Semaine 13 du 8 au 12 janvier 2024

Arithmétique dans $\mathbb{Z}$

I) Divisibilité

- Diviseurs, multiples
- Congruences : somme et produit
- Division euclidienne

II) PGCD et PPCM

- PGCD d'un nombre fini d'entiers
- Algorithme d'Euclide
- Relation de Bézout
- Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$
- $(ka) \wedge (kb) = k(a \wedge b)$ si $k \in \mathbb{N}^*$
- PPCM d'un nombre fini d'entiers

III) Entiers premiers entre eux

- Couple d'entiers premiers entre eux
- Théorème de Bézout
- Lemme de Gauss
- Si a et b premiers entre eux divisent n, alors ab divise n
- Si a et b sont premiers à n, alors ab est premier à n
- Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux

IV) Nombres premiers

- Crible d'Eratosthène
- L'ensemble des nombres premiers est infini
- Existence et unicité de la décomposition d'un nombre entier non nul en produit de nombres premiers
- Valuation p-adique : caractérisation de la divisibilité, expressions du PGCD et du PPCM
- Petit théorème de Fermat

Démonstrations exigibles

Arithmétique dans $\mathbb{Z}$

- Compatibilité de la congruence avec la somme et le produit
- Division euclidienne : existence et unicité du quotient et du reste
- Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$
- Lemme de Gauss
- Si $a \wedge b = 1$, $a|n$ et $b|n$ alors $ab|n$
- Si $a \wedge n = 1$ et $b \wedge n = 1$, alors $(ab) \wedge n = 1$
- Petit théorème de Fermat

Exercices préparés

Structures algébriques

- Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$. Justifier l'existence de $a = \inf(G \cap \mathbb{R}_+^*)$. Montrer que si $a > 0$, alors $G = a\mathbb{Z}$.

Arithmétique dans $\mathbb{Z}$

- Soit $n \in \mathbb{N}^*$. Montrer que $n+1$ et $2n+1$ sont premier entre eux. En déduire que $n+1$ divise $\binom{2n}{n}$.
- Résoudre dans $\mathbb{Z}^2$, l'équation $12x + 18y = 36$