Semaine 6 - Arithmétique

Tout le chapitre a été fait. Mais peu d'exercices ont été corrigés.

1 Reprise du programme précédent

- Ensembles, applications
- Relations binaires ; relations d'équivalence, relations d'ordre

2 Divisibilité dans $\mathbb{Z}$

- Relation de divisibilité, diviseurs, multiples
- Division euclidienne, quotient, reste
- PGCD, *défini comme le plus grand (pour l'ordre usuel) diviseur commun à deux entiers non tous les deux nuls*
- Identité de Bachet-Bézout
- Les diviseurs du PGCD sont les diviseurs communs ; interprétation en termes de relation d'ordre
- $ka \wedge kb = k(a \wedge b)$
- Généralisation rapide à un nombre fini d'entiers
- Calculs du PGCD et des relations de Bézout par l'algorithme d'Euclide (étendu)
- Entiers premiers entre eux
- Théorème de Bézout
- Lemme de Gauss ; si a et b sont premiers avec c, ab est premier avec c ; si a et b divisent c et sont premiers entre eux, alors ab divise c.
- PPCM, *défini comme le plus petit (pour l'ordre usuel) multiple commun de deux entiers non nuls*
- Les multiples du PPCM sont les multiples communs ; interprétation en termes de relations d'ordre
- Ensemble d'entiers premiers entre eux dans leur ensemble.

3 Nombres premiers

- Nombres premiers
- Lemme d'Euclide
- Un nombre $n \geq 2$ est premier ou admet un diviseur premier $\leq \lfloor \sqrt{n} \rfloor$
- Évocation du crible d'Ératosthène

- L'ensemble des nombres premiers est infini
- Théorème fondamental de l'arithmétique : tout entier $n \geq 2$ s'écrit d'une unique façon $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$, avec $v_p(n) \in \mathbb{N}$, valant 0 sauf pour un nombre fini de nombres premiers. *On permet l'écriture d'un produit infini dont tous les facteurs, sauf un nombre fini, valent* 1.
- Valuations p-adique
- Valuation d'un produit, d'un PGCD, d'un PPCM

4 Arithmétique modulaire

- Relation de congruence modulo n. On note $a \equiv b\,[n]$
- Compatibilité des opérations avec la congruence
- Inverse modulo n ; a admet un inverse modulo n ssi a est premier avec n
- Petit théorème de Fermat
- Application à la détermination de la valeur de a^N modulo p, où a et N sont des grands nombres
- Théorème des restes chinois ; avec calcul effectif d'une solution

5 Exemples de questions de cours

- Calculs effectifs de PGCD/de relations de Bézout
- Existence d'une identité de Bézout
- Démonstration du lemme de Gauss/du lemme d'Euclide
- Théorème fondamental de l'arithmétique (existence ou unicité)
- Petit théorème de Fermat – *deux démonstrations ont été données, au choix de l'élève*
- Résolution effective d'un système de congruences par le théorème des restes chinois