

**6.15** Le petit théorème de Fermat fournit  $a^{17-1} \equiv a^{16} \equiv 1 \pmod{17}$  pour tout entier  $a$  non divisible par 17.

D'après l'exercice 6.13, l'ordre de tout élément non nul de  $\mathbb{Z}/17\mathbb{Z}$  doit être un diviseur de 16; ce ne peut donc être que 1, 2, 4, 8 ou 16.

- 1)  $1^1 \equiv 1 \pmod{17}$   
 $\overline{1}$  est d'ordre 1.
- 2)  $2^1 \equiv 2 \not\equiv 1 \pmod{17}$   
 $2^2 \equiv 4 \not\equiv 1 \pmod{17}$   
 $2^4 \equiv 16 \not\equiv 1 \pmod{17}$   
 $2^8 \equiv (2^4)^2 \equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$   
 $\overline{2}$  est d'ordre 8.
- 3)  $3^1 \equiv 3 \not\equiv 1 \pmod{17}$   
 $3^2 \equiv 9 \not\equiv 1 \pmod{17}$   
 $3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81 \equiv 13 \not\equiv 1 \pmod{17}$   
 $3^8 \equiv (3^4)^2 \equiv 13^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$   
 $3^{16} \equiv 1 \pmod{17}$   
 $\overline{3}$  est d'ordre 16.
- 4)  $4^1 \equiv 4 \not\equiv 1 \pmod{17}$   
 $4^2 \equiv 16 \not\equiv 1 \pmod{17}$   
 $4^4 \equiv (4^2)^2 \equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$   
 $\overline{4}$  est d'ordre 4.
- 5)  $5^1 \equiv 5 \not\equiv 1 \pmod{17}$   
 $5^2 \equiv 25 \equiv 8 \not\equiv 1 \pmod{17}$   
 $5^4 \equiv (5^2)^2 \equiv 8^2 \equiv 64 \equiv 13 \not\equiv 1 \pmod{17}$   
 $5^8 \equiv (5^4)^2 \equiv 13^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$   
 $5^{16} \equiv 1 \pmod{17}$   
 $\overline{5}$  est d'ordre 16.
- 6)  $6^1 \equiv 6 \not\equiv 1 \pmod{17}$   
 $6^2 \equiv 36 \equiv 2 \not\equiv 1 \pmod{17}$   
 $6^4 \equiv (6^2)^2 \equiv 2^2 \equiv 4 \not\equiv 1 \pmod{17}$   
 $6^8 \equiv (6^4)^2 \equiv 4^2 \equiv 16 \not\equiv 1 \pmod{17}$   
 $6^{16} \equiv 1 \pmod{17}$   
 $\overline{6}$  est d'ordre 16.
- 7)  $7^1 \equiv 7 \not\equiv 1 \pmod{17}$   
 $7^2 \equiv 49 \equiv 15 \not\equiv 1 \pmod{17}$   
 $7^4 \equiv (7^2)^2 \equiv 15^2 \equiv (-2)^2 \equiv 4 \not\equiv 1 \pmod{17}$

$$7^8 \equiv (7^4)^2 \equiv 4^2 \equiv 16 \not\equiv 1 \pmod{17}$$

$$7^{16} \equiv 1 \pmod{17}$$

$\overline{7}$  est d'ordre 16.

$$8) \quad 8^1 \equiv 8 \not\equiv 1 \pmod{17}$$

$$8^2 \equiv 64 \equiv 13 \not\equiv 1 \pmod{17}$$

$$8^4 \equiv (8^2)^2 \equiv 13^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$$

$$8^8 \equiv (8^4)^2 \equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$$

$\overline{8}$  est d'ordre 8.

$$9) \quad 9^1 \equiv 9 \not\equiv 1 \pmod{17}$$

$$9^2 \equiv 81 \equiv 13 \not\equiv 1 \pmod{17}$$

$$9^4 \equiv (9^2)^2 \equiv 13^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$$

$$9^8 \equiv (9^4)^2 \equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$$

$\overline{9}$  est d'ordre 8.

$$10) \quad 10^1 \equiv 10 \not\equiv 1 \pmod{17}$$

$$10^2 \equiv (-7)^2 \equiv 49 \equiv 15 \not\equiv 1 \pmod{17}$$

$$10^4 \equiv (10^2)^2 \equiv 15^2 \equiv (-2)^2 \equiv 4 \not\equiv 1 \pmod{17}$$

$$10^8 \equiv (10^4)^2 \equiv 4^2 \equiv 16 \not\equiv 1 \pmod{17}$$

$$10^{16} \equiv 1 \pmod{17}$$

$\overline{10}$  est d'ordre 16.

$$11) \quad 11^1 \equiv 11 \not\equiv 1 \pmod{17}$$

$$11^2 \equiv (-6)^2 \equiv 36 \equiv 2 \not\equiv 1 \pmod{17}$$

$$11^4 \equiv (11^2)^2 \equiv 2^2 \equiv 4 \not\equiv 1 \pmod{17}$$

$$11^8 \equiv (11^4)^2 \equiv 4^2 \equiv 16 \not\equiv 1 \pmod{17}$$

$$11^{16} \equiv 1 \pmod{17}$$

$\overline{11}$  est d'ordre 16.

$$12) \quad 12^1 \equiv 12 \not\equiv 1 \pmod{17}$$

$$12^2 \equiv (-5)^2 \equiv 25 \equiv 8 \not\equiv 1 \pmod{17}$$

$$12^4 \equiv (12^2)^2 \equiv 8^2 \equiv 64 \equiv 13 \not\equiv 1 \pmod{17}$$

$$12^8 \equiv (12^4)^2 \equiv 13^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$$

$$12^{16} \equiv 1 \pmod{17}$$

$\overline{12}$  est d'ordre 16.

$$13) \quad 13^1 \equiv 13 \not\equiv 1 \pmod{17}$$

$$13^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$$

$$13^4 \equiv (13^2)^2 \equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$$

$\overline{13}$  est d'ordre 4.

- 14)  $14^1 \equiv 14 \not\equiv 1 \pmod{17}$   
 $14^2 \equiv (-3)^2 \equiv 9 \not\equiv 1 \pmod{17}$   
 $14^4 \equiv (14^2)^2 \equiv 9^2 \equiv 81 \equiv 13 \not\equiv 1 \pmod{17}$   
 $14^8 \equiv (14^4)^2 \equiv 13^2 \equiv (-4)^2 \equiv 16 \not\equiv 1 \pmod{17}$   
 $14^{16} \equiv 1 \pmod{17}$   
 $\overline{14}$  est d'ordre 16.
- 15)  $15^1 \equiv 15 \not\equiv 1 \pmod{17}$   
 $15^2 \equiv (-2)^2 \equiv 4 \not\equiv 1 \pmod{17}$   
 $15^4 \equiv (15^2)^2 \equiv 4^2 \equiv 16 \not\equiv 1 \pmod{17}$   
 $15^8 \equiv (15^4)^2 \equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$   
 $\overline{15}$  est d'ordre 8.
- 16)  $16^1 \equiv 16 \not\equiv 1 \pmod{17}$   
 $16^2 \equiv (-1)^2 \equiv 1 \pmod{17}$   
 $\overline{16}$  est d'ordre 2.