PGCD, PPCM, groupes cycliques, et sous-groupes

Jean-François Burnol, 12 avril 2018

Dans

http://jf.burnol.free.fr/agreg180411chinoiseriesII.pdf

je me suis intéressé au théorème suivant :

Théorème 1. *Soit $A, B, C \in \mathbb{Z}$. Alors :*

$$\operatorname{pgcd}\big(\operatorname{ppcm}(A,B),C\big) = \operatorname{ppcm}\big(\operatorname{pgcd}(A,C),\operatorname{pgcd}(B,C)\big) \tag{1}$$

J'y ai donné une démonstration qui ne passe pas par l'utilisation de la caractérisation des PGCD/PPCM via les nombres premiers.

> L'objet de cette fiche est de relier cette formule (d'au moins deux façons) à l'étude des groupes cycliques $\mathbb{Z}/N\mathbb{Z}$.

Mais la problématique du Théorème 1 est à peu près inépuisable. Commençons par énoncer un Théorème « dual » (au sens de l'échange PGCD↔PPCM) :

Théorème 2. *Soit $A, B, C \in \mathbb{Z}$. Alors :*

$$\operatorname{ppcm}\big(\operatorname{pgcd}(A,B),C\big) = \operatorname{pgcd}\big(\operatorname{ppcm}(A,C),\operatorname{ppcm}(B,C)\big) \tag{2}$$

Ici encore $ABC = 0$ se traite aisément (et le plus commodément via les idéaux de $\mathbb{Z}$ si par malheur on a oublié momentanément la définition de $\operatorname{pgcd}(0,0)$ par exemple) et on peut supposer $A, B, C > 0$. À ce stade vous avez le choix entre :

- je développe toute une théorie des « idéaux fractionnaires » qui sont des sous-groupes additifs de $\mathbb{Q}$ finiment engendrés,
- ou j'utilise un truc de ouf pour déduire le Théorème 2 du Théorème 1,
- ou encore je redémontre ab initio le Théorème 2 mais par des techniques comme dans la preuve du 1.

De toute façon ça vous est sans doute égal car déjà pour commencer vous préférez démontrer 2 par les nombres premiers. Donc je choisis la deuxième proposition.

Lemme 1 (Lemme de ouf)**.** *Soit $A, B, X > 0$ des entiers, tels que A et B divisent X. Alors*

$$\operatorname{pgcd}\left(\frac{X}{A},\frac{X}{B}\right) = \frac{X}{\operatorname{ppcm}(A,B)} \tag{3}$$

$$\operatorname{ppcm}\left(\frac{X}{A},\frac{X}{B}\right) = \frac{X}{\operatorname{pgcd}(A,B)} \tag{4}$$

Preuve. Posons $D = \operatorname{pgcd}(A, B)$, $X = k\operatorname{ppcm}(A, B)$, alors $\frac{X}{A} = k\frac{B}{D}$, $\frac{X}{B} = k\frac{A}{D}$. Or le PGCD possède une propriété d'homogénéité importante

$$\operatorname{pgcd}(kx, ky) = |k| \operatorname{pgcd}(x, y) \,, \tag{5}$$

qui n'est pas si triviale si on utilise la définition « de l'École », mais l'est avec les idéaux. Donc $\operatorname{pgcd}(X/A, X/B) = k\operatorname{pgcd}(B/D, A/D) = k$ ce qui est en fait la première équation...

L'homogénéité vaut aussi pour PPCM (comme conséquence de

$$\operatorname{ppcm}(kx, ky) \operatorname{pgcd}(kx, ky) = k^2|xy|$$

et de l'homogénéité du PGCD), donc $\operatorname{ppcm}(X/A, X/B) = k\operatorname{ppcm}(B/D, A/D) = kBA/D^2$ (ils sont premiers entre eux) ce qui donne une fois multiplié par D le résultat $kAB/D = k\operatorname{ppcm}(A, B) = X$, d'où la deuxième affirmation ! (on aurait pu simplement appliquer la première à $A' = X/A$, $B' = X/B$). □

Preuve du Théorème 2 comme conséquence du 1. Soit $X = ABC$, $A' = BC$, $B' = AC$, $C' = AB$, on suppose $A, B, C > 0$. On calcule :

$$\begin{aligned}
\operatorname{ppcm}\big(\operatorname{pgcd}(A, B), C\big) &= \operatorname{ppcm}\left(\operatorname{pgcd}(\frac{X}{A'}, \frac{X}{B'}), \frac{X}{C'}\right) && (6)\\
&= \operatorname{ppcm}\left(\frac{X}{\operatorname{ppcm}(A', B')}, \frac{X}{C'}\right) && (7)\\
&= \frac{X}{\operatorname{pgcd}\big(\operatorname{ppcm}(A', B'), C'\big)} && (8)\\
&= \frac{X}{\operatorname{ppcm}\big(\operatorname{pgcd}(A', C'), \operatorname{pgcd}(B', C')\big)} && (9)\\
&= \operatorname{pgcd}\left(\frac{X}{\operatorname{pgcd}(A', C')}, \frac{X}{\operatorname{pgcd}(B', C')}\right) && (10)\\
&= \operatorname{pgcd}\left(\operatorname{ppcm}(\frac{X}{A'}, \frac{X}{C'}), \operatorname{ppcm}(\frac{X}{B'}, \frac{X}{C'}\right) && (11)\\
&= \operatorname{pgcd}\big(\operatorname{ppcm}(A, C), \operatorname{ppcm}(B, C)\big) && (12)
\end{aligned}$$

Rien de bien sorcier, juste être systématique et buté et à la fin on voit qu'on a fini. De plus il est clair qu'on peut par la même méthode aller dans l'autre sens et déduire le Théorème 1 du Théorème 2. □

Bon, mais passons à ce que je voulais mettre en avant :

Théorème 3. *Soit $N \geqslant 1$. Soit $x \in \mathbb{N}$ et $\dot{x}$ sa classe de congruence modulo N. De plus on note $\langle \dot{x} \rangle$ le sous-groupe engendré dans $\mathbb{Z}/N\mathbb{Z}$. Soit de même $y \in \mathbb{N}$, $\dot{y}$, $\langle \dot{y} \rangle$. Alors :*

$$\langle \dot{x} \rangle \cap \langle \dot{y} \rangle = \left\langle \overdot{\operatorname{ppcm}(x, y)} \right\rangle \tag{13}$$

Preuve. Tout d'abord (comme il est bien connu et facile à vérifier par $x\mathbb{Z} + N\mathbb{Z} = d\mathbb{Z}$) :

$$\langle \dot{x} \rangle = \left\{ \dot{0}, \dot{d}, \widehat{2d}, \dots, \widehat{N-d} \right\} \tag{14}$$

avec $d = \mathrm{pgcd}(x, N)$. Et par conséquent :

$$\langle \dot{x} \rangle = \{ t \in \mathbb{Z}/N\mathbb{Z}, \quad \frac{N}{d} t = \dot{0} \} \tag{15}$$

En effet si $u \in \mathbb{Z}$ (et en particulier pour $0 \leqslant u < N$) alors $\frac{N}{d} u$ est divisible par N si et seulement si u est divisible par d. Donc les solutions de l'équation sont exactement les éléments précédemment énumérés de $\mathbb{Z}/N\mathbb{Z}$ et qui composent $\langle \dot{x} \rangle$.

Par conséquent, en posant $e = \mathrm{pgcd}(y, N)$, on a :

$$\langle \dot{x} \rangle \cap \langle \dot{y} \rangle = \{ t \in \mathbb{Z}/N\mathbb{Z}, \quad \frac{N}{d} t = \dot{0} \text{ et } \frac{N}{e} t = \dot{0} \} \tag{16}$$

$$= \{ t \in \mathbb{Z}/N\mathbb{Z}, \quad \forall k, l \in \mathbb{Z} \quad (k\frac{N}{d} + l\frac{N}{e}) t = \dot{0} \} \tag{17}$$

$$= \{ t \in \mathbb{Z}/N\mathbb{Z}, \quad \mathrm{pgcd}(\frac{N}{d}, \frac{N}{e}) t = \dot{0} \} \tag{18}$$

$$= \{ t \in \mathbb{Z}/N\mathbb{Z}, \quad \frac{N}{\mathrm{ppcm}(d, e)} t = \dot{0} \} \tag{19}$$

$$= \langle \widehat{\mathrm{ppcm}(d, e)} \rangle \tag{20}$$

C'est là où le Théorème 1 intervient :

$$\mathrm{ppcm}(d, e) = \mathrm{ppcm}\left(\mathrm{pgcd}(x, N), \mathrm{pgcd}(y, N)\right) = \mathrm{pgcd}(\mathrm{ppcm}(x, y), N) \tag{21}$$

et on peut donc conclure

$$\langle \widehat{\mathrm{ppcm}(d, e)} \rangle = \langle \widehat{\mathrm{pgcd}(\mathrm{ppcm}(x, y), N)} \rangle = \langle \widehat{\mathrm{ppcm}(x, y)} \rangle \tag{22}$$

□

Notez bien que la formule du Théorème :

$$\langle \dot{x} \rangle \cap \langle \dot{y} \rangle = \left\langle \widehat{\mathrm{ppcm}(x, y)} \right\rangle \tag{23}$$

est relativement triviale si x et y divisent N, mais comme on le vient de voir semble essentiellement équivalente au Théorème 1 en général. Si vous trouvez une démonstration directe de cette formule, cela donnera sûrement une autre preuve du Théorème 1.

Je vais maintenant utiliser d'une autre façon les groupes du type $\mathbb{Z}/N\mathbb{Z}$ pour aboutir à une nouvelle preuve du Théorème 1. Je rappelle qu'il dit

$$\operatorname{pgcd}\big(\operatorname{ppcm}(A,B),C\big) = \operatorname{ppcm}\big(\operatorname{pgcd}(A,C),\operatorname{pgcd}(B,C)\big) \tag{24}$$

Dans la preuve précédente il est intervenu dans un contexte avec $\mathbb{Z}/C\mathbb{Z}$. Maintenant on va plutôt travailler avec $\mathbb{Z}/A\mathbb{Z}$ et $\mathbb{Z}/B\mathbb{Z}$.

L'idée est la suivante. À nouveau, $A, B, C > 0$. Par un raisonnement déjà fait dans la preuve ci-dessus, on sait que :

$$\{t \in \mathbb{Z}/A\mathbb{Z}, \quad Ct = \dot{0}\} = \{t \in \mathbb{Z}/A\mathbb{Z}, \quad \forall k,l \in \mathbb{Z} \quad (kC + lA)t = \dot{0}\} \tag{25}$$

$$= \{t \in \mathbb{Z}/A\mathbb{Z}, \quad \operatorname{pgcd}(A,C)t = \dot{0}\} \tag{26}$$

$$= \left\{\dot{0}, \dot{u}, \dot{2u}, \dots, \overbrace{\dot{A-u}}\right\} \qquad u = \frac{A}{\operatorname{pgcd}(A,C)} \tag{27}$$

et par conséquent

$$\operatorname{pgcd}(A,C) = \#\{t \in \mathbb{Z}/A\mathbb{Z}, \quad Ct = \dot{0}\} \tag{28}$$

Considérons maintenant le morphisme de groupes (additifs) :

$$\begin{aligned} \psi \ : \quad \mathbb{Z}/\operatorname{ppcm}(A,B)\mathbb{Z} &\longrightarrow \mathbb{Z}/A\mathbb{Z} \times \mathbb{Z}/B\mathbb{Z} \\ n \bmod \operatorname{ppcm}(A,B) &\longmapsto (n \bmod A, n \bmod B) \end{aligned} \tag{29}$$

Il est injectif. Soit respectivement $\mathscr{H}, \mathscr{G}_A, \mathscr{G}_B$ les sous-groupes des solutions des équations $Cx = \dot{0}$ dans ces groupes additifs, c'est-à-dire les sous-groupes des éléments qui sont d'ordre un diviseur de C. Ce sont tous des groupes cycliques (voir la description plus générale plus haut, et se rappeler aussi que tout sous-groupe d'un groupe cyclique est cyclique), dont on connaît les cardinalités par des équations du type (28).

Le morphisme ψ se restreint en une injection de $\mathscr{H}$ vers le produit cartésien $\mathscr{G}_A \times \mathscr{G}_B$. Soit $\dot{x}$ un générateur du groupe cyclique $\mathscr{H}$[1]. L'ordre de x est $\#\mathscr{H}$ mais il est aussi l'ordre de $\psi(x) = (x_1, x_2)$. Donc il est égal au PPCM des ordres de $x_1 \in \mathscr{G}_A$ et de $x_2 \in \mathscr{G}_B$. Et chacun divise la cardinalité du groupe ambiant. Conclusion :

$$\#\mathscr{H} \,|\, \operatorname{ppcm}(\#\mathscr{G}_A, \#\mathscr{G}_B) \tag{30}$$

Mais ceci dit exactement :

$$\operatorname{pgcd}\big(\operatorname{ppcm}(A,B),C\big) \ \text{ divise } \ \operatorname{ppcm}\big(\operatorname{pgcd}(A,C),\operatorname{pgcd}(B,C)\big) \tag{31}$$

Or la divisibilité opposée est la « partie facile ». Donc le Théorème 1 est à nouveau démontré. Je m'arrête car il n'y a plus de place sur cette feuille.

1. On peut prendre $x = \operatorname{ppcm}(A,B)/\operatorname{pgcd}(\operatorname{ppcm}(A,B),C)$.