



# Interrogation 15

## Arithmétique

### Exercice 1 :

Donner les définitions ou énoncés précis suivants avec quantificateurs et rédaction :

1. Théorème de Bézout.

Soit  $a, b \in \mathbb{Z}$ .

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}, au + bv = 1.$$

2. Lemme d'Euclide.

Soit  $p \in \mathbb{N}$  premier,  $a, b \in \mathbb{Z}$ . Si  $p|ab$ , alors  $p|a$  ou  $p|b$ .

3. Lemme de Gauss.

Soit  $a, b, c \in \mathbb{Z}$ ,  $a \neq 0$ . Si  $a|bc$  et  $a \wedge b = 1$ , alors  $a|c$ .

4. Définition d'un nombre premier.

Soit  $p \in \mathbb{N}$ .  $p$  est premier si  $p \geq 2$  et  $\text{Card}(\text{Div}_+(p)) = 2$  (i.e.  $\text{Div}_+(p) = \{1, p\}$ ).

5. Lien entre PGCD et PPCM.

Soit  $a, b \in \mathbb{Z}$ . Si  $a \wedge b = 1$ , alors  $a \vee b = |ab|$ . Et en général :  $(a \wedge b)(a \vee b) = |ab|$

6. Division euclidienne.

Soit  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ . Alors  $\exists!(q, r) \in \mathbb{Z}^2$  tel que  $a = bq + r$ ,  $0 \leq r < b$ .

7. Caractérisation du PGCD par des entiers premiers entre eux.

Soit  $a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$ . Soit  $d \in \mathbb{N}$ . Alors  $d = a \wedge b \iff \exists a', b' \in \mathbb{Z}$ ,  $a' \wedge b' = 1$ ,  $a = da'$ ,  $b = db'$ .

8. Définition de la valuation  $p$ -adique.

Soit  $n \in \mathbb{Z}^*$  et  $p \in \mathcal{P}$ . La valuation  $p$ -adique de  $n$ , noté  $v_p(n)$ , est défini par

$$v_p(n) = \max\{k \in \mathbb{N}, p^k | n\}.$$

### Exercice 2 :

Résoudre l'équation  $3x + 7y = 9$ .

Notons que le couple  $(3, 0)$  est solution de l'équation.

Soit  $x, y \in \mathbb{Z}$  tels que  $3x + 7y = 9$ . Alors  $7y = 3(3 - x)$ . Donc  $3|7y$ . Or  $3 \wedge 7 = 1$ . Donc, par lemme de Gauss,  $3|y$ . Donc  $\exists k \in \mathbb{Z}$  tel que  $y = 3k$ . Et donc  $7k = 3 - x$ . Donc  $x = 3 - 7k$ . Donc  $\exists k \in \mathbb{Z}$  tel que  $(x, y) = (3 - 7k, 3k)$ .

Réciproquement,  $\forall k \in \mathbb{Z}$ ,  $3(3 - 7k) + 7 \times 3k = 9$ .

Donc :

$$\{(x, y) \in \mathbb{Z}, 3x + 7y = 9\} = \{(3 - 7k, 3k), k \in \mathbb{Z}\}.$$