

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{we know that } M^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$$

we want  $M^n$ , without doing  $n$  multiplications

trick: only need  $\log(n)$  multiplications

$$M \cdot M = M^2; \quad M^2 \cdot M^2 = M^4; \quad M^4 \cdot M^4 = M^8, \dots$$

what powers of  $M$  do we need?

Example:  $n = 77 = 64 + 8 + 4 + 1$

$$M^{77} = M^{2^6} \cdot M^{2^3} \cdot M^{2^2} \cdot M^{2^0}$$

~~$M \cdot M = M^2$~~

~~$M^8 \cdot M^8 = M^{16}$~~

$M^2 \cdot M^2 = M^4$  ✓

~~$M^{16} \cdot M^{16} = M^{32}$~~

$M^4 \cdot M^4 = M^8$  ✓

~~$M^{32} \cdot M^{32} = M^{64}$~~

6 multiplications

$$M^{77} = M^{64} \cdot M^8 \cdot M^4 \cdot M \quad \text{3 multiplications}$$

total: 9 multiplications instead of 76.