Chapitre 18 : Arithmétique

C) Nombres premiers

- Définition nombre premier, nombre composé
- Tout entier admet un diviseur premier
- lien entre nombre premier et entiers premiers entre eux
- Crible d'Erastothène
- Décomposition en produit de facteurs premiers
- Valuation p-adique
- Valuation p-adique du produit
- Lien entre valuation p-adique et divisibilité
- Expression du pgcm et pgcd à l'aide de la valuation p-adique

D) Congrueneces

- Relation de congruence (relation d'équivalence)
- Opération sur les congruences
- Utilisation inverse modulo n pour résoudre congruences
- Petit théorème de Fermat

Chapitre 19 : Polynômes

A) Anneau des polynômes à une indéterminée

- Anneau $\mathbb{K}[X]$ pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Cet anneau est commutatif
- Dégré, coefficient dominant,polynôme unitaire,
- Dégré d'une somme, d'un produit
- Composition de deux polynômes.
- $(\mathbb{K}_n[X], +)$ sous groupe de $(\mathbb{K}[X], +)$
- $K[X]$ est intègre.

B) Divisibilité

- Définition divisibilité de polynômes, diviseurs, multiples...
- Premières propriétés
- Lien entre divisibilité et degré
- Caractérisation des polynômes associés
- Théorème et algorithme de la division euclidienne

C) Fonction polynomiales et racines

- Fonction polynomiale associée à un polynôme

Questions de cours :

- On prouvera les résultats suivants :
  Soit p un nombre premier.
  1) Pour tout $k \in [\![1, p-1]\!]$, le coefficient binomial $\begin{pmatrix} p \\ k \end{pmatrix}$ est divisible par p.
  2) Pour tout $(a, b) \in \mathbb{Z}^2$, on a $(a+b)^p \equiv a^p + b^p [p]$
  3) Soit $n \in \mathbb{N}$, montrer que $n^p \equiv n[p]$ (on explicitera la récurrence) puis que si $p \nmid n, n^{p-1} \equiv 1[p]$ (Petit théorème de Fermat).
- Prouver le théorème de la division euclidienne pour les polynômes (existence et unicité) puis calcul d'une division euclidienne de polynôme au choix du colleur.
- Montrer l'existence et l'unicité d'une décomposition en facteurs premiers pour tout nombre $n \geq 2$ (on reprouvera que tout nombre $n \geq 2$ est produit de nombre premiers).