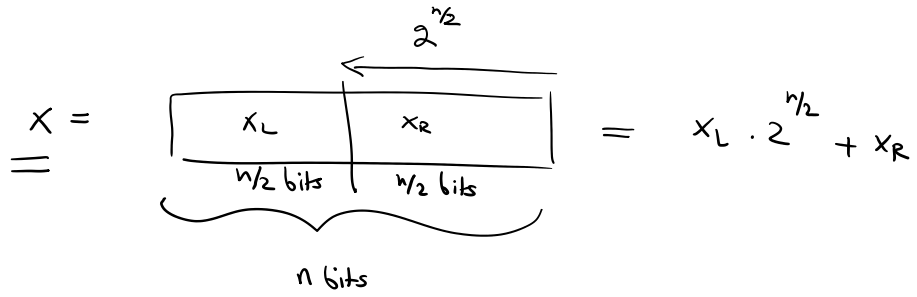
Divide and Conquer Multiplication



$x^{86} \equiv 6 \mod 29$ (29 prime)

Use Fermat's Little theorem

$x^{28 \cdot 3 + 2} \equiv 6 \mod 29$

$(x^{28})^3 \cdot x^2 \equiv 6 \mod 29$

$1^3 \cdot x^2 \equiv 6$

$x^2 \equiv 6 \mod 29$

$\Rightarrow x^2$ divided by 29 leaves remainder 6

$x^2 = 29t + 6$ (t: some integer)

Hi

$t = 2$

$x^2 = 29 \cdot 2 + 6 = 58 + 6 = 64$

$x = 8$

HW 4

Q 1.33 $LCM(x, y)$: $x < y$, x, y are n-bit numbers, analyse the running time!

↓

least common multiple

$(x, y) = (2, 20)$

Naive:

1) y x divides y, return y
2) for $t = 1, 2, \ldots,$
   $z = y \cdot t$
   y x divides z

$lcm(x, y) = \frac{x \cdot y}{gcd(x, y)}$

$x = (5 \cdot 3 = 15$

$z = y \cdot t$

y x divides z

return z

gcd(x,y) ←

$x = 5 \cdot 3 = 15$

$y = 5 \cdot 7 = 35$

lcm = $5 \cdot 3 \cdot 7$

$gcd(x,y) = 5$

$$\frac{15 \cdot 35}{5} = \frac{3 \cdot 5 \cdot \cancel{5} \cdot 7}{\cancel{5}}$$

1) gcd (x,y) — $O(n^3)$ ←

2) $x \cdot y$ — $O(n^2)$

3) $\frac{x \cdot y}{gcd}$ — $O(n^2)$

Q 1.39

$a^{b^c} \bmod p$ ← prime

$a^{p-1} \equiv 1 \bmod p$

1) $z = b^c$ ← exponentiation $O(n^3)$

express this in terms of p-1

2) $z \bmod p-1 = r$ ← remainder

$b^c = z = (p-1) \cdot t + r$ ← integer division $O(n^2)$

$a^{(p-1)t+r} \bmod p$

a^1

$a^r \bmod p$ ← exponentiation $(O(n^3))$

division $O(n^2)$

$O(n^3)$ final

Q 1.40

if $x^2 \equiv 1 \bmod N$, but $x \not\equiv 1$ $x \not\equiv -1$ mod N, then N must be composite

$x^2 - 1$ is divisible by N

2

$x^2 - 1$ is divisible by N

$x^2 - 1 = Nt$ ← some integer

$(x+1)(x-1) = Nt$ (both factors $\neq 0$)

$x \neq 1$

$x \neq -1$

Q 1.42

RSA: $N = pq$ — why?

public $N = p$

$M = (p-1)$

$d = e^{-1} \bmod p-1$

e : public key

e is relatively prime to $p-1$

× encrypt $y = x^e \bmod p$

$y^d \bmod p$

Q 2.1

1001 1011 (x_L x_R)

1011 1010 (y_L y_R)

Q 2.4

A: $T(n) = 5T\left(\frac{n}{2}\right) + O(n)$

B: $T(n) = 2T(n-1) + O(1)$

C: $T(n) = 9T\left(\frac{n}{3}\right) + O(n^2)$

Q 2.12

f(n):

If n > 1:

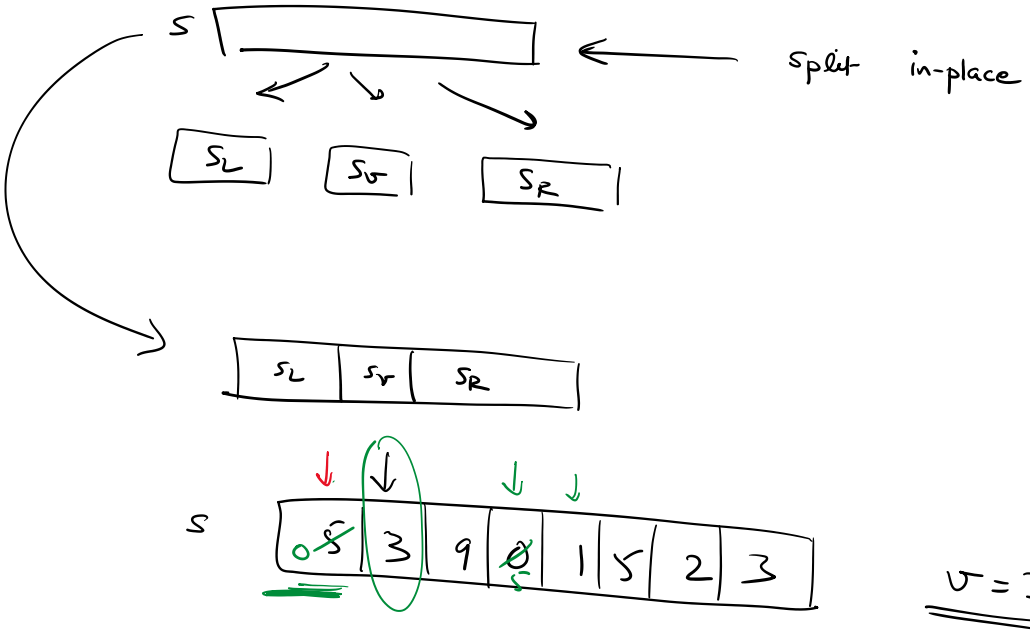
print "

$T(n) = 2T\left(\frac{n}{2}\right) + O(1)$

print "i"
f(n/2)
f(n/2)

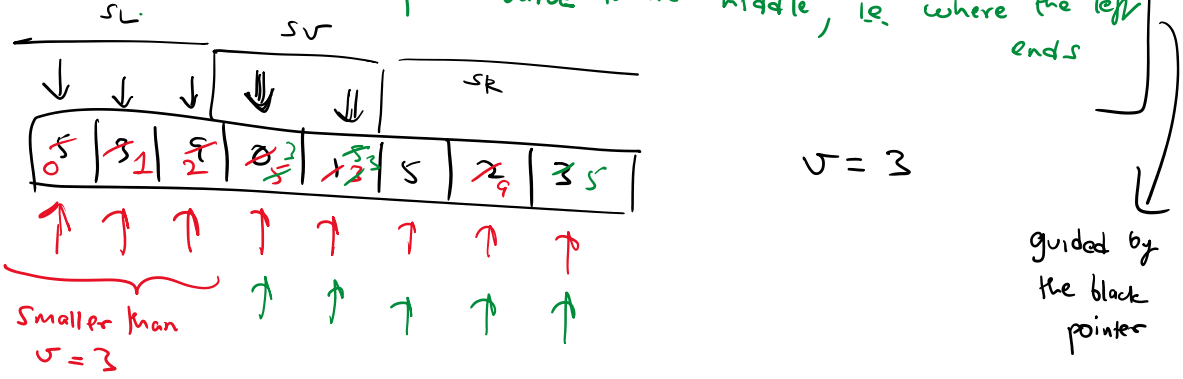
$T(n) = 2T\left(\frac{n}{2}\right) + O(1)$

Q2.15 selection



red pointer: moves value less than v to the left/front side

green pointer: moves the pivot value to the "middle", i.e. where the left ends

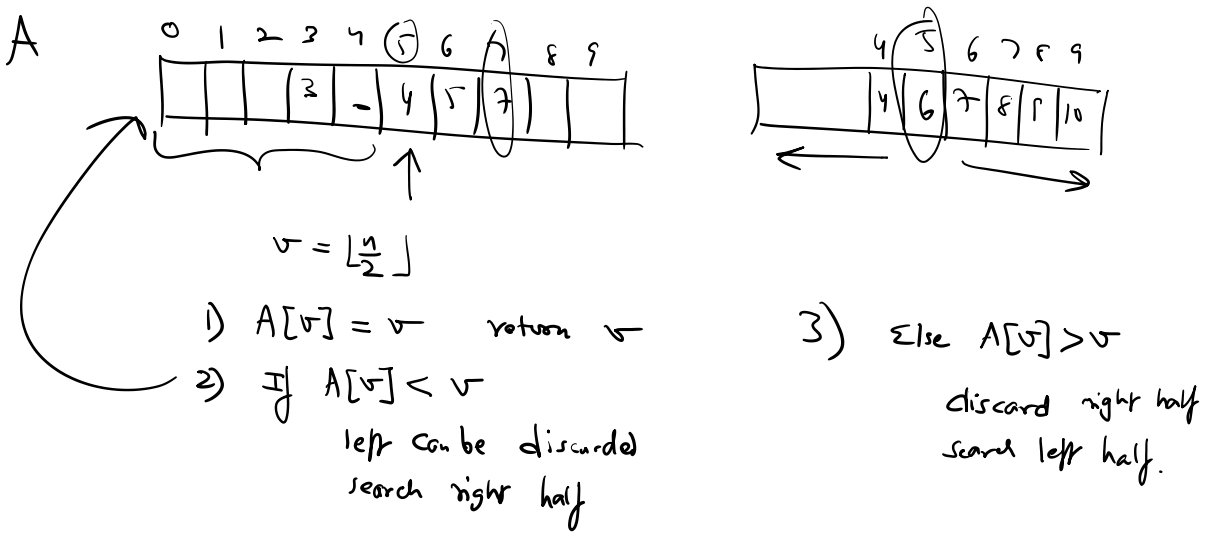


Q2.17

A sorted of size n, distinct integers

find an index where A[i] = i

in O(log n) time



For Recursive time equations

→ Unrolling, summation, solve

Master Theorem

$$T(n) = a\,T\left(\frac{n}{b}\right) + O(n^d)$$

- $T(n)$: problem of size n
- a: divide into a parts
- b: reduction factor; size of subproblems n/b
- d: polynomial degree
- $O(n^d)$: time per call

$$T(n) = a\,T\left(\frac{n}{b}\right) + O(n^d)$$

$n \to \frac{n}{b}$

$$= a\left(a\,T\left(\frac{n}{b^2}\right) + O\left(\frac{n}{b}\right)^d\right) + O(n^d)$$

$$= a^2\,T\left(\frac{n}{b^2}\right) + a\,O\left(\left(\frac{n}{b}\right)^d\right) + O(n^d)$$

$$= \cdots$$

$$O(n^d) = a^0 \cdot \left(\frac{n}{b^0}\right)^d$$

$O(n^0) = a^0 \cdot \left(\frac{n}{b^0}\right)^d$

$a^1\left(\left(\frac{n}{b^1}\right)^d\right)$

$a^2\left(\left(\frac{n}{b^2}\right)^d\right)$

$= \cdots$

$$T(n) = \sum_{i=0}^{\log_b n} a^i \left(\frac{n^d}{b^i}\right)$$

$$T(n) = n^d \sum_{i=0}^{\log_b n} \left(\frac{a}{b^d}\right)^i$$

Case I: $a = b^d$ or $\log a = d \log b$

$$T(n) = n^d \sum_{i=0}^{\log_b n} 1$$

$$= O(n^d \log_b n)$$

Case II: $a < b^d \Rightarrow \frac{a}{b^d} < 1$

$r = \frac{a}{b^d}$

$$T(n) = n^d \cdot \left(\frac{1}{1 - \frac{a}{b^d}}\right)$$

$$= n^d \cdot \left(\frac{b^d}{b^d - a}\right)$$

Some constant value

$$= O(n^d)$$

Case III $a > b^d \Rightarrow \frac{a}{b^d} > 1$

$r = \frac{a}{b^d}$ $\quad \frac{r^{k+1} - 1}{r - 1}$ $\quad k = \log_b n$

$$T(n) = n^d \left(\frac{\left(\frac{a}{b^d}\right)^{\log_b n + 1} - 1}{\frac{a}{b^d} - 1}\right)$$

$$\approx n^d \frac{a^{\log_b n} \cdot a}{(b^d)^{\log_b n} \cdot b^d}$$

$$\approx \frac{n^d \, n^{\log_b a}}{\left(b^{\log_b n}\right)^d}$$

$$a^{\log_b n} = n^{\log_b a}$$

$$\left(b^{\log_b n}\right)^d$$

$$= \frac{n^d \, n^{\log_b a}}{n^d}$$

$$= O\left(n^{\log_b a}\right)$$