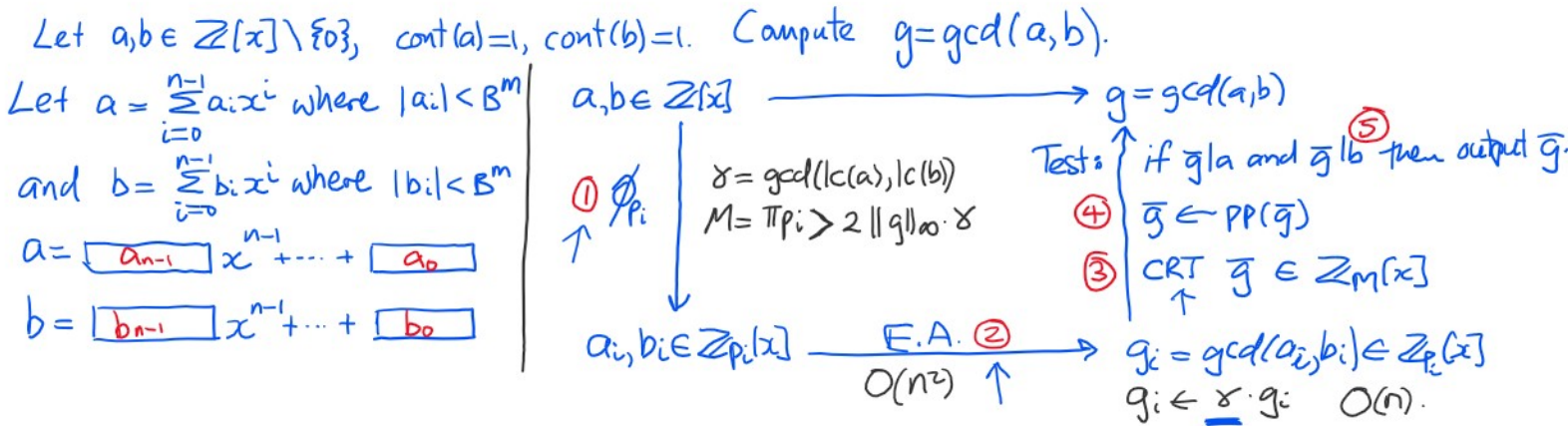


Assignment #3 is due on Monday @ 11pm.



How many primes do we need?
 ?? Assume no unlucky primes ??

Mignotte bound.

$\prod p_i > \frac{2 \delta \|g\|_{\infty}}{2^{n-1} \sqrt{n} B^{2m}}$
 $\prod p_i > \frac{2 \delta \|g\|_{\infty}}{2^{n-1} \sqrt{n} B^{2m}}$

$\begin{cases} \|g\|_{\infty} < 2^{n-1} \sqrt{n} \|a\|_{\infty} < 2^{n-1} \sqrt{n} B^m \\ \delta = \text{gcd}(\text{lc}(a), \text{lc}(b)) < B^m \end{cases}$

If $B < p < 2B$ then $\# \text{primes} \leq \lceil \log_B 2^{n-1} \sqrt{n} B^{2m} \rceil < 1$
 $= 2m + \log_B 2^n + \log_B \sqrt{n}$
 $\leq 2m$

- ① Cost of $\phi_{p_i}(a)$ & $\phi_{p_i}(b) \leq \underbrace{2^m}_{\# \text{primes}} \cdot \underbrace{2^n}_{\# \text{coeffs in } a \& b} \cdot O(m) = O(m^2 n)$.
- ② Cost of gcds in $\mathbb{Z}_{p_i}[x]$ $\leq 2^m \cdot O(n^2) = O(mn^2)$.
 $\text{deg}(a) = \text{deg}(b) \leq n-1$
- ③ Cost of the CRT : $\leq n \cdot O((2^m)^2) = O(nm^2)$
 $\text{deg } g \leq n-1$
 $g \text{ has } \leq n \text{ coefficients.}$ Excl Alg. in \mathbb{Z}
- ④ Cost of $\bar{g} \leftarrow \text{pp}(\bar{g}) \leq (n-1) O((2^m)^2) + n O((2^m)^2) = O(nm^2)$
 $n-1$ integer gcds
 n divisions.
 $\text{size} \leq 2^m \div \square$
- ⑤ Cost of $\bar{g} | a$ and $\bar{g} | b$: $2 O(n^2 m^2) = O(n^2 m^2)$.

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

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