Notes for 13 March (Wednesday)

1 The road so far...

1. Irreducibles are the same as primes in $\mathbb{F}[x]$ (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.)

2. Stated the fundamental theorem of arithmetic for polynomials.

3. Defined congruences, the ring $\mathbb{F}_m[x]$ and solved linear Diophantine equations $au \equiv_m b$.

2 Polynomials

If u is any other solution, then $v = u - u_0$ solves $av = mk$. Therefore, $v = \frac{m}{d}k_2$. For example,
In $\mathbb{F}_3[x]$, let $m(x) = x^3 + x + 2$ and $f(x) = x^2 + 2x$. Find $z(x)$ so that $fz \equiv_m 1$, i.e., $fz + mw = 1$. We use the extended Euclidean algorithm : $m = f(x-2) + 2x + 2$. So $x^2 + 2x = (2x+2).(2x+2) - 1$. So $-1 = x^2 + 2x - (2x+2)(2x+2) = x^2 + 2x - (m - f(x-2))(2x+2) = f(1 + (x-2)(2x+2)) - m(2x+2)$.
As in the case of integers we can completely characterise the units and zero-divisors.

Theorem 1. *Let $m(x) \in \mathbb{F}[x]$ have deg > 0. For $f(x) \in \mathbb{F}[x]$,*

1. *f is a unit modulo m iff $gcd(m, f) = 1$.*

2. *f is a zero divisor modulo m iff f is not divisible by m and $gcd(m, f)$ has degree ≥ 1.*

We can now state and prove the Chinese remainder theorem.

Theorem 2. *Let $a_1, \ldots, a_d, m_1, m_2, \ldots, m_d(x) \in \mathbb{F}[x]$ such that m_i are pairwise coprime. Then there exists an $f \in \mathbb{F}[x]$ such that $f \equiv_{m_i} a_i \; \forall \; i$. Such an f is unique up to multiples of $m_1 m_2 \ldots m_d$.*

Proof. Firstly, we find $e_i(x) \; \forall \; i$ such that $e_i(x) \equiv_{m_i} 1$ and $e_i(x) \equiv_{m_j} 0 \; \forall \; i \neq j$. This can be done as follows : Firstly, let $e_i(x) = f_i(x)\Pi_{j \neq i} m_j(x)$. Since $gcd(m_i, \Pi_{j \neq i} m_j) = 1$, by Bezout's identity we can find such an f_i and hence e_i. Now let $f = \sum_i a_i e_i$. Then $f \equiv_m a_i$. If g is any other solution, then $g - f \equiv_{m_i} 0$. By coprimeness and induction one can easily prove that $g - f$ is a multiple of $m_1 m_2 \ldots m_d$. □

Applying the remainder theorem and the Chinese remainder theorem, we see the following corollary.

Theorem 3. *If $n_0, n_1 \ldots, n_d$ are distinct elements of $\mathbb{F}$ and $s_0, \ldots s_d$ are arbitrary elements of $\mathbb{F}$, there exists a unique $q \in \mathbb{F}[x]$ of degree $\leq d$ such that $q(n_i) = s_i$.*

This theorem is called the Lagrange Interpolation theorem. We can in fact give an explicit formula for q. This formula comes from an explicit formula for $e_i(x)$ such that $e_i(n_i) = 1, e_i(n_j) = 0 \ \forall \ i \neq j$. Let $g(x) = (x - n_0)(x - n_1) \ldots (x - n_j)$ and $g_i(x) = \frac{g(x)}{x - n_i}$. Note that $g_i(n_j) = 0 \ \forall \ i \neq j$. It is easy to see that $e_i(x) = \frac{g_i(x)}{g_i(n_i)}$ does the job (and has degree $\leq d$). The Chinese Remainder theorem tells us that $q = \sum s_i e_i$ is the unique polynomial of degree $\leq d$ that interpolates. A nice way of writing g_i is as follows : Since $g'(n_i) = (n_i - n_0) \ldots (n_i - n_{i-1})(n_i - n_{i+1}) = g(n_i)$, $e_i(x) = \frac{g_i(x)}{g'(n_i)}$.

3 The fundamental theorem of algebra and algebraic numbers

Note that $x + a = 0$ where $a > 0 \in \mathbb{N}$ can be solved in $\mathbb{Z}$ but not in $\mathbb{N}$. However, if $a \in \mathbb{Z}$, it continues to have a solution in $\mathbb{Z}$. Likewise, $ax + b = 0$ can be solved only in $\mathbb{Q}$. However, $x^2 = 2$ cannot be solved in $\mathbb{Q}$. One can invent the real numbers $\mathbb{R}$ (the crucial point being the least upper bound property) to solve this equation. Unfortunately, $x^2 + 1 = 0$ cannot be solved in real numbers and so we invent $\mathbb{C}$.

The usual definition of $\mathbb{C}$ notwithstanding, here is another one : Consider the polynomials $\mathbb{R}[x]$. We want to morally substitute $x = \sqrt{-1}$. So x^2 should be replaced by -1 everywhere. One way to achieve this is as follows : Define an equivalence relation on $\mathbb{R}[x]$ as $p(x) \equiv q(x)$ if $p(x) = q(x) + h(x)(x^2 + 1)$ for some $h(x) \in \mathbb{R}[x]$. It is easy to see that this is an equivalence relation. The set of equivalence classes is denoted as $\mathbb{C}$ and it equals $\{[a + bx]\}$ where $a, b \in \mathbb{R}$. Addition and multiplication are inherited from $\mathbb{R}[x]$. It is not hard to prove that the resulting object is a field isomorphic to our usual definition of $\mathbb{C}$.

What about other polynomial equations with $\mathbb{C}$ coefficients ?

Theorem 4. *Every degree-n polynomial in $\mathbb{C}[x]$ has exactly n complex roots (counted with multiplicity)*

This so-called Fundamental Theorem of Algebra is not at all easy to prove. The fastest way to do this is by using complex analysis (or at least power series). Here is a definition : An algebraic number is a complex number satisfying a polynomial with rational coefficients. The set of algebraic numbers is countable whereas complex numbers are uncountable (and so are reals). So most real numbers and complex numbers are not algebraic. They are "transcendental". Here is a concrete example of a transcendental number. Concrete examples of transcendental numbers are produced by the following theorem (actually a special case of the theorem is stated here) : Lindemann-Weierstrass theorem (proof on Wikipedia).

Theorem 5. *If $x \neq 0$ is algebraic then e^x is transcendental.*

So, $e, \pi, e^{\sqrt{2}}, \ldots$ are transcendental.

4 Symmetric polynomials

The next order of business is to actually find formulae to find the roots of polynomials. Before that, we need an important theorem in the theory of polynomials. Firstly, here is the definition of a symmetric polynomial : A polynomial $p(x_1, x_2, \ldots, x_n) \in R[x_1, x_2 \ldots, x_n]$ where R is a commutative ring is called a symmetric polynomial if $p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots) = p(x_1, \ldots, x_n)\ \forall\ \sigma \in S_n$. For example,

1. $e_1(X) = \sum_i X_i$, $e_2(X) = \sum_{i<j} X_i X_j$, etc. Basically, coefficients of $(X - X_1)(X - X_2) \ldots (X - X_n)$ are symmetric polynomials. These polynomials $e_k(X)$ are called the elementary symmetric polynomials (and there are n of them).