MP2I : Colle 14 (20/01/25 au 24/01/25)

Reprise du programme précédent (structures algébriques) plus :

Chapitre 16 : Arithmétique

- Relation de divisibilité dans $\mathbf{Z}$. Notations : $\mathcal{D}(a)$ pour l'ensemble des diviseurs de a, $a\mathbf{Z}$ pour l'ensemble de ses multiples.
- Règles de calcul modulo n.
- Division euclidienne par un entier positif : existence et unicité.
- Nombres premiers : définition, infinité, crible d'Ératosthène. Décomposition d'un entier en produit de facteurs premiers : existence (sans unicité pour l'instant).
- PGCD (notation : $a \wedge b$) : définition (plus grand diviseur commun de a et b), algorithme d'Euclide. Un entier est un diviseur commun de a et b ssi c'est un diviseur de $a \wedge b$. Identité de Bézout. Algorithme d'Euclide étendu pour le calcul des coefficients d'une relation de Bézout.
- Entiers premiers entre eux. Un entier est premier avec un produit ssi il est premier avec chacun de ses facteurs. Lemme de Gauss. Si $a \wedge b = 1$, et si $a \mid n$ et $b \mid n$, alors $ab \mid n$.
  Si $ka \equiv kb \ [n]$ et si $k \wedge n = 1$, alors $a \equiv b \ [n]$.
  Forme irréductible d'un rationnel.
- PPCM : notation $a \vee b$. Un entier est multiple de a et b ssi c'est un multiple de $a \vee b$. Lien avec le PGCD : $(a \wedge b)(a \vee b) = ab$.
- PGCD de n nombres, entiers premiers dans leur ensemble.
- Décomposition d'un entier en produit de premiers : existence et unicité. Valuation p-adique d'un entier positif. Caractérisation de la divisibilité en termes de valuations p-adiques. Expression du pgcd et du ppcm à l'aide des décompositions primaires.
- Petit théorème de Fermat : si p est premier, alors pour tout $a \in \mathbf{Z}$, $a^p \equiv a \pmod{p}$. Si de plus $a \wedge p = 1$, alors $a^{p-1} \equiv 1 \pmod{p}$.