Lec14B A p-adic Newon iteration Michael Monagan

March 4, 2021 1:43 PM

6.3 The Linear p-adic Newton iteration

Let $a \in \mathbb{Z}$, $a > 0$, $u = \sqrt{a}$. Suppose $u \in \mathbb{Z}$.

Let $f(x) = a - x^2 \in \mathbb{Z}[x]$.

To compute u we want to solve $f(u) = 0$ for $u \in \mathbb{Z}$.

Let p be an odd prime and let

$$u = \underbrace{u_0 + u_1 p + \cdots + u_{k-1}p^{k-1}}_{u^{(k)}} + u_k p^k + \cdots + u_{n-1}p^{n-1} \quad \text{with } -\frac{p}{2} < u_i < \frac{p}{2}.$$

$u^{(k)}$ a k'th order approximation to u.

$f(u^{(k)}) \equiv 0 \pmod{p^k}$. i.e. $a - (u^{(k)})^2 \equiv 0 \pmod{p^k}$.

① Solve $a - x^2 \equiv 0 \bmod p$ for $x = u_0 \Rightarrow u^{(1)} = u_0$ (a first order approx. to u).

Factor $a - x^2 = (a-\alpha)(a-\beta)$. in $\mathbb{Z}_p[x]$?? Ch. 8.

② Given $u^{(k)}$ s.t. $f(u^{(k)}) \equiv 0 \pmod{p^k}$ $k \geq 1$. $\Rightarrow p^k \mid f(u^{(k)})$.

find $u^{(k+1)} = u^{(k)} + u_k p^k$ s.t. $f(u^{(k+1)}) \equiv 0 \pmod{p^{k+1}}$.

$$f(u^{(k+1)}) = f(u^{(k)} + u_k p^k) = a - (u^{(k)} + u_k p^k)^2$$

$$= \underbrace{a - u^{(k)2}}_{f(u^{(k)})} - 2u^{(k)}u_k p^k - u_k^2 p^{2k}$$

$$f(u^{(k+1)}) = f(u^{(k)}) - 2u^{(k)}u_k p^k - u_k^2 p^{2k}. \qquad k \geq 1.$$

$\bmod p^{k+1}$ $\quad \| \quad 0$

$$0 \equiv f(u^{(k)}) - 2u^{(k)}u_k p^k - 0 \pmod{p^{k+1}}.$$

$\div p^k \Rightarrow$ $\quad 0 \equiv \dfrac{f(u^{(k)})}{p^k} - 2u^{(k)}u_k \pmod{p}$ $\quad u^{(k)} = u_0 + u_1 p + \cdots + u_{k-1}p^{k-1}$

$$u_k = \left(\frac{f(u^{(k)})}{p^k}\right) / (2u_0) \pmod{p}.$$

$$u_k = \left(\frac{a - u^{(k)2}}{p^k}\right) / (2u_0) \Rightarrow p \neq 2 \text{ and } u_0 \neq 0.$$

Let $e_k = a - u^{(k)2}$ be the error in $u^{(k)}$.

$$\boxed{u_k = \left(\frac{e_k}{p^k}\right) / (2u_0) \bmod p}$$

③ Stop? when $a - u^{(n)2} = 0 \Rightarrow \sqrt{a} = \pm u^{(n)}$

$\sqrt{21} \notin \mathbb{Z}$ but $\sqrt{21}$ in $\mathbb{Z}_5$ $\sqrt{1} = \pm 1$.

Stop when $p^k > 2\lceil\sqrt{a}\rceil \Rightarrow$ Need a bound $B > \sqrt{a}$.

Example. $\sqrt{49}$ $\quad 49 < 100 \quad \sqrt{49} < \sqrt{100} = 10 = B$.

$p = 5$ ① Solve $49 - x^2 \equiv 0 \bmod 5$

$4 - x^2 \equiv 0 \bmod 5 \quad x = \pm 2$.

② $u_0 = 2 \quad u^{(1)} = u_0 = 2$.

$e_1 = f(u^{(1)}) = 49 - 2^2 = 45 \neq 0$

$u_1 = \frac{e_1}{p} / (2u_0) \quad \frac{45}{5} / (4)$

$4^{-1} \equiv 4 \bmod 5$ $\quad = 9 \cdot 4 \bmod 5$

$= 1$.

$u^{(2)} = u_0 + u_1 p = 2 + 1 \cdot 5 = 7$.

$e_2 = f(u^{(2)}) = 49 - 7^2 = 0$.

Stop. $u = 7$

$u_0 = -2$ $\quad -2 \leq u_i \leq 2$

$e_1 = 49 - (-2)^2 = 45$

$u_1 = \frac{45}{5} / (-4) = 9 \cdot 1 \bmod 5$

$= -1$

$u^{(2)} = u_0 + u_1 p = -2 - 1 \cdot 5 = -7$

$e_2 = 49 - (-7)^2 = 0$.

Let $a \in \mathbb{Z}[x]$. $\quad \sqrt{a} \in \mathbb{Z}[x]$? $\quad \sqrt{x+1} \notin \mathbb{Z}[x]$

If yes compute $\quad \sqrt{x^2+2x+1} = \pm(x+1) \in \mathbb{Z}[x]$.

Eg. $a = x^3 + 6x^2 + 9x + 5$.

$a(x) = x^4 - 14x^3 + 53x - 28x + 4 \longrightarrow$

$\phi_{x=\alpha}$ $\quad \alpha \geq 2\|\sqrt{a}\|$

$\alpha = B^k \quad 1000$

$a(1000) = 9860529\,2004 \xrightarrow{\sqrt{\ } \text{in } \mathbb{Z}?} \sqrt{a(1000)} = \pm 993\,002$.

$1 \cdot 1000^2 - 7 \cdot 1000 + 2$

$\pm(1 \cdot x^2 - 7x + 2)$ gcdpoly

ϕ_p $\quad p = 5$

N.I.

$a(1000) \bmod 5 = 4$ $\quad \sqrt{4}$ in $\mathbb{Z}_5$ $\quad \pm 2$

Must choose p s.t. $a(\alpha) \not\equiv 0 \bmod p$ so that $u_0 \neq 0$.

If $p \mid a(\alpha)$ is a bad prime.

Take $a = x^3 + 6x^2 + 9x$ and $\alpha = 10{,}000$.

$a(10{,}000) = (100030000^2 \xrightarrow{\text{gcdpoly}} 100 \cdot x + 300$ which is not $\sqrt{a}$.

Check if $a - u^2 = 0$

If $a \neq u^2$ we say α is an unlucky evaluation point.