

Exercice (1):

1) Théorème de Bézout:

Soient a, b , deux entiers naturels non-nuls, (1)
 $\text{PGCD}(a; b) = 1 \Leftrightarrow \exists (u; v) \in \mathbb{Z}^2, au + bv = 1$

Démonstration: On suppose connue l'identité de Bézout

c'est-à-dire: Si $\text{PGCD}(a; b) = d$, alors il existe $(u; v) \in \mathbb{Z}^2, au + bv = d$

En prenant $d = 1$, on obtient l'implication:

$$\text{PGCD}(a; b) = 1 \Rightarrow \exists (u; v) \in \mathbb{Z}^2, au + bv = 1$$

Supposons maintenant que: $\exists (u; v) \in \mathbb{Z}^2, au + bv = 1$

notons $d = \text{PGCD}(a; b)$ ($d \in \mathbb{N}^*$)

(1.5)

$d \mid a$ et $d \mid b$, d'où d divise toute combinaison linéaire à coefficients entiers de a et b

En particulier: $d \mid au + bv = 1$

Comme $d \in \mathbb{N}$, alors $d = 1$

Par conséquent: $\text{PGCD}(a; b) = 1 \Leftrightarrow \exists (u; v) \in \mathbb{Z}^2, au + bv = 1$

2) Théorème de Gauss:

Soient a, b, c , trois entiers naturels, non nuls tels que:
 $a \mid bc$ et $\text{PGCD}(a; b) = 1$ (1)
 Alors, $a \mid c$

Démonstration: Comme $\text{PGCD}(a; b) = 1$, d'après le théorème de Bézout: $\exists (u; v) \in \mathbb{Z}^2, au + bv = 1$

En multipliant les deux membres de cette égalité, on obtient:

$$acu + bcv = c$$

$$a/bc \text{ et } a/ac$$

d'où a divise toute combinaison linéaire à coefficients entiers de bc et ac

En particulier: $a | ac + bc = c$

Donc $a | c$

3) $11x - 7y = 0 \Leftrightarrow 11x = 7y$

$$11 | 7y$$

$$\text{et } \text{PGCD}(11, 7) = 1$$

D'après le théorème de Gauss, $11 | y$

Or, $11 | y \Leftrightarrow \exists k \in \mathbb{Z}, y = 11k$

De même:

$$7 | 11x$$

$$\text{avec } \text{PGCD}(7, 11) = 1$$

D'après le théorème de Gauss, $7 | x$

Or, $7 | x \Leftrightarrow \exists k' \in \mathbb{Z}, x = 7k'$

Réciproquement:

$$11 \times 7k' = 7 \times 11k$$

$$\Leftrightarrow k' = k$$

Donc les solutions entières de l'équation $11x - 7y = 0$ sont données par:

$$S = \{ (7k; 11k), k \in \mathbb{Z} \}$$

4) a)

9 et 5 sont premiers entre eux, c'est-à-dire $\text{PGCD}(9, 5) = 1$

① D'après le théorème de Bézout: $\exists (x; y) \in \mathbb{Z}^2, 9x + 5y = 1$

b) Algorithme d'Euclide:

$$9 = 5 \times 1 + 4$$

$$5 = 4 \times 1 + \text{① dernier reste non nul}$$

$$4 = 1 \times 4 + 0$$

$$1 = 5 - 4 \times 1 = 5 - (9 - 5) = 9 \times (-1) + 5 \times 2$$

a	b	Reste
9	5	4
5	4	1
4	1	0

①

Donc $(-1; 2)$ est une solution particulière de l'équation (3)

Exercice (2) (16)

$$1) J^2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 1 + 1 \times 1 & 1 \times 1 + 1 \times 1 \\ 1 \times 1 + 1 \times 1 & 1 \times 1 + 1 \times 1 \end{pmatrix}$$

(0,5)

$$\text{Donc } J^2 = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} = 2J = 2^1 \times J$$

$$J^3 = J^2 \times J = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 2 \times 1 + 2 \times 1 & 2 \times 1 + 2 \times 1 \\ 2 \times 1 + 2 \times 1 & 2 \times 1 + 2 \times 1 \end{pmatrix} \quad (0,5)$$

$$J^3 = \begin{pmatrix} 4 & 4 \\ 4 & 4 \end{pmatrix} = 4J = 2^2 \times J$$

A la calculatrice, on trouve $J^4 = \begin{pmatrix} 8 & 8 \\ 8 & 8 \end{pmatrix} = 2^3 \times J$

On pourrait montrer par récurrence (pas demandé) que pour tout $n \in \mathbb{N}^*$, $J^n = 2^{n-1} \times J$ (0,5)

$$2) \underline{A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} = 2J + I}, \text{ en effet } 2J = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

(0,5)

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$2J + I = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} = A$$

$$A^2 = (2J + I)^2$$

$$= 4J^2 + 4J + I$$

(car I et J commutent)

$$= 4 \times 2J + 4J + I$$

(1)

$$\underline{A^2 = 12J + I}$$

$$A^3 = A \times A^2 = (2J + I) \times (12J + I)$$

$$A^3 = 24J^2 + 2J + 12J + I \quad (4)$$

$$= 24 \times 2J + 14J + I$$

$$A^3 = 62J + I \quad (1)$$

3) Raisonnons par récurrence:

* Initialisation:

$$A^0 = I \text{ et } I + \frac{5^0 - 1}{2} J = I + 0J$$

$$\text{d'où } A^0 = I + \frac{5^0 - 1}{2} J = I$$

donc la propriété est initialisée

* Hérédité:

on suppose la propriété vraie jusqu'à un certain rang $n \in \mathbb{N}$.

$$A^{n+1} = A \times A^n = (2J + I) \times \left(I + \frac{5^n - 1}{2} J \right)$$

$$= 2J + (5^n - 1)J^2 + I + \frac{5^n - 1}{2} J$$

$$= 2J + 2(5^n - 1)J + I + \frac{5^n - 1}{2} J$$

$$= I + \left[\frac{4}{2} + \frac{4(5^n - 1)}{2} + \frac{5^n - 1}{2} \right] J$$

$$= I + \left[\frac{4}{2} + \frac{4 \times 5^n}{2} - \frac{4}{2} + \frac{5^n - 1}{2} \right] J$$

$$= I + \left(\frac{5 \times 5^n - 1}{2} \right) J$$

$$A^{n+1} = I + \frac{5^{n+1} - 1}{2} J$$

donc la propriété est héritée

Par conséquent:

$$\text{Pour tout } n \in \mathbb{N}, A^n = I + \frac{5^n - 1}{2} J$$

Exercice (3): (5)

1)

$$\begin{cases} xy = 7776 \\ \text{PGCD}(x; y) = 18 \end{cases}$$

$$\text{on a } x = 18x'$$

$$\text{et } y = 18y', \text{ avec } \text{PGCD}(x'; y') = 1$$

$$\text{d'au}(S) \Leftrightarrow \begin{cases} 18^2 x' y' = 7776 \\ \text{PGCD}(x'; y') = 1 \end{cases}$$

(5)

$$\Leftrightarrow \begin{cases} x' y' = 24 \\ \text{PGCD}(x'; y') = 1 \end{cases}$$

(2)

Diviseurs de 24

$$\text{dans } \mathbb{N} = \{1; 2; 3; 4; 6; 8; 12; 24\}$$

x' et y' doivent être des diviseurs de 24, premiers entre eux
Différents cas possibles:

① $(x'; y') = (1; 24)$

② $(x'; y') = (24; 1)$

③ $(x'; y') = (3; 8)$

④ $(x'; y') = (8; 3)$

J'ai tous les couples solutions de (S):

$$(18 \times 1; 18 \times 24)$$

$$(18 \times 24; 18 \times 1)$$

$$(18 \times 3; 18 \times 8)$$

$$(18 \times 8; 18 \times 3)$$

C'est-à-dire :

$$S = \{(18; 432), (432; 18), (54; 144), (144; 54)\}$$

2) $n \in \mathbb{N}$: $a = 21n + 4$ $b = 16n + 3$

$$16a - 21b = 16 \times (21n + 4) - 21 \times (16n + 3)$$

$$= 64 - 63$$

$$= 1$$

(1,5)

car 16 et -21 sont des entiers.

D'après le théorème de Bézout, a et b sont premiers entre eux

3) $(a, b) \in \mathbb{N}^2$:

$$ab \equiv 0 [19] \Leftrightarrow 19 | ab$$

Or, 19 est un nombre premier

$$\text{et } 19 | a \Leftrightarrow a \equiv 0 [19]$$

* Soit $19 \nmid a$ et abais a et 19 sont premiers entre eux ⁽⁶⁾
d'après le théorème de Gauss, $19 \mid b \Rightarrow b \equiv 0 [19]$

Donc: $ab \equiv 0 [19] \Rightarrow a \equiv 0 [19] \text{ ou } b \equiv 0 [19]$ ⁽¹⁵⁾