Lec16 A Hensel's Lemma

March 11, 2021 1:14 PM

Assignment #4 is due on Monday @ 11pm.

6.4 Hensel's Lemma (Kurt Hensel 1861–1941)

Problem: Given $f \in \mathbb{Z}[x][u,w]$ solve $f(u,w)=0$ for $u,v \in \mathbb{Z}[x]$.

Example: $f(u,w) = a - u\cdot w$ where $a \in \mathbb{Z}[x]$.

GCD: $a,b \in \mathbb{Z}[x]$, $g=\gcd(a,b) \Rightarrow a = g\bar{a} \Rightarrow \underbrace{a - \underset{\uparrow\, u}{g}\cdot\underset{\uparrow\, w}{\bar{a}} = 0}_{f}$

FACTOR: $a = f_1 f_2 \cdots f_n \Rightarrow a - \underset{\uparrow\, u}{f_1}\underbrace{f_2\cdots f_n}_{\uparrow\, w} = 0$

Since $u,w \in \mathbb{Z}[x]$ $\exists!\ u_0,u_1,\dots,u_{n-1} \in \mathbb{Z}_p[x]$ s.t. $u = u_0 + u_1 p + \dots + u_{n-1}p^{n-1}$.
$\exists!\ w_0,w_1,\dots,w_{n-1} \in \mathbb{Z}_p[x]$ s.t. $w = w_0 + w_1 p + \dots + w_{n-1}p^{n-1}$.

① Find $u_0,w_0 \in \mathbb{Z}_p[x]$ s.t. $a - u_0 \cdot w_0 \equiv 0 \pmod p$.

② Given $u^{(k)} = u_0 + u_1\cdot p + \dots + u_{k-1}p^{k-1}$ where $u_i \in \mathbb{Z}_p[x]$ and
$w^{(k)} = w_0 + w_1 p + \dots + w_{k-1}p^{k-1}$ where $w_i \in \mathbb{Z}_p[x]$ s.t.
$$f(u^{(k)},w^{(k)}) = a - u^{(k)}\cdot w^{(k)} \equiv 0 \pmod{p^k}.$$
find $u^{(k+1)} = u^{(k)} + u_k p^k$ and $w^{(k+1)} = w^{(k)} + w_k p^k$ s.t.
$u_k, w_k \in \mathbb{Z}_p[x]$ and $a - u^{(k+1)}\cdot w^{(k+1)} \equiv 0 \pmod{p^{k+1}}$.

③ Stop "lifting" when $f(u^{(n)},w^{(n)}) = a - \underline{u^{(n)}}\cdot\underline{w^{(n)}} = 0$ over $\mathbb{Z}$.
or we exceed some bound. a factorization of a.

$$a - (u^{(k)} + u_k p^k)\cdot(w^{(k)} + w_k p^k) \equiv 0 \pmod{p^{k+1}}.$$

$$\Rightarrow a - u^{(k)}w^{(k)} - u_k p^k w^{(k)} - w_k p^k u^{(k)} - u_k w_k p^{2k} \equiv 0 \pmod{p^{k+1}}$$

$$\Rightarrow \underbrace{a - u^{(k)}w^{(k)}}_{e_k} - [u_k w^{(k)} + w_k u^{(k)}]\cdot p^k \equiv 0 \pmod{p^{k+1}}.\ k \geq 1.$$

$$/p^k \Rightarrow \frac{e_k}{p^k} - u_k \underset{w_0 + w_1 p + \cdots}{\underset{\parallel}{w^{(k)}}} - w_k \underset{u_0 + u_1 p + \cdots}{\underset{\parallel}{u^{(k)}}} \equiv 0 \pmod p.$$

$$\Rightarrow \frac{e_k}{p^k} - u_k w_0 - w_k u_0 \equiv 0 \pmod p.$$

$$\Rightarrow \underbrace{u_k\, w_0}_{\in\, \mathbb{Z}_p[x]} + \underbrace{w_k\, u_0}_{\in\, \mathbb{Z}_p[x]} = \phi_p\left[\frac{e_k}{p^k}\right] = c_k \in \mathbb{Z}_p[x]$$

This is a polynomial diophantine equation of the form

This is a polynomial diophantine equation of the form

$$\sigma w_0 + \tau u_0 = c_k \quad \text{in } \mathbb{Z}_p[x].$$

Th 2.6 says it has a solution iff $\gcd(w_0,u_0) \mid c_k$.
We will require $\gcd(w_0,u_0)=1$. Hence, we solve.

Solve $\quad s\cdot \underline{w_0} + t\cdot \underline{u_0} = 1$ for s,t using the EEA in $\mathbb{Z}_p[x]$.

$$\Rightarrow (c_k s) w_0 + (c_k t)\cdot u_0 = c_k$$

$c_k s \div u_0$ Let $c_k s = \boxed{q\cdot u_0 + r}$ with $r=0$ or $\deg(r)<\deg(u_0)$

$$\Rightarrow \underbrace{r}_{u_k=\sigma} w_0 + (\underbrace{c_k t + q w_0}_{w_k=\tau}) u_0 = c_k \quad \text{with } \deg\sigma < \deg(u_0)$$

Theorem 6.2 Hensel's Lemma (in $\mathbb{Z}[x]$).

Let $a \in \mathbb{Z}[x]$, $a \neq 0$, p be a prime.
Let $u_0, w_0 \in \mathbb{Z}_p[x]$ s.t. $a - u_0 w_0 \equiv 0 \pmod p$
If $\gcd(u_0,w_0)=1$ then $\forall n \in \mathbb{N}$ $\exists$ $u^{(n)}, w^{(n)} \in \mathbb{Z}_{p^n}[x]$ s.t.
$a - u^{(n)}\cdot w^{(n)} \equiv 0 \pmod{p^n}$ and $u^{(n)} \equiv u_0 \pmod p$ and $w^{(n)} \equiv w_0 \pmod p$.

The solutions $u^{(n)}$ and $w^{(n)}$ are unique upto $\times$ by a scalar in $\mathbb{Z}^*_{p^n}$
because
$$a - (s\,u^{(k)})(s^{-1} w^{(k)}) \equiv 0 \pmod{p^k}$$

Leading Coefficient Problem 6.6

Suppose we want to factor

$$a = 16x^2 + 58x + 7 = (\overset{u}{2x+7})(\overset{w}{8x+1})$$

$p=5$ $\quad \underset{a}{a} \equiv 1\cdot x^2 + 3x + 2 \pmod 5 = \underset{u_0}{(x+1)}\underset{w_0}{(x+2)} \Rightarrow a - u_0 w_0 \equiv 0 \pmod p$.

Let $u_0 = x+1$, $w_0 = x+2$. $\gcd(u_0,w_0)=1$
$u^{(1)} = 1\cdot x + 1 \quad w^{(1)} = 1\cdot x + 2$

$$e_1 = a - u^{(1)}\cdot w^{(1)} = 16x^2 + 58x + 7 - (x^2 + 3x + 2)$$
$$= 15x^2 + 55x + 5.$$

$$c_1 = \left(\frac{e_1}{p}\right) \bmod p = 3\cdot x^2 + 11\cdot x + 1 = 3x^2 + x + 1. \bmod 5.$$

Solve $\quad \sigma\cdot \overset{w_0}{(x+2)} + \tau\cdot \overset{u_0}{(x+1)} = 3x^2 + x + 1$ in $\mathbb{Z}_5[x]$.

$\deg(\sigma) < \deg(u_0) = 1$

Solve $\overset{=}{\underset{-2}{\sigma}} \cdot \overset{w_0}{(x+2)} + \overset{=}{\underset{-2x}{\tau}} \cdot \overset{u_0}{(x+1)} = 3x^2+x+1$ in $\mathbb{Z}_5[x]$.

$\deg(\sigma) < \deg(u_0) = 1$

$u_1 = -2 \qquad w_1 = -2x.$

$$u^{(2)} = \overset{u_0}{1\cdot x+1} + \overset{u_1 \cdot p}{(-2)\cdot 5} = 1\cdot x - 9.$$
$$w^{(2)} = \overset{w_0}{x+2} \overset{+\ w_1 \cdot p}{-2x\cdot 5} = -9\cdot x+2.$$
$\Rightarrow a - u^{(2)} \cdot w^{(2)} \equiv 0 \pmod{25}.$

$$e_2 = a - u^{(2)} \cdot w^{(2)} = 16x^2+58x+7 - [-9x^2+83x-18]$$
$$= 25x^2 - 25x + 25$$
$$c_2 = \left(\frac{e_2}{25}\right) \bmod 5 = 1\cdot x^2 - x + 1.$$

Solve $\underset{-2 = u_2}{\sigma} \overset{w_0}{(x+2)} + \underset{x = w_2}{\tau} \overset{u_0}{(x+1)} = \overset{c_2}{x^2 - x + 1}$ in $\mathbb{Z}_5[x]$.

$\deg(\sigma) < \deg(u_0) = 1.$

$$u^{(3)} = u^{(2)} + u_2 \cdot 25 = (x-9) - 2\cdot 25 = 1\cdot x - 59. \neq 2x+7 \mod 125$$
$$w^{(3)} = w^{(2)} + w_2 \cdot 25 = (-9x+2) + x\cdot 25 = 16\cdot x - 2 \neq 8x+1 \mod 125$$
$\div 2$

$$a - \underset{\times 2}{u^{(3)}} \cdot \underset{\div 2}{w^{(3)}} \equiv 0 \pmod{125}.$$

$$2\cdot(1\cdot x - 59) = 2x - 118 \mod 125$$
$$= 2x+7$$

$\deg \sigma < \deg u_0 = 1 \Rightarrow \deg u_k < 1 \Rightarrow \mathrm{lc}\, u^{(n)}$ is never updated.

What we are computing is this solution.

$$a - \left(\frac{\overset{u}{2x+7}}{\underset{\substack{\uparrow \\ \text{monic.}}}{2}}\right)\left(2\left(\overset{w}{8x+1}\right)\right) \equiv 0 \pmod{p^k}.$$

$a = 16x^2 + 58x + 7 = (2x+7)(8x+1)$

Let $\alpha = \mathrm{lc}(a) = 16$. Solve $\alpha a - uw = 0$ for u, w with $\mathrm{lc}(u) = \mathrm{lc}(w) = \alpha$.

E.g. $16a - \left(8\overset{u}{(2x+7)}\right)\left(2\overset{w}{(8x+1)}\right)$

$$= \underline{16x+56} = \underline{16x+2}$$

Output $pp(u)$ and $pp(w)$.

We will require $\mathrm{cont}(a) = 1$.