Def The *discriminant* of $f(X) = a_n X^n + \dots + a_0 \in K[X]$

$$\operatorname{disc}(f) = \frac{(-1)^{n(n-1)/2}\operatorname{Res}(f,f')}{a_n}.$$

Ex $\operatorname{disc}(aX^2+bX+c) = b^2-4ac$

Lemma 7.3.4

$$\operatorname{disc}(f) = a_n^{2n-2}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$$

if $\alpha_1,\dots,\alpha_n \in \bar{K}$ are the roots of f (with mult.)

Pf $\deg(f)=n$, $\deg(f')=n-1$ $\qquad f(X) = a_n\cdot\prod_j (X-\alpha_j)$

$$\underset{\text{Lemma 7.3.3}}{\Rightarrow} \operatorname{Res}(f,f') = (-1)^{n(n-1)/2} a_n^{n-1}\cdot\prod_{i=1}^{n} f'(\alpha_i)$$

$$= (-1)^{n(n-1)/2} a_n^{2n-2}\cdot\prod_i\prod_{j\ne i}(\alpha_i-\alpha_j)$$

$$= a_n^{2n-2}\cdot\prod_{i<j}(\alpha_i-\alpha_j).$$

$\square$

~~7.4. Greatest common divisor~~

7.4. Bounds on polynomial factors

Thm 7.4.1 ~~(cf. Cohen, section 3.5.1, for a better thm)~~

Let $f(x)=a_nX^n+\dots+a_0\in\mathbb{C}[X]$,

$g(x)=b_mX^m+\dots+b_0\in\mathbb{C}[X]$ be pol.

with $g\mid f$. Then,

$$\left|\frac{b_i}{b_m}\right| \le \binom{m}{i}\cdot\left(\sum_{j=0}^{n}\left|\frac{a_j}{a_n}\right|^2\right)^{1/2} \quad \text{for } i=0,\dots,m.$$

Rmk There are better bounds; see for example Thm 3.5.1 in Cohen.

Cor 7.4.2 If $f\in\mathbb{Z}[X]$ is divisible by $g\in\mathbb{Z}[X]$ in the ring $\mathbb{Z}[X]$ ~~are primitive (gcd of coeff. = 1)~~

then $$|b_i|\le \underbrace{\binom{m}{i}}_{\le 2^m}\cdot\underbrace{\left(\sum_{j=0}^{n}|a_j|^2\right)^{1/2}}_{\le\sqrt{n+1}\cdot(\max a_j)} \quad \text{for } i=0,\dots,m.$$

Pf of Cor ~~$g\mid f$ in $\mathbb{C}[X]$, g,f primitive $\Rightarrow$ $g\mid f$ in $\mathbb{Z}[X]$ (Gauss's lemma)~~

$g\mid f$ in $\mathbb{Z}[X]$
$\Rightarrow b_m\mid a_n \Rightarrow |b_m|\le|a_n|.$ □

The Thm follows from:

Lemma 7.4.3 (Landau's inequality) Let $r_1,\dots,r_n\in\mathbb{C}$ be the roots of $f(x)=a_nX^n+\dots+a_0\in\mathbb{C}[X]$. Then,

$$\prod_{\substack{1\le i\le n:\\ |r_i|\ge 1}}|r_i| \le \left(\sum_j\left|\frac{a_j}{a_n}\right|^2\right)^{1/2}.$$

7.5. Gcd of integer polynomials

Thm 7.5.1 Let $0 \neq f, g \in \mathbb{Z}[X]$ be polynomials of degree $\leq n$ whose coefficients c satisfy $|c| \leq B$. We can compute $\gcd(f,g) \in \mathbb{Z}[X]$ in average time $\tilde{O}(n(n+\log B))$ on a randomized $O(\log(n+\log B))$-bit RAM.

Here, $\tilde{O}(X)$ means $O(X(\log X)^k)$ for some fixed $k \geq 0$.

Rmk There's a subtle difference between gcd in $\mathbb{Q}[X]$ and in $\mathbb{Z}[X]$: The gcd in $\mathbb{Q}[X]$ is only defined up to mult. by elements of $\mathbb{Q}^{\times}$ but the gcd in $\mathbb{Z}[X]$ is defined up to mult. by el. of $\mathbb{Z}^{\times} = \{$
For example, $\gcd_{\mathbb{Z}[X]}(2X, 6X^3) = 2X$.
But the correct multiple is easy to determine, so it suffices to find $\gcd(f,g)$ up to mult. by a scalar.

Rmk Let $\tilde{h} = \gcd_{\mathbb{Q}[X]}(f,g) \in \mathbb{Z}[X]$ be primitive (relatively prime coefficients). Then, $\tilde{h} \mid f, g$ by Gauss's ~~lemma. Let t = gcd (lc(f), lc(g))~~ lemma, so in part. $lc(\tilde{h}) \mid lc(f), lc(g)$.
Let $t = \gcd(lc(f), lc(g))$. We'll explain how to compute the gcd $h(X) = \frac{t}{lc(\tilde{h})} \cdot \tilde{h}(X) \in \mathbb{Z}[X]$ of f, g (over $\mathbb{Q}[X]$) that has leading coefficient $lc(h) = t$.

~~Let $k = O($ large enough so that~~

~~$p_1 \cdots p_k > 2^n \cdot \sqrt{n+1} \cdot B$. upper bd. on coeff. of $\tilde{h}(x)$~~

Pf of Thm 7.5.1

Find $K = O(n + \log B)$ large enough so that

$$\prod_{\substack{p \le K \\ p \nmid t}} p > \underbrace{2^n \cdot \sqrt{n+1} \cdot B}_{\substack{\text{upper bd.} \\ \text{on coeff. of } \tilde{h}(x)}}.$$

(Note that $\prod_{p \mid t} p \le |t| \le B$.)

Find $L = O(n \log(nB))$ large enough so that

$$\prod_{\substack{K < p \le L \\ p \nmid t}} p > \underbrace{(2n)! \cdot B^{2n}}_{\substack{\text{upper bd.} \\ \text{for } |s_d(f,g)|}}.$$

Find $M = O(n \log(nB))$ large enough so that

$$\#\{K < p \le M,\ p \nmid t\} > 2 \cdot \#\{K < p \le L,\ p \nmid t\}.$$

~~Let $A := \#\{p \le K,\ p \nmid t\} = O\left(\frac{n + \log B}{\log(n + \log B)}\right)$. Pick different primes $p_1, \dots, p_A \le M$ uniformly at random. For $i = 1, \dots, A$ compute $h_i := \gcd(f \bmod p_i,\ g \bmod p_i)$ where w.l.o.g. $lc(h_i) = t \bmod p_i$.~~

let $A = \#\{p \le K,\ p \nmid t\} = O\left(\frac{n + \log B}{\log(n + \log B)}\right)$.

Pick a random prime $p_0 \le M$, $p_0 \nmid t$ and compute $d' := \deg(\gcd(f \bmod p_0,\ g \bmod p_0))$.

(With prob. $\ge \frac{1}{2}$, we have $d' = d$. Always $d' \ge d$.)

compute $\gcd(f \bmod p, g \bmod p)$ for random $p \le M$, $p \nmid t$
until you found $p_1, \dots, p_A \le M$ such that

$\deg(\gcd(f \bmod p_i, g \bmod p_i)) = d'$ for $i = 1, \dots, A$.

The expected nr. of primes to try is $O(A)$.

Let $h_i = \gcd(\dots)$ where w.l.o.g. $lc(h_i) \equiv t \bmod p_i$.

Note that $p_1 \cdots p_A \ge \prod_{\substack{p \le k \\ p \nmid t}} p > 2^n \cdot \sqrt{n+1} \cdot B$, so there is at most one pol. $\tilde{h}'$ with coeff. $\le 2^n \cdot \sqrt{n+1} \cdot B$ s.t.

$\tilde{h}' \equiv h_i \bmod p_i$ for $i = 1, \dots, A$.

If there is one and it divides f and g, then it must be the gcd of f and g in $\mathbb{Q}[X]$.

Otherwise (with prob. $\le \frac{1}{2}$), start over!

□

Rmk There's another "efficient" alg. that avoids reduction modulo primes:
The subresultant algorithm (cf. section 3.3 in Cohen).
It's basically the Euclidean alg., but avoids exponential growth of coefficients by dividing by an appropriate (easy to compute) integer (dividing all coeffs) at each step!

Rmk You can use a similar alg. as in Thm 7.5.1 for example to compute the gcd of polynomials $f, g \in \mathbb{F}_q[T][X]$. The running time is better: $\tilde{O}(\underbrace{nD}_{\text{size of input}})$, where all coeff. of f, g are pol. in T of deg $\le D$.

The reason is again that the triangle ineq. in $\mathbb{F}_q(T)$ is stronger than in $\mathbb{R}$. (Instead of Cor. 7.4.2, you have the obvious fact that the degree of any coeff. of $\gcd(f, g)$ is also at most D)