Lec16C Leading Coefficients and GCDs

March 11, 2021 1:15 PM

Hensel lifting to compute GCDs in $\mathbb{Z}[x]$

$$\begin{tikzcd}
\text{Input } a,b \in \mathbb{Z}[x] \\ \text{cont}(a)=\text{cont}(b)=1 \arrow[r] \arrow[d, "\phi_p"', "\substack{\text{(one prime)}\\ \alpha = lc(a) \\ p \nmid \alpha}"] & g = gcd(a,b).\quad a = g\cdot\bar{a} \\
a_p, b_p \in \mathbb{Z}_p[x] \arrow[r, "E.A."] & g_p = gcd(a_p, b_p) \text{ in } \mathbb{Z}_p[x] \arrow[u, "\substack{\text{check if } g \mid b.}"', "\substack{\text{Hensel lifting.}\\ p \text{ could be unlucky.}}"]
\end{tikzcd}$$

Let $a_p = g_p \cdot \bar{a}_p \Rightarrow a_p - \overset{u_0}{g_p}\cdot\overset{w_0}{\bar{a}_p} = 0 \bmod p$

$b_p = g_p \cdot \bar{b}_p \Rightarrow b_p - \underset{u_0}{g_p}\cdot\underset{w_0}{\bar{b}_p} = 0 \bmod p$

The requirement $gcd(u_0, w_0) = 1$.

Consider $a = (x+1)(x+2)^2(x+3)$ $\quad g = (x+1)(x+2)$

$b = (x+1)^2(x+2)\cdot(x+4)$ $\quad \bar{a} = (x+2)(x+3)$

$\bar{b} = (x+1)(x+4)$

Notice $gcd(g, \bar{a}) = x+2$ and $gcd(g, \bar{b}) = x+1 \Rightarrow gcd(u_0, w_0) \neq 1 \ \forall p.$

Fix: Set $a = a + \beta b$ for some $\beta \in \mathbb{Z}$ chosen randomly.

$\Rightarrow a = g\cdot(\bar{a} + \beta\cdot\bar{b})$

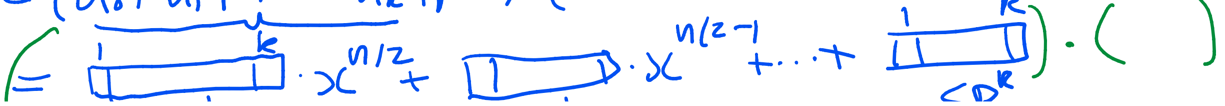
$\beta = 2$ $\quad a = \underbrace{(x+1)(x+2)}_{g}\left(\underset{\underset{3x^2+15x+14 \text{ (irreducible).}}{\shortparallel}}{(x+2)(x+3) + 2(x+1)(x+4)}\right)$

Cost of Hensel lifting to mod p^m

$deg(a) = n$, $deg\, u = deg\, w = n/2$

At the k'th step of H.L. we compute $e_k = a - u^{(k)}\cdot w^{(k)}$

$= a - (\underbrace{\overset{\overset{\mathbb{Z}_p[x]}{\Downarrow}}{u_0} + \overset{\overset{\mathbb{Z}_p[x]}{\Downarrow}}{u_1}\cdot p + \cdots + u_{k-1}p^{k-1}}) \cdot (w_0 + w_1\cdot p + \cdots + w_{k-1}p^{k-1})$



$$\left(= \underset{<p^k}{\boxed{1 \qquad\qquad k}} \cdot x^{n/2} + \underset{<p^k}{\boxed{1 \qquad\qquad}} \cdot x^{n/2-1} + \cdots + \underset{<p^k}{\boxed{1 \qquad\qquad k}} \right) \cdot (\qquad)$$

Mult. of $u^{(k)} \cdot w^{(k)}$ costs $(n/2+1)(\frac{n}{2}+1) \cdot O(k^2)$.

Cost of H.L. upto p^m is $\sum_{k=1}^{m} (\frac{n}{2}+1)^2 \cdot O(k^2) = (\frac{n}{2}+1)^2 \cdot O(\sum_{k=1}^{m} k^2)$

$$\sum_{k=1}^{m} k^2 = \frac{m(2m+1)(m+1)}{6} = \frac{1}{6}m^3 + \cdots \qquad = O(n^2 m^3).$$

In 1974 Miola and Yun reduced it to $O(\underline{n}^2 \underline{m}^2)$.

Idea: $a - (u^{(k-1)} + u_{k-1}p^{k-1})(w^{(k-1)} + w_{k-1}p^{k-1})$

$$= [a - \underbrace{u^{(k-1)} \cdot w^{(k-1)}}] - (u_k \cdot w^{(k-1)}, + w_k u^{(k-1)}] \cdot p^{k-1} - (u_{k-1} \cdot w_{k-1}) \underset{\uparrow}{p}^{2k}.$$

$\mathbb{Z}_p[x]$

e_{k-1}. !! Don't recompute e_{k-1}.

In 2018 I reduced it. to $O(n^2 m + n m^2)$.