HW 2: Solution for 2^{21} mod 18

(4 points)

```
modexp ($x$, $y$, $N$)
if $y$ = 0: return 1
$z$ = modexp($x$, floor($y$/2), $N$)
if $y$ is even:     return $z^2$ mod $N$
else:               return $x \cdot z^2$ mod $N$
```

x	y	y_{binary}	power of x	z	return value
2	21	1	x^{1}	16	512 mod 18 = 8
2	10	0	x^{2}	14	196 mod 18 = 16
2	5	1	x^{4}	4	32 mod 18 = 14
2	2	0	x^{8}	2	4
2	1	1	x^{16}	1	2
2	21		x^{21}		