CS 681: Computational Number Theory and Algebra Lecture 18: Modified Hensel Lifting
Lecturer: Manindra Agrawal **Notes by: Shashi Mittal**

September 16, 2005.

1 Introduction

In previous lecture, we had discussed hensel lifting, and its application in polynomial division. We had also made a remark that during lifting, $deg\ h'$ or $deg\ g'$ may exceed $deg\ f$, which is undesirable. We present an example to show this, and the discuss the modification needed to remove this drawback.

2 Drawback of hensel lifting : an example

Consider $f(x) = x^4 + x^3 + 2x + 2$, $g(x) = x - 2$ and $h(x) = x^3 - 1$. It can be easily verified that $f \equiv gh\ (mod\ 3)$. If $s(x) = 2x^2 + x + 2$ and $t = 1$, then $sg\ +\ ht\ =\ 1$. Now, if we lift this to $mod\ 3^2$, then

$$\begin{aligned} e &= f - gh(mod\ 9) \\ &= (x^4 + x^3 + 2x + 2) - (x^3 - 1)(x - 2)(mod\ 9) \\ &= (3x^3 + 3x)(mod\ 9) \end{aligned}$$

g' and h' are calculated as follows :

$$\begin{aligned} g' &= h + se \\ &= (x - 2) + 1.(3x^3 + 3) \\ &= 3x^3 + 4x - 2 \end{aligned}$$

$$\begin{aligned} h' &= h + se \\ &= (x^3 - 1) + (2x^2 + x + 2)(3x^3 + 3x) \\ &= 6x^5 + 3x^4 + 4x^3 + 3x^2 - 3x - 1 \end{aligned}$$

We see that $deg\ h' > deg\ f$, which is undesirable.

3 Modified hensel lifting

Let $f \equiv gh(mod\, m)$, and s, t, e as define before. We assume that g is monic, and $deg\, f = deg\, g + deg\, h$. Let,

$$\begin{aligned} te &= qg + r(mod\ m^2) \\ g' &= g + r(mod\ m^2) \\ h' &= h + se + qh(mod\ m^2) \end{aligned}$$

Then,

$$\begin{aligned} g'h' &= (g + r)(h + se + qh) \\ &= (g + te - qg)(h + se + qh) \end{aligned}$$

Since $te = qg + r(mod\ m^2)$, therefore $q \equiv 0(mod\ m)$ and $r \equiv 0(mod\ m)$. Hence,

$$\begin{aligned} g'h' &= gh + gse + hte - qe(sg - th) + ste^2 - q^2gh \\ &= gh + e(mod\ m^2) \\ &= f(mod\ m^2) \end{aligned}$$

Therefore, $deg\ g = deg\ g'$, $deg\ h' = deg\ h$ and g is monic.

Assignment : Define s' and t' in such a way that $deg\ s' = deg\ s$ and $deg\ t' = deg\ t$.