Semaine 6 - Arithmétique

Le cours est presque fini (il me reste à parler des applications du petit théorème de Fermat et du théorème des restes chinois) ; peu d'exercices ont été traités en cours pour le moment.

1 Reprise du programme précédent

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. *La définition d'un produit infini dont tous les termes sauf un nombre fini valent* 1 *a été donnée rapidement.*
– Valuations p-adique
– Valuation d'un produit, d'un PGCD, d'un PPCM

4 Arithmétique modulaire

On a adopté un point de vue élémentaire. Le point de vue $\mathbb{Z}/n\mathbb{Z}$ n'est pas exigible.
– 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 (*démonstrations non exigibles cette semaine*)

5 Exemples de questions de cours

– Calculs effectifs de PGCD/de relations de Bézout
– Démonstration du lemme de Gauss/du lemme d'Euclide
– Théorème fondamental de l'arithmétique (existence ou unicité)
– Calcul d'un inverse modulo n