§1 Lecture 11-25

Lemma 1.1 (Gauss's Lemma)
Let $p \in \mathbb{Z}[x]$ be monic. Suppose p is reducible over $\mathbb{Q}$. So $p = \alpha\beta$ where $\alpha, \beta \in \mathbb{Q}[x]$ and $\deg(\beta), \deg(\alpha) \geq 1$.

Then $p = a \cdot b$ where $a, b \in \mathbb{Z}[x]$ and $\deg(a) = \deg(\alpha)$, $\deg(b) = \deg(\beta)$.

Corollary 1.2
Let $p \in \mathbb{Z}[x]$ where $p = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Suppose p has a zero in $\mathbb{Q}$. Then p has a zero $z \in \mathbb{Z}$. Moreover $z \mid a_0$.

Proof. If $p(z) = 0$, then $p(x) = q(x)(x - z)$. Hence $p(x) = a(x) \cdot b(x)$ where $\deg(b) = 1$ and $b \in \mathbb{Z}[[x]$. Hence $b = (x - z)$ for some $z \in \mathbb{Z}$ and $p(z) = q(z)b(z) = 0$. □

Often recognize irreducible deg 3 polynomials in $\mathbb{Q}[x]$. $x^2 + x + 1$ must be irreducible in $\mathbb{Q}[x]$. Since it has no $\mathbb{Q}$ zero, since no $\mathbb{Z}$ zero.

§1.1 Eisenstein's Criterion

Let p be prime. Let $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$.

Suppose p divides each a_i for $i < n$, p does not divide a_n, and p^2 does not divide a_0.

Example 1.3

$$7x^4 + 5x^3 + 10x^2 + 25x^1 + 5x^0$$

Show it is irreducible over $\mathbb{Q}$.

Under assumption f monic by Gauss's Lemma, it suffices to show that f is irreducible over $\mathbb{Z}$.

Suppose $f = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$. Note either $p \nmid b_0$ or $p \nmid c_0$ because $p^2 \nmid a_0 = b_0 c_0$.

Suppose $p \nmid b_0$, hence $p \mid c_0$.

Let m be the smallest such that $p \nmid c_m$.

Note $p \nmid c_s$ because $p \nmid a_n = b_r c_s$ so $m < s$.

Then $a_m = b_1 c_{m-1} + \cdots + b_m c_0$.

$p \mid a_m$ by hypothesis. $p \nmid b_0$, $b \nmid c_m$ and $p | c_{m-1} \cdots c_0$. So $P|$left but $\nmid$ right. Contradiction! □

For each $n \geq 1$, there is a homomorphism $\phi_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ induced by $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

$$\phi_n(f) = f \quad \text{with coefficients mod } n$$

Example 1.4

$$\underbrace{\phi_3(5x^3 + 4x + 7)}_{\in \mathbb{Z}[x]} = \underbrace{2x^3 + x + 1}_{\in \mathbb{Z}_3[x]}$$

Lemma 1.5
If $\phi_n(f)$ is irreducible in $\mathbb{Z}_n[x]$ (and $f \neq mf'$ for some $m \in \mathbb{Z}$), then f is irreducible in $\mathbb{Z}[x]$.

Proof. Indeed, if $f = g \cdot h$ in $\mathbb{Z}[x]$, then $\phi_n(f) = \phi_n(gh) = \phi_n(g)\phi_n(h)$. □

Example 1.6
$\mathbb{Q}[x]/\langle 5x^3 + 4x + 7\rangle$ is a field.
To compute $\gcd(f, g)$, $f, g \in \mathbb{F}[x]$, just apply Euclid's algorithm.

Example 1.7
$\gcd(x^3 + x + 1, x^2 + 2)$ in $\mathbb{Z}_3[x]$.

$$\begin{array}{r|l} & x \\ \hline x^2+2 & x^3 \quad + x + 1 \\ & -x^3 - 2x \\ \hline & -x + 1 \end{array}$$

$\gcd(x^2 + 2, 2x + 1) = 2x + 1$

$$\begin{array}{r|l} & \frac{1}{2}x - \frac{1}{4} \\ \hline 2x+1 & x^2 \qquad + 2 \\ & -x^2 - \frac{1}{2}x \\ \hline & -\frac{1}{2}x + 2 \\ & \frac{1}{2}x + \frac{1}{4} \\ \hline & \frac{9}{4} \end{array}$$