Pf of Hensel's lemma

Assume $f \equiv gh \mod \mathfrak{p}^k$ with f, g, h monic.

Let $\tilde{g} = g + \pi^k r$, $\tilde{h} = h + \pi^k s$.

$$\Rightarrow \tilde{g}\tilde{h} \equiv \underbrace{gh}_{f \bmod \mathfrak{p}^k} + \pi^k (rh + sg) \mod \mathfrak{p}^{2k}.$$

If g, h are relatively prime modulo $\mathfrak{p}$, then they are rel. prime modulo $\mathfrak{p}^k$, so the residue class $\frac{f-gh}{\pi^k}$ mod $\mathfrak{p}^k$ can be written uniquely as $rh + sg \mod \mathfrak{p}^k$ with polynomials r, s, where

$\deg(r) < \deg(g)$, $\deg(s) < \deg(h)$.

~~There are unique pol. $\tilde{g}, \tilde{h} \mod \mathfrak{p}^{2k}$ s.t. $f \equiv \tilde{g}\tilde{h} \mod \mathfrak{p}^{2k}$,~~

~~$\deg(\tilde{g}) = \deg(g)$, $\deg(\tilde{h}) = \deg(h)$.~~

Then, $\tilde{g}\tilde{h} \equiv f \mod \mathfrak{p}^{2k}$. $\square$

Proceed by induction.

Hensel's lemma Let $f, g, h \in \mathcal{O}(x)$ be monic polynomials such that $f \equiv gh \mod \mathfrak{p}$, where g, h are relatively prime mod $\mathfrak{p}$. Then, there are unique pol. $\tilde{g}, \tilde{h} \in \mathcal{O}(x)$ s.t. $f = \tilde{g}\tilde{h}$, $\tilde{g} \equiv g \mod \mathfrak{p}$, $\tilde{h} \equiv h \mod \mathfrak{p}$.

Thm 11.1 ~~Let~~ We can compute $\hat{g}, \hat{h} \bmod \wp^k$ in time $\tilde{O}(nk)$.

Pf HW. $\square$

More generally:

Thm 11.2 Let $f, g_1, \dots, g_r \in \mathcal{O}[x]$ be monic pol. such that $f \equiv g_1 \cdots g_r \bmod \wp$, where $g_1, \dots, g_r$ are pairwise relatively prime mod $\wp$. Then, we can compute the (unique) pol. $\hat{g}_1, \dots, \hat{g}_r$ mod $\wp^k$ such that

$$f = \tilde{g}_1 \cdots \tilde{g}_r, \quad \hat{g}_i \equiv g_i \bmod \wp \quad \text{in time } \tilde{O}(n).$$

Pf HW. $\square$

__Rmk__ In general, knowing a (monic) polynomial $f \in \mathcal{O}[X]$ of degree n modulo $\mathfrak{p}^k$ isn't enough to determine the structure of the factorisation of f in $K[X]$ no matter how large k is.

For example, a monic degree 2 pol. $f(X) \equiv X^2 \mod \mathfrak{p}^k$ could be

- a square: $f(X) = X^2$
- a product of two lin. pol.: $f(X) = (X - \pi^i)(X + \pi^i) = X^2 - \pi^{2i}$ for $2i \geq k$
- irreducible: $f(X) = X^2 - \pi^{2i+1}$ for $2i+1 \geq k$.

(Similarly, $X^2 + \varepsilon \in \mathbb{R}[X]$ could be a square, prod. of lin., or irred. for arbitrarily small ε.)

But if f is squarefree, then knowing $f \mod \mathfrak{p}^k$ suffices for sufficiently large k (depending of f).

12. Factoring pol. over $\mathbb{Z}$ (attempt 1)

Let $f \in \mathbb{Z}[X]$ be squarefree and monic.

Factor f mod p for a suitable prime p.

How does that factorization relate to that of f?

Let $f = f_1 \cdots f_r$.

$\Rightarrow f \equiv f_1 \cdots f_r \bmod p$.

But $f_1, \dots, f_r$ could factor further mod p.

<u>Rmk</u> If $p \nmid \operatorname{disc}(f)$, then f mod p is still squarefree, and vice-versa.

<u>Lemma 12.1</u> Let K be a nr. field, $\mathfrak{q}$ a prime ideal of K, $f \in \mathcal{O}_K[X]$ be a pol. whose leading coeff. and discriminant are not divisible by $\mathfrak{q}$.

Consider the number field $L = K[X]/(f)$.

The polynomial f splits mod $\mathfrak{q}$ in the same way as the prime ideal splits in L:

$f \equiv g_1 \cdots g_t \bmod \mathfrak{q}$ with $g_1, \dots, g_t$ irreducible mod $\mathfrak{q}$ $\in (\mathcal{O}_K/\mathfrak{q})[X]$

$\mathfrak{q} = \mathfrak{Q}_1 \cdots \mathfrak{Q}_t$ with prime ideals $\mathfrak{Q}_1, \dots, \mathfrak{Q}_t$ of L

with $\mathcal{O}_L / \mathfrak{Q}_i \cong (\mathcal{O}_K/\mathfrak{q})[X]/(g_i)$.

<u>Pf</u> See e.g. Prop I.8.3 in Neukirch's Algebraic Number Theory. ∎

Def Let $L|K$ be a Galois ext. of number fields, $\mathfrak{p}$ a prime of K and $\mathfrak{q}$ a prime of L dividing $\mathfrak{p}$.

The *decomposition group* is $D(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$.

The *inertia group* is $I(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in D(\mathfrak{q}|\mathfrak{p}) : \sigma(x) \equiv x \bmod \mathfrak{q} \ \forall x \in \mathcal{O}_L\}$.

Thm 12.2 a) G acts transitively on the primes $\mathfrak{q}$ of L dividing $\mathfrak{p}$.

b) $D(\tau\mathfrak{q}|\mathfrak{p}) = \tau D(\mathfrak{q}|\mathfrak{p})\tau^{-1}$

c) $I \ \ldots = \tau I \ \ldots \tau^{-1}$

d) $\mathfrak{q}$ divides $\mathfrak{p}$ exactly $|I(\mathfrak{q}|\mathfrak{p})|$ times.

e) $I(\mathfrak{q}|\mathfrak{p})$ is a normal subgroup of $D(\mathfrak{q}|\mathfrak{p})$ with $D(\mathfrak{q}|\mathfrak{p})/I(\mathfrak{q}|\mathfrak{p}) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} \mid \mathcal{O}_K/\mathfrak{p})$.

Cor 12.3 If $e = |I(\mathfrak{q}|\mathfrak{p})|$ and $ef = |D(\mathfrak{q}|\mathfrak{p})|$ and $efr = |G| = [L:K]$

then $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^e \cdots \mathfrak{q}_r^e$ with $[\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}] = f$.

Unfortunate Cor 12.4 Let $f \in \mathbb{Z}[X]$ be an irreducable monic pol. such that $L = \mathbb{Q}[X]/(f)$ is a Galois ext. of $\mathbb{Q}$ with Galois group G.

Unless G is cyclic, f splits modulo every prime p.

Pf If $p \mid \mathrm{disc}(f)$, then $f \bmod p$ is not squarefree.

If $p \nmid \mathrm{disc}(f)$, then $f \bmod p$ is squarefree and splits like p in L. $\Rightarrow I(\mathfrak{q}|p) = 1$ (unram.)

If $p\mathcal{O}_L = \mathfrak{q}$, then $e = 1$, $f = |$