Colle 20 : Arithmétique et polynômes

Résultats et preuves à connaître

Proposition 1 Lemme

Soit $p \in \mathscr{P}$. Pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.

Proposition 2 Petit théorème de Fermat

Si $p \in \mathscr{P}$ alors $\forall m \in \mathbb{Z}, m^p \equiv m\,[p]$ et si $p \not| m$, alors $m^{p-1} \equiv 1\,[p]$

Proposition 3 Théorème (Infinité des nombres premiers)

Il y a une infinité de nombres premiers.

Proposition 4 Décomposition en produit de facteurs premiers

Tout entier $n \geqslant 2$ peut s'écrire sous la forme

$$n = q_1 q_2 \dots q_r$$

où les q_i sont premiers et $r \in \mathbb{N}$.
De plus, cette décomposition est unique à l'ordre des facteurs près si on l'écrit

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

où les p_i sont premiers, 2 à 2 distincts, $k \in \mathbb{N}$ et les α_i entiers naturels.

Proposition 5 Propriétés

Rappeler que $v_p(n) = \max\{k \in \mathbb{N} / p^k | n\}$ et montrer qu'elle correspond à l'exposant de p dans la décomposition de en facteurs premiers de n.
• La suite $(v_p(n))_p$ est nulle à partir d'un certain rang et $n = \prod_{p \in \mathscr{P}} p^{v_p(n)}$.
• $\forall (n,m) \in (\mathbb{N}^*)^2$, $v_p(mn) = v_p(m) + v_p(n)$.

Proposition 6 Calcul du PPCM et du PGCD

Soient $(a,b) \in (\mathbb{N}^*)^2$.
i) $a \,|\, b \iff \forall p \in \mathscr{P}, v_p(a) \leqslant v_p(b)$
ii) $a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))}$ et $a \vee b = \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}$

Proposition 7 Propriétés

Soient $(P,Q) \in \mathbb{K}[X]^2$, P et Q non nuls.
• $\deg(P+Q) \leqslant \max(\deg(P),\deg(Q))$
$\deg(P+Q) = \max(\deg(P),\deg(Q))$ ssi $\deg(P) \neq \deg(Q)$ ou la somme des coefficients dominants est non nulle.
• $\deg(P \times Q) = \deg(P) + \deg(Q)$.
• $\deg(\lambda P) = \deg(P)$ pour tout $\lambda \neq 0$.

Proposition 8 $(\mathbb{K}[X])^*$

Les inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0, c'est-à-dire les polynômes constants non nuls. On a donc $(\mathbb{K}[X])^* = \mathbb{K}^*$.

Proposition 9

Soient $(A,B) \in \mathbb{K}[X]^2$.

$$A \mid B \quad \text{et} \quad B \mid A \iff \exists \lambda \in \mathbb{K}^*, A = \lambda B$$

Les polynômes A et B sont dits **associés**.

Proposition 10 Théorème de la division euclidienne

Soient $(A,B) \in \mathbb{K}[X]^2$ et $B \neq 0$.
Il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ tel que :

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B)$$

Q et R sont respectivement le quotient et le reste de la division euclidienne de A par B.

Proposition 11

Soient $(A,B) \in \mathbb{K}[X]^2$ et $B \neq 0$.
Si $A = BQ + R$ avec $\deg(R) < \deg(B)$ alors $\mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(B) \cap \mathscr{D}(R)$.

À savoir faire

- ☐ Tout sur l'arithmétque de la semaine précédente
- ☐ Calculer le PGCD de deux entiers et déterminer les coefficients de Bezout pour ces deux entiers
- ☐ Calculer le PGCD, le PPCM de p entiers.
- ☐ Résoudre une équation diophantienne
- ☐ Décomposer un nombre en facteurs premiers, déterminer la valuation p-adique d'un entier, utiliser les décompositions en facteurs de deux entiers pour trouver leur PGCD et PPCM.
- ☐ Faire des calculs modulo n.
  Utiliser le petit théorème de Fermat
  Penser à calculer une quantité modulo n pour montrer qu'elle est multiple de n.
- ☐ Poser une division euclidienne de polynômes

Ce qu'en dit le programme

Arithmétique sur $\mathbb{Z}$: fin

CONTENUS	CAPACITÉS & COMMENTAIRES
d) Nombres premiers La semaine prochaine	
Nombre premier. L'ensemble des nombres premiers est infini. Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers. Pour p premier, valuation p-adique. Valuation p-adique d'un produit.	Crible d'Ératosthène. Notation $v_p(n)$. Caractérisation de la divisibilité en termes de valuations p-adiques. Expressions du PGCD et du PPCM à l'aide des valuations p-adiques.

Polynômes : début

L'arithmétique de $\mathbb{K}[X]$ est développée selon le plan déjà utilisé pour l'arithmétique de $\mathbb{Z}$, ce qui autorise un exposé allégé. Le programme se limite au cas où le corps de base $\mathbb{K}$ est égal à $\mathbb{R}$ ou $\mathbb{C}$.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Anneau des polynômes à une indéterminée	
Anneau $\mathbb{K}[X]$. Degré, coefficient dominant, polynôme unitaire. Degré d'une somme, d'un produit. Composition.	La construction de $\mathbb{K}[X]$ est hors programme. Ensemble $\mathbb{K}_n[X]$ des polynômes de degré au plus n. L'anneau $\mathbb{K}[X]$ est intègre.
b) Divisibilité et division euclidienne	
Divisibilité dans $\mathbb{K}[X]$, diviseurs, multiples. Caractérisation des couples de polynômes associés. Théorème de la division euclidienne.	 Algorithme de la division euclidienne.
c) Fonctions polynomiales et racines : la semaine prochaine	
d) Dérivation	
Dérivée formelle d'un polynôme. Opérations sur les polynômes dérivés : combinaison linéaire, produit. Formule de Leibniz.	Pour $\mathbb{K} = \mathbb{R}$, lien avec la dérivée de la fonction polynomiale associée.