Arithmétique dans $\mathbb{Z}$

1 – Divisibilité, notation $a|b$, propriétés. Entiers associés. Théorème de division euclidienne dans $\mathbb{Z}$. Théorème : les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ (avec $n \in \mathbb{N}$).

2 – Congruences. La congruence modulo n est une relation d'équivalence compatible avec la somme et le produit. Applications : critères de divisibilité en base 10.

3 – PGCD. Existence d'une relation $a \wedge b = au + bv$. Homogénéité : $(ak) \wedge (bk) = (a \wedge b)|k|$. Algorithme d'Euclide. Calcul des coefficients u et v (en « remontant » l'algorithme d'Euclide).

4 – Entiers premiers entre eux. Théorème de Bézout. Lemme de Gauss. Application : représentant irréductible d'un rationnel et résolution des équations $ax + by = c$ dans $\mathbb{Z}^2$.

5 – Nombres premiers. L'ensemble $\mathscr{P}$ est infini. Théorème de décomposition en facteurs premiers. Valuation p-adique. Caractérisation de la divisilité en termes de décomposition en facteurs premiers.

6 – Définition du PPCM. Décomposition du facteurs premiers du PGCD et du PPCM. Relation $ab = (a \wedge b)(a \vee b)$ pour $a, b \in \mathbb{N}^*$.

7 – Inversibilité modulo n.

8 – Si p est premier, $(a + b)^p \equiv a^p + b^p \mod p$.

9 – Petit théorème de Fermat.