PGCD – PPCM ; Equations diophantiennes

La notion de PGCD (Plus grand commun diviseur) a déjà été entrevue en collège, en classe de 3ème. Elle sera largement poursuivie cette année avec l'étude approfondie de ses propriétés, l'étude de la méthode générale pour trouver le PGCD de 2 nombres, figurant dans les *Eléments* du fameux gai luron Euclide ; et son application à la résolution d'équations du type $ax + by = c$.

Remarque : Dans tout le chapitre, sauf indication contraire on considèrera les diviseurs positifs communs à deux nombres entiers positifs.

1. Diviseurs communs à deux entiers naturels – PGCD

a. Définition

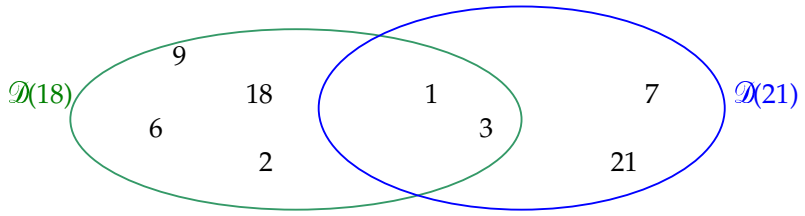
Avant tout, précisons que la notation généralement admise pour désigner « l'ensemble des diviseurs positifs de a » est $\mathcal{D}(a)$.
Faisons une petite remarque au passage : quel que soit a positif, $\mathcal{D}(a)$ = {diviseurs de a} = {1 ; … ; a}.
Tous les diviseurs de a sont compris entre 1 et a. Ce qui revient à dire, comme au chapitre précédent, qu'un diviseur (au sens large) de a est toujours plus petit que a.
Remarque fantastique : a possède aussi des diviseurs négatifs, qui sont les opposés de tous les diviseurs positifs de a.

En ce qui concerne l'ensemble des diviseurs communs à deux nombres a et b, noté $\mathcal{D}(a,b)$; il représente l'ensemble des nombres qui divisent à la fois a et b ; ou encore, en d'autres termes :

$$\mathcal{D}(a,b) = \mathcal{D}(b,a) = \mathcal{D}(a) \cap \mathcal{D}(b)$$

Le plus grand des diviseurs communs à deux nombres a et b est donc leur PGCD, que l'on note dans la pratique PGCD(a ; b) ou plus souvent $a \wedge b$.

Pour donner de tout cela une image ensembliste et plus concrète :



Les diviseurs communs à 18 et 21, ou encore les éléments de $\mathcal{D}(18) \cap \mathcal{D}(21)$, sont 1 et 3. Le plus grand de ces deux éléments est 3 : c'est donc lui le PGCD de ces deux nombres.

b. Premières propriétés

P1 **L'ensemble des diviseurs communs entre c et 0 est égal à l'ensemble des diviseurs de c :**

$$\mathcal{D}(c\ ;\ 0) = \mathcal{D}(c)$$

La « démonstration » est très simple : elle tient simplement dans le fait que 0 est un multiple de tous les nombres.

P2 **Si $b \mid a$, alors b = PGCD(a ; b).**

Si $b \mid a$, alors $b \in \mathcal{D}(a)$. Or, bien sûr, $b \in \mathcal{D}(b)$ et c'est le plus grand « diviseur » de b. D'où la propriété.

P_3 Soit $b < a$. L'ensemble des diviseurs de a et b est égal à l'ensemble des diviseurs de b et $a - b$.

$$\mathcal{D}(a,b) = \mathcal{D}(b, a-b)$$

Autre formulation (en Français) : l'ensemble des diviseurs communs de deux nombres est égal à l'ensemble des diviseurs communs du plus petit et de la différence des deux nombres.

Détail navrant : au début de l'année, chercher la démonstration est la première occasion de voir combien aspirine et arithmétique sont des éléments inséparables dans la quête du bonheur. Dans un grand élan de bonté, je vous propose donc la preuve ci-dessous (les non-tricheurs peuvent se creuser la tête un peu avant de regarder) :
On doit ici démontrer l'égalité de deux ensembles. Le procédé général est de démontrer une « double inclusion » : chaque élément de l'un est contenu dans l'autre ; et réciproquement, chaque élément de l'autre est contenu dans l'un. Les deux ensembles sont alors bien *identiquement les mêmes*.

• Première étape : soit $d \in \mathcal{D}(a,b)$. On cherche à prouver que d appartient alors aussi à $\mathcal{D}(b, a-b)$.

$$d \in \mathcal{D}(a,b) \Rightarrow \begin{cases} d \mid a \Leftrightarrow a = dk \\ d \mid b \Leftrightarrow b = dk' \end{cases}$$

Donc $a - b = dk - dk' = d\,(k - k')$: $a - b$ est multiple de d.
Par conséquent, $d \mid a - b$. Or, nous avions bien posé au début que $d \mid b$! Donc d divise b et $(a - b)$: on a bien démontré que $d \in \mathcal{D}(a,b) \Rightarrow d \in \mathcal{D}(b, a-b)$, c'est-à-dire que $\mathcal{D}(a,b) \subset \mathcal{D}(b, a-b)$. **($R_1$)**

• Deuxième étape : reste à faire la même chose dans l'autre sens !

$$d \in \mathcal{D}(b, a-b) \Rightarrow \begin{cases} d \mid a - b \Leftrightarrow a - b = dk \\ d \mid b \Leftrightarrow b = dk' \end{cases}$$

Donc $a = dk + dk' = d(k + k')$: d divise a.
Or on sait aussi, par hypothèse, que d divise b. Donc $d \in \mathcal{D}(a,b)$.
On a bien démontré que $d \in \mathcal{D}(b, a-b) \Rightarrow d \in \mathcal{D}(a,b)$, c'est-à-dire que $\mathcal{D}(b, a-b) \subset \mathcal{D}(a,b)$. **($R_2$)**

• Troisième étape : conclusion !
En rassemblant les propriétés **(R_1)** et **(R_2)**, on déduit immédiatement que $\mathcal{D}(a,b) = \mathcal{D}(b, a-b)$.

C'est à peu près les seules propriétés que l'on peut lister pour l'instant, mais l'important jusqu'ici est surtout de retenir le procédé de démonstration par double inclusion.

2. Recherche du PGCD : l'algorithme d'Euclide

C'est ici que les réjouissances commencent véritablement ! En troisième, plusieurs méthodes pour trouver le PGCD de deux nombres ont été étudiées : décomposition en produit de facteurs premiers, algorithme des différences… et bien sûr algorithme d'Euclide ! Cette dernière méthode est désormais la seule à être employée. Commençons par la décortiquer et la démontrer dans le cas général (sinon c'est un peu lâche, n'est-ce pas ?)

a. Petit résultat utile

Avant tout, une petite aide qui nous servira très bientôt :
Soit $a = bq + r$, avec $0 \leq r < b$. Si d divise a et b, alors il divise aussi leur reste dans la division euclidienne de a par b. Autrement dit,

Si $a = bq + r$, alors $\mathcal{D}(a,b) = \mathcal{D}(b,r)$.

En effet, $a = bq + r \Rightarrow r = a - bq$, ce qui est une combinaison linéaire de a et b. Donc la propriété est démontrée : si d divise a et b, il divise r en tant que combinaison linéaire de ces deux nombres.
On va en sentir l'importance pas plus loin que tout de suite.

b. Algorithme d'Euclide

On cherche à déterminer le PGCD de deux nombres entiers positifs a et b.

- Si $b \mid a$, alors PGCD $(a,b) = b$. (évident)
- Si b ne divise pas a, la recherche du PGCD s'effectue par l'algorithme d'Euclide.

On peut établir la division euclidienne de a par b : $a = bq + r$ avec $0 \leq r < b$.
Selon le résultat du paragraphe a. , la recherche de $\mathcal{D}(a,b)$ équivaut à la recherche de $\mathcal{D}(b,r)$. Quel intérêt à cela ? Un intérêt considérable puisque (b,r) est un couple strictement plus petit que (a,b). En effet, $b < a$; et $r < b$.
Or, nous avons pris pour postulat de départ que b ne divise pas a. Ainsi, le reste r dans la division euclidienne de a par b est forcément non nul. On va donc pouvoir réitérer le processus autant de fois que nécessaire, et former une « boucle » à la façon de celle que l'on peut créer en programmation (QBasic, C++, etc.)

Détail de la « boucle » :

• Je cherche le PGCD de a et b. Ce nombre, que l'on notera g, appartient forcément à $\mathcal{D}(a,b)$. Or, justement, $\mathcal{D}(a,b) = \mathcal{D}(b,r)$. J'ai tout intérêt à chercher dans $\mathcal{D}(b,r)$ plutôt que $\mathcal{D}(a,b)$, car le couple (b,r) est plus petit. J'effectue donc la division de a par b : $a = bq + r$ avec $0 \leq r < b$.
• Je recommence : $\mathcal{D}(b,r) = \mathcal{D}(r,r_1)$, où r_1 est le reste dans la division de b par r. De même qu'auparavant, (r,r_1) est un couple plus petit. Donc j'effectue la division : $b = rq' + r_1$.
• Une nouvelle fois, j'utilise la propriété : $\mathcal{D}(r,r_1) = \mathcal{D}(r_1,r_2)$, où r_2 est le reste dans la division de r par r_1. J'effectue la division : $r = r_1q'' + r_2$.
• On poursuit de cette façon : $\mathcal{D}(a,b) = \mathcal{D}(b,r) = \mathcal{D}(r,r_1) = \mathcal{D}(r_1,r_2) = \ldots$ On continue autant de fois que nécessaire.

Justement, combien de fois sont nécessaires ? On peut continuer tant qu'on ne trouve pas un reste r_k nul. Lorsque ce sera le cas, il faudra forcément cesser l'algorithme : on ne pourra pas effectuer de division par ce nombre au « tour » d'après (comment diviser ensuite par $r_k = 0$?).
Pourtant, il est sûr et certain que l'on finira par aboutir, à un moment donné, à un reste nul. Pour une raison simple : les restes r, r_1, r_2… sont des entiers positifs qui vont en décroissant strictement. On arrive, après un certain nombre d'itérations, à ceci :

$$\mathcal{D}(a,b) = \mathcal{D}(b,r) = \mathcal{D}(r,r_1) = \mathcal{D}(r_1,r_2) = \ldots = \mathcal{D}(r_k,0)$$

Or $\mathcal{D}(r_k,0) = \mathcal{D}(r_k)$.
Donc, au final, $\mathcal{D}(a,b) = \mathcal{D}(r_k)$. Cet ensemble contient le PGCD g : c'est le plus grand élément de cet ensemble. Et puisque r_k est le plus grand élément de $\mathcal{D}(r_k)$; alors r_k est le PGCD de a et b.

Conclusion : Lorsque b ne divise pas a, le PGCD de a et b est le dernier reste non nul obtenu par l'algorithme d'Euclide.

Exemple : Trouver le PGCD de 264 et 168.

$$264 = 168 \times 1 + 96$$
$$168 = 96 \times 1 + 72$$
$$96 = 72 \times 1 + 24$$
$$72 = 24 \times 3 + 0$$

Le dernier reste non nul est 24 : c'est donc le PGCD de 264 et 168.

3. Propriétés du PGCD

a. Propriété évidente

Il est bon, avant de débuter, d'avoir en tête une petite « propriété » (qui en fait n'en est pas vraiment une), conséquence directe de l'algorithme :

L'ensemble des diviseurs de a et b est aussi l'ensemble des diviseurs du PGCD : $\mathcal{D}(a,b) = \mathcal{D}(g)$.

En particulier, tous les diviseurs communs à deux nombres sont aussi des diviseurs de leur PGCD. La démonstration est immédiate : on a vu précédemment que $\mathcal{D}(a,b) = \mathcal{D}(r_k)$ et que r_k est le PGCD.

b. Caractérisation du PGCD

a, b et g sont trois entiers positifs.
On appelle caractérisation du PGCD l'équivalence de définition suivante :

$$g = \text{PGCD}(a,b) \Leftrightarrow \begin{cases} g|a \ \ et \ \ g|b \\ \dfrac{a}{g} \wedge \dfrac{b}{g} = 1 \end{cases} \Leftrightarrow \begin{cases} g|a \ \ et \ \ g|b \\ \exists_v^u \ / \ ua + vb = g \end{cases}$$

(I) **(II)** **(III)**

Démonstration :
On procédera en trois étapes (I) $\Rightarrow$ (II) ; (II) $\Rightarrow$ (III) ; (III) $\Rightarrow$ (I).
Remarque : la compréhension de la deuxième étape nécessite d'avoir vu le théorème de Bézout un peu plus loin… Un rapide coup d'œil en page 6 suffira.

• Prouvons que (I) implique (II).
Hypothèse de départ : g = PGCD (a,b). Donc g divise forcément les deux nombres a et b.
$a' = \dfrac{a}{g}$ et $b' = \dfrac{b}{g}$ sont deux entiers positifs. Il ne reste « plus qu'à » prouver qu'ils sont premiers entre eux. Pour cela ; supposons que d soit un diviseur commun à a' et b'. Alors $a' = dp$ et $b' = dq$. D'où $a = dgp$ et $b = dgq$. On observe alors que dg est un diviseur commun à a et b. Or nous avons une restriction importante : g, de par son statut de PGCD, est le plus grand diviseur commun à a et b ! Donc $dg \leq g$. Et ceci n'est possible que si $d = 1$.
En résumé, le seul diviseur commun à a' et b' est 1 : on a bien démontré la première implication.

• Prouvons que (II) implique (III).
Hypothèse de départ : g est un diviseur de a et b ; et de plus, a' et b' sont premiers entre eux. On peut donc écrire, selon le théorème de Bézout, que $ua' + vb' = 1$; pour u et v relatifs.
On a alors immédiatement la propriété $ua + vb = g$ en multipliant par g chaque terme de l'équation.

• Prouvons enfin que (III) implique (I).
Hypothèse de départ : g divise a et b et il existe deux entiers relatifs u et v tels que $ua + bv = g$.
On note g' le PGCD de a et b. Le but est de montrer que $g' = g$. Puisque g divise a et b il divise aussi leur PGCD g'.
Mais g' divise aussi a et b, donc il divise toute combinaison linéaire entre ces deux nombres : $g' \mid (ua+vb)=g$
On rappelle que le système $\begin{cases} g'|g \\ g|g' \end{cases}$ implique obligatoirement que $g' = g$: nous pouvons être heureux, la démonstration est donc terminée !

c. Propriété multiplicative du PGCD

Le PGCD est compatible avec la multiplication :
Si g est le PGCD de deux entiers naturels a et b, alors quel que soit l'entier naturel c ; gc est le PCGD de ac et bc.

Démonstration :
D'après la propriété énoncée plus haut, g = PGCD (a,b) $\Rightarrow \exists_v^u \ / \ ua + vb = g$; et g divise a et b.
Donc en multipliant les deux membres de l'égalité par c, on obtient : $uac + vbc = gc$.
Ce qui entraîne que gc = PGCD (ac,bc).

4. Plus petit commun multiple : PPCM

a. Définition

a et b sont deux entiers naturels. Ils ont forcément toujours des multiples communs. En particulier, ab en est un. Le plus petit multiple commun à a et b est leur PPCM (comme son nom l'indique…).

b. Relation avec le PGCD

PPCM et PGCD sont liés entre eux par une relation très simple qui était autrefois très utilisée au baccalauréat, mais beaucoup moins aujourd'hui. Elle reste néanmoins à savoir.

Si g est le PGCD de a et b, et m leur PPCM ; alors :

- **Tout multiple commun à a et b est un multiple du PPCM.**
- $mg = ab \Leftrightarrow m = \dfrac{ag}{b}$

Maintenant, démontrons-le : c'est là que les hostilités commencent. (on pourra au préalable regarder le théorème de Gauss en page 8…)

g = PGCD $(a,b) \Rightarrow \begin{matrix} g \mid a \Rightarrow a = a'g \\ g \mid b \Rightarrow b = b'g \end{matrix}$ avec a' et b' premiers entre eux.

Considérons l'ensemble des multiples communs à a et b ; et soit M l'un quelconque de ces multiples.

Alors, $M = ap = bq \Leftrightarrow a'gp = b'gq \Leftrightarrow a'p = b'q \Leftrightarrow a' \mid b'q$. (avec p et q entiers, bien sûr)

Or, a' et b' premiers entre eux, donc d'après le théorème de Gauss, $a' \mid q$; ou encore, $q = a'k$.

Donc $M = bq = b \times a'k = b'g \times a'k = ga'b'k$. On obtient un résultat tout à fait fantastique (si si !), qui consiste à dire que tout multiple commun à a et b peut s'écrire sous la forme $M = ga'b'k$.

Démontrons également que tout nombre M s'écrivant sous la forme $M = ga'b'k$ est un multiple de a et b. Il suffit de regrouper astucieusement les différents facteurs dans l'expression de M :

$M = ga'b'k = k(ga')b' = kab'$.

Les multiples communs à a et b sont donc les multiples de $ga'b'$. Le plus petit de tous est donc $ga'b'$… qui est par conséquent le PPCM !

Alors, $mg = ga'gb' = ab$. On vérifie bien que tout multiple de a est multiple de m.

c. Caractérisation du PPCM

De façon analogue au PGCD, le PPCM possède aussi une propriété caractéristique :

$$m = \text{PPCM}(a,b) \Leftrightarrow \begin{cases} m \text{ multiple de } a \text{ et } b & (P_1) \\ \dfrac{m}{a} \text{ et } \dfrac{m}{b} \text{ sont premiers entre eux} & (P_2) \end{cases}$$

Puisqu'elle est assez divertissante, n'oublions pas la démonstration. Comme d'habitude, on procèdera « dans un sens puis l'autre ».

• Commençons par le sens « $\Rightarrow$ ». Le postulat de départ est donc : m = PPCM (a,b) ; et le but est alors de retrouver **(P_1)** et **(P_2).** Comme **(P_1)** ne nécessite pas de démonstration, occupons-nous directement de **(P_2).**

Nous avons vu, auparavant (reprendre la démonstration du b.), que pour tout multiple m de a et b, et avec $g = a \wedge b$; on avait $m = a'b'g$ avec a' et b' premiers entre eux. Or $\begin{cases} a = a'g \\ b = b'g \end{cases} \Rightarrow m = a'b = ab'$.

Donc $\dfrac{m}{a} = b'$; $\dfrac{m}{b} = a'$. Et de plus, $a' \wedge b' = 1 \Rightarrow \dfrac{m}{a} \wedge \dfrac{m}{b} = 1$. CQFD.

• Démontrons maintenant la propriété dans l'autre sens, « $\Leftarrow$ ». Le postulat de départ est alors : M est un multiple commun à a et b tel que $\frac{M}{a} \wedge \frac{M}{b} = 1$. Le but est ici de montrer que M est alors égal au PPCM de a et b, c'est-à-dire $M = m$.

De même que ci-dessus, on utilise le fait que $M = a'b'gk$; avec $a' = \frac{a}{g}$; $b' = \frac{b}{g}$; et $g = a \wedge b$.

On en déduit immédiatement les deux égalités suivantes : $(R_1)\ \frac{M}{a} = b'k$; $(R_2)\ \frac{M}{b} = a'k$. De là, on peut affirmer que $k \left| \frac{M}{a} \right.$ et $k \left| \frac{M}{b} \right.$.

A ce stade, un suppose l'existence d'un diviseur d diviseur à $\frac{M}{a}$ et $\frac{M}{b}$. On sait, par hypothèse, que ces deux nombres sont premiers entre eux. Donc tout diviseur commun d est égal à 1.
Or k est bien un diviseur commun. Donc $k = 1$; et $M = a'b'gk = a'b'g = m$. CQFD aussi !

5. Théorème de Bézout (joie !)

a. Petit historique

Etienne Bézout (1730 – 1783) fut un génie assez précoce puisqu'à 19 ans il était déjà adjoint de l'Académie des sciences ! Sa plus grande œuvre, *Théorie générale des équations algébriques*, un traité clair et détaillé, témoigne de sa pédagogie et de sa volonté de rendre parfaitement accessible ses découvertes. Toutes les publications de Bézout (dont aussi un Cours de mathématiques en 5 volumes) restèrent très usitées pendant tout le XIX^{ème} siècle.
Bézout fit aussi une brillante carrière dans la marine royale, et fut chargé de l'enseignement des élèves du corps d'artillerie. Son *Cours de mathématiques à l'usage de l'artillerie* fit autorité très longtemps encore après sa mort.

b. Rappel : nombres premiers entre eux

On rappelle que deux nombres entiers positifs sont premiers entre eux si et seulement s'ils ne possèdent aucun diviseur commun (autre que 1, bien sûr !). Ce qui revient à dire que leur PGCD est 1. Par exemple, 9 et 25 sont premiers entre eux.
Dans $\mathbb{Z}$, cela ne change pas grand-chose : puisque 1 et –1 y divisent tous les nombres, deux nombres sont premiers entre eux si et seulement s'ils ne possèdent pas d'autres diviseurs communs que ces deux-là.

c. Le théorème tant attendu (et sa succulente démonstration)

Voici donc ce qu'énonça Etienne à propos des nombres premiers entre eux :
Deux nombres positifs a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $ua + vb = 1$.

Démonstration :
Avant de poursuivre, deux avertissements. L'un d'ordre théorique : la démonstration ci-dessous n'est pas réellement exigible, et encore moins à connaître par cœur. Il est juste intéressant de la suivre parfaitement et activement au moins une fois, pour continuer de se familiariser aux raisonnements et aux outils propres à l'arithmétique. Second avertissement, d'ordre pratique : il est conseillé de faire une pause, un goûter, une sieste, ou toute autre activité de détente avant de continuer !

Comme d'habitude, pour démontrer une équivalence, on démontre la propriété « dans un sens puis dans l'autre ».

• Commençons par supposer qu'il existe u et v tels que $ua + vb = 1$, et prouvons alors que a et b sont premiers entre eux.
Soit d tel que $d \mid a$ et $d \mid b$. Alors d divise toute combinaison linéaire entre ces deux nombres : $d \mid ua+vb$. Or, nous avons supposé que $ua + vb = 1$.
Donc $d \mid 1$. Et des nombres qui divisent 1, il n'y en a qu'un… lui-même. Donc $d = 1$, il n'y a aucune autre possibilité que celle-ci.
Ainsi, à part 1, il n'existe aucun autre nombre d qui divise à la fois a et b ! Par conséquent, a et b sont bien premiers entre eux.

• Plus délicate est la seconde mission. Posons que a et b sont premiers entre eux et démontrons qu'alors, forcément, $1 = ua + vb$.
Soit E l'ensemble des nombres de la forme $ua + vb$; avec évidemment u et v entiers relatifs. Alors on peut dire que $E \neq \emptyset$; car il contient au moins a. En effet, pour $u = 1$ et $v = 0$; $ua + vb = a$.
E contient donc des entiers positifs. Parmi eux, il en existe un plus petit que tous les autres, que l'on notera $m = au_1 + bv_1$.
Le but est désormais de montrer que $m \mid a$ et $m \mid b$. Tout simplement car alors m sera forcément égal 1 (seul diviseur commun à a et b), et on arriverait finalement à $1 = au_1 + bv_1$; et, joie, c'est précisément ce que l'on veut.
Pour cela, effectuons la division de a par m. Cela donne : $a = mq + r$ avec $0 \leq r < m$.
Donc $a = (au_1 + bv_1)q + r$; d'où $r = a(1 - u_1q) + b(-v_1q) = aU + bV$ avec U et V entiers relatifs.
Donc r appartient à son tour à E ! Or, on a bien posé au départ que $0 \leq r < m$.
r est donc plus petit que le plus petit élément de E ! Il n'a alors qu'un seul choix : être égal à 0. Le reste dans la division de a par m est nul : $m \mid a$.
On démontrerait de la même façon que $m \mid b$. Tout va bien : $m \mid a$ et $m \mid b$. Comme on l'a expliqué plus haut, cela suffit pour achever la démonstration.

• Ainsi, la démonstration s'est bien effectuée « dans les deux sens » : l'implication est prouvée, et le théorème de Bézout est démontré sans encombres (mais éventuellement avec une légère et passagère migraine).

6. Théorème de Gauss

a. La vie d'un vilain Gauss

Carl Friedrich Gauss (1777- 1855) fut un mathématicien, astronome et physicien allemand. Il n'existe pas un seul domaine scientifique qu'il n'ait pas abordé, et on lui doit, entre autres, des travaux sur les polygones réguliers, sur les nombres complexes, le magnétisme, l'algèbre, et bien sûr, l'arithmétique ! Il inventa également la méthode dite des « moindres carrés » pour l'astronomie. De plus, comme tout génie, il s'impliqua aussi dans les affaires politiques de son temps.
Tout cela n'empêchait pas le personnage d'être truculent : un grand nombre d'anecdotes amusantes courent sur lui. Dès sa prime enfance, le petit Gauss témoigne d'un goût prononcé pour la torture, qui s'exerce tout d'abord envers ses pauvres professeurs. Ces derniers étaient littéralement martyrisés et découragés par les facultés de calculateur prodige du gamin, qui avait pour habitude de finir leurs calculs et autres problèmes sans crayon, et presque avant qu'ils aient fini de les énoncer. De nos jours, une tradition fait que les professeurs d'aujourd'hui vengent ceux d'hier et donnent des maux de tête aux pauvres Terminales S, en leur faisant étudier les bêtises du gars Gauss : la boucle est ainsi bouclée, non sans ironie.
Toujours est-il que Gauss avait une affinité incroyable avec les nombres, et trouva moult combines et méthodes pour simplifier de façon considérable calculs et problèmes les plus nébuleux. A l'âge de cinq ou six ans, sur demande de son professeur, il calcule presque immédiatement, grâce à une ruse de sioux qu'il trouva de tête, la somme des cent premiers nombres ($1 + 2 + 3 + \ldots + 99 + 100$). Il regroupa simplement et instinctivement les nombres de cette façon :

$(1 + 2 + 3 + \ldots + 99 + 100) = (1 + 100) + (2 + 99) + (3 + 98) + \ldots + (50 + 51) = 50 \times 101 = 5050$.
Plutôt impressionnant pour un si jeune écolier…
Avec l'étude du théorème qui suit, vous aurez une plus ample idée du vieux Carl, bonhomme pittoresque s'il en est.

b. Son théorème fabuleux

Théorème de Gauss : soient *a*, *b*, *c* trois entiers naturels.
Si $a \mid bc$, et si *a* est premier avec *b* ; alors $a \mid c$.

Remarques : l'élève sérieux (le lecteur se reconnaîtra sûrement…) s'abstiendra d'oublier l'hypothèse « *a* et *b* premiers entre eux ». Il saura aussi que la réciproque du théorème est fausse.

Une rapide démonstration, beaucoup moins tordue que celle de Bézout :

- $a \mid bc \Leftrightarrow bc = aq$
- $a \wedge b = 1 \Leftrightarrow ua + vb = 1$; pour *u* et *v* entiers relatifs.
  Donc, en multipliant membre à membre l'égalité précédente par *c* :
  $uac + vbc = c$
  $uac + vaq = c$
  $a \times \underbrace{(uc + vq)}_{\in Z} = c \Rightarrow a \mid c$. CQFD

Ou encore, on peut dire que $a \mid auc$; et $a \mid vbc = vaq$
Par conséquent, *a* divise toute combinaison linéaire entre *auc* et *vaq*, en particulier leur somme : $a \mid auc + vbc \Rightarrow a \mid c\,(ua + vb)$. Or *a* et *b* premiers entre eux : on conclut en utilisant Bézout.

c. Son corollaire

Comme tout bon théorème, celui de Gauss a son corollaire ! Le voici :

Si *n* est divisible par *a* et par *b* premiers entre eux ; alors il est divisible par leur produit.

$$\left.\begin{array}{l} a \mid n \\ b \mid n \\ a \wedge b = 1 \end{array}\right\} \Rightarrow ab \mid n$$

Démonstration : *a* divise *n* donc il existe un entier *p* tel que $n = ap$. De même, *b* divise *n* donc il existe un entier *q* tel que $n = bq$.
Donc $ap = bq$. De ceci, on peut déduire que $a \mid bq$. Mais *a* et *b* sont premiers entre eux ! On utilise donc le théorème de Gauss pour affirmer que $a \mid q$.
A ce stade, c'est quasiment fini : il existe un entier *l* tel que $q = al$. Donc $n = bq = bal$.
Et enfin, $ba \mid n$.

7. Application à la résolution d'équations diophantiennes

Le titre peut faire peur, et il s'agit pourtant de la partie la plus simple du chapitre (et une des plus simples de l'année), à condition bien sûr de connaître les théorèmes précédemment énoncés.
Une équation diophantienne est une équation de la forme $ax + by = c$; d'inconnues entières *x* et *y* et dont les coefficients sont également entiers (et $ab \neq 0$). Il y a donc deux inconnues pour une seule et même équation. Le réflexe immédiat est de se dire « c'est impossible ». Tout simplement parce que depuis le collège on a appris que l'on peut résoudre n'importe quel problème algébrique du moment qu'il y a autant d'inconnues que d'équations. Une équation à une inconnue est soluble, deux équations simultanées à deux inconnues sont solubles, etc.
Pourtant, on peut parfaitement résoudre une équation à deux inconnues (sous certaines conditions). La preuve ! Essayez de résoudre ceci : $3x - y = 1$. Facile : $x = 1$ et $y = 2$ sont solutions !
Mais, si l'on n'a pas tout oublié du collège, on pourra objecter que nous n'avons pas résolu

l'équation à proprement parler. Car, qu'est-ce que résoudre une équation ? C'est trouver *toutes* les solutions vérifiant la relation demandée ! Lorsqu'on a une équation de la forme $ax + b = 0$; ou un système de deux équations à deux inconnues, il existe au plus une unique solution (un système est l'intersection de deux droites, et Euclide a brillamment eu l'intuition qu'il n'y avait pas plus d'un point de jonction possible). Mais ici, il existe bigrement plus qu'une solution !
Si on reprend l'exemple $3x - y = 1$; on a certes $(x\ ;\ y) = (1\ ;\ 2)$ comme couple solution. Mais on a également $x = 0$ et $y = 2$; $x = 3$ et $y = 8$; $x = 120$ et $y = 359$… Bref, vous l'aurez compris, on en a une infinité !
Le problème devient alors épineux, lorsqu'il s'agit de *résoudre* cette équation ! On se doit d'en trouver *tous* les couples solutions appartenant à $(\mathbb{Z}\times\mathbb{Z})$… mais s'il y en a une infinité, comment peut-on faire ? Puisqu'on ne pourra pas toutes les écrire, il faudra trouver une autre astuce. Tentons de « bidouiller » allégrement une équation de ce genre et voyons ce que l'on peut en tirer.

Prenons, pour changer, l'équation $8x + 5y = 1$, à résoudre dans $(\mathbb{Z}\times\mathbb{Z})$. Puisque nous ne savons pas trop quoi en faire à première vue, commençons par chercher une solution particulière.

Procédé à retenir (s'appliquant également en analyse à certaines équations différentielles) : pour résoudre certains problèmes algébriques, on cherche d'abord une solution particulière de l'équation.

Pour cela, on va utiliser l'algorithme d'Euclide ; et effectuer la division euclidienne de 8 par 5 :

$$8 = 5\times 1 + 3 \quad (L_1)$$
$$5 = 3\times 1 + 2 \quad (L_2)$$
$$3 = 2\times 1 + 1 \quad (L_3)$$

On arrive à un reste de 1 à un certain moment : c'est exactement ce que l'on recherche. On s'arrête donc ici. Pourquoi ? Car 1 est précisément le second membre de l'équation à résoudre. L'idée est alors de « remonter » dans l'algorithme.

$$(L_3):\quad 1 = 3 - 2\times 1$$
$$(L_2):\quad 1 = 3 - (5 - 3\times 1)\times 1 = 3\times 2 - 5$$
$$(L_1):\quad 1 = (8 - 5\times 1)\times 2 - 5 = -3\times 5 + 2\times 8$$

On obtient donc au final : $8\times 2 + 5\times(-3) = 1$. On a trouvé notre solution particulière !

Et maintenant ?... maintenant, une règle toute simple nous dit que nous pouvons retrancher membre à membre deux égalités. Ne résistons pas à la tentation, et retranchons la solution particulière, de la solution générale (classique en analyse aussi, à retenir).

$$\begin{array}{rl} 8x + 5y & = 1 \\ \underline{-\ 8\times 2 + 5\times(-3) = 1} & \\ 8(x-2) + 5(y+3) = 0 & \quad \textbf{(E}_2\textbf{)} \end{array}$$

Et ici, ô joie ! le second membre est nul. Ce qui nous arrange bien, et on ne se privera certainement pas d'arranger ainsi l'équation obtenue :

$$8(x-2) = 5(-y-3)$$

Ce n'est peut-être pas beau, mais ça va parfaitement ! Même si ça ne semble pas évident, à ce stade, le travail est quasiment terminé.
Il suffit ici d'utiliser le théorème de Gauss : on voit ici de façon évidente que 8 divise $5(-y - 3)$. Or 8 et 5 sont premiers entre eux, donc 8 divise $(-y - 3)$. Ce qui peut encore s'écrire :

$$8k = (-y - 3)$$

On en déduit une expression de y en fonction d'un paramètre k (entier relatif) : $y = -8k - 3$.
Il suffit alors de remplacer cette valeur de y dans l'équation **(E₂)** pour exprimer x en fonction du même paramètre :

$$8(x-2) + 5(-8k - 3 + 3) = 0$$

Quelques lignes de calcul nous conduisent alors au résultat recherché :

$$8(x-2)+5(-8k)=0$$
$$8x=40k+16$$
$$x=5k+2$$

On a donc établi, au total, les relations suivantes : $\begin{cases} x=5k+2 \\ y=-8k-3 \end{cases}$

Notons bien qu'il s'agit bien sûr du *même* paramètre k dans l'expression de x et dans celle de y : le but est justement d'établir un lien entre ces deux valeurs ! Si on prend deux paramètres différents, aucun lien ne sera mis en évidence.
Pour chaque valeur de k, on obtient alors un couple unique $(x\,;\,y)$, solution de l'équation diophantienne $8x + 5y = 1$.
Par exemple, pour $k = 2$, on a : $x = 12$ et $y = -19$. On vérifie aisément que $8\times(12)+5\times(-19)=1$.

Conclusion : les solutions de l'équation sont les couples d'entiers relatifs $(x\,;\,y)$ de la forme $(5k+2;-8k-3)$.

Cela demande un peu d'entraînement, c'est pourquoi vous pourrez vous amuser à résoudre les équations suivantes et à vérifier vos résultats :

- (I) : $3x + 4y = 1$
- (II) : $5x - 7y = 4$
- (III) : $5x - 8y = 2$.

Corrigés :

- L'équation (I) est très classique : il suffit d'appliquer strictement la méthode décrite dans le cours. Les couples solutions sont de la forme $(4k-1;-3k+1)$; avec k entier relatif.
- L'équation (II) est un peu plus « fine » car le second membre n'est pas égal à 1 mais à 4 ; ce qui paraît poser quelques difficultés. L'idée est de trouver d'abord une solution particulière à l'équation $5x - 7y = 1$. Par exemple, le couple $(3\,;\,2)$ est une solution. On a donc : $5\times3-7\times2=1$.
  D'où : $4(5\times3-7\times2)=4 \quad\Leftrightarrow\quad 5\times(12)-7\times(8)=4$.
  On a donc notre solution particulière de (II) : le couple (12 ; 8). On peut ensuite enchaîner sur la procédure classique :
  $$\begin{array}{rcl} 5x & - & 7y = 4 \\ \underline{-\ 5\times12} & \underline{-} & \underline{7\times8 = 4} \\ 5(x-12) & - & 7(y-8)=0 \end{array}$$
  Il ne reste plus qu'à utiliser le théorème de Gauss et à conclure !
  Solution finale : couples de la forme $(12+7k\,;\,8+5k)$.
- Pour l'équation (III), on ne donnera que la solution finale : ce sont les couples d'entiers de la forme $(8k+2\,;\,5k+1)$.

Remarque : toutes les équations diophantiennes ne sont pas solubles dans $\mathbb{Z}\times\mathbb{Z}$. On pourra se reporter aux exercices pour découvrir une condition n écessaire et suffisante pour qu'une telle équation admette des solutions.

Remerciements sincères à Gilles Costantini, Pierre Fructus
(et à tous ceux qui m'ont signalé des erreurs dans mon document, et m'ont permis de les rectifier !)