

Exercice 1 :

Soit A l'ensemble des entiers naturels de l'intervalle $[1 ; 46]$.

1. On considère l'équation

$$(E) : 23x + 47y = 1$$

où x et y sont des entiers relatifs.

- (a) Donner une solution particulière (x_0, y_0) de (E) .
 - (b) Déterminer l'ensemble des couples (x, y) solutions de (E) .
 - (c) En déduire qu'il existe un unique entier x appartenant à A tel que $23x \equiv 1 \pmod{47}$.
2. Soient a et b deux entiers relatifs.
- (a) Montrer que si $ab \equiv 0 \pmod{47}$ alors $a \equiv 0 \pmod{47}$ ou $b \equiv 0 \pmod{47}$.
 - (b) En déduire que si $a^2 \equiv 1 \pmod{47}$ alors $a \equiv 1 \pmod{47}$ ou $a \equiv -1 \pmod{47}$.
3. (a) Montrer que pour tout entier p de A , il existe un entier relatif q tel que $p \times q \equiv 1 \pmod{47}$.
Pour la suite, on admet que pour tout entier p de A , il existe un unique entier, noté $inv(p)$, appartenant à A tel que
 $p \times inv(p) \equiv 1 \pmod{47}$.
Par exemple :
 $inv(1) = 1$ car $1 \times 1 \equiv 1 \pmod{47}$, $inv(2) = 24$ car $2 \times 24 \equiv 1 \pmod{47}$,
 $inv(3) = 16$ car $3 \times 16 \equiv 1 \pmod{47}$.
- (b) Quels sont les entiers p de A qui vérifient $p = inv(p)$?
 - (c) On rappelle que $46! = 46 \times 45 \times \cdots \times 2 \times 1$.
Montrer que $46! \equiv -1 \pmod{47}$.

Correction :

Soit A l'ensemble des entiers naturels de l'intervalle $[1 ; 46]$.

1. On considère l'équation

$$(E) : 23x + 47y = 1$$

où x et y sont des entiers relatifs.

(a) $(-2; 1)$ est une solution de (E) car $-2 \times 23 + 1 \times 47 = 1$.

(b) $(x ; y)$ solution de $(E) \Rightarrow 23x + 47y = 1$

$$\begin{cases} 23x + 47y &= 1 \\ -2 \times 23 + 1 \times 47 &= 1 \end{cases} \quad \begin{array}{l} \text{par soustraction} \\ \Rightarrow \end{array} \quad 23(x + 2) + 47(y - 1) = 0 \Rightarrow 23(x + 2) = 47(1 - y)$$

Donc 23 divise $47(1 - y)$, mais 47 et 23 sont premiers entre eux, d'après le théorème de Gauss, 23 divise $1 - y$.

Donc il existe un entier relatif k tel que $1 - y = 23k$ soit $y = 1 - 23k$

On a donc aussi, $23(x + 2) = 47 \times 23k \iff x = 47k - 2$

On vérifie que, réciproquement, pour tout entier relatif k , $(47k - 2; 1 - 23k)$ est bien solution de (E) .

L'ensemble des solutions de (E) est l'ensemble des couples $(47k - 2; 1 - 23k)$ où $k \in \mathbb{Z}$.

(c) $23x \equiv 1 \pmod{47} \iff$ il existe $y \in \mathbb{Z}$, $23x = 1 - 47y \iff$ il existe $k \in \mathbb{Z}$, $x = 47k - 2$ et $y = 1 - 23k$

De plus $x \in A \iff 1 \leq 47k - 2 \leq 46 \iff 3 \leq 47k \leq 48$.

Or un seul multiple de 47 se trouve dans cet encadrement, c'est 47. Donc $k = 1$ et $x = 45$.

Le seul entier x appartenant à A tel que $23x \equiv 1 \pmod{47}$ est 45.

2. Soient a et b deux entiers relatifs.

(a) $ab \equiv 0 \pmod{47} \iff 47$ divise ab .

Or 47 est un nombre premier, il apparaît donc au moins dans l'une des deux décompositions de a ou de b . D'où le résultat.

(b) $a^2 \equiv 1 \pmod{47} \iff a^2 - 1 \equiv 0 \pmod{47} \iff (a - 1)(a + 1) \equiv 0 \pmod{47} \xrightarrow{2a} a - 1 \equiv 0 \pmod{47}$ ou $a + 1 \equiv 0 \pmod{47} \dots$

3. (a) Tout entier p de A est premier avec 47, donc le théorème de Bezout assure l'existence de (q, s) entiers relatifs tels que $qp + 47s = 1$.

On a alors $p \times q \equiv 1 \pmod{47}$.

(b) $p = \text{inv}(p) \Rightarrow p^2 \equiv 1 \pmod{47} \xrightarrow{2b} p \equiv -1 \pmod{47}$ ou $p \equiv 1 \pmod{47} \xrightarrow{p \in A} p = 46$ ou $p = 1$

Réciproquement 1 et 46 conviennent bien.

(c) Pour tout entier p de A compris entre 2 et 45, il existe (d'après 3a) un entier de A **distinct** (d'après 3b) $\text{inv}(p)$ tel que $p \times \text{inv}(p) \equiv 1 \pmod{47}$, donc $45! \equiv 1 \pmod{47}$. On en déduit $46! \equiv 46 \pmod{47}$ soit enfin $46! \equiv -1 \pmod{47}$.