PGCDs liés à des suites récurrentes d'ordre deux

Jean-François Burnol, 21 octobre 2017

Soit $\mathcal{A}$ un anneau unitaire intègre commutatif principal. On note $\mathcal{K}$ son corps des fractions. On a principalement en tête les cas $\mathcal{A} = \mathbf{Z}$ et $\mathcal{A} = \mathbf{K}[X]$ avec $\mathbf{K}$ un corps. On suppose que pour chaque idéal $I \subset \mathcal{A}$ on a fixé une règle choisissant un générateur d de l'idéal I (en particulier $d = 1$ pour $I = \mathcal{A}$) donc on peut parler du PGCD d'éléments de $\mathcal{A}$ en tant qu'élément de $\mathcal{A}$. On pourrait s'en passer et alors un PGCD serait simplement un idéal, mais bref. On utilisera la notation $\mathrm{pgcd}(a_1, a_2, \dots)$ et par endroits pour être très clair $\mathrm{pgcd}_{\mathcal{A}}(a_1, a_2, \dots)$.

On va s'intéresser à des suites récurrentes $(u_n)_{n\in\mathbf{N}}$ dans $\mathcal{A}$ vérifiant :

$$u_0 = 0\,, \tag{1}$$
$$u_1 \neq 0\,, \tag{2}$$
$$u_{n+2} = pu_{n+1} + qu_n\,, \tag{3}$$

et les coefficients de la récurrence vérifient :

$$p, q \in \mathcal{A}\,, \tag{4}$$
$$\mathrm{pgcd}_{\mathcal{A}}(p, q) = 1\,, \tag{5}$$
$$q \neq 0\,. \tag{6}$$

Ne pas perdre de vue par la suite que p et q ne sont pas nécessairement des entiers, mais bien des éléments de $\mathcal{A}$.

Il est commode de définir les u_n pour $n < 0$ de sorte que la récurrence soit aussi valable pour les indices négatifs, mais cela nécessite d'utiliser le corps des fractions $\mathcal{K}$, par exemple $u_1 = qu_{-1}$ donc $u_{-1} = \frac{1}{q}u_1$.

Un rôle central est joué par la matrice suivante :

$$A = \begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix}\,, \tag{7}$$

car il est bien connu et facile à montrer par récurrence que :

$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = A^n \cdot \begin{pmatrix} u_1 \\ u_0 \end{pmatrix} = u_1 \cdot A^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8}$$

On a aussi (maintenant que u_{-1} est défini) :

$$\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A^n \cdot \begin{pmatrix} u_0 \\ u_{-1} \end{pmatrix} = u_{-1} \cdot A^n \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{q} u_1 \cdot A^n \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{9}$$

Donc :

$$A^n = A^n \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u_1^{-1} u_{n+1} & q \cdot u_1^{-1} u_n \\ u_1^{-1} u_n & q \cdot u_1^{-1} u_{n-1} \end{pmatrix} \tag{10}$$

Comme A^n est à coefficients dans $\mathcal{A}$, $u_n/u_1 \in \mathcal{A}$ (ce qui était assez clair a priori). On posera par la suite $\boxed{v_n = u_n/u_1}$.

$$A^n = \begin{pmatrix} v_{n+1} & q \cdot v_n \\ v_n & q \cdot v_{n-1} \end{pmatrix} \tag{11}$$

La définition (7) nous permet de calculer A^n modulo q facilement (et aussi modulo p, mais je n'en ai pas besoin).

$$n \geqslant 1 \implies A^n \bmod q \equiv \begin{pmatrix} p^n & 0 \\ p^{n-1} & 0 \end{pmatrix} \tag{12}$$

La vérification par récurrence est immédiate. Donc, pour $n \geqslant 1$, $v_n \equiv p^{n-1} \bmod q$, i.e. il existe une écriture $v_n = p^{n-1} + qy$, $y \in \mathcal{A}$. Mais, comme il est bien connu, de $\operatorname{pgcd}_{\mathcal{A}}(p, q) = 1$ résulte $\operatorname{pgcd}_{\mathcal{A}}(p^{n-1}, q) = 1$, donc on a une identité de Bézout $1 = ip^{n-1} + jq = i(v_n - yq) + jq = iv_n + (j - iy)q$ (attention ici $i, j \in \mathcal{A}$!) et $\operatorname{pgcd}_{\mathcal{A}}(v_n, q) = 1$. Cela nous servira par la suite.

La matrice A^n est diagonale modulo v_n. Donc si n divise N alors la matrice A^N est à nouveau diagonale modulo v_n. Donc v_N est zéro modulo v_n :

$$n \mid N \implies v_n \mid v_N \tag{13}$$

Par conséquent $v_{\operatorname{pgcd}(n,m)}$ divise à la fois v_n et v_m. On peut donc affirmer :

$$v_{\operatorname{pgcd}(n,m)} \mid D = \operatorname{pgcd}(v_n, v_m) \tag{14}$$

On va prouver la divisibilité dans l'autre sens. Pour cela on part d'une identité de Bézout dans $\mathbf{Z}$, $d = \operatorname{pgcd}(n, m) = un + vm$. Attention l'un de u ou v est négatif (sauf si $n \mid m$ ou $m \mid n$).

Considérons la matrice $\bar{A}$ qui est A réduite modulo D.

Son déterminant est la réduction modulo D du déterminant $-q$ de A. Mais D divise v_n et on a vu que $\operatorname{pgcd}(v_n, q) = 1$ donc aussi $\operatorname{pgcd}(D, q) = 1$. Par conséquent le déterminant $\det \bar{A}$ est un inversible de $\mathcal{A}/(D)$. Et donc la

matrice réduite est inversible dans cet anneau.[1] On peut donc sans entourloupes écrire :

$$\bar{A}^{d} = \bar{A}^{un+vm} = (\bar{A}^{n})^{u} \cdot (\bar{A}^{m})^{v} \qquad \text{dans } \mathcal{A}/(D) \tag{15}$$

La matrice A^n est diagonale modulo v_n donc modulo D qui le divise. La matrice A^m est diagonale modulo v_m donc modulo D qui le divise. Nous avons donc un produit d'une puissance d'une matrice diagonale par une puissance négative d'une matrice diagonale (inversible) ce qui donne une matrice diagonale. Ceci implique que D divise les coefficients non-diagonaux de A^d, c'est-à-dire D divise v_d, c.q.f.d.

Conclusion :

$$\operatorname{pgcd}(v_n, v_m) \sim v_{\operatorname{pgcd}(n,m)}\,, \tag{16}$$

où le $\sim$ signifie que les éléments sont associés.

Si l'on revient aux $u_n = u_1 v_n$, on sait que $\operatorname{pgcd}(u_1 v_n, u_1 v_m) \sim u_1 \operatorname{pgcd}(v_n, v_m)$ donc $\sim u_1 v_{\operatorname{pgcd}(n,m)} = u_{\operatorname{pgcd}(n,m)}$. Donc :

Théorème 1. *Sous les conditions* (1), (2), (3), (4), (5), (6) *dans l'anneau principal $\mathcal{A}$:*

$$\boxed{\operatorname{pgcd}(u_n, u_m) \sim u_{\operatorname{pgcd}(n,m)}} \tag{17}$$

PLUS CONCRÈTEMENT

Supposons $1 \leqslant d < m < n$ avec $d = \operatorname{pgcd}(m, n)$. Rendons concrète la preuve faite plus haut que v_d appartient à l'idéal engendré par v_m et v_n. L'algorithme d'Euclide étendu fournit une identité de Bézout $d = im + jn$ et sous les hypothèses faites soit $i > 0 > j$ soit $i < 0 < j$. Supposons le premier cas, remplaçons j par $-j$ donc $d = im - jn$, $i, j > 0$.[2] On écrit alors :

$$A^d A^{jn} = \begin{pmatrix} v_{d+1} & q \cdot v_d \\ v_d & q \cdot v_{d-1} \end{pmatrix} \cdot \begin{pmatrix} v_{jn+1} & q \cdot v_{jn} \\ v_{jn} & q \cdot v_{jn-1} \end{pmatrix} = A^{im} = \begin{pmatrix} v_{im+1} & q \cdot v_{im} \\ v_{im} & q \cdot v_{im-1} \end{pmatrix} \tag{18}$$

La matrice A^{jn} a pour déterminant $(-q)^{jn}$. Donc :

$$\begin{pmatrix} v_{d+1} & q \cdot v_d \\ v_d & q \cdot v_{d-1} \end{pmatrix} = (-q)^{-jn} \begin{pmatrix} q v_{jn-1} & -q \cdot v_{jn} \\ -v_{jn} & v_{jn+1} \end{pmatrix} \cdot \begin{pmatrix} v_{im+1} & q \cdot v_{im} \\ v_{im} & q \cdot v_{im-1} \end{pmatrix} \tag{19}$$

1. Il faut en toute rigueur soit vérifier que ce que l'on dit marche aussi si $D = 1$, donc dans le cas où l'anneau quotient est l'anneau nul, soit traiter $D = 1$ à part et dire simplement qu'on n'a rien à prouver dans ce cas…

2. L'algorithme garantit (le savez-vous ?) que les i, j trouvés vérifient $i < n$, $j < m$.

$$\implies (-q)^{jn} \cdot v_d = -v_{jn}v_{im+1} + v_{jn+1}v_{im} \tag{20}$$

La preuve donnée plus haut se traduit alors en cet argument : déjà on sait que $v_{jn} = \alpha v_n$ et $v_{im} = \beta v_m$ pour $\alpha, \beta \in \mathcal{A}$. Donc à ce stade on voit concrètement que $q^{jn}v_d$ est dans l'idéal $v_n\mathcal{A}+v_m\mathcal{A}$. Il faut se débarrasser de la puissance parasite q^{jn}. On a expliqué que comme v_n modulo q vaut p^{n-1}, et que $\mathrm{pgcd}_{\mathcal{A}}(p, q) = 1$, on peut trouver une identité de Bézout dans $\mathcal{A}$ du type $1 = \gamma v_n + \delta q$.[3] En élevant à la puissance jn et en mettant v_n en facteur, on obtient $1 = \Gamma v_n + \delta^{jn}q^{jn}$ avec un $\Gamma \in \mathcal{A}$. Donc $v_d = \Gamma v_n v_d + \delta^{jn}q^{jn}v_d$ et en utilisant l'équation (20) pour $q^{jn}v_d$, on exhibe ainsi v_d comme combinaison de v_n, v_{jn} et v_{im} donc de v_n et v_m.

Ça marche mais on voit que c'est un peu compliqué à la fin et ne donne pas une expression explicite *a priori* (on n'a que (20)) : il faudrait peut-être que j'y réfléchisse un peu plus.

EXEMPLES

Avec $\mathcal{A} = \mathbf{Z}$, $p = q = 1$ on a les nombres de Fibonacci.

$$\boxed{\mathrm{pgcd}(F_n, F_m) = F_{\mathrm{pgcd}(n,m)}} \tag{21}$$

Ici on a $q = 1$ donc l'équation (20) donne directement une chose concrète, modulo le fait de savoir que F_n divise F_{jn} et F_m divise F_{im}.

Avec $\mathcal{A} = \mathbf{Z}$, et a et b deux entiers *non nuls et premiers entre eux*, on peut considérer les $u_n = a^n - b^n$. On a $u_0 = 0, u_1 = a - b$, et pour assurer $u_1 \neq 0$ il faut exclure les couples $(a = 1, b = 1)$ et $(a = -1, b = -1)$. On prend p et q les coefficients du polynôme caractéristique $(X - a)(X - b) = X^2 - (a + b)X + ab$, donc $p = a + b$ et $q = -ab$.

Il est vrai que q est non nul, et aussi que p *et* q *sont premiers entre eux*. Car si un nombre premier ℓ divise q il divise soit a soit b ; dans le premier cas si ℓ divise p il divise aussi b, et dans le deuxième cas si ℓ divise p il divise aussi a. Dans les deux cas si ℓ divise q et p il divise a et b, donc cela n'arrive jamais, c.q.f.d.[4]

Les conditions sont réunies pour pouvoir donc affirmer :

$$\boxed{\mathrm{pgcd}(a^n - b^n, a^m - b^m) = \pm(a^{\mathrm{pgcd}(n,m)} - b^{\mathrm{pgcd}(n,m)})} \tag{22}$$

3. On peut faire ça concrètement si on connaît concrètement une identité de Bézout dans $\mathcal{A}$ pour $1 = \mathrm{pgcd}_{\mathcal{A}}(p, q)$.

4. Il est aussi vrai que $\mathrm{pgcd}(a + b, ab) = 1 \implies \mathrm{pgcd}(a, b) = 1$.

pour tous $n, m \geqslant 0$, et tout couple (a, b) d'entiers relatifs tous les deux non nuls et premiers entre eux. [5] [6]

Remarque 1. Soit $a > b > 0$ des entiers premiers entre eux et $n > 1$. Pour que $a^n - b^n$ soit premier il est nécessaire que n soit premier et que $a = b + 1$.

Preuve. Si $n > 1$ n'est pas premier il admet un diviseur propre $d > 1$, donc $a^n - b^n$ admet le diviseur propre $a^d - b^d > 1$ (attention !), et n'est donc pas premier.

Par ailleurs $a^n - b^n$ est divisible par $a - b$ et lui est strictement supérieur, donc ne peut être premier que si $a = b + 1$.

Pour $(a, b) = (2, 1)$ on retrouve la notion de Nombres premiers de Mersenne, mais on ne sait pas à l'heure actuelle s'il en existe une infinité.

Pour $(a, b) = (3, 2)$, on trouve 5 ($n = 2$), 19 ($n = 3$), 211 ($n = 5$), 129009091 ($n = 17$),et 68629840493971 ($n = 29$) mais 7, 11, 13, 19, et 23 ne donnent pas des nombres premiers. □

À cause de la divisibilité par $a - b$ il n'est pas correct de s'intéresser qu'aux $u_n = a^n - b^n$, il vaut mieux regarder les $v_n = \frac{a^n - b^n}{a - b}$.

Remarque 2. Soit $a > b + 1$, $b > 0$ des entiers premiers entre eux et $n > 1$. Pour que $\frac{a^n - b^n}{a - b}$ soit premier il est nécessaire que n soit premier.

Preuve. Si $n > 1$ n'est pas premier il admet un diviseur propre $d > 1$. Nous savons que $v_d = \frac{a^d - b^d}{a - b}$ divise $v_n = \frac{a^n - b^n}{a - b}$. Or $1 < v_d$:

$$v_d = \sum_{k=0}^{d-1} a^{d-1-k} b^k > a^{d-1} ,$$

et $v_d < v_n$:

$$v_n / v_d = \sum_{k=0}^{n/d-1} (a^d)^{n/d-1-k} (b^d)^k > (a^d)^{n/d-1} .$$

Donc v_n admet le diviseur propre $v_d > 1$, et n'est donc pas premier.

Pour $(a, b) = (3, 1)$, nous trouvons que $(3^n - 1)/2$ est premier pour n égal à 3 (13), 7 (1093), 13 (797161), ...

Pour $(a, b) = (5, 3)$, nous trouvons que $(5^n - 3^n)/2$ est premier pour n égal à 13 (609554401), 19 (9536162033329), 23 (5960417405949649), ... □

5. Bien sûr si $a > b > 0$ on prend le signe plus dans l'équation.

6. Le cas spécial $a = b = 1$ fonctionne, mais sa vraie signification est après avoir divisé par $a - b$ et pris une limite, ce qui reconstitue simplement les entiers n, m et la formule marche aussi dans cette limite. Idem pour $a = b = -1$.

Avec $\mathcal{A} = \mathbf{Q}[X]$, on fait l'analogue de ce qui précède pour $a = X$ et $b = 1$, donc $p = X + 1$, $q = -X$. Il est vrai que p et q sont premiers entre eux et que q est non nul. Et $u_n = X^n - 1$ vérifie bien $u_0 = 0$ et $u_1 \neq 0$. On obtient donc

$$\boxed{\mathrm{pgcd}_{\mathbf{Q}[X]}(X^n - 1, X^m - 1) = X^{\mathrm{pgcd}(n,m)} - 1} \tag{23}$$

La formule ci-dessus marche pour $n = 0$ ou $m = 0$ mais imposons maintenant $n, m \geq 1$ pour éviter les cas particuliers dans la preuve qui suit.

Soit $T \in \mathbf{Z}[X]$ divisant à la fois $X^n - 1$ et $X^m - 1$ dans $\mathbf{Z}[X]$ (attention ce dernier anneau n'est pas principal donc je ne peux pas appliquer directement notre théorie générale). Le contenu $c(T)$ divise $c(X^n - 1) = 1$, donc T est de contenu 1. On sait que T divise $X^{\mathrm{pgcd}(n,m)} - 1$ dans $\mathbf{Q}[X]$, d'où une égalité

$$T \cdot U = X^{\mathrm{pgcd}(n,m)} - 1 \,, \tag{24}$$

avec un certain $U \in \mathbf{Q}[X]$. Posons $U = \frac{1}{d}V$ avec $V \in \mathbf{Z}[X]$. De

$$T \cdot V = d(X^{\mathrm{pgcd}(n,m)} - 1) \,, \tag{25}$$

il résulte en passant aux contenus que $c(V) = \pm d$, donc quitte à diviser les coefficients de V par d, on se ramène à $V \in \mathbf{Z}[X]$. On vient de démontrer ainsi que T divise $X^{\mathrm{pgcd}(n,m)} - 1$ dans $\mathbf{Z}[X]$.

L'anneau $\mathbf{Z}[X]$ est factoriel ce qui y autorise une notion de PGCD (via la décomposition en irréductibles), et on vient d'établir que $\mathrm{pgcd}(X^n - 1, X^m - 1)$ divisait $X^{\mathrm{pgcd}(n,m)} - 1$. La réciproque est évidente par identité remarquable (suites géométriques finies). Ainsi :

$$\boxed{\mathrm{pgcd}_{\mathbf{Z}[X]}(X^n - 1, X^m - 1) = X^{\mathrm{pgcd}(n,m)} - 1} \tag{26}$$