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

On se donne un anneau $A \neq \{0\}$ commutatif unitaire intègre et $\mathbb{K}$ un corps.

1 PGCD et PPCM selon les anneaux

Soit $(a_1, ..., a_r) \in (A^*)^r$ où $r \geq 2$.

1.1 Dans un anneau quelconque

Définition 1 (ROM 242)**.** On dit que $a_1, .., a_r$ admettent un plus grand commun diviseur s'il existe $\delta \in A^*$ tel que :

$$\begin{cases} \forall k \in \{1, ..., r\}, \delta \text{ divise } a_k \\ \text{tout diviseur commun à } a_1, .., a_r \text{ divise } \delta \end{cases}$$

Notation 2 (ROM 243)**.** On le note $pgcd(a_1, ..., a_r)$ ou $a_1 \wedge ... \wedge a_r$.

Proposition 3 (ROM 242)**.** Deux *pgcd* de $a_1, ..., a_r$ sont associés.

Contre-exemple 4 (No ref)**.** Dans l'anneau, $\mathbb{Z}[i\sqrt{3}]$, $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ et $2(1 + i\sqrt{3})$ n'ont pas de pgcd. Ceci montre qu'il n'y a pas toujours existence du *pgcd*.

Définition 5 (ROM 243)**.** On dit que l'anneau A est un anneau à pgcd si deux éléments quelconques $a, b \in A^*$ admettent un pgcd.

On considère désormais que A est un anneau à pgcd.

Définition 6 (ROM 245)**.** On dit que $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si leur pgcd est dans $A^\times$.

Proposition 7 (ROM 245)**.** Soit d un diviseur commun à $a_1, ..., a_r$. Pour tout k compris entre 1 et r, considérons $\alpha_k \in A$ tel que $a_k = d\alpha_k$. On a : $d = pgcd(a_1, ..., a_k) \iff pgcd(\alpha_1, .., \alpha_r) = 1$

Théorème 8 (ROM 245)**.** [Gauss] Soit $a, b \in A$. a et b sont premier entre eux si et seulement si pour tout $c \in A^*$, $a|bc$ implique $a|c$.

On se replace dans le cas d'un anneau A quelconque.

Définition 9 (ROM 246)**.** On dit que $a_1, .., a_r$ admettent un plus petit commun multiple s'il existe $\mu \in A^*$ tel que :

$$\begin{cases} \forall k \in \{1, ..., r\}, \mu \text{ est multiplie de } a_k \\ \text{tout multiple commun à } a_1, .., a_r \text{ multiple } \mu \end{cases}$$

Notation 10. On le note $ppcm(a_1, ..., a_r)$ ou $a_1 \vee ... \vee a_r$.

Proposition 11 (ROM 243)**.** Deux *ppcm* de $a_1, ..., a_r$ sont associés.

Proposition 12 (ROM 243 246)**.** Le ppcm et le pgcd sont associatifs et commutatifs.

Proposition 13 (ROM 246)**.** A est un anneau à pgcd si et seulement si tout éléments $a, b \in A^*$ admettent un ppcm.
Dans ce cas, on a $ab = pgcd(a, b)ppcm(a, b)$ à une unité près. BOOF

1.2 Dans un anneau factoriel

Définition 14 (ROM 224)**.** On dit que A est un anneau factoriel s'il est intègre et si tout élément non nul et non inversible s'écrit de manière unique comme produit d'éléments irréductibles (à l'ordre près des facteurs).

Supposons dans la suite que A soit factoriel.

Proposition 15 (ROM 244)**.** A est un anneau à pgcd. Plus précisément, pour $a = u \prod_{k=1}^{r} p_k^{m_k}$, et $b = v \prod_{k=1}^{r} p_k^{n_k}$ dans $A^* \setminus A^\times$, où u, v sont inversibles, les p_k sont irréductibles deux à deux non associés et les n_k, m_k sont des entiers naturels. On a $a \wedge b = \prod_{k=1}^{r} p_k^{min(m_k, n_k)}$.

Proposition 16 (ROM 244)**.** Pour tout $\lambda \in A^*$, $pgcd(\lambda a_1, ..., \lambda a_n) = \lambda pgcd(a_1, ..., a_n)$.

1.3 Dans un anneau principal

Définition 17 (ROM 137)**.** On dit que l'anneau A est principal s'il est intègre et si tout idéal de A est prinicpal.

On suppose désormais A prinicpal.

Proposition 18 (ROM 243)**.** A est un anneau à pgcd. Plus précisément, il existe $\delta \in A^*$ tel que $(a_1, ..., a_r) = (\delta)$ et cet élément s'écrit $\delta = \sum_{i=1}^{r} u_k a_k$ où $u_1, .., u_r \in A$ et $\delta = pgcd(a_1, ..., a_r)$.

Théorème 19 (ROM 247)**.** [Bézout] Les $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si et seulement si il existe $(u_1, ..., u_k) \in A^r$ tel que $\sum_{k=1}^{r} u_k a_k = 1$.

Application 20 (GOU 185)**.** [lemme des noyaux] Sot $\mathbb{K}$ un corps. Soient $P = P_1...P_r \in \mathbb{K}[X]$ où les P_i sont premiers entre eux deux à deux. Soit $f \in \mathcal{L}(E)$ où E est un $\mathbb{K}-$ev. On a :

$$ker(P(f)) = ker(P_1(f)) \oplus ... \oplus ker(P_k(f))$$

Corollaire 21 (ROM 247)**.** Soient $a, b, c \in A$. Si $a \wedge c = 1$, alors $a \wedge b = a \wedge (bc)$.

Proposition 22 (ROM 248)**.** Il existe $\mu \in A$ tel que $(a_1) \cap ... \cap (a_r) = (\mu)$ et μ est un ppcm de $a_1, ..., a_r$.

Corollaire 23. A voir ! Si les a_k sont deux à deux premiers entre eux, on a alors $ppcm(a_1, ..., a_r) = \prod_{i=1}^{r} a_k$ à une unité près.

Exemple 24 (No ref)**.** Comme $ppcm(8, 6) = 24$, on a $(\mathbb{Z}/8\mathbb{Z}) \cap (\mathbb{Z}/6\mathbb{Z}) = (\mathbb{Z}/24\mathbb{Z})$.

Théorème 25 (thm chinois)**.** [TL1 149, DEV 1] Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. Étant donné des entiers $a_1, .., a_r$, considérons le système de congruences :
$(S) : x \equiv a_i \ [m_i] \ (i = 1, ..., r)$
Ce système possède une solution $x \in \mathbb{Z}$ qui est unique modulo M.

Corollaire 26 (TL1 150)**.** Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. On a alors :

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/m_i\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$$

2 Algorithmes de calcul dans un anneau euclidien

Définition 27 (ROM 261)**.** L'anneau A est dit euclidien s'il existe un stathme $\varphi : A^* \to \mathbb{N}$ tel que pour tout $(a, b) \in A^2$ avevc $b \neq 0$, il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0_A$ ou $r \neq 0_A$ et $\varphi(r) < \varphi(b)$.

Exemple 28 (ROM 266)**.** L'anneau $\mathbb{Z}$ est euclidien pour le stathme $\varphi : n \in \mathbb{Z}^* \mapsto |n|$.

Proposition 29 (ROM 263)**.** Un anneau euclidien est factoriel.

Dans la suite, (A, φ) est un anneau euclidien.

Algorithme 30 (Euclide)**.** [ROM 265] Soit $a, b \in A$ tels que $\varphi(a) \geq \varphi(b)$. On définit la suite $(r_n)_n$ de la manière suivante :

1. $r_0 = b$
2. r_1 est un reste de la division euclidienne de a par b. On a alors $r_1 = 0_A$ ou $0 \leq \varphi(r_1) < \varphi(r_0)$.
3. Pour $n \geq 2$, si $r_{n-1} \neq 0_A$, on pose désigne par r_n un reste dans la division euclidienne de r_{n-2} par r_{n-1}. On a alors $r_n = 0_A$ ou $0 \leq \varphi(r_n) < \varphi(r_{n-1})$.

Il existe alors un entier $p \in \mathbb{N}^*$ tel que $r_p = 0_A$, $0 \leq \varphi(r_{p-1}) < ... < \varphi(r_1) < \varphi(r_0)$ et $a \wedge b = r_0 \wedge r_1 = ...r_{p-1} \wedge r_p = r_{p-1}$. De plus on a construit deux suites $(q_n)_{0 \leq n \leq p}$ et $(r_n)_{0 \leq n \leq p}$ tels que :

$$\begin{cases} a = q_1 r_0 + r_1 \\ r_0 = q_2 r_1 + r_2 \\ ... \\ r_{p-2} = q_p r_{p-1} + r_p \end{cases}$$

Exemple 31 (GOU 12)**.** Considérons les nombre 47 et 111. On effectue l'algorithme d'euclide :
$111 = 47 * 2 + 17$
$47 = 17 * 2 + 13$
$17 = 13 * 1 + 4$
$13 = 4 * 3 + 1$
Le pgcd de 47 et 111 est donc 1.

Algorithme 32 (Euclide étendu)**.** [ROM 265] L'algorithme précédent permet également de trouver les coefficients de l'identité de Bézout, en le remontant. Pour tout k allant de 0 à $p - 1$, il existe u_k et v_k dans A tels que $r_k = au_k + bv_k$:

1. pour $k=0$, $r_0 = a \cdot 0_A + b \cdot 1_A$
2. Pour $k=1$, $r_1 = a \cdot 1_A + b \cdot (-q_1)$
3. En supposant le résultat acquis jusqu'à l'ordre $k-1$, pour $0 \leq k-1 \leq p-2$, on a

$$\begin{aligned} r_k &= -q_k r_{k-1} + r_{k-2} \\ &= -q_k(au_{k-1} + bv_{k-1}) + au_{k-2} + bv_{k-2} \\ &= a(u_{k-2} - q_k u_{k-1}) + b(v_{k-2} - q_k v_{k-1}) \end{aligned}$$

En particulier, pour $k = p-1$, on a $a \wedge b = r_{p-1} = au_{p-1} + bv_{p-1}$.

Exemple 33 (GOU 12)**.** Effectuons la méthode de la remontée dans l'exemple précédent.

$$\begin{aligned} 1 &= 13 - 4 * 3 \\ &= 13 - (17 - 13 * 1) * 3 = 4 * 13 - 3 * 17 \\ &= 4 * (47 - 17 * 2) - 3 * 17 = 4 * 47 - 11 * 17 \\ &= 4 * 47 - 11 * (111 - 47 * 2) = 26 * 47 - 11 * 111 \end{aligned}$$

Les entiers $u = 26$ et $v = -11$ vérifient l'égalité de Bézout.

Remarque 34 (No ref)**.** Cette méthode est effective pour 2 éléments. Pour obtenir le *pgcd* d'une famille d'éléments, on peut procéder par cette algorithme en utilisant l'associativité du *pgcd*.

3 Applications

3.1 Équations diophantiennes

On considère toujours n un entiers supérieur ou égal à 2.

Définition 35 (ROM 289)**.** Une équation diophantienne est une équation à solutions dans $\mathbb{Z}$ de la forme $ax \equiv b\ [n]$ où $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$.

Exemple 36. Si $b = 1$, cette équation a des solutions si et seulement si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Théorème 37 (ROM 290)**.** Soit $\delta = pgcd(a, n)$. L'équation diophantienne $ax \equiv b\ [n]$ a des solutions entières si et seulement si δ divise b.
Dans ce cas, l'ensemble des solutions est $S = \{b'x'_0 + kn' | k \in \mathbb{Z}\}$ où x_0 est une solution particulière de $a'x \equiv 1\ [n]$.

Exemple 38 (No ref)**.** $9x \equiv 15\ [23]$ admet une unique solution modulo 23

Application 39 (un peu ROM 290, 291)**.** Le théorème chinois permet de résoudre des système d'équations diophantienne. Le système

$$\begin{cases} k \equiv a_1\ [n_1] \\ \quad \ldots \\ k \equiv a_r\ [n_r] \end{cases}$$

a toujours une infinité de solutions si la famile $(a_i)_{1 \leq i \leq r}$ est une famille d'éléments 2 à 2 premiers entre eux. Cette solution est unique modulo $n = n_1..n_r$.

Exemple 40 (BER 469)**.** Considérons le système d'équations diophantiennes :

$$\begin{cases} k \equiv 1\ [3] \\ k \equiv 2\ [4] \\ k \equiv -1\ [7] \end{cases}$$

3, 4 et 7 sont deux à deux premiers entre eux donc ce système a des solutions. La 1ère équation donne $x = 1 + 3y, y \in \mathbb{Z}$. En reportant dans la 2−ème, on obtient $3y \equiv 1[4]$. On a alors $y \equiv -1\ [4]$, soit $y = -1 + 4z, z \in \mathbb{Z}$ donc $x = 1 + 3(-1 + 4z) = -2 + 12z$ avec $z \in \mathbb{Z}$. En reportant dans la dernière égalité on a $12z \equiv 1\ [7]$ soit $5z \equiv 1[7]$ puis $z \equiv 3[7]$ car 3 est l'inverse de 5 modulo 7. Ainsi $z = 3 + 7t, t \in \mathbb{Z}$ et finalement $x =_2 +12(3 + 7t) = 34 + 84t, t \in \mathbb{Z}$.

Application 41 (ROM 291)**.**

$$\begin{cases} k \equiv a_1\ [n_1] \\ k \equiv a_2\ [n_2] \end{cases}$$

a des solutions si et seulement si $\delta = n_1 \wedge n_2$ divise $a_2 - a_1$

Une autre app du thm chinois : Si $n \geq 2$ avec $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, on a $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$.

3.2 Théorème de Fermat

Théorème 42 (TL1 138)**.** [dernier théorème de Fermat, admis] Pour des entiers $n \leq 3$ et $xyz \neq 0$, l'égalité $x^n + y^n = z^n$ est impossible.

Exemple 43 (No ref)**.** Pour $n = 2$, $((x, y, z) = (3, 4, 5)$ est une solution de cette équation.

Théorème 44 (ORAUX XENS Al1)**.** [Théorème de Sophie Germain][DEV 2] Soit p un nombre premier de Sophie Germain, i.e. tel que p est impair et $q = 2p + 1$ est premier. Il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tels que $xyz \not\equiv 0\ [p]$ et $x^p + y^p + z^p = 0$

3.3 Ordre dans un groupes

Soit G un groupe fini. On suppose connue la définition d'ordre. On note $o(g)$ l'ordre de $g \in G$.

Proposition 45 (ROM 8)**.** Soient $g, h \in G$ et $k \in \mathbb{Z}^*$.

1. $o(g^k) = \frac{o(g)}{pgcd(o(g),k)}$
2. Si $k|o(g)$, alors $o(g^k) = \frac{o(g)}{|k|}$
3. Si k est premier avec $o(g)$, on a $o(g^k) = o(g)$
4. Si $gh = hg$, alors $o(hg)|o(g) \vee o(h)$. Si $o(g) \wedge o(h) = 1$, alors $o(gh) = ppcm(o(g), o(h)) = o(g)o(h)$

Proposition 46 (ROM 9)**.** Si $(G, \cdot)$ est un groupe commutatif et $g_1, .., g_r$ des éléments deux à deux distincts de G d'ordres respectifs $m_1, .., m_r$. Alors il existe $g_0 \in G$ tel que $o(g_0) = ppcm(m_1, .., m_r)$.

Proposition 47 (ROM 9)**.** Si G est commutatif alors $\max_{g \in G} o(g) = ppcm\{o(g)|g \in G\}$.

3.4 Les polynômes

Définition 48 (ROM 382)**.** Le contenu d'un polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X] \setminus \{0\}$ est l'entier $c(P) = pgcd(a_0, .., a_n)$.
Si $c(P) = 1$, on dit que P est primitif

Lemme 49 (GOU 62)**.** Soient $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. Si p divise tous les coefficients de PQ, alors p divise tous les coefficients de P ou tous ceux de Q.

Lemme 50 (GOU 62)**.** [Gauss] Si $P, Q \in \mathbb{Z}[X]$ alors $c(PQ) = c(P)c(Q)$.

Lemme 51 (GOU 62)**.** Si $\phi \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, alors il est irréductible dans $\mathbb{Q}[X]$.

Théorème 52 (GOU 62)**.** [critère d'Eisenstein] Soit $P = a_n X^n + .. + a_1 X + a_n \in \mathbb{Z}[X]$ et p un nombre premier. Si on a :

1. p ne divise pas a_n
2. p divide a_i, pour tout $1 \leq i \leq n-1$
3. p^2 ne divise pas a_0

Alors P est irréductible dans $\mathbb{Q}[X]$.