

6.8

1) $m = 11$

$$2^1 \equiv 2 \not\equiv 1 \pmod{11}$$

$$2^2 \equiv 4 \not\equiv 1 \pmod{11}$$

$$2^3 \equiv 8 \not\equiv 1 \pmod{11}$$

$$2^4 \equiv 16 \equiv 5 \not\equiv 1 \pmod{11}$$

$$2^5 \equiv 2^4 \cdot 2 \equiv 5 \cdot 2 \equiv 10 \not\equiv 1 \pmod{11}$$

$$2^6 \equiv 2^5 \cdot 2 \equiv 10 \cdot 2 \equiv 20 \equiv 9 \not\equiv 1 \pmod{11}$$

$$2^7 \equiv 2^6 \cdot 2 \equiv 9 \cdot 2 \equiv 18 \equiv 7 \not\equiv 1 \pmod{11}$$

$$2^8 \equiv 2^7 \cdot 2 \equiv 7 \cdot 2 \equiv 14 \equiv 3 \not\equiv 1 \pmod{11}$$

$$2^9 \equiv 2^8 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \not\equiv 1 \pmod{11}$$

$$2^{10} \equiv 2^9 \cdot 2 \equiv 6 \cdot 2 \equiv 12 \equiv 1 \pmod{11}$$

$\bar{2}$ est d'ordre 10 dans $\mathbb{Z}/11\mathbb{Z}$.

2) $m = 17$

$$2^1 \equiv 2 \not\equiv 1 \pmod{17}$$

$$2^2 \equiv 4 \not\equiv 1 \pmod{17}$$

$$2^3 \equiv 8 \not\equiv 1 \pmod{17}$$

$$2^4 \equiv 16 \not\equiv 1 \pmod{17}$$

$$2^5 \equiv 32 \equiv 15 \not\equiv 1 \pmod{17}$$

$$2^6 \equiv 2^5 \cdot 2 \equiv 15 \cdot 2 \equiv 30 \equiv 13 \not\equiv 1 \pmod{17}$$

$$2^7 \equiv 2^6 \cdot 2 \equiv 13 \cdot 2 \equiv 26 \equiv 9 \not\equiv 1 \pmod{17}$$

$$2^8 \equiv 2^7 \cdot 2 \equiv 9 \cdot 2 \equiv 18 \equiv 1 \pmod{17}$$

$\bar{2}$ est d'ordre 8 dans $\mathbb{Z}/17\mathbb{Z}$.

3) $m = 31$

$$2^1 \equiv 2 \not\equiv 1 \pmod{31}$$

$$2^2 \equiv 4 \not\equiv 1 \pmod{31}$$

$$2^3 \equiv 8 \not\equiv 1 \pmod{31}$$

$$2^4 \equiv 16 \not\equiv 1 \pmod{31}$$

$$2^5 \equiv 32 \equiv 1 \pmod{31}$$

$\bar{2}$ est d'ordre 5 dans $\mathbb{Z}/31\mathbb{Z}$

4) $m = 9$

On a déjà établi, à l'exercice 6.7, que $\bar{2}$ est d'ordre 6 dans $\mathbb{Z}/9\mathbb{Z}$.

5) $m = 14$

$\bar{2}$ n'est pas une unité de $\mathbb{Z}/14\mathbb{Z}$, car $\text{pgcd}(2, 14) = 2 \neq 1$.

Il ne peut exister d'entier positif k tel que $a^k \equiv 1 \pmod{m}$, vu l'exercice 6.5