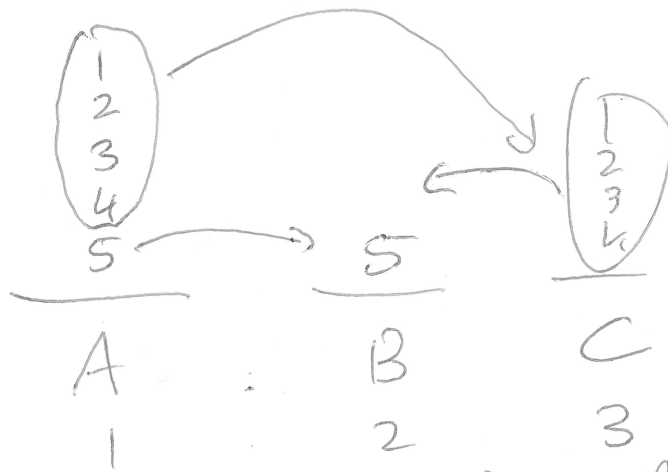


6/14/24

Towers



Can I move 5?
NO

	2	1
5	4	3
A	B	C

towers (5, 1, 2) — move n disks from start to end
n, start end mid = 3rd tower ≠ start ≠ end

① Disk n must move!

When can disk n move?

- ② 1 - (n-1) must all be moved elsewhere
- ③ 1 - (n-1) must ALL move to a single tower because another tower must be empty to "receive" disk n.

⇒ towers (n-1, start, mid)

2. Move disk n from start to end

3. towers (n-1, mid, end)

Let $T(n)$ = # moves solve tower w/n disks

$$T(1) = 1$$

$$T(n) = T(n-1) + 1 + T(n-1)$$

$$T(n) = 2T(n-1) + 1$$

$$T(2) = 2 \times T(1) + 1 = 2 + 1 = 3$$

$$T(3) = 2 \times T(2) + 1 = 2 \times 3 + 1 = 7$$

$$T(n) = 15$$

1, 3, 7, 15, ...

$$T(n) = 2^n - 1$$

Fast Modular Exponentiation

Reg expo: b^e ? 2^5 ?

mod expo $b^e \% m$ $2^5 \% 13 = 6$

// $m > 1$

// $\text{modexpo}(b, e, m)$ {

if $(e == 0)$ return 1;

return $(b * \text{modexpo}(b, e-1)) \% m$;

3

$$2^5 = 2 * 2^4$$

$$2^5 \neq 2 * 2^5$$

$a = 1$;
for $(i = 0; i < e; i++)$
 $a = (a * b) \% m$
return a ;

→ Memory $O(1)$ Run-time $O(e)$

→ Memory $O(e)$ Run-time $O(e)$

$$2^{100} \% 13$$

$$2^{100} = (2^{50} * 2^{50}) \% 13$$

provided
 e is
even

$$\text{mod-expo}(b, e, m) = \left(\begin{array}{l} \text{modexpo}(b, e/2, m) * \\ \text{modexpo}(b, e/2, m) \end{array} \right) \% m$$

$\text{modexp}(b, e, m)$ {

$x = \text{modexp}(b, e/2, m)$

return $(x+x) \% m$

if e is even $\rightarrow$

if e is odd $(b + \text{modexp}(b, e-1, m)) \% m$

e
85
84
42
21
20
10
5
4
2
1

every 2 steps we at least go by 2
in total of 85 rec calls,
10 rec calls

$$e = 2^k$$

$$k = \log_2 e$$

$$\# \text{ steps} \leq 2 \log_2 e$$

$$e = 10^{100} \rightarrow 332$$

$$\log_2 10^{100} \approx 332$$

$$\# \text{ steps} \leq 660$$

RSA encryption

Ron Rivest, Adi Shamir, Leonard Adleman