Ganesh Budhathoki

Problem #1.

$P = 131$, $Q = 137$ and $e = 3$.

* What is Bob's public modulus N?

$N = P * Q = 137 * 131 = 17947$.

* What is Bob's secret exponent d?

we have $\phi(N) = (P-1)(Q-1)$
$= 130 * 136$
$= 17680$

From rules of d.

$d * e \mod \phi(N) = 1$.

$d = e^{-1} \mod \phi(N)$

Using extended euclid's algorithms

$eE(\overset{a}{17680}, \overset{b}{3}) = (1, 0 - \lfloor 17680/3 \rfloor * 1, 1) = (1, -5893$

$eE(3, 1) = (0, 1 - 0, 1) = (0, 1, 1)$

$eE(1, 0) = (1, 0, 1)$

so $d = e^{-1} \mod \phi(N)$
$= 11787$

* Suppose Alic wishes to send Bob the message $x = 36$

Derive the encoded message y that she actually sends

we have $N = 17947$ and $e = 3$
Let y be the encode message

$y = x^e \mod N$ where x is the original message
i.e $y = 10762$.

* Show the calculation by which Bob decodes the message
$y = 10762$, $N = 17947$, $e = 3$
$d = 11787$.

$x = y^d \mod N$.
$= 10762^{(11787)} \mod 17947$
$= 36$

Ans

Problem # 2

2.4 Solution

For A

$T(n) = 5\,T(n/2) + O(n)$

$a = 5 \quad b = 2$ and $d = 1$

General form of Master Theorem

$\frac{d}{1} \qquad \frac{\log_b a}{\log_2 5} = 2.3$

If $d < \log_b a$ then

$T(n) = O(n^{\log_2 5}) = O(n^{2.3})$

For B

$T(n) = 2\,T(n-1) + O(1)$

$\leq 2T(n-1) + c$ for $K = 1$

$\leq 2(2T(n-1) + c) + c$

$\leq 4T(n-1) + 3c$ } for $K = 2$

$\leq 4(2T(n-1) + c) + 3c$

$\leq 8T(n-1) + 7c$ } for $K = 3$

General Term: $2^K\, T(n-K) + (2^K - 1)\,c$

plug $K = n$.

$\simeq 2^n T(n-n) + (2^n - 1)c$

$\simeq 2^n \cancel{T(0)} + (2^n \cancel{-1})\cancel{c}$

$\simeq 2^n$

$= O(2^n)$

For c

$T(n) = 9T(n/3) + O(n^2)$

General Form of Master Theorem

$a = 9$, $b = 3$, $d = 2$

$\frac{d}{2}$ $\qquad$ $\frac{\log_b a}{\log_3 9 = 2}$

If $d = \log_b a$ then

$T(n) = O(n^d \log n)$

$= O(n^2 \log n)$

Therefore, ALGORITHM C is the best of the three

Problem # 3
2.5 solution.

a) $T(n) = 2T(n/3) + 1$.

$a = 2 \quad b = 3 \quad d = 0$

General master theorem form

so,

d	$\log_b a$
0	$\log_3 2 = 0.63$

If $d < \log_b a$
then
$T(n) = \Theta(n^{\log_b a}) = \Theta(n^{0.63})$

~~$= \Theta(n)$~~

b) $T(n) = 5T(n/4) + n$.

$a = 5, \; b = 4, \; d = 1$

General master theorem form

d	$\log_b a$
1	$\log_4 5 = 1.16$

~~T(n)~~ If $d < \log_b a$ Then,
$T(n) = \Theta(n^{\log_b a}) = \Theta(n^{1.16})$ ~~$= \Theta(n)$~~

(c) $T(n) = 7T(n/7) + n$

$a = 7,\ b = 7,\ d = 1$

General master Theorem Form

$\frac{d}{1}$ $\frac{\log_b a}{\log_7 7} = 1$

If $d = \log_b a$

then.

$T(n) = \Theta(n^d \log n)$

$~~= \Theta(n)~~$

$= \Theta(n \log n)$ #

(d) $T(n) = 9T(n/3) + n^2$

$a = 9,\ b = 3,\ d = 2$

General Master Theorem Form.

$\frac{d}{2}$ $\frac{\log_b a}{\log_3 9} = 2$

If $d = \log_b a$ then.

$T(n) = \Theta(n^d \log n)$

$= \Theta(n^2 \log n)$. #

e) $T(n) = 8T(n/2) + n^3$

$a = 8 \quad b = 2 \quad d = 3$

General master theorem form

$\underline{d} \qquad \log_b a$

$3 \qquad \log_2 8 = 3$

If $d = \log_b a$ then

$T(n) = \Theta(n^d \log n) = \Theta(n^3 \log n)$ *

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

$\leq T(n-1) + 2$

$\leq T(n-2) + 2 + 2.$

$\leq T(n-3) + 2 + 2 + 2$

$\vdots$

General Term $\leq T(n-k) + 2k.$

plug in $k = n$

$\simeq T(n-n) + 2n$

$= T(0) + 2n$

$\simeq \Theta(\cancel{2}n)$

$\simeq \Theta(n)$ #

Scanned by CamScanner

h) $T(n) = T(n-1) + n^c$ where $c \geq 1$ is constant

$\leq T(n-1) + n^c$

$\leq T(n-2) + (n-1)^c + n^c$

$\leq T(n-3) + (n-2)^c + (n-1)^c + n^c$

General Form $\leq T(n-k) + (n-(k-1))^c + \cdots + (n-2)^c + (n-1)^c + n^c$

Plug $k = n$.

$\approx T(0) + 1 + \cdots (n-2)^c + (n-1)^c + n^c$

$\approx n^{c+1}$

$= \Theta(n^{c+1})$ #

i) $T(n) = T(n-1) + c^n$ where $c > 1$ is constan

$\leq T(n-1) + c^n$

$\leq T(n-2) + c^{n-1} + c^n$

$\leq T(n-3) + c^{n-2} + c^{n-1} + c^n$

$\vdots$

General form $\leq T(n-k) + c^{n-(k-1)} + \cdots + c^{n-2} + c^{n-1} + c^n$

Plug $k = n$

$\approx T(0) + c + \cdots + c^{n-2} + c^{n-1} + c^n$

$\approx c + c^2 + c^3 + \cdots + c^{n-2} + c^{n-1} + c^n$

Geometric series

$$\simeq \frac{c(c^n - 1)}{(c-1)}$$

$$\simeq \Theta\left(\frac{c^{n+1} - \cancel{c}}{\cancel{c-1}}\right)$$

$$= \Theta(c^{n+1}) \quad \#$$