Notes for 12 March (Tuesday)

1 The road so far...

1. Proved that polynomial functions are the same as polynomials for infinite fields (but not necessarily so for finite fields).

2. Developed the division and Euclidean algorithms. Stated Bezout's identity for polynomials.

2 Polynomials

Now we wish to prove a fundamental theorem of arithmetic for polynomials. Before that, recall that an irreducible element e of a commutative ring R is a non-zero non-unit such that if $e = fg$ then f or g has to be a unit. Likewise, a prime element p is a non-zero non-unit that if fg is divisible by p, then either f or g is divisible by p. On an integral domain, primes are irreducibles.

Theorem 1. *Irreducibles are primes in* $\mathbb{F}[x]$.

Proof. (I am sorry. The proof I gave in the class today was incorrect. So was the corresponding proof for integers on 31 Jan. I corrected the notes for that day.) If e is an irreducible such that $ek = fg$, then by Bezout's identity, if f is not divisible by e, $en + fm = 1$ and hence $e(ng + km) = g$. Thus e is a prime. □

As a HW you will show the following theorem holds.

Theorem 2. *In* $\mathbb{F}[x]$, *every* f *factors uniquely (up to) units into a product of irreducible polynomials. If we use monic irreducibles, the factors are unique upto permutation.*

Just as in integers, we write $f(x) = p_1^{e_1} p_2^{e_2} \ldots$. If $e_i > 1$, then p_i is said to be a multiple factor with multiplicity e_i. If $p_i(x) = x - a$ then a is said to be a multiple root with multiplicity e_i (if $e_i > 1$ that is). Now we defined congruences : Let $\mathbb{F}$ be a field and $f, g, m \in \mathbb{F}[x]$ ($m \notin \mathbb{F}$). Then $f \equiv_m g$ iff $f = g + hm$ where $h \in \mathbb{F}[x]$. It can be proven easily that $\equiv_m$ is an equivalence relation. Here are some basic properties. For all $f_1, f_2, g, g_1, g_2, k \in \mathbb{F}[x]$,

1. If $f \equiv_m g$, then $kf \equiv_m kg$.

2. If $f_1 \equiv_m g_1$, $f_2 \equiv_m g_2$, then $f_1 + f_2 \equiv_m g_1 + g_2$. Likewise for multiplication.

3. If $f \equiv_m g$ then $f^n \equiv_m g^n \ \forall \ n \geq 0$.

The set of f modulo m can be checked to be a ring under the above operations. Constructing it from $\mathbb{F}[x]$ is not entirely trivial. We may return to it later if time permits.

Lemma 2.1. *Let $f, g, h, m \in \mathbb{F}[x]$ and $m \neq 0$. If $hf \equiv_m hg$, and h, m are coprime, then $f \equiv_m g$.*

Proof. $h(f - g) = mk$. Since h, m are coprime, $f - g = mk_1$. (This follows from a theorem we proved earlier.) □

As in the case of integers, applying the Division theorem produces the following lemmata.

Lemma 2.2. *Let m be a polynomial of degree ≥ 0. If f is any polynomial in $\mathbb{F}[x]$, then $f \equiv_m g$ for a unique g s.t. $deg(g) < deg(m)$ called the residue of least degree.*

Lemma 2.3. *Two polynomials are congruent iff their least degree residues are equal.*

The remainder theorem shows that

Lemma 2.4. *If $f(x) \in \mathbb{F}[x]$, then $f(x) \equiv_{x-r} f(r)$.*

Here are a couple of examples.

1. Find the least degree residues of x^n modulo $m(x) = x^3 + x + 1$ in $\mathbb{F}_2[x]$: Note that $1, x, x^2$ are residues anyway. Now $x^3 \equiv_m -x - 1 \equiv_m x + 1$ (because $-1 = 1$ in $\mathbb{F}_2$). $x^4 \equiv x.(x + 1) = x^2 + x$. $x^5 \equiv x^2.(x + 1) = x^3 + x^2 \equiv x^2 + x + 1$. $x^6 \equiv x^5.x = x^3 + x^2 + x = x^2 + x + x + 1 = x^2 + 1$ and $x^7 = x^3 + x = 1$. Therefore, if $n = 7q + r$, then $x^n \equiv_m x^r$.

2. Let $m(x) = x^2 + x + 1$ in $\mathbb{F}_3[x]$. Find the least degree residues of x^n : Note that $1, x$ are residues anyway. Since $x^3 - 1 = (x - 1)(x^2 + x + 1)$, $x^3 \equiv_m 1$. Thus if $n = 3q + r$, then $x^n \equiv x^r$.

Just as in the case of integers, we can solve linear "Diophantine"-type equations.

Theorem 3. *Let $a, b, m \in \mathbb{F}[x]$. There exists a solution $u \in \mathbb{F}[x]$ to $au \equiv_m b$ iff $d = gcd(a, m)|b$.*

Proof. If there is a solution, then $au = mk + b$ and hence d divides b. If d divides b, then by Bezout's identity, there exist k_1, u_1 such that $au_1 - mk_1 = d$ and hence $u_0 = \frac{b}{d}u_1$ works. □