Factoring univariates over $\mathbb{Q}$

- Suppose $f(x) \in \mathbb{Q}[x]$ is a polynomial to be factored.

  By multiplying it with a positive integer we could clear away the denominators.

- So, wlog $f(x) \in \mathbb{Z}[x]$. Let n be its degree and the coefficients a_i be of l-bits.

- How do we factor, or test the irreducibility of, the integral polynomial $f(x)$?

- Starting idea is to factor it modulo a prime p, do Hensel lifting and "solve a linear system" (much like bivariate factoring).

- Let us first see the algorithm & then the analysis.

  It was discovered by (Lenstra, Lenstra, Lovász) in 1982, starting a new field.

Input: $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $|a_i| < 2^{\ell-1}$ $(0 \le i \le n)$.

Output: A nontrivial integral factor (if one exists).

L^3-algorithm:

1) Preprocess: Assume that f is square-free. Find the smallest prime p s.t. $\begin{cases} p \nmid a_n, \\ f(x) \bmod p \text{ is sq.-free.} \end{cases}$

[If f is sq.-full then $\gcd(f, f')$ factors f.
$f(x) \bmod p$ is sq.-full iff $p \mid \mathrm{res}(f, f')$.
Now, $|a_n \cdot \mathrm{res}(f, f')| < 2^{\ell} \cdot (2^{\ell})^{n+1} \cdot (2^{\ell+\lg n})^{n} \cdot (2n+1)!$
$\Rightarrow$ # primes p dividing $a_n \cdot \mathrm{res}(f, f')$ are at most $2\ell(n+1) + 3n\lg n < 3n(\ell + \lg n)$ many.
$\Rightarrow$ A prime $p = \tilde{O}(\ell n)$ will work.]

2) Factor mod p: Using Berlekamp's algorithm compute a factorization $f(x) \equiv g_0 \cdot h_0 \pmod p$ where $g_0(x) \bmod p$ is monic, irreducible & coprime to h_0.

3) Hensel lift: Compute $f \equiv g_k \cdot h_k \pmod{p^{2^k}}$,

for $k = \lceil \lg 2n^3\ell \rceil$.

4) Linear system: Find $\tilde{g}, t_k$ s.t. $\tilde{g} \equiv g_k \cdot t_k \pmod{p^k}$ with $\deg \tilde{g} < n$ & the coefficients of $\tilde{g}$ are at most $2^{n\cdot(\ell+\lg n)}$ in magnitude.

5) Output $\gcd(f, \tilde{g})$.

Analysing the steps

Step 2: Since $p = \tilde{O}(\ell n)$, this step finds g_0 in deterministic poly$(n\ell)$ time. □

Step 3: Clearly, in poly$(n\ell)$ time. □

Step 4: For this we need to estimate the size of the factors of f.

Lemma 1: (Mignotte's bound) Any root α of a polynomial

$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ satisfies $|\alpha| \le n \cdot \max_i |a_i|$.

Proof:

- If $|\alpha| < 1$ then done.
- Else $|f(\alpha)| = |a_n \alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i|$

$\geqslant |\alpha|^n - \sum_{i=0}^{n-1} |a_i \alpha^i|$

$\geqslant |\alpha|^n - n \cdot (\max_i |a_i|) \cdot |\alpha|^{n-1}$

$\Rightarrow |\alpha| \leqslant n \cdot \max_i |a_i|$. □

Lemma 2: Any factor g of f has coefficients of magnitude at most $2^{(\ell + \lg n - 1)n}$.

Proof:

- Let $g(x) = \prod_{i=1}^{m} (x - \alpha_i)$, $\alpha_i \in \mathbb{C}$.
- The coeff. of x^{m-j} is $\sum_{S \in \binom{[m]}{j}} \prod_{i \in S} (-\alpha_i)$.
- Its magnitude $\leqslant \sum_{S} \prod_{i \in S} |\alpha_i|$

$< \binom{m}{j} \cdot (n 2^{\ell-1})^j < (1 + n 2^{\ell-1})^{n-1} < 2^{(\ell + \lg n - 1)n}$. □

– Thus, $\exists$ suitable $\tilde{g}$ if f is reducible. □

Step 5: • If a $\tilde{g}$ exists in Step 4, and $(f, \tilde{g}) = 1$, then

$\exists\, u, v \in \mathbb{Z}[x]$, $\quad uf + v\tilde{g} = res(f, \tilde{g}) \neq 0$.

$\Rightarrow u \cdot g_k \cdot h_k + v \cdot g_k \cdot \ell_k \equiv res(f, \tilde{g}) \pmod{p^{2^k}}$.

$\Rightarrow g_k \cdot (u h_k + v \ell_k) \equiv$ " " .

`----- (i)

• Note that $|res(f, \tilde{g})| < (2n)! \cdot (2^\ell)^{n+1} \cdot (2^{(\ell + \log n) \cdot n})^n$

$< 2^{2n^3 \ell} < p^{2^k}$.

$\Rightarrow$ In eqn. (i), the RHS is a nonzero constant while the LHS is a nonconstant integral polynomial. ↯

$\Rightarrow$ This contradiction implies that Step 5 factors f, whenever $\tilde{g}$ exists. □

How do we compute $\tilde{g}$ (with "small" coeffs.)?

– Let g_k be of deg $n' < n$. The unknown polynomials are: $\tilde{g} = \sum_{i=0}^{n-1} c_i x^i$ & $\ell_k = \sum_{i=0}^{n-1-n'} \alpha_i x^i$ s.t.

$\tilde{g} \equiv g_k \cdot \ell_k \pmod{p^{2^k}}$.