Lecture 12A Analysis of the Modular GCD Algorithm Michael Monagan

February 25, 2021 1:52 PM

Assignment #3 is due on Monday @ 11pm.

Let $a,b \in \mathbb{Z}[x] \setminus \{0\}$, $\text{cont}(a)=1$, $\text{cont}(b)=1$. Compute $g=\gcd(a,b)$.

Let $a = \sum_{i=0}^{n-1} a_i x^i$ where $|a_i| < B^m$

and $b = \sum_{i=0}^{n-1} b_i x^i$ where $|b_i| < B^m$

$a = \boxed{a_{n-1}}\, x^{n-1} + \cdots + \boxed{a_0}$

$b = \boxed{b_{n-1}}\, x^{n-1} + \cdots + \boxed{b_0}$

$$\begin{tikzcd}
a,b \in \mathbb{Z}[x] \arrow[rr] \arrow[d, "① \phi_{p_i}"'] & & g=\gcd(a,b) \\
a_i,b_i \in \mathbb{Z}_{p_i}[x] \arrow[rr, "E.A. ②", "O(n^2)"'] & & g_i = \gcd(a_i,b_i) \in \mathbb{Z}_{p_i}[x] \arrow[u, "\text{Test:}"']
\end{tikzcd}$$

$\gamma = \gcd(lc(a), lc(b))$

$M = \prod p_i > 2\|g\|_\infty \cdot \gamma$

Test: if $\bar{g} | a$ and $\bar{g} | b$ ⑤ then output $\bar{g}$.

④ $\bar{g} \leftarrow pp(\bar{g})$

③ CRT $\bar{g} \in \mathbb{Z}_M[x]$

$g_i \leftarrow \underline{\gamma} \cdot g_i \quad O(n)$.

How many primes do we need?

?? Assume no unlucky primes ??

$\prod p_i > \underbrace{2\,\underline{\gamma}\,\|g\|_\infty}$

$\prod p_i > 2^n \sqrt{n}\, B^{2m}$

$$\left\{ \begin{array}{l} \|g\|_\infty < \overbrace{2^{n-1}\sqrt{n}\,\underline{\|a\|_\infty}}^{\text{Mignotte bound.}} < 2^{n-1}\sqrt{n}\, B^m \\ \gamma = \gcd(lc(a), lc(b)) < B^m \end{array} \right.$$

If $B < p < 2B$ then $\#\text{primes} \le \lceil \log_B 2^n \sqrt{n}\, B^{2m} \rceil$

Assume $\|g\|_\infty \le \|a\|_\infty$.

$= 2m + \underbrace{\log_B 2^{n} + \log_B \sqrt{n}}$ <1

$\le 2m$

① Cost of $\phi_{p_i}(a)$ & $\phi_{p_i}(b) \le 2m \cdot 2n \cdot O(m) = O(m^2 n)$.

$\overset{1 \quad\quad m}{\boxed{\cdots}} \div \overset{1}{\boxed{}} p_i$

# primes   \# coeffs in a & b

② Cost of gcds in $\mathbb{Z}_{p_i}[x] \le 2m \cdot O(n^2) = O(mn^2)$.

$\deg(a) = \deg(b) \le \underline{n-1}$

cost of mixed radix.

③ Cost of the CRT : $\le n \cdot O((2m)^2) = O(nm^2)$

deg $g \le n-1$.

g has $\le n$ coefficients.

Eucl Alg. in $\mathbb{Z}$

④ Cost of $\bar{g} \leftarrow pp(\bar{g})$ $\le (n-1)\, O((\underline{2m})^2) + n\, O((2m)^2) = O(nm^2)$

n−1 integer gcds

n divisions.

size $\le 2m \div \square$

⑤ Cost of $\bar{g}|a$ and $\bar{g}|b$: $2\,O(n^2m^2) = O(n^2m^2)$.

Modular $\div$ algorithm $\longrightarrow O(n^2m + m^2n)$.

Total ①+②+③+④ $= O(m^2n) + O(n^2m) + O(m^2n) + O(m^2n) = O(m^2n + n^2m)$