Lec 15C The Linear x-adic Newton iteration

March 8, 2021 10:12 PM

Assignment #4 Q1 Q4

$$
\begin{tikzcd}
a = 49x^2 - 56x + 16 \arrow[rr] \arrow[d, "\phi_{x=\alpha}"'] & & \sqrt{a} \in \mathbb{Z}[x] = \pm(7x-4) \\
a(1000) = 48944016 \arrow[rr, "\sqrt{48944016} \in \mathbb{Z}"] \arrow[d, "\phi_p"'] & & \pm 6996 \arrow[u, "\text{genpoly}"'] \\
a(\alpha) \bmod p = 1 \in \mathbb{Z}_p \arrow[rr, "\sqrt{\ } \text{ in } \mathbb{Z}_p\ ?"', "\text{Factor } 1-x^2 \text{ over } \mathbb{Z}_p"] & & u_0 = \pm 1 \arrow[u]
\end{tikzcd}
$$

?

$\alpha > 2\|\sqrt{a}\|_\infty$, $\alpha = B^k$

$\alpha = 1000$

$p = 5$

$= \pm(7 \cdot 1000 - 4)$

$= \pm 7000 - 4$

① Linear p-adic lift

$u = u_0 + u_1 \cdot p + u_2 \cdot p^2 + \cdots$

$-\frac{p}{2} < u_i < \frac{p}{2}$

$$
\begin{tikzcd}
a = 49x^2 - 56x + 16 \arrow[rr] \arrow[d, "\phi_p"'] & & \sqrt{a} = \pm(7x-4) \\
a_p = 4x^2 + 4x + 1 \in \mathbb{Z}_5[x] \arrow[rr, "\sqrt{\ } \text{ in } \mathbb{Z}_5[x]"] \arrow[d, "\phi_{x=\alpha}"'] & & u_0 = \pm(2x+1) \arrow[u] \\
a_p(0) = 1 \arrow[rr, "\sqrt{\ } \text{ in } \mathbb{Z}_p"] & & u_0 = \pm 1 \arrow[u]
\end{tikzcd}
$$

$p = 5$

$\alpha = 0.$

Linear p-adic lift

$u = u_0 + u_1(x)p + u_2(x)p^2 + \cdots$

② Linear x-adic lift

$u = u_0 + u_1(x-\alpha) + u_2(x-\alpha)^2 + \cdots$

where $u_i \in \mathbb{Z}_p$.

① $u_k = \dfrac{e_k}{p^k} / (2u_0) \bmod p$ where $e_k = a - u^{(k)^2}$

② $u_k = \dfrac{e_k}{(x-\alpha)^k} / (2u_0) \bmod (x-\alpha)$ where $e_k = a - u^{(k)^2}$

Example $a = 4x^2 + 4x + 1 \in \mathbb{Z}_5[x]$

$\alpha = 0$ $u = u_0 + u_1(x-\alpha) = \underline{u_0} + \underline{u_1} \cdot x$

$u_0 = 1.$ $u^{(1)} = u_0 = 1$ $1/2u_0 = 1/2 = 3 \bmod 5.$

$= \underline{u_0} + \underline{u_1} x$

$$u_0 = 1. \qquad u^{(1)} = u_0 = 1 \qquad 1/2u_0 = 1/2 = 3 \bmod 5.$$

$$e_1 = a - u^{(1)2} = (4x^2+4x+1) - (1)^2 = 4x^2+4x.$$

$$u_1 = \left(\frac{e_1}{x-0}\right)/(2u_0) \mod (x-0)$$

$$= (4x+4)\cdot 3 \mod x$$

$$\simeq 12x+12 \mod x \mod 5$$

$$= 2x+2 \mod x$$

$$= 2$$

$$u^{(2)} = u_0 + u_1 \cdot x = 1 + 2\cdot x$$

Ex. Repeat using $u_0 = -1$. .... $u^{(2)} = -1-2x$.

Theorem 28 Let $\overset{= \mathbb{Z}[x]}{D}$ be an integral domain, and $\overset{= a(x) - u^2}{f \in D[u]}$

Then $\exists\, g \in D[u,y]$ s.t.

$$f(u+y) = f(u) + f'_u(u)\cdot y + g(u,y)\cdot y^2$$

Proof. $f(\overset{D[u]}{\overset{\in}{u+y}}) \in D[u,y]$ because f is a polynomial

$$\Rightarrow f(u+y) = a_0(u) + a_1(u)\cdot y + \underbrace{a_2(u)\cdot y^2 + \dots + a_n(u)\cdot y^n}$$

for some $n \geq 0$ and some $a_i \in D[u]$.

$$\Rightarrow f(u+y) = \underset{f(u)}{\underset{\parallel}{a_0(u)}} + \underset{f'_u(u)}{\underset{\parallel}{a_1(u)}}\cdot y + y^2 g(u,y) \text{ for some } g \in D[u,y]. \ (1)$$

(1) $y=0$ $\Rightarrow f(u) = a_0(u) + 0.$

$$\frac{\partial}{\partial y} f(u+y) \overset{C.R.}{=} f'_u(u+y)\cdot \frac{\partial (u+y)}{\partial y} = f'_u(u+y)\cdot 1.$$

$$\frac{\partial}{\partial y} RHS(1) = 0 + a_1(u) + 2y\, g(u,y) + y^2 \cdot \square.$$

$$\Rightarrow f'_u(u+y) = a_1(u) + y\cdot\triangle \text{ for some } \triangle \in D[u,y]$$

$$\underset{y=0}{\Rightarrow} f'_u(u) = a_1(u) + 0.$$