# Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Matei Lefebvre

2025/2026

## 1 Notion de PGCD et PPCM.

### 1.1 Dans un anneau quelconque.

[Rom21], VIII.2
$\sim$ 7 items.
définition pgcd, éléments premiers entre-eux | exemple | définition anneau à pgcd | homogénéité pgcd | théorème de Gauss | définition ppcm | cas des anneaux à pgcd

### 1.2 Dans un anneau principal.

[Ber20], XIV.4, XVII.2-3 et XV.3
$\sim$ 5 items.
définition anneau principal | exemple | relations de Bézout, existence de pgcd, ppcm | caractérisation éléments premiers entre eux | exemple

### 1.3 Dans un anneau factoriel.

[Ber20], XVII.2 et XVII.5
$\sim$ 7 items.
définition anneau factoriel | principal $\Rightarrow$ factoriel | exemples | irréductible $\Rightarrow$ premier (Euclide) | théorème de Gauss | existence pgcd, ppcm | contre-exemple : DEV 1 **D1**

**Lemme.** $\forall |z| \leqslant 1$, $\forall p \in \mathbb{N} : |1 - E_p(z)| \leqslant |z|^{p+1}$ *où* $E_p(z) = (1-z)\exp\left(\sum_{k=1}^{p} \frac{z^k}{k}\right)$.

**Théorème.** *Soit* $(a_n) \in \mathbb{C}^{\mathbb{N}}$ *une suite injective sans point d'accumulation telle que* $a_n \neq 0$ $\forall n$. *Soit* $m_n \in (\mathbb{N}^*)^{\mathbb{N}}$ *et notons* $(z_n)$ *la suite où chaque* $a_n$ *est répété* $m_n$ *fois. Soit* $f : z \mapsto \prod_{n=1}^{+\infty} E_n\left(\frac{z}{z_n}\right)$. *Alors* $f$ *est bien définie, holomorphe sur* $\mathbb{C}$ *et ses zéros sont exactement les* $a_n$, *d'ordres respectifs* $m_n$.

[Rud20], XV.2
**Remarque :** si on a du temps on peut également faire la démonstration pour un ouvert quelconque de $\mathbb{C}$ mais ça nécessite d'admettre certaines choses sur les fonctions holomorphes sur la sphère de Riemann. On peut également montrer comme corollaires presque immédiats de ce théorème le théorème de factorisation de Weierstrass et le fait que $\mathcal{M}(\mathbb{C}) = \mathrm{Frac}(\mathcal{H}(\mathbb{C}))$.
**Remarque pour cette leçon :** pour cette leçon, mettre en corollaire que $\mathcal{H}(\mathbb{C})$ est un anneau à pgcd non factoriel.

# 2 Cas d'un anneau euclidien : existence d'algorithmes.

[Ber20], XVII.3
$\sim$ 6 items.
définition anneau euclidien | exemples | euclidien $\Rightarrow$ principal | corollaires | algorithme d'Euclide étendu | exemple

# 3 Applications.

## 3.1 Théorème des restes chinois.

[Rom21], VIII.3 et X.3-4
$\sim$ 4 items.
théorème chinois | corollaire : multiplicativité de $\varphi$, formule explicite | équations diophantiennes, systèmes | exemple

## 3.2 Anneaux de polynômes.

[Per96], II.4.a
$\sim$ 9 items.
$\mathbb{K}[X]$ euclidien, unicité de la D.E | exemple | $A[X]$ principal $\Leftrightarrow$ $A$ corps | définition contenu, polynômes primitifs | lemme de Gauss | factorialité de $A[X]$, irréductibles | exemples | $P$ sans facteur carré $\Leftrightarrow$ $P \wedge P' = 1$ | DEV 2 **D2**

**Théorème** (Algorithme de Berlekamp)**.** *Soit $P = P_1 \dots P_r \in \mathbb{F}_q[X]$ avec $P_1, \dots, P_r$ irréductibles 2 à 2 premiers entre eux. On note* $S_P : \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P) \\ \overline{Q} & \mapsto & \overline{Q}^q = \overline{Q(X^q)} \end{array}$ *, c'est une application $\mathbb{F}_q$-linéaire.*
*On a alors $r = \dim(\ker(S_P - id)) = \deg(P) - \mathrm{rg}(S_P - id)$. Si de plus $r \geqslant 2$ et $\overline{V} \in \ker(S_P - id) \backslash \mathbb{F}_q$, alors $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$ est une décomposition non triviale de $P$.*

**Lemme.** *Soit $P \in \mathbb{F}_q[X]$, alors :*

1. $\mathrm{pgcd}(P, P') = 1 \Leftrightarrow$ *$P$ n'a pas de facteur carré.*
2. $\mathrm{pgcd}(P, P') = P \Leftrightarrow \exists R \in \mathbb{F}_q[X], P = R^p$.
3. *Si on est dans aucun des deux cas précédents, alors* $P = \mathrm{pgcd}(P, P').\dfrac{P}{\mathrm{pgcd}(P, P')}$ *est une décomposition non triviale de $P$.*

(L'algo suivant est sûrement à mettre en annexe).

**Algorithme** (de factorisation d'un polynôme $P \in \mathbb{F}_q[X]$)**.** *Soit $P \in \mathbb{F}_q[X]$.*
*.Si $P$ est constant :*
*. Fin de l'algorithme.*
*.Sinon :*
*. On calcule $D \coloneqq \mathrm{pgcd}(P, P')$.*
*. Si $D = 1$ :*
*. On applique l'algorithme de Berlekamp à $P$.*
*. Si $D = P$ :*

. *On trouve* $R \in \mathbb{F}_q[X]$ *tq* $P = R^p$ *(il suffit de mettre les coefficients de* $P$ *à la puissance* $p^{n-1}$*).*
. *On applique l'algorithme à* $R$*.*
. *Sinon :*
. *On applique l'algorithme à* $D$ *et* $\frac{P}{D}$*.*

[BMP05], V.3.2 et [Dem09], IX.6

# Références


[Per96] D. Perrin. *Cours d'algèbre (Agrégation)*. ELLIPSES, 1996. ISBN : 9782729855529.

[BMP05] V. Beck, J. Malick et G. Peyré. *Objectif Agrégation*. H&K, 2005. ISBN : 9782914010924.

[Dem09] M. Demazure. *Cours d'algèbre*. CASSINI, 2009. ISBN : 9782842251277.

[Ber20] G. Berhuy. *Algèbre : le grand combat*. CALVAGE&MOUNET, 2020. ISBN : 9782916352831.

[Rud20] W. Rudin. *Analyse réelle et complexe*. DUNOD, 2020. ISBN : 9782100820542.

[Rom21] J.E. Rombaldi. *Mathématiques pour l'agrégation - Algèbre et géométrie*. DEBOECK, 2021. ISBN : 9782807332201.