Q1

Written by Xiao Hu
Z5223731

Answer:

By using repeated squaring, we can simply write n in binary. For example, let us say n = 13, thus, the binary form of 13 is $(1101)_2$, then we can write $13 = 2^3 + 2^2 + 2^0 = 8 + 4 + 1$. Clearly, the representation of n is $2^{k1} + 2^{k2} + \cdots + 2^{km}$ where $k_1 > k_2 > \cdots > k_m$ and $k_1 = floor(\log_2 n) = \lfloor \log_2 n \rfloor$. Hence, M^n can be represented as $M^{2^{k1}} \cdot M^{2^{k2}} \cdots M^{2^{km}}$ and this algorithm does only $O(\log n)$ multiplications.