Lec 15A The linear p-adic Newton iteration

March 2, 2021 1:48 PM

Let $a \in \mathbb{Z}[x]$ and let $u = \sqrt{a}$.
Is $u \in \mathbb{Z}[x]$? If yes how can we compute u?

$a = 49x^2 - 56x + 16$ —? factor $a \in \mathbb{Z}[x]$→ $u = \sqrt{a} \in \mathbb{Z}[x]$ $\pm(7x-4)$ (u)

ϕ_p ↓ p odd prime, $p=5$

Linear p-adic N.I. in $\mathbb{Z}_p[x]$

$a_5 = 4x^2+4x+1 \in \mathbb{Z}_5[x]$ —factor as in $\mathbb{Z}_5[x]$→ $u_0 = \sqrt{a_p} = \pm(2x+1)$

Theorem 2. Let $u, p \in \mathbb{Z}$, $p \geq 3$. If $-\frac{p^n}{2} < u < \frac{p^n}{2}$ then $\exists$ unique integers $u_0, u_1, \ldots, u_{n-1}$ s.t. $u = u_0 + u_1 \cdot p + \cdots + u_{n-1}p^{n-1}$ and $-\frac{p}{2} < u_i < \frac{p}{2}$.

Suppose $u(x) \in \mathbb{Z}[x]$ and p an odd prime.
Let $u(x) = \sum_{i=0}^{m} a_i x^i$ where $-\frac{p^n}{2} < a_i < \frac{p^n}{2}$

$$= \sum_{i=0}^{m}\left[\sum_{j=0}^{n-1} u_{ij} p^j\right] \cdot x^i = \sum_{j=0}^{n-1}\left[\sum_{i=0}^{m} u_{ij} \cdot x^i\right] p^j$$

$u_i(x) \in \mathbb{Z}_p[x]$

Example. $u = 7x-4$ $p=5$.

$u_0 = 2x+1 \mod 5$
$u \leftarrow (u-u_0)/p = (5x-5)/5 = x-1.$
$u_1 = x-1 \mod 5 = 1x-1.$
$u \leftarrow (u-u_1)/p = 0$ STOP.

$u = \underbrace{2x+1}_{u_0} + \underbrace{(1x-1)}_{u_1} \cdot 5$

Linear p-adic Newton update formula

Let $f(u) \in \mathbb{Z}[x][u]$ (e.g. $f(u) = a - u^2$ where $a \in \mathbb{Z}[x]$)
satisfying $f(u_0) \equiv 0 \pmod p$. Find $\bar{u} \in \mathbb{Z}[x]$ s.t. $f(\bar{u}) = 0$.
Let $\bar{u} = u_0 + u_1 \cdot p + \cdots + u_{k-1}p^{k-1} + u_k p^k + \cdots + u_{n-1}p^{n-1}$ where $u_i \in \mathbb{Z}_p[x]$.
Define $u^{(k)} = u_0 + u_1 \cdot p + \cdots + u_{k-1}p^{k-1}$ is called a k'th order approx. to $\bar{u}$ if $f(u^{(k)}) \equiv 0 \pmod{p^k}$
Given $u^{(k)}$ find $u^{(k+1)} = u^{(k)} + u_k \cdot p^k$ s.t. $f(u^{(k+1)}) \equiv 0 \pmod{p^{k+1}}$

Theorem 28 If $f(u) \in \mathbb{Z}[x][u]$, $\exists\, g(u,v) \in \mathbb{Z}[x][u,v]$ s.t.

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

remainder term.

$$f(u^{(k+1)}) = f(\overbrace{u^{(k)}}^{u} + \overbrace{u_k p^k}^{v})$$

$$= f(u^{(k)}) + f_u'(u^{(k)})\cdot u_k p^k + g(u^{(k)}, u_k p^k)\cdot u_k^2 p^{2k} \quad \text{for } k \geq 1.$$

$\pmod{p^{k+1}}$

$$0 = f(u^{(k)}) + f_u'(u^{(k)})\cdot u_k \cdot p^k + 0 \pmod{p^{k+1}}$$

$$\Rightarrow p^{k+1} \mid f(u^{(k)}) + f_u'(u^{(k)})\cdot u_k \cdot p^k$$

$$\Rightarrow p \mid \frac{f(u^{(k)})}{p^k} + f_u'(u^{(k)})\cdot u_k$$

$$\Rightarrow \frac{f(u^{(k)})}{p^k} + f_u'(u^{(k)})\cdot u_k \equiv 0 \pmod{p}.$$

$$\Rightarrow u_k = -\phi_p\left(\frac{f(u^{(k)})}{p^k}\right) \Big/ \left[\phi_p(f_u'(u^{(k)})) = f_u'(\phi_p(u^{(k)}))\right]$$

$$\phi_p\left(u^{(k)} = u_0 + u_1 p + \cdots + u_{k-1}p^{k-1}\right) = u_0$$

$$\Rightarrow u_k = -\phi_p(\quad) / \phi_p(f_u'(u_0)) \quad \text{in } \mathbb{Z}_p[x]$$

If $f(u) = a - u^2$ then $f_u'(u) = -2u$ so

$$u_k = -\phi_p\left(\frac{\overbrace{a - u^{(k)^2}}^{e_k}}{p^k}\right) \Big/ (-2u_0)$$

$u_0 \neq 0$, $p \neq 2$.

$$u_k = \phi_p\left(\frac{e_k}{p^k}\right) / (2u_0) \in \mathbb{Z}_p(x).$$

u_k: Linear p-adic update.

polynomial division must work if $\sqrt{a} \in \mathbb{Z}[x]$.

$$\begin{array}{r|l} -x^2-2x-2 & -x+2 \\ -(-x^2+2x) & x-1 \\ \hline -x-2 & \\ -(-x-2) & \\ \hline 0 & \end{array}$$

Example. $u = \sqrt{49x^2 - 56x + 16} = \pm(7x-4)$.

$p = 5$

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

$e_1 = a - u^{(1)^2} = (49x^2 - 56x + 16) - (2x+1)^2 = 45x^2 - 60x + 15$

$u_1 = \phi_5\left(\left(\frac{e_1}{p}\right)/(2u_0)\right) = \phi_5\left(\frac{9x^2 - 12x + 3}{-x+2}\right) = \frac{-x^2-2x-2}{-x+2} = x-1$

$\mathbb{Z}_5[x]$.

$u^{(2)} = u_0 + u_1 \cdot p = 2x+1 + (x-1)\cdot 5 = 7x-4.$

$e_2 = (a - u^{(2)^2}) = (49x^2 - 56x + 16) - (7x-4)^2 = 0$ STOP.

Exercise. Start with $u_0 = -2x-1$. You should get $u^{(2)} = -7x+4$.