Lec11A The Modular GCD Algorithm, Michael Monagan

February 10, 2021 11:49 PM

Let $a = \sum_{i=0}^{n-1} a_i x^i$, $b = \sum_{i=0}^{n-1} b_i x^i$, $a_i, b_i \in \mathbb{Z}$, $|a_i| < B^m$, $|b_i| < B^m$.

$$a = \overset{1 \qquad\qquad m}{\boxed{\qquad\qquad\quad}}\, x^{n-1} + \cdots + \boxed{\qquad\qquad}\, x + \boxed{\qquad\qquad}$$

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

How fast can we multiply $a \times b$?

Classical polynomial & integer arithmetic $n^2 \cdot \underbrace{O(m^2)}_{\text{classical } \times \text{ in } \mathbb{Z}} = O(n^2 m^2) \overset{n=m}{=} O(n^4)$.

Modular algorithm [uses the CRT] $O(nm^2 + n^2 m) \overset{n=m}{=} O(n^3)$.

How fast can we compute $\gcd(a,b)$?

Primitive Euclidean algorithm does $\underline{O(n^2)}$ integer $\times, \div$, gcds. $\underline{pp(r_k)}$

The integers grow linearly with k to have size $\le \underline{c\,k \cdot m}$.

$$\text{Cost} \le \sum_{k=1}^{n-1} \underbrace{O(n-k)}_{\substack{\#\text{ integer } \times, \div, \text{gcds}\\ \text{at step } k}} \cdot O(\underbrace{(ckm)}_{\substack{\text{size of integers}\\ \text{at step } k}}{}^{2}) = O(m^2 n^4) \overset{n=m}{=} \underline{O(n^6)}$$

classical algs.

20 yrs.

$\underline{n=1000}$, $m=1000$, $\underline{B=10}$

7.4 Modular gcd algorithm: $O(mn^2 + m^2 n) \overset{n=m}{=} O(n^3) = 0.63\,s$.

Main idea: Let $a, b \in \mathbb{Z}[x]$ and $\underline{g = \gcd(a,b)}$.

Then $\exists\ \bar{a}, \bar{b} \in \mathbb{Z}[x]$ s.t. $\underline{a = g \cdot \bar{a}}$ and $\underline{b = g \cdot \bar{b}}$ $\Rightarrow \gcd(\bar{a}, \bar{b}) = 1$

cofactors of a & b.

Let $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ where $\phi_p(a) = a \bmod p$.

Then

$$\gcd(\underline{\phi_p(a), \phi_p(b)}) = \gcd(\phi_p(g \cdot \bar{a}), \phi_p(g \cdot \bar{b}))$$

in $\underline{\mathbb{Z}_p[x]}$

$$= \gcd(\phi_p(g) \cdot \phi_p(\bar{a}), \phi_p(g) \cdot \phi_p(\bar{b}))$$

$$= \phi_p(g) \cdot \gcd(\phi_p(\bar{a}), \phi_p(\bar{b})).$$

$\times$ units ?? $\qquad$ 1 ??

Use CRT: $\prod p_i > \underline{2 \cdot \|g\|_\infty}$??

Unlucky Primes

Let $a, b \in \mathbb{Z}[x]$, $g = \gcd(a,b)$ and $a = g \cdot \bar{a}$ and $b = g \cdot \bar{b}$.

Unlucky Primes

Let $a, b \in \mathbb{Z}[x]$. $g = \gcd(a,b)$ and $a = g\cdot\bar{a}$ and $b = g\cdot\bar{b}$.

Example.

$$\gcd(\,(x+1)\cdot x,\ (x+1)\cdot(x+pq)\,) = x+1$$

mod $p_1 = p$ $\quad = (x+1)\cdot x = 1\cdot x^2 + 1\cdot x + 0$

mod $p_2 = q$ $\quad = (x+1)\cdot x = 1\, x^2 + 1\cdot x + 0$

mod $p_i \notin \{p,q\}$ $\quad = \underline{x+1} = 0\, x^2 + 1\cdot x + 1.$

CRT: $\quad = a x^2 + x + c.$

Definition. A prime p is unlucky if $\gcd(\phi_p(\bar{a}), \phi_p(\bar{b})) \neq 1$.
We cannot reconstruct g using any unlucky prime.

Theorem: The # of unlucky primes is finite.
How can we identify them? Know a, b, $\gcd(\phi_p(a), \phi_p(b))$.
? Take the g_i mod p_i of least degree.

Example.

$$\gcd(\,(px+1)(x+1),\ (px+1)(x+p+1)\,) = px+1.$$

mod $\underline{p_1 = p}$ $\quad = \underline{x+1}$

mod $p_2 \neq p$ $\quad = 1\cdot x + \frac{1}{p}$ mod p_2

Definition. A prime p is <u>bad</u> if $p \mid lc(g)$.
$p \mid lc(g)$ and $\underline{a} = \bar{a}\cdot\underline{g}$ then $p \mid lc(a)$.
We will avoid bad primes by requiring $p \nmid lc(a)$,
then keeping g_i mod p_i of least degree.

Lemma 7.3 Let $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ where $\phi_p(a) = a \bmod p$.
Let $a, \in \mathbb{Z}[x]\setminus\{0\}$, $g = \gcd(a,b)$, $g_p = \gcd(\phi_p(a), \phi_p(b)) \in \mathbb{Z}_p[x]$.
If $\phi_p(lc(a)) \neq 0$ then $\deg(g_p \geq \deg(g)$ and $\phi_p(g) \mid g_p$.
$\Rightarrow$ If $\deg(\underline{g_p}) = \deg(\underline{g})$ then. $\phi_p(g) = u\cdot g_p$ for some $u \in \mathbb{Z}_p$.
[Either get an associate of $\phi_p(g)$ or g_p has too high degree.]

Corollary: If $g_p = \gcd(\phi_p(a), \phi_p(b)) = 1 \Rightarrow \deg(g) = 0 \Rightarrow g \in \mathbb{Z}$.
If a, b are primitive $\Rightarrow g = 1$.

If a, b are primitive $\Rightarrow g = 1$.

Proof. Let $a = g\cdot\bar{a}$ and $b = g\cdot\bar{b}$.

$$g_p = \gcd(\phi_p(a = g\cdot\bar{a}), \phi_p(b = g\cdot\bar{b}))$$

$$= \gcd(\underset{\neq 0}{\underline{\phi_p(g)}}\cdot\underset{\neq 0}{\phi_p(\bar{a})}, \underset{\neq 0}{\phi_p(g)}\cdot\underset{= 0\,??}{\phi_p(\bar{b})}).$$

$\phi_p(lc(a)) \neq 0 \Rightarrow p \nmid lc(a = g\cdot\bar{a}) = lc(g)\cdot lc(\bar{a}) = p\nmid lc(g)$ and $p \nmid lc(\bar{a})$.

$$g_p = \omega\cdot\phi_p(g)\cdot \gcd(\underset{\neq 0}{\phi_p(\bar{a})}, \phi_p(\bar{b})) \quad \text{for some } \omega \in \mathbb{Z}_p.$$

$$g_p = \omega\cdot\phi_p(g)\cdot\Delta \quad \text{for some } \Delta \in \mathbb{Z}_p[x] \text{ with } \Delta \neq 0.$$

$\Rightarrow \deg g_p \geq \deg(g)$. and $\phi_p(g) \mid g_p$.