Modular Exponentiation via Binary Algorithm

Exercise

Compute:

$$7^{644} \bmod 645.$$

Solution

We apply the binary exponentiation method.

Step 1: Binary expansion

$$644 = (1010000100)_2 = 2^9 + 2^7 + 2^2.$$

Hence,

$$7^{644} = 7^{2^9} \cdot 7^{2^7} \cdot 7^{2^2}.$$

Step 2: Successive squaring modulo 645

$$\begin{aligned}
7^{2^0} &\equiv 7 \pmod{645},\\
7^{2^1} &\equiv 49 \pmod{645},\\
7^{2^2} &\equiv 2401 \equiv 466 \pmod{645},\\
7^{2^3} &\equiv 466^2 = 217156 \equiv 436 \pmod{645},\\
7^{2^4} &\equiv 436^2 = 190096 \equiv 466 \pmod{645},\\
7^{2^5} &\equiv 466^2 \equiv 436 \pmod{645},\\
7^{2^6} &\equiv 436^2 \equiv 466 \pmod{645},\\
7^{2^7} &\equiv 466^2 \equiv 436 \pmod{645},\\
7^{2^8} &\equiv 436^2 \equiv 466 \pmod{645},\\
7^{2^9} &\equiv 466^2 \equiv 436 \pmod{645}.
\end{aligned}$$

Step 3: Final computation

$$7^{644} = 7^{2^9} \cdot 7^{2^7} \cdot 7^{2^2},$$

$$\equiv 436 \cdot 436 \cdot 466 \pmod{645}.$$

First,

$$436 \cdot 436 = 190096 \equiv 466 \pmod{645},$$

then,

$$466 \cdot 466 = 217156 \equiv 436 \pmod{645}.$$

Conclusion

$$\boxed{7^{644} \equiv 436 \pmod{645}}$$

And

$$\boxed{7^{644} \bmod 645 = 436}.$$