Introduction à l'arithmétique

Environ la moitié du programme de spécialité de Terminale S est constituée d'arithmétique. Réputée d'un abord difficile, cette discipline nécessitera en effet un « temps d'adaptation » avant d'en saisir les mécanismes un peu particuliers et déroutants.

Qu'est-ce que l'arithmétique ? Il s'agit de la théorie des nombres entiers, un des plus vieux domaines abordés par les mathématiques. Euclide fut le premier à donner des fondements à cette science, mais elle ne pourra prendre réellement son essor qu'avec l'arrivée du système de numérotation arabe : Euclide représentait les chiffres avec des segments de droites, ce qui n'est pas le plus adapté pour construire une « théorie des nombres ».
Considérée dès l'origine comme une excellente formation pour l'esprit humain, elle trouve aujourd'hui, en plus de cet extraordinaire entraînement à la réflexion pour ceux qui s'y intéressent, des applications beaucoup plus concrètes. Citons notamment la cryptographie, qui repose sur l'utilisation des nombres premiers.
De plus, le développement des outils et des méthodes pour résoudre des problèmes d'arithmétique le plus souvent abstraits a permis par ailleurs l'utilisation de ces outils dans des parties plus « concrètes » des mathématiques : l'arithmétique a été indiscutablement, de façon indirecte, un facteur important de l'évolution de tous les autres domaines mathématiques.

Depuis 1998, l'arithmétique occupe donc une place de choix dans le programme de spécialité en Terminale S. Les objectifs au niveau des connaissances restent somme toute modestes mais les raisonnements à mettre en œuvre dans la résolution des problèmes sont souvent décourageants au début. L'entraînement intensif et l'apprentissage rigoureux du cours et surtout de ses démonstrations constituent la seule solution pour dépasser ce stade inévitable où l'élève se sentira « perdu ». Avoir fait le choix de la spécialité mathématiques en terminale, c'est avoir fait le choix du travail mais aussi du courage. C'est un potentiel de valorisation pour son avenir qu'il convient de ne pas gâcher en menant un travail continu et approfondi dans cette matière : ce ne sera que plus apprécié par la suite.

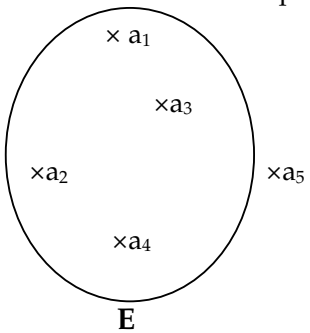
Quelques notions utiles avant d'aborder le cours à proprement parler :

1. Théorie des ensembles : généralités

L'arithmétique étudiant les nombres entiers, il sera important de bien préciser certaines propriétés que possède l'ensemble de ces nombres. Mais il est avant tout essentiel de se faire une petite idée de la notion d'ensemble en général et de voir (ou revoir) certaines propriétés et définitions.

a. Ensembles et éléments : notions essentielles

Donner une définition d'un « ensemble » au sens mathématique n'est pas le plus aisé : les encyclopédies indiquent en général qu'il s'agit d'une « collection d'éléments ayant des propriétés en commun » : ensemble des diviseurs d'un nombre, ensemble des nombres négatifs… Un exemple sera plus parlant.
Soit E un ensemble formé par 4 éléments. On peut le représenter de la façon suivante :



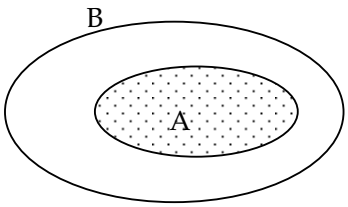
On note $E = \{a_1 ; a_2 ; a_3 ; a_4\}$

Propriété fondamentale : un élément appartient à l'ensemble, ou non (pas d'autre choix). Ici, $a_5 \notin E$. a_1, a_2, a_3, a_4 appartiennent à E.

Cette propriété peut paraître totalement inutile car triviale. Mais la facilité n'a rien à voir avec l'utilité ! On fait souvent appel à cette propriété dans des schémas démonstratifs, en raisonnant par disjonction des cas : on le verra notamment lorsqu'il s'agira de prouver le petit théorème de Fermat.

En effet, si pour démontrer une propriété, on distingue bien deux cas : $x \in E$, $x \notin E$; et que la propriété reste vraie dans les deux cas, alors elle est vraie pour tout x, il n'y pas d'autre cas à envisager. De façon tacite, c'est cette propriété évidente qui assure la cohérence et la validité de la démonstration.

Inclusion et sous ensembles : On dit que A est inclus dans B, ou encore que A est un sous ensemble de B, si tout élément de A est aussi un élément de B.



On note $A \subset B$.

Traduction mathématique de l'équivalence de définition :

$$A \subset B \Leftrightarrow \forall x \in A,\ x \in B.$$

Egalité de deux ensembles : deux ensembles sont égaux si et seulement si ils ont *identiquement les mêmes éléments*. (il ne s'agit pas d'un pléonasme mais bien de la définition rigoureuse).
Le procédé privilégié pour démontrer l'égalité de deux ensembles est donc de raisonner par double inclusion : on prouve que tout élément de l'un appartient à l'autre, et réciproquement.
Si $A \subset B$, et $B \subset A$; alors $A = B$.

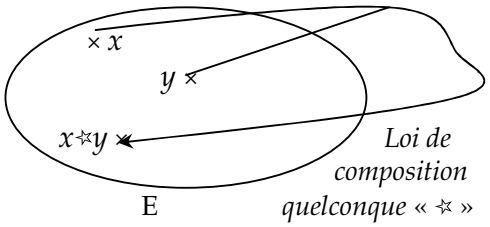
b. Produit cartésien

Soient E et F deux ensembles. Le produit cartésien E×F (lire « E croix F ») est l'ensemble des couples (x,y) tels que $x \in$ E et $y \in$ F.
Exemples : l'ensemble des couples (n_1, n_2) avec n_1 et n_2 entiers naturels correspond au produit cartésien $\mathbb{N}\times\mathbb{N}$, que l'on peut également noter $\mathbb{N}^2$.
Dans un exercice, la question « Résoudre dans $\mathbb{Z}^2$ l'équation $4x + 3y = 2$» signifie : trouver l'ensemble des couples d'entiers relatifs (x,y) tels que $4x + 3y = 2$.

2. Propriétés des ensembles de nombres

a. Loi de composition interne

On appelle loi de composition interne toute application de E×E dans E.
Une loi de composition interne dans un ensemble E, peut être schématisée de la façon suivante :



« ☆ » est en quelque sorte, ici, le symbole de la loi de composition (comme le sont ailleurs +, ou ÷, par exemple).
Une loi de composition interne « ☆ » est donc définie par :

$$T : \quad E\times E \to E$$
$$(x,y) \mapsto x\star y, \text{ qui est le composé de } x \text{ et } y \text{ appartenant à E.}$$

Exemple : dans $\mathbb{N}$, la loi d'addition (loi « + ») est une loi de composition interne. En effet, pour tout couple de nombres a et b appartenant à $\mathbb{N}$, $(a+b)$ appartient à $\mathbb{N}$.
Par contre, la loi de soustraction (loi « – ») n'est pas interne dans l'ensemble des entiers naturels. En effet, $3 - 5 = -2$; et $-2 \notin \mathbb{N}$.

Propriétés : une loi de composition interne ☆ peut être :

- *Associative :* $a \star (b \star c) = (a \star b) \star c$. Exemple : dans $\mathbb{R}$, $a + (b + c) = (a + b) + c$.
- *Commutative :* $a \star b = b \star a$. Exemple : dans $\mathbb{R}$, $a \times b = b \times a$.

- *Distributive :* on dit que l'opération $\star$ est distributive par rapport à la loi ϕ si *:*

$$x \star (y \phi z) = (x \star y) \phi (x \star z.)$$

Exemple : dans $\mathbb{R}$, la loi $\times$ est distributive par rapport à la loi + : $x \times (y + z) = (x \times y) + (x \times z)$

Eléments particuliers :

- *Elément neutre : e* est neutre si et seulement si, pour tout x, $x \star e = e \star x = x$. L'élément neutre d'une opération laisse tout x inchangé lors de cette opération. Par exemple, dans $\mathbb{R}$, 0 est l'élément neutre pour l'addition ; 1 est l'élément neutre pour la multiplication.
- *Elément symétrique* : On note toujours e l'élément neutre. Dans la loi $\star$, x' est le symétrique de x si et seulement si $x' \star x = x \star x' = e$. Par exemple, dans $\mathbb{R}$, pour l'addition, le symétrique de 8 est (-8) : 8 + (-8) = 0, l'élément neutre.

b. Loi de groupe

On dit qu'un ensemble est muni d'une structure de groupe si on a défini dans cet ensemble une loi de composition interne associative, possédant un élément neutre et dont chaque élément possède un symétrique.
Si de plus, la loi en question est commutative, le groupe est dit *Abélien* (ou commutatif).

Théorème : dans un groupe G, toute équation d'inconnue x de la forme $a + x = b$ est soluble. (a et b sont dans G)
En effet, nous n'avons pas réellement conscience des opérations que nous effectuons lorsque nous résolvons une telle équation, mais les conditions énoncées ci-dessus sont impératives. Illustration : Résoudre $x + 3 = 8$.

$x + 3 + (-3) = 8 + (-3)$: suppose l'existence d'un symétrique pour « éliminer 3 ».
$x + (3 + (-3)) = 8 + (-3)$: suppose l'existence de la propriété d'associativité.
$x + 0 = 5$
$x = 5$: suppose l'existence d'un élément neutre

3. Ensembles de nombres usuels – Historique

- L'ensemble des entiers naturels : $\mathbb{N}$

L'ensemble des entiers naturels, nombres appartenant à l'ensemble $\mathbb{N}$ = {0 ; 1 ; 2 ; 3 …}, s'est construit de façon tout à fait… « naturelle ». Ce nom qui leur a été attribué, provient du fait qu'ils remplissaient à l'origine la fonction fondamentale des mathématiques : le dénombrement d'objets. Les besoins des Hommes, dès lors que l'on vit en société, sont et doivent être quantifiés : ne serait-ce par exemple que la nourriture ! Le dénombrement des ressources est une fonction vitale pour la survie du groupe.
En cela, l'ensemble des entiers naturels ne s'est pas construit de façon mathématique mais purement empirique, lorsque l'Homme a dû quantifier et compter les éléments nécessaires à son existence. La création de ces nombres correspond aux premières structures de vie sociale et de sédentarisation : c'est la vie en groupe qui rend nécessaire le dénombrement.
Toutefois, cet ensemble ne permet alors que de sommer des quantités : la soustraction est impossible (pas d'existence de symétrique à 1 ; 2 ; …) : mathématiquement parlant, $\mathbb{N}$ n'est pas un groupe pour la loi d'addition. Il devient donc bien vite insuffisant lorsque les besoins (et le cerveau !) de l'Homme évoluent : on ne s'occupe plus que de dénombrer, mais d'établir des lois entre ces quantités dénombrables. L'ensemble des naturels ne répond pas à cette attente, c'est pour cela qu'un nouvel ensemble plus vaste et permettant plus d'opérations va être créé : l'ensemble des entiers relatifs.
La création de cet ensemble devait alors permettre, intuitivement, d'obtenir un groupe pour la loi d'addition ; autrement dit, de pouvoir additionner et soustraire toutes les quantités que l'on voudrait, ce qui était impossible dans $\mathbb{N}$.

- L'ensemble des entiers relatifs : $\mathbb{Z}$

L'anneau des entiers relatifs est obtenu en rajoutant tous les symétriques des nombres entiers naturels pour la loi d'addition (c'est-à-dire, les opposés). $\mathbb{Z}$ a bien une structure de groupe, celle que l'on recherchait précisément. Remarque : on trouvera parfois dans certains ouvrages propriété évidente : « $\mathbb{Z}+ = \mathbb{N}$ ».
Toutefois, l'ensemble des entiers relatifs n'a pas une structure de groupe pour la multiplication par exemple ! 5 n'a pas de symétrique dans $\mathbb{Z}$, $\frac{1}{5}$ n'existe pas dans cet ensemble. Il va donc falloir inventer un autre ensemble muni d'une structure de groupe pour la loi de multiplication : l'ensemble des rationnels $\mathbb{Q}$ est né.

- Construction progressive des autres ensembles de nombres

Les autres ensembles de nombres se sont construits selon cette logique : puisque l'ensemble le plus vaste connu à l'heure actuelle ne permet pas de faire telle ou telle opération alors on en invente tout simplement un autre ! Quitte à ce que cela défie la logique et se fasse de façon tout à fait artificielle : c'est le cas pour la construction de l'ensemble $\mathbb{R}$ à partir de $\mathbb{Q}$.
En effet, « $\mathbb{R} = \mathbb{Q}$ + les irrationnels », et le mot irrationnels montre bien que les mathématiques, au début si « naturels », s'éloignent désormais de ce qui existe réellement pour construire des théories plus complexes.

- Trois axiomes fondamentaux pour l'arithmétique

Trois postulats de départ évidents qui ne se démontrent pas mais doivent se comprendre parfaitement.
Axiome 1 : toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Cela est faux dans $\mathbb{Z}$.
Axiome 2 : toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
Axiome 3 : toute suite d'entiers naturels strictement décroissante est finie. Faux dans $\mathbb{Z}$ aussi.

Divisibilité dans $\mathbb{Z}$

Pour une approche « en douceur » de l'arithmétique, nous commencerons par un chapitre d'introduction concernant la relation de divisibilité entre deux entiers.
Remarque : Pour l'ensemble du cours, la dénomination « entier » devra être comprise au sens d'entier relatif, sauf indication contraire.

1. Définition de la divisibilité

a. Multiples d'un entier relatif

Soit un entier n. On dit que m est un multiple de n si, et seulement si, il existe un nombre entier quelconque k tel que $m = k \times n$.
Par exemple, les multiples de 7 sont l'ensemble des nombres s'écrivant sous la forme $7k$, c'est-à-dire $\{0 ; 7 ; 14 ; 21 ; \ldots\}$.
On remarquera au passage que 0 est alors un multiple de tous les nombres.

b. Relation de divisibilité

Soient deux entiers relatifs a et b. a divise b si et seulement si : (les propositions ci-dessous sont équivalentes)

- il existe un entier k tel que $b = ak$.
- b est un multiple de a

« a divise b » est noté $a \mid b$.

Quelques remarques bonnes à savoir pour les exercices et les démonstrations :

- 1 et -1 divisent tous les nombres.
- Un nombre a admet au minimum 4 diviseurs : $\{1 ; -1 ; a ; -a\}$.
- La relation de divisibilité est *réflexive* : a divise a.

c. Propriétés de la relation de divisibilité

Ces propriétés sont relativement simples mais il faudra porter une attention toute particulière à leurs démonstrations, qui pourront donner de bons réflexes pour les exercices.

P_1 Si b divise a, alors $-b$ divise a.
En effet, $b \mid a \Leftrightarrow \exists k \in \mathbb{Z} \ / \ a = bk$. Donc $a = \underbrace{(-k)}_{\in Z} \times (-b)$. On obtient donc bien $-b \mid a$.

P_2 Si b divise a, alors $|b| \leq |a|$ (avec $a \neq 0$)
En valeur absolue, le diviseur est plus petit que le dividende.
Démonstration : b divise a, donc $a = bk$. Ce qui implique que $|a| = |b| \times |k|$. Et comme $a \neq 0$; alors $|k| \neq 0$ et $|k| \geq 1$ puisque k est un entier. D'où la propriété.

P_3 Si $a \mid b$ et $b \mid c$; alors $a \mid c$.
La relation de divisibilité est *transitive*. En effet :
$a \mid b \Leftrightarrow \exists k \in \mathbb{Z} \ / \ b = ak$; et $b \mid c \Leftrightarrow \exists k' \in \mathbb{Z} \ / \ c = bk'$.
Donc : $c = k'b = k' \times (ak) = \underbrace{(k \times k')}_{\in Z} a \Rightarrow a \mid c$.

P_4 Si $a \mid b$ et $b \mid a$ alors $a = b$ ou $a = -b$.
Démonstration : a divise $b \Rightarrow |a| \leq |b|$ d'après P_2.
b divise $a \Rightarrow |b| \leq |a|$ d'après P_2.
$\Big\}$ $|a| = |b|$ et donc $a = \pm b$

P_5 Si $a \mid b$ et $a \mid c$ alors $a \mid ub + vc$ (avec u et v entiers)
Si a divise b et c alors il divise aussi toute combinaison linéaire entre ces deux nombres (en particulier la somme et la différence de ces nombres).

Démonstration : $\left.\begin{array}{l} a \mid b \Leftrightarrow b = ak \\ a \mid c \Leftrightarrow c = ak' \end{array}\right\}$ Alors $\begin{aligned} ub + vc &= uak + vak' \\ &= a \times \underbrace{(uk + vk')}_{\in Z}. \end{aligned}$ Et donc $a \mid ub+vc$

P_6 Si $a \mid b$ alors $a \mid bc$ pour tout entier c.
En effet, si $a \mid b$ alors il existe un entier k tel que $b = ak$. Alors $bc = (ak)c = a(kc)$ donc $a \mid bc$.

P_7 Si $a \mid b$ alors $ac \mid bc$ pour tout entier c.
Démonstration : $a \mid b \Leftrightarrow b = ak \Leftrightarrow bc = akc \Leftrightarrow bc = (ac) \times k \Leftrightarrow ac \mid bc$.

2. La division euclidienne

a. Division euclidienne dans $\mathbb{N}$

Soient a et b deux entiers positifs, avec $b \neq 0$ et $a < b$. Il existe un unique couple $(q ; r)$ d'entiers naturels tels que $\boldsymbol{a = bq + r}$ avec $\boldsymbol{0 \leq r < b}$.
Démontrons l'unicité du couple $(q ; r)$. Pour cela, utilisons un raisonnement par l'absurde (fréquent en arithmétique donc à retenir) :
Supposons qu'il existe deux couples distincts $(q ; r)$ et $(q' ; r')$. Alors nous aurions les relations suivantes :

$$a = bq + r \qquad \text{et} \qquad a = bq' + r'$$

Donc $bq + r = bq' + r'$
$\Leftrightarrow b(q - q') + (r - r') = 0$
$\Leftrightarrow b(q - q') = (r' - r)$: $(r' - r)$ est alors un multiple de b.
Or $|r' - r| < b$. Au total, on a donc un multiple de b qui est plus petit que b ! La seule valeur possible est 0. Donc $(r - r') = 0$ et par conséquent $r = r'$ et $q = q'$.
Il est donc impossible de trouver deux couples distincts $(q ; r)$ et $(q' ; r')$: on a démontré l'unicité de la décomposition de a dans la division euclidienne par b.

Effectuer la division euclidienne de a par b, c'est trouver le couple d'entiers naturels $(q ; r)$ tels que $a = bq + r$; avec $0 \leq r < b$ (et bien sûr $b \neq 0$).
$r = 0$ si et seulement si b divise a.

Remarque : on prendra bien garde à ne pas négliger la condition $0 \leq r < b$, souvent oubliée. Elle est pourtant essentielle. Par exemple, $24 = 7 \times 2 + 10$ n'est pas l'écriture de la division euclidienne de 24 par 7 : le reste est plus grand que le diviseur !

b. Division euclidienne dans $\mathbb{Z}$

Cela n'a qu'une importance toute relative (et théorique) mais peut se définir ainsi :
Pour deux entiers relatifs a et b (avec $b \neq 0$), il existe un unique couple $(q ; r)$ avec $q \in \mathbb{Z}$, $r \in \mathbb{N}$; tel que : $\boldsymbol{a = bq + r}$ avec $\boldsymbol{0 \leq r < |b|}$
Le reste est toujours un entier naturel.

c. Effectuer une division euclidienne

Même si les calculatrices en ont fait perdre l'habitude, chacun devrait être capable de poser et d'effectuer à la main une division euclidienne ; par exemple celle de 573 par 19. Car les « mécanismes » de cette division sont très utiles lorsqu'il s'agit de faire *en la posant* (donc *sans*

employer la méthode d'identification) la division d'un polynôme par un autre : par exemple la division de $3x^2-2x-8$ par $(x-2)$. Si si ! Même si cette méthode n'est plus explicitement au programme depuis fort longtemps, elle peut être employée à bon escient dans bon nombre d'exercices et est d'une efficacité redoutable. Elle se retrouve aussi en analyse, pour trouver une asymptote oblique à une courbe. Posons cette division, donc !

$3x^2-2x-8$	$x-2$
$-3x^2+6x$	$3x+4$
$4x-8$	
$-4x+8$	
0	

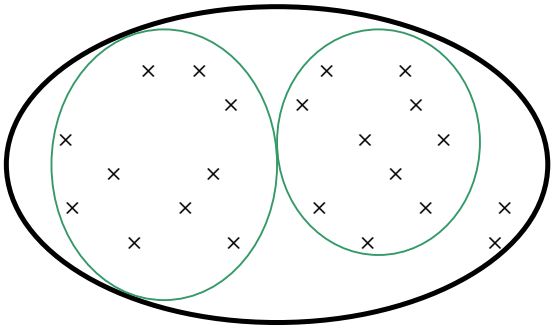
On procède à peu près comme à l'école primaire :
① « dans $3x^2$, combien de fois x ? $3x$ fois ». Je pose donc $3x$ au niveau du quotient.
② « $-2\times(3x)=-6x$ » : je place et je soustrais $3x^2$ - $2x$ et $3x^2-6x$; puis j'abaisse le 8.
③ J'obtiens $4x-8$ et je repars : « dans $4x$, combien de fois x ? 4 fois ». Je pose donc 4 au niveau du quotient.
④ C'est un morceau de chance puisque $4\times(-2)=-8$: après soustraction j'obtiens donc 0 comme reste.
Bilan : $3x^2-2x-8=(x-2)(3x+4)+0$ $\quad (a=bq+r)$

Cette méthode, lorsqu'elle est bien maîtrisée, permet un gain de temps énorme par rapport à l'identification ou au bestial calcul de delta pour le second degré ; et s'avèrera très utile en exercice.

Pour vous entraîner, vous pouvez poser la division de $2x^2+3x-4$ par $x-1$; et vérifier que le quotient est $2x+5$ et le reste 1.

3. Complément : Systèmes de numération

Notre système de numération est en base 10 : on dispose de 10 symboles pour écrire tous nos nombres. Tout nombre peut donc se décomposer en une somme de puissances de 10. Par exemple : $2549 = 2\times10^3 + 5\times10^2 + 4\times10^1 + 9\times10^0$. Cela aura, notamment dans le chapitre sur les congruences, des conséquences tout à fait remarquables.
Cela est du au fait que l'on « regroupe par paquets de 10 » comme ci-dessous :



Il y a, dans l'ensemble total, 22 objets. Pour pouvoir dire qu'il y en a « 22 », il faut les avoir regroupés au préalable en paquets de 10 : il y a deux paquets de 10 et deux unités S'il existait ici des paquets de 100, ce ne seraient en fait que des « paquets de paquets de 10», ce qui équivaut à 10^2.

Il existe d'autres systèmes de numération assez connus :

- Système binaire (ou « en base 2 ») :

Fondamental en informatique, ce système ne se compose que de deux symboles : 0 et 1 ; ce qui est très pratique pour toute l'électronique puisqu'il n'y a que deux possibilités : le courant passe ou ne passe pas. Tout nombre se décompose donc ici en « paquets de 2 » au lieu de « paquets de 10 », et donc en puissances de 2.
Pour passer du système décimal au système binaire (ou inversement), il existe plusieurs méthodes plus ou moins intéressantes.

La première est tout simplement de dresser la liste, au fur et à mesure, de l'équivalence binaire/décimal, comme ci-dessous :

Système décimal	Système binaire
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

Ici, 9 équivaut à 1001 en base 2 ; soit à $1\times2^3+0\times10^2+0\times10^1+1\times10^0$; soit encore à une unité seule et un « paquet de 2^3 ».
Toutefois, si on demandait de convertir « 43 » en écriture binaire, cela risque de prendre un certain temps… C'est pourquoi il est préférable d'utiliser une autre méthode : celle des restes successifs dans la division par 2.
On commence par diviser 43 par 2 ; puis le quotient obtenu par 2 ; puis le nouveau quotient par 2… Seuls les restes nous intéressent : en « remontant » ces restes, on obtiendra l'écriture binaire de « 43 ».
Détail du procédé :

$$43 = 2\times21+1$$
$$21 = 2\times10+1$$
$$10 = 2\times5+0$$
$$5 = 2\times2+1$$
$$2 = 2\times1+0$$
$$1 = 2\times0+1$$

On remonte ensuite les restes de bas en haut et on obtient « 101011 » : c'est l'écriture de 43 en base 2.

- Système hexadécimal :

On dispose ici de 16 symboles et on décompose selon les puissances de 16. Les chiffres s'écrivent ainsi : 0 ; 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 ; 8 ; 9 ; A ; B ; C ; D ; E ; F.
La taille démesurée des nombres en écriture binaire (voir l'exemple ci-dessus) est assez gênante pour les informaticiens, qui préfèrent souvent travailler avec une base hexadécimale, moins « encombrante ».

Un peu d'entraînement…

Voici quelques exercices qui vous permettront de vous familiariser avec les raisonnements les plus fréquemment utilisés sur cette partie de l'arithmétique ; et de mieux assimiler le cours en l'illustrant par des exemples concrets.

Exercice 1 : Le problème des changements de bases

1) Soit N = 2183 dans le système décimal. Déterminer son écriture en base 8.

2) Soit le nombre 5241, écrit dans une certaine base.

a) Peut-il être écrit en base 5 ?

b) Supposons qu'il soit écrit en base 6. Donner sa correspondance dans le système décimal.

Exercice 2 : Propriétés de la divisibilité et diviseurs communs

k est un entier naturel. Soient $a = 6k + 5$; et $b = 8k + 3$. Prouver qu'il n'existe que deux diviseurs positifs communs à a et b.

Exercice 3 : Divisibilité par un nombre

Soit un entier quelconque a. Prouver que le nombre $N = a(a^2 - 1)$ est un multiple de 6.

Exercice 4 : Questions classiques sur la divisibilité

Les trois questions sont indépendantes.

1) Soit n un entier relatif. En vérifiant que $2n + 1 = 2(n - 3) + 7$; trouver l'ensemble des entiers n tels que $(n - 3)$ divise $(2n + 1)$.

2) n est ici un entier naturel. En vérifiant que $n^2 - n + 3 = (n - 2)(n + 1) + 5$; trouver l'ensemble des entiers naturels n tels que $(n + 1)$ divise $(n^2 - n + 3)$.

3) Déterminer les valeurs de l'entier relatif n pour les quelles la fraction $\frac{3n+8}{n+4}$ peut se simplifier sous forme d'un entier relatif.

Exercice 5 : Division euclidienne

Déterminer selon les valeurs de l'entier naturel n le reste de la division euclidienne de $n^2 + 5n + 9$ par $n + 2$.

Exercice 6 : Un problème de bac

1) Démontrer que $n^2 + 5n + 4$ et $n^2 + 3n + 2$ sont divisibles par $n + 1$

2) Déterminer l'ensemble des valeurs de n pour lesquelles $3n^2 + 15n + 19$ est divisible par $n + 1$.

3) En déduire que pour tout n, $3n^2 + 15n + 19$ n'est pas divisible par $n^2 + 3n + 2$.

Exercice 7 : Une propriété de la division euclidienne

a et b sont deux entiers naturels. Dans la division euclidienne de a par b, le quotient n'est pas nul. Prouver que a est supérieur au double du reste.

Exercice 8 : Utilisation des propriétés de la divisibilité pour résoudre $x^2 - y^2 = a$

Trouver tous les couples d'entiers relatifs (x , y) tels que $x^2 - y^2 = 13$.

Exercice 9 : Un autre classique

Soit $n \in \mathbb{N}$. Démontrer que quel que soit n, $3n^4 + 5n + 1$ est impair ; puis que ce polynôme n'est jamais divisible par $n(n + 1)$.

Corrigés des exercices

Exercice 1

1) On applique simplement la méthode des divisions successives par 8 :

$2183 = 8 \times 272 + \mathbf{7}$
$272 = 8 \times 34 + \mathbf{0}$
$34 = 8 \times 4 + \mathbf{2}$
$4 = 8 \times 0 + \mathbf{4}$

N s'écrit donc 4207 en base 8.

2) a) L'écriture de ce nombre comporte le signe « 5 ». Ce nombre ne donc peut pas être écrit en base 5 puisque celle-ci ne comporte que 5 symboles : 0 ; 1 ; 2 ; 3 ; 4.

b) $5241 = 1 + 4\times6 + 2\times6^2 + 5\times6^3 = 1 + 24 + 72 + 1080 = 1177$. Ce nombre s'écrit 1177 en base 10.

Exercice 2

On doit ici faire usage de la propriété la plus importante de la divisibilité : si d divise a et b alors il divise aussi toute combinaison linéaire entre ces deux nombres.
Si l'on note d un diviseur commun de a et b, alors d doit aussi diviser toute expression de la forme $ua + vb$. Le but ici est de faire « sauter » les k. On va donc choisir $u = 4$ et $v = -3$.
On a alors : $d \mid 4\times(6k + 5) - 3\times(8k + 3)$.
Donc $d \mid 11$, après réduction. Or, 11 ne possède que deux diviseurs : 1 et 11.
Il n'existe donc bien que deux diviseurs positifs communs à a et b : 1 et 11.

Exercice 3

On n'arrivera à rien si l'on cherche à démontrer « directement » que ce nombre est multiple de 6. Il faut avoir en tête une ruse importante : un nombre est multiple de 6 si et seulement si il est à la fois multiple de 2 et de 3. On va donc démontrer successivement ces deux assertions.
Avant cela, remarquons juste que $N = a(a^2 - 1) = a(a + 1)(a - 1)$.

- Est-il multiple de 2 ? On va raisonner par disjonction des cas.

Envisageons pour commencer le cas où a est pair : a s'écrit sous la forme $2k$. On a alors : $N = 2k\times(2k+1)\times(2k-1)$. N est donc pair puisque sa décomposition en produit de facteurs comporte le facteur 2.
Envisageons ensuite le cas où a est impair ; c'est-à-dire le cas où $a = 2k + 1$. On a alors : $N = (2k+1)\times(2k+1+1)\times(2k+1-1) = (2k+1)\times(2k+2)\times2k$. Même conclusion que ci-dessus : N est donc pair.
Au total, N est donc toujours pair, quel que soit a.

- Est-il multiple de 3 ? On raisonne de la même façon.

Premier cas : a est multiple de 3, ou encore $a = 3k$. On peut déjà déduire que dans ce cas N est aussi un multiple de 3.
Deuxième cas : a n'est pas un multiple de 3 ; donc $a = 3k + 1$ ou $a = 3k + 2$. On peut vérifier, comme on l'a fait plus haut, que dans les deux cas N est un multiple de 3.
N est donc toujours un multiple de 3, et ce pour tout valeur de a.

- Conclusion : N est multiple de 2 et de 3 ; donc de 6.

Exercice 4

1) Un calcul simple prouve que $2n + 1 = 2(n - 3) + 7$. Donc dire « $(n - 3)$ divise $(2n + 1)$ » ; ou dire « $(n - 3)$ divise $2(n - 3) + 7$ » sont deux propositions équivalentes.
Cherchons donc l'ensemble des valeurs de n pour lesquelles $(n - 3)$ divise $2(n - 3) + 7$.

$(n-3)$ divise $2(n-3)+7$ si et seulement si $\frac{2(n-3)+7}{n-3}$ est un entier ; donc ssi $\frac{2(n-3)}{n-3}+\frac{7}{n-3}$ est un entier. Or $\frac{2(n-3)}{n-3}=2$: il faut juste que $\frac{7}{n-3}$ soit un nombre entier. (pour tout ce qui précède, $n \neq 3$)
Quelles sont les valeurs de n pour lesquelles cette assertion se vérifie ?
Il faut que $n-3=7$; ou $n-3=1$; ou $n-3=-1$; ou $n-3=-7$. Ce qui correspond à des valeurs de n respectivement égales à 10 ; 4 ; 2 et – 4.
L'ensemble des entiers relatifs n pour lesquels $(n-3)$ divise $(2n+1)$ est donc {– 4 ; 2 ; 4 ; 10}.

2) On va procéder de manière analogue et trouver que l'ensemble des entiers recherché est {0 ; 4}.

3) Remarquons avant tout que n doit être différent de – 4 pour que la fraction ait un sens.
Il suffit ici d'affirmer que $3n+8=3(n+4)-4$. De même qu'en **1)**, on recherche ensuite l'ensemble des entiers relatifs tels que $\frac{4}{n+4}$ soit un entier. Cela se produit pour les valeurs de n suivantes :

$$-8\ ;\ -6\ ;\ -5\ ;\ -3\ ;\ -2\ ;\ 0.$$

Exercice 5

On pose la division euclidienne :

$$\begin{array}{r|l} n^2+5n+9 & n+2 \\ \cline{2-2} -n^2-2n & n+3 \\ \cline{1-1} 3n+9 & \\ -3n-6 & \\ \cline{1-1} 3 & \end{array}$$

On en déduit que $n^2+5n+9=(n+2)(n+3)+3$

A partir de là, l'essentiel est fait. On a écrit n^2+5n+9 sous la forme $a=bq+r$; mais il faut encore que l'on ait : $0 \leq r < n+2$.
On serait en effet tenté de dire qu'ici $r=3$: c'est évident en observant l'écriture ci-dessus ! Mais attention, il faut avant cela vérifier à partir de quelle valeur de n on a effectivement $0 \leq r < n+2$!

- Si $n > 2$; $n+2 > 4 > 3$: le reste est alors bien 3.
- Si $n=1$; $n+2=3$. Or 3 n'est, bien sur, pas strictement supérieur à 3 ! Donc il nous faut calculer la valeur du reste dans ce cas précis. Pour $n=1$; $n^2+5n+9=15$ et $n+2=3$. Le reste dans la division euclidienne de 15 par 3 est 0.
- Si $n=0$; $n+2=2$. De même, il nous faut donc calculer la valeur du reste pour ce cas particulier. Pour $n=0$; $n^2+5n+9=9$ et $n+2=2$. Le reste dans la division euclidienne de 9 par 2 est 1.

Conclusion :

Valeurs de n	$n>2$	$n=1$	$n=0$
Reste dans la division de n^2+5n+9 par $n+2$	3	0	1

Exercice 6

1) En posant la division euclidienne (ou, moins malin, en calculant le delta de l'expression et en la factorisant ; ou encore en factorisant ces expressions à l'aide d'une racine évidente), on voit immédiatement que $n^2+5n+4=(n+1)(n+4)$; et que $n^2+3n+2=(n+1)(n+2)$. Par conséquent, n^2+5n+4 et n^2+3n+2 sont bien divisibles pas $(n+1)$.

2) Le mieux ici est encore de poser la division :

$$\begin{array}{r|l} 3n^2+15n+19 & n+1 \\ \cline{2-2} -3n^2-3n & 3n+12 \\ \cline{1-1} 12n+19 & \\ -12n-12 & \\ \cline{1-1} 7 & \end{array}$$

Conclusion : $3n^2+15n+19=(3n+12)(n+1)+7$

Piqûre de rappel : ensuite, comme plus haut (non non, encore plus haut) on recherche les valeurs de n pour lesquelles $\frac{7}{n+1}$ est un entier : cela se produit si $n \in \{0 ; 6\}$.

3) $n^2+3n+2 = (n+1)(n+2)$; donc si $3n^2+15n+19$ est divisible par $(n+1)(n+2)$, alors il est divisible à la fois par $(n + 1)$ et $(n + 2)$. Etant divisible par $(n + 1)$, selon **2)**, n ne peut prendre que les valeurs 0 ou 6. Observons alors ce qui se passe au niveau de la divisibilité par $(n + 2)$ pour ces valeurs de n.
Si $n = 0$; alors $3n^2+15n+19 = 19$ et ce nombre n'est pas divisible par $(n + 2)$, qui vaut 2.
Si $n = 6$; alors $3n^2+15n+19 = 217$ et $(n + 2) = 8$. Or 8 ne divise pas 217.
En fin de compte, $3n^2+15n+19$ n'est jamais divisible par n^2+3n+2.

Exercice 7

La division euclidienne de a par b est définie par : $\begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$
b et q sont non nuls et (dans cet exercice) appartiennent à $\mathbb{N}$. On en déduit que :

$$b > r \quad \text{et} \quad q > 1$$

Donc : $bq > b > r \implies bq > r \Rightarrow bq + r > 2r \Rightarrow \boldsymbol{a > 2r}$.
On a bien démontré que a est supérieur au double du reste.

Exercice 8

$x^2 - y^2 = 13 \Leftrightarrow (x + y)(x - y) = 13$
On est donc confronté à un produit de deux facteurs égal à 13. Or 13 n'est divisible que par les nombres suivants : – 13 ; – 1 ; 1 ; 13. Il n'existe donc que deux possibilités (éventuellement quatre) :

$$\begin{cases} x+y=-13 \\ x-y=-1 \end{cases} \quad \text{ou} \quad \begin{cases} x+y=13 \\ x-y=1 \end{cases}$$

$$\begin{cases} x+y=1 \\ x-y=13 \end{cases} \quad \text{ou} \quad \begin{cases} x+y=-1 \\ x-y=-13 \end{cases}$$

La résolution de ces systèmes montre qu'il n'existe que 2 couples possibles : (–7 ; –6) et (7 ;6).

Exercice 9

- Démontrons que le polynôme donné n'est jamais pair :

Comme dans l'exercice 3, raisonnons par disjonction des cas. Envisageons deux cas possibles :
Si n est pair, alors $n = 2k$. Donc $n^4 = 16k^4$ est pair. $3n^4$ est pair également, tout comme $3n^4 + 5n$. Par contre, $3n^4 + 5n + 1$ est impair.
Si n est impair, alors $n = 2k + 1$. $n^4 = (2k + 1)^4 = \underbrace{(2k)^4}_{pair} + \underbrace{4\times(2k)^3}_{pair} + \underbrace{6\times(2k)^2}_{pair} + \underbrace{4\times 2k}_{pair} + 1$. n^4 est donc impair. $3n^4$ aussi. Or $5n$ est impair et la somme de deux impairs donne un nombre pair : $3n^4 + 5n$ est donc pair. Pour finir, $3n^4 + 5n + 1$ est impair.

- On peut alors en déduire qu'il n'est jamais divisible par $n(n + 1)$:

$n(n + 1)$ est le produit de deux nombres consécutifs donc est toujours pair (facile à démontrer en envisageant n pair ou n impair, puis en concluant). Et par conséquent, il ne peut pas diviser $3n^4 + 5n + 1$ qui, quant à lui, est impair.

Remerciements à MM. Gilles Costantini et Pierre Fructus pour leur aide !

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

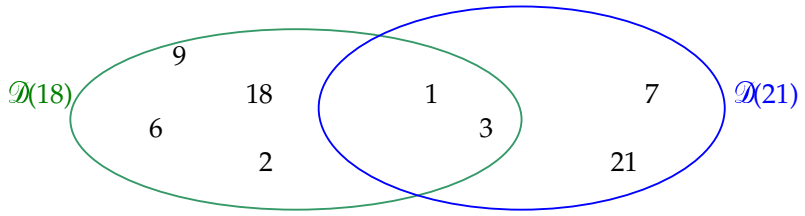
Avant tout, précisons que la notation généralement admise pour désigner « l'ensemble des diviseurs positifs de a » est $\mathcal{D}(a)$.
Faisons une petite remarque au passage : quel que soit a positif, $\mathcal{D}(a) = \{\text{diviseurs de } a\} = \{1 ; \dots ; a\}$.
Tous les diviseurs de a sont compris 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,

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

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 :

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

(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.
$a' = \frac{a}{g}$ et $b' = \frac{b}{g}$ 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, $M = ap = bq \quad \Leftrightarrow \quad a'gp = b'gq \quad \Leftrightarrow \quad a'p = b'q \quad \Leftrightarrow \quad a' \mid b'q$. (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 $\dfrac{m}{a} = b' \quad ; \quad \dfrac{m}{b} = a'$. 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).

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

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 :
  $$\begin{array}{rcl} 5x & - & 7y = 4 \\ \underline{-\ 5\times12 & - & 7\times8 = 4} \\ 5(x-12) & - & 7(y-8)=0 \end{array}$$
  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 !)