Sam Hopkins
HW 2 1.7, 1.25
$2^{21} \bmod 18$

1.7) $X = n \quad y = m$

Each time y is divided by two, and a new call to multiply() is initiated. So if $m = y$, then there are m recursive calls, as each call shifts the bits right by one, so $O(m)$

Each call also requires Odd/even confirmation, and multiplying by 2, so total bit operations are $O(m)$

Total $O(m^2)$ from each recursion and equations in said function.

1.25) $2^{125} \bmod 127$, because 127 is prime,

using fermat's little Theorm, we get $a^{p-1} \equiv 1 \bmod p$,

so [redacted] $2^{126} \equiv 1 \pmod{127}$,

so $2^{125} \cdot 2 \equiv 1 \pmod{127}$ so when $64 \pmod{127} \cdot 2 \equiv 1 \bmod 127$,

so $2^{125} \equiv 64 \pmod{127}$. $2^{125} \bmod 127 = \underline{64}$

a) $2^{21} \bmod 18$

$8 \cdot 2 = 162 \% 18$

modexp(2, 21, 18) $z=9$ $y=21$ $x=2$ $N=18$

modexp(2, 10, 18) $z=3$ $y=10$ $x=2$ $N=18$

modexp(2, 5, 18) $z=4$ $y=5$ $x=2$ $N=18$ $16 \cdot 2 = 32 \to 14$

modexp(2, 2, 18) $z=2$, $y=2$, $x=2$, $N=18$

modexp(2, 1, 18)

modexp(2, 0, 18)

$z=1$

$z=2$

$z=4$

$z=16$

$z=14$

9

$2^{21} \bmod 18 = 8$

8 mod 18

	X	Y	N	Z
modexp(2, 21, 18)	2	21	18	8
" (2, 10, 18)	2	10	18	16
" (2, 5, 18)	2	5	18	14
" (2, 2, 18)	2	2	18	4
" (2, 1, 18)	2	1	18	2
" (2, 0, 18)	2	0	18	1