Math 115. Slides from the Lecture of October 3

This handout contains the slides from the lecture of October 3.

§ 2.7. Prime Modulus

The first sentence of Section 2.7 reads,

> "We have now reduced the problem of solving $f(x) \equiv 0 \pmod{m}$ to its last stage, congruences with prime moduli."

Well, not quite ... (what if $f'(a) \equiv 0 \pmod{p}$?).
But, we proceed.
We'll start by reviewing some facts about polynomials with coefficients in $\mathbb{C}$ or $\mathbb{R}$.

Polynomials with Coefficients in $\mathbb{C}$

The main line of today's class will mimic the following statements and proofs for polynomials with coefficients in $\mathbb{C}$ (or $\mathbb{R}$ or $\mathbb{Q}$).

Definition. $\mathbb{C}[x]$ is the set of polynomials with coefficients in $\mathbb{C}$. $\mathbb{R}[x]$ and $\mathbb{Q}[x]$ are defined analogously.

We prove here that a nonzero polynomial in $\mathbb{C}[x]$ of degree n has at most n roots (in $\mathbb{C}$). (In fact, it has exactly n roots, when counted with multiplicities, but this is not true for congruences modulo p. For example the congruence $x^2 \equiv -1 \pmod 3$ has degree 2, but no solutions.)
For the rest of today's class, we will use the convention that the zero polynomial in $\mathbb{C}[x]$ or $\mathbb{Z}[x]$, etc. has degree $-\infty$.

Theorem (Division Algorithm for Polynomials in $\mathbb{C}[x]$). *Let $f, g \in \mathbb{C}[x]$ with $g \ne 0$. Then there are polynomials $q, r \in \mathbb{C}[x]$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg r < \deg g$. Moreover, q and r are unique with these properties.*

Proof. Existence holds by long division of polynomials.
For uniqueness, suppose that

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$

with $\deg r_1 < \deg g$ and $\deg r_2 < \deg g$. If $q_1 \ne q_2$ then

$$r_2 - r_1 = -(q_1 - q_2)g ,$$

with $q_1 - q_2 \ne 0$. Then the right-hand side has degree $\ge \deg g$, but the left-hand side has degree $< \deg g$, a contradiction. So $q_1 = q_2$, and it then follows that $r_1 = r_2$. □

Corollary. *Let* $f \in \mathbb{C}[x]$ *and* $a \in \mathbb{C}$*. Then* a *is a root of* f *(i.e.,* $f(a) = 0$ *) if and only if* $(x-a) \mid f$ *(i.e.,* $f(x) = (x-a)g(x)$ *for some* $g \in \mathbb{C}[x]$ *).*

Proof. Write $f(x) = (x-a)g(x) + r(x)$ with $\deg r < 1$. Then r is a constant c (which may be zero). Substituting $x = a$ gives $f(a) = (a-a)g(a) + c = c$ (because $a - a = 0$), so $f(a) = c$. Therefore

$$f(a) = 0 \iff c = 0 \iff f(x) = (x-a)g(x) \iff (x-a) \mid f\ . \qquad \square$$

Corollary. *If* $f \in \mathbb{C}[x]$ *and* $a_1, \dots, a_r \in \mathbb{C}$ *are distinct roots of* f *(with* $r > 0$ *), then writing* $f(x) = (x - a_1)g(x)$ *, we have that* $a_2, \dots, a_r$ *are distinct roots of* g *.*

Proof. Exercise. □

Polynomials and Congruences Modulo p

Throughout the rest of today's class, p is a prime number.

We'll start by showing that a congruence modulo p of degree d can have at most d solutions, by mimicking what was done above for polynomials in $\mathbb{C}$.

Notes:

(1). For all nonzero $z \in \mathbb{C}$ there is a number $z^{-1} \in \mathbb{C}$ such that $zz^{-1} = 1$.

(2). For all $a \in \mathbb{Z}$ such that $a \not\equiv 0 \pmod{p}$ there is a number $a^{-1} \in \mathbb{Z}$ such that $aa^{-1} \equiv 1 \pmod{p}$.

Both are unique (up to congruence modulo p in the case of (2)).

Some Definitions

Definition. Let $f \in \mathbb{Z}[x]$ and let $m \in \mathbb{Z}_{>0}$. Then a **root of** f **modulo** m is an integer a such that $f(a) \equiv 0 \pmod{m}$ (i.e., a solution of the congruence).

Definition. A polynomial in $\mathbb{C}[x]$ (or $\mathbb{Z}[x]$) is **monic** if (it is nonzero and) its leading coefficient is 1.

Theorem (Division Algorithm in $\mathbb{Z}[x]$). *Let* $f, g \in \mathbb{Z}[x]$ *, and assume that* g *is monic. Then there are polynomials* $q, r \in \mathbb{Z}[x]$ *such that*

$$f(x) = q(x)g(x) + r(x) \qquad \text{and} \qquad \deg r < \deg g\ .$$

Moreover, q *and* r *are unique with these properties.*

Proof. Again, existence holds by long division (the only division of integers that occurs is division by the leading coefficient of g, which is possible in $\mathbb{Z}$).

Uniqueness holds by the same proof as before. □

Corollary. *Let* $f \in \mathbb{Z}[x]$ *and* $a \in \mathbb{Z}$*. Write* $f(x) = (x-a)g(x) + c$ *for some* $g \in \mathbb{Z}[x]$ *and* $c \in \mathbb{Z}$*. Then* $c = f(a)$*. In particular, for any* $m \in \mathbb{Z}_{>0}$ *, an integer* a *is a root of* f *modulo* m *if and only if* $f(x) \equiv (x-a)g(x) \pmod{m}$*.*

Proof. As before, we can write $f(x) = (x-a)g(x) + r(x)$ with $g, r \in \mathbb{Z}[x]$ and $\deg r < 1$. Since r has degree ≤ 0, it equals a constant $c \in \mathbb{Z}$, so $f(a) = c$ and therefore

$$\begin{aligned} a \text{ is a root of } f \text{ modulo } m &\iff f(a) \equiv 0 \pmod{m} \\ &\iff c \equiv 0 \pmod{m} \\ &\iff f(x) \equiv (x-a)g(x) \pmod{m} . \end{aligned}$$

□