Semaine 14 du 12 au 16 janvier 2025

Arithmétique dans $\mathbb{Z}$

I) Divisibilité

- Diviseurs, multiples
- Congruences, compatibilité avec la somme et le produit
- Division euclidienne

II) PGCD et PPCM

- PGCD d'un nombre fini d'entiers, algorithme d'Euclide
- Relation de Bézout et algorithme d'Euclide étendu
- Les diviseurs communs à a et b sont les diviseurs du pgcd $a \wedge b$
- $(ka) \wedge (kb) = |k|(a \wedge b)$
- PPCM d'un nombre fini d'entiers
- Les multiples communs à a et b sont les multiples du ppcm
- $(ka) \vee (kb) = |k|(a \vee b)$
- $(a \wedge b)(a \vee b) = |ab|$

III) Entiers premiers entre eux

- Couple d'entiers premiers entre eux
- Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux
- Théorème de Bézout
- Lemme de Gauss
- Si $a_1, a_2, \dots, a_n$ sont deux à deux premiers entre eux et divisent n, alors leur produit divise n
- Si $a_1, a_2, \dots, a_n$ sont premiers à n, alors leur produit est premier à n

IV) Nombres premiers

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

V) Utilisation des congruences et applications

- Petit théorème de Fermat
- Utilisation d'un inverse modulo n
- Résolution d'équations diophantiennes $ax + by = c$

Démonstrations

Arithmétique dans $\mathbb{Z}$

- Compatibilité de la congruence avec la somme et le produit
- Division euclidienne : existence et unicité du quotient et du reste
- 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

cices prép

Arithmétique

- Montrer que, pour tout $n \in \mathbb{N}$, 17 divise $7^{8n+1} + 10(-1)^n$.
- Résoudre dans $\mathbb{Z}^2$, l'équation $12x + 18y = 36$.