Modular Powers: $b^e \pmod m$

b: base

e: exponent m: modulus

Method 1: result = 1

multiply result by base, exponent number of times, reducing mod m each time

Method 2: example: compute 3^{64}

$3^2 = 3 \cdot 3$, $3^4 = 3^2 \cdot 3^2$, $3^8 = 3^4 \cdot 3^4$, $3^{16} = 3^8 \cdot 3^8$,

$3^{32} = 3^{16} \cdot 3^{16}$, $3^{64} = 3^{32} \cdot 3^{32}$

Now: compute $3^{25} = 3^{16+8+1} = 3^{16} \cdot 3^8 \cdot 3^1$

Base 2: $25 = 16 + 8 + 1$

$25 \equiv 1 \pmod 2$

$\lfloor \frac{25}{2} \rfloor = 12 \equiv 0 \pmod 2$

$\lfloor \frac{12}{2} \rfloor = 6 \equiv 0 \pmod 2$

$\lfloor \frac{6}{2} \rfloor = 3 \equiv 1 \pmod 2$

$\lfloor \frac{3}{2} \rfloor = 1 \equiv 1 \pmod 2$

1 1 0 0 1

sixteens eights fours twos ones

$a^{n-1} \pmod n$ — use modPow2 for this