Semaine du 27/01 au 31/01

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 $\mathbb{K}^{\mathrm{X}}$ 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.

Somme de sous-espaces vectoriels Somme de deux sous-espaces vectoriels.

2 Méthodes à maîtriser

- De manière générale, divisibilité = factorisabilité.
- Montrer que deux entiers positifs sont égaux en montrant qu'ils se divisent l'un l'autre (notamment pour montrer que deux PGCD sont égaux).
- Pour montrer qu'un entier a divise un entier b, on peut suivant le cas :
  - factoriser b par a (on pensera notamment à la formule de Bernoulli) ;
  - montrer que $b \equiv 0[a]$.
- Calculer avec des congruences (notamment lorsque $a \equiv 1[n]$, alors $a^k \equiv 1[n]$).
- Caractériser le reste d'une division euclidienne par une relation de congruence.
- 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.
- Résoudre un système de congruences.
- Se ramener à des entiers premiers entre eux en factorisant par le pgcd.
- Pour montrer que des entiers sont premiers entre eux, on peut suivant le cas :
  - montrer que leur PGCD divise 1 et donc vaut 1 ;
  - exhiber une relation de Bezout ;
  - montrer par l'absurde qu'ils ne possèdent pas de diviseur premier commun ;
- Montrer qu'un entier p est premier : on se donne un diviseur positif de p et on montre qu'il vaut 1 ou p.
- Savoir montrer qu'une partie d'un espace vectoriel en est un sous-espace vectoriel.
  - inclusion, vecteur nul, stabilité par combinaison linéaire ;
  - «mettre sous forme d'un vect».
- Savoir déterminer une partie génératrice d'un sous-espace vectoriel («mettre sous forme d'un vect»).

3 Questions de cours

Nombres de Fermat

1. Soit $m \in \mathbb{N}$ tel que 2^m+1 est premier. Montrer qu'il existe $n \in \mathbb{N}$ tel que $m = 2^n$.
2. On pose $\mathrm{F}_n = 2^{2^n}+1$ pour $n \in \mathbb{N}$. Soit $(m,n) \in \mathbb{N}^2$ tel que $m \neq n$. Montrer que $\mathrm{F}_m \wedge \mathrm{F}_n = 1$.

BCCP 86 (petit théorème de Fermat)

1. Soit $(a,b,p) \in \mathbb{Z}^3$. Prouver que si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge ab = 1$.
2. Soit p un nombre premier.
   (a) Prouver que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ et en déduire que p divise $\binom{p}{k}$.
   (b) Prouver par récurrence que : $\forall n \in \mathbb{N},\ n^p \equiv n[p]$.
   (c) En déduire que pour tout entier naturel n non divisible par p, $n^{p-1} \equiv 1[p]$.

Somme de deux sous-espaces vectoriels Soient F et G deux sous-espaces vectoriels d'un espace vectoriel E. Montrer que $\mathrm{F}+\mathrm{G}$ est un sous-espace vectoriel de E.

Récurrences linéaires homogènes On note F l'ensembles des suites réelles vérifiant une relation de récurrence linéaire homogène d'ordre 2 à coefficients constants **au choix de l'examinateur**. Déterminer une famille génératrice de F («mettre sous forme d'un vect»).

Equations différentielles linéaires homogènes On note F l'ensemble des solutions à valeurs réelles d'une équation différentielle d'ordre 2 homogène à coefficients constants **au choix de l'examinateur**. Déterminer une famille génératrice de F («mettre sous forme d'un vect»).