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.

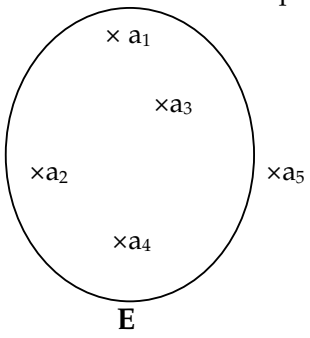
Quelques notions utiles avant d'aborder le cours à proprement parler :

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 :



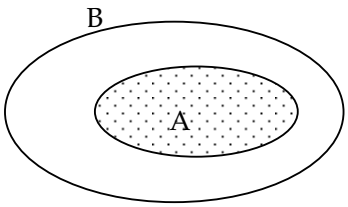
On note E = {a_1 ; a_2 ; a_3 ; a_4}

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 $A = B$.

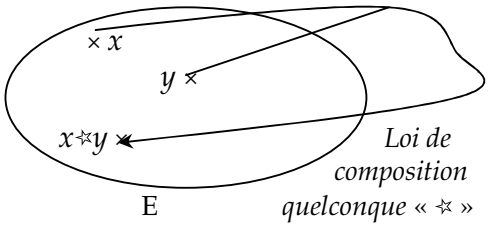
b. Produit cartésien

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 :

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

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

P5 **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 $\begin{array}{l} ub + vc = uak + vak' \\ \qquad\quad = a \times \underbrace{(uk + vk')}_{\in Z}. \end{array}$ Et donc $a \mid ub+vc$

P6 **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 $a \mid bc$.

P7 **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	

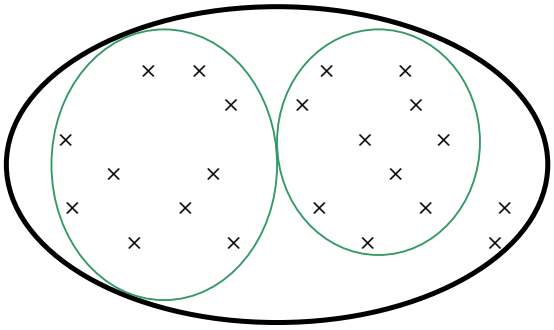
On procède à peu près comme à l'école primaire :
① « dans $3x^2$, combien de fois x ? $3x$ fois ». Je pose donc $3x$ au niveau du quotient.
② « $-2\times(3x)=-6x$ » : je place et je soustrais $3x^2$ - $2x$ et $3x^2-6x$; puis j'abaisse le 8.
③ J'obtiens $4x-8$ et je repars : « dans $4x$, combien de fois 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 :

$$\begin{aligned} 43 &= 2\times21+1 \\ 21 &= 2\times10+1 \\ 10 &= 2\times5+0 \\ 5 &= 2\times2+1 \\ 2 &= 2\times1+0 \\ 1 &= 2\times0+1 \end{aligned}$$

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

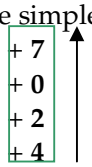
Soit $n \in \mathbb{N}$. Démontrer que quel que soit n, $3n^4 + 5n + 1$ est impair ; puis que ce polynôme n'est jamais divisible par $n(n + 1)$.

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 !