HOMEWORK 2 – Q1

MINGLANG XIE

z5228006

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

Solution:

There are two ways to solve this question.

1. We first divide M^n into two parts, then we have $M^n = M^{\left(\frac{n}{2}\right)^2}$. We solve it recursively, then we have $M * M = M^2, M^4 = (M^2)^2 = M * M * M * M, and\ ((M^2)^2)^2 = M * M * ... * M\ (there\ are\ 8\ multiplications)$, but we only need $log_2(8) = 3$ multiplications to get a answer that need 8 multiplications. Thus, we can compute M^2 using only $O(\log(n))$ many multiplications. However, if n is a odd number, we have $M^n = M * (M^{n-1})$, we need to do the same thing with M^{n-1}, and multiple one more M into the finally answer we compute (which is M^{n-1}), it also using only $(\log(n) + 1) = O(\log(n))$ many multiplications.
2. We can write M^n in binary as $M^n = 2^{k1} + 2^{k2} + 2^{k3} ... 2^{km}\ where\ k1 > k2 > k3 > \cdots km\ and\ k1 = \log_2 n$; then $\mathrm{M}^{\mathrm{n}} = \mathrm{M}^{2^{\mathrm{k1}}}\mathrm{M}^{2^{\mathrm{k2}}}\mathrm{M}^{2^{\mathrm{k3}}} ... \mathrm{M}^{2^{\mathrm{km}}}$.This involves at most $log_2(n)$ multiplications. So it is enough to compute all of $M^{2^j}\ for\ all\ 1 \leq j \leq log_2(n)$ with at

most $log_2(n)$ multiplications. To do that, use repeated squaring, as show below:

```
result = 1;
base = 2;
while (b != 0){
    if (b&1 > 0){
        result *= base;
    }
    base *= base;
    b >>= 1;
}
return result
```