FIT3155: Week 9 Tutorial - Answer Sheet

(Scribe: Dinithi Sumanaweera)

Question 2

Time complexity of divide-and-conquer based fast integer multiplication:

Recurrence to solve:

$$T(2d) = 3T(d) + c\cdot d$$

Expanding r.h.s.

$$= 3\left[3T\left(\tfrac{d}{2}\right) + c\cdot\tfrac{d}{2}\right] + c\cdot d = 3^2 T\left(\tfrac{d}{2}\right) + \left(1+\tfrac{3}{2}\right)c\cdot d$$

$$= 3^2\left[3T\left(\tfrac{d}{4}\right) + c\cdot\tfrac{d}{4}\right] + \left(1+\tfrac{3}{2}\right)c\cdot d = 3^3 T\left(\tfrac{d}{4}\right) + \left(1+\tfrac{3}{2}+\tfrac{3^2}{2^2}\right)c\cdot d$$

$$= 3^3\left[3T\left(\tfrac{d}{8}\right) + c\cdot\tfrac{d}{8}\right] + \left(1+\tfrac{3}{2}+\tfrac{3^2}{2^2}\right)c\cdot d = 3^4 T\left(\tfrac{d}{8}\right) + \left(1+\tfrac{3}{2}+\tfrac{3^2}{2^2}+\tfrac{3^3}{2^3}\right)c\cdot d$$

Expanding until base-case $T(1)$

$\vdots$

$$= 3^k\left[3T(1) + c\cdot\tfrac{d}{2^k}\right] + \left(1+\tfrac{3}{2}+\tfrac{3^2}{2^2}+\cdots+\tfrac{3^{k-1}}{2^{k-1}}\right)c\cdot d = \boxed{3^{k+1}T(1) + \left(1+\tfrac{3}{2}+\tfrac{3^2}{2^2}+\cdots+\tfrac{3^k}{2^k}\right)c\cdot d} \quad (1)$$

Since we are halving each time from $d \to \frac{d}{2} \to \frac{d}{4} \to \cdots 1$

$k = \log_2 d$. Also, separately, $T(1) = \text{Constant} = b$ (say).

From (1)

$$\therefore\ T(2d) = b3^{k+1} + \left(1+\tfrac{3}{2}+\tfrac{3^2}{2^2}+\cdots+\tfrac{3^k}{2^k}\right)c\cdot d$$

$$= b3^{k+1} + \left[\frac{\left(\frac{3}{2}\right)^{k+1}-1}{\frac{3}{2}-1}\right]c\cdot d = b3^{k+1} + \left[\frac{3^{k+1}-2^{k+1}}{2^{k+1}\times\frac{1}{2}}\right]c\cdot d$$

$$= b3^{k+1} + \left[\frac{3^{k+1}-2^{k+1}}{2^k}\right]c\cdot d$$

Since $k = \log_2 d \Rightarrow 2^k = d$

$$\Rightarrow T(2d) = b3^{k+1} + \left[\frac{3^{k+1}-2^{k+1}}{\cancel{d}}\right]c\cdot\cancel{d} = (b+c)3^{k+1} - c\cdot 2^{k+1}$$

$$\leq (b+c)3^{k+1}$$

$$\leq 3(b+c)3^k$$

$$= O(3^k)$$

Replace k with $\log_2 d$

$$\Rightarrow T(2d) = O\left(3^{\log_2 d}\right) = O\left(3^{\log_3 d\cdot\log_2 3}\right)$$

$$= O\left[\left(3^{\log_3 d}\right)^{\log_2 3}\right] = O\left(d^{\log_2 3}\right)$$

∎

Question 3

Compute 7^{330} mod 13 by hand using the repeated squaring method

$$\begin{array}{ccccccccc} 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{array}$$

$\text{binary}(330) = \underline{1}\ 0\ \underline{1}\ 0\ 0\ \underline{1}\ 0\ \underline{1}\ 0$

$330 = (2^1 + 2^3 + 2^6 + 2^8)$

$\Rightarrow 7^{330} = 7^{2^1+2^3+2^6+2^8} = 7^{2^1} \cdot 7^{2^3} \cdot 7^{2^6} \cdot 7^{2^8}$

Start 7^{2^i} mod 13 with $i=0$ and continue until $i=8$

1. 7^{2^0} mod 13 = 7 mod 13 = $\underline{\underline{7}}$

2. 7^{2^1} mod 13 = $(7^{2^0} \times 7^{2^0})$ mod 13
$= [(7^{2^0} \text{ mod } 13)(7^{2^0} \text{ mod } 13)]$ mod 13
$= 7^2$ mod 13 = $\underline{\underline{10}}$

3. 7^{2^2} mod 13 = $(7^{2^1} \times 7^{2^1})$ mod 13
$= [(7^{2^1} \text{ mod } 13)(7^{2^1} \text{ mod } 13)]$ mod 13
$= 10^2$ mod 13 = $\underline{\underline{9}}$

4. 7^{2^3} mod 13 $= [(7^{2^2} \text{ mod } 13)(7^{2^2} \text{ mod } 13)]$ mod 13
$= 9^2$ mod 13 = $\underline{\underline{3}}$

5. 7^{2^4} mod 13 = $(7^{2^3} \text{ mod } 13)^2$ mod 13 = 3^2 % 13 = $\underline{\underline{9}}$

6. 7^{2^5} mod 13 = $(7^{2^4} \text{ mod } 13)^2$ mod 13 = 9^2 % 13 = $\underline{\underline{3}}$

7. 7^{2^6} mod 13 = $(7^{2^5} \text{ mod } 13)^2$ mod 13 = 3^2 % 13 = $\underline{\underline{9}}$

8. 7^{2^7} mod 13 = $(7^{2^6} \text{ mod } 13)^2$ mod 13 = 9^2 % 13 = $\underline{\underline{3}}$

9. 7^{2^8} mod 13 = $(7^{2^8} \text{ mod } 13)^2$ mod 13 = 3^2 % 13 = $\underline{\underline{9}}$

Only green highlighted values are needed.

$$7^{330} \bmod 13 = \left(7^{2^1} \times 7^{2^3} \times 7^{2^6} \times 7^{2^8}\right) \bmod 13$$

$$= \left[\left(7^{2^1} \times 7^{2^3} \times 7^{2^6}\right) \bmod 13\right]\left[7^{2^8} \bmod 13\right] \bmod 13$$

$$= \left\{\left[7^{2^1} 7^{2^3} 7^{2^6} \% 13\right] \times 9\right\} \% 13$$

$$= \left[\left(7^{2^1} \cdot 7^{2^3} \% 13\right)\left(7^{2^6} \% 13\right) \bmod 13\right] 9 \quad \% \quad 13$$

$$= \left[\left[\left(7^{2^1} 7^{2^3} \% 13\right) \times 9\right] \% 13\right] 9 \quad \% \quad 13$$

$$= \left[\left[\left(7^{2^1} \% 13\right)\left(7^{2^3} \% 13\right) \% 13\right] 9 \quad \% \quad 13\right] 9 \quad \% \quad 13$$

$$= \left[\left[(10 \times 3) \% 13\right] 9 \quad \% \quad 13\right] 9 \quad \% \quad 13$$

$$= \left[9\left(30 \% 13\right) \quad \% \quad 13\right] 9 \quad \% \quad 13$$

$$= \left[9 \times 4 \quad \% \quad 13\right] 9 \quad \% \quad 13$$

$$= 9\left(36 \% 13\right) \% 13 = (9 \times 10) \% 13$$

$$= 90 \% 13 = \underline{\underline{12}}$$