**Math 418H** **Fall 2005**

## Lecture: Wed 9/21/05

1. Gauss Lemma for primitive polynomials in $\mathbb{Z}[x]$

- Divisibility: $g(x) \mid f(x)$ in $\mathbb{Z}[x]$ means $f(x) = g(x)\,h(x)$ for some $h(x) \in \mathbb{Z}[x]$. We say $p(x)$ is *irreducible* in $\mathbb{Z}[x]$ if its only divisors are 1 and $p(x)$ (times $\pm 1$).
- A constant $n \in \mathbb{Z}$ divides $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ whenever $n \mid a_0, \ldots, a_n$. A constant $p \in \mathbb{Z}$ is irreducible in $\mathbb{Z}[x]$ whenever it is prime in $\mathbb{Z}$.
  These just restate the above in the case of constant polynomials.
- Primitive polynomial: $f(x) \in \mathbb{Z}[x]$ with $\gcd(a_0, a_1, \ldots, a_n) = 1$. That is, no integer $n$ divides $f(x)$ (except units $\pm 1$).
- *Lemma:* If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive, then the product $f(x)\,g(x)$ is also primitive.
- Equivalently: If $f(x)\,g(x)$ is not primitive, then $f(x)$ or $g(x)$ is not primitive. That is, if a prime $p \in \mathbb{Z}$ divides $f(x)\,g(x)$ in $\mathbb{Z}[x]$, then $p$ divides $f(x)$ or $g(x)$.
- *Proof:* Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$, and suppose $p$ divides the product:

$$f(x)\,g(x) = \sum_{k=0}^{n+m} c_k x^k = \sum_{k=0}^{n+m} \left( \sum_{i=0}^{k} a_i b_{k-i} \right) x^k .$$

  Assume we have: $p \mid a_0, a_1, \ldots, a_k$ and $p \mid b_0, b_1, \ldots, b_\ell$ for some $k < n$ and $\ell < m$. Either or both lists are allowed to be empty, containing no elements, in which case we have assumed *nothing.* Now we have:

$$c_{k+\ell+2} \;=\; \begin{array}{l} a_0 b_{k+\ell+2} + a_1 b_{k+\ell+1} + \cdots + a_k b_{\ell+2} \\ a_{k+\ell+2} b_0 + a_{k+\ell+1} b_1 + \cdots + a_{k+2} b_\ell \end{array} + a_{k+1} b_{\ell+1} \quad .$$

  By assumption, $p$ divides the lefthand side $c_{k+\ell+2}$, and $p$ divides all the terms on the righthand side except possibly $a_{k+1}b_{\ell+1}$. But then $p$ *must* divide the last term, and $p \mid a_{k+1}$ or $p \mid b_{\ell+1}$.

  Hence we can add one item ($a_{k+1}$ or $b_{\ell+1}$) to our list of coefficients divisible by $p$. We can keep repeating this argument and enlarging our list: the process will only end when $k = n$ or $\ell = m$, which means $p \mid f(x)$ or $p \mid g(x)$.

2. Factorization in $\mathbb{Z}[x]$ versus $\mathbb{Q}[x]$

   - *Gauss Lemma:* If a non-constant $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.
   - Equivalently: If $f(x) \in \mathbb{Z}[x]$ has non-trivial factors in $\mathbb{Q}[x]$, then it has non-trivial factors in $\mathbb{Z}[x]$.
   - *Proof:* Suppose $f(x) = g(x)h(x)$ with $f(x) \in \mathbb{Z}[x]$ and $g(x), h(x) \in \mathbb{Q}[x]$. We must find factors of $f(x)$ in $\mathbb{Z}[x]$. Let $f(x) = af_0(x)$, $g(x) = bg_0(x)$, $h(x) = ch_0(x)$, where $f_0, g_0, h_0 \in \mathbb{Z}[x]$ are primitive polynomials, and $a \in \mathbb{Z}$, $b, c \in \mathbb{Q}$.

     Then $\frac{a}{bc} f_0(x) = g_0(x)h_0(x)$, which is a primitive polynomial by Gauss' Lemma above. Thus both $f_0(x)$ and $\frac{a}{bc} f_0(x)$ are primitive integer polynomials, so we must have $a/bc = 1$ and $a = bc$. Thus $f(x) = bcg_0(x)h_0(x) = ag_0(x)h_0(x)$, with all factors in $\mathbb{Z}[x]$.

3. Unique factorization for $\mathbb{Z}[x]$

   - $\mathbb{Z}[x]$ has no possible division algorithm because $\gcd(2, x) = 1$, but $2n(x) + xm(x) \neq 1$ for any $n(x), m(x) \in \mathbb{Z}[x]$.
   - *Proposition:* Any integer polynomial factors into a product of irreducibles in $\mathbb{Z}[x]$, namely into prime constants and irreducible primititve polynomials, and this factorization is unique except for re-ordering and $\pm$ signs.
   - *Proof:* Suppose

     $$p_1 \cdots p_r \, f_1(x) \cdots f_u(x) = q_1 \cdots q_s \, g_1(x) \cdots g_v(x) \,,$$

     where $p_i, q_i \in \mathbb{Z}$ are prime constants and $f_i(x), g_i(x) \in \mathbb{Z}[x]$ are primitive irreducibles. Thus $f_i(x), g_i(x)$ are also irreducibles in $\mathbb{Q}[x]$ by the above Gauss Lemma on Factorization. By the Unique Factorization for $\mathbb{Q}[x]$ we may assume $f_i(x) = c_i g_i(x)$ for constants $c_i \in \mathbb{Q}^\times$. But since both $f_i(x)$ and $g_i(x)$ are primitive integer polynomials, we must have $c_i = \pm 1$. Factoring $f_i(x) = g_i(x)$ from both sides, we have $p_1 \cdots p_r = q_1 \cdots q_s$. By Unique Factorization for $\mathbb{Z}$, we may assume $p_i = \pm q_i$, so we are done.