# Colle 20 : Arithmétique (et polynômes)

## Résultats et preuves à connaître

**Proposition 1**

- $a \wedge b = 1$ et $a \wedge c = 1 \iff a \wedge (bc) = 1$
- $a \wedge b = 1 \implies \forall (m,n) \in \mathbb{N}^2,\ a^m \wedge b^n = 1$
- Un produit de facteurs est premier avec $a$ ssi chacun des facteurs est premier avec $a$.
- $a \wedge b = 1, a \mid c$ et $b \mid c \implies ab \mid c$.

**Proposition 2** Calcul du PPCM

- Si $a \wedge b = 1$ alors $a \vee b = |ab|$.
- Si $d = a \wedge b$, comme $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$, alors

$$a \vee b = d\left|a'b'\right| \quad \text{et} \quad (a \wedge b)(a \vee b) = |ab|$$

**Proposition 3** Équation diophantienne $ax + by = c$

Soient $(a,b,c) \in \mathbb{Z}^3$.
On cherche les couples $(x,y) \in \mathbb{Z}^2$ solution de l'équation

$$ax + by = c$$

Si $a \wedge b$ ne divise pas $c$, l'équation n'a pas de solution.
(à savoir démontrer) Sinon la solution générale de l'équation est la somme d'une solution particulière (obtenue par remontée de l'algorithme d'Euclide du calcul de $a \wedge b$) et de la solution générale de l'équation homogène associée $ax + by = 0$.
On ne demandera pas de démonstration, mais de savoir appliquer la méthode pour résoudre une telle équation diophantienne sur un exemple précis.

**Définition 1**

Soit $(a_k)_{1 \leqslant k \leqslant p}$ une famille d'entiers ($p \geqslant 2$) non tous nuls. L'ensemble des diviseurs communs à $a_1, a_2 \dots a_p$ admet un plus grand élément appelé **plus grand commun diviseur** de la famille $(a_k)_{1 \leqslant k \leqslant p}$ et est noté $a_1 \wedge a_2 \wedge \cdots \wedge a_p$.

Le PGCD est commutatif et associatif, de plus, $\bigcap_{i=1}^{p} \mathcal{D}(a_i) = \mathcal{D}(\wedge_{i=1}^{p} a_i)$

Si $a_1 = a_2 = \cdots = a_p = 0$, on pose $a_1 \wedge a_2 \wedge \cdots \wedge a_p = 0$.

**Proposition 4** Coefficients de Bézout

Il existe une famille d'entiers relatifs $(u_k)_{1 \leqslant k \leqslant p}$ tels que

$$\sum_{k=1}^{p} u_k a_k = \bigwedge_{k=1}^{p} a_k$$

**Proposition 5** Lemme

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

**Proposition 6** Petit théorème de Fermat (en admettant le lemme ci-dessus)

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 7** Infinité des nombres premiers

Il y a une infinité de nombres premiers.

**Proposition 8** 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 $\alpha_i$ entiers naturels.

**Proposition 9** Valuation p-adique

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 10** 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 11** Degré d'une somme-d'un produit

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

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

# À savoir faire

- ☐ Tous les exercices sur les fonctions convexes
- ☐ Calculer le PGCD de deux entiers et déterminer les coefficients de Bézout pour ces deux entiers
- ☐ Calculer le PGCD, le PPCM de $p$ entiers.
- ☐ Résoudre une équation diophantienne de la forme $ax+by=c$
- ☐ Faire des calculs modulo $n$.
- ☐ Penser à calculer une quantité modulo $n$ pour montrer qu'elle est multiple de $n$.
- ☐ 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 $n$. Pas d'exercices sur les polynômes cette semaine

# Ce qu'en dit le programme

## Arithmétique sur $\mathbb{Z}$ : fin

| CONTENUS | CAPACITÉS & COMMENTAIRES |
|---|---|
| **c) Entiers premiers entre eux** | |
| Couple d'entiers premiers entre eux.<br>Théorème de Bézout.<br>Lemme de Gauss.<br>Si $a$ et $b$ sont premiers entre eux et divisent $n$, alors $ab$ divise $n$.<br>Si $a$ et $b$ sont premiers à $n$, alors $ab$ est premier à $n$.<br>PGCD d'un nombre fini d'entiers, relation de Bézout.<br>Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux. | Forme irréductible d'un rationnel. |
| **d) Nombres premiers** | |
| Nombre premier.<br>L'ensemble des nombres premiers est infini.<br>Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers. | Crible d'Ératosthène. |
| Pour $p$ premier, valuation $p$-adique.<br>Valuation $p$-adique d'un produit. | Notation $v_p(n)$.<br>Caractérisation de la divisibilité en termes de valuations $p$-adiques.<br>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 $\mathbb{K}[X]$. | La construction de $\mathbb{K}[X]$ est hors programme. |
| Degré, coefficient dominant, polynôme unitaire. | Ensemble $\mathbb{K}_n[X]$ des polynômes de degré au plus $n$. |
| Degré d'une somme, d'un produit. | L'anneau $\mathbb{K}[X]$ est intègre. |
| Composition. | |