ASSIGNMENT2 QUESTION1

1. Given positive integers M and n compute M^n using only $O(\log n)$ many multiplications. (15 pts)

Answer:

There is two way to do this.

1. For all n are positive integers we have $m^n = \begin{cases} m\left(m^{\frac{n-1}{2}}\right)^2, when\ n\ is\ odd \\ \left(m^{\frac{n}{2}}\right)^2, when\ n\ is\ even \end{cases}$.

0 is not positive integer. In order to archive $O(log\, n)$, if n is even, we compute $m^{\frac{n}{2}}$ first then get the square. If n is odd, we compute $m^{\mathrm{n}-1}$ first, then multiply by m. To get the $m^{\frac{n-1}{2}}\ or\ m^{\frac{n}{2}}$, we will follow the similar rules, but make n $=\frac{n-1}{2}\ or\ \frac{n}{2}$. We will do this recurrence until m^1 then we can get the m^n in $O(log\, n)$ multiplications by many squares.

For example, let n = 12, 12 is even we will compute m^6 first, to get m^6 we will compute m^3 first, to get m^3 we will get m^{3-1} first, to get m^2.

1. Get $m^2 = m \cdot m$
2. Get $m^3 = m^2 \cdot m$
3. Get $m^6 = (m^3)^2$
4. Get $m^{12} = (m^6)^2$

And we will do 4 calculate to get m^{12}.

In this way, we can get result using many multiplications.

2. We can write n in binary. Make $n = 2^{K_1} + 2^{k_2} + \cdots + 2^{k_m}\ whereK_1 > k_2 > \cdots k_m\ and\ k_1 = \lfloor \log_2 n \rfloor$; Then $M^n = M^{2^{k_1}} \cdot M^{2^{k_2}} \cdots M^{2^{k_m}}$ So we can compute at most $\lfloor \log_2 n \rfloor$ times to get all $M^{2^{\mathrm{j}}}$for all $1 \le j \le \lfloor \log_2 n \rfloor$ by square the $M^{2^{\mathrm{j}}}$ and get the value of M^n.For example, let n = 15. 15 = $2^3 + 2^2 + 2^1 + 2^0$,then$M^{15} = M^8 \cdot M^4 \cdot M^2 \cdot M = ((M^2)^2)^2 \cdot (M^2)^2 \cdot M^2 \cdot M$

In this way, we can get m^n in $O(log\, n)$ multiplications.