Lecture 06

2/27/2012

Note Title 2/26/2012

Today

- Division in $R[x]$ in $O(n \text{ polylog } n)$ time
- GCD in $F[x]$

PreNotes for Division can be found in prenotes for LECTURE 04.
These notes only discuss GCD

Definition

GCD can be defined over any UFD R
(unique factorization domain)

- $a \in R$ is a unit if it has a multiplicative inverse.
- a divides b if $\exists c$ s.t. $a \cdot c = b$.
  $(a \mid b)$
- a irreducible if $b \cdot c = a \Rightarrow b$ is unit or c is unit.
- a associate of b $(a \sim b)$ if
  $\exists$ unit c s.t. $a = b \cdot c$
  [$\sim$ is an equivalence relation]
- R UFD if $a_1 \ldots a_k = b_1 \ldots b_l$ with a_i, b_i irreducible $\Rightarrow l = k$ & $\exists$ 1-1 π s.t. $a_i = b_{\pi(i)}$
- $g = GCD(a, b)$ if $h \mid a$ & $h \mid b \Rightarrow h \mid g$.

Proposition [Eq. Definition of GCD in $F[x]$]

$g = GCD(a,b)$ iff

1. $g \mid a$, $g \mid b$
2. $\exists\, u, v \in F[x]$ s.t.

$$g = u \cdot a + v \cdot b$$

Proof: (Sketched)

Let $I(a,b) = \{ \alpha \cdot a + \beta \cdot b \mid \alpha, \beta \in R \}$

("ideal": closed under addition & multiplication by R.)

1. $\forall\, h \in I(a,b)$, $g \mid h$
2. Let g' be lowest degree el't of I. Then $g' \mid a$, $g' \mid b$. (Else $a \bmod g'$ has smaller degree & is in I.)
3. Thus $g' \mid g$ & $g \mid g'$ ....
(Defn. of GCD)

Euclid's Algorithm

- Maintain pair of polynomials (a_i, b_i)
- Initially $(a_0, b_0) \leftarrow (a, b)$
  with $\deg(a_0) \geq \deg(b_0)$
- $a_{i+1} \leftarrow b_i$
  $b_{i+1} \leftarrow a_i \pmod{b_i}$
- Stop if $b_{i+1} = 0$; return (a_{i+1}).

Correctness : follows from Proposition

Running Time : $O(n^2)$

FAST GCD

Think of Euclid's alg as producing a series of matrices in $F[x]^{2\times 2}$

$M_1, M_2, \ldots$

$$\begin{pmatrix} a_i \\ b_i \end{pmatrix} = M_i \cdot \begin{pmatrix} a_{i-1} \\ b_{i-1} \end{pmatrix}$$

Let $N_i = M_1 \cdot M_2 \cdot M_3 \cdots M_i$

Main Idea: Compute N_i fast using only high degree parts of a, b.

Key Lemma:

$$a = c \cdot x^k + d$$
$$b = e \cdot x^k + f$$

Let $N_1, N_2 \ldots N_i \ldots$ be matrices for (a,b)

Let $L_1 \ldots L_i$ " (c,e)

$\deg(c_i, e_i) > \frac{\deg c}{2} \Rightarrow N_i = L_i$

$\boxtimes$