Semaine du 23/01 au 27/01

1 Cours

Arithmétique

Division dans $\mathbb{Z}$ Relation de divisibilité. Opérations sur la divisibilité. Relation de congruence. Opérations sur la congruence. Division euclidienne.

Diviseurs et multiples communs PGCD : définition, existence et unicité d'un pgcd positif. Opérations sur le pgcd. Algorithme d'Euclide. Théorème de Bézout. Algorithme d'Euclide étendu. Nombres premiers entre eux. Théorème de Bézout (équivalence). Théorème de Gauss. Si $a|n$ et $b|n$ avec $a \wedge b = 1$, alors $ab|n$. Si $a \wedge n = 1$ et $b \wedge n = 1$, alors $ab \wedge n = 1$. PPCM : définition, existence et unicité d'un ppcm positif. Relation $(a \vee b)(a \wedge b) = |ab|$. Opérations sur le ppcm.

Nombres premiers Définition. Lemme d'Euclide. Tout entier $n > 1$ admet un diviseur premier. Infinité des nombres premiers. Décomposition en facteurs premiers. Valuation p-adique. Lien avec la divisibilité, le pgcd et le ppcm.

Compléments PGCD d'un nombre fini d'entiers. Théorème de Bézout. Entiers premiers entre eux dans leur ensemble. Théorème de Bézout (équivalence).

Espaces vectoriels

Définition et exemples fondamentaux Définition d'un $\mathbb{K}$-espace vectoriel. Exemples. Si X est un ensemble, on peut munir $\mathbb{K}^X$ d'une struture de $\mathbb{K}$-espace vectoriel. Conséquence : $\mathbb{K}^n$, $\mathbb{K}^{\mathbb{N}}$, $\mathbb{K}^{\mathbb{K}}$ sont des $\mathbb{K}$-espaces vectoriels.

Sous-espaces vectoriels Définition. Intersection de sous-espaces vectoriels. Combinaisons linéaires d'une famille de vecteurs. Espace vectoriel engendré par une partie ou une famille.

2 Méthodes à maîtriser

- Se ramener à des entiers premiers entre eux en factorisant par le pgcd.
- Résoudre des équations diophantiennes linéaires i.e. du type $ax + by = c$ avec $a, b, c \in \mathbb{Z}$ et x, y des inconnues entières.
- Caractériser le reste d'une division euclidienne par une relation de congruence.
- Montrer que deux entiers positifs sont égaux en montrant qu'ils se divisent l'un l'autre
- Savoir montrer que deux entiers sont premiers entre eux en exhibant une relation de Bézout.
- Savoir montrer qu'une partie d'un espace vectoriel en est un sous-espace vectoriel.
- Savoir déterminer une partie génératrice d'une partie de $\mathbb{K}^n$ définie par des équations linéaires.
- Dans le cadre de l'algèbre linéaire, se fier à son intuition **géométrique**.

3 Questions de cours

- Démontrer le petit théorème de Fermat : si p est un nombre premier, alors pour tout $x \in \mathbb{Z}$, $x^p \equiv x[p]$.
- Soient r un entier supérieur ou égal à 2 et $(a_1, \dots, a_r) \in \mathbb{Z}^r$. On pose pour $i \in [\![1, r]\!]$, $b_i = \prod_{j \in [\![1,r]\!] \setminus \{i\}} a_j$. Montrer que $a_1, \dots, a_r$ sont premiers entre eux deux à deux **si et seulement si** $b_1, \dots, b_r$ sont premiers entre eux dans leur ensemble.
- Résoudre un système de congruences $\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases}$ d'inconnue $x \in \mathbb{Z}$ au choix de l'examinateur.
- Nombres de Fermat. Soit $m \in \mathbb{N}$. Montrer que si $2^m + 1$ est premier, alors m est une puissance de 2. On pose alors $F_n = 2^{2^n} + 1$ pour $n \in \mathbb{N}$. Montrer que pour $m \neq n$, $F_m \wedge F_n = 1$.