Office hours: same as last 2 weeks

Eliza M 3:30 – 5:30

Nick T 2:00 – 3:00

Eliza T 3:30 – 5:30

Last HW: due Monday after Thanksgiving.

Gauss's Lemma

$f \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$

example: $f = 6x^2 - x - 1$

roots are $1/2$ and $-1/3$

Prop: if $f = gh$ with $g, h \in \mathbb{Q}[x]$
then $f = \tilde{g}\tilde{h}$ with $\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$

and $\tilde{g} = \text{const} \cdot g$ $\quad \tilde{h} = \text{const} \cdot h$

$f = (3x - \frac{3}{2})(2x + \frac{2}{3})$

$g = 3x - 3/2$

$h = 2x + 2/3$

$\tilde{g} = \frac{2}{3} g = 2x - 1$

$\tilde{h} = \frac{3}{2} h = 3x + 1$

Proof: clear denominators to get

$g_1 = kg \in \mathbb{Z}[x]$

$h_1 = \ell h \in \mathbb{Z}[x]$

where $k, \ell \in \mathbb{Z}$

$k = 2$

$g_1 = 6x - 3$

(want: k divides h_1 and ℓ divides g_1 ...)

$\ell = 3$

$h_1 = 6x + 2$

Let p be a prime dividing $k \cdot \ell$

Then $p \mid g_1 \cdot h_1 = k \cdot \ell \cdot g \cdot h$

$k\ell = 6$

$p = 2$ (or 3)

$p \mid h_1$

[Claim: $p \mid g_1$ or $p \mid h_1$.

Have $k\ell \cdot g \cdot h = g_1 \cdot h_1$

cancel a factor of p from $k\ell$ and from <u>either</u> g_1 or h_1

and we stay in $\mathbb{Z}[x]$ — no denominators appear.

keep going, cancelling more factors of $k\ell$ till it's gone.

Example: $6x^2-x+1 = (3x-\frac{3}{2})(2x+\frac{2}{3})$

$$\cancel{6}\cdot(3x-\tfrac{3}{2})(2x+\tfrac{2}{3}) = (\cancel{6}^{\,2}x-\cancel{3}^{\,1})(\cancel{6}^{\,3}x+\cancel{2}^{\,1})$$

$\cancel{2}\cdot\cancel{3}$

Proof of the claim:
if $p \mid g_1h_1$ then $\overline{g_1h_1} = 0$ in $\mathbb{Z}_p[x]$

so $\bar{g}_1\bar{h}_1 = 0$ in $\mathbb{Z}_p[x]$

$\mathbb{Z}_p$ is a field $\rightsquigarrow$ $\mathbb{Z}_p[x]$ is an integral domain (i.e. no zero-divisors) ||

$\rightsquigarrow$ either $\bar{g}_1 = 0$ or $\bar{h}_1 = 0$
$\rightsquigarrow$ either $p \mid g_1$ or $p \mid h_1$.

Example: $(6x-3)(6x+2) = 36x^2-6x-6$ in $\mathbb{Z}[x]$

$$\downarrow$$

$\underline{(\bar{0}x+\bar{1})(\bar{0}x+\bar{0})} = \underline{\bar{0}x^2+\bar{0}x+\bar{0}}$ $\mathbb{Z}_2[x]$

$\boxed{\text{Q}}$

Eisenstein's Criterion

Example: $f = x^4 + 5x^3 + 10x^2 + 10x + 5 \in \mathbb{Z}[x]$

Coeffs: $1, 5, 10, 10, 5$

Take $p = 5$. $5 \nmid 1$ but $5 \mid 5, 10, 10, 5$

$5^2 \nmid 5$ ☆

Want to show that f is irreducible.

Suppose we could factor $f = g \cdot h$ where $g, h \in \mathbb{Z}[x]$
deg ≥ 1

pass to $\mathbb{Z}_5[x]$

then $\bar{f} = \boxed{x^4} \in \mathbb{Z}_5[x]$

and $\bar{f} = \bar{g}\bar{h}$.

$\mathbb{Z}_5$ is a field so $\mathbb{Z}_5[x]$ has unique factorization

so either $\bar{g} = x$ and $\bar{h} = x^3$
or $\bar{g} = x^2$ and $\bar{h} = x^2$
or $\bar{g} = x^3$ and $\bar{h} = x$

in any case: Const term of $\bar{g}$ is $\bar{0}$
so $5 \mid$ const. term of g

Sim. $5 \mid$ const term of h.

if $g = (x^m + \dots + c)$ and $h = (x^n + \dots + d)$
c: mult. of 5? d: mult. of 5?

then $f = g \cdot h = x^{m+n} + \dots + cd$.
cd: mult. of 25?!

but $25 \nmid 5$ so f did not factor after all.

Thm: let $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, and let p be a prime #.

If $p \nmid a_n$, $p \mid a_{n-1}, \ldots, a_0$, $p^2 \nmid a_0$ then f is irreducible. | use

Equiv:

If $p \nmid a_n$ and $p \mid a_{n-1}, \ldots, a_0$ and f is reducible then $p^2 \mid a_0$. | prove

Proof: f is reducible, so write

$$f = g \cdot h \qquad g, h \in \mathbb{Z}[x]$$

$$g = b_k x^k + \cdots + b_0 \qquad k \geq 1$$
$$h = c_\ell x^\ell + \cdots + c_0 \qquad \ell \geq 1 \qquad (k + \ell = n)$$

In $\mathbb{Z}_p[x]$, $\bar{f} = \bar{g}\bar{h}$

and also $\bar{f} = \bar{a}_n x^n$

so by unique factorization must have

$$\bar{g} = \bar{b}_k x^k \qquad \bar{h} \overset{!}{=} \bar{c}_\ell x^\ell$$

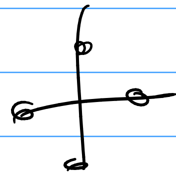
so $\bar{b}_0 = \bar{0}$ and $\bar{c}_0 = \bar{0}$ in $\mathbb{Z}_p$

so $p \mid b_0$ and $p \mid c_0$ so $p^2 \mid b_0 c_0 = a_0$ $\square$

Cyclotomic Polynomials / Roots of Unity.

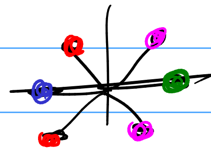
4^{th} roots of 1 are the roots of

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



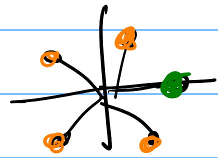
6^{th} roots:

$$x^6-1 = \underline{(x-1)}\,\underline{(x+1)}\,\underline{(x^2+x+1)}\,\underline{(x^2-x+1)}$$



5^{th} roots:

$$x^5-1 = (\underline{x-1})\,\underbrace{(x^4+x^3+x^2+x+1)}_{f(x)}$$



does this factor any further?

Eisenstein: no. sub $x \rightsquigarrow x+1$

$$(x+1)^5-1 = x\cdot f(x+1)$$

$$\|$$

$$(x^{\cancel{5}\,4}+5x^{\cancel{4}\,3}+10x^{\cancel{3}\,2}+10x^{\cancel{2}\,1}+5\cancel{x}\cancel{+1})\cancel{-1} = \cancel{x}\cdot f(x+1)$$

↑ Eisenstein applies here because $p \mid \binom{p}{k}$ $1\le k\le p-1$

Same trick works for p^{th} roots of 1 $\quad p^2 \nmid p$

$\forall$ prime p.