

Exercice 1. $24x + 38y = 44$ (*)

page 1/4

Calculons $\text{pgcd}(24, 38)$ par l'algorithme d'Euclide :

$$38 = 24 + 14, \quad 24 = 14 + 10, \quad 14 = 10 + 4, \quad 10 = 4 \times 2 + 2 \quad \text{et} \quad 4 = 2 \times 2 + 0$$

Donc $\text{pgcd}(24, 38) = 2$. Comme 2 divise 44, l'équation (*) admet des solutions et est équivalente à $12x + 19y = 22$.

Cherchons une solution particulière en remontant l'algorithme d'Euclide pour déterminer une relation de Bézout :

$$2 = 10 - 4 \times 2 = 10 - (14 - 10) \times 2 = 10 \times 3 - 14 \times 2 = (24 - 14) \times 3 - 14 \times 2 = 24 \times 3 - 14 \times 5$$

$$2 = 24 \times 3 - (38 - 24) \times 5 = 24 \times 8 - 38 \times 5 \quad \text{donc} \quad 44 = 2 \times 22 = 24 \times 8 \times 2 - 38 \times 5 \times 2 \\ = 24 \times 176 - 38 \times 110$$

Donc $(x_0, y_0) = (176, -110)$ est une solution particulière de l'équation (*).

On a alors $24x + 38y = 24x_0 + 38y_0 \iff 24(x - x_0) = 38(y_0 - y)$.

$$\iff 12(x - x_0) = 19(y_0 - y)$$

Comme 12 divise $19(y_0 - y)$ et 12 est premier avec 19, d'après le lemme de Gauss, 12 divise $y_0 - y$ donc il existe $k \in \mathbb{Z}$ tel que $y_0 - y = 12k$.

donc $y = y_0 - 12k$. Alors $12(x - x_0) = 19 \times 12k \iff x - x_0 = 19k \iff x = x_0 + 19k$.

Par conséquent $\{(176 + 19k, -110 - 12k), k \in \mathbb{Z}\}$ est l'ensemble des solutions de l'équation (*).

Exercice 2

1. Soit $n \in \mathbb{N}$. Si $n \equiv 0 [2]$ alors $n^2 \equiv 0 [2]$

Si $n \equiv 1 [2]$ alors $n^2 \equiv 1 [2]$

2. Donc si n^2 est pair, c'est-à-dire $n^2 \equiv 0 [2]$, on ne peut avoir que $n \equiv 0 [2]$ donc n est pair.

2. Soit $n \in \mathbb{N}$ multiple de 3. Alors il existe $k \in \mathbb{Z}$ tel que $n = 3k$.

2. On a $2^n - 1 = 2^{3k} - 1 = (2^3)^k - 1 \equiv 1^k - 1 \equiv 0 [7]$ car $2^3 \equiv 8 \equiv 1 [7]$.

Donc 7 divise $2^n - 1$.

Exercice 3

1. $368 = 123 \times 3 - 1$ donc $368 \equiv -1 [123]$

On a alors $368^n \equiv (-1)^n [123]$ pour tout $n \in \mathbb{N}$

1.5 Comme pour $n = 12345678 \dots 20$, n est pair, on a alors $368^n \equiv 1 [123]$

Donc le reste dans la division par 123 de $368^{12345 \dots 20}$ est 1.

2. On a $2021 \equiv 1 [2]$

alors $2021^{19} \equiv 1^{19} \equiv 1 [2]$

1.5

Le dernier chiffre de l'écriture en binaire de 2021^{19} correspond au reste de la division de 2021^{19} par 2, c'est donc un 1.

Exercice 4 $S: \begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 17 \pmod{20} \end{cases}$

$$20 = 5 \times 2^2 \text{ et } 12 = 3 \times 2^2$$

On a $\text{pgcd}(20, 12) = 4$. Comme 4 divise $17 - 5 = 12$, le système S admet des solutions et $S \Rightarrow S': \begin{cases} x \equiv 5 \pmod{3} \\ x \equiv 17 \pmod{5} \end{cases}$

(Cherchons une solution particulière du système S' en utilisant une relation de Bézout: $1 = 5 \times 2 - 3 \times 3$

On a donc $\begin{cases} 5 \times 2 \equiv 1 \pmod{3} \\ 5 \times 2 \equiv 0 \pmod{5} \end{cases}$ et $\begin{cases} -3 \times 3 \equiv 0 \pmod{3} \\ -3 \times 3 \equiv 1 \pmod{5} \end{cases}$

on peut en déduire que $x_0 = 5 \times 5 \times 2 - 3 \times 3 \times 17 = 50 - 153 = -103$ est une solution particulière de S' , mais aussi de S . En effet,

$$\begin{cases} -103 \equiv 100 - 103 \equiv 17 \equiv 5 \pmod{12} \\ -103 \equiv 100 - 103 \equiv -3 \equiv 17 \pmod{20} \end{cases}$$

On a donc $\begin{cases} x \equiv x_0 \pmod{12} \\ x \equiv x_0 \pmod{20} \end{cases} \Leftrightarrow \begin{cases} x - x_0 \equiv 0 \pmod{12} \\ x - x_0 \equiv 0 \pmod{20} \end{cases}$

$$\Leftrightarrow x - x_0 \equiv 0 \pmod{\text{ppcm}(12, 20)} \Leftrightarrow x \equiv x_0 \pmod{60} \Leftrightarrow x \equiv -103 \equiv 17 \pmod{60}$$

Par conséquent, $\{17 + 60k, k \in \mathbb{Z}\}$ est l'ensemble des solutions de S .

Exercice 5

1. $8x \equiv 4 \pmod{12}$

Comme $\text{pgcd}(8, 12) = 4$ et 4 divise 4, l'équation admet des solutions et est équivalente à: $2x \equiv 1 \pmod{3}$

(Cherchons l'inverse de 2 modulo 3 en passant par une relation de Bézout:

2 $1 = 2 \times 2 - 3$ donc 2 est l'inverse de 2 modulo 3.

On a alors $2x \equiv 1 \pmod{3} \Leftrightarrow 2 \times 2 \times x \equiv 1 \times 2 \pmod{3} \Leftrightarrow x \equiv 2 \pmod{3}$

Par conséquent, $\{2 + 3k, k \in \mathbb{Z}\}$ est l'ensemble des solutions de l'équation

2. $8x \equiv 3 \pmod{12}$ Comme $\text{pgcd}(8, 12) = 4$ et 4 ne divise pas 3, donc l'équation n'admet pas de solution dans \mathbb{Z} .

Exercice 6

1. Soient $a, n \in \mathbb{N}^*$ alors a est inversible modulo n \Leftrightarrow il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 [n]$ \Leftrightarrow il existe $b \in \mathbb{Z}, k \in \mathbb{Z}$ tel que $ab = 1 + kn \Leftrightarrow ab - kn = 1$ 2 $\Leftrightarrow a$ et n sont premiers entre eux d'après le théorème de Bézout pour des nombres premiers entre eux.2. $(\mathbb{Z}/12\mathbb{Z})^*$ est l'ensemble des éléments de $\mathbb{Z}/12\mathbb{Z}$ qui sont inversibles1 D'après la question 1, \bar{a} est inversible ^{dans $\mathbb{Z}/12\mathbb{Z}$} si et seulement si a et 12 sont premiers entre eux donc $(\mathbb{Z}/12\mathbb{Z})^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

Exercice 7

On a $2^2 \equiv 4 [17]$, $2^3 \equiv 8 [17]$, $2^4 \equiv 16 \equiv -1 [17]$ donc $2^8 \equiv 1 [17]$ On a aussi $83 \equiv 3 [8]$ et $3^2 \equiv 9 \equiv 1 [8]$ donc $83^{100} \equiv 3^{100} \equiv (3^2)^{50} \equiv 1 [8]$ 2 Donc il existe $k \in \mathbb{Z}$ tel que $83^{100} = 8k + 1$ Par conséquent $2^{(83^{100})} \equiv 2^{8k+1} \equiv (2^8)^k \times 2 \equiv 1^k \times 2 \equiv 2 [17]$ Donc le reste de $2^{(83^{100})}$ dans la division euclidienne par 17 est 2