

Exercice 1 : 1. On sait que  $4 \equiv 1 \pmod{3}$ , donc pour tout entier naturel  $n$ ,  $4^n \equiv 1^n \equiv 1 \pmod{3}$ .

2. Les nombres 4 et 29 étant premiers entre eux, d'après le petit théorème de Fermat,  $4^{28} \equiv 1 \pmod{29}$ , donc  $4^{28} - 1$  est divisible par 29.

3. a) Pour  $n = 1$ ,  $4 \equiv 4 \pmod{17}$ . Pour  $n = 2$ ,  $4^2 \equiv 16 \pmod{17}$ . Pour  $n = 3$ ,  $4^3 = 64 \equiv 13 \pmod{17}$ . Pour  $n = 4$ ,  $4^4 = 256 \equiv 1 \pmod{17}$ .

b) Donc, pour tout entier  $k$ , le nombre  $4^{4k} = (4^4)^k \equiv 1^k \equiv 1 \pmod{17}$ , donc  $4^{4k} - 1$  est divisible par 17.

4. Pour  $n = 1$ ,  $4 \equiv 4 \pmod{5}$ . Pour  $n = 2$ ,  $4^2 \equiv 1 \pmod{5}$ . Donc, pour tous les entiers naturels  $n$  pairs,  $4^n = (4^2)^k \equiv 1^k \equiv 1 \pmod{5}$ , et le nombre  $4^n - 1$  est-il divisible par 5.

5. D'après les questions précédentes, les nombres premiers 3, 5, 17 et 29 sont des diviseurs premiers de  $4^{28} - 1$ .

Exercice 2 : A. Question de cours : Montrons que l'ensemble des diviseurs communs de  $a$  et  $b$  est égal à l'ensemble des diviseurs communs de  $a$  et  $a - b$  :

Soit  $d \in D(a; b)$  ; alors il existe des entiers  $k$  et  $k'$  tels que  $a = kd$  et  $b = k'd$ , donc  $a - b = kd - k'd = d(k - k')$ , donc  $d$  divise  $a - b$ , donc  $d \in D(a; a - b)$ . Ainsi  $D(a; b) \subset D(a; a - b)$ .

Soit  $d \in D(a; a - b)$  ; alors il existe des entiers  $k$  et  $k'$  tels que  $a = kd$  et  $a - b = k'd$ , donc

$b = a - (a - b) = kd - k'd = d(k - k')$ , donc  $d$  divise  $b$ , donc  $d \in D(a; b)$ . Ainsi  $D(a; a - b) \subset D(a; b)$ .

Donc  $D(a; b) = D(a; a - b)$ . Leur plus grand élément est le même, soit  $\text{PGCD}(a; b) = \text{PGCD}(a; a - b)$ .

D'où, pour tout entier  $k$ ,  $\text{PGCD}(k + 1; k) = \text{PGCD}(k; 1) = 1$ .

B. 1. Montrons par récurrence que, pour tout entier naturel  $n$ ,  $x_n = 2^{n+1} + 1$  :

Initialisation : pour  $n = 0$ ,  $2^{0+1} + 1 = 3 = x_0$ .

Hérédité : supposons que pour une valeur de  $n$ ,  $x_n = 2^{n+1} + 1$  et montrons que  $x_{n+1} = 2^{n+2} + 1$  :

$x_{n+1} = 2x_n - 1 = 2(2^{n+1} + 1) - 1 = 2^{n+2} + 1$ . Ainsi, pour tout entier naturel  $n$ ,  $x_n = 2^{n+1} + 1$ .

2. Pour tout entier naturel  $n$ , le  $\text{PGCD}(x_{n+1}; x_n) = \text{PGCD}(2x_n - 1; x_n) = \text{PGCD}(x_n - 1; x_n) = 1$  en utilisant la partie A.

3. a) Démontrons par récurrence que, pour tout entier naturel  $n$ ,  $2x_n - y_n = 5$  :

Initialisation : pour  $n = 0$ ,  $2x_0 - y_0 = 2 \times 3 - 1 = 5$ .

Hérédité : supposons que pour une valeur de  $n$ ,  $2x_n - y_n = 5$  et montrons que  $2x_{n+1} - y_{n+1} = 5$  :

$2x_{n+1} - y_{n+1} = 2(2x_n - 1) - (2y_n + 3) = 2(2x_n - y_n) - 5 = 2 \times 5 - 5 = 5$ . Ainsi, pour tout entier naturel  $n$ ,  $2x_n - y_n = 5$ .

b) Donc, pour tout entier naturel  $n$ ,  $y_n = 2x_n - 5 = 2(2^{n+1} + 1) - 5 = 2^{n+2} - 3$ .

4. Soit  $d_n$  le PGCD de  $x_n$  et  $y_n$ . Alors  $d_n$  divise toute combinaison linéaire de  $x_n$  et  $y_n$ , donc divise  $2x_n - y_n = 5$ .

5.  $d_n = \text{PGCD}(x_n; y_n) = \text{PGCD}(x_n; 2x_n - 5) = \text{PGCD}(x_n; x_n - 5) = \text{PGCD}(x_n; 5)$ . Comme 5 est un nombre premier, si 5 divise  $x_n$ , alors  $d_n = 5$ , sinon  $d_n = 1$ . Donc  $x_n$  et  $y_n$  soient premiers entre eux si et seulement si  $d_n = 1$  si et seulement si 5 ne divise pas  $x_n$ . 5 divise  $x_n$ , si et seulement si  $x_n \equiv 0 \pmod{5}$  si et seulement si  $2^{n+1} \equiv -1 \equiv 4 \pmod{5}$  si et seulement si  $2^n \times 2 \equiv 2 \times 2 \pmod{5}$ , et en multipliant par 3, on obtient  $2^n \equiv 2 \pmod{5}$ . En regardant les puissances de 2 modulo 5, on trouve que  $n = 4k + 1$  avec  $k \in \mathbb{N}$ .

Donc,  $x_n$  et  $y_n$  soient premiers entre eux si et seulement si  $n \neq 4k + 1$  avec  $k \in \mathbb{N}$ .

Exercice 3 : 1. a) Une solution particulière de l'équation (E) est  $x_0 = 2$  et  $y_0 = -3$ .

b) Soit  $(x; y)$  un couple solution de (E). Alors  $8x + 5y = 8x_0 + 5y_0$ , soit  $8(x - x_0) = 5(y_0 - y)$ . D'après le théorème de Gauss, comme 8 et 5 sont premiers entre eux, 5 divise  $x - x_0$  donc il existe un entier  $k$  tel que  $x - x_0 = 5k$ , soit  $x = x_0 + 5k = 2 + 5k$ . Et  $8(5k) = 5(y_0 - y)$ , soit  $8k = y_0 - y$ , soit  $y = y_0 - 8k = -3 - 8k$ .

L'ensemble solution de l'équation (E) est  $\{(2 + 5k; -3 - 8k), k \in \mathbb{Z}\}$ .

2. a) On sait que  $N = 8a + 1 = -5b + 2$ , soit  $8a + 5b = 2 - 1 = 1$ , donc le couple  $(a; b)$  est solution de (E).

b) Alors le couple  $(a; b)$  est de la forme  $(2 + 5k; -3 - 8k)$  avec  $k \in \mathbb{Z}$ , donc  $N = 8a + 1 = 8(2 + 5k) + 1 = 40k + 17$ . Ainsi le reste, dans la division euclidienne de  $N$  par 40 est 17.