Résumé de CM10

Applications simples de Congruence

Les propriétés suivantes sont faciles à voir.

Pour un entier $n \in \mathbb{N}^*$ qui s'écrit sous la forme

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \cdots + a_1 \cdot 10^1 + a_0, \quad r \in \mathbb{N}, \quad 0 \leq a_i \leq 9 \quad (0 \leq i \leq r),$$

1. $2|n$ si et seulement si $2|a_0$, i.e., $a_0 \in \{0, 2, 4, 6, 8\}$,
2. $5|n$ si et seulement si $5|a_0$, i.e., $a_0 \in \{0, 5\}$,
3. $3|n$ si et seulement si $3|(a_0 + a_1 + \cdots + a_r)$,
4. $9|n$ si et seulement si $9|(a_0 + a_1 + \cdots + a_r)$.

Pour la preuve, il suffit d'utiliser les faits que $2|10$, $5|10$, $10 \equiv 1 \pmod{3}$ et $10 \equiv 1 \pmod{9}$.

Vocabulaires et Opérations sur Polynômes

$\mathbb{K}$: un corps commutatif, e.g., $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.

1. Vocabulaires:

- Pour $a_i \in \mathbb{K}$ ($0 \leq i \leq n$), une formule (ou expression)

$$P(X) = a_0 + a_1X + \cdots + a_nX^n$$

où X est un indéterminée, est appelée un **polynôme**.

- Pour un $\alpha \in \mathbb{K}$, on peut substituer X par α ; on obtient un nombre $P(\alpha)$.
L'application associée $\mathbb{K} \rightarrow \mathbb{K}; \alpha \mapsto P(\alpha)$ sera notée P .
- Le **degré** de P est le plus grand d tel que $a_d \neq 0$, noté $\deg(P)$.
Pour le **polynôme nul** 0 , le degré est $-\infty$, par convention.
- Pour un polynôme P de degré d , le coefficient a_d de X^d est appelé le **coefficient dominant**.
- Un polynôme est dit **unitaire** si son coefficient dominant vaut 1.
- L'ensemble des polynômes à coefficients dans $\mathbb{K}$ sera noté $\mathbb{K}[X]$.

2. Opérations: $P(X) = a_0 + a_1X + \cdots + a_pX^p$, $a_k := 0$ pour $k > p$,
 $Q(X) = b_0 + b_1X + \cdots + b_qX^q$, $b_k := 0$ pour $k > q$.

- La **somme** $P + Q$: le polynôme $c_0 + c_1X + \cdots + c_{\max(p,q)}X^{\max(p,q)}$
où $c_k := a_k + b_k \quad \forall k \geq 0$.
- Le **produit** PQ : le polynôme $c_0 + c_1X + \cdots + c_{p+q}X^{p+q}$
où $c_k := \sum_{i+j=k} a_i b_j \quad \forall k \geq 0$.
- Le **polynôme dérivé** P' : le polynôme $a_1 + 2a_2X + \cdots + pa_pX^{p-1}$.
- Le **polynôme composé** $P \circ Q$: le polynôme

$$(P \circ Q)(X) := P(Q(X)) = a_0 + a_1Q(X) + \cdots + a_pQ(X)^p.$$

- Le **conjugué** $\bar{P}$ (pour $P \in \mathbb{C}[X]$): le polynôme $\bar{P}(X) = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_pX^p$.
Pour un $\alpha \in \mathbb{C}$; $\bar{P(\alpha)} = \bar{P}(\bar{\alpha})$.

Lemme Pour $P, Q \in \mathbb{K}[X] \setminus \{0\}$,

1. $\deg(PQ) = \deg(P) + \deg(Q)$,
2. $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$,
3. $\deg(P') = \deg(P) - 1$ si P n'est pas un constant.
4. $\deg(P \circ Q) = (\deg P)(\deg Q)$. □

Pour la dernière propriété, il suffit de considérer le cas $P(X) = X^m$ et $Q(X) = X^n$.

Arithmétique sur $\mathbb{K}[X]$ $\mathbb{K}$: un corps commutatif, e.g., $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ etc.

L'ensemble $\mathbb{K}[X]$ muni de l'addition $+$ et la multiplication $\cdot$ vérifie les propriétés suivantes:

1. $(\mathbb{K}[X], +)$: groupe abélien, i.e.,
 - i) $(P + Q) + R = P + (Q + R)$,
 - ii) $P + 0 = 0 + P = P$ où $0 \in \mathbb{K}[X]$ est le polynôme nul,
 - iii) pour $P \in \mathbb{K}[X]$, posons $-P = (-1) \cdot P$. Alors, $P + (-P) = (-P) + P = 0$.
 - iv) $P + Q = Q + P$.
2. $(\mathbb{K}[X], \cdot)$: monoïde commutatif, i.e.,
 - i) $(P \cdot Q) \cdot R = P \cdot (Q \cdot R)$,
 - ii) $1 \cdot P = P \cdot 1 = P$,
 - iii) $P \cdot Q = Q \cdot P$.
3. Distributivité: $P, Q, R \in \mathbb{K}[X]$,

$$(P + Q) \cdot R = P \cdot R + Q \cdot R, \quad P \cdot (Q + R) = P \cdot R + Q \cdot R.$$

On dit que $(\mathbb{K}[X], +, \cdot)$ est un **anneau commutatif**. De plus, grâce aux résultat suivant, les propriétés suivantes sont montrés par une méthode très similaire comme pour $\mathbb{Z}$:

Théorème (Division Euclidienne).

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

1. $A = BQ + R$,
2. $R = 0$ ou $\deg(R) < \deg(B)$. □

Les structures en commun entre l'anneau des entiers $\mathbb{Z}$ et l'anneau des polynômes $\mathbb{K}[X]$ est appelé **anneau euclidienne**, ou plus généralement **anneau principal**. Les théorèmes mentionnés sur $\mathbb{Z}$ ont une analogie sur $\mathbb{K}[X]$ qui peuvent être montrés de façon complètement parallèle.