1 Hensel lifts

Let p be a prime and suppose we have a polynomial factorization

$$u = \bar{v} \cdot \bar{w} \mod p$$

with p-prime, where $\bar{v}$ and $\bar{w}$ are relatively prime monic polynomials in the variable x. Set

$$\deg \bar{v} = m \quad \deg \bar{w} = n.$$

Our goal is to construct monic polynomials v, w of the same degrees as $\bar{v}, \bar{w}$ with

$$u = v \cdot w \mod p^k.$$

Since factorization $\mod p$ is unique, it follows that $v = \bar{v} \mod p$ and $w = \bar{w} \mod p$. Our secondary goal is to show that, $\mod p^k$, these polynomials are unique. Proceed by induction. Suppose we have already found v, w as above and are looking for v', w' with

$$u = v' \cdot w' \mod p^{k+1}$$

Over $\mathbb{Z}$, we have that

$$u = vw + p^k z$$

for some polynomial z. Since u, v, w are monic, the leading monomials of u and vw are x^{m+n} and so $\deg z = m + n - 1$. Since v, w are unique $\mod p^k$, it follows that v', w' must be of the form

$$v' = v + p^k a \quad w' = w + p^k b$$

with $\deg a < \deg v = m$ and $\deg b < \deg w = n$.

$$\begin{array}{rcl} v'w' & = & \left(v + p^k a\right)\left(w + p^k b\right) \\ & = & vw + p^k(aw + bv) + p^{2k}ab \\ & = & u + p^k z + p^k(aw + bv) + p^{2k}ab \\ & = & u + p^k\left(z + aw + bv\right) + p^{2k}ab \end{array}$$

It follows that

$$z + aw + bv = 0 \mod p \tag{1}$$

Introduce notation for the coefficients of the polynomials in (1):

$$\begin{array}{rcl} a & = & a_1 x^{m-1} + \cdots + a_m \\ b & = & b_1 x^{n-1} + \cdots + b_m \\ z & = & z_1 x^{m+n-1} + \cdots + z_{m+n} \\ w & = & x^m + w_1 \cdot x^{m-1} + \cdots + w_m \\ v & = & x^n + v_1 \cdot x^{n-1} + \cdots + v_n \end{array} \tag{2}$$

Then (1) is a linear system in the $m+n$ variables $a_1, \ldots, a_m, b_1, \ldots, b_n$ with $\deg z + 1 = m + n$ equations. More precisely, the matrix form of the equation (1) is given by the Sylvester matrix:

$$\begin{pmatrix} w_0 & 0 & \cdots & 0 & v_0 & 0 & \cdots & 0 \\ w_1 & w_0 & \cdots & 0 & v_1 & v_0 & \cdots & 0 \\ w_2 & w_1 & \ddots & 0 & v_2 & v_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & w_0 & \vdots & \vdots & \ddots & v_0 \\ w_m & w_{m-1} & \cdots & \vdots & v_n & v_{n-1} & \cdots & \vdots \\ 0 & w_m & \ddots & \vdots & 0 & v_n & \ddots & \vdots \\ \vdots & \vdots & \ddots & w_{m-1} & \vdots & \vdots & \ddots & v_{n-1} \\ 0 & 0 & \cdots & w_m & 0 & 0 & \cdots & v_n \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \\ b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \\ z_{m+1} \\ z_{m+2} \\ \vdots \\ z_{m+n} \end{pmatrix}, \tag{3}$$

where for convenience we have set $v_0 = w_0 = 1$. The determinant of the matrix above, called the resultant, is known to equal $\operatorname{res}(v, w) = w_0^m v_0^n \prod_{i,j} (\nu_i - \mu_j)$, where ν_i, μ_j are the roots of v and w over the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$. In our starting factorization $u = \bar{v} \cdot \bar{w}$, the factors $\bar{v}, \bar{w}$ are relatively prime and so have no common roots and we have that $\operatorname{res}(\bar{v}, \bar{w}) \neq 0$. At the same time we established that $v = \bar{v} \mod p$ and $w = \bar{w} \mod p$ and so $\operatorname{res}(\bar{v}, \bar{w}) = \operatorname{res}(v, w) \neq 0$. Since the determinant of (3) is non-zero, (3) has a unique solution. This shows both the existence and uniqueness of v', w'. This in turn concludes our inductive step.