Semaine du 19/1 au 25/1

Arithmétique

- Divisibilité, multiplicité, ensemble des diviseurs, ensemble des multiples d'un entier, Propriétés de la relation de divisibilité
- Relation de congruence et propriétés, Application aux critères de divisibilité en base 10
- Division euclidienne, écriture en base quelconque (les étudiants doivent savoir passer d'une base à une autre)
- Définitions de PGCD, PPCM, $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$, $\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(a \wedge b)$,
  Utilisation du PGCD via l'équivalence $d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$
  PGCD et PPCM d'une famille d'entiers
- Algorithme d'Euclide et Algorithme d'Euclide étendu (les étudiants doivent savoir retrouver les coefficients de Bézout), théorème de Bézout,
- Nombres premiers entre eux, Propriétés si $a \wedge b = 1$ alors $\left| \begin{array}{l} a \wedge c = 1 \Rightarrow a \wedge (bc) = 1 \\ a^p \wedge b^q = 1 \text{ pour tous } p, q \in \mathbb{N} \\ a, b \mid c \Rightarrow ab \mid c \end{array} \right|$, Lemme de Gauss, nombres premiers entre eux 2 à 2 ~~$\Rightarrow$~~ nombres premiers entre eux dans leur ensemble.
- $(a \wedge b) \cdot (a \vee b) = |ab|$
- Nombres premiers, propriétés, Théorème de Fermat,
- Théorème fondamentale de l'arithmétique, définition de la valuation p-adique et propriétés première
- Résolution de systèmes congruentiels

Les étudiants n'auront pas un grand recul sur les équations diophantiennes. Un peu d'aide sur les techniques à utiliser, est à donner rapidement en cas de blocage.

Preuves

Seules les preuves dans cette section sont à savoir par coeur par les étudiants. Les autres preuves peuvent être demandées, en proposant une méthode et/ou en aidant l'étudiant durant la réalisation de la preuve.

La question de cours sera composée d'un énoncé rapide (définition, propriété ou théorème), suivi d'une démonstration (ou exemple) de cours choisie parmi :

1. Théorème de Fermat (y compris $n^{p-1} \equiv 1[p]$, pour $n \notin p\mathbb{Z}$)
2. Retrouver tous les coefficients de Bézout, avec un algorithme d'Euclide étendu (pas trop d'étapes, comme pour 1515 et 274).
   La question peut être "Résoudre l'équation diophantienne 1515x+ 274y=1".
3. Preuve du théorème fondamental de l'arithmétique (comprends la proposition 13)
4. Preuve des critères de divisibilité de 2,3,4,5,9 et 11.