Programme de khôlle MPSI n°16 - du 03/02/25 au 07/02/25

1. Arithmétique

   - Divisibilité : diviseurs, multiples, nombres associés
   - Division euclidienne
   - PGCD
   - Algorithme d'Euclide
   - Coefficients de Bézout
   - Algorithme d'Euclide étendu
   - PPCM, propriétés
   - entiers premiers entre eux
   - PGCD d'un nombre fini d'éléments (généralisation de Bézout)
   - Nombres premiers
   - Crible d'Eratosthène
   - Théorème fondamental de l'arithmétique
   - Valuation p-adique, propriétés
   - Congruences
   - Petit théorème de Fermat

2. Polynômes

   - Polynômes : définitions et opérations
   - Dégré d'un polynôme
   - Dérivation
   - Division euclidienne
   - Racines d'un polynôme
   - Racines d'un polynôme à coefficients entiers
   - Méthode de Hörner pour l'évaluation polynomiale
   - Relations coefficients-racines
   - Ordre de multiplicité d'une racine
   - Formule de Taylor polynomiale
   - Arithmétique dans $\mathbb{K}[X]$
   - Polynômes irréductibles dans $\mathbb{R}[X]$, $\mathbb{C}[X]$
   - Théorème de d'Alembert-Gauss

Questions de cours (démonstrations à connaître)

- **Arithmétique**

  1. Soient a et b deux entiers naturels, $b \neq 0$. On suppose $a = bq + r$, avec $(q, r) \in \mathbb{N}^2$.
     Alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$ et en particulier $a \wedge b = b \wedge r$.
  2. a premier avec b et a premier avec $c \Rightarrow a$ premier avec bc.
  3. Soit $n \in \mathbb{N}^*$. Pour tout $(a_1, \dots, a_n) \in (\mathbb{Z}^n)^*$ il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que
     $$a_1 u_1 + \cdots + a_n u_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$$
     (on admet l'identité de Bézout pour deux éléments)
  4. L'ensemble des nombres premiers est infini
  5. Soit p un nombre premier. Montrer que : $\forall a \in \mathbb{Z},\ a^p \equiv a\ [p]$ (**petit théorème de Fermat**).
     (on pourra admettre que $(a+b)^p \equiv a^p + b^p\ [p]$)

- **Polynômes**

  1. a est racine de P si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)Q(X)$ (c'est-à-dire si $(X-a)$ divise P).
  2. Si $\deg P \leq n$ et P possède au moins $(n+1)$ racines distinctes, alors P est le polynôme nul.
  3. Soit $P \in \mathbb{R}[X]$ et soit α une racine d'ordre de multiplicité (exactement) 2 de P.
     Montrer qu'alors $P'(\alpha) = 0$ et $P''(\alpha) \neq 0$. *(→ Exercice 8 du cours)*
  4. Tout polynôme de degré 1 est irréductible dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.
  5. Savoir énoncer et justifier quels sont les polynômes irréductibles dans $\mathbb{R}[X]$.