14. Factoring over the integers, attempt 2

We will identify a pol. $f = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ ~~with the set~~ of degree $\leq n$ with the vector $(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$.

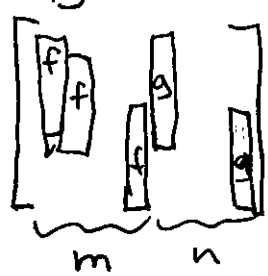
We'll write $|f| = |f|_2 = \sqrt{a_0^2 + \dots + a_n^2}$ for its Euclidean length.

Reminders:

Lemma 14.1 If $f \in \mathbb{Z}[x]$ is divisible by the pol. $g \in \mathbb{Z}[x]$ of degree d in the ring $\mathbb{Z}[x]$, then $|g| \leq \sqrt{d+1} \cdot 2^d \cdot |f|$.

Pf Imediate consequence of Cor 7.42. □

Lemma 14.2 If $f, g \in \mathbb{Z}[x]$ are pol. of degrees n, m, then
$|\mathrm{Res}(f,g)| \leq |f|^m \cdot |g|^n$

Pf $\mathrm{Res}(f,g) = \det$ 

. □

<u>Thm 14.3</u> We can factor any polynomial $f \in \mathbb{Z}[X]$ of degree n with $|f| \leq B$ in the ring $\mathbb{Q}[X]$ in time $\tilde{O}(n^{10} + n^{8} (\log B)^2)$.

<u>Pf</u> Let p be a prime.

We can factor $f \bmod p$. Let [redacted] $a \in \mathbb{F}_p[X]$ be an irreducible factor [redacted] of degree t.

Goal: Find [redacted] an (the) irreducible factor $g \in \mathbb{Z}[X]$ of f which is divisible by a modulo p.

~~Let $d \geq \deg(g)$. We'll find d by trying $d = 1, 2, \dots, n$~~

[redacted] We don't know $\deg(g)$, so will try $d = t, t+1, \dots, n$.

$\Rightarrow |g| \leq \sqrt{d+1} \cdot 2^{d} \cdot |f| =: A.$

[redacted]

Consider the set

$\Lambda = \{ \tilde{g} \in \mathbb{Z}[X]$ of deg. $\leq d \mid$ u divisible by a mod $p \}$.

It is a lattice $\Lambda \subseteq \mathbb{Z}^{d+1} \subset \mathbb{R}^{d+1}$ [redacted]

(of rank $d+1$ because it contains $p \cdot \mathbb{Z}^{d+1}$).

<u>How to find a basis?</u>

Let $\Lambda' := \{ h \in \mathbb{F}_p[X]$ of deg. $\leq d \mid h$ divisible by $a \}$.

This $\mathbb{F}_p$-vector space is generated by

$a(X), X \cdot a(X), \dots, X^{d-t} \cdot a(X)$.

[redacted] The ref of [redacted] the matrix with rows $a(X), \dots,$ [redacted] $X^{d-t} \cdot a(X)$ [redacted] gives us a basis of Λ'.

A basis of Λ consists of the lifts of these basis vectors (to $\mathbb{Z}$) together with the vectors $p \cdot X^{i}$ where [redacted] the column corr. to X^{i} in the ref has no leading 1. [redacted] of the matrix with rows $X^{d-t} \cdot a(X), p, pX, \dots, pX^{d}$, sto

~~Note that~~

~~Of course, $g \in \Lambda$~~ If $d = \deg(g)$, then $g \in \Lambda$.

We can use Alg. 13.6 to find an LLL-reduced basis of Λ. By Lemma 13.5, the first basis vector $\tilde{g} \in \Lambda$ has "almost-minimal length", so in particular

$$|\tilde{g}| \leq 2^{d/2} \cdot |g| \leq 2^{d/2} \cdot A =: \tilde{A} \text{ if } d = \deg(g).$$

By definition, both g and $\tilde{g}$ are modulo p divisible by a.

$\Rightarrow \gcd(g \bmod p, \tilde{g} \bmod p) \neq 1$

$\Rightarrow \mathrm{Res}(g, \tilde{g}) \equiv 0 \bmod p.$ (I)

Let's choose $p > (A \cdot \tilde{A})^d$.

$\Rightarrow p > (|g| \cdot |\tilde{g}|)^d \underset{\text{Lemma 14.2}}{\geq} |\mathrm{Res}(g, \tilde{g})|.$ (II)

(I), (II) $\Rightarrow \mathrm{Res}(g, \tilde{g}) = 0.$

$\Rightarrow \gcd(g, \tilde{g}) \neq 1$

$\underset{g \text{ irreducible}}{\Rightarrow} \quad g \mid \tilde{g} \text{ in } \mathbb{Q}[X]$

$\underset{\deg(\tilde{g}) \leq d \leq \deg(g)}{\Rightarrow} \quad \tilde{g} = \lambda \cdot g$ for some $\lambda \in \mathbb{Q}^\times$.

$\rightsquigarrow$ we've found an irred. factor g of f. Divide f by g and eliminate all mod p factors of dividing g. Then continue ...

If $d < \deg(g)$, then the basis vector $\tilde{g}$ obviously can't divide f.

Total running time: $\tilde{O}(n^{10} + n^{8}(\log B)^2)$.

$\square$

Some practical remarks:

Rmk 14.4 Since the alg. for Hensel's lemma has near-linear running time but factoring in $\mathbb{F}_p$ has an extra running time factor of $\log p$, it's better to factor $f \bmod p^k$ with $p^k > (A\tilde{A})^d$ and p chosen randomly from an interval large enough to make $f \bmod p$ squarefree.

(this saves time in the factoring mod p^k step in the beginning, but doesn't change the theoretical upper bd. on the r. time

Rmk 14.5 If $(f \bmod p) = lc(f)\, a_1 \cdots a_r$ for small r (with $a_1, \dots, a_r \in \mathbb{F}_p[X]$ monic and irreducible), it can be faster to try for every subset $S \subseteq \{1, \dots, r\}$ whether there is a divisor of f divisible exactly (mod p) by a_i $(i \in S)$, but not by a_i $(i \notin S)$.

To check this, as long as $\frac{p}{2} > lc(f) \cdot A$, it suffices to just try whether the pol. $g \in \mathbb{Z}[X]$ with $g \equiv lc(f) \cdot \prod_{i \in S} a_i \bmod p$ and coeffs. $\in [-\frac{p}{2}, \frac{p}{2}]$ divides f.

But since r can be large, this can have exponential running time (cf. extreme example in section 12).

Rmk 14.6 You can (should) combine 14.4, 14.5.