

6.16 $\varphi(24) = \varphi(2^3 \cdot 3) = 24 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$

Le théorème d'Euler implique $a^{\varphi(24)} \equiv a^8 \equiv 1 \pmod{24}$ pour tout entier a tel que $\text{pgcd}(a, 24) = 1$.

D'après l'exercice 6.13, l'ordre de tout élément non nul de $\mathbb{Z}/24\mathbb{Z}$ doit être un diviseur de 8; ce ne peut donc être que 1, 2, 4, ou 8.

1) $1^1 \equiv 1 \pmod{24}$
 $\bar{1}$ est d'ordre 1.

2) $\bar{2}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(2, 24) = 2 \neq 1$.

3) $\bar{3}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(3, 24) = 3 \neq 1$.

4) $\bar{4}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(4, 24) = 4 \neq 1$.

5) $5^1 \equiv 5 \not\equiv 1 \pmod{24}$
 $5^2 \equiv 25 \equiv 1 \pmod{24}$
 $\bar{5}$ est d'ordre 2.

6) $\bar{6}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(6, 24) = 6 \neq 1$.

7) $7^1 \equiv 7 \not\equiv 1 \pmod{24}$
 $7^2 \equiv 49 \equiv 1 \pmod{24}$
 $\bar{7}$ est d'ordre 2.

8) $\bar{8}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(8, 24) = 8 \neq 1$.

9) $\bar{9}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(9, 24) = 3 \neq 1$.

10) $\bar{10}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(10, 24) = 2 \neq 1$.

11) $11^1 \equiv 11 \not\equiv 1 \pmod{24}$
 $11^2 \equiv 121 \equiv 1 \pmod{24}$
 $\bar{11}$ est d'ordre 2.

12) $\bar{12}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(12, 24) = 12 \neq 1$.

13) $13^1 \equiv 13 \not\equiv 1 \pmod{24}$
 $13^2 \equiv (-11)^2 \equiv 121 \equiv 1 \pmod{24}$
 $\bar{13}$ est d'ordre 2.

14) $\bar{14}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(14, 24) = 2 \neq 1$.

15) $\bar{15}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(15, 24) = 3 \neq 1$.

16) $\bar{16}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(16, 24) = 8 \neq 1$.

- 17) $17^1 \equiv 17 \not\equiv 1 \pmod{24}$
 $17^2 \equiv (-7)^2 \equiv 49 \equiv 1 \pmod{24}$
 $\overline{17}$ est d'ordre 1.
- 18) $\overline{18}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(18, 24) = 6 \neq 1$.
- 19) $19^1 \equiv 19 \not\equiv 1 \pmod{24}$
 $19^2 \equiv (-5)^2 \equiv 25 \equiv 1 \pmod{24}$
 $\overline{19}$ est d'ordre 2.
- 20) $\overline{20}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(20, 24) = 4 \neq 1$.
- 21) $\overline{21}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(21, 24) = 3 \neq 1$.
- 22) $\overline{22}$ n'est pas une unité de $\mathbb{Z}/24\mathbb{Z}$, car $\text{pgcd}(22, 24) = 2 \neq 1$.
- 23) $23^1 \equiv 23 \not\equiv 1 \pmod{24}$
 $23^2 \equiv (-1)^2 \equiv 1 \pmod{24}$
 $\overline{23}$ est d'ordre 2.