

## Programme de colle - Semaine 16

---

### Notation

On adoptera les principes suivants pour noter les étudiants :

- × si l'étudiant sait répondre à la question de cours, il aura une note  $> 8$ .
- × si l'étudiant ne sait pas répondre à la question de cours ou s'il y a trop d'hésitations, il aura une note  $\leq 8$ .

### Questions de cours

#### • PGCD et algorithme d'Euclide

Soit  $(a, b) \in \mathbb{Z}^2$ . Soit  $\lambda \in \mathbb{Z}$ .

$$a \wedge b = a + \lambda b \wedge b$$

On demandera à l'étudiant, en plus de la démonstration de l'égalité précédente, un calcul de pgcd par algorithme d'Euclide.

*Démonstration.*

On procède par double divisibilité.

- Démontrons :  $a \wedge b \mid (a + \lambda b) \wedge b$ .

Par définition de  $a \wedge b$ , on a :

$$\begin{array}{llll} & a \wedge b \mid a & \text{ET} & a \wedge b \mid b \\ \text{donc} & a \wedge b \mid a & \text{ET} & a \wedge b \mid \lambda b \quad (\text{car } \lambda \in \mathbb{Z}) \\ \text{d'où} & a \wedge b \mid (a + \lambda b) & \text{ET} & a \wedge b \mid b \\ \text{ainsi} & a \wedge b \mid (a + \lambda b) \wedge b & & (\text{par définition de } \\ & & & (a + \lambda b) \wedge b) \end{array}$$

- Démontrons :  $(a + \lambda b) \wedge b \mid a \wedge b$ .

On note :  $d = (a + \lambda b) \wedge b$ . Par définition de  $(a + \lambda b) \wedge b$ , on a :

$$\begin{array}{llll} & d \mid (a + \lambda b) & \text{ET} & d \mid b \\ \text{donc} & d \mid (a + \lambda b) & \text{ET} & d \mid \lambda b \quad (\text{car } \lambda \in \mathbb{Z}) \\ \text{d'où} & d \mid a & \text{ET} & d \mid b \\ \text{ainsi} & & & \mid a \wedge b \quad (\text{par définition de } a \wedge b) \end{array}$$

Finalement :  $|a \wedge b| = |(a + \lambda b) \wedge b|$ . Or un pgcd est positif. Ainsi :

$$a \wedge b = (a + \lambda b) \wedge b$$

□

• **Existence d'un diviseur premier**

Tout entier supérieur ou égal à 2 admet au moins un diviseur premier.

*On demandera à l'étudiant, en plus de la démonstration de la proposition précédente, un calcul de pgcd par décomposition en facteurs premiers.*

*Démonstration.*

Démontrons par récurrence (forte) :  $\forall n \in \llbracket 2, +\infty \llbracket, \mathcal{P}(n)$  où  $\mathcal{P}(n)$  :  $n$  admet au moins un diviseur premier.

► **Initialisation**

Le nombre 2 admet 2 comme diviseur premier.

D'où  $\mathcal{P}(2)$ .

► **Hérédité** : soit  $n \in \llbracket 2, +\infty \llbracket$ .

Supposons :  $\forall d \in \llbracket 2, n \llbracket, \mathcal{P}(d)$ . Démontrons  $\mathcal{P}(n+1)$  (i.e.  $n+1$  admet au moins un diviseur premier).

Deux cas se présentent :

× si  $n+1$  est premier, alors il admet un diviseur premier : lui-même.

× si  $n+1$  n'est pas premier, alors il admet des diviseurs positifs autres que 1 et  $n+1$ .

Notons  $d$  l'un de ces diviseurs positifs. Alors il existe  $k \in \mathbb{N}$  tel que :  $n+1 = kd$ . De plus :

$$\begin{aligned} 1 &< d < n+1 \\ \text{donc } 2 &\leq d \leq n && (\text{car } d \in \mathbb{N}) \end{aligned}$$

Par hypothèse de récurrence,  $d$  admet un diviseur premier. Notons le  $\delta$ . Alors il existe  $k' \in \mathbb{N}$  tel que :  $d = k'\delta$ . D'où :

$$n+1 = kd = k k' \delta$$

Ainsi :  $\delta \mid n+1$ . Comme  $\delta$  est premier, on en déduit que  $n+1$  admet bien un diviseur premier. D'où  $\mathcal{P}(n+1)$ .

□

• **Résolution d'un système linéaire par pivot de Gauss**

## Connaissances exigibles

### Arithmétique

- Relation de divisibilité dans  $\mathbb{Z}$  : définition et propriétés
- Division euclidienne dans  $\mathbb{Z}$  et  $\mathbb{N}$
- Descente de Fermat : principe et code **Python**
- Congruence : définition et propriétés
- PGCD : définition et propriétés
- Algorithme d'Euclide : principe et code **Python** (impératif et récursif)
- PPCM : définition et propriétés
- Nombres premiers entre eux : définition
- Nombres premiers : définition et propriétés
- Existence d'une infinité de nombres premiers
- Crible d'Ératostène
- Décomposition en produit de facteurs premiers. Application au calcul de PGCD et PPCM

### Systèmes linéaires et matrices

- Système linéaire, homogène, de Cramer, échelonné, triangulaire
- Algorithme du pivot de Gauss
- Matrice rectangle, carrée, ligne, colonne, nulle, identité, élémentaire, scalaire, triangulaire inférieure, triangulaire supérieure, diagonale
- Somme de matrices
- Produit externe d'une matrice par un scalaire
- Produit de matrices (interne dans le cas de matrices carrées de même ordre)
- Puissance  $m^{\text{ème}}$  d'une matrice
- Symbole de Kronecker
- Interprétation des opérations élémentaires à l'aide de matrices



On sanctionnera fortement les points suivants :

- × toute confusion d'objets,
- × toute confusion variable libre / liée (ou muette),
- × tout oubli d'introduction de variable (cela rejoint le point précédent),
- × toute erreur de logique (absence ou erreur de connecteur logique par exemple),
- × tout manque de réflexe dans l'utilisation des structures de démonstration.