Dennis Kuzminer CSCI-UA 310-001 PS4

8. By modular multiplication, we know that $(A * B) \mod C = (A \mod C * B \mod C) \mod C$. Therefore, $3^{99} \mod 100$ can be shown as

((some combination of numbers that multiply to 3⁹⁹) each mod 100) mod 100.

We can have the combination of numbers be powers of 2 using base 2 and the repeated squaring algorithm.

$$e = 99_{10} = 1100011_{2}$$

 $\beta \leftarrow [1] // 0$
 $\beta \leftarrow \beta^{2}, \ \beta \leftarrow \beta * \alpha // 1 \rightarrow 3^{1} \ mod \ 100 = 3$
 $\beta \leftarrow \beta^{2}, \ \beta \leftarrow \beta * \alpha // 11 \rightarrow 3^{3} \ mod \ 100 = 27$
 $\beta \leftarrow \beta^{2} // 110 \rightarrow 3^{6} \ mod \ 100 = 27^{2} \ mod \ 100 = 29$
 $\beta \leftarrow \beta^{2} // 1100 \rightarrow 3^{12} \ mod \ 100 = 29^{2} \ mod \ 100 = 41$
 $\beta \leftarrow \beta^{2} // 11000 \rightarrow 3^{24} \ mod \ 100 = 41^{2} \ mod \ 100 = 81$
 $\beta \leftarrow \beta^{2}, \ \beta \leftarrow \beta * \alpha // 110001 \rightarrow 3^{49} \ mod \ 100 = 81^{2} \ mod \ 100 * 3 = 83$
 $\beta \leftarrow \beta^{2}, \ \beta \leftarrow \beta * \alpha // 1100011 \rightarrow 3^{99} \ mod \ 100 = 83^{2} \ mod \ 100 * 3 = 67$