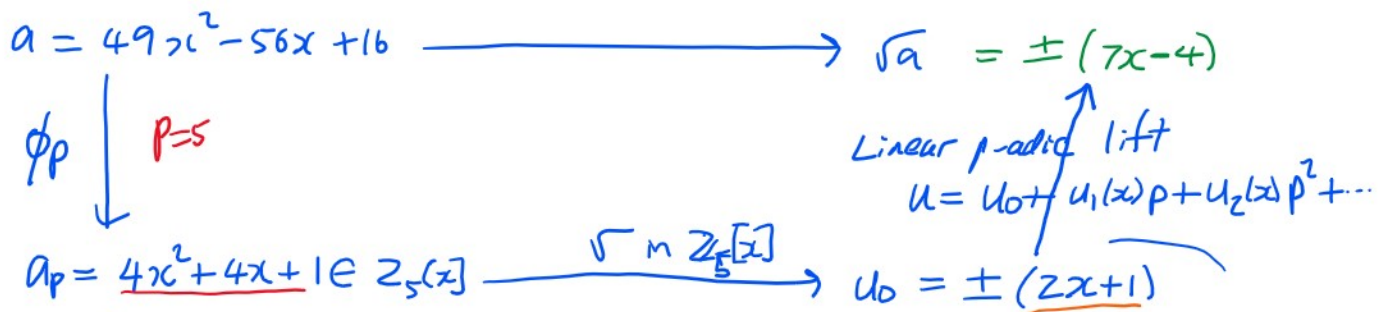
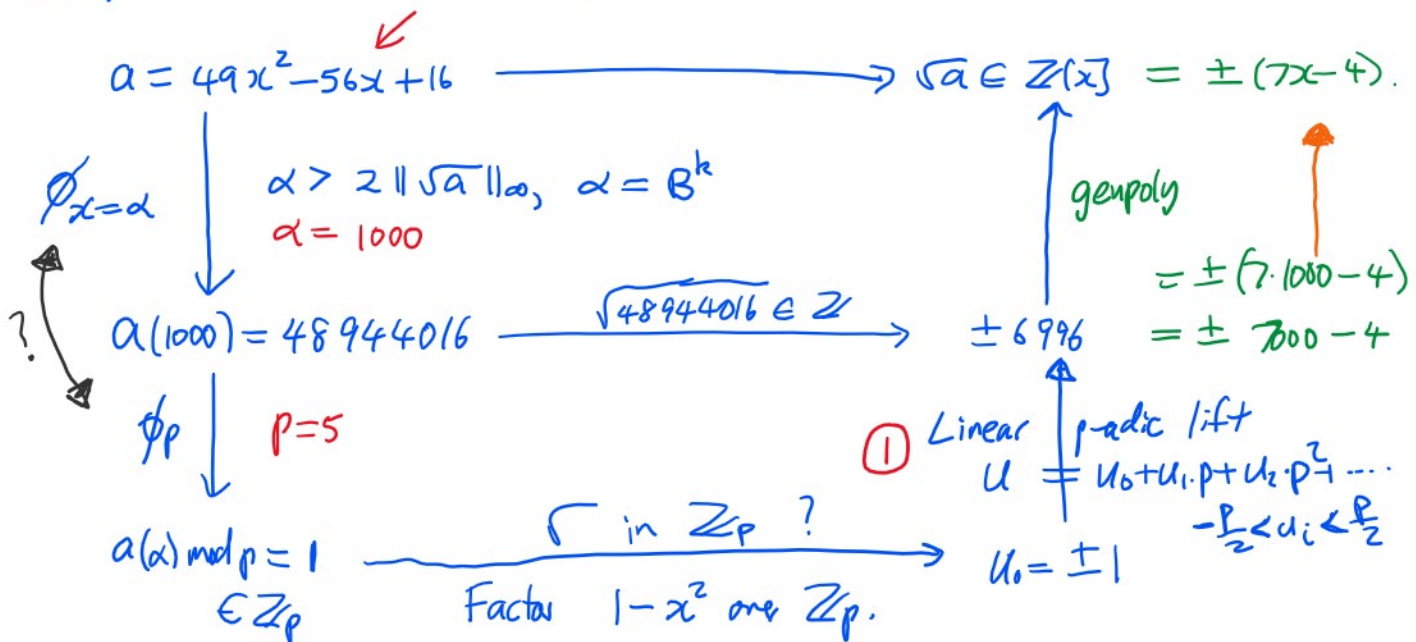


Lec 15C The Linear x-adic Newton iteration

March 8, 2021 10:12 PM

Assignment #4  $\mathbb{Q}_1$   $\mathbb{Q}_4$



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

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

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

$\alpha = 0$   $u = u_0 + u_1(x-\alpha) = u_0 + u_1 x$

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

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

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

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

$$= (4x+4) \cdot 3 \pmod{x}$$

$$\cong 12x+12 \pmod{x} \pmod{5}$$

$$= 2x+2 \pmod{x}$$

$$= 2$$

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

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

Theorem 28 Let  $D \stackrel{=}{=} \mathbb{Z}[x]$  be an integral domain, and  $f \in D[u] \stackrel{=}{=} a(x) - u^2$ .  
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.  $f(u+y) \in D[u, y]$  because  $f$  is a polynomial

$$\Rightarrow f(u+y) = a_0(u) + a_1(u) \cdot y + \underbrace{a_2(u) \cdot y^2 + \dots + a_n(u) \cdot y^n}_{\text{for some } n \geq 0 \text{ and some } a_i \in D[u].}$$

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

$$(1) y=0 \Rightarrow \begin{matrix} f(u) = a_0(u) + 0. \\ \frac{\partial}{\partial y} f(u+y) \stackrel{\text{C.R.}}{=} f'_u(u+y) \cdot \frac{\partial (u+y)}{\partial y} = f'_u(u+y) \cdot 1. \end{matrix}$$

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

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

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