Math 320 April 14 2020

Irreducibility in $\mathbb{Q}[x]$.

We'll learn methods to prove polynomials in $\mathbb{Z}[x]$ are irreducible in $\mathbb{Q}[x]$

Thm 4.21 (Rational Root Test):
Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$.
If $r \neq 0$ and $r/s \in \mathbb{Q}$ is a root of $f(x)$, then:

$$r \mid a_0 \quad , \quad s \mid a_n$$

That is, the numerator divides the constant term and the denominator divides the leading coefficient.

Ex: $3x^2 + 4x + 8 = g(x)$

If $q = r/s$ is a rational root of $g(x)$, then $r \mid 8$ and $s \mid 3$.

This narrows down what the possible rational roots of a poly are.

In this case, the possible values of r and s are:

$$r = \pm 1, \pm 2, \pm 4, \pm 8$$

$$s = \pm 1, \pm 3$$

Ex: Check if the following poly is irreducible:

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

$\deg h(x) = 3$, so we can check for irreducibility by checking for roots.

The rational root test tells us there are only 4 possible roots:

$\pm 1, \pm 2$

$h(1) = 1 - 1 + 2 + 2 \neq 0$ X no root

$h(-1) = -1 - 1 - 2 + 2 \neq 0$ X no root

$h(2) = 8 + 2 + 4 + 2 \neq 0$ X no root

$h(-2) = -8 - 2 - 4 + 2 \neq 0$ X no root

We've checked all possible roots, and have shown $h(x)$ has none, and since $\deg h(x) = 3$, this implies $h(x)$ is irreducible in $\mathbb{Q}[x]$. (roots in $\mathbb{Q}[x]$)

Next theorem: reducible in $\mathbb{Q}[x]$ $\Leftrightarrow$ reducible in $\mathbb{Z}[x]$

Thm 4.23: Let $f(x)$ be a polynomial with integer coefficients. Then, $f(x)$ can be written as a product of polynomials with rational coefficients if and only if it can be written as a product of

polynomials with integer coefficients.

Use of this theorem: to show a poly. $f(x)$ is irreducible in $\mathbb{Q}[x]$, all we need to do is show it cannot be written as a product of polynomials with integer coefficients

Ex: Show $\underbrace{x^4 + 2x^3 + x + 1}_{f(x)}$ is irreducible in $\mathbb{Q}[x]$.

notice: $\deg f(x) = 4$.

need to show it has no factors of degree 1, 2, or 3.

First, check for roots: by the Rational Root Theorem, the only possible roots are ± 1.

$f(1) = 5 \neq 0$

$f(-1) = 1 - 2 - 1 + 1 = -1 \neq 0$

$\Rightarrow$ no roots.

first, note that no roots ⇒ no degree-1 factors.

Why? if $ax+b \mid f(x)$, then $-\frac{b}{a}$ is a root of $f(x)$.

But we just showed $f(x)$ has no roots.

★ In general, if $f(x)$ has no roots, then $f(x)$ has no degree-1 factors.

Since $f(x)$ is degree 4 and has no degree 1 factors, $f(x)$ has no degree 3 factors.

Why? if $h(x) \mid f(x)$ and $\deg h(x) = 3$, then $f(x) = h(x)k(x)$, and the degree of $k(x)$ must be 1, since:

$$4 = \deg f = \deg h(x) + \deg k(x) = 3 + \deg k(x)$$

We've shown: no degree 1 or

degree 3 factors.

In the future: if a degree 4 polynomial has no roots, then you may assume it has no degree 1 or degree 3 factors.

However, this leaves the possibility of degree 2 factors. That is, there may exist $a(x)$ such that $\deg a(x) = 2$ and $a(x) \mid f(x)$.

If this is true, then $\exists\, b(x)$ such that $f(x) = a(x)b(x)$, and $\deg b(x) = 2$.

both degree 2.

By theorem 23, we can assume that $a(x)$ and $b(x)$ have integer coefficients. This will make the next part easier.

We have

$$x^4 + 2x^3 + x + 1 = a(x) \cdot b(x)$$

We can assume $a(x)$, $b(x)$ are both monic degree-2 polys with integer coefficients.

So, $a(x) = x^2 + ux + v$

$b(x) = x^2 + cx + d$

where $u, v, c, d \in \mathbb{Z}$.

Expand:

$$x^4 + 2x^3 + x + 1 = (x^2 + ux + v)(x^2 + cx + d)$$

$$x^4 + 2x^3 + x + 1 = x^4 + (c+u)x^3 + (d + v + uc)x^2 + (ud + vc)x + vd$$

If such a factorization exists then the coefficients on both sides need to be equal, so

$u + u = 2$, $d + v + uc = 0$,

$ud + vc = 1$, $vd = 1$.

We want to show $f(x)$ is irreducible, so our goal is to show this system has no solution.

Remember, all of these terms are integers.

Since $vd = 1$, $v = d = 1$ or -1.

Plug this into the equation $ud + vc = 1$:

If $v = d = 1$, then

$$ud + vc = u + c = 1$$

If $v = d = -1$, then

$$ud + vc = -(u + c) = 1.$$

i.e. $u + c = -1$

Notice that we have $u + c = 2$.

In either case, we have $u + c$ equal to two different values, which is impossible.

So, this factorization doesn't exist

$\Rightarrow$ no degree 2 factors.

This shows $f(x)$ is irreducible.

Summary: $f(x)$ is degree 4 with integer coefficients. To show it's irreducible:

(1) Use rational root theorem to show $f(x)$ has no roots.

(2) Show $f(x) \neq a(x)b(x)$ where $a(x), b(x)$ are both degree 2 by showing the system of equations given by the coefficients has no solution.

Another example in book on pg 116.

Next Theorem: simple way to prove irreducibility in $\mathbb{Q}[x]$:

Thm 4.24 (Eisenstein's Criterion): Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients.

If there is a prime p such that

(1) p divides $a_{n-1}, a_{n-2}, \ldots, a_2, a_1, a_0$

(2) p does <u>not</u> divide the leading coefficient a_n

(3) p^2 does <u>not</u> divide the constant term.

then $f(x)$ is irreducible.

Examples:

(1) $x^4 - 16x^2 + 4x + 2$

By Eisenstein, with $p=2$, this is irreducible:

$2 \mid 2$, $2 \mid 4$, $2 \mid 16$, and $2 \nmid 1$

and $2^2 = 4 \nmid 2$.

(2) $3x^5 + 21x^4 + 343x^2 + 98x + 84$.

try $p=7$:

$21 = 3 \cdot 7$ ✓, $343 = 7^3$ ✓

$98 = 14 \cdot 7$ ✓, $84 = 12 \cdot 7$ ✓

also, $7 \nmid 3$, and $7^2 = 49 \nmid 84$ ✓

So, by Eisenstein with $p=7$, this

polynomial is irreducible.

(3) $14x^{3002} + 39x^{476} + 52x^{180} + 156$

Try $p = 13$.

$39 = 3 \cdot 13$ ✓, $52 = 4 \cdot 13$, ✓

$156 = 12 \cdot 13$ ✓

and $13 \nmid 14$ and $13^2 = 169 \nmid 156$.

So by Eisenstein with $p=13$, this poly is irreducible.

Warning: this only works with integer coefficients.

So if the coefficients are in $\mathbb{Z}_n$, do not use this.

However, if we have a polynomial with rational coefficients, we can do something to make the coefficients integers: factor out the denominators:

Ex: $\frac{1}{3}x^{18} + \frac{4}{7}x + \frac{2}{9} = a(x)$

$= \frac{1}{3}\cdot\frac{1}{7}\cdot\frac{1}{9}\left(7\cdot 9\,x^{18} + 4\cdot 3\cdot 9\,x + 2\cdot 3\cdot 7\right)$

$= \frac{1}{189}\left(\underbrace{63x^{18} + 108x + 42}_{b(x)}\right)$

Now, to check if the original poly is irreducible, we can just look at the "new" poly with integer coefficients.

$b(x)$ is irreducible by Eisenstein with $p=2$.

$a(x) = \frac{1}{189}\cdot b(x)$, so if $b(x)$ is irreducible, then so is $a(x)$.

Other "warnings"

(1) if you find a prime p such that $f(x)$ fails Eisenstein, this does <u>not</u> mean $f(x)$ is reducible

for example: $b(x)$ above fails with $q=7$, but succeeds with $p=2$.

(2) you can't always use Eisenstein, namely when the constant coefficient is 1. Actually, we can't use Eisenstein if any coeff. (besides the leading coeff.) is ± 1.

Thm 4.25: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a poly with integer coefficients and let p be a prime that does not divide a_n.

If

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

is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Ex:

(1) $f(x) = 7x^3 + 6x^2 + 4x + 6$

Let's consider this poly in $\mathbb{Z}_5[x]$:

$$\overline{f}(x) = 2x^3 + x^2 - x + 1$$

This is degree 3, so we can just check for roots in $\mathbb{Z}_5$:

$\bar{f}(0) = 1$, $\bar{f}(1) = 3$, $\bar{f}(2) = 11 = 1$

$\bar{f}(3) = \bar{f}(-2) = -9 = 1$

$\bar{f}(4) = \bar{f}(-1) = 1$.

$\bar{f}(x)$ has no roots in $\mathbb{Z}_5$, so it's irreducible in $\mathbb{Z}_5[x]$.

Therefore, by theorem 4.25, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Try on your own:

$$g(x) = 9x^4 + 4x^3 - 3x + 7$$

consider this poly in $\mathbb{Z}_2[x]$.