Lec9A Modular Multiplication Algorithm for Z[x]

10:45 PM

Modular Algorithms

Let $a, b \in \mathbb{Z}[x]$ and let $c = a \times b$.

How fast can we compute c?

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

(e.g. $B=10$)

$$a = \boxed{1 \quad\quad m} \cdot x^{n-1} + \boxed{\quad\quad} x^{n-2} + \cdots + \boxed{\quad\quad} x + \boxed{\quad\quad} \cdot x^0$$

$$b = \boxed{1 \quad\quad m} \cdot x^{n-1} + \boxed{\quad\quad} x^{n-2} + \cdots + \boxed{\quad\quad} x + \boxed{\quad\quad}$$

Classical poly $\times$: n^2 mults. in $\mathbb{Z}$.

+ Classical $\times$ in $\mathbb{Z}$: $n^2 O(m^2) = O(n^2 m^2) \overset{m=n}{=} O(n^4)$.
+ Karatsuba $\times$ in $\mathbb{Z}$: $n^2 O(m^{1.585})$
+ Karatsuba for poly : $O(n^{1.585}) O(m^{1.585}) \overset{m=n}{=} O(n^{3.17})$
+ <u>CRT</u> $\Rightarrow$ $O(mn^2 + m^2 n) \overset{n=m}{=} O(n^3)$.

Let $\phi_p : \mathbb{Z} \to \mathbb{Z}_p$ where $\phi_p(a) = a \bmod p$ where p is prime.

Let $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ where $\phi_p(\sum a_i x^i) = \sum \phi_p(a_i) \cdot x^i$

[So ϕ_p is a ring morphism].

Let $a, b \in \mathbb{Z}[x]$ and $c = a \cdot b$.

$$\phi_p(c) = \phi_p(a \cdot b) = \phi_p(a) \underset{\mathbb{Z}_p[x]}{\cdot} \phi_p(b).$$

Idea: compute $\phi_{p_i}(c)$ via $\phi_{p_i}(a) \cdot \phi_{p_i}(b)$ for sufficiently many primes p_i so we can recover the integers in c using the CRT.

How many primes? Which primes?

Homomorphism Diagram <u>for $\times$ in $\mathbb{Z}[x]$</u>

Homomorphism Diagram for $\times$ in $\mathbb{Z}[x]$

$$
\begin{tikzcd}
\text{Input: } a,b \in \mathbb{Z}[x] \arrow[rr, "\text{classical } \times"', "n^2 O(m^2)"] \arrow[d, "\phi_{p_i}"', "{M = \prod p_i,\ M > 2\|C\|_\infty}"] & & \text{Output } C = a \times b \in \mathbb{Z}[x] \\
a_i, b_i \in \mathbb{Z}_{p_i}[x] \arrow[rr, "\text{classical } \times \text{ in } \mathbb{Z}_{p_i}[x]", "\le n^2 \text{ mults in } \mathbb{Z}_{p_i}"'] & & C_i = a_i \times b_i \arrow[u, "{\text{Find } C \in \mathbb{Z}_M[x] \text{ s.t. } C \equiv C_i \bmod p_i}"']
\end{tikzcd}
$$

Put C in the symmetric range $-\frac{M}{2} < y < \frac{M}{2}$

How many primes?

Def: The height of $a(x)$ is $\|a\|_\infty = \max_{i=0}^{n-1} |a_i|$

E.g. $\|2x^2 - 5\|_\infty = +5$

Need $\prod p_i > 2 \cdot \|C\|_\infty$

Example. $a = 3x - 4 \quad b = 6x + 5 \quad C = 18x^2 - 9x - 20.$

Bound $\|C\|_\infty \le \|a\|_\infty \cdot \|b\|_\infty \cdot \min(\#\text{terms in } a, \#\text{terms in } b).$

$\le 4 \cdot 6 \cdot \min(2,2) = 48.$

$-48 \le u \le 48 \implies M \ge 97$

	a_i	b_i	C_i
$p_1 = 5$	$3x+1$	$1 \cdot x + 0$	$3x^2 + 1x + 0$
$p_2 = 7$	$3x+3$	$6x+5$	$4x^2 + 5x + 1$
$p_3 = 3$	$0 \cdot x + 2$	$0 \cdot x + 2$	$0x^2 + 0x + 1$

$M = 105 \ge 97$ CRT $u = 18 \cdot x^2 + 96x + 85$

$0 \le u < 105$ $\quad \mathrm{mods}(u, M) = 18 \cdot x^2 - 9x - 20 = C.$

$-52 \le u \le 52$

Analysis of the "modular multiplication algorithm"

Given $|a_i| < B^m$ and $|b_i| < B^m$ and $\deg(a) = \deg(b) \le n-1.$

Need $\prod p_i > 2\|C\|_\infty \le 2\|a\|_\infty \|b\|_\infty \min(n,n)$

$\le 2 \cdot B^m \cdot B^m \cdot n.$

Need $\prod p_i > \underline{2}\|C\|_\infty \leq \underline{2}\|a\|_\infty \|b\|_\infty \min(n,n)$

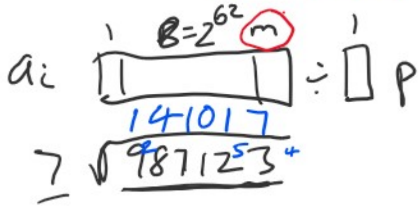
$\leq 2 \cdot B^m \cdot B^m \cdot n.$

Suppose $\underline{B < p_i < 2B}$ where $B = 2^{62}$ say, i.e. machine primes.

$\#\text{primes} < \lceil \log_{\underline{B}} 2B^m B^m n \rceil = \lceil \log_B \underbrace{2n}_{<1 \text{ in practice}} \rceil + 2m < 2m+1 \in O(m)$

Cost of $\phi_{p_i}(a), \phi_{p_i}(b)$ is $2n \cdot O(m) \cdot O(m) = O(nm^2)$

coefficients in a & b. #primes $a_i \bmod p_i$



#primes. # of arithmetic ops in $\mathbb{Z}_{p_i}$ cost of each op.

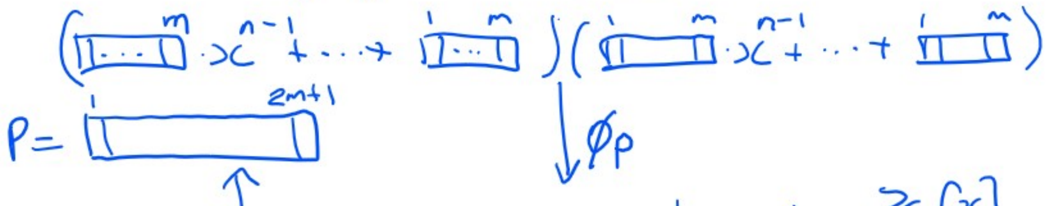
Cost of the $O(m)$ $\times$ in $\mathbb{Z}_{p_i}[x]$ is $O(m) \cdot O(n^2) O(1) = O(mn^2)$

Cost of the CRT is $(2n-1) \cdot O(m)^2 = O(nm^2)$.

$\deg(a) = \deg(b) = n-1$ # coeffs in C Cost of one CR application

Total: $O(nm^2) + O(mn^2) + O(nm^2) = O(nm^2 + n^2 m)$.

Why not use one big prime $P > \underline{2nB^{2m}}$



$\underline{a} \cdot \underline{b}$ in $\mathbb{Z}_P[x]$

We do n^2 $\times$ in $\mathbb{Z}$ of $a_i \cdot b_j$ which costs $n^2 \cdot O(m^2)$
$= O(n^2 m^2)$.

Conclusion: The CRT buys us one order of magnitude speedup.