Math 320 April 16, 2020

Last time: showing polynomials in $\mathbb{Q}[x]$ are (ir)reducible

Summary of methods for proving polynomials are irreducible:

(1) Check for roots
- if $\deg f(x) = 2$ or 3, then this is enough to test for reducibility
- for $\mathbb{Q}[x]$: rational root test is useful.
    - best used when constant/leading terms are 1 or prime.

If polynomial has higher degree, need other methods:

(1) directly check for divisors
- Ex: for $f(x)$ being degree-4, consider the equation

$$f(x) = (ax^2 + bx + c)(dx^2 + ex + f)$$

see if we can find a, b, c, d, e, f
that solve this equation
- if solution exists: reducible
- if not: irreducible
- note: if dealing with $\mathbb{Q}[x]$, we may assume all of these coefficients are integers.

(2) Eisenstein's criterion
- if $f(x) = a_n x^n + \cdots + a_1 x + a_0$, find prime p s.t. a_i's $\in \mathbb{Z}$
  (1) $p \nmid a_n$ (p doesn't divide leeding coefficient)

  (2) $p \mid a_0, a_1, \ldots, a_{n-1}$ (p divides other coefficients)

  (3) $p^2 \nmid a_0$ (p^2 doesn't divide constant term)
- if such a prime exists, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

- note: there's a general version of Eisenstein, but for now we may only use it for <u>integer coefficients</u>

(3) if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$, find prime p such that

(1) $p \nmid a_n$ (p doesn't divide leading coeff)

(2) the polynomial

$$\bar{f}(x) = [a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \dots + [a_1]_p x + [a_0]_p$$

is irreducible in $\mathbb{Z}_p[x]$

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

One last thing: prove Cor 4.19!

Let F be field, $f(x) \in F[x]$ has degree 2 or 3. Then, $f(x)$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in F.

Pf: "$\Longrightarrow$" If $f(x)$ is irreducible, then $f(x)$ has no roots

This is true in general (for polys of any degree) and we already proved this.

"$\Leftarrow$" "If $f(x)$ has no roots, then $f(x)$ is irreducible."

We'll prove the contrapositive:

"If $f(x)$ is reducible, then $f(x)$ has roots."

We have two cases:

(1) $\deg f(x) = 2$.

In this case, if $f(x)$ is reducible, then $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are nonconstant and have lower degree than $f(x)$.

Since $\deg f = 2$, this forces $\deg g, h = 1$, so

$$g(x) = ax+b, \quad h(x) = cx+d.$$

Then, $f(x)$ has roots $-ba^{-1}$ and $-dc^{-1}$:

$$f(x) = (ax+b)(cx+d)$$

(2) $\deg f(x) = 3$.

Again, if $f(x)$ is reducible then it factors into

$$f(x) = g(x)\,h(x)$$

where $g(x)$, $h(x)$ are nonconstant with lower degree than $f(x)$.

So $g(x)$, $h(x)$ must be degree 1 or 2.

They can't both be degree 2, since then $\deg[g(x)h(x)]$ would be 4.

So, one of $g(x)$ or $h(x)$ must have degree 1, say $g(x)$.

So, $g(x) = ax+b$, so

$$f(x) = (ax+b)\,h(x)$$

From here, we can see that $-ba^{-1}$ is a root of $f(x)$.

We've proved the contrapositive in both cases, so we have proved the original statement. $\blacksquare$

Chapter 5: Congruence in $F[x]$ and congruence Class Arithmetic.

This is the polynomial version of chapter.

As before, F will always denote a field.

Def: Let $f(x), g(x), p(x) \in F[x]$ with $p(x)$ nonzero. Then we say $f(x)$ is <u>congruent to $g(x)$ modulo $p(x)$</u> if $p(x) \mid (f(x) - g(x))$

we denote this by

$$f(x) \equiv g(x) \mod p(x).$$

Examples:

1) $x^2 - 1 \equiv 0 \mod (x-1)$ (in $\mathbb{Q}[x]$)

because $x^2 - 1 - 0 = x^2 - 1 = (x-1)(x+1)$

so $x-1 \mid (x^2-1-0)$

(2) $\underbrace{3x^4+2x^3+5}_{f(x)} \equiv \underbrace{2x^4+2x^3+9}_{g(x)} \mod (x^2-4)$ in $\mathbb{R}[x]$

Since

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

so $x^2-4 \mid (f(x)-g(x))$

(3) $\underbrace{(4x^5+x^4+2x^3+3x+1)}_{h(x)} \equiv \overbrace{2x^5+x^4-3x^3+1}^{k(x)}$ mod (x^2+1) in $\mathbb{Q}[x]$

$$h(x)-k(x) = (x^2+1)(2x^3+3x)$$

$$= 2x^5+5x^3+3x.$$