

## Programme de colle (DERNIER) - semaine 30 du 08/06/2026 au 14/06/2026

### 1 Arithmétique dans $\mathbb{Z}$

Les démonstrations à savoir sont marquées d'un (\*)

- Divisibilité. Division euclidienne (énoncé à connaître).
- PGCD de deux entiers naturels  $a, b$  avec  $(a, b) \neq (0, 0)$ . Algorithme d'Euclide (savoir l'expliquer), relation de Bézout. Extension du PGCD à  $\mathbb{Z}^2$ .  
Équivalence entre  $(d|a \text{ et } d|b)$  et  $d|a \wedge b$  (\*).  
Commutativité, associativité,  $\forall a, b, k \in \mathbb{N}, (ka) \wedge (kb) = k(a \wedge b)$ .
- Couple d'entiers premiers entre eux. Théorème de Bézout (\*).  
Lemme de Gauss (si  $a|bc$  et  $a \wedge b = 1$ , alors  $a|c$ ) et propriété sans nom (si  $a|c, b|c$  et  $a \wedge b = 1$ , alors  $ab|c$ ) (ces 2 propriétés \*).
- Généralisation à  $n$  entiers ( $n \geq 3$ ) : PGCD, entiers premiers entre eux dans leur ensemble / premiers entre eux deux à deux. Relation et théorème de Bézout.
- PPCM de deux entiers naturels non nuls. Relation entre le PGCD et le PPCM. Équivalence entre  $(a|m \text{ et } b|m)$  et  $a \vee b|m$ .
- Nombres premiers : définition, l'ensemble est infini (\*). Théorème de décomposition en produit de facteurs premiers (existence et unicité) (démonstration non exigible). Si un nombre premier divise un produit de facteurs, alors il divise l'un des facteurs (\*). Valuation  $p$ -adique d'un entier  $> 0$ , utilisation pour le calcul du PGCD, PPCM.
- Petit théorème de Fermat (\*) : si  $p$  est premier et  $x \in \mathbb{Z}$ , alors  $x^p \equiv x[p]$ . Si en plus  $p$  ne divise pas  $x$ , alors  $x^{p-1} \equiv 1[p]$ .  
Les ensembles  $\mathbb{Z}/n\mathbb{Z}$  ne sont pas au programme en MPSI.

### 2 Exercices faits

#### 1. Équation diophantienne linéaire

*L'exercice est long, ne pas hésiter à n'en donner qu'une partie, ou travailler directement sur un exemple.*

Soit  $a, b, c$  des entiers ( $a$  et  $b$  non nuls). Le but de l'exercice est de décrire la méthode générale permettant de résoudre l'équation  $(E) : ax + by = c$ , d'inconnue  $(x, y) \in \mathbb{Z}^2$ .

- a) Montrer que si  $(E)$  admet des solutions, alors  $a \wedge b|c$ .  
Dans toute la suite, on suppose que  $a \wedge b|c$ .
- b) Donner  $a', b', c' \in \mathbb{Z}$  avec  $a' \wedge b' = 1$ , tels que  $(E)$  soit équivalente à  $a'x + b'y = c'$ .
- c) Montrer que  $(E)$  admet au moins une solution.
- d) On considère l'équation  $(E_0) : a'x + b'y = 0$ .  
Montrer que si  $(x, y)$  est solution de  $(E_0)$ , alors  $a'|y$ .
- e) Décrire l'ensemble des solutions de  $(E_0)$  puis l'ensemble des solutions de  $(E)$ .
- f) Un exemple à résoudre

#### 2. CCINP exo 94

- a) Énoncer le théorème de Bézout dans  $\mathbb{Z}$ .
- b) Soit  $a$  et  $b$  deux entiers naturels premiers entre eux. Soit  $c \in \mathbb{N}$ .  
Prouver que :  $(a|c \text{ et } b|c) \Leftrightarrow ab|c$ .

c) On considère le système  $(S) : \begin{cases} x \equiv 6 & [17] \\ x \equiv 4 & [15] \end{cases}$  dans lequel l'inconnue  $x$  appartient à  $\mathbb{Z}$ .

i) Déterminer une solution particulière  $x_0$  de  $(S)$  dans  $\mathbb{Z}$ .

ii) *Déduire des questions précédentes* la résolution dans  $\mathbb{Z}$  du système  $(S)$ .

### 3. Questions indépendantes

a) Pour  $n \in \mathbb{N}$ , soit  $u_n = 5^{2^n} - 1$ .

i) Déterminer  $v_2(u_0), v_2(u_1)$  ( $v_2$  : valuation 2-adique).

ii) Montrer que  $\forall n \in \mathbb{N}, v_2(u_n) = n + 2$ .

b) Soit  $n \in \mathbb{N}$ . Vérifier que  $(2n + 1) \binom{2n}{n} = (n + 1) \binom{2n + 1}{n + 1}$ . En déduire que  $n + 1$  divise  $\binom{2n}{n}$ .