

---

# REPORT: HENSEL LIFTING AND NEWTON ITERATION IN VALUTATION RINGS

*Instructor: Amit Kumar Sinhababu and Sumanta Ghosh*

---

SOHAM CHATTERJEE

SOHAMCHATTERJEE999@GMAIL.COM

WEBSITE: SOHAMCH08.GITHUB.IO

# CONTENTS

<b>CHAPTER 1</b>	<b>INTRODUCTION</b>	<b>PAGE 2</b>
<b>CHAPTER 2</b>	<b>HENSEL LIFTING</b>	<b>PAGE 3</b>
2.1	Hensel Ring	3
2.2	Conditions related to Hensel's Lemma	4
2.3	Hensel's Lemma	5
2.4	Hensel's Computation	9
2.5	Proof of Hensel's Lemma	9
<b>CHAPTER 3</b>	<b>NEWTON ITERATION</b>	<b>PAGE 10</b>
<b>CHAPTER 4</b>	<b>SOLVING DIFFERENTIAL EQUATIONS</b>	<b>PAGE 11</b>
<b>CHAPTER 5</b>	<b>FINDING SHORT VECTORS IN MODULES</b>	<b>PAGE 12</b>
<b>CHAPTER 6</b>	<b>FACTORIZATION OF POLYNOMIALS</b>	<b>PAGE 13</b>
<b>CHAPTER 7</b>	<b>BIBLIOGRAPHY</b>	<b>PAGE 14</b>

# CHAPTER 1



## Introduction

# Hensel Lifting

The hensel method described here will lift an approximate factorization of a polynomial over a Hensel Ring  $R$  with valuation  $v$  where the factors are relatively prime. We will show a linear convergence and a quadratic convergence behavior for the liftings.

## 2.1 Hensel Ring

### Definition 2.1.1: Hensel Ring

A ring with valuation  $v : R \rightarrow \mathbb{R}_{\geq 0}$  is called a Hensel Ring if:

- (i)  $\forall a \in R, v(a) \leq 1$
- (ii)  $\forall a, b \in R, \forall \epsilon > 0, \exists c \in R$  such that  $(v(a) \leq v(b) \implies v(a - bc) \leq \epsilon)$

In other words  $R$  is Hensel iff it is contained and dense in the valuation ring of its quotient field (with respect to the unique extension of  $v$ ). We sometimes call such  $v$  a Hensel Valuation.

In condition (ii) we assume we can compute the  $c$  efficiently.

### Theorem 2.1.1

Condition (i) of Hensel Ring  $\implies v$  is Non-Archimedean.

*Proof.* Let  $a, b \in R$ . Now

$$\begin{aligned}
 v(a + b)^k &= v((a + b)^k) \\
 &= v\left(\sum_{i=0}^k \binom{k}{i} a^{n-i} b^i\right) \leq \sum_{i=0}^k v\left(\binom{k}{i}\right) v(a)^{n-i} v(b)^i \\
 &\leq \sum_{i=0}^k v(a)^{n-i} v(b)^i \leq \sum_{i=0}^k M^{n-i} M^i \quad [m = \max v(a), v(b)] \\
 &= \sum_{i=0}^k M^k = M^k (k + 1)
 \end{aligned}$$

Hence

$$\left(\frac{v(a + b)}{M}\right)^k \leq (k + 1) \iff \frac{v(a + b)}{M} \leq (1 + k)^{\frac{1}{k}}$$

As  $k \rightarrow \infty$  the RHS approaches 1 so  $v(a + b) \leq M$ . ■

### Example 2.1 ( $p$ -adic Valuations)

- $\mathbb{Z}$  with  $p$ -adic valuation  $v_p$  where  $p \in \mathbb{N}$  is prime is a Hensel ring. Here  $v_p(a) = p^{-n}$  where  $n = \max\{k \geq 0 \mid p^k \mid a\}$
- $\mathbb{F}[y]$  with  $p$ -adic valuation  $v_p$  where  $p \in \mathbb{F}[y]$  is an irreducible polynomial is a Hensel Ring. Here  $v_p(f) = 2^{-n \deg p}$  where  $n = \max\{k \geq 0 \mid p^k \mid f\}$

#### Note:-

From the valuation  $v$  over  $R$  we naturally get a valuation  $v$  over the polynomial ring  $R[x]$  by defining

$$\forall f \in R[x], \text{ let } f = \sum_{i=0}^n f_i x^i, \text{ then } v\left(\sum_{i=0}^n f_i x^i\right) = \max_i \{v(f_i)\}$$

## 2.2 Conditions related to Hensel's Lemma

We will define 5 conditions. First suppose we have:

- (1)  $f \in R[x]$
- (2)  $f_0, \dots, f_m \in R[x]$      $\mathcal{F} = \{f_i : 0 \leq i \leq m\}$
- (3)  $f_0^*, \dots, f_m^* \in R[x]$      $\mathcal{F}^* = \{f_i^* : 0 \leq i \leq m\}$
- (4)  $s_0, \dots, s_m \in R[x]$      $\mathcal{S} = \{s_i : 0 \leq i \leq m\}$
- (5)  $s_0^*, \dots, s_m^* \in R[x]$      $\mathcal{S}^* = \{s_i^* : 0 \leq i \leq m\}$
- (6)  $z \in R$
- (7)  $\alpha, \delta, \epsilon \in \mathbb{R}$
- (8)  $\delta^* \in \mathbb{R}$
- (9)  $\gamma = \max\{\delta, \alpha\epsilon\}$

As you can see the set  $\mathcal{F}^*$  basically represents the lift of  $\mathcal{F}$  but here since we are saying the conditions in more generality we are not assuming any relations among them and we define some conditions involving them.

- $H_1(m, f, \mathcal{F}, \mathcal{S}, \epsilon) := v\left(f - \prod_{i=0}^m f_i\right) \leq \epsilon < 1$
- $H_2(m, f, \mathcal{F}, \mathcal{S}, z, \delta) := v\left(\sum_{i=0}^m s_i \prod_{j \neq i} f_j - z\right) \leq \delta < 1$
- $H_3(m, f, \mathcal{F}, \mathcal{S}, z, \alpha, \delta, \epsilon) :=$ 
  - (1)  $f_1, \dots, f_m$  are monic
  - (2)  $\deg\left(\prod_{i=0}^m f_i\right) \leq \deg f$
  - (3)  $\deg s_i \leq \deg f_i \forall i \in [m]$
  - (4)  $\alpha\delta \leq 1, \alpha\epsilon^2 \leq 1$
  - (5)  $1 \leq \alpha v(z)$
- $H_4(m, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon) :=$ 
  - (1)  $v(f_i^* - f_i) \leq \alpha\epsilon$      $\forall 0 \leq i \leq m$
  - (2)  $v(s_i^* - s_i) \leq \alpha\epsilon$      $\forall 0 \leq i \leq m$
  - (3)  $\deg f_i^* = \deg f_i$      $\forall i \in [m]$
  - (4)  $\deg s_i < \deg f_i \implies \deg s_i^* < \deg f_i^*$      $\forall i \in [m]$
- $H_5(m, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon, \delta^*) :=$  Let  $p \in [m]$ . Then suppose
  - $\mathcal{I}_p = \{I_0, I_1, \dots, I_p\}$  be a partition of  $\{0, \dots, m\}$  with  $0 \in I_0$ .
  - $\overline{\mathcal{F}}_p^m = \{\bar{f}_i : i \in [p]\} \subseteq R[x]$  be a set of monic polynomials

Then define:

$$F_i = \prod_{j \in I_i} f_j, \quad F_i^* = \prod_{j \in I_i} f_j^*, \quad \mathfrak{s}_i^* = \sum_{j \in I_i} s_j \frac{F_i^*}{f_j^*}$$

So now we denote:

$$\mathcal{F} = \{F_i : 0 \leq i \leq p\}, \quad \mathcal{F}^* = \{F_i^* : 0 \leq i \leq p\}, \quad \mathcal{S} = \{\mathfrak{s}_i^* : 0 \leq i \leq p\}$$

Assume:

1.  $v(\bar{f}_i - F_i) \leq \alpha\epsilon \forall i \in [p]$
2.  $\alpha v(s_i) \leq 1 \forall 0 \leq i \leq m$
3.  $\alpha\delta < 1, \alpha^2\delta \leq 1$
4.  $\alpha^2\epsilon < 1, \alpha^3\epsilon \leq 1$

Then the following are equivalent:

- (i)  $\exists \bar{f}_0, \bar{s}_0, \dots, \bar{s}_p \in R[x]$  denote

$$\bar{\mathcal{F}} = \{\bar{f}_i : 0 \leq i \leq p\}, \quad \bar{\mathcal{S}} = \{\bar{s}_i : 0 \leq i \leq p\}$$

then the following conditions are true:

- (a)  $H_1(p, f, \bar{\mathcal{F}}, \bar{\mathcal{S}}, \epsilon^*)$
- (b)  $H_2(p, f, \bar{\mathcal{F}}, \bar{\mathcal{S}}, z, \delta^*)$
- (c)  $H_3(p, f, \bar{\mathcal{F}}, \bar{\mathcal{S}}, z, \alpha^*, \delta^*, \epsilon^*)$
- (d)  $H_4(p, f, \bar{\mathcal{F}}, \bar{\mathcal{S}}, z, \alpha^*, \delta^*, \epsilon^*)$

where  $\alpha^* = \alpha, \epsilon^* = \alpha\epsilon\gamma$

- (ii)  $\exists \bar{f}_0 \in R[x]$  such that  $H_1(p, f, \bar{\mathcal{F}}, \bar{\mathcal{S}}, \epsilon^*)$  is true

- (iii)  $\forall i \in [p]$  we have  $v(\bar{f}_i - F_i^*) \leq \epsilon^*$ .

The first 3 conditions here together imply that: From  $H_1$  we get that  $f_0 \cdots f_m$  is a good approximation of factorization of  $f$  with  $\epsilon$ -precision,  $H_2 \implies z$  plays a similar role to the gcd of  $f_0, \dots, f_m$  and it shows the generalized bezout's identity for gcd for multiple elements. In the usual treatment of Hensel's Lemma  $f_0, \dots, f_m$  are relatively prime (more precisely their images in the residue class field or  $R$  modulo the maximal ideal  $\langle a \in R \mid v(a) < 1 \rangle$  satisfy the assumption then one can find  $s_0, \dots, s_m, \delta$  satisfying  $H_2$  with  $z = 1$ . One can set  $\alpha = 1$  or in general one can choose  $\alpha = \frac{1}{v(z)}$ . Thus  $H_2$  states that  $f_0, \dots, f_m$  are approximately pairwise relatively prime.

$H_4$  shows the connection between the lifts  $f_i^*, s_i^*$  and  $f_i, s_i$ .

$H_5$  basically states that the lifts are unique in the sense that one can group some of the  $f_i^*$ s to form  $F_0, \dots, F_p$  and change  $F_i$  to  $\bar{f}_i$  with precision  $\epsilon^*$  and still one will have the factorization of  $f$  with precision  $\epsilon^*$ .  $H_5$  is very important for the factorization algorithm in chapter 6.

Now we will state the Hensel's Lemma and will later give the algorithm to obtain the lifts.

## 2.3 Hensel's Lemma

First we will prove a helping lemma which will be very much usefull in the proof of Hensel's Lemma then we will state the actual theorem.

### Theorem 2.3.1

- (i) Let  $a, f, p, s \in R[x]$  such that  $f$  is monic and  $s = pf + a$  with  $\deg a < \deg f$ . Then we have  $v(p) \leq v(s)$  and  $v(a) \leq v(s)$
- (ii) Let  $h_0, \dots, h_m \in R[x]$  and  $h_0^*, \dots, h_m^* \in R[x]$  such that we have  $v(h_i^* - h_i) \leq \epsilon$  for all  $0 \leq i \leq m$ . Then we have  $v\left(\prod_{i=0}^m h_i - \prod_{i=0}^m h_i^*\right) \leq \epsilon$

*Proof.* (i) Suppose  $\deg s \geq \deg f \geq 0$  otherwise  $\deg s < \deg f$  Then  $s = 0 \times f + a = a$  so we get  $v(a) = v(s)$  and  $v(p) = v(0) = 0 \leq v(s)$ . Hence assume  $l = \deg s - \deg f \geq 0$ . Then  $p = \sum_{i=0}^l p_i x^i$  where  $p_i \in R$  for all  $0 \leq i \leq l$ .

Now we will induct on  $l - i$ . Let  $\deg f = n$  and  $\deg s = m$ . Hence assume  $f = \sum_{i=0}^n f_i x^i$  and  $s = \sum_{i=0}^m s_i x^i$  where for all  $0 \leq i \leq n$  and  $0 \leq j \leq m$ ,  $f_i, s_j \in R$ . Since  $f$  is monic  $f_n = 1$

Base Case ( $i = l$ ) :

$$v(p_l) = v(p_l)v(f_n) = v(p_l f_n) = v(s_m) \leq v(s)$$

Inductive Step :  $v(p_i) \leq v(s)$  for all  $l - k \leq i \leq l$ . Now coefficient of  $x^{(l-k-1)+n}$  in  $S$  is

$$s_{l-k-1+n} = \sum_{i=l-k-1}^l p_i f_{l-k-1+n-i}$$

Therefore  $p_{l-k-1} f_n = s_{l-k-1+n} - \sum_{i=l-k}^l p_i f_{l-k-1+n-i}$ . Therefore

$$\begin{aligned} v(p_{l-k-1}) &= v(p_{l-k-1} f_n) \leq \max\{v(s_{l-k-1+n}), v(p_i f_{l-k-1+n-i}) \mid l-k \leq i \leq l\} \\ &\leq \max\{v(s_{l-k-1+n}), v(p_i) \mid l-k \leq i \leq l\} \\ &\leq v(s) \end{aligned}$$

Therefore by induction we have  $v(p_i) \leq v(s)$  for all  $0 \leq i \leq l$ . Then  $v(p) \leq v(s)$ .

Hence

$$v(a) = v(s - pf) \leq \max\{v(s), v(pf)\} \leq \max\{v(s), v(p)\} \leq v(s)$$

Therefore we have  $v(a) \leq v(s)$ .

(ii) We will induct on  $0 \leq i \leq m$ .

Base Case :  $v(h_0 - g_0^*) \leq \epsilon$  Given

Inductive Step : Let this is true for  $i = k$  i.e.

$$v\left(\prod_{j=0}^k h_j - \prod_{j=0}^k h_j^*\right) \leq \epsilon$$

Now

$$\prod_{j=0}^k h_j (h_{k+1} - h_{k+1}^*) + \prod_{j=0}^k h_j^* (h_{k+1} - h_{k+1}^*) = \left[ \prod_{j=0}^{k+1} h_j - \prod_{j=0}^{k+1} h_j^* \right] - \left[ h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^* \right]$$

Therefore we have

$$\prod_{j=0}^{k+1} h_j - \prod_{j=0}^{k+1} h_j^* = \prod_{j=0}^k h_j (h_{k+1} - h_{k+1}^*) + \prod_{j=0}^k h_j^* (h_{k+1} - h_{k+1}^*) + \left[ h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^* \right]$$

Hence we have

$$\begin{aligned} v\left(\prod_{j=0}^{k+1} h_j - \prod_{j=0}^{k+1} h_j^*\right) &\leq \max\left\{v\left(\prod_{j=0}^k h_j\right) v(h_{k+1} - h_{k+1}^*), v\left(\prod_{j=0}^k h_j^*\right) v(h_{k+1} - h_{k+1}^*), v\left(h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^*\right)\right\} \\ &\leq \max\left\{v(h_{k+1} - h_{k+1}^*), v\left(h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^*\right)\right\} \\ &\leq \max\left\{\epsilon, v\left(h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^*\right)\right\} \end{aligned}$$

Now we need to show that

$$v \left( h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^* \right) \leq \epsilon$$

Now

$$\begin{aligned} h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^* &= \left( h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1}^* h_k^* \prod_{j=0}^{k-1} h_j \right) + \left( \left[ \prod_{j=k}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{k-1} h_j \right] - \left[ \prod_{j=k-1}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{k-2} h_j \right] \right) \\ &\quad + \left( \left[ \prod_{j=k-1}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{k-2} h_j \right] - \left[ \prod_{j=k-2}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{k-3} h_j \right] \right) \\ &\quad \vdots \\ &\quad + \left( \left[ \prod_{j=t+1}^{k+1} h_j^* \right] \left[ \prod_{j=0}^t h_j \right] - \left[ \prod_{j=t}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{t-1} h_j \right] \right) \\ &\quad \vdots \\ &\quad + \left( \left[ \prod_{j=1}^{k+1} h_j^* \right] h_0 - \prod_{j=0}^{k+1} h_j^* \right) + \left( \prod_{j=0}^{k+1} h_j^* - \left[ \prod_{j=0}^k h_j^* \right] h_{k+1} \right) \\ &= h_{k+1}^* \prod_{j=0}^{k-1} h_j^* (h_k - h_k^*) + \left[ \prod_{j=k}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{k-2} h_j \right] (h_{k-1} - h_{k-1}^*) \\ &\quad + \left[ \prod_{j=k-1}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{k-3} h_j \right] (h_{k-2} - h_{k-2}^*) \\ &\quad \vdots \\ &\quad + \left[ \prod_{j=t+1}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{t-1} h_j \right] (h_t - h_t^*) \\ &\quad \vdots \\ &\quad + \left[ \prod_{j=1}^{k+1} h_j^* \right] (h_0 - h_0^*) + \left[ \prod_{j=1}^k h_j^* \right] (h_{k+1}^* - h_{k+1}) \end{aligned}$$

Now for each  $0 \leq t \leq k$  we have

$$v \left( \left[ \prod_{j=t+1}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{t-1} h_j \right] (h_t - h_t^*) \right) \leq v(h_t - h_t^*) \leq \epsilon, \quad v \left( \left[ \prod_{j=1}^k h_j^* \right] (h_{k+1}^* - h_{k+1}) \right) \leq v(h_{k+1}^* - h_{k+1}) \leq \epsilon$$

Hence

$$v \left( h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^* \right) \leq \max_{0 \leq t \leq k} \left\{ v \left( \left[ \prod_{j=t+1}^{k+1} h_j^* \right] \left[ \prod_{j=0}^{t-1} h_j \right] (h_t - h_t^*) \right), v \left( \left[ \prod_{j=1}^k h_j^* \right] (h_{k+1}^* - h_{k+1}) \right) \right\} \leq \epsilon$$

Therefore we have

$$v \left( h_{k+1}^* \prod_{j=0}^k h_j - h_{k+1} \prod_{j=0}^k h_j^* \right) \leq \epsilon \implies v \left( \prod_{j=0}^{k+1} h_j - \prod_{j=0}^{k+1} h_j^* \right) \leq \epsilon$$

Hence by induction we have

$$v \left( \prod_{j=0}^m h_j - \prod_{j=0}^m h_j^* \right) \leq \epsilon$$

■



**Theorem 2.3.2 Hensel's Lemma**

Assume that we have  $f \in R[x]$ ,  $\mathcal{F} = \{f_0, \dots, f_m\} \subseteq R[x]$ ,  $\mathcal{S} = \{s_0, \dots, s_m\} \subseteq R[x]$ ,  $z \in R$  and  $\alpha, \delta, \epsilon \in \mathbb{R}$  which satisfy:

1.  $H_1(m, f, \mathcal{F}, \mathcal{S}, \epsilon)$
2.  $H_2(m, f, \mathcal{F}, \mathcal{S}, z, \delta)$
3.  $H_3(m, f, \mathcal{F}, \mathcal{S}, z, \alpha, \delta, \epsilon)$

Then we can compute efficiently

$$\mathcal{F}^* = \{f_i^* : 0 \leq i \leq m\} \quad \text{and} \quad T = \{t_0, \dots, t_m\}$$

such that

- (i) **Linear Case:**  $\mathcal{S}^* = \mathcal{S}$  and  $\delta^* = \gamma$ ,  $\epsilon^* = \alpha\gamma\epsilon$ . Then we have the following conditions hold:

- (a)  $H_1(m, f, \mathcal{F}^*, \mathcal{S}^*, \epsilon^*)$
- (b)  $H_2(m, f, \mathcal{F}^*, \mathcal{S}^*, z, \delta^*)$
- (c)  $H_3(m, f, \mathcal{F}^*, \mathcal{S}^*, z, \alpha, \delta^*, \epsilon^*)$
- (d)  $H_4(m, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon)$
- (e)  $H_5(m, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon, \delta^*)$

- (ii) **Quadratic Case:**  $\mathcal{S}^* = T$  and  $\delta^* = \alpha\gamma^2$ ,  $\epsilon^* = \alpha\gamma\epsilon$ . Assume that  $\deg s_i > \deg f_i$  for  $0 \leq i \leq m$ . Then we have the following conditions hold:

- (a)  $H_1(m, f, \mathcal{F}^*, \mathcal{S}^*, \epsilon^*)$
- (b)  $H_2(m, f, \mathcal{F}^*, \mathcal{S}^*, z, \delta^*)$
- (c)  $H_3(m, f, \mathcal{F}^*, \mathcal{S}^*, z, \alpha, \delta^*, \epsilon^*)$
- (d)  $H_4(m, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon)$
- (e)  $H_5(m, f, \mathcal{F}, \mathcal{F}^*, \mathcal{S}, \mathcal{S}^*, \alpha, \delta, \epsilon, \delta^*)$

## 2.4 Hensel's Computation

---

**Algorithm 1:** Hensel's Computation

---

**Input:**

1.  $f \in R[x], \mathcal{F} = \{f_0, \dots, f_m\} \subseteq R[x], \mathcal{S} = \{s_0, \dots, s_m\} \subseteq R[x]$
2.  $z \in R$
3.  $\alpha, \delta, \epsilon \in \mathbb{R}$

**Output:**  $\mathcal{F}^* = \{f_0^*, \dots, f_m^*\}, T = \{t_0, \dots, t_m\}$

```

1 begin
2   Set  $\gamma = \max\{\delta, \alpha\epsilon\}, \alpha^* = \alpha, \epsilon^* = \alpha\gamma\epsilon$  and  $e = f - \prod_{i=0}^m f_i$ 
3   for  $1 \leq i \leq m$  do
4     Compute  $a_i, b_i, p_i \in R[x]$  such that
           
$$s_i e = p_i f_i + a_i, \quad v(zb_i - a_i) \leq \epsilon\gamma, \quad \deg b_i \leq \deg a_i < \deg f_i$$

5   Compute  $a_0, b_0 \in R[x]$  such that
           
$$a_0 = s_0 e + f_0 \sum_{i=1}^m p_i, \quad v(zb_0 - a_0) \leq \epsilon\gamma, \quad \deg b_0 \leq \deg f - m$$


6   for  $0 \leq i \leq m$  do
7      $f_i^* = f_i + b_i$ 
8   for  $1 \leq i \leq m$  do
9     Compute  $c_i, d_i, g_i^* q_i \in R[x]$  such that
           
$$g_i^* = \prod_{j \neq i} f_j^*, \quad s_i(s_i g_i^* - z) = q_i f_i^* + c_i \quad v(zd_i - c_i) \leq \gamma^2 \quad \deg d_i \leq \deg c_i < \deg f_i^*$$

10  Compute  $g_0^* = \prod_{i=1}^m f_i^*$  and  $c_0, d_0 \in R[x]$  such that
           
$$c_0 = s_0 \left( \sum_{i=0}^m s_i g_i^* - z \right) + f_0^* \sum_{i=1}^m \left[ q_i + s_i \left( \sum_{j \neq i} s_j \frac{g_j^*}{f_j^*} \right) \right], \quad v(zd_0 - c_0) \leq \gamma^2, \quad \deg d_0 \leq \deg f - \deg g_0$$


11  for  $0 \leq i \leq m$  do
12     $t_i = s_i - d_i$ 
13  return  $\mathcal{F}^* = \{f_i^* : 0 \leq i \leq m\}, T = \{t_i : 0 \leq i \leq m\}$ 

```

---

## 2.5 Proof of Hensel's Lemma

CHAPTER 3

# Newton Iteration

CHAPTER 4

# Solving Differential Equations

CHAPTER 5

# Finding Short Vectors in Modules

CHAPTER 6

# Factorization of Polynomials

CHAPTER 7

# Bibliography