# L3 MAF "Algèbre 1" : TD n° 1

**Exercice 1 (Cours)** 1) Soient $a, b \in \mathbf{Z}$ premiers entre eux. Il existe donc $u_0, v_0 \in \mathbf{Z}$ tels que $u_0 a + v_0 b = 1$. Déterminer tous les couples $(u, v) \in \mathbf{Z} \times \mathbf{Z}$ tels que $ua + vb = 1$.
2) On suppose $b > 0$. Montrer qu'il existe un unique couple $(u, v) \in \mathbf{Z} \times \mathbf{Z}$ tel que $ua + vb = 1$ et $0 \leq u \leq b - 1$.
3) Comment s'étendent ces résultats lorsque le pgcd de $a$ et $b$ est un entier $d > 0$ arbitraire ?
4) Résoudre, pour $c \in \mathbf{Z}$ quelconque, l'équation $ax + by = c$ avec $(x, y) \in \mathbf{Z} \times \mathbf{Z}$.

**Exercice 2 (Cours)** 1) Soient $A, B \in K[X]$ non tous deux constants et premiers entre eux. Montrer que, pour tout couple $(F, G) \in K[X] \times K[X]$ tel que $FA + GB = 1$, les conditions et $\deg F < \deg B$ et $\deg G < \deg A$ sont équivalentes ; et qu'il existe un unique couple les vérifiant.
2) Comment s'étend ce résultat lorsque le pgcd de $A$ et $B$ est un polynôme arbitraire ?

**Exercice 3 (Cours)** 1) Soient $a_1, \ldots, a_n \in \mathbf{Z}$. Montrer qu'il existe un unique $d \in \mathbf{N}$ tel que :

$$\mathrm{Div}(d) = \mathrm{Div}(a_1) \cap \cdots \cap \mathrm{Div}(a_n).$$

C'est donc le pgcd de $a_1, \ldots, a_n$.
2) Montrer qu'il existe $x_1, \ldots, x_n \in \mathbf{Z}$ tels que $d = a_1 x_1 + \cdots + a_n x_n$.
3) Enoncer et prouver les assertions correspondantes pour $K[X]$.

**Exercice 4 (Cours)** 1) Soient $a = \varepsilon \prod p_i^{r_i}$ et $a' = \varepsilon' \prod p_i^{r_i'}$ (décompositions en facteurs premiers). Montrer que $a'$ divise $a$ si, et seulement si, $\forall i$ , $r_i' \leq r_i$. En déduire le nombre de diviseurs de $a$.
2) Montrer qu'en général $a \wedge a' = \prod p_i^{\min(r_i, r_i')}$.
3) Donner une condition nécessaire et suffisante pour que $a$ soit un carré.
4) On suppose $a$ et $a'$ premiers entre eux et tels que $aa'$ soit un carré. Montrer que soit $a$ et $a'$ sont des carrés, soit $-a$ et $-a'$ sont des carrés.
5) Montrer que 2 n'est pas le carré d'un nombre rationnel.

**Exercice 5 (Cours)** 1) Soit $p$ un nombre premier. Montrer que les coefficients binomiaux $\binom{p}{k}$ sont multiples de $p$ pour $k = 1, \ldots, p-1$.
2) En déduire, pour $x, y \in \mathbf{Z}$ arbitraires, la congruence $(x+y)^p \equiv x^p + y^p \pmod{p}$.
3) Démontrer le petit théorème de Fermat : $a^p \equiv a \pmod{p}$ pour tout $a \in \mathbf{Z}$.
4) Démontrer que $a^{561} \equiv a \pmod{561}$ pour tout $a \in \mathbf{Z}$.

**Exercice 6 (Cours)** 1) Soient $a_1, \ldots, a_n \in \mathbf{Z}$ strictement positifs et premiers entre eux deux à deux. Montrer que les entiers $b_i := \prod_{\substack{1 \leq j \leq n \\ j \neq i}} a_j$ sont premiers entre eux dans leur ensemble, et en déduire, pour tout $b \in \mathbf{Z}$, l'existence de $x_1, \ldots, x_n, y \in \mathbf{Z}$ tels que :

$$\frac{b}{a_1 \cdots a_n} = y + \frac{x_1}{a_1} + \cdots + \frac{x_n}{a_n}.$$

Montrer que l'on peut imposer $0 \leq x_i \leq a_i - 1$ pour $i = 1, \ldots, n$ et que l'écriture est alors unique.
2) Enoncer et prouver les assertions correspondantes pour $K[X]$. Détailler en particulier le cas du corps $K = \mathbf{C}$. (On aura reconnu la *décomposition en éléments simples* des fractions rationnelles.)

**Exercice 7 (Cours)** Quels sont les irréductibles de $\mathbf{R}[X]$ ? de $\mathbf{C}[X]$ ? Quels sont les irréductibles de degré 2 de $\mathbf{Q}[X]$ ? Quel lien y a-t-il en général entre l'existence de racines de $P(X)$ dans $K$ et son irréductibilité dans $K[X]$ ? Que peut-on dire de mieux pour les degrés 2 et 3 ?

**Exercice 8** 1) Soient $x,y,z \in \mathbf{Z}$ tels que $x^2+y^2=z^2$. On suppose tout d'abord $x,y,z$ premiers entre eux dans leur ensemble, autrement dit, que leur pgcd est 1. Montrer : qu'ils sont premiers entre eux deux à deux ; que $x$ ou $y$ est impair, mais pas les deux ; que $z$ est impair.
2) On suppose que c'est $x$ qui est impair. Montrer que $z-x$ et $z+x$ ont pour pgcd 2, puis que $(z-x)/2$ et $(z+x)/2$ sont des carrés. En déduire qu'il existe $u,v \in \mathbf{Z}$ tels que $x=u^2-v^2$, $y=2uv$ et $z=u^2+v^2$.
3) Décrire toutes les solutions entières de l'équation $x^2+y^2=z^2$ sans hypothèse sur $x,y,z$.
4) Montrer que l'équation $x^4+y^4=z^4$ n'admet pas de solutions entières non évidentes, *i.e.* telles que $xy \neq 0$.

**Exercice 9** 1) Montrer que le reste de la division euclidienne de $X^a-1$ par $X^b-1$ est $X^r-1$, où $r$ est le reste de la division euclidienne de $a$ par $b$.
2) Montrer que le pgcd de $X^n-1$ et de $X^p-1$ est $X^q-1$, où $q$ est le pgcd de $n$ et $p$.

**Exercice 10** 1) On pose $P_n(X) := \dfrac{1}{n!}\prod_{i=0}^{n-1}(X-i)$. (Donc, par la convention usuelle sur les produits vides, $P_0=1$.) Montrer que tout polynôme de $\mathbf{C}[X]$ de degré $\leq n$ admet une unique décomposition $P=a_0P_0+\cdots+a_nP_n$ avec $a_0,\ldots,a_n \in \mathbf{C}$.
2) Montrer que $P(\mathbf{Z}) \subset \mathbf{Z}$ si, et seulement si, $a_0,\ldots,a_n \in \mathbf{Z}$.

**Exercice 11** 1) Soient $a,b \in \mathbf{Z}$ avec $a>b>0$. On définit une suite $(x_n)$ d'entiers par $x_0 := a$, $x_1 := b$ ; et, pour tout $n \geq 2$ tel que $x_n$ est non nul, $x_{n+1}$ est le reste de la division euclidienne de $x_{n-1}$ par $x_n$. Montrer que la suite $(x_n)$ décroît strictement et qu'il existe $p$ tel que $x_p \neq 0$ et $x_{p+1}=0$. (La suite est donc finie.) Vérifier que $d := x_p$ est le pgcd de $a$ et $b$.
2) On note $q_n$ le quotient de la division euclidienne de $x_{n-1}$ par $x_n$. Démontrer la formule :

$$\begin{pmatrix} a \\ b \end{pmatrix} = M \begin{pmatrix} d \\ 0 \end{pmatrix}, \text{ où } M := \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_p & 1 \\ 1 & 0 \end{pmatrix}.$$

3) Montrer que $M^{-1}$ est à coefficients entiers et permet de calculer les coefficients de Bézout.

**Exercice 12** 1) Soient $A,B \in K[X]$ tous deux non nuls et tels que $\deg A > \deg B$. On définit une suite $(A_n)$ de polynômes par $A_0 := A$, $A_1 := B$ ; et, pour tout $n \geq 2$ tel que $A_n$ est non nul : $A_{n+1}$ est le reste de la division euclidienne de $A_{n-1}$ par $A_n$. Montrer que la suite $(\deg A_n)$ décroît strictement et qu'il existe $p$ tel que $A_p \neq 0$ et $A_{p+1}=0$. Vérifier que $\Delta := A_p$ est un pgcd de $A$ et $B$.
2) On note $Q_n$ le quotient de la division euclidienne de $A_{n-1}$ par $A_n$. On pose $F_0 := 1$, $G_0 := 0$, $F_1 := 0$, $G_1 := 1$, puis, pour $n=1,\ldots,p$ :

$$F_{n+1} := F_{n-1} - Q_nF_n \text{ et } G_{n+1} := G_{n-1} - Q_nG_n.$$

3) Montrer que $A_n = F_nA + G_nB$ pour $n=0,\ldots,p+1$. Vérifier, pour $n=1,\ldots,p$, les relations :

$$\deg Q_n = \deg A_{n-1} - \deg A_n \text{ et } \deg G_n = \deg Q_1 + \cdots + \deg Q_{n-1}.$$

4) En déduire que $F_p, G_p$ sont, à un facteur constant près, les coefficients obtenus à l'exercice 2.