CS 681: Computational Number Theory and Algebra **Lecture 17**
Lecturer: Manindra Agrawal **Notes by: Ashwini Aroskar**

September 15, 2005.

1 Hensel Lifting

Let R be a unique factorization domain.
e.g. $R = Z$, the ring of integers; or $R = F[x]$, F is a field.

Let $f(y) \in R[y]$.
Let $m \in R$.

Suppose we know $f = gh (\text{mod } m)$ and s and t are such that $sg + th = 1(mod\ m)$.
Then, Hensel Lifting efficiently computes $f = g^{'}h^{'} (\text{mod } m^2)$ and $s^{'}$, $t^{'}$,
such that, $s^{'}g^{'} + t^{'}h^{'} = 1(\text{mod } m^2)$,
and $g^{'} = g(\text{mod } m)$ & $h^{'} = h(\text{mod } m)$.

Let $e = f - gh(\text{mod } m^2)$.

Assume $e \neq 0$. [If $e = 0$, then we need not use Hensel Lifting.]

Let $g^{'} = g + te(\text{mod } m^2)$
& $h^{'} = h + se(\text{mod } m^2)$

$$\begin{aligned} g^{'}h^{'}(mod m^2) &= (g + te)(h + se)(\text{mod } m^2) \\ &= gh + (sg + th)e + ste^2(\text{mod } m^2) \\ &= gh + (1 + m\mu)e(\text{mod } m^2) \quad \text{as } e|m \\ &= gh + e(\text{mod } m^2) \\ &= f(\text{mod } m^2) \end{aligned}$$

Let $d = sg^{'} + th^{'} - 1(\text{mod } m^2)$
Note that $d = 0(\text{mod } m)$ as $g^{'} = g(\text{mod } m)$ & $h^{'} = h(\text{mod } m)$
Let $s^{'} = s(1 - d)(\text{mod } m^2)$
and $t^{'} = t(1 - d)(\text{mod } m^2)$

$$\begin{aligned} s'g' + t'h' &= s(1-d)g' + t(1-d)h' (\text{mod } m^2) \\ &= (sg' + th')(1-d)(\text{mod } m^2) \\ &= (1+d)(1-d)(\text{mod } m^2) \\ &= 1 - d^2 (\text{mod } m^2) \\ &= 1 (\text{mod } m^2) \end{aligned}$$

Remark : As described above, $\deg g'$ or $\deg h'$ can exceed $\deg f$, while $f = g'h' (\text{mod } m^2)$. So the degrees of factors can keep increasing at every iteration, which is undesirable. This problem can be resolved, as we shall see later.

2 Polynomial Division

Given f, g of degree n and m respectively, compute q and r such that $f = qg + r$ with $\deg r < m$.

Obvious Time Complexity = $\bigcirc(nm)$ (using long division)

Let $\hat{f} = x^n f(\frac{1}{x})$.

So, $x^n f(\frac{1}{x}) = x^n [q(\frac{1}{x}) g(\frac{1}{x}) + r(\frac{1}{x})]$
$\hat{f}(x) = \hat{q}(x)\hat{g}(x) + x^{n-\deg r}\hat{r}(x)$ and $n - \deg r \geq n - m + 1$
$\hat{f}(x) = \hat{q}(x)\hat{g}(x)(\text{mod } x^{n-m+1})$

Now the constant term of $\hat{g}(x)$ is the leading coefficient of $g(x)$ and hence non-zero. So, $\hat{g}(x)$ has an inverse modulo x^{n-m+1}.
So, $\hat{q}(x) = \hat{f}(x)\hat{g}^{-1}(x)(\text{mod } x^{n-m+1})$

Problem: To compute $\hat{g}^{-1}(x)$ from $g(x)$ (mod x^{n-m+1})

Let $\hat{g}h = 1(\text{mod } x)$.
So, h =a constant, the inverse of the leading coefficient of g.
Let $s = h$ and $t = 0$. So, $s\hat{g} + th = 1(\text{mod } x)$.

Note that, $\hat{g}' = g$ and $t' = 0$ as $t = 0$. Hence, $\hat{g}$ and t remain unchanged for every application of Hensel lifting.
Eventually we get $\hat{g}\tilde{h} = 1(\text{mod } x^{2^k})$ with $2^k \geq n - m + 1$

Once we obtain $\hat{g}^{-1}(x) = \tilde{h}(x)$, we can get $\hat{q}(x)$ & $q(x)$ and then compute $r(x)$.

At the i^{th} step, we carry out a constant number of additions and multiplications (using FFT) of polynomials of deg $< 2^i$ and also quotient polynomials (mod x^{2^i})

Time complexity $= \bigcirc(\sum_{i=1}^{\log n} 2^i i) + \bigcirc(n \log n) = \bigcirc(n \log n)$

Note that we started with $m = x$ for Hensel lifting in this case, but $x \notin R$. But this lifting is valid because of our choice of $t = 0$.