in F$ then $x - \alpha$ divides f if and only if $f(\alpha) = 0$.

Problem 1.7. Let F be a field, $f \in F[x]$ and $d = \deg f$. Show that f has at most d roots in F.

Although in class we only worked with polynomials defined over fields, we can form, for any commutative ring R, the ring $R[x]$ of *univariate polynomials defined over* R. A typical element of $R[x]$ is

$$a_d x^d + \cdots + a_1 x + a_0 \qquad \textit{with } a_0, \ldots, a_d \in R.$$

Problem 1.8. Give an example of a ring R and polynomial $f \in R[x]$ for which the last exercise fails.