Ex. 1 (exam), algo. and proof that it converge

1) $a \in \mathbb{R}_+^*$, we want to compute $\sqrt{a}$,

$\sqrt{a}$ is a solution of the equation

$f(x) = 0$ with $f(x) = x^2 - a$.

Newton iteration.

$$x_0 > 0$$

$$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)} = x_k - \frac{x_k^2 - a}{2x_k}$$

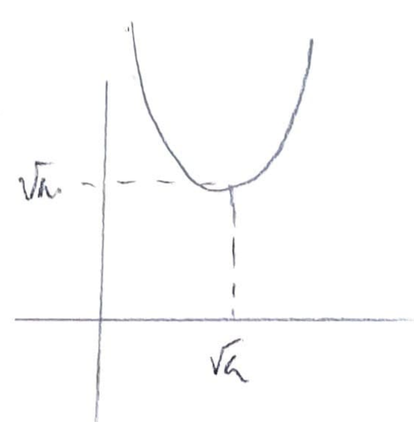
$$= \frac{1}{2}\left(x_k + \frac{a}{x_k}\right)$$

2) let us define $g(x) = \frac{1}{2}\left(x + \frac{a}{x}\right)$

We have $x_{k+1} = g(x_k)$

$$g'(x) = \frac{1}{2}\left(1 - \frac{a}{x^2}\right)$$

x	0		$\sqrt{a}$		$+\infty$
$g'(x)$	$\|\|$	$-$	0	$+$	
$g(x)$	$-\infty$	$\searrow$	$\sqrt{a}$	$\nearrow$	$+\infty$



$x_0>0$. For any $k\geq 1$, $x_k\geq\sqrt{a}$ and $x_k>0$

$$x_{k+1}-x_k=\frac{1}{2}\left(x_k+\frac{a}{x_k}\right)-x_k=\frac{a}{2x_k}-\frac{1}{2}x_k=\frac{a-x_k^2}{2x_k}\leq 0$$

So the sequence (x_k) is decreasing and lower banded by $\sqrt{a}$. So (x_k) is convergent.

Let $x_k\to l$. Then as $x_{k+1}=g(x_k)$ and the fact that g is continuse then by taking the limit we have $l=g(l)$ and so,

$$l=\frac{1}{2}\left(l+\frac{a}{l}\right)\iff l=\sqrt{a}\text{ as } l>0.$$

3) $$x_{k+1}-\sqrt{a}=\frac{1}{2}\left(x_k+\frac{a}{x_k}\right)-\sqrt{a}.$$

$$=\frac{1}{2}\left(\frac{x_k^2+a-2\sqrt{a}x_k}{x_k}\right)=\frac{1}{2x_k}\left(x_k-\sqrt{a}\right)^2$$

As $x_k\geq\sqrt{a}$, we have

$$|x_{k+1}-\sqrt{a}|\leq\underbrace{\frac{1}{2\sqrt{a}}}_{\text{constant}}|x_k-\sqrt{a}|^2$$

this means we have a quadreic convergent.

ANUM-TD 5 22. Feb. 23

Ex. 2

1.) $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$.

$$f'(x) = \sum_{i=0}^{n} \underbrace{i a_i}_{\in \mathbb{Z}} x^{i-1} \in \mathbb{Z}[x]$$

If we use the Tayler expansion of order 1, we obtain.

$$f(x+h) = f(x) + f'(x)h + r(x,h)h^2.$$

2) $f(x_1) = 0 \bmod p$ and $f'(x_1) \neq 0 \bmod p$

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field if p prime.

So, there exists $s \in \mathbb{Z}$ such that $s \cdot f'(x_1) = 1 \bmod p$

let us define the "Newton iteration"

$$x_k = x_{k-1} - s f(x_{k-1}) \bmod p^k.$$

By injection

$x_k = x_{k-1} \bmod p$ because $f(x_{k-1}) = 0 \bmod p^{k-1}$ So

$f(x_k) = 0 \bmod p$. so $f'(x_k) = f'(x_{k-1}) \bmod p$.

$$f(x_k) = f(x_{k-1} - S f(x_{k-1}) + \alpha p^k)$$

$$= f(x_{k-1}) + f'(x_{k-1})(-S f(x_{k-1}) + \alpha p^k) + \beta(-S f(x_{k-1}) + \alpha p^k)^2 \mod p^k$$

$$= \underbrace{f(x_{k-1}) - S f'(x_{k-1}) f(x_{k-1})}_{0} + \underbrace{f'(x_{k-1})\alpha p^k}_{0 \mod p}$$

$$+ \beta(-S f(x_{k-1}) + \alpha p^k)^2 \mod p^k$$

$$= \beta(\underbrace{S^2 f(x_{k-1})^2}_{0} + \underbrace{\alpha^2 p^{2k}}_{0} - 2S \underbrace{f(x_{k-1})\alpha p^k}_{0} \mod p^k$$

$$f(x_{k-1}) = 0 \mod p^{k-1}$$

$$f(x_{k-1})^2 \equiv 0 \mod p^{2k-2} \equiv 0 \mod p^k$$

So, finally $f(x_k) = 0 \mod p^k$

$$x_k = x_{k-1} - S f(x_{k-1}) + \alpha p^k$$

$$= x_{k-1} - S(\beta p^{k-1}) + \alpha p^k$$

$$= x_{k-1} \mod p^{k-1}$$