M 375 – Homework 3

10.4.1

Compute:

$$a_0 = 2$$
$$a_1 = 2^2$$
$$a_2 = 2^{2^2} = 2^4$$
$$a_3 = 2^{2^{2^2}} = 2^8$$
$$a_4 = a_3{}^2 = 2^{8^2} = 2^{16}$$
$$a_5 = a_4{}^2 = 2^{16^2} = 2^{32}$$
$$a_6 = a_5{}^2 = 2^{32^2} = 2^{64}$$

One needs 6 multiplication to compute $a_6 = 2^{64}$; store all previous calculations (i.e. $a_1, a_2, ..., a_6$). Then:

$$2^{75} = a_6 \underbrace{\cdot a_3 \cdot a_1 \cdot a_0}_{3\,\text{multiplications}}$$

We need 6 + 3 = 9 multiplications.

10.4.2

By definition: For any x such that $1 \le x < \phi(n)$, $a^x \ne 1$. In order to have multiple solutions of $y = a^x \bmod n$ there would have to be a value w such that $1 \le x < \phi(n) - 1$ and $a^w = 1 \bmod n$. This can't happen by the given definition.

10.4.3

Choose: $a = 4$, $n = 5$, and $y = 4$ for $y = a^x \bmod n$.

$$4 = 4^x \bmod 5 \text{ for } x = 1 \text{ and } x = 3.$$

10.4.4

Without loss of generality choose $y = a^x \bmod n$ and $z = a^w \bmod n \Rightarrow yz = a^{(x+w)}$.

$$\log(yz) = \log_a a^{(x+w)} = x + w \text{ and } \log_a y + \log_a z = \log_a a^x + \log_a a^w = x + w$$

$$\Rightarrow \log_a y + \log_a z = \log_a (yz).$$