Université Joseph Fourier, Grenoble I
Mathématiques, Informatique et Mathématiques Appliquées
Licence Sciences et Technologies 1e année

Arithmétique

Didier Piau et Bernard Ycart

Guère d'introduction tonitruante à faire, sinon pour souligner que ce chapitre a le charme de n'utiliser comme notions admises que les notations de la théorie des ensembles naïve et les connaissances évidentes sur les entiers, et qu'il présente donc l'agrément de donner une image de démonstrations (que l'on espère) totalement crédibles.

Table des matières

1 Cours

1.1 Nombres premiers

On appelle entier (ou entier relatif, c'est-à-dire positif ou négatif) tout élément de

$$\mathbb{Z} = \{ \ldots, -3, -2, -1, \ 0, \ 1, \ 2, \ 3, \ldots \}$$

Définition 1. *On dit qu'un entier a est un* multiple *d'un entier b, ou que b est un* diviseur *de a lorsqu'il existe un entier k tel que $a = kb$.*

Définition 2. *On dit qu'un entier $p \geq 2$ est premier lorsqu'il possède pour seuls diviseurs positifs 1 et lui-même.*

On notera au passage qu'au hasard des définitions, on parlera parfois d'entiers relatifs (les éléments de $\mathbb{Z}$) et parfois d'entiers naturels (les éléments de $\mathbb{N}$). Ce n'est qu'exceptionnellement très significatif ; la principale fonction est d'être cohérent avec le reste du monde. Ainsi, comme partout ailleurs, dans ce cours, le nombre 3 est un nombre premier alors que -3 n'en est pas un. En revanche, les nombres négatifs étant autorisés dans la définition de « diviseurs », l'entier 3 possède en tout et pour tout quatre diviseurs (à savoir -3, -1,1 et 3).

Et tout de suite un joli théorème, qui remonte aux *Éléments* d'Euclide, écrits au IIIème siècle avant notre ère (c'est la proposition 20 du livre IX).

Théorème 1. *Il existe une infinité de nombres premiers.*

Vous connaissez probablement déjà une démonstration, il en existe plusieurs qui sont toutes bonnes à connaître, en voici une qui est très proche de celle du traité d'Euclide lui-même.

Démonstration : Soit A l'ensemble des nombres premiers. A est une partie de $\mathbb{N}$, et est non vide car 2 est premier. On va supposer A finie et aboutir à une absurdité.

Supposons donc A finie. Dès lors que A est une partie finie de $\mathbb{N}$, évidemment non vide car 2 est premier, A possède un plus grand élément. Notons P ce plus grand élément, le mystérieux « plus grand nombre premier ».

Considérons alors l'entier $N = P! + 1$ (la factorielle de P, plus 1). Pour tout entier k tel que $2 \leq k \leq P$, comme k divise $P!$ et ne divise pas 1, k ne peut diviser N. Tout diviseur de N, et en particulier tout diviseur premier de N, est donc strictement supérieur à P.

Or tout entier, et par exemple N, possède au moins un diviseur premier (pourquoi ? exercice...). Mais alors, chacun de ces diviseurs premiers contredit la maximalité de P. Absurdité ! □

1.2 Division euclidienne

Il s'agit de formaliser avec précision la bonne vieille division euclidienne, celle que vous connaissez depuis l'école primaire.

Théorème 2. *Soit a un entier (relatif) et $b \geq 1$ un entier strictement positif. Alors il existe un couple (q, r) unique (d'entiers) vérifiant la double condition :*

$$a = bq + r \qquad \text{et} \qquad 0 \leq r < b.$$

Démonstration : On va prouver successivement l'existence et l'unicité de (q, r).

Existence de (q, r) : la démonstration se prête bien à discuter selon le signe de a. Le cas où $a \geq 0$ est le cas contenant l'essentiel de la démonstration ; lorsque $a < 0$, on ne peut utiliser mot à mot la même preuve, mais on se ramène alors sans mal au cas intéressant déjà traité.

• Premier cas (le cas significatif) : si $a \geq 0$.

L'idée de la démonstration est de dire que le quotient de a par b est le plus grand entier q tel que bq soit encore plus petit que a.

Introduisons donc l'ensemble $A = \{c \in \mathbb{N}\,,\ bc \leq a\}$. L'ensemble A est un ensemble d'entiers naturels ; il est non vide, car il contient 0. Il est fini : en effet soit d un entier tel que $d \geq a + 1$; on a alors $bd \geq b(a + 1) \geq a + 1 > a$, donc $d \notin A$ et ainsi A ne contient que des entiers inférieurs ou égaux à a.

L'ensemble A possède donc un plus grand élément q. Posons $r = a - bq$. La première condition sur (q, r) est alors évidemment vérifiée, c'est la seconde qui nécessite une vérification.

Comme $q \in A$, par définition de A, on a $bq \leq a$. Donc $r = a - bq \geq 0$.

Comme q est maximal parmi les éléments de A, $q + 1 \notin A$. Donc $b(q + 1) > a$, donc $r = a - bq < b$.

L'existence est démontrée dans ce cas.

• Second cas (preuve sans imagination) : si $a < 0$.

Posons $a' = a(1 - b)$. Comme $a < 0$ et $1 - b \leq 0$, on obtient $a' \geq 0$.

On peut donc, en appliquant le premier cas, faire la division euclidienne de a' par b ; notons (q', r) le couple ainsi obtenu : on a alors $a' = bq' + r$, avec en outre $0 \leq r < b$. En réinjectant la définition de a', on écrit alors $a - ba = bq' + r$, donc $a = b(q' + a) + r$. Si on pose $q = q' + a$, on constate qu'on a réussi la division euclidienne de a par b.

Unicité de (q, r) : soit (q_1, r_1) et (q_2, r_2) des couples vérifiant les deux conditions exigées dans l'énoncé du théorème.

On déduit de $a = bq_1 + r_1 = bq_2 + r_2$ que $b(q_1 - q_2) = r_1 - r_2$. Ainsi, $r_1 - r_2$ est un multiple de b.

Des conditions $0 \leq r_1$ et $r_2 < b$, on déduit que $-b < r_1 - r_2$.

Des conditions $r_1 < b$ et $0 \leq r_2$, on déduit que $r_1 - r_2 < b$.

Ainsi $r_1 - r_2$ est un multiple de b compris strictement entre $-b$ et b. La seule possibilité est que $r_1 - r_2$ soit nul. On en déduit $r_1 = r_2$, puis, en allant reprendre l'égalité $b(q_1 - q_2) = r_1 - r_2$, que $q_1 = q_2$. □

1.3 PGCD et PPCM

Les deux théorèmes qui se suivent sont agréablement parallèles ; il est donc amusant de constater que leurs preuves sont plus différentes qu'on ne pourrait s'y attendre. Il est possible de les déduire l'un de l'autre, mais il est instructif de les prouver très séparément. Vous verrez donc plusieurs preuves de l'un comme de l'autre.

Théorème 3. *Soit $a \geq 1$ et $b \geq 1$ deux entiers. Alors il existe un unique entier $m \geq 1$ tel que pour tout entier $c \geq 1$,*

c est un multiple de a et de b si et seulement si c est un multiple de m.

Théorème 4. *Soit $a \geq 1$ et $b \geq 1$ deux entiers. Alors il existe un unique entier $d \geq 1$ tel que pour tout entier $c \geq 1$,*

c divise a et b si et seulement si c divise d.

Ces théorèmes sont vendus avec deux compléments, le premier occasionnellement utile, le second totalement fondamental.

Complément 1 Pour tous a et b, $md = ab$.

Complément 2 (Identité de Bézout)

Pour tous a et b, il existe deux entiers (relatifs) s et t tels que $d = sa + tb$.

Et tant qu'on y est avant de passer aux démonstrations :

Définition 3. *Le* plus petit multiple commun *de deux entiers a et b est l'entier m apparaissant dans l'énoncé du théorème 3.*

Notation 1. *Le plus petit multiple commun de a et b sera noté* $\mathrm{ppcm}(a, b)$.

Définition 4. *Le* plus grand commun diviseur *de deux entiers a et b est l'entier d apparaissant dans l'énoncé du théorème 4.*

Notation 2. *Le plus grand commun diviseur de a et b sera noté* $\mathrm{pgcd}(a, b)$.

Première démonstration du théorème 3

Cette démonstration est la plus élémentaire ; elle consiste à choisir pour m le multiple commun de a et b le plus « petit » au sens de la relation habituelle $\leq$, puis à

vérifier qu'il marche. La preuve est en deux parties : d'abord l'existence de m (partie significative) puis son unicité (partie très facile).

Existence de m

Introduisons l'ensemble A formé des entiers strictement positifs simultanément multiples de a et de b. L'ensemble A n'est pas vide, puisqu'il contient l'entier ab. Il admet donc un plus petit élément m. On va vérifier que cet entier m convient.

Pour faire cette vérification, soit un entier $n \geq 1$; nous avons désormais à montrer une équivalence, distinguons méthodiquement les deux sens.

• Preuve de l'implication directe : Supposons donc que n est un multiple commun de a et b, et montrons que n est un multiple de m. Pour ce faire, effectuons la division euclidienne de n par m, soit $n = mq + r$, avec $0 \leq r < m$. Comme n et m sont des multiples de a, $r = n - mq$ aussi ; de même avec b. Ainsi r est un multiple commun de a et b. Si r était un entier strictement positif, vu l'inégalité $r < m$ il contredirait la minimalité de m. C'est donc que $r = 0$ et donc que n est un multiple de m.

• Preuve de l'implication réciproque : Supposons ici que n est un multiple de m. Comme m est lui-même multiple de a, n est à son tour multiple de a ; de même avec b. C'est réglé.

Unicité de m

Soit m et m' vérifiant les hypothèses du théorème. Comme m est un multiple de m (eh oui !), c'est un multiple commun de a et b, donc un multiple de m'. De même, m' est un multiple de m. Cela implique que m et m' sont forcément égaux au signe près. Comme ils sont tous deux strictement positifs, ils sont égaux. Fin de la démonstration.

Voici maintenant une première démonstration de l'existence (et l'unicité) du pgcd, qui l'obtient à partir du ppcm. Cette démonstration a le confort d'être dépourvue d'idée subtile et l'avantage de prouver le Complément 1. Elle a l'inconvénient de ne pas prouver le Complément 2 et de ne pas fournir une méthode rapide de calcul du pgcd.

Première démonstration du théorème 4

Existence de d

On note m le ppcm de a et b et on pose $d = ab/m$. Remarquons que ce nombre d est bien un entier : en effet, ab étant un multiple commun évident de a et b, c'est un multiple de leur ppcm. Reste à prouver qu'il convient.

Pour faire cette vérification, soit $n \geq 1$ un entier ; nous avons désormais à montrer une équivalence, distinguons méthodiquement les deux sens.

• Preuve de l'implication directe : supposons que n est un diviseur commun de a et b. On peut donc introduire deux entiers k et ℓ tels que $a = kn$ et $b = \ell n$. Pour travailler sur ce sur quoi nous avons des informations, à savoir les multiples de a et b, introduisons le nombre $n' = ab/n$. Ce nombre n' vaut aussi $(a/n)b = kb$ et $(b/n)a = \ell a$. C'est donc un entier, et même un multiple commun de a et b. C'est donc un multiple

de m. Il existe donc un entier c tel que $n' = cm$, soit $ab/n = c\,ab/d$, donc $d = cn$. On a bien prouvé que n divise d.

• Preuve de l'implication réciproque : puisque $a = d\,(m/b)$ où m/b est un entier, d divise a ; symétriquement puisque $b = d\,(m/a)$, d divise b. Supposons maintenant que n divise d. On voit alors aussitôt que n divise a et b.

Unicité de d

C'est exactement le même principe que pour le ppcm, on laisse donc cette partie de la démonstration en exercice (très) facile.

Preuve du Complément 1 : Il tombe immédiatement au vu de la formule qui donne d à partir de m. Fin de la démonstration.

Comme promis, voici maintenant une deuxième démonstration du théorème 4, très différente dans son esprit, et qui permet pour guère plus cher de montrer simultanément le Complément 2.

Deuxième démonstration du théorème 4

La démonstration est une récurrence sur b ; techniquement, on gagne sérieusement en confort si on autorise b à être nul, ce que l'on n'a pas fait, volontairement, en énonçant le théorème dans l'espoir qu'il soit plus clair. On montrera donc légèrement mieux que l'énoncé de la page précédente, puisqu'on prouvera le résultat sous l'hypothèse « $a \geq 1$ et $b \geq 0$ ».

Avant de se lancer dans la récurrence proprement dite, on va donner un « résumé de la preuve » sous forme de programme informatique récursif.

`Début du programme`
`*` $\mathrm{pgcd}(a, 0) = a$.
`*` `Soit` r `le reste de la division euclidienne de` a `par` b.
`Les diviseurs communs de` a `et` b `sont les diviseurs communs de` b `et` r.
`D'où :` $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.
`Fin du programme`

Ce résumé de démonstration convaincra peut-être les esprits les plus agiles, mais à notre niveau d'entraînement, il est plus prudent de faire ce qui est derrière les formulations récursives : une bonne vieille récurrence.

On va démontrer par « récurrence forte » sur $b \geq 0$ l'hypothèse (H_b) suivante :

> (H_b) Pour tout entier $a \geq 1$, il existe deux entiers (relatifs) s et t tels que, pour tout $n \geq 1$, n divise a et b si et seulement si n divise $sa + tb$.

Vérifions (H_0).

Soit a un entier avec $a \geq 1$; tout entier $n \geq 1$ qui divise a divise aussi $b = 0$ puisque $0n = 0$. Pour tout $n \geq 1$, on a donc : n divise a et 0 si et seulement si n divise a. Prenons alors $s = 1$ et $t = 0$. On a donc bien pour tout $n \geq 1$: n divise a et 0 si et seulement si n divise $sa + t \times 0$.

Soit b un entier fixé, avec $b \geq 1$. Supposons la propriété (H_c) vraie pour tout c avec $0 \leq c < b$ et montrons (H_b).

Soit a un entier avec $a \geq 1$. Notons $a = bq + r$ la division euclidienne de a par b (qu'on peut réaliser puisque $b \geq 1$).

Vérifions l'affirmation intermédiaire suivante : pour tout $n \geq 1$, n est un diviseur commun de a et b si et seulement si n est un diviseur commun de b et r. C'est-à-dire, avec des mots peut-être plus lisibles : « les diviseurs communs de a et b sont les mêmes que ceux de b et r. »

Soit n un diviseur commun de a et b, alors n divise aussi $r = a - bq$; réciproquement soit n un diviseur commun de b et r, alors n divise aussi $a = bq + r$.

L'affirmation intermédiaire est donc démontrée.

On peut alors appliquer l'hypothèse de récurrence (H_r) (puisque précisément $0 \leq r < b$) sur l'entier $b \geq 1$.

On en déduit qu'il existe deux entiers relatifs s' et t' tels que pour tout $n \geq 1$, n divise b et r si et seulement si n divise $s'b + t'r$.

Remarquons enfin que $s'b + t'r = s'b + t'(a - bq) = t'a + (s' - q)b$, et qu'ainsi, si on pose $s = t'$ et $t = s' - q$, on a bien prouvé que, pour tout $n \geq 1$, n divise a et b si et seulement si n divise $sa + tb$.

(H_b) est donc démontrée.

On a donc bien prouvé (H_b) pour tout $b \geq 0$, donc a fortiori pour tout $b \geq 1$, ce qui prouve le théorème 4 et son Complément 2.

En fait, il reste à prouver l'unicité de d, pour laquelle on renvoie à la démonstration précédente (où on écrivait qu'on la laissait en exercice).

Fin de la démonstration.

À présent, donnons un petit exemple sur des vrais nombres concrets, pour nous soulager l'esprit après tant de lettres.

Calcul du pgcd de 137 **et** 24

On fait des divisions euclidiennes successives et on écrit dans la colonne de droite les conséquences de ces divisions.

(1)	137	=	5	×	24	+	17	$\text{pgcd}(137, 24) = \text{pgcd}(24, 17)$
(2)	24	=	1	×	17	+	7	$\text{pgcd}(24, 17) = \text{pgcd}(17, 7)$
(3)	17	=	2	×	7	+	3	$\text{pgcd}(17, 7) = \text{pgcd}(7, 3)$
(4)	7	=	2	×	3	+	1	$\text{pgcd}(7, 3) = \text{pgcd}(3, 1)$
(5)	3	=	3	×	1	+	0	$\text{pgcd}(3, 1) = \text{pgcd}(1, 0) = 1$

Donc $\text{pgcd}(137, 24) = 1$.

Ces calculs permettent ensuite sans mal de reconstituer une identité de Bézout.

– La dernière division avec un reste non nul est (4) qui donne $1 = 7 - 2 \times 3$.

- On va repêcher une expression de 3 comme un reste dans la relation précédente, soit (3), ce qui donne $3 = 17 - 2 \times 7$.
- On reporte cette expression de 3 donc $1 = 7 - 2 \times (17 - 2 \times 7)$.
- On regroupe les termes en 17 et 7 donc $1 = -2 \times 17 + 5 \times 7$.
- On va repêcher une expression de 7 comme un reste dans la relation précédente, soit (2), ce qui donne $7 = 24 - 1 \times 17$.
- On reporte cette expression de 7 donc $1 = -2 \times 17 + 5 \times (24 - 1 \times 17)$.
- On regroupe les termes en 24 et 17 donc $1 = 5 \times 24 - 7 \times 17$.
- On va repêcher une expression de 17 comme un reste dans la relation précédente, soit (1), ce qui donne $17 = 137 - 5 \times 24$.
- On reporte cette expression de 17 donc $1 = 5 \times 24 - 7 \times (137 - 5 \times 24)$.
- On regroupe les termes en 137 et 24 donc

$$1 = -7 \times 137 + 40 \times 24.$$

- Et voilà !

Voici un autre exemple.

Calcul du pgcd de 141 **et** 24

Voici les divisions euclidiennes successives et leurs conséquences en termes de pgcd.

$$\begin{array}{lrcrcrcrl}
(1) & 141 & = & 5 & \times & 24 & + & 21 & \quad \mathrm{pgcd}(141,24) = \mathrm{pgcd}(24,21) \\
(2) & 24 & = & 1 & \times & 21 & + & 3 & \quad \mathrm{pgcd}(24,21) = \mathrm{pgcd}(21,3) \\
(3) & 21 & = & 7 & \times & 3 & + & 0 & \quad \mathrm{pgcd}(21,3) = \mathrm{pgcd}(3,0) = 3
\end{array}$$

Donc $\mathrm{pgcd}(141, 24) = 3$ et on vérifiera que ces calculs permettent de reconstituer l'identité de Bézout

$$-141 + 6 \times 24 = 3.$$

Donnons une dernière définition avant de quitter les pgcd.

Définition 5. *On dit que deux entiers $a \geq 1$ et $b \geq 1$ sont* premiers entre eux *lorsque leur seul diviseur commun positif est* 1*.*

On veillera à ne pas confondre cette notion avec celle de nombre premier. (Par exemple, les calculs ci-dessus montrent que 137 et 24 sont premiers entre eux mais 24 n'est pas premier.)

1.4 Lemme de Gauss et décomposition en facteurs premiers

Le lemme de Gauss permet de démontrer l'unicité de la décomposition en facteurs premiers. Ce dernier résultat semble plus facile d'usage pour un utilisateur peu expérimenté, donc on énonce le lemme de Gauss sans commentaire, ou plus exactement sans autre commentaire que ce commentaire négatif.

Lemme 1. *Soit a, b et c trois entiers strictement positifs. Si a divise le produit bc et si a est premier avec c, alors a divise b.*

Démonstration : Puisque a est premier avec c, le pgcd de a et c est 1, donc il existe des entiers relatifs s et t tels que $sa + tc = 1$. Multiplions cette identité par b : on obtient $b = asb + tbc$. Mais dans cette écriture, asb est évidemment multiple de a tandis que tbc l'est parce que bc est multiple de a. On en déduit que b, somme des deux multiples de a que sont asb et tbc, est lui-même un multiple de a. □

Théorème (énoncé approximatif) *Tout entier $n \geq 2$ peut être écrit de façon unique comme produit de facteurs premiers.*

L'énoncé est approximatif car il n'est pas si clair de savoir ce que signifie « unique » : on peut écrire $6 = 2 \times 3 = 3 \times 2$ mais il faut évidemment considérer que c'est la même chose. Pour pouvoir comprendre voire utiliser le théorème, cet énoncé suffira bien ; mais pour le démontrer, il faut être plus précis.

Théorème 5 (énoncé précis)**.** *Tout entier $n \geq 2$ peut être écrit comme produit de facteurs premiers. De plus, si on dispose de deux écritures*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad \text{et} \qquad n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_i^{\beta_i},$$

dans lesquelles $k \geq 1$, $i \geq 1$, les entiers $p_1 < p_2 < \ldots < p_k$ et $q_1 < q_2 < \ldots < q_i$ sont tous premiers et rangés en ordre croissant, les exposants α_1, α_2, …, α_k et β_1, β_2, …, β_i sont tous des entiers strictement positifs, alors ces deux écritures sont les mêmes au sens précis suivant : $k = i$ et pour tout j avec $1 \leq j \leq k = i$, $p_j = q_j$ et $\alpha_j = \beta_j$.

Démonstration : À énoncé indigeste, démonstration indigeste.

L'existence provient d'une récurrence élémentaire. Pour tout entier $n \geq 2$, considérons l'hypothèse de récurrence (forte) suivante :

> (E_n) Tout entier $2 \leq k \leq n$ peut s'écrire comme un produit de facteurs premiers comme dans l'énoncé du théorème.

Alors (E_2) est évidente car 2 est premier.

Soit $n \geq 2$ un entier fixé, supposons (E_n) vraie et montrons (E_{n+1}).

Si $n + 1$ est premier, (E_{n+1}) est évidente.

Si $n + 1$ n'est pas premier, il existe un entier $2 \leq k \leq n$ qui divise $n + 1$. Notons ℓ l'entier $\ell = (n + 1)/k$. Alors $2 \leq \ell \leq n$ donc on peut appliquer l'hypothèse (E_n) aux deux entiers k et ℓ. Il existe donc des entiers premiers p_i et q_j et des exposants a_i et b_j strictement positifs tels que

$$k = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}, \qquad \ell = q_1^{b_1} q_2^{b_2} \cdots q_v^{b_v},$$

avec $p_1 < p_2 < \ldots < p_u$ et $q_1 < q_2 < \ldots < q_v$. Par conséquent,

$$n + 1 = k \times \ell = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} \times q_1^{b_1} q_2^{b_2} \cdots q_v^{b_v}.$$

L'ensemble $\{p_1, p_2, \ldots, p_u\} \cup \{q_1, q_2, \ldots, q_v\}$ comporte $w \leq u + v$ éléments. Notons et ordonnons ces éléments comme $r_1 < r_2 < \cdots < r_w$. En regroupant les entiers qui apparaissent dans les deux factorisations, on obtient

$$n + 1 = r_1^{c_1} r_2^{c_2} \cdots r_w^{c_w},$$

où les exposants c_k sont définis comme suit :
- $c_k = a_i$ si $r_k = p_i$ et $r_k \neq q_j$ pour tout j,
- $c_k = b_j$ si $r_k = q_j$ et $r_k \neq p_i$ pour tout i,
- et enfin $c_k = a_i + b_j$ si $r_k = p_i = q_j$.

Donc (E_{n+1}) est vraie.

Ceci conclut la preuve de l'existence.

Passons à l'unicité. On va donc montrer par récurrence (forte) sur n le résultat d'unicité (H_n) écrit dans l'énoncé du théorème.

Démonstration de (H_2), et en fait même de (H_p) pour tout nombre premier p

Supposons $n = p$ premier écrit sous forme de produit $p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Chaque p_i est un diviseur positif de p non égal à 1, donc chaque p_i est égal à p. Ceci entraîne aussitôt que $k = 1$ et que $\alpha_1 = 1$ (sans cela le produit serait supérieur ou égal à p^2 donc distinct de p). L'écriture $p = p$ est donc la seule possible pour p, ce qui démontre (H_p) quand p est premier.

Soit maintenant n un entier fixé, non premier, avec $n > 2$, et supposons l'hypothèse d'unicité (H_m) prouvée pour tout entier m avec $2 \leq m < n$.

Première étape Montrons que $p_k = q_i$ (toujours dans les notations de l'énoncé du théorème).

Supposons tout d'abord que $p_k > q_i$ et montrons que l'on aboutit à une absurdité.

Puisque les q_j sont supposés rangés dans l'ordre croissant, p_k est alors forcément distinct de tous les q_j ; p_k et chaque q_j étant premiers, on en conclut que leur seul diviseur commun positif est 1 : p_k et q_j sont donc premiers entre eux.

Fixons un j entre 1 et i et montrons par récurrence sur $b \geq 0$ l'énoncé fort intuitif suivant : (H'_b) : p_k est premier avec q_j^b.

(H'_0) est évident puisque $q_j^0 = 1$.

Soit $b \geq 0$ un entier fixé, supposons (H'_b) vrai et montrons (H'_{b+1}).

Si (H'_{b+1}) était faux, le pgcd de p_k et q_j^{b+1} ne serait pas 1 ; comme c'est un diviseur positif de p_k, ce serait p_k qui diviserait donc q_j^{b+1}. On peut alors appliquer le lemme de Gauss : comme p_k divise $q_j^{b+1} = q_j^b q_j$ et que p_k est premier avec q_j, p_k divise q_j^b. Mais ceci contredit l'hypothèse (H'_b). L'hypothèse (H'_{b+1}) est donc vraie.

On a donc bien montré que pour tout $b \geq 0$, p_k est premier avec q_j^b. En particulier, p_k est premier avec $q_j^{\beta_j}$. Comme on a prouvé cette affirmation pour un j quelconque, on a prouvé que pour tout j entre 1 et i, p_k est premier avec $q_j^{\beta_j}$. Ce qu'on a fait avec

les puissances de chaque q_j, on va maintenant le recommencer avec le produit de ces puissances. Précisément, on va montrer par récurrence sur l'entier j que pour tout j avec $1 \leq j \leq l$, on a l'énoncé (H''_j) : p_k est premier avec $q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j}$.

Les lecteurs encore éveillés (s'il en reste) comprendront que la preuve est à peu près la même que celle des (H'_b), pour les autres, la voilà :

Pour $j = 1$, on doit prouver que p_k est premier avec $q_1^{\beta_1}$. C'est déjà fait.

Fixons un entier j avec $1 \leq j < i$ et supposons l'hypothèse (H''_j) vraie.

Si (H''_{j+1}) était fausse, le pgcd de p_k et $q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j} q_{j+1}^{\beta_{j+1}}$ ne serait pas 1 ; comme c'est un diviseur positif de p_k, ce serait p_k qui diviserait donc $q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j} q_{j+1}^{\beta_{j+1}}$. On peut alors appliquer le lemme de Gauss : comme p_k divise le nombre

$$q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j} q_{j+1}^{\beta_{j+1}} = \left(q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j} \right) q_{j+1}^{\beta_{j+1}}$$

et comme p_k est premier avec $q_{j+1}^{\beta_{j+1}}$, p_k divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j}$. Mais ceci contredit l'hypothèse (H''_j). L'hypothèse (H''_{j+1}) est donc vraie.

On a donc montré (H''_j) pour tout j entre 1 et i ; en particulier on a montré (H''_i), à savoir que p_k est premier avec $q_1^{\beta_1} q_2^{\beta_2} \cdots q_i^{\beta_i} = n$. Mais pourtant p_k figure dans l'autre décomposition en facteurs premiers de n (ce n'est pas une illusion d'optique, puisqu'on a pris soin de supposer $\alpha_k \geq 1$), donc p_k divise n. D'où contradiction. Ouf !

On ne peut donc avoir $p_k > q_i$. En échangeant les rôles des coefficients p et q, on voit qu'on ne peut pas non plus avoir $q_i > p_k$. On en déduit donc que $q_i = p_k$.

Fin de la première étape

Deuxième étape On va profiter de ce tout petit morceau d'égalité pour arriver à utiliser l'hypothèse de récurrence et faire tomber toutes les autres égalités requises en cascade.

Notons $N = n/p_k = n/q_i$, on a ainsi :

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k - 1} \qquad \text{et} \qquad N = q_1^{\beta_1} q_2^{\beta_2} \cdots q_i^{\beta_i - 1}.$$

De plus N est strictement inférieur à n, et N est strictement plus grand que 1 car on a fort opportunément supposé n non premier. On va donc appliquer l'hypothèse de récurrence (H_N) à ces deux écritures de N en facteurs premiers. Si on n'est pas méticuleux, on oubliera de s'assurer que tous les exposants sont strictements positifs, et on aura fini tout de suite ; ce sera faux, mais de peu. Hélas, un enseignant scrupuleux ne peut se le permettre et doit donc veiller à ce petit détail, qui nous force à distinguer deux sous-cas.

Premier sous-cas : $\alpha_k = 1$. Dans ce cas, la première écriture de m se lit en réalité, après effacement du p_k^0 qui l'encombre :

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}.$$

Ainsi N possède une décomposition en facteurs premiers dans laquelle p_k ne figure pas. Comme sa décomposition est unique, p_k ne peut non plus figurer dans l'autre décomposition, et comme $q_i = p_k$, la seule possibilité est que l'exposant $\beta_i - 1$ soit nul ; ainsi $\beta_i = \alpha_k = 1$, et les deux représentations

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}} \quad \text{et} \quad N = q_1^{\beta_1} q_2^{\beta_2} \cdots q_{i-1}^{\beta_{i-1}}$$

sont deux décompositions de N en facteurs premiers. On en déduit que $k - 1 = i - 1$, donc $k = i$, puis l'égalité de tous les facteurs premiers et exposants encore en attente d'élucidation.

Second sous-cas : $\alpha_k > 1$. C'est la même chanson. On remarque tout d'abord qu'on a aussi $\beta_i > 1$ (sans cela, en échangeant les rôles des coefficients p et q et en utilisant le premier cas, on montrerait que $\alpha_k = 1$) ; donc les deux décompositions

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k - 1} \quad \text{et} \quad N = q_1^{\beta_1} q_2^{\beta_2} \cdots q_i^{\beta_i - 1}$$

vérifient bien les hypothèses du théorème. Elles sont égales, donc $k = i$ et chaque coefficient p est égal au coefficient q correspondant, avec le même exposant.

Fin de la deuxième étape

(H_n) est donc prouvée.

La récurrence est donc terminée, et avec elle la démonstration. □

La décomposition en facteurs premiers permet d'énumérer facilement les diviseurs d'un entier.

Proposition 1. *Soit n un entier et*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

sa décomposition en facteurs premiers. L'ensemble des diviseurs positifs de n est :

$$D = \left\{ N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \,,\ \forall i = 1, \ldots, k \quad 0 \leqslant \beta_i \leqslant \alpha_i \right\}$$

Par exemple l'ensemble des diviseurs positifs de $60 = 2^2\ 3^1\ 5^1$ est :

$$D = \Big\{ 2^0\ 3^0\ 5^0\,,\ 2^1\ 3^0\ 5^0\,,\ 2^0\ 3^1\ 5^0\,,\ 2^2\ 3^0\ 5^0\,,\ 2^0\ 3^0\ 5^1\,,\ 2^1\ 3^1\ 5^0\,,$$
$$2^1\ 3^0\ 5^1\,,\ 2^2\ 3^1\ 5^0\,,\ 2^0\ 3^1\ 5^1\,,\ 2^2\ 3^1\ 5^0\,,\ 2^2\ 3^0\ 5^1\,,\ 2^2\ 3^1\ 5^1 \Big\}\,,$$

soit,

$$D = \Big\{ 1\,,\ 2\,,\ 3\,,\ 4\,,\ 5\,,\ 6\,,\ 10\,,\ 12\,,\ 15\,,\ 20\,,\ 30\,,\ 60 \Big\}$$

Démonstration : Soit

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{et} \quad N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

Si pour tout $i = 1, \ldots, k$, $0 \leqslant \beta_i \leqslant \alpha_i$, alors :

$$n = N \times \left(p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_k^{\alpha_k - \beta_k} \right)$$

Donc tout élément de l'ensemble D est diviseur de n.

Réciproquement, soit N un diviseur de n. Tout facteur premier de N divise n, donc c'est l'un des p_i. Si $p_i^{\beta_i}$ divise N, alors $p_i^{\beta_i}$ divise aussi n, donc $\beta_i \leqslant \alpha_i$. Ceci montre que tout diviseur de n est élément de D. □

Quand on connaît la décomposition en facteurs premiers de deux nombres, il est facile de calculer leur pgcd et leur ppcm.

Proposition 2. *Soient m et n deux entiers. Quitte à admettre des exposants nuls, nous pouvons considérer que leurs facteurs premiers sont les mêmes. Ecrivons donc :*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \textit{et} \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \ ,$$

où pour $i = 1, \ldots, k$, $\alpha_i \geqslant 0$ et $\beta_i \geqslant 0$.

Alors :

$$\mathrm{pgcd}(m, n) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k} \quad \textit{et} \quad \mathrm{ppcm}(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k} \ ,$$

où pour tout $i = 1, \ldots, k$,

$$\delta_i = \min\{\alpha_i, \beta_i\} \quad \textit{et} \quad \gamma_i = \max\{\alpha_i, \beta_i\}$$

Considérons par exemple :

$$n = 172872 = 2^3\ 3^2\ 7^4 \quad \text{et} \quad m = 525525 = 3^1\ 5^2\ 7^2\ 11^1\ 13^1$$

Quitte à admettre des puissances nulles, nous pouvons écrire la décomposition sur les mêmes facteurs.

$$n = 2^3\ 3^2\ 5^0\ 7^4\ 11^0\ 13^0 \quad \text{et} \quad m = 2^0\ 3^1\ 5^2\ 7^2\ 11^1\ 13^1$$

Donc :

$$\mathrm{pgcd}(m, n) = 2^0\ 3^1\ 5^0\ 7^2\ 11^0\ 13^0 = 3^1\ 7^2 = 147,$$

et

$$\mathrm{ppcm}(m, n) = 2^3\ 3^2\ 5^2\ 7^4\ 11^1\ 13^1 = 618017400.$$

Démonstration : Posons :

$$d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}.$$

On vérifie facilement que d est bien un diviseur commun de m et de n. Réciproquement, soit d' un diviseur commun de m et n. Tout facteur premier p de d est aussi un facteur premier de m et de n. Si p_i^{δ} divise n et m, alors $\delta \leqslant \alpha_i$ et $\delta \leqslant \beta_i$, donc

$$\delta \leqslant \delta_i = \min\{\alpha_i, \beta_i\}.$$

Ceci entraîne que d' est diviseur de d. Donc d est bien le pgcd de m et n.

L'expression du ppcm se déduit de celle du pgcd par la formule :

$$\text{pgcd}(m,n)\ \text{ppcm}(m,n) = m\ n.$$

□

1.5 Sous-groupes de $\mathbb{Z}$

Notation 3. *Soit b un entier. On note $b\mathbb{Z}$ l'ensemble des multiples de b.*

Par exemple $0\mathbb{Z} = \{0\}$ et $2\mathbb{Z}$ est l'ensemble des entiers relatifs pairs.

L'objet de la section est un théorème d'énoncé très simple, et assez pratique.

Théorème 6. *Les sous-groupes de $\mathbb{Z}$ sont exactement les ensembles $b\mathbb{Z}$ avec $b \geq 0$.*

Démonstration : Il y a deux choses à démontrer : que les ensembles $b\mathbb{Z}$ sont des sous-groupes, et que tout sous-groupe est un ensemble $b\mathbb{Z}$.

Commençons donc par vérifier (c'est très facile) que pour $b \geq 0$ fixé, $b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

• 0 est multiple de b, donc $b\mathbb{Z}$ n'est pas vide.

• Soit x et y deux éléments de $b\mathbb{Z}$, c'est-à-dire deux multiples de b. Il est clair que $x - y$ est aussi un multiple de b, donc appartient à $b\mathbb{Z}$.

C'est fait. Pour les amateurs d'abstraction, on pouvait remarquer que $b\mathbb{Z} = \langle b \rangle$ (le sous-groupe engendré par b), ce qui est camouflé par la notation additive de l'opération.

Soit maintenant H un sous-groupe de $\mathbb{Z}$, montrons qu'il existe un entier $b \geq 0$ tel que $H = b\mathbb{Z}$. On distinguera deux cas.

Premier cas : Si $H = \{0\}$, on remarque que $H = 0\mathbb{Z}$ et on a fini.

Second cas : Si $H \neq \{0\}$, H possède au moins un élément non nul x, donc au moins un élément strictement positif y (on prendra $y = x$ ou $y = -x$ selon le signe de x). Si on introduit l'ensemble $B = H \cap \mathbb{N}^*$, B est donc un ensemble d'entiers positifs non vide. Il possède un plus petit élément b. On va montrer que b convient.

Il semble raisonnablement clair que $b\mathbb{Z} \subset H$. (Hum, est-ce si clair ou est-ce un petit moment de paresse du rédacteur ? Le lecteur est invité à se forger par lui-même une opinion sur cette épineuse question.)

Réciproquement soit a un élément de H. Si on fait la division euclidienne de a par b, soit $a = qb + r$, on en déduit que $r = a - bq$ est aussi un élément de H. Comme $r < b$, $r \notin B$, et comme $r \in H \cap \mathbb{N}$ la seule possibilité est que $r = 0$. On en déduit donc que $a = bq \in b\mathbb{Z}$. Ceci prouve l'inclusion $H \subset b\mathbb{Z}$.

On a donc montré que $H = b\mathbb{Z}$.

On a donc montré, dans les deux cas, que H est de la forme $b\mathbb{Z}$. □

En application de ce théorème, donnons de nouvelles et élégantes démonstrations des théorèmes 3 et 4 ; l'outil à la base reste la division euclidienne, mais il aura été utilisé une seule fois, dans la preuve du théorème qui précède, et on ne fait plus que d'assez simples manipulations ensemblistes.

Deuxième démonstration du théorème 3 :

Introduisons les sous-groupes de $\mathbb{Z}$ que sont $H = a\mathbb{Z}$ et $K = b\mathbb{Z}$. Pour tout $m \geq 1$, m est un diviseur commun de a et b si et seulement si m est dans $H \cap K$. Or $H \cap K$, comme intersection de deux sous-groupes de $\mathbb{Z}$, est lui-même un sous-groupe de $\mathbb{Z}$ (bon, d'accord, on n'a pas mentionné ce résultat dans le cours sur les sous-groupes, mais on aurait dû, et de toutes façons c'est très facile). Il existe donc un entier $m \geq 0$ tel que $H \cap K = m\mathbb{Z}$ (et il est clair que $m > 0$, car $H \cap K$ contient d'autres entiers que 0, par exemple ab). On a alors pour tout $n \geq 1$ les équivalences : n est un diviseur commun de a et b si et seulement si n appartient à $H \cap K$ si et seulement si n appartient à $m\mathbb{Z}$ si et seulement si n est un multiple de m.

L'unicité reste à prouver comme dans la preuve initiale.

Fin de la démonstration.

Troisième démonstration du théorème 4 :

Introduisons l'ensemble $L \subset \mathbb{Z}$ défini par $L = \{sa + tb\,,\ s \in \mathbb{Z}, t \in \mathbb{Z}\}$.

On vérifie sans mal que L est un sous-groupe de $\mathbb{Z}$. C'est si facile, qu'on va le laisser au lecteur.

Il existe donc un entier $d \geq 0$ tel que $L = d\mathbb{Z}$. De plus L n'est manifestement pas réduit à $\{0\}$ (il contient par exemple $a = 1a + 0b$, et même aussi $b = 0a + 1b$), donc $d > 0$. Montrons que d convient.

On a remarqué que a et b sont dans $L = d\mathbb{Z}$. En d'autres termes, ils sont tous deux multiples de d, ou, pour dire cela encore autrement, d est un diviseur commun de a et b. Il est donc clair que tout diviseur de d est à son tour un diviseur commun de a et b.

Par ailleurs, d est dans L, donc peut être mis sous forme $sa + tb$ pour des entiers relatifs s et t. Si on part d'un diviseur commun $n \geq 1$ de a et b, sa et tb sont à leur tour des multiples de n, donc aussi d, et n est donc bien un diviseur de d.

Là aussi, on renvoie à la preuve initiale pour l'unicité.

Fin de la démonstration.

1.6 Congruences

Juste quelques notations pratiques. La section se réduit à quasiment rien.

Définition 6. *Soit a et b des entiers relatifs et $n \geq 1$ un entier strictement positif. On dit que a est* congru *à b modulo n lorsque $b - a$ est un multiple de n.*

Il est tellement évident de vérifier que, pour n fixé, la relation « est congru à » est une relation d'équivalence sur $\mathbb{Z}$ que cet énoncé n'aura pas même l'honneur d'être qualifié de proposition.

Notation 4. *Lorsque a est congru à b modulo n, on note :*

$$a \equiv b \ [n].$$

Exemple 1. *On repère les jours de l'année par leur numéro de* 1 *à* 365 *ou* 366 *selon les cas. Alors les numéros de tous les lundis sont congrus les uns aux autres modulo* 7*.*

L'intérêt des congruences est d'être compatibles avec l'addition et la multiplication, au sens suivant :

Proposition 3. *Soit $n \geq 1$ fixé et soit a, b et c trois entiers relatifs. Alors :*

$$\text{si} \quad a \equiv b \ [n] \quad \text{alors} \quad a + c \equiv b + c \ [n] \quad \text{et} \quad ac \equiv bc \ [n].$$

Démonstration : C'est vraiment trop facile. □

Exemple 2. *Quel est le reste de la division par* 9 *de* 12345 *? On commence par écrire*

$$12345 = 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 5.$$

Comme $10 \equiv 1$ [9]*, on en déduit*

$$123456 \equiv 1^4 + 2 \cdot 1^3 + 3 \cdot 1^2 + 4 \cdot 1 + 5 = 1 + 2 + 3 + 4 + 5 = 15,$$

et

$$12345 \equiv 1 \cdot 10 + 5 \equiv 1 \cdot 1 + 5 = 1 + 5 = 6,$$

donc la réponse est 6*. Et par* 11 *? Ici, on utilise le fait que* $10 \equiv -1$ [11]*, donc*

$$12345 \equiv (-1)^4 + 2 \cdot (-1)^3 + 3 \cdot (-1)^2 + 4 \cdot (-1)^1 + 5 = 3,$$

et la réponse est 3*.*

Exercice : Formaliser les règles de calcul des congruences modulo 9 et modulo 11 utilisées dans l'exemple 2.

Exercice : Montrer qu'une règle de calcul possible pour calculer des congruences modulo 7 est la suivante. On décompose l'écriture de n en base 10 en groupes de 3 chiffres consécutifs en commençant par le chiffre des unités. Si un bloc vaut $B = abc$, on note $s(B) = 2a + 3b + c$. Puis on effectue la somme alternée $s(n)$ des $s(B)$ en commençant par le bloc du chiffre des unités. Alors n et $s(n)$ sont congrus modulo 7.

Par exemple, si $n = 12345678$, les blocs sont $B_3 = 012$, $B_2 = 345$ et $B_1 = 678$. On calcule $s(B_3) = 2 \times 0 + 3 \times 1 + 1 \times 2 = 5$, $s(B_2) = 2 \times 3 + 3 \times 4 + 1 \times 5 = 23$, $s(B_1) = 2 \times 6 + 3 \times 7 + 1 \times 8 = 41$, puis

$$s(n) = s(B_1) - s(B_2) + s(B_3) = 41 - 23 + 5 = 23,$$

donc $n \equiv 23$ [7] et enfin $n \equiv 2$ [7].

1.7 $\mathbb{Z}/n\mathbb{Z}$

En apparence, cette section est consacrée à un formalisme assez gratuit consistant à remplacer l'écriture :

$$a \equiv b\ [n],$$

par l'écriture équivalente :

$$\mathfrak{cl}(a) = \mathfrak{cl}(b) \quad \text{dans } \mathbb{Z}/n\mathbb{Z},$$

où $\mathfrak{cl}$ est l'abréviation de « classe ». Maigre progrès en apparence ! Toutefois, comme des exemples judicieusement choisis le montreront en fin de section, on a fait plus qu'un simple changement de notations : on a construit un pont entre ce chapitre et le chapitre précédent, pont par lequel on pourra rapatrier des résultats connus sur les groupes pour effectivement affiner notre connaissance des entiers.

Définition 7. *Soit $n \geq 1$ un entier fixé. On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble-quotient de $\mathbb{Z}$ par la relation d'équivalence « est congru à » (modulo n).*

Exemple 3. *Pour $n = 2$, soit a un entier. Si a est pair, la classe d'équivalence $\mathfrak{cl}(a)$ pour la relation de congruence modulo 2 est l'ensemble P de tous les nombres pairs ; si a est impair, $\mathfrak{cl}(a)$ est l'ensemble I de tous les nombres impairs, et finalement $\mathbb{Z}/2\mathbb{Z} = \{I, P\}$.*

Proposition 4. *Pour tout $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ possède exactement n éléments.*

Démonstration : Montrons tout d'abord que $\mathbb{Z}/n\mathbb{Z} = \{\mathfrak{cl}(0), \mathfrak{cl}(1), \ldots, \mathfrak{cl}(n-1)\}$, d'où on déduit aussitôt que $\mathbb{Z}/n\mathbb{Z}$ possède au plus n éléments.

Soit x un élément de $\mathbb{Z}/n\mathbb{Z}$; il existe alors $a \in \mathbb{Z}$ tel que $x = \mathfrak{cl}(a)$. Effectuons la division euclidienne de a par n, soit $a = nq + r$; on voit alors que $a \equiv r\ [n]$ ou encore que $x = \mathfrak{cl}(a) = \mathfrak{cl}(r)$. Mais $0 \leq r < n$, donc on a bien prouvé que x était dans l'ensemble proposé.

Montrons maintenant que ces n éléments sont deux à deux distincts, prouvant ainsi que $\mathbb{Z}/n\mathbb{Z}$ possède au moins n éléments.

Soit a et b deux entiers distincts avec $0 \leq a < n$ et $0 \leq b < n$. Des inégalités $0 \leq a$ et $b < n$ on déduit que $-n < b - a$; des inégalités $a < n$ et $0 \leq b$ on déduit que $b - a < n$ et de l'hypothèse $a \neq b$ on déduit que $b - a \neq 0$. On en conclut que $a \not\equiv b\ [n]$, c'est-à-dire que $\mathfrak{cl}(a)$ et $\mathfrak{cl}(b)$ sont deux éléments distincts de $\mathbb{Z}/n\mathbb{Z}$.

On a donc bien prouvé que $\mathbb{Z}/n\mathbb{Z}$ possède exactement n éléments. □

Définition 8. *Soit $\mathfrak{cl}(a)$ et $\mathfrak{cl}(b)$ deux éléments de $\mathbb{Z}/n\mathbb{Z}$. On définit la* somme *de $\mathfrak{cl}(a)$ et $\mathfrak{cl}(b)$ par $\mathfrak{cl}(a) + \mathfrak{cl}(b) = \mathfrak{cl}(a+b)$ et leur* produit *par $\mathfrak{cl}(a) \times \mathfrak{cl}(b) = \mathfrak{cl}(ab)$.*

Prudence ! Cette définition est aussi innocente en apparence que celles qui l'ont précédée. Et pourtant, elle pourrait n'avoir rigoureusement aucun sens.

En effet, la définition de la somme de deux éléments x et y de $\mathbb{Z}/n\mathbb{Z}$ nécessite implicitement de les mettre préalablement sous forme $x = \mathfrak{cl}(a)$ et $y = \mathfrak{cl}(b)$. Mais il y a plusieurs façons de les mettre sous cette forme ! Il faut donc vérifier que la définition ne dépend pas du choix fait dans cette phase préparatoire. Pour montrer à quel point c'est indispensable, donnons une

Fausse définition (buggée) *Soit* $\mathfrak{cl}(a)$ *et* $\mathfrak{cl}(b)$ *deux éléments de* $\mathbb{Z}/n\mathbb{Z}$. *On dira que* $\mathfrak{cl}(a) \leq \mathfrak{cl}(b)$ *lorsque* $a \leq b$.

Il est facile de comprendre pourquoi cette « définition » est bonne pour la corbeille à papier : dans $\mathbb{Z}/3\mathbb{Z}$, prenons $x = \mathfrak{cl}(0)$ et $y = \mathfrak{cl}(2)$. En les écrivant ainsi, la « définition » nous donne : $x \leq y$. Mais on peut aussi écrire $x = \mathfrak{cl}(3)$ et comme précédemment $y = \mathfrak{cl}(2)$. En s'y prenant ainsi, $y \leq x$. Cette « définition » n'a donc en fait aucun sens.

Sermon (ou : Prudence II, le retour) Malgré ses dehors anecdotiques, il est indispensable de comprendre cette remarque. La fausse définition et la bonne sont semblables formellement, alors que l'une est absurde et l'autre non. Fin du sermon.

Procédons donc à cette indispensable vérification. Soit $x = \mathfrak{cl}(a) = \mathfrak{cl}(\alpha)$ et $y = \mathfrak{cl}(b) = \mathfrak{cl}(\beta)$ deux éléments de $\mathbb{Z}/n\mathbb{Z}$. La cohérence de la définition exige de prouver que $\mathfrak{cl}(a+b) = \mathfrak{cl}(\alpha+\beta)$. La vérification est alors évidente $(\alpha+\beta)-(a+b) = (\alpha-a)+(\beta-b)$ étant un multiple de n parce que $\alpha - a$ et $\beta - b$ le sont tous les deux. De même $\mathfrak{cl}(ab) = \mathfrak{cl}(\alpha\beta)$ car $\alpha\beta - ab = \alpha\beta - \alpha b + \alpha b - ab = \alpha(\beta - b) + b(\alpha - a)$.

Ainsi au point où nous en sommes, $\mathbb{Z}/n\mathbb{Z}$ est muni d'une addition et d'une multiplication. Traçons un exemple de tables, pour voir quelle tête elles ont et pour rentabiliser le travail qu'a été d'apprendre à taper de belles tables. Ce sera l'exemple de $\mathbb{Z}/5\mathbb{Z}$.

On note dans cette table et dans les suivantes $\dot{a} = \mathfrak{cl}(a)$.

$+$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Après la présentation de l'objet, un peu de théorie à son sujet.

Proposition 5. *Pour tout $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.*

Démonstration : Elle est d'un ennui mortel, et ne présente aucune difficulté. Pour en faire un tout petit bout, montrons que l'addition est associative : soit x, y et z trois éléments de $\mathbb{Z}/n\mathbb{Z}$. On peut les écrire sous forme $x = \mathfrak{cl}(a)$, $y = \mathfrak{cl}(b)$, $z = \mathfrak{cl}(c)$. Vu la définition de l'addition dans $\mathbb{Z}/n\mathbb{Z}$, on a alors $(x + y) + z = (\mathfrak{cl}(a) + \mathfrak{cl}(b)) + \mathfrak{cl}(c) = \mathfrak{cl}(a+b)+\mathfrak{cl}(c) = \mathfrak{cl}((a+b)+c) = \mathfrak{cl}(a+(b+c)) = \mathfrak{cl}(a)+\mathfrak{cl}(b+c) = \mathfrak{cl}(a)+(\mathfrak{cl}(b)+\mathfrak{cl}(c)) = x + (y + z)$.

Et toutes les vérifications seraient de ce genre. Nous décidons donc de les laisser au lecteur. □

Plus intéressant et légèrement plus subtil est le résultat suivant.

Théorème 7. *Pour tout $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un corps commutatif si et seulement si n est un nombre premier.*

Démonstration : Montrons tour à tour les deux sens de l'équivalence.

Preuve de l'implication directe. On va montrer cette implication par contraposition. Supposons donc que n n'est pas premier, et montrons que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps commutatif (on verra même en passant que ce n'est même pas un anneau intègre).

Traitons à part le cas, « stupide », où n vaudrait 1. Dans ce cas, $\mathbb{Z}/\mathbb{Z}$ ne possède qu'un élément, donc n'est pas un corps commutatif.

Examinons le cas, significatif, où n n'est pas premier, mais n'est pas non plus égal à 1. Dans ce cas, on peut écrire $n = ab$, où $1 < a < n$ et $1 < b < n$. Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, on obtient alors la relation $\mathfrak{cl}(n) = \mathfrak{cl}(a)\mathfrak{cl}(b)$, soit $\mathfrak{cl}(a)\mathfrak{cl}(b) = \mathfrak{cl}(0)$. Pourtant, au vu des inégalités vérifiées par a et b, ni $\mathfrak{cl}(a)$ ni $\mathfrak{cl}(b)$ n'est nul. Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, et a fortiori n'est pas un corps commutatif.

On a bien prouvé dans les deux cas que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps commutatif.

Preuve de l'implication inverse. Supposons n premier, et montrons que $\mathbb{Z}/n\mathbb{Z}$ est alors un corps commutatif.

Nous savons déjà que la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ est commutative.

Comme $\mathbb{Z}/n\mathbb{Z}$ possède n éléments, il en possède au moins deux.

Soit x un élément non nul de $\mathbb{Z}/n\mathbb{Z}$. On peut écrire $x = \mathfrak{cl}(a)$ pour un entier a dans l'ensemble $\{1, \ldots, n-1\}$. Puisque n est premier, a ne possède d'autre diviseur positif commun avec n que 1 et donc a et n sont premiers entre eux. Il existe donc deux entiers relatifs s et t tels que $1 = sa + tn$. En passant aux classes d'équivalence, on obtient : $\mathfrak{cl}(1) = \mathfrak{cl}(s)\mathfrak{cl}(a) + \mathfrak{cl}(t)\mathfrak{cl}(n)$, soit $\mathfrak{cl}(1) = \mathfrak{cl}(s)\mathfrak{cl}(a) + \mathfrak{cl}(t)\mathfrak{cl}(0) = \mathfrak{cl}(s)x$.

On a donc trouvé un inverse de x, à savoir $\mathfrak{cl}(s)$.

Finalement, $\mathbb{Z}/n\mathbb{Z}$ est donc bien un corps commutatif. □

Remarque On retiendra de cette démonstration la technique pratique de calcul de l'inverse d'un élément non nul de $\mathbb{Z}/n\mathbb{Z}$: écrire une identité de Bézout entre un représentant de cet élément et n, et redescendre aux classes d'équivalence.

Et voilà, on sait tout. Reste à donner quelques illustrations afin de convaincre de l'utilité de l'introduction de cette notion abstraite.

Exemple 4. Résoudre dans $\mathbb{Z}$ l'équation suivante, d'inconnue x :

$$24x + 5 \equiv 0 \ [137].$$

On peut traiter cet exemple avec ou sans usage de $\mathbb{Z}/137\mathbb{Z}$. Faisons les deux successivement ; on constatera que les énoncés simples sur les propriétés algébriques de $\mathbb{Z}/137\mathbb{Z}$ remplacent avantageusement les techniques, il est vrai elles aussi simples, d'arithmétique classique.

Première résolution (sans $\mathbb{Z}/137\mathbb{Z}$)

Remarquons que 137 est premier, et donc que 137 et 24 sont premiers entre eux ; cherchons à écrire une identité de Bézout entre 137 et 24 ; en utilisant l'algorithme décrit plus haut, on découvre que :

$$1 = 40 \times 24 - 7 \times 137,$$

d'où on déduit (par une simple multiplication par 5) que :

$$5 = 200 \times 24 - 35 \times 137.$$

Reportons cette identité dans l'équation, qui devient donc :

$$24x + 200 \times 24 - 35 \times 137 \equiv 0 \ [137].$$

À son tour, cette équation est équivalente à la condition suivante :

$$24(x + 200) \equiv 0 \ [137],$$

qui signifie que 137 divise $24(x + 200)$, donc, en utilisant le lemme de Gauss puisque 137 et 24 sont premiers entre eux, que 137 divise $x + 200$. Finalement, x est solution si et seulement si $x + 200 \equiv 0$ [137], c'est-à-dire $x \equiv -200$ [137], c'est-à-dire $x \equiv 74$ [137].

Deuxième résolution (avec $\mathbb{Z}/137\mathbb{Z}$)

Remarquons que 137 est premier, et donc que $\mathbb{Z}/137\mathbb{Z}$ est un corps commutatif. Faisons tous les calculs dans ce corps.

L'équation proposée se réécrit $\mathfrak{cl}(24)\mathfrak{cl}(x) + \mathfrak{cl}(5) = \mathfrak{cl}(0)$, soit $\mathfrak{cl}(24)\mathfrak{cl}(x) = -\mathfrak{cl}(5)$, soit $\mathfrak{cl}(x) = -\mathfrak{cl}(5)(\mathfrak{cl}(24))^{-1}$.

Calculons donc $(\mathfrak{cl}(24))^{-1}$; pour cela nous connaissons la bonne méthode : écrire une identité de Bézout entre 24 et 137, à savoir

$$1 = 40 \times 24 - 7 \times 137,$$

puis redescendre aux classes d'équivalence dans $\mathbb{Z}/137\mathbb{Z}$: $\mathfrak{cl}(1) = \mathfrak{cl}(40) \cdot \mathfrak{cl}(24)$, soit : $(\mathfrak{cl}(24))^{-1} = \mathfrak{cl}(40)$.

On en conclut que l'équation proposée équivaut à :

$$\mathfrak{cl}(x) = -\mathfrak{cl}(5)(\mathfrak{cl}(24))^{-1} = -\mathfrak{cl}(5) \times \mathfrak{cl}(40) = -\mathfrak{cl}(200) = \mathfrak{cl}(74) \ .$$

Exemple 5. Résoudre dans $\mathbb{Z}$ l'équation suivante, d'inconnue x :

$$x^4 \equiv 81 \ [73].$$

Là aussi, écrire deux solutions serait possible, mais celle utilisant $\mathbb{Z}/73\mathbb{Z}$ est tellement plus agréable à écrire que l'on s'en contentera.

Tout d'abord, l'équation s'écrit $x^4 - 81 \equiv 0 \ [73]$ et, dans $\mathbb{Z}$,

$$x^4 - 81 = (x^2 - 9)(x^2 + 9) = (x - 3)(x + 3)(x^2 + 9).$$

Dans $\mathbb{Z}/73\mathbb{Z}$, l'équation s'écrit donc

$$(\mathfrak{cl}(x) - \mathfrak{cl}(3))(\mathfrak{cl}(x) + \mathfrak{cl}(3))(\mathfrak{cl}(x)^2 + \mathfrak{cl}(9)) = \mathfrak{cl}(0).$$

Mais $\mathfrak{cl}(9) = -\mathfrak{cl}(64)$ donc

$$\mathfrak{cl}(x)^2 + \mathfrak{cl}(9) = \mathfrak{cl}(x)^2 - \mathfrak{cl}(64) = (\mathfrak{cl}(x) - \mathfrak{cl}(8))(\mathfrak{cl}(x) + \mathfrak{cl}(8)).$$

Finalement, en utilisant $\mathfrak{cl}(8) = -\mathfrak{cl}(65)$ et $\mathfrak{cl}(3) = -\mathfrak{cl}(70)$, on voit que l'équation de départ s'écrit

$$(\mathfrak{cl}(x) - \mathfrak{cl}(3))(\mathfrak{cl}(x) - \mathfrak{cl}(70))(\mathfrak{cl}(x) - \mathfrak{cl}(8))(\mathfrak{cl}(x) - \mathfrak{cl}(65)) = \mathfrak{cl}(0),$$

soit $\mathfrak{cl}(x) = \mathfrak{cl}(3)$ ou $\mathfrak{cl}(x) = \mathfrak{cl}(8)$ ou $\mathfrak{cl}(x) = \mathfrak{cl}(65)$ ou $\mathfrak{cl}(x) = \mathfrak{cl}(70)$, car $\mathbb{Z}/73\mathbb{Z}$ est un corps commutatif, donc intègre.

Les solutions de l'équation proposée sont donc

$$x \equiv 3 \ [73] \text{ ou } x \equiv 8 \ [73] \text{ ou } x \equiv 65 \ [73] \text{ ou } x \equiv 70 \ [73].$$

Exemple 6. Résoudre dans $\mathbb{Z}$ l'équation suivante, d'inconnue x :

$$x^{17} \equiv 3 \ [19].$$

Là encore, on ne saurait trop recommander le passage dans $\mathbb{Z}/19\mathbb{Z}$. L'équation s'écrit dès lors : $\mathfrak{cl}(x)^{17} = \mathfrak{cl}(3)$. Notons a l'inconnue auxiliaire $a = \mathfrak{cl}(x)$ et remarquons que $\mathfrak{cl}(0)^{17} \neq \mathfrak{cl}(3)$. Il suffit donc de résoudre $a^{17} = \mathfrak{cl}(3)$ dans $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$.

Mais, si $a \neq \mathfrak{cl}(0)$, alors $a^{17} = \mathfrak{cl}(3)$ si et seulement si $a^{18} = \mathfrak{cl}(3)a$. Maintenant, pour tout a dans le groupe multiplicatif $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$, on sait que l'ordre de a, qui est le nombre d'éléments du groupe $\langle a \rangle$, divise le nombre d'éléments de $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$, c'est-à-dire 18.

Ainsi, pour tout élément a de $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$, $a^{18} = \mathfrak{cl}(1)$. L'équation étudiée se simplifie donc grandement en $\mathfrak{cl}(1) = \mathfrak{cl}(3)a$, c'est-à-dire $a = (\mathfrak{cl}(3))^{-1}$. Sa résolution se ramène donc à la recherche de l'inverse de $\mathfrak{cl}(3)$ dans $\mathbb{Z}/19\mathbb{Z}$; on écrit alors une relation de Bézout : $13 \times 3 - 2 \times 19 = 1$ et on en déduit que $(\mathfrak{cl}(3))^{-1} = \mathfrak{cl}(13)$.

Finalement les solutions de l'équation initiale sont donc

$$x \equiv 13 \ [19].$$

Exemple 7. Résoudre dans $\mathbb{Z}$ l'équation suivante, d'inconnue x :

$$x^{14} \equiv 1 \ [19].$$

Ce sont les mêmes idées que dans l'exemple précédent qui font marcher cet exercice, en un peu plus astucieux encore.

Comme dans l'exemple prédédent, on commence par passer dans $\mathbb{Z}/19\mathbb{Z}$, où l'équation s'écrit dès lors : $\mathfrak{cl}(x)^{14} = \mathfrak{cl}(1)$. On note $a = \mathfrak{cl}(x)$, on remarque que $\mathfrak{cl}(0)$ n'est pas solution, et on décide donc de résoudre $a^{14} = \mathfrak{cl}(1)$ dans $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$.

Maintenant, on remarque que pour tout a de $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$, dire que $a^{14} = \mathfrak{cl}(1)$ équivaut à dire que l'ordre de a divise 14. Par ailleurs, comme dans l'exemple précédent, pour tout élément a de $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$, l'ordre de a divise 18. Ainsi, l'ordre de a divise 14 si et seulement s'il divise 14 et 18, donc si et seulement s'il divise $\text{pgcd}(14, 18) = 2$.

On a donc montré que pour tout a de $(\mathbb{Z}/19\mathbb{Z}) \setminus \{\mathfrak{cl}(0)\}$, $a^{14} = \mathfrak{cl}(1)$ si et seulement si $a^2 = \mathfrak{cl}(1)$.

Cette nouvelle équation est alors très facile à résoudre : $a^2 = \mathfrak{cl}(1)$ si et seulement si $(a + \mathfrak{cl}(1))(a - \mathfrak{cl}(1)) = \mathfrak{cl}(0)$ si et seulement si $a = \mathfrak{cl}(1)$ ou $a = -\mathfrak{cl}(1) = \mathfrak{cl}(18)$.

Les solutions de l'équation initiale sont donc

$$x \equiv 1 \ [19] \text{ ou } x \equiv 18 \ [19].$$

2 Entraînement

2.1 Vrai ou Faux

Vrai-Faux 1. Étant donnés cinq nombres entiers consécutifs, on trouve toujours parmi eux (vrai ou faux et pourquoi) :

1. ☒ au moins deux multiples de 2.
2. ☒ au plus trois nombres pairs.
3. ☐ au moins deux multiples de 3.
4. ☒ exactement un multiple de 5.
5. ☐ au moins un multiple de 6.
6. ☐ au moins un nombre premier.

Vrai-Faux 2. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ 60 a plus de diviseurs que 100.
2. ☐ 60 a moins de diviseurs que 90.
3. ☒ 60 a moins de diviseurs que 120.
4. ☒ si un entier divise 60, alors il divise 120.
5. ☐ si un entier strictement inférieur à 60 divise 60, alors il divise 90.
6. ☒ si un nombre premier divise 120, alors il divise 60.

Vrai-Faux 3. On veut constituer la somme exacte de 59 € seulement à l'aide de pièces de 2 € et de billets de 5 €. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ Il y a au plus 22 pièces de 2 €.
2. ☐ Il peut y avoir exactement 10 pièces de 2 €.
3. ☒ Il peut y avoir exactement 12 pièces de 2 €.
4. ☐ Il peut y avoir un nombre pair de billets de 5 €.
5. ☒ Il y a au moins un billet de 5 €.

Vrai-Faux 4. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☐ Si un nombre est divisible par 9, alors il est divisible par 6.
2. ☒ Si un nombre est divisible par 100, alors il est divisible par 25.
3. ☐ Si un nombre est divisible par 2 et par 3, alors il est divisible par 12.
4. ☒ Si un nombre est divisible par 10 et par 12, alors il est divisible par 15.
5. ☐ Si un nombre est divisible par 6 et par 8, alors il est divisible par 48.
6. ☐ Le produit des entiers de 3 à 10 est divisible par 1000.
7. ☒ Le produit des entiers de 3 à 10 est divisible par 1600.
8. ☒ Si la somme des chiffres d'un entier en écriture décimale vaut 39, alors il est divisible par 3 mais pas par 9.
9. ☐ Si la somme des chiffres d'un entier en écriture décimale vaut 18, alors il est divisible par 6 et par 9.

Vrai-Faux 5. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☐ Si un entier est divisible par deux entiers, alors il est divisible par leur produit.
2. ☒ Si un entier est divisible par deux entiers premiers entre eux, alors il est divisible par leur produit.

3. ☒ Si un entier est divisible par deux entiers, alors il est divisible par leur ppcm.
4. ☐ Si un nombre divise le produit de deux entiers, alors il divise au moins un de ces deux entiers.
5. ☒ Si un nombre premier divise le produit de deux entiers, alors il divise au moins un de ces deux entiers.
6. ☐ Si un entier est divisible par deux entiers, alors il est divisible par leur somme.
7. ☒ Si un entier divise deux entiers, alors il divise leur somme.
8. ☒ Si deux entiers sont premiers entre eux, alors chacun d'eux est premier avec leur somme.
9. ☐ Si deux entiers sont premiers entre eux, alors chacun d'eux est premier avec leur produit.
10. ☒ Si deux entiers sont premiers entre eux, alors leur somme et leur produit sont premiers entre eux.

Vrai-Faux 6. Soient a, b, d trois entiers. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ Si d divise a et b, alors d divise leur pgcd.
2. ☐ S'il existe deux entiers u et v tels que $au + bv = d$, alors $d = \text{pgcd}(a, b)$.
3. ☐ S'il existe deux entiers u et v tels que $au + bv = d$, alors d divise $\text{pgcd}(a, b)$.
4. ☒ S'il existe deux entiers u et v tels que $au + bv = d$, alors $\text{pgcd}(a, b)$ divise d.
5. ☐ Si $\text{pgcd}(a, b)$ divise d, alors il existe un couple d'entiers (u, v) unique, tel que $au + bv = d$.
6. ☒ L'entier d est un multiple de $\text{pgcd}(a, b)$ si et seulement si il existe un couple d'entiers (u, v), tel que $au + bv = d$.

Vrai-Faux 7. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ Si un entier est congru à 0 modulo 6, alors il est divisible par 6.
2. ☐ Si le produit de deux entiers est congru à 0 modulo 6 alors l'un des deux est multiple de 6.
3. ☒ Si un entier est congru à 5 modulo 6 alors toutes ses puissances paires sont congrues à 1 modulo 6.
4. ☒ Si deux entiers sont congrus à 4 modulo 6, alors leur somme est congrue à 2 modulo 6.
5. ☐ Si deux entiers sont congrus à 4 modulo 6, alors leur produit est congru à 2 modulo 6.
6. ☒ Si un entier est congru à 4 modulo 6 alors toutes ses puissances sont aussi congrues à 4 modulo 6.

Vrai-Faux 8. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ Si le produit de deux entiers est congru à 0 modulo 5 alors l'un des deux est multiple de 5.
2. ☒ Si un entier est congru à 2 modulo 5 alors sa puissance quatrième est congrue à 1 modulo 5.
3. ☐ Si deux entiers sont congrus à 2 modulo 5, alors leur somme est congrue à 1 modulo 5.
4. ☒ Pour tout entier, il existe un entier tel que le produit des deux soit congru à 1 modulo 5.
5. ☐ Aucun entier n'est tel que son carré soit congru à -1 modulo 5.
6. ☒ Aucun entier n'est tel que son carré soit congru à 2 modulo 5.
7. ☐ La puissance quatrième d'un entier quelconque est toujours congrue à 1 modulo 5.
8. ☒ La puissance quatrième d'un entier non multiple de 5 est toujours congrue à 1 modulo 5.

2.2 Exercices

Exercice 1. Soit $n \in \mathbb{N}$ un entier.

1. Démontrer que si n n'est divisible par aucun entier inférieur ou égal à $\sqrt{n}$, alors n est premier.
2. Démontrer que les nombres $n! + 2$, $n! + 3$,..., $n! + n$ ne sont pas premiers.
3. En déduire que pour tout n, il existe n entiers consécutifs non premiers.

Exercice 2. Le premier janvier 2007 était un lundi. Calculer quel jour de la semaine sera le

1. 2 juillet 2007
2. 15 janvier 2008
3. 19 mars 2008 (attention, 2008 est une année bissextile)
4. 14 juillet 2010
5. 26 août 2011

Exercice 3. On choisit un nombre entier, on le divise par 7 et on trouve un reste égal à 5. On divise à nouveau le quotient obtenu par 7, on trouve un reste égal à 3 et un quotient égal à 12. Quel était le nombre de départ ?

Exercice 4. On donne l'égalité suivante.

$$96\ 842 = 256 \times 375 + 842$$

Déterminer, sans effectuer la division, le quotient et le reste de la division euclidienne de 96 842 par 256 et par 375.

Exercice 5. On donne les deux égalités suivantes.

$$3379026 = 198765 \times 17 + 21, \qquad 609806770 = 35870986 \times 17 + 8.$$

On s'intéresse au nombre entier $N = 3379026 \times 609806770$. Quel est le reste de la division euclidienne de N par 17 ?

Exercice 6. Quel est le plus petit entier naturel, qui divisé par 8, 15, 18 et 24 donne pour restes respectifs 7, 14, 17 et 23 ?

Exercice 7. Dans une UE de maths à l'université Joseph Fourier, il y a entre 500 et 1000 inscrits. L'administration de l'université a remarqué qu'en les répartissant en groupes de 18, ou bien en groupes de 20, ou bien aussi en groupes de 24, il restait toujours 9 étudiants. Quel est le nombre d'inscrits ?

Exercice 8. Soient a et b deux entiers tels que $1 \leqslant a < b$.

1. Soient q_1 et r_1 (respectivement : q_2 et r_2) le quotient et le reste de la division euclidienne de a (respectivement : b) par $b - a$. Démontrer que
$$r_1 = r_2 \quad \text{et} \quad q_2 = q_1 + 1$$
2. On note q le quotient de la division euclidienne de $b - 1$ par a. Soit $n \geqslant 0$ un entier. Exprimer en fonction de q et n le quotient de la division euclidienne de $ba^n - 1$ par a^{n+1}.
3. Soit d le pgcd de a et b. Déterminer le pgcd de A et B, où :
$$A = 15a + 4b \quad \text{et} \quad B = 11a + 3b$$
4. Montrer que $d = \text{pgcd}(a + b, \text{ppcm}(a, b))$.
5. Démontrer que si $d = 1$, alors pour tout $m, n \in \mathbb{N}$, a^m et b^n sont premiers entre eux.
6. En déduire que pour tout $n \in \mathbb{N}$, le pgcd de a^n et b^n est d^n.

Exercice 9. Soient a, b et c trois entiers relatifs.

1. Montrer que $\text{pgcd}(ca, cb) = |c| \times \text{pgcd}(a, b)$.
2. Montrer que si $\text{pgcd}(a, b) = 1$ et si c divise a, alors $\text{pgcd}(c, b) = 1$.
3. Montrer que $\text{pgcd}(a, bc) = 1$ si et seulement si $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$.

4. Montrer que si $\text{pgcd}(b,c)=1$ alors $\text{pgcd}(a,bc)=\text{pgcd}(a,b)\text{pgcd}(a,c)$.

Exercice 10. Soient $a,b\in\mathbb{N}$ deux entiers tels que $0<a<b$.

1. Démontrer que si a divise b, alors pour tout $n\in\mathbb{N}^*$, n^a-1 divise n^b-1.
2. Démontrer que le reste de la division euclidienne de n^b-1 par n^a-1 est n^r-1, où r est le reste de la division euclidienne de b par a.
3. Démontrer que le pgcd de n^b-1 et n^a-1 est n^d-1, où d est le pgcd de a et b.

Exercice 11. Soit p un nombre premier.

1. On rappelle que pour tout $k=1,\dots,p-1$,
$$k\binom{p}{k}=p\binom{k-1}{p-1}$$
En déduire que pour tout $k=1,\dots,p-1$, $\binom{p}{k}$ est divisible par p.
2. Grâce à la formule du binôme, en déduire que pour tous entiers relatifs a et b dans $\mathbb{Z}$, $(a+b)^p-a^p-b^p$ est divisible par p.
3. Démontrer par récurrence que pour tout $a\in\mathbb{N}$, a^p-a est divisible par p (ce résultat est connu sous le nom de « petit théorème de Fermat »).

Exercice 12. Soit n un entier relatif. On pose $a=2n+3$ et $b=5n-2$.

1. Calculer $5a-2b$. En déduire le pgcd de a et b en fonction de n.
2. Procéder de même pour exprimer en fonction de n le pgcd de $2n-1$ et $9n+4$.

Exercice 13. Donner la décomposition en facteurs premiers des entiers suivants.

60 ; 360 ; 2400 ; 4675 ; 9828 ; 15200 ; 45864 ; 792792.

Exercice 14. On considère les couples d'entiers (a,b) suivants.

- $a=60$, $b=84$
- $a=360$, $b=240$
- $a=160$, $b=171$
- $a=360$, $b=345$
- $a=325$, $b=520$
- $a=720$, $b=252$
- $a=955$, $b=183$
- $a=1665$, $b=1035$
- $a=18480$, $b=9828$

Pour chacun de ces couples :

1. Calculer $\text{pgcd}(a,b)$ par l'algorithme d'Euclide.
2. En déduire une identité de Bézout.

3. Calculer $\text{ppcm}(a, b)$.
4. Déterminer l'ensemble des couples (u, v) d'entiers relatifs tels que :

$$au + bv = \text{pgcd}(a, b) \ .$$

5. Donner la décomposition en facteurs premiers de a et b.
6. En déduire la décomposition en facteurs premiers de $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$, et retrouver les résultats des questions 1 et 3.

Exercice 15. Soit n un entier naturel.

1. Démontrer qu'il existe deux entiers a_n et b_n tels que :

$$(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$$

2. Soient u et v deux entiers. Vérifier que

$$(v - u)a_{n+1} + (2u - v)b_{n+1} = ua_n + vb_n$$

3. Démontrer par récurrence que pour tout n, a_n et b_n sont premiers entre eux.
4. Démontrer que a_n est premier avec b_{n+1}, pour tout n.
5. Démontrer que b_n est premier avec a_{n+1} et avec b_{n+1}, pour tout n.

Exercice 16. Soit a un entier naturel impair.

1. Démontrer que $a^2 \equiv 1\ [8]$.
2. Démontrer que $a^4 \equiv 1\ [16]$.
3. Démontrer que si $a \equiv 1\ [2^n]$, alors $a^2 \equiv 1\ [2^{n+1}]$.
4. Démontrer par récurrence que pour tout $n \geqslant 3$,

$$a^{2^{n-2}} \equiv 1\ [2^n]$$

Exercice 17. Soient a et b deux entiers naturels premiers entre eux.

1. Démontrer que pour tout entier relatif n, il existe un couple d'entiers relatifs (s, t) tels que $n = sa + tb$.
2. Soit q un entier strictement plus grand que a, et r un entier tel que $0 \leqslant r \leqslant a$. Vérifier que $qa + r = (q - r)a + r(a + 1)$. En déduire que pour tout entier $n \geqslant a(a+1)$, il existe un couple d'entiers *naturels* (s, t) tels que $n = sa+t(a+1)$.
3. En utilisant une identité de Bézout, montrer qu'il existe deux entiers naturels consécutifs, l'un multiple de a, l'autre multiple de b.
4. Déduire des questions précédentes qu'il existe un entier n_0 tel que pour tout $n \geqslant n_0$, il existe un couple d'entiers *naturels* (s, t) tels que $n = sa + tb$.

5. Au rugby, on peut marquer un essai (5 points), une transformation suivant un essai (2 points), un drop (3 points) ou une pénalité (3 points). Montrer que le nombre de points qu'une équipe de rugby ne peut pas atteindre à la fin d'un match est fini. Quel est le plus grand score non réalisable ?

Exercice 18. Calculer le reste de la division par 3, par 4, par 5, par 6, par 7, des nombres suivants.

$$314^{314} \quad ; \quad 999^{999} \quad ; \quad 2007^{2007} \quad ; \quad 31416^{31416}$$

Exercice 19.

1. Montrer que 7 divise $2222^{5555} + 5555^{2222}$
2. Montrer que 11 divise
$$5^{10^{5^{10^{5^{10}}}}} + 10^{5^{10^{5^{10^{5}}}}}$$

Exercice 20. Soient a, b, c trois entiers relatifs quelconques.

1. Démontrer que $a + b + c$ divise $a^3 + b^3 + c^3 - 3abc$.
2. Démontrer que si 7 divise $a^3 + b^3 + c^3$, alors 7 divise abc.

Exercice 21. Démontrer que chacune des relations suivantes est vraie pour tout $n \in \mathbb{N}$.

1. 5 divise $2^{2n+1} + 3^{2n+1}$
2. 6 divise $n^3 - n$
3. 6 divise $5n^3 + n$
4. 6 divise $4(4^{2n} - 1)$
5. 7 divise $3^{2n+1} + 2^{n+2}$
6. 8 divise $5^n + 2 \times 3^{n-1} + 1$
7. 9 divise $4^n - 1 - 3n$
8. 11 divise $3^{n+3} - 4^{4n+2}$
9. 11 divise $2^{6n+3} + 3^{2n+1}$
10. 16 divise $5^n - 1 - 4n$
11. 17 divise $2^{6n+3} + 3^{4n+2}$
12. 17 divise $2^{7n+1} + 3^{2n+1} + 5^{10n+1} + 7^{6n+1}$
13. 18 divise $2^{2n+2} + 24n + 14$
14. 19 divise $2^{3n+4} + 3^{3n+1}$
15. 19 divise $2^{2^{6n+2}} + 3$
16. 21 divise $2^{4^{n+1}} + 5$

Exercice 22. Déterminer l'ensemble des entiers relatifs x, solutions des équations suivantes.

1. $35x - 7 \equiv 0$ [4]
2. $22x - 33 \equiv 0$ [5]
3. $2x + 3 \equiv 0$ [7]
4. $9x + 5 \equiv 0$ [8]
5. $x^2 + x + 7 \equiv 0$ [13]
6. $x^2 \equiv 1$ [16]
7. $x^4 \equiv 7$ [11]
8. $x^2 + x + 7 \equiv 0$ [13]
9. $x^2 - 4x + 3 \equiv 0$ [12]
10. $x^2 + (x+1)^2 + (x+3)^2 \equiv 0$ [10]

Exercice 23. Déterminer l'ensemble des entiers naturels x, solutions des équations suivantes.

1. $2^{2x} + 2^x + 1 \equiv 0$ [21]
2. $2^{2x} + 2^x + 1 \equiv 0$ [7]
3. $3^x + 4x + 1 \equiv 0$ [8]
4. $1^x + 2^x + 3^x + 4^x \equiv 0$ [5]

Exercice 24. Dans tout l'exercice, a et b sont deux entiers naturels.

1. Démontrer que
$$a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a,b)\mathbb{Z} \ .$$
2. Démontrer que a divise b si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$.
3. Démontrer que $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous groupe de $\mathbb{Z}$.
4. Démontrer que $a\mathbb{Z} \cup b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ si et seulement si a divise b ou b divise a.

Exercice 25.

1. Écrire l'ensemble des multiples de $\mathfrak{cl}(x)$ dans $\mathbb{Z}/5\mathbb{Z}$, pour $x = 0, \ldots, 4$.
2. Écrire l'ensemble des multiples de $\mathfrak{cl}(x)$ dans $\mathbb{Z}/6\mathbb{Z}$, pour $x = 0, \ldots, 5$.
3. Écrire l'ensemble des multiples de $\mathfrak{cl}(x)$ dans $\mathbb{Z}/8\mathbb{Z}$, pour $x = 0, \ldots, 7$.
4. Soient n et x deux entiers naturels. Démontrer que les trois propositions suivantes sont équivalentes.
   (a) $\mathfrak{cl}(x)$ admet un inverse pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.
   (b) x et n sont premiers entre eux.
   (c) tout élément de $\mathbb{Z}/n\mathbb{Z}$ est multiple de $\mathfrak{cl}(x)$ dans $\mathbb{Z}/n\mathbb{Z}$.
5. Calculer l'inverse de $\mathfrak{cl}(4)$ dans $\mathbb{Z}/9\mathbb{Z}$.

6. Calculer l'inverse de $\mathfrak{cl}(8)$ dans $\mathbb{Z}/15\mathbb{Z}$.
7. Soit n un entier *non premier*. Montrer qu'il existe deux éléments de $\mathbb{Z}/n\mathbb{Z}$ dont le produit est $\mathfrak{cl}(0)$. En déduire que $(n-1)!$ est divisible par n.
8. Soit p un entier *premier*. Montrer que pour tout entier $x = 2, \ldots, p-2$ il existe un entier $y = 2, \ldots, p-2$, différent de x, tel que le produit xy soit congru à 1 modulo p. En déduire que $(p-1)! + 1$ est divisible par p. (Bravo ! vous venez de démontrer le *théorème de Wilson*.)

2.3 QCM

Donnez-vous une heure pour répondre à ce questionnaire. Les 10 questions sont indépendantes. Pour chaque question 5 affirmations sont proposées, parmi lesquelles 2 sont vraies et 3 sont fausses. Pour chaque question, cochez les 2 affirmations que vous pensez vraies. Chaque question pour laquelle les 2 affirmations vraies sont cochées rapporte 2 points.

Question 1. Étant donnés 7 nombres entiers consécutifs, on trouve toujours parmi eux :

A au moins 4 multiples de 2.
B au moins un multiple de 6.
C au moins un nombre premier.
D au moins 2 multiples de 3.
E au moins deux multiples de 4.

Question 2. Soit n un entier.

A Si n est divisible par 4, alors n a au moins 4 diviseurs.
B Si n est divisible par 8, alors n a au moins 4 diviseurs.
C Si n a au moins 3 diviseurs, alors n n'est pas premier.
D Si n a au moins 3 diviseurs, alors n est pair.
E Si n est pair, alors n a au moins 3 diviseurs.

Question 3. On veut constituer la somme exacte de 63 € seulement à l'aide de pièces de 2 € et de billets de 5 €.

A Il y a au plus 31 pièces de 2 €.
B Il peut y avoir exactement 10 pièces de 2 €.
C Il peut y avoir exactement 6 billets de 5 €.
D Il peut y avoir exactement 19 pièces de 2 €.
E Il peut y avoir 12 billets de 5 €.

Question 4.

A Si un nombre est divisible par 6 et par 9, alors il est divisible par 12.
B Si un nombre est divisible par 6 et par 4, alors il est divisible par 24.

C Si un nombre est divisible par 9 et par 4, alors il est divisible par 36.
D Si un nombre est divisible par 36 alors il est divisible par 24.
E Si un nombre est divisible par 24, alors il est divisible par 12.

Question 5. Soient a et b deux entiers quelconques.
A Si a divise b, alors $\text{pgcd}(a,b) = a$.
B Si un nombre divise $\text{ppcm}(a,b)$, alors il divise a ou b.
C Si $b = \text{pgcd}(a,b) \times a$ alors $b = a^2$.
D Si $a^2 = \text{pgcd}(a,b) \times b$, alors $a^2 = b$.
E Si $\text{ppcm}(a,b) \times a$ divise ab alors $b = 1$.

Question 6. Soient a et b deux entiers quelconques.
A Si a et b sont premiers entre eux, alors tout multiple commun de a et b est multiple de ab.
B Si a et b sont pairs, alors $\text{ppcm}(a,b) = ab/4$.
C Si un entier est divisible à la fois par a et b, il est divisible par $2a - 3b$.
D L'entier $a^2 - b^2$ est divisible par $\text{pgcd}(a,b)$.
E L'entier $a^2 + b^2$ est divisible par $\text{ppcm}(a,b)$.

Question 7. Soient a et b deux entiers premiers entre eux.
A Les entiers $a + b$ et $a - b$ sont premiers entre eux.
B Les entiers $a + 2b$ et $2a + b$ sont premiers entre eux.
C Les entiers ab et $a - b$ sont premiers entre eux.
D Les entiers a^2b et ab^2 sont premiers entre eux.
E Les entiers a et b sont chacun premiers avec $a + b$ et avec $a - b$.

Question 8. Soient a, b, d trois entiers.
A S'il existe 2 entiers u et v tels que $au + bv = d$, alors $d = \text{pgcd}(a,b)$.
B S'il existe 2 entiers u et v tels que $au + bv = d$, alors d divise a et b.
C S'il existe 2 entiers u et v tels que $au + bv = d$, alors tout diviseur commun de a et b divise d.
D Si $d = \text{pgcd}(a,b)$, alors il existe un couple unique d'entiers (u,v) tel que $au + bv = d$.
E Si a et b sont premiers entre eux, alors pour tout entier k, il existe deux entiers u et v tels que $au + bv = dk$.

Question 9.
A Si un entier est congru à 0 modulo 12, alors, il est divisible par 9.
B Si le produit de deux entiers est congru à 0 modulo 12, alors l'un des deux au moins est pair.
C Si le produit de deux entiers est congru à 1 modulo 12, alors l'un des deux au moins est pair.

D Si le produit de deux entiers est congru à 1 modulo 12, alors ces deux entiers sont congrus entre eux modulo 12.

E Si on divise par 12 le produit de 7 et d'un entier quelconque, on n'obtient jamais un reste égal à 1.

Question 10.

A Si un entier est congru à 6 modulo 7, alors sa puissance troisième est congrue à 1 modulo 7.

B Aucun entier n'est tel que son carré soit congru à -3 modulo 7.

C La puissance troisième de tout entier est congrue à 0 ou 1 modulo 7.

D Si le produit de deux entiers est congru à 0 modulo 7, alors l'un des deux au moins est multiple de 7.

E Si un entier est congru à 2 modulo 7, alors sa puissance neuvième est congrue à 1 modulo 7.

Réponses : 1–BD 2–BC 3–AD 4–CE 5–AC 6–AD 7–CE 8–CE 9–BD 10–DE

2.4 Devoir

Essayez de bien rédiger vos réponses, sans vous reporter ni au cours, ni au corrigé. Si vous souhaitez vous évaluer, donnez-vous deux heures ; puis comparez vos réponses avec le corrigé et comptez un point pour chaque question à laquelle vous aurez correctement répondu.

Questions de cours :

1. Soit a un entier. Montrer que l'ensemble des multiples entiers de a, noté $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
2. Soit G un sous-groupe de $\mathbb{Z}$. Montrer qu'il existe un entier positif ou nul a tel que $G = a\mathbb{Z}$.
3. Soient a et b deux entiers non nuls. Montrer qu'il existe un entier strictement positif d tel que :
$$\{\, sa + tb\,,\ s,t \in \mathbb{Z}\,\} = d\mathbb{Z}\ .$$
4. Montrer que tout entier n qui divise à la fois a et b est un diviseur de d.
5. Soient a, b deux entiers premiers entre eux. Montrer qu'il existe deux entiers s et t tels que $sa + tb = 1$ (identité de Bézout). En déduire que si c est un troisième entier tel que a divise le produit bc, alors a divise c (lemme de Gauss).

Exercice 1 :

1. Démontrer par récurrence que pour tout $n \in \mathbb{N}$, il existe deux nombres entiers a_n et b_n tels que $(2+\sqrt{3})^n = a_n + b_n\sqrt{3}$.
2. Soient u et v deux entiers et $n \in \mathbb{N}$. Vérifier l'égalité suivante :
$$(2u - v)a_{n+1} + (2v - 3u)b_{n+1} = ua_n + vb_n\ .$$

3. Démontrer par récurrence que pour tout n, a_n et b_n sont premiers entre eux.
4. Démontrer que pour tout $n \in \mathbb{N}$, b_n et b_{n+1} sont premiers entre eux.
5. Démontrer que pour tout $n \in \mathbb{N}$, soit a_n et b_{n+1} sont premiers entre eux, soit leurs diviseurs communs sont 1 et 2.

Exercice 2 : On pose $a = 960$ et $b = 528$.

1. Calculer $\text{pgcd}(a, b)$ par l'algorithme d'Euclide, et en déduire une identité de Bézout. Calculer $\text{ppcm}(a, b)$.
2. Déterminer l'ensemble des couples (u, v) d'entiers relatifs tels que :

$$au + bv = \text{pgcd}(a, b) \ .$$

3. Donner la décomposition en facteurs premiers de a et b.
4. En déduire la décomposition en facteurs premiers de $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$, et retrouver les résultats de la question 1.

Exercice 3 :

1. Montrer que pour tout $n \in \mathbb{N}$, $8^{2n} \equiv 1\ [21]$.
2. En déduire que pour tout $n \in \mathbb{N}$, $2^{4^{n+1}} + 5 \equiv 0\ [21]$.
3. Calculer les restes de la division par 21 de $64^{16^{8^{4^2}}}$, $2^{16^{8^{4^2}}}$ et $32^{16^{8^{4^2}}}$.

Exercice 4 :

1. Résoudre dans $\mathbb{Z}$ l'équation $18x - 31 \equiv 0\ [7]$.
2. Résoudre dans $\mathbb{Z}$ l'équation $18x^2 - 31x + 11 \equiv 0\ [7]$.
3. Résoudre dans $\mathbb{Z}$ l'équation $18x^3 - 31x^2 + 11x - 45 \equiv 0\ [7]$.

2.5 Corrigé du devoir

Questions de cours :

1. Il suffit de vérifier que l'ensemble des multiples de a est stable par addition et passage à l'opposé. Si s et t sont deux entiers, alors $sa - ta = (s - t)a$ est bien un multiple de a, d'où le résultat.
2. Le groupe G peut être réduit à $\{0\} = 0\mathbb{Z}$. Sinon, il contient un élément non nul, et son opposé. Il contient donc forcément un élément strictement positif. Donc $G \cap \mathbb{N}^*$ est non vide. Notons a le plus petit élément de G *strictement positif*. Puisque G est un sous-groupe de $\mathbb{Z}$, $a\mathbb{Z} \subset G$. Nous voulons montrer que $G \subset a\mathbb{Z}$. Soit b un élément quelconque de G. Effectuons la division euclidienne de b par a : $b = aq + r$, avec $r \in \{0, \ldots, a - 1\}$. Or b, aq et $r = b - aq$ appartiennent à G. Puisque a est le plus petit élément strictement positif de G, $r = 0$, donc $b = aq \in a\mathbb{Z}$.

3. D'après la question précédente, il suffit de vérifier que l'ensemble proposé est un sous-groupe de $\mathbb{Z}$, non réduit à $\{0\}$.

$$G = \{\, sa + tb\,,\ s, t \in \mathbb{Z}\,\}\ .$$

Observons que G n'est pas réduit à $\{0\}$ car a et b sont non nuls. Soient s, s', t, t' 4 entiers :

$$(sa + tb) - (s'a + t'b) = (s - s')a + (t - t')b \in G\ .$$

Donc G est bien un sous-groupe de $\mathbb{Z}$. Donc $G = d\mathbb{Z}$, où d est le plus petit élément strictement positif de G.

4. Soit k un diviseur commun à a et b : k divise tout entier de la forme $sa+tb$, donc tout élément de G, en particulier d. Donc d est le pgcd de a et b.

5. Si a et b sont premiers entre eux, leur pgcd est 1 et le groupe G de la question 3 est $\mathbb{Z}$ tout entier. Donc il existe deux entiers s et t tels que $sa+tb = 1$. Multiplions les deux membres par c : $sac + tbc = c$. Or a divise ac et bc, donc $sac + tbc$. D'où le résultat.

Exercice 1 :

1. La propriété est vraie pour $n = 0$: $a_0 = 2$ et $b_0 = 1$. Supposons-la vraie pour $n \in \mathbb{N}$.

$$\begin{aligned}(2+\sqrt{3})^{n+1} &= (2+\sqrt{3})(a_n + b_n\sqrt{3}) \\ &= (2a_n + 3b_n) + (a_n + 2b_n)\sqrt{3}\ .\end{aligned}$$

Donc la propriété est vraie pour $n + 1$, avec :

$$a_{n+1} = 2a_n + 3b_n \quad \text{et} \quad b_{n+1} = a_n + 2b_n\ .$$

2. Il suffit d'utiliser les relations de récurrence donnant a_{n+1} et b_{n+1} en fonction de a_n et b_n.

$$\begin{aligned}(2u - v)a_{n+1} + (2v - 3u)b_{n+1} &= (2u - v)(2a_n + 3b_n) + (2v - 3u)(a_n + 2b_n) \\ &= ua_n + vb_n\ .\end{aligned}$$

3. La propriété est vraie pour $n = 0$, car $a_0 = 1$ et $b_0 = 1$ sont premiers entre eux. Supposons-la vraie pour n : il existe deux entiers u et v tels que $ua_n + vb_n = 1$. D'après la question précédente, $(2u - v)a_{n+1} + (2v - 3u)b_{n+1} = 1$, donc a_{n+1} et b_{n+1} sont premiers entre eux. Donc pour tout $n \in \mathbb{N}$, a_n et b_n sont premiers entre eux.

4. Reprenons la relation donnant b_{n+1} en fonction de a_n et b_n : $b_{n+1} = a_n + 2b_n$. Soit d un entier divisant à la fois b_n et b_{n+1}. Alors d divise a_n. Or le seul diviseur commun de a_n et b_n est 1, d'après la question précédente. Donc le seul diviseur commun à b_n et b_{n+1} est 1 : b_n et b_{n+1} sont premiers entre eux.

5. Soit d un diviseur commun à a_n et b_{n+1}. Alors d divise $b_{n+1}-a_n = 2b_n$. Or puisque d divise a_n, d est premier avec b_n, donc d divise 2, d'après le lemme de Gauss.

Exercice 2 : On pose $a = 960$ et $b = 528$.

1.
$$\begin{array}{rcl|rcl} 960 &=& 528+432 & 48 &=& 5\times 960 - 9\times 528 \\ 528 &=& 432\times 1+96 & 48 &=& -4\times 528 + 5\times 432 \\ 432 &=& 96\times 4+48 & 48 &=& 432 - 4\times 96 \\ 96 &=& 48\times 2+0 & & & \end{array}$$

   Le pgcd de a et b est 48. Le ppcm est leur produit divisé par 48, soit 10560.

2. Posons $a' = a/\text{pgcd}(a,b) = 20$ et $b' = b/\text{pgcd}(a,b) = 11$. Deux entiers u et v vérifient $au + bv = \text{pgcd}(a,b)$ si et seulement si $a'u + b'v = 1$. Par l'algorithme d'Euclide, nous avons déterminé deux entiers $u_0 = 5$ et $v_0 = -9$ tels que $au_0 + bv_0 = \text{pgcd}(a,b)$, soit $a'u_0 + b'v_0 = 1$. Deux entiers u et v vérifient $a'u + b'v = 1$ si et seulement si $a'(u-u_0) + b'(v-v_0) = 0$. Or a' et b' sont premiers entre eux. Par le lemme de Gauss, a' divise $(v-v_0)$ et b' divise $(u-u_0)$. Donc deux entiers u et v vérifient $a'u + b'v = 1$ si et seulement s'il existe un entier k tel que $u = u_0 + kb'$ et $v = v_0 - ka'$. L'ensemble demandé est donc :

$$\{\,(5+11k, -9-20k)\,,\ k\in\mathbb{Z}\,\}\,.$$

3. On trouve :
$$a = 2^6\times 3\times 5 \quad\text{et}\quad b = 2^4\times 3\times 11\,.$$

4. De la décomposition de a et b en facteurs premiers, on déduit :
$$\text{pgcd}(a,b) = 2^4\times 3 = 48 \quad\text{et}\quad \text{ppcm}(a,b) = 2^6\times 3\times 5\times 11 = 10560\,.$$

Exercice 3 :

1. Le résultat est vrai pour $n = 0$. Il est vrai aussi pour $n = 1$, car $8^2 = 64 = 63+1 \equiv 1$ [21]. Supposons-le vrai pour $n\in\mathbb{N}$. Alors :
$$8^{2(n+1)} = 8^2\,8^{2n} \equiv 1\times 1 \equiv 1\ [21]\,.$$
   Donc pour tout $n\in\mathbb{N}$, $8^{2n}\equiv 1$ [21].

2. Observons que pour tout entier n :
$$2^{4^{n+1}} - 2^{4^n} = 2^{4^n}\left(2^{4^{n+1}-4^n}-1\right) = 2^{4^n}\left(2^{3\times 4^n}-1\right) = 2^{4^n}\left(8^{4^n}-1\right)\,.$$
   Or pour $n\geqslant 1$, 8^{4^n} est une puissance paire de 8, qui d'après la question précédente, est congrue à 1 modulo 21. Donc pour $n\geqslant 1$, $2^{4^{n+1}} \equiv 2^{4^n}$ [21]. Or $2^4+5 = 21\equiv 0$ [21]. Le résultat s'ensuit, par récurrence.

3. On déduit de la première question que :

$$64^{16^{8^{4^2}}} = 8^{2\times 16^{8^{4^2}}} \equiv 1\ [21]\ .$$

On déduit de la deuxième question que :

$$2^{16^{8^{4^2}}} = 2^{4^{2\times 8^{4^2}}} \equiv -5\ [21]\ .$$

Or :

$$64^{16^{8^{4^2}}} = 2^{16^{8^{4^2}}}\ 32^{16^{8^{4^2}}}\ .$$

Donc le reste de la division par 21 de $32^{16^{8^{4^2}}}$ est l'entier r compris entre 0 et 20 tel que $-5r \equiv 1\ [21]$, à savoir $r = 4$.

Exercice 4 :

1. Observons que $18 \equiv 4\ [7]$ et $31 \equiv 3\ [7]$. Le tableau suivant donne les valeurs de $4x$ quand x parcourt $\mathbb{Z}/7\mathbb{Z}$.

x	0	1	2	3	4	5	6
$4x$	0	4	1	5	2	6	3

L'ensemble des solutions de l'équation $18x - 31 \equiv 0\ [7]$ est l'ensemble des entiers congrus à 6 modulo 7.

2. Procédons de même, en observant que $-11 \equiv 3\ [7]$.

x	0	1	2	3	4	5	6
$4x^2$	0	4	2	1	1	2	4
$3x$	0	3	6	2	5	1	4
$4x^2 - 3x$	0	1	3	6	3	1	0

Donc l'ensemble des solutions de l'équation proposée est l'ensemble des entiers congrus à 2 ou à 4 modulo 7.

3. On procède comme dans les questions précédentes, après avoir ramené l'équation proposée à $4x^3 + 4x^2 + 4x \equiv 3\ [7]$.

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6
$4x^3 + 4x^2 + 4x$	0	5	0	2	0	4	3

L'ensemble des solutions est l'ensemble des entiers congrus à 6 modulo 7.

---

3 Compléments

3.1 Le code RSA

3.2 La course aux nombres premiers

3.3 La répartition des nombres premiers