Math 320 April 21, 2020

Congruence in $F[x]$

F ← field

Last time: $f(x), g(x), p(x) \in F[x]$, w/ $p(x) \neq 0_F$.

We say $f(x)$ is congruent to $g(x)$ modulo $p(x)$ if $p(x) \mid (f(x) - g(x))$

Write this as $f(x) \equiv g(x) \bmod p(x)$

- Pretty much exactly the same as the integer definition.

Examples: ($f(x)$)

(1) $3x^4 + x^3 \equiv \underbrace{12x^2 + 4x}_{g(x)} \bmod \underbrace{(3x^2 + 6)}_{p(x)}$ in $\mathbb{Q}[x]$.

Why?

$$f(x) - g(x) = 3x^4 + x^3 - 12x^2 - 4x$$

$$= (x^2 - 4)(3x^2 + x)$$

$$= (x^2 - 4)\, p(x)$$

$\Rightarrow p(x) \mid f(x) - g(x)$, so $f(x) \equiv g(x) \bmod p(x)$

(2) $\overbrace{x^2 + 4x}^{f(x)} \equiv \underbrace{x - 1}_{g(x)} \bmod \underbrace{(2x + 3)}_{p(x)}$ in $\mathbb{Z}_5[x]$

Why?

$$f(x) - g(x) = x^2 + 4x - x + 1$$

$$= x^2 + 3x + 1$$

$$= (3x + 2)(2x + 3)$$

$$= (3x + 2)\, p(x)$$

$\Rightarrow p(x) \mid (f(x) - g(x))$, so $f(x) \equiv g(x) \bmod p(x)$.

Thm 5.1: Let $p(x) \in F[x]$ be nonzero. Then congruence mod $p(x)$ satisfies:

(1) $f(x) \equiv f(x) \bmod p(x)$ (reflexive)

(2) If $f(x) \equiv g(x) \bmod p(x)$, then $g(x) \equiv f(x) \bmod p(x)$ (symmetric)

(3) If $f(x) \equiv g(x) \bmod p(x)$ and $g(x) \equiv h(x) \bmod p(x)$, then $f(x) \equiv h(x) \bmod p(x)$ (transitive)

Pf of 3:

$$f(x) - h(x) = f(x) - g(x) + g(x) - h(x)$$
$$= (f(x) - g(x)) + (g(x) - h(x))$$

We know $p(x) \mid f(x) - g(x)$ and $p(x) \mid g(x) - h(x)$, which implies

$$p(x) \mid ((f(x) - g(x)) + (g(x) - h(x))) = f(x) - h(x). \blacksquare$$

Thm 5.2: $p(x) \in F[x]$ nonzero. If $f(x) \equiv g(x) \bmod p(x)$ and $h(x) \equiv k(x) \bmod p(x)$, then

(i) $(f(x) + h(x)) \equiv (g(x) + k(x)) \bmod p(x)$

(ii) $f(x)\,h(x) \equiv g(x)\,k(x) \bmod p(x)$

Pf: same as thm 2.2. Replace integers with polynomials.

Def: Let $f(x), p(x) \in F[x]$, $p(x) \neq 0_F$. The congruence (or residue) class of $f(x) \bmod p(x)$, denoted $[f(x)]$, is the set consisting of all polynomials in $F[x]$ congruent to $f(x) \bmod p(x)$.

This is similar to the integer version of congruence classes.

$$[f(x)] = \{ g(x) \in F[x] : f(x) \equiv g(x) \bmod p(x) \}$$

$$= \{ g(x) : p(x) \mid (f(x) - g(x)) \}$$

$$= \{ g(x) : f(x) - g(x) = p(x) k(x) \text{ f.s. } k(x) \in F[x] \}$$

$$= \{ f(x) + p(x) h(x) : h(x) \in F[x] \}$$

If $f(x) \equiv g(x) \bmod p(x)$, then

$$f(x) - g(x) = p(x) k(x)$$

so $$g(x) = f(x) - p(x) k(x)$$

$$= \boxed{f(x) + p(x) h(x)}$$

(where $h(x) = -k(x)$).

So, every poly congruent to $f(x)$ mod $p(x)$ is of the form

$$f(x) + p(x) h(x).$$

Compare to integer version:

$$[a]_n = \{ a + kn : k \in \mathbb{Z} \}$$

★ Thm 5.3: $f(x) \equiv g(x) \bmod p(x)$ if and only if $[f(x)] = [g(x)]$.

↑ ↗

classes mod $p(x)$.

Pf: Take proof of thm 2.3 and replace the integers with polys.

Tip: To show $[f(x)] = [g(x)]$, show that $f(x) \equiv g(x) \bmod p(x)$.

That means: show $p(x) \mid (f(x) - g(x))$.

Ex:

(1) $[3x^4 + x^3] = [12x^2 + 4x]$

mod $3x^2 + x$, because

$3x^4 + x^3 \equiv 12x^2 + 4x \bmod 3x^2 + x$

(2) Consider congruence mod x^2-2.

Then, $[x^2] = [2]$

because $x^2 \equiv 2 \bmod x^2-2$,

since $x^2-2 \mid x^2-2$.

In general, if we consider congruence mod $x^2 - a$, $a \in \mathbb{Z}$, then

(1) $[x^2-a] = [0]$

(2) $[x^2] = [a]$

Also, in congruence mod $p(x)$,

$[p(x)] = [0_F]$

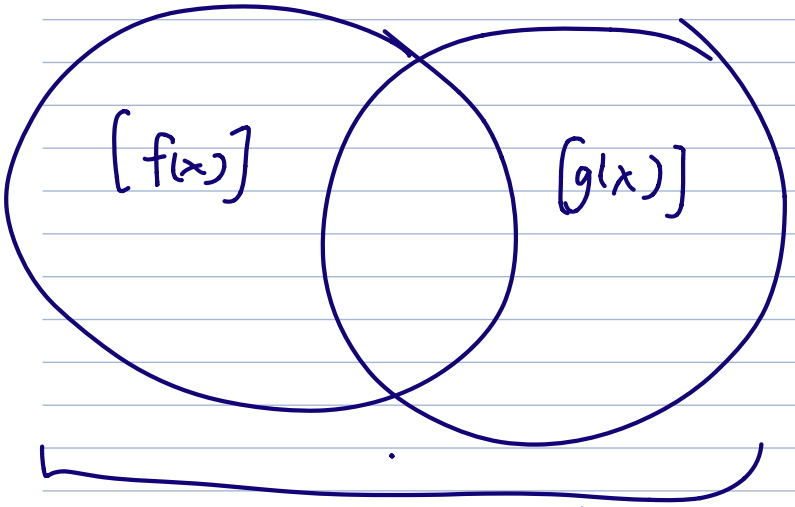
Just like in congruence mod an integer n,

$[n] = [0]$.

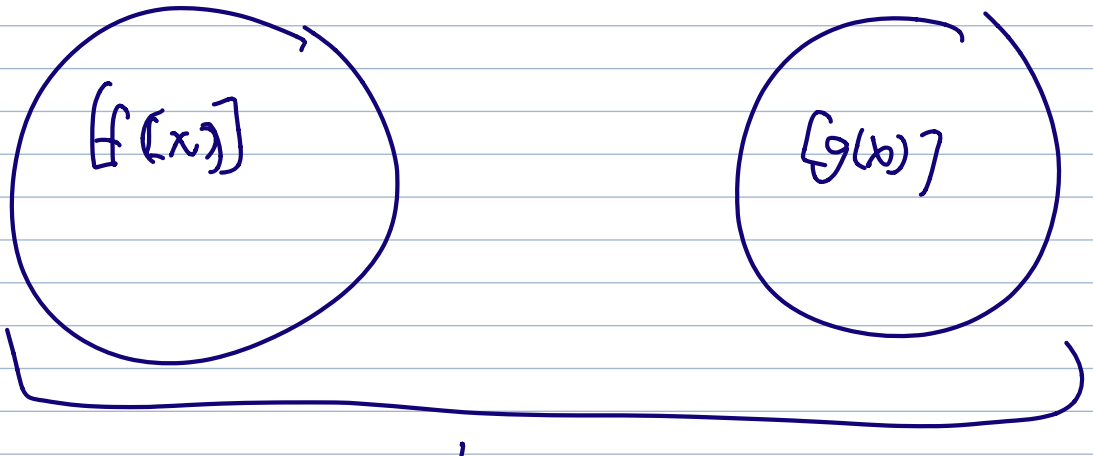
Cor 5.4: Two congruence classes mod $p(x)$ are either disjoint or identical.

So, if you can show that two classes share a single element, then they must be the same class.

In pictures:



not allowed



ok

Congruence classes of an integer n:

$$\mathbb{Z}_n = \underbrace{\{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}}_{n \text{ distinct classes}}$$

So fairly simple when modding by an integer.

It's more complicated with polynomials:

Cor 5.5: F is a field and $p(x) \in F[x]$ with $\deg p(x) = n$.

(1) If $f(x) \in F[x]$ and $r(x)$ is the remainder when $f(x)$ is divided by $p(x)$, then $[f(x)] = [r(x)]$.

(2) Let S be the set consisting of the zero poly and all polys of degree less than n.

Then, every congruence class mod $p(x)$

is the class of some poly in S. Also, the congruence classes of different polys in S are different.

Pf: (1) We have, by the Division Alg,

$$f(x) = q(x) \cdot p(x) + r(x)$$

Then, $f(x) - r(x) = q(x) \cdot p(x)$

$\Rightarrow p(x) \mid (f(x) - r(x))$

$\Rightarrow f(x) \equiv r(x) \mod p(x)$

$\Rightarrow [f(x)] = [r(x)]$

(2) $S = \{$ 0, and all polys of degree $< n\}$

↖ deg $p(x)$.

first thing we want to show:

If $[f(x)] \mod p(x)$, we want to show that $[f(x)] = [u(x)]$, where $u(x) \in S$. To do this, we use part 1:

Let $f(x) \in F[x]$. By the Division

Algorithm,

$f(x) = q(x) \cdot p(x) + r(x)$ where

$r(x) = 0_F$ or $0 \le \deg r(x) < \deg p(x)$

$0 \le \deg r(x) < n$

This means $r(x) \in S$.

By (1), $[f(x)] = [r(x)]$.

Since $f(x)$ is arbitrary, this shows that every class mod $p(x)$ can be represented by a poly in S.

We've shown:

Congruence class mod $p(x)$ are of the form $[r(x)]$, where

either $r(x) = 0_F$ or $\deg r(x) < n$.

Now, suppose $r_1(x), r_2(x) \in S$, and $r_1(x) \neq r_2(x)$. We want to show that $[r_1(x)] \neq [r_2(x)]$.

To do, this, note that $r_1(x) - r_2(x) \neq 0_F$.

Also, since $r_1(x), r_2(x) \in S$,

$\deg(r_1(x) - r_2(x)) < n$.

Since $\deg p(x) = n$, this means

$p(x) \nmid (r_1(x) - r_2(x))$

$\Rightarrow r_1(x) \not\equiv r_2(x) \mod p(x)$

$\Rightarrow [r_1(x)] \neq [r_2(x)]$

So, if $r_1(x)$, $r_2(x)$ are distinct elements of S, then $[r_1(x)]$, $[r_2(x)]$ are distinct congruence classes. ▨

Example: (1) Consider congruence classes mod $x^2 - 2$ in $\mathbb{Q}[x]$.

$\deg(x^2 - 2) = 2$.

So, the set of congruence classes mod $x^2 - 2$ are of the form:

$[ax + b]$ where $a, b \in \mathbb{Q}$.

$[0]$, $[1]$, $[x]$, $[x+1]$, $[3x + \frac{1}{2}]$,

$[53x - \frac{102}{7}]$

(2) Now, consider classes mod x^2+1 in $\mathbb{Z}_2[x]$. Again, $\deg(x^2+1) = 2$. So, its cong. classes are of the form

$$[ax+b], \quad a, b \in \mathbb{Z}_2$$

Possible classes:

$[0]$, $[1]$, $[x]$, $[x+1]$

This is it, since these are the only polys of degree <2.

So,

(# of cong classes mod $p(x)$)

$=$

(# of polys in $F[x]$ of deg $<$ deg $p(x)$)

If F is infinite, then there will be infinitely many classes mod $p(x)$

- If F is finite, then there will be finitely many classes.

In particular, if we consider classes mod $p(x)$ in $\mathbb{Z}_q[x]$ and $\deg p(x) = n$, then

> # of classes mod $p(x)$ $= q^n$.

(3) $p(x) = x^3 + 3x^2 + 1$ in $\mathbb{Q}[x]$, so $\deg p(x) = 3$.

Then its congruence classes will be of the form

$$[ax^2 + bx + c] \quad ; a, b, c \in \mathbb{Q}.$$

$[1]$, $[x]$, (x), $[x^2+1]$, $\left[x^2 + 3x + \frac{32}{5}\right]$, ---

- for integers, the set of congruence classes mod n is denoted by $\mathbb{Z}_n$.
- the set of congruence classes mod $p(x) \in F[x]$ is denoted:

$$F[x]/(p(x))$$

"F adjoin x mod p(x)"

- So first example was $\mathbb{Q}[x]/(x^2-2)$
- 2nd example: $\mathbb{Z}_2[x]/(x^2+1)$
- 3rd example: $\mathbb{Q}[x]/(x^3+3x^2+1)$

One more example: what are the elements of

$$\mathbb{Z}_3[x]/(x^3+2) \; ?$$

(x^3+2 ↖ $p(x)$)

$\deg(x^3+2)=3$, so the classes are of the form

$$[ax^2+bx+c]; \quad a,b,c \in \mathbb{Z}_3$$

Some classes:

$[0], [1], [2], [x], [x^2+2],$

$[x^2+x+2], \ldots$

Since $|\mathbb{Z}_3| = 3$,

# of coeff.

$$\left| \frac{\mathbb{Z}_3[x]}{(x^3+2)} \right| = 3 \cdot 3 \cdot 3 = 3^3 = 27$$

↑ # of choices per coeff.