Semaine du 22/01 au 26/01

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.

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.
- Résoudre un système de deux congruences du type $\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases}$.

3 Questions de cours

- Résoudre une équation diophantienne du type $ax + by = c$ au choix de l'examinateur.
- Montrer que tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{Z}$.
- Démontrer le petit théorème de Fermat : si p est un nombre premier, alors pour tout $x \in \mathbb{Z}$, $x^p \equiv x[p]$.
- 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.
- Soit a et r deux entiers supérieurs ou égaux à 2. Montrer que si $a^r - 1$ est premier, alors $a = 2$ et r est premier.