Office hours: same as last 2 weeks
Elia M 3:30 - 5:30
Nick T 2:00 - 3:00
Elia T 3:30 - 5:30

Last HW: due Monday after Thanksgiving.

Gauss’s Lemma

\[ f \in \mathbb{F}[x] \Rightarrow g \in \mathbb{F}[x] \]

Example: \[ f = 6x^2 - x - 1 \]

Roots are \( \frac{1}{2} \) and \( -\frac{1}{3} \)

Prop: if \( f = gh \) with \( g, h \in \mathbb{F}[x] \)
then \( f = \tilde{g} \tilde{h} \) with \( \tilde{g}, \tilde{h} \in \mathbb{F}[x] \)

and \( \tilde{g} = \text{cont.} \cdot g = \text{const.} \cdot h \)

Proof: clear denominators to get

\[ \tilde{g} = 3g = 2x - 1 \]
\[ \tilde{h} = 2h = 3x + 1 \]

where \( k, l \in \mathbb{F} \)

(want: \( k \) divides \( h \), and \( l \) divides \( g \), ...)

Let \( p \) be a prime dividing \( k \cdot l \)

Then \( pl \mid g \cdot h \Rightarrow k \cdot l \mid g \cdot h \)

Claim: \( pl \mid g \) or \( pl \mid h \)

Have \( kl \cdot g \cdot h = g \cdot h \).
cancel a factor of \( p \) from \( k \) and from either \( g \), or \( h \),

and we stay in \( \mathbb{Z}[k] \) — no denominators appear.

keep going, cancelling more factors of \( k \) till it's gone.

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

\[
6 \cdot (3x-\frac{3}{2})(2x+\frac{2}{3}) = (\frac{\sqrt{2}}{3}x-\frac{\sqrt{2}}{3})(\sqrt{2}x+\frac{\sqrt{2}}{3})
\]

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

\[
(\overline{6}_2x-\overline{3}_2)(\overline{6}_2x+\overline{2}_2) = \overline{6}_2x^2 + \overline{\delta}_2x + \overline{\delta}_2 \in \mathbb{Z}_2[x]
\]
Eisenstein's Criterion

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

Coeffs: \( 1, 5, 10, 10, 5 \)

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

\[ 5^2 \nmid 5 \]

Want to show that \( f \) is irreducible.

Suppose we could factor \( f = g \cdot h \) where \( g, h \in \mathbb{Z}[x] \)

\( \deg g \geq 1 \)

pass to \( \mathbb{F}_5[x] \)

then \( \overline{f} = \overline{x^4} \in \mathbb{F}_5[x] \)

and \( \overline{f} = \overline{g} \cdot \overline{h} \).

\( \mathbb{F}_5 \) is a field so \( \mathbb{F}_5[x] \) has unique factorization

so either \( \overline{g} = x \) and \( \overline{h} = x^3 \)

or \( \overline{g} = x^2 \) and \( \overline{h} = x^2 \)

or \( \overline{g} = x^3 \) and \( \overline{h} = x \)

in any case:

\( \begin{cases} \text{const term of } \overline{g} \text{ is } 0 & \text{so } 5 \nmid \text{const. term of } g \text{ and } \\ \text{sim. } 5 \nmid \text{const. term of } h. \end{cases} \)

if \( g = (x^n + \ldots + c) \) and \( h = (x^m + \ldots + d) \)

then \( f = g \cdot h = x^{m+n} + \ldots + cd \)

\( \text{mul. of } 5 \)?

\( \text{mul. of } 75 \)!

but \( 25 \nmid 5 \) so \( f \) did not factor after all.
Thus: let $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, and let $p$ be a prime.

If $p | a_n, \quad p | a_{n-1}, \quad \ldots \quad p | a_0$, then $p^2 | a_0$.

Hence $f$ is irreducible.

Equiv.

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

Proof: $f$ is reducible, so write

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

where

$$g = b_k x^k + \cdots + b_0, \quad k \geq 1$$
$$h = c_l x^l + \cdots + c_0, \quad l \geq 1 \quad (k + l = n)$$

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

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

so by unique factorization, $f$ must have

$$\bar{g} = \bar{b}_k x^k, \quad \bar{h} = \bar{c}_l x^l$$

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

so $p | b_0$ and $p | c_0$, so $p^2 | b_0 c_0 = a_0$.
Cyclotomic Polynomials / Roots of Unity.

4th roots of 1 are the roots of

\[ x^4 - 1 = (x - 1)(x + 1)(x^2 + 1) \]

6th roots:

\[ x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1) \]

5th roots:

\[ x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) \]

\[ \text{does this factor any further?} \]

Eisenstein: no. sub \( x \to x + 1 \)

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

\[ (x^4 + 5x^3 + 10x^2 + 10x + 5 - 1) = x \cdot f(x + 1) \]

\[ \text{Eisenstein applies here because } p \mid (p^5) \text{ if } 1 \leq k^2 + 1 \]

Same trick works for \( p^k \)th root of 1 

\[ p^2 \times p \text{ for prime } p \]