Lecture 15
March 5th, 2015

whether e_i is odd affects r_i

FASTER ITERATIVE POWER

$(123)^{237} = (123)^{236} \cdot (123)^1$
$= ((123)^2)^{118} \cdot (123)^1$
$= (((123)^2)^2)^{59} \cdot (123)^1$
$= ((((123)^2)^2)^2)^{29} \cdot [((123)^2)^2 \cdot (123)^1]$

S_i	e_i	r_i
123	237	$1 = (123)^0$
~~123~~	~~236~~	~~123^1~~
123^2	118	123^1
$((123)^2)^2$	59	123^1
$(((123)^2)^2)^2$	28	$((123)^2)^2 \cdot 123^1$
$= \cdots$		$= \cdots$

using floor

skip this by

$(123)^{237} = ((((123)^2)^2)^2)^{29} \cdot ((123)^2)^2 \cdot (123)^1$

For $i \in \mathbb{N}$, let $I(i)$ be : $\boxed{b^n = (S_i)^{e_i} \cdot r_i}$

```
def: pow(b,n):
    s = b
    e = n
    r = 1
    while  e > 0 :
        if e%2 == 1:
            r = s·r
        e = e//2
        S_{i+1} = S_i * S_i
    return r
```

Translation of the code:

$s_0 = b,\ e_0 = n,\ r_0 = 1$

$$\left.\begin{aligned} S_{i+1} &= S_i^2 \\ e_{i+1} &= \lfloor e_i/2 \rfloor \\ r_{i+1} &= \begin{cases} S_i \cdot r_i & \text{if } e_i \text{ is odd} \\ r_i & \text{if } e_i \text{ is even} \end{cases} \end{aligned}\right\} \text{for each } i \in \mathbb{N}$$

Proof of the invariant :

Base Case $I(0)$: $(S_0)^{e_0} \cdot r_0 \overset{\text{from code}}{=} b^n \cdot 1 = b^n$

I.S. Let $i \in \mathbb{N}$, assume $b^n = (S_i)^{e_i} \cdot r_i$ (IH)

Assume at least $i+1$ iterations. (so $e_i > 0$)

Case e_i odd: $(S_{i+1})^{e_{i+1}} r_{i+1} = (S_i^2)^{\lfloor e_i/2 \rfloor} \cdot S_i \cdot r_i$ (from code)

$= (S_i^2)^{\frac{e_i - 1}{2}} S_i \cdot r_i$

$= S_i^{e_i - 1} \cdot S_i \cdot r_i = S_i^{e_i} r_i = b^n$ by (IH)

Case e_i even: $(S_{i+1})^{e_{i+1}} r_{i+1} = (S_i^2)^{\lfloor e_i/2 \rfloor} \cdot r_i = (S_i^2)^{e_i/2} \cdot r_i = S_i^{e_i} r_i = b^n$ by (IH)

problematic?

Variant : e_i

assume $\geq i+1$ iterations so passed ith loop condition i.e. $e^i > 0$

$e_{i+1} = \lfloor \frac{e_i}{2} \rfloor < e_i$, since $e_{i/2} < e_i$ ($\because e_i > 0$)

so $\lfloor e_{i/2} \rfloor \leq e_{i/2} < e_i$

Let $i \in \mathbb{N}$.

Assume $\geq i$ iterations

prove $e_i \in \mathbb{N}$

case $i=0$, $e_0 = n \in \mathbb{N}$ by PRE.

case $i \geq 1$, $e_{i-1} > 0$ from passing loop condition

so $\frac{e_{i-1}}{2} > 0$, so $\lfloor \frac{e_{i-1}}{2} \rfloor \in \mathbb{N}$

Let t be the ??? of last condition, $e_t \in \mathbb{N}$, but $e_t > 0$ failed.

so $e_t \leq 0$, so $e_t = 0$

By $I(t)$, $(S_t)^{e_t} \cdot r_t = b^n$, $(S_t)^0 \cdot r_t = 1 \cdot r_t = b^n$ so return $r_t = b^n$.