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

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

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 $2 \leqslant k \leq P$, 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 $b \geqslant 1$ un entier strictement positif. Alors il existe un couple (q, r) unique (d'entiers) vérifiant la double condition :*

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

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 $a \geqslant 0$ 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 $a \geqslant 0$.

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 $A = \{c \in \mathbb{N}\,,\ bc \leqslant a\}$. 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 $d \geqslant a + 1$; on a alors $bd \geqslant b(a + 1) \geqslant a + 1 > a$, 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 $bq \leqslant a$. Donc $r = a - bq \geqslant 0$.

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 $1 - b \leqslant 0$, on obtient $a' \geqslant 0$.

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 $0 \leqslant r < b$. 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 $0 \leqslant r_1$ et $r_2 < b$, on déduit que $-b < r_1 - r_2$.

Des conditions $r_1 < b$ et $0 \leqslant r_2$, 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 $a \geqslant 1$ et $b \geqslant 1$ deux entiers. Alors il existe un unique entier $m \geqslant 1$ tel que pour tout entier $c \geqslant 1$,*

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

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

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 $n \geqslant 1$; 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 $0 \leqslant r < m$. 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 $n \geqslant 1$ 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 « $a \geqslant 1$ et $b \geqslant 0$ ».

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 $b \geqslant 0$ l'hypothèse (H_b) suivante :

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

Vérifions (H_0).

Soit a un entier avec $a \geqslant 1$; tout entier $n \geqslant 1$ qui divise a divise aussi $b = 0$ puisque $0n = 0$. Pour tout $n \geqslant 1$, 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 $n \geqslant 1$: n divise a et 0 si et seulement si n divise $sa + t \times 0$.

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

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

Vérifions l'affirmation intermédiaire suivante : pour tout $n \geqslant 1$, 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 $0 \leqslant r < b$) sur l'entier $b \geqslant 1$.

On en déduit qu'il existe deux entiers relatifs s' et t' tels que pour tout $n \geqslant 1$, 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 $n \geqslant 1$, 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 $b \geqslant 0$, donc a fortiori pour tout $b \geqslant 1$, 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 $a \geqslant 1$ et $b \geqslant 1$ 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 $n \geqslant 2$ 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 $n \geqslant 2$ 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 $k \geqslant 1$, $i \geqslant 1$, 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 $1 \leqslant j \leqslant k = i$, $p_j = q_j$ 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 $2 \leqslant k \leqslant n$ 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 $2 \leqslant k \leqslant n$ qui divise $n + 1$. Notons ℓ l'entier $\ell = (n + 1)/k$. Alors $2 \leqslant \ell \leqslant n$ 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 $w \leqslant u + v$ 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 $2 \leqslant m < n$.

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 $b \geqslant 0$ 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 $b \geqslant 0$ 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 $b \geqslant 0$, 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 $1 \leqslant j \leqslant l$, 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 $1 \leqslant j < i$ 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 $\alpha_k \geqslant 1$), 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 $b \geqslant 0$.*

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 $b \geqslant 0$ 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 $b \geqslant 0$ 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 $n \geqslant 1$, n est un multiple commun de a et b si et seulement si n 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 $m \geqslant 0$ 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 $n \geqslant 1$ les équivalences : n est un multiple 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 $d \geqslant 0$ 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 $n \geqslant 1$ 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 $n \geqslant 1$ 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*

$$12345 \equiv 1^4 + 2 \cdot 1^3 + 3 \cdot 1^2 + 4 \cdot 1 + 5 = 1 + 2 + 3 + 4 + 5 = 15,$$

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 $n \geqslant 1$ 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 $n \geqslant 1$, $\mathbb{Z}/n\mathbb{Z}$ 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 $0 \leqslant r < n$, 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 $0 \leqslant a < n$ et $0 \leq b < n$. Des inégalités $0 \leqslant a$ et $b < n$ on déduit que $-n < b - a$; des inégalités $a < n$ et $0 \leqslant b$ 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* $a \leqslant b$.

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 : $x \leqslant y$. Mais on peut aussi écrire $x = \mathfrak{cl}(3)$ et comme précédemment $y = \mathfrak{cl}(2)$. En s'y prenant ainsi, $y \leqslant x$. 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. Ce sera l'exemple de $\mathbb{Z}/5\mathbb{Z}$.

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

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

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

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

Proposition 5. *Pour tout* $n \geqslant 1$, $\mathbb{Z}/n\mathbb{Z}$ *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 $n \geqslant 1$, $\mathbb{Z}/n\mathbb{Z}$ 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, $\mathbb{Z}/1\mathbb{Z}$ 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 27 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 un entier supérieur ou égal à 2.

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. 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 3. 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 4. 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 5. 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 6. 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 7. 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 8. 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 9. 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 10. Soit p un nombre premier.

1. On rappelle que pour tout $k = 1, \ldots, p-1$,
$$k\binom{p}{k} = p\binom{p-1}{k-1}$$
En déduire que pour tout $k = 1, \ldots, p-1$, $\binom{p}{k}$ 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. (Bravo ! Vous venez de démontrer le *Petit Théorème de Fermat.*)

Exercice 11. 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 12. Donner la décomposition en facteurs premiers des entiers suivants.

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

Exercice 13. 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 14. 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 15. 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 16. 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 17. Soient k un entier supérieur ou égal à 2 et $m_1, \ldots, m_k$ des entiers, premiers entre eux deux à deux. Pour tout $i = 1, \ldots, k$, soit $a_i \in \mathbb{Z}/m_i\mathbb{Z}$. On note E l'ensemble des entiers n tels que :

$$\forall i = 1, \ldots, k\ , \quad n \equiv a_i\ [m_i]\ .$$

1. On note M le produit $m_1 \cdots m_k$ et pour tout $i = 1, \ldots, k$, $\widehat{m}_i = M/m_i$. Montrer que m_i et $\widehat{m}_i$ sont premiers entre eux.
2. Pour tout $i = 1, \ldots, k$, soient u_i et v_i deux entiers tels que $u_i m_i + v_i \widehat{m}_i = 1$. On pose $e_i = v_i \widehat{m}_i$. Montrer que $e_i \equiv 1\ [m_i]$ et $e_i \equiv 0\ [m_j]$, $\forall j \neq i$.
3. On pose $n_0 = a_1 e_1 + \cdots + a_k e_k$. Montrer que $n_0 \in E$.
4. Soit n un élément quelconque de E. Montrer que $n - n_0$ est un multiple de M.
5. Démontrer que $E = n_0 + M\mathbb{Z} = \{n = n_0 + hM\ ,\ h \in \mathbb{Z}\}$. (Bravo ! Vous venez de démontrer le *Théorème des Restes Chinois*.)

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.

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

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 Abacistes contre algoristes

Dans toutes les civilisations ayant développé un système d'écriture, une notation pour les nombres est apparue. La majorité de ces systèmes de numération étaient décimaux (en base 10) à l'exception notable des Babyloniens (base 60 : il nous en reste des traces dans notre manière de diviser les heures et les minutes) et des Mayas (base 20). Quelle que soit la base, le système de notation par chiffres que nous utilisons actuellement ne s'imposait aucunement. Les Babyloniens, les Égyptiens, les Grecs et les Romains avaient des notations différentes pour chaque puissance de la base. Vous connaissez sans doute la notation en chiffres romains : I pour un, V pour cinq, X pour dix, C pour cent, D pour cinq cent, M pour mille. Mais l'écriture de très grands nombres était vite limitée.

Parallèlement aux systèmes de notation des chiffres, des outils de calcul, permettant de réaliser les opérations usuelles sont également apparus très tôt. On les désigne sous le nom générique d'*abaques* (qui vient d'un mot grec signifiant « table à poussière »). Le principe commun est de constituer des colonnes dans lesquelles on place de petits cailloux (calculus en latin, d'où le mot « calcul ») ou des jetons. Chaque colonne est associée à une puissance de dix : le nombre de jetons dans la colonne de droite indique le chiffre des unités, dans la colonne suivante le chiffre des dizaines, etc. Les bouliers sont des abaques dont les colonnes sont remplacées par des tiges le long desquelles on fait descendre les jetons. Pour passer d'un abaque à la numération de position, il fallait d'une part avoir l'idée de représenter par un symbole chacune des 9 quantités de jetons que l'on pouvait trouver dans une colonne, et aussi inventer un symbole pour noter une colonne vide. Ce passage a été effectué en Inde, semble-t-il dès les premiers siècles de notre ère. Mais noter ainsi un nombre en calquant sa représentation sur un abaque, ne signifiait pas pour autant que l'on sache effectuer des calculs sans abaque, en écrivant seulement des nombres. Il fallait pour cela accepter de considérer le symbole de la colonne vide, le zéro, comme un nombre ayant ses propres règles de calcul. Il est difficile de dater précisément l'apparition du zéro. La première trace indiscutable se trouve dans l'œuvre du mathématicien-astronome Āryabhata, en 499 après J.-C. On y trouve explicitement énoncée la notion de position. Voici le début de son poème, écrit en strophes de deux vers.

> Ayant rendu hommage à Brahma, à la Terre, à la Lune, à Mercure, à Vénus, au Soleil, à Mars, à Jupiter, à Saturne et aux constellations, Āryabhata en la Cité des Fleurs (Pataliputra), expose comme suit les éléments de la science très vénérable.
>
> Eka (unités), daçan (dizaines), çata (centaines), sahasra (milliers), ayuta (dix-milliers), niyuta (cent milliers), prayuta (millions), kôti (dix-millions), arbuda (cent millions), et vārnda (milliards) sont, de place en place, décuples l'un de l'autre.

Brāhmagupta (598–668) est l'un des plus célèbres mathématiciens-astronomes indiens. Il reprend la nomenclature des puissances de 10, la pousse jusqu'à 10^{17}, et ne laisse lui non plus aucun doute sur la nouveauté de la notation.

> Eka, daçann, çata, sahasra, ayuta, laxa, prayuta-kôti, arbuda, abja (ou padna), kharva, nikharva, nahāpadma, çanku, jahadri, anlya, madhya, parārdha, sont les places successives, croissant par multiplication de dix en dix, établies pour la pratique par les anciens.

Son œuvre principale, Brāhmasphutasiddhānta (écrite en 628), contient deux chapitres de mathématiques. Pour la première fois les règles de calcul avec le zéro sont énoncées explicitement. Pour Brāhmagupta, le zéro est défini comme la somme de deux quantités opposées : un bien et une dette. Les commerçants indiens ne tardent pas à diffuser la découverte, qui se répand rapidement vers le monde musulman alors en plein essor (l'Égire date de 622). Plus tard en Inde, Bhāskara II (1114–1185) donne les règles de multiplication et de division par zéro, et donc invente l'infini.

> Cette quantité appelée « celle dont le diviseur est zéro », ni l'addition ni la soustraction d'aucune quantité finie ne peut la modifier, exactement comme nulle altération n'a lieu en Brahman immuable et infini quand en Lui la totalité des mondes est résorbée à la fin d'une création ni quand de Lui est soustraite la totalité des mondes au début d'une création nouvelle.

Au nom de Bhāskara est souvent associé Achārya (le Professeur) ; appréciez sa façon de poser un exercice.

> Dis-moi, chère et belle Lilavati, toi qui as des yeux comme ceux du faon, dis-moi quel est le résultat de la multiplication de 135 par 12.

La première mention des chiffres indiens hors de l'Inde est due à Sévère Sebôkht, figure de proue de l'Église nestorienne en Syrie au VII^{e} siècle.

> J'éviterai toute discussion sur la science des Indiens, [...] sur leurs découvertes subtiles en astronomie, découvertes qui sont plus ingénieuses que celles des Grecs et des Babyloniens, sur leurs méthodes de calcul de grande valeur qui dépassent la description. Je désire seulement dire que leurs calculs sont faits au moyen de neuf signes. Si ceux qui croient, parce qu'ils parlent Grec, qu'ils sont arrivés aux limites de la science, lisaient les textes indiens, ils seraient convaincus bien qu'un peu tard, que d'autres savent des choses de valeur.

Ces « méthodes de calcul de grande valeur » convainquirent les savants musulmans, qui se mirent à les diffuser. Al-Khawarizmi écrit son livre « sur le calcul avec les nombres Hindous » en 825, puis al Kindi publie quatre tomes sur le même sujet en 830. Ces livres furent responsables de la diffusion du système de numération indien dans le monde islamique, puis finalement en occident. Le mot algorithme s'est d'abord écrit algorizme en l'honneur d'al-Khawarizmi puis a changé d'orthographe sous l'influence du grec. Son sens a beaucoup varié au cours des siècles. L'Encyclopédie de Diderot et

d'Alembert le définit joliment comme « l'Art de supputer avec justesse et facilité ». Il a longtemps désigné le calcul par la numération de position, dont les partisans étaient nommés algoristes.

La diffusion de la numération décimale en Europe a certainement démarré en Espagne, où marchands et savants musulmans, juifs et chrétiens ont eu de très nombreux contacts au cours des siècles. D'ailleurs la première trace écrite des chiffres arabes dans un texte en latin se trouve dans le « Codex Vigilianus » écrit dans un monastère aragonais en 976. On ignore si Gerbert d'Aurillac (938–1003) a eu connaissance de ce texte. Fils de serf auvergnat, il entre très jeune au monastère d'Aurillac et y commence ses études. Emmené à Barcelone par le comte Borel II en 963, il y découvre la numération de position. Devenu évêque, puis pape sous le nom de Sylvestre II, il use de son autorité pour la promouvoir auprès des savants occidentaux. Il invente en particulier un système d'abaque dans lequel il remplace les cailloux dans une colonne par un jeton portant l'un des chiffres arabes. Certains voient dans ce genre d'artifice une des origines possibles de la grande variété de forme qu'ont pu prendre les chiffres au cours du temps. Encore de nos jours, deux séries de chiffres cohabitent : ceux que vous connaissez, et les chiffres « arabes orientaux » utilisés dans de nombreux pays. Elles ont émergé petit à petit de quantités d'écritures différentes. Ce qui frappe pourtant dans les différentes formes qu'ont pu prendre les dix symboles c'est qu'elles se déduisent souvent les unes des autres par rotation. Dans leur forme actuelle, le 2 et le 3 sont des rotations de 90 degrés des chiffres arabes orientaux correspondants. D'où sont venues ces rotations ? Deux explications sont avancées. L'une tient à la pratique d'écrire ces chiffres sur des jetons pour le calcul sur abaque, comme le préconisait Gerbert d'Aurillac : ces jetons étant ronds, on a pu facilement oublier la position exacte dans laquelle il convenait de les placer. L'autre explication tient à l'habitude des copistes d'écrire horizontalement sur des rouleaux de payrus qui pouvaient ensuite être lus verticalement. Nous vous laissons choisir...

Même après Gerbert, la numération de position mit encore très longtemps à s'imposer en Europe. Quand Fibonacci écrit son « Liber Abaci » en 1202, il fait encore figure de précurseur. Il est probablement responsable de l'équivalent latin « zephirum » du mot arabe Sifr signifiant « vide », qui a donné chiffre, et zéro (mais pas zéphir, qui vient du Grec). La controverse entre abacistes et algoristes bat son plein pendant la Renaissance (figure 1). Elle mettra très longtemps à s'éteindre : en France sous Louis XIV, on enseignait encore l'usage du boulier plutôt que le calcul sur papier. La victoire des algoristes ne sera totale qu'au XVIII^{e} siècle.

3.2 Des grains de sable dans l'univers

Cherchant à évaluer le nombre de grains de sable contenus dans l'univers dans son « Arénaire », Archimède est amené à théoriser la notation des grands nombres. Dans ce texte, il désigne par « myriade » notre dizaine de milliers.

FIGURE 1 – Abacistes et algoristes : illustration du livre de Georg Reisch, Margarita philosophica cum additionibus novis, Basilae, Schottus, (1508)

> Il est des personnes, ô roi Gélon, qui pensent que le nombre des grains de sable est infini. Je ne parle point du sable qui est autour de Syracuse et qui est répandu dans le reste de la Sicile, mais bien de celui qui se trouve non seulement dans les régions habitées, mais encore dans les régions inhabitées. Quelques-uns croient que le nombre des grains de sable n'est pas infini, mais qu'il est impossible d'assigner un nombre plus grand. Si ceux qui pensent ainsi se représentaient un volume de sable qui fût égal à celui de la terre, qui remplît toutes ses cavités, et les abîmes de la mer, et qui s'élevât jusqu'aux sommets des plus hautes montagnes, il est évident qu'ils seraient bien moins persuadés qu'il pût exister un nombre qui surpassât celui des grains de sable.
>
> Quant à moi, je vais faire voir par des démonstrations géométriques auxquelles tu ne pourras refuser ton assentiment, que parmi les nombres dénommés par nous dans les livres adressés à Zeuxippe, il en est qui excèdent le nombre des grains d'un volume de sable égal non seulement à la grandeur de la terre, mais encore à celui de l'univers entier.
>
> [...]
>
> Telles sont les suppositions que nous faisons. Mais je pense qu'il est nécessaire à présent d'exposer les dénominations de nombres ; si je n'en disais rien dans ce livre, je craindrais que ceux qui n'auraient pas lu celui que j'ai adressé à Zeuxippe ne tombassent dans l'erreur. On a donné des noms aux

> nombres jusqu'à une myriade et au-delà d'une myriade, les noms qu'on a donné aux nombres sont assez connus, puisqu'on ne fait que répéter une myriade jusqu'à dix mille myriades.
>
> Que les nombres dont nous venons de parler et qui vont jusqu'à une myriade de myriades soient appelés nombres premiers, et qu'une myriade de myriades des nombres premiers soit appelée l'unité des nombres seconds ; comptons par ces unités, et par les dizaines, les centaines, les milles, les myriades de ces mêmes unités, jusqu'à une myriade de myriades. Qu'une myriade de myriades des nombres seconds soit appelée l'unité des nombres troisièmes ; comptons par ces unités, et par les dizaines, les centaines, les milles, les myriades de ces mêmes unités, jusqu'à une myriade de myriades ; qu'une myriade de myriades des nombres troisièmes soit appelée l'unité des nombres quatrièmes ; qu'une myriade de myriades de nombres quatrièmes soit appelée l'unité des nombres cinquièmes, et continuons de donner des noms aux nombres suivants jusqu'aux myriades de myriades de nombres composés de myriades de myriades des nombres troisièmes.

Bon, vous avez compris, Archimède sait compter jusqu'à beaucoup !

3.3 Les comptes binaires de l'Empereur de Chine

Voici ce qu'on trouve à l'article « Numération » dans l'Encyclopédie de Diderot et d'Alembert.

> Weigelius enseigne comment on pourroit nombrer sans passer le chiffre 4, c'est-à-dire, en répétant seulement les chiffres 1, 2, 3, 4 ; & M. Léibnitz, dans ce qu'il appelloit son arithmétique binaire, s'est servi des deux chiffres 1, 0, seulement, pour exprimer toutes sortes de nombres. Mais ces sortes de manieres de calculer sont plus curieuses qu'utiles. Voyez Binaire.

Les informaticiens apprécieront le « plus curieuses qu'utiles ». Mais Leibniz est-il bien l'inventeur de l'arithmétique binaire ? Reportons-nous à l'article « Binaire ».

> [. . .] ainsi dans toute l'arithmétique binaire il n'y auroit que deux caracteres, 1 & 0. Le zéro auroit la puissance de multiplier tout par deux, comme dans l'Arithmétique ordinaire il multiplie tout par dix : 1 seroit un ; 10, deux ; 11, trois ; 100, quatre ; 101, cinq ; 110, six ; 111, sept ; 1000, huit ; 1001, neuf ; 1010, dix, &c. ce qui est entierement fondé sur les mêmes principes que les expressions de l'Arithmétique commune. Il est vrai que celle-ci seroit très incommode par la grande quantité de caracteres dont elle auroit besoin, même pour de très-petits nombres. Il lui faut, par exemple, quatre caracteres pour exprimer huit, que nous exprimons par un seul. Aussi M. Leibnitz ne vouloit-il pas faire passer son arithmétique dans un usage populaire ; il prétendoit seulement que dans les recherches difficiles elle auroit des avantages que l'autre n'a pas, & qu'elle conduiroit à des spéculations

> plus élevées. Le P. Bouvet, jésuite, célebre missionnaire de la Chine, à qui M. Leibnitz avoit écrit l'idée de son arithmétique binaire, lui manda qu'il étoit très-persuadé que c'étoit-là le véritable sens d'une ancienne énigme chinoise laissée il y a plus de 4000 ans par l'empereur Fohi, fondateur des Sciences à la Chine, aussi-bien que de l'empire, entendue apparemment dans son siecle, & plusieurs siecles après lui, mais dont il étoit certain que l'intelligence s'étoit perdue depuis plus de 1000 ans, malgré les recherches & les efforts des plus savans lettrés, qui n'avoient vû dans ce monument que des allégories puériles & chimériques. Cette énigme consiste dans les différentes combinaisons d'une ligne entiere & d'une ligne brisée, répetées un certain nombre de fois, soit l'une, soit l'autre. En supposant que la ligne entiere signifie 1, & la brisée 0, on trouve les mêmes expressions des nombres que donne l'arithmétique binaire. La conformité des combinaisons des deux lignes de Fohi, & des deux uniques caracteres de l'arithmétique de M. Leibnitz, frappa le P. Bouvet, & lui fit croire que Fohi & M. Leibnitz avoient eu la même pensée.

Loin d'être vexé de n'être pas le premier, Leibniz s'était montré très intéressé, et avait beaucoup réfléchi aux implications philosophiques de l'arithmétique binaire. Voici ce qu'il écrit le 18 août 1705 dans une lettre au Révérent Père Verjus.

> Et comme il s'est trouvé que ma nouvelle Arithmétique binaire (qui au lieu de la progression décadique se sert de la dyadique, et n'a point d'autres notes que 0 et 1, et par conséquent montre d'abord beaucoup d'ordre des périodes et une liaison merveilleuse en toute sorte de suites des nombres) est parfaitement exprimée par les anciens caracteres de Fohi dont les Chinois des le temps de Confucius avaient déja perdu la signification ; il me semble que cette découverte, petite a la vérité, mais surprenante, doit contribuer a nous éveiller, tant en Europe qu'a la Chine, parce qu'elle pourra faire une grande impression sur l'empereur de la Chine et sur des personnes intelligentes de ce pays, pour réveiller leur curiosité par rapport a la recherche des origines et de la théologie et philosophie des anciens Chinois, que ce rapport des caracteres de Fohi montre de n'avoir pas toujours été des gens aussi superficiels qu'on pourrait bien avoir cru. Je crois qu'a Rome meme la connaissance de cette découverte pourra faire un bon effet, pour donner une meilleure opinion de l'antiquité reculée de ces peuples éloignés. Et aupres des Chinois memes elle peut servir a leur rendre plus recevable un des grands articles, et non pas des plus aisés de notre religion, et de notre métaphysique, qui porte que Dieu et rien font l'origine de toutes choses, que Dieu a tout créé de rien, et le fait encore, la conservation n'étant qu'une création continuelle. Car cette origine des choses de Dieu et de rien, reçoit un grand éclaircissement de l'analogie qu'elle a avec l'origine de tous les nombres de l'unité et du zéro, puisque tous les nombres se peuvent et meme se doivent exprimer le plus scientifiquement par les deux notes 1 et

> 0, et par conséquent par un rapport unique et continuel a ces deux premiers éléments des nombres.

Il développera encore plus sa philosophie du binaire dans un « Discours sur la théologie naturelle des Chinois » (1716). Mais qu'en est-il de la numération binaire chinoise, et d'abord qui était ce Fohi ?

Premier empereur mythique de la Chine, Fohi (ou Fu-xi ou Fu Hsi) aurait inventé, quelque 3000 ans avant notre ère, à peu près tout : mariage, noms de famille, écriture, numération décimale... Quid des symboles binaires ? Ils apparaissent dans le Yi Jing, ou *traité des mutations*, sur l'auteur duquel on ne sait à peu près rien, sauf qu'il a dû vivre au moins 800 ans avant notre ère. À la base se trouvent le Yin (solaire, masculin...) et le Yang (lunaire, féminin...) Le Yin est représenté par un trait plein et le Yang par un trait discontinu. On forme alors les huit trigrammes qui sont les huit manières de représenter 3 traits, pleins ou discontinus. Chacun est associé à plusieurs interprétations. Par exemple $\overline{=\,=}$ a pour image naturelle le feu, comme qualités la clarté, la lucidité, la vivacité, l'éclat, et est aussi associé à ce qui s'attache, à la fille cadette, à l'œil, etc. Observez le drapeau actuel de la République de Corée du Sud : quatre des des huit trigrammes y entourent le symbole du Yin et du Yang. En combinant deux à deux chacun des huit trigrammes, on obtient 64 hexagrammes, chargés à leur tour chacun d'une signification symbolique. Mais faut-il voir pour autant dans cet outil de divination le premier code ascii ? Ce serait aller un peu vite. Rien n'indique que les Chinois aient associé les 64 premiers entiers aux 64 hexagrammes. D'ailleurs dans le Bagua, les 8 trigrammes sont toujours représentés autour d'un octogone, et dans un ordre autre que lexicographique.

Il est bien possible que Leibniz se soit laissé quelque peu emporter par son enthousiasme, et que l'invention de l'informatique ne soit pas à mettre entièrement au crédit de Fohi, comme celles du mariage et de l'écriture.

3.4 Chasles contre Libri

À l'article « Inde » de l'Encyclopédie de Diderot et d'Alembert, publiée entre 1751 et 1772, on lit :

> L'Arithmétique n'y étoit pas moins perfectionnée ; les chiffres dont nous nous servons, & que les Arabes ont apportés en Europe du tems de Charlemagne, nous viennent de l'Inde.

Il n'y avait donc pas de doute sur l'origine de la numération. Et pourtant il ne fut pas facile pour les savants occidentaux, pétris d'humanisme et de belles lettres, formés aux mathématiques par Euclide, d'admettre qu'une invention aussi fondamentale que la numération de position ne venait pas des Grecs, mais des Indiens et des Arabes. L'un des débats les plus virulents oppose à partir de 1836, Michel Chasles (1793–1880) à Guillaume Libri (1803–1869).

Le second, aristocrate italien d'origine, est un personnage peu ordinaire. Son nom complet est « Guglielmo Bruto Icilio Timoleone Libri Carruci dalla Sommaja ». Nommé

à 20 ans professeur de physique mathématique à Pise, il part dès l'année suivante pour une année sabbatique en France, où ses origines et ses connaissances lui permettent de se lier avec les plus grands scientifiques de l'époque. De retour en Italie, ses idées libérales et son activisme politique le compromettent vite, et il doit s'exiler. Revenu en France, sa réputation scientifique grandit. Il est naturalisé français en 1833 et est élu la même année à l'Académie des Sciences. Il obtient une chaire de professeur à la Sorbonne puis au Collège de France, et reçoit la Légion d'Honneur. Il est même nommé Inspecteur Général des Bibliothèques en 1841. Les doutes des bibliothécaires sur les coïncidences entre ses visites et des disparitions de manuscrits, conduisent à sa mise en accusation. Il est expulsé de l'Académie en 1847 par un billet laconique.

> Monsieur, vous ignorez sans doute la découverte qui a été faite du rapport judiciaire concernant votre inspection dans les bibliothèques publiques. Croyez-moi, épargnez à la Société Nouvelle des réactions qui lui répugnent ; ne venez plus à l'Institut.

Il a la sagesse de suivre le conseil, et quitte Paris pour l'Angleterre avant d'être condamné par contumace à 10 ans de réclusion par la cour d'assise du département de la Seine en 1850. On trouve dans le jugement des détails impressionnants sur la masse de livres et de manuscrits que Libri avait accumulés : 17 caisses saisies chez lui, sans compter tous ceux qu'il avait réussi à expédier à l'étranger, en tout une collection estimée à 30 000 documents. On y trouve aussi quelques détails savoureux.

> Le jeune Abry aurait déclaré à deux témoins qu'il avait travaillé chez Libri ; que pendant quinze jours ou trois semaines il avait été employé à gratter et à faire disparaître des cachets et timbres sur les livres ; que Libri avait voulu se mêler de ce travail mais qu'il avait dû l'abandonner parce qu'il s'en acquittait mal et qu'il faisait des trous dans le papier.

Libri se défend vigoureusement depuis Londres dans un long plaidoyer, intitulé « Lettre à M. De Falloux, Ministre de l'Instruction Publique et des cultes contenant le récit d'une odieuse persécution et le jugement porté sur cette persécution par les hommes les plus compétents et les plus considérables de l'Europe. » Elle commence ainsi.

> On ne me taxera pas l'impatience. Il y a aujourd'hui un an, que le *Moniteur Universel*, obéissant aux ordres de mes ennemis personnels, me calomniait officiellement au nom du Gouvernement provisoire de la République française ! Cette publication a rencontré le blâme général : ce *Rapport*, à l'aide duquel on avait espéré me perdre, est devenu la risée de l'Europe, et pourtant je n'ai encore vu mettre un terme à aucune des mesures exceptionnelles qui ont été prises contre moi. Tous mes biens saisis et mal protégés ; ma bibliothèque, mes travaux scientifiques, ma correspondance la plus intime, tous mes papiers, livrés sans inventaire, sans aucune forme protectrice à mes ennemis devenus maîtres absolus chez moi [...]

Rien n'y fera : malgré le soutien de quelques amis, dont Prosper Mérimée qui ira même en prison pour une défense un peu trop vigoureuse, son procès ne sera pas révisé et il

ne reviendra jamais en France. Il réussira tout de même à revendre une partie de sa collection en Angleterre à des acheteurs de bonne foi, que les bibliothèques devront plus tard dédommager pour récupérer leur bien. On découvre encore de temps en temps, éparpillés ici ou là, des manuscrits de la « collection Libri » d'une importance cruciale pour l'histoire des mathématiques : une lettre de Descartes, un mémoire d'Abel, les manuscrits de Sophie Germain...

Mais Libri (un nom prédestiné pour un bibliophile aussi acharné) n'est pas connu que pour sa condamnation. Il est l'auteur de plusieurs mémoires de mathématiques, et surtout d'une monumentale « Histoire des Sciences Mathématiques en Italie depuis la renaissance des lettres jusqu'à la fin du dix-septième siècle », en quatre tomes. Dans un style très vivant, il y laisse libre cours aux trois passions de sa vie : son combat pour la nation italienne, son goût pour les livres et manuscrits anciens, et les sciences.

> [...] à la fin du seizième siècle, lorsque le peuple italien ne savait même plus murmurer, Galilée a rendu à sa patrie une gloire qu'elle ne semblait pas pouvoir espérer. Ces exemples devraient de nos jours servir de guide en Italie aux esprits élevés et imposer silence à ces hommes qui attribuent toujours au peuple la cause de leur petitesse, et qui voudraient trouver dans les circonstances politiques une excuse à leur nullité.

Dans le premier tome, il défend vigoureusement l'origine indienne de la numération de position, et règle au passage quelques comptes.

> L'Histoire de l'astronomie ancienne de Delambre (Tom. I, p.400–556) contient un exposé assez détaillé des méthodes astronomiques des Hindous. Cependant, il faut avouer que Delambre, plus occupé à combattre Bailly qu'à suivre la marche des sciences, a toujours montré une trop grande prévention contre les travaux des Orientaux. Quoiqu'il eût connaissance des Mémoires de la société asiatique de Calcutta, ainsi que du Liliwati et du Bija Ganita, où se trouvent exposées tant de belles recherches mathématiques, il ne craignit pas d'écrire le passage suivant : « Après ce que nous avons annoncé des Chinois et des Indiens, il serait fort inutile d'exposer ici des travaux grossiers ou tardifs de ces deux peuples, qui sont toujours restés étrangers aux progrès de la science. Nous renverrons aux deux chapitres que nous avons consacrés à leur histoire. Qu'il nous suffise de rappeler qu'on ne leur connaît aucun instrument, aucune science géométrique, aucune méthode qui n'ait été tirée directement ou indirectement des écrits des Grecs. »

Dans le tome 2, paru en 1840, Libri s'étend longuement sur sa controverse avec Chasles à propos de l'origine de la numération de position, même si au détour d'une page, il reconnaît :

> Au reste, M. Chasles et moi nous nous trouvons d'accord sur beaucoup d'autres points. Je suis heureux de voir qu'il a adopté mes idées sur la

> prétendue géométrie de position des Arabes et sur le peu de cas que l'on doit faire de l'inexactitude de Delambre.

Qu'avait donc affirmé Chasles qui prête autant à controverse ? Il avait publié en 1836 à Bruxelles un mémoire « sur le passage du premier livre de la géométrie de Boèce relatif à un nouveau système de numération »

> De ce qui précède nous croyons pouvoir conclure que le système de numération exposé par Boèce est le système décimal, dans lequel les neuf chiffres, dont il se sert prenaient des valeurs de position, croissant en progression décuple de droite à gauche.

Boèce (480-524) est bien l'auteur d'une « Institution Arithmétique » dans laquelle il traduit en Latin et commente les œuvres de Nicomaque de Gérase, il a peut-être écrit un traité de géométrie commentant l'œuvre d'Euclide, mais celui-ci n'a jamais été retrouvé. La « Géométrie » que Chasles lui attribue est un faux. Le bibliophile averti qu'est Libri n'a aucune peine à tailler en pièces le mémoire de Chasles. La controverse a eu au moins deux suites heureuses : l'étude des sources mathématiques arabes en a été ravivée, et Chasles, après la condamnation de Libri a finalement obtenu comme il le souhaitait depuis si longtemps son siège à l'Académie. Mais le manuscrit de Boèce n'était qu'un galop d'essai : trente ans plus tard, Chasles réalisera son coup de maître en achetant à un certain Vrain-Lucas des milliers de faux grossiers dont il tirera encore quelques communications retentissantes à l'Académie des Sciences.

3.5 Ils sont amicaux, parfaits... voire excessifs

Si n est un entier, ses diviseurs autres que lui-même sont dits *propres* : 1, 2, et 5 sont les diviseurs propres de 10. On disait autrefois « partie aliquote », du mot latin signifiant « plusieurs fois ». Notons $s(n)$ la somme des diviseurs propres de n.

- Si $s(n) < n$, n est dit *déficient*
- Si $s(n) = n$, n est dit *parfait*
- Si $s(n) > n$, n est dit *excessif*, *excédent* ou *abondant*
- Si $s(n) = n + 1$, n est dit *quasi-parfait*

En bon successeur de Pythagore, Nicomaque de Gérase accompagne cette classification d'une interprétation symbolique dans son « Introduction à l'arithmétique », au II^{e} siècle ap. J.C. Il associe aux nombres abondants l'excès, l'ambition... et aux nombres déficients le manque, les défauts, la pauvreté, les nombres parfaits étant parés de toutes les vertus :

> Il arrive que, de même que le beau et le parfait sont rares et se comptent aisément, tandis que le laid et le mauvais sont prolifiques, les nombres excédents et déficients sont en très grand nombre et en grand désordre ; leur découverte manque de toute logique. Au contraire, les nombres parfaits se comptent facilement et se succèdent dans un ordre convenable ; on n'en trouve qu'un seul parmi les unités, 6, un seul dans les dizaines, 28, un

> troisième assez loin dans les centaines, 496 ; quant au quatrième, dans le domaine des mille, il est voisin de dix mille, c'est 8128. Ils ont un caractère commun, c'est de se terminer par un 6 ou par un 8, et ils sont tous invariablement pairs.

Il n'y a bien que 4 nombres parfaits inférieurs à 10000 : 6, 28, 496 et 8128. La Proposition IX.36 des Éléments d'Euclide affirme que tous les nombres de la forme $2^{k-1}(2^k-1)$ pour $k \in \mathbb{N}$ sont parfaits si $2^k - 1$ est premier : sauriez-vous le démontrer ? Le problème de la réciproque (tous les nombres parfaits sont-ils de cette forme ?) a été posé par Thabit ibn Qurra au IX$^{\text{e}}$ siècle, Ibn al-Haytham vers l'an 1000, puis par Descartes en 1638 dans une lettre à Mersenne, puis par Franz van Schooten en 1658 dans une lettre à Fermat. Ce n'est qu'en 1732 qu'Euler montre qu'il n'y a pas d'autre nombre parfait pair. On ignore toujours s'il y en a une infinité, et s'il existe des nombres parfaits impairs : aucun n'a été trouvé jusqu'à 10^{300}, mais qui sait ? De même, on ignore toujours s'il existe des nombres quasi-parfaits. Le plus petit nombre abondant impair est 945 mais il en existe une infinité : tout multiple strict d'un nombre parfait ou abondant est abondant.

Deux nombres n et m tels que $s(n) = m$ et $s(m) = n$ sont dits *amicaux* ou *amiables*. Les nombres amicaux sont depuis très longtemps chargés d'une forte connotation symbolique. Dans la Bible, Jacob donne deux cent chèvres et vingt boucs, et autant de brebis et de béliers à son frère aîné Ésaü (pour éviter que celui-ci le tue...) ; pourquoi 220 ? On rapporte que Pythagore aurait qualifié un ami d'« un autre lui, comme le sont 220 et 284 ». Ce couple de nombres amicaux était apparemment le seul connu des Grecs, mais les Arabes en trouvèrent bien d'autres. Thabit ibn Qurra (826-901) ouvrit la première voie systématique, en démontrant le résultat suivant.

Soit n un entier supérieur à 1, et soient $a = 3(2^n) - 1$, $b = 3(2^{n-1}) - 1$ et $c = 9(2^{2n-1}) - 1$. Si a, b et c sont premiers, alors $2^n(ab)$ et $2^n(c)$ sont amicaux.

Al-Farisi (1260-1320) découvrit le couple (17 296 , 18 416), Muhammad Baqir Yazdi le couple (9 363 584 , 9 437 056). Comme souvent, ces résultats furent ignorés puis redécouverts par les Européens, et c'est ainsi que le couple d'Al Farisi porte le nom de Fermat, celui de Yazdi le nom de Descartes, les nombres de la forme $2^n - 1$ sont les nombres de Mersenne. Les nombres de la forme $3(2^n) - 1$ ont tout de même été nommés « nombres de Thebit », en l'honneur de Thabit ibn Qurra.

3.6 Le Théorème des Restes Chinois

On trouve des traces de ce résultat, que nous vous avons proposé en exercice, dans les travaux mathématiques d'à peu près tous les pays, du Sunzi suanji (« Classique de calcul de Sunzi »), au Liber Abaci de Fibonacci, en passant par Āryabhata et Brāhmagupta en Inde, ainsi que par les mathématiciens arabes Ibn Tahir et al-Haytham ; mais curieusement, il n'est pas énoncé par les grecs. Au travers de ses multiples généralisations, le théorème des restes chinois est à la base de nombreux algorithmes de calcul arithmétique et symbolique, ainsi que de méthodes de cryptographie.

Le Sunzi suanji n'a pas pu être daté précisément : probablement entre le IIIe et le VIe siècle. Voici le problème 26, chapitre 3 [1].

> Soit des objets dont on ignore le nombre. En les comptant 3 par 3 il en reste 2 ; en les comptant 5 par 5, il en reste 3 et en les comptant 7 par 7, il en reste 2. Combien y a-t-il d'objets ?
>
> Réponse : 23.
>
> Règle : « En comptant par 3, il en reste 2 » : poser 140 ; « En comptant par 5, il en reste 3 » : poser 63 ; « En comptant par 7, il en reste 2 » : poser 30. Faire la somme de ces 3 nombres, obtenir 233. Soustraire 210 de ce total, d'où la réponse.
>
> En général : pour chaque unité restante d'un décompte par 3, poser 70 ; pour chaque unité restante d'un décompte par 5, poser 21 ; pour chaque unité restante d'un décompte par 7, poser 15. Si la somme ainsi obtenue vaut 106 ou plus, ôter 105 pour trouver la réponse.

Si vous avez bien compris le théorème, vous ne devriez pas avoir de peine à retrouver les nombres que Sunzi recommande de « poser », et à reconnaître le produit $3\times5\times7 = 105$.

Tant que vous y serez, renseignez le cuisinier sur son bateau de pirates :

> Dix-sept pirates s'emparent d'un lot de pièces d'or toutes identiques. Leur loi exige un partage à égalité : chacun doit recevoir le même nombre de pièces d'or et, s'il en reste, elles sont attribuées au cuisinier de bord. Dans le cas présent, la part du cuisinier serait de trois pièces, mais les pirates se querellent et six d'entre eux sont tués, ce qui porte la part du cuisinier à quatre pièces. Au cours d'une terrible tempête, le bateau fait naufrage et ne survivent que six pirates et le cuisinier. Par bonheur, le butin est sauvé. La part du cuisinier est maintenant de cinq pièces. Que peut espérer gagner le cuisinier lorsqu'il décide d'empoisonner le reste de l'équipage, sachant que c'est la plus petite des solutions possibles ?

3.7 Le Théorème de Ibn al-Haytham

Selon son histoire, rapportée par Roshdi Rashed [2], il devrait s'appeler Théorème d'Al-Haytham-Leibniz-Wilson-Waring-Lagrange-Euler-Gauss ; mais c'est sous le nom de Théorème de Wilson qu'il est connu dans la littérature, et que nous vous l'avons proposé en exercice.

Théorème 8. *Si n est un nombre premier, alors $(n-1)!$ est congru à -1 modulo n.*

Cette condition nécessaire est aussi suffisante, puisque si n n'est pas premier, $(n-1)!$ est divisible par tous les facteurs premiers de n, et est donc congru à 0 modulo n.

1. J.C. Martzloff : Histoire des Mathématiques Chinoises, *Masson, Paris 1987*
2. R. Rashed : Ibn al-Haytham et le Théorème de Wilson, *Archive for History of Exact Sciences, 22(4) p.305–321 (1980)*

Le théorème apparaît dans un livre en latin de « Meditationes Algebraicae » publié en 1770 par E. Waring. Celui-ci attribue le résultat à un de ses élèves, John Wilson, qu'il qualifie de « vir clarissimus, rerumque mathematicorum peritissimus ». Pourtant, ni Wilson ni Waring ne savaient en donner de démonstration ; selon Waring : « demonstrationes vero hujusmodi propositionum eo magis difficiles erunt ». En fait, le résultat avait déjà été énoncé, et peut-être démontré, par Leibniz au siècle précédent. Lagrange en 1771, Euler, puis Gauss en publieront différentes démonstrations. Mais bien avant, autour de l'an mil, le mathématicien Ibn al-Haytham (965-1040) avait déjà publié un court « Opuscule » dans lequel il énonçait le résultat, et où il apparaît clairement qu'il en possédait la justification, probablement basée sur une forme de l'identité de Bézout. Malheureusement, beaucoup de ses écrits n'ayant pas été retrouvés, ses connaissances exactes n'ont pas pu être reconstituées.

L'Opuscule d'al-Haytham commence par l'énoncé du problème suivant.

> Trouver un nombre tel que si on le divise par deux il en reste un ; si on le divise par trois, il en reste un ; si on le divise par quatre il en reste un ; si on le divise par cinq il en reste un ; si on le divise par six il en reste un ; si on le divise par sept il n'en reste rien ;

Al-Haytham donne deux méthodes. La première, qu'il qualifie de « canonique » consiste à exhiber le nombre $6! + 1 = 721$, qui répond à la question. La seconde permet de trouver toutes les solutions du problème, qui en a une infinité. On pourrait penser qu'al-Haytham n'a résolu qu'un problème particulier, une devinette arithmétique en quelque sorte. Mais voici comment il poursuit son exposé, après la description des deux méthodes dans le cas particulier $n = 7$.

> Ceci étant posé, nous disons que cette propriété est nécessaire pour tout nombre premier, c'est-à-dire que pour tout nombre premier – qui est un nombre qui n'est multiple que de l'unité –, si on multiplie les nombres qui le précèdent les uns par les autres selon la manière que nous avons introduite, et si on ajoute un au produit, alors si on divise la somme par chacun des nombres qui précèdent le nombre premier, il en reste un, et si on la divise par le nombre premier, il n'en reste rien.

Le cas particulier $n = 7$ n'est qu'un artifice pédagogique. Al-Haytham a bien conscience que son exposé est tout à fait général, et parfaitement clair. Beaucoup plus clair d'ailleurs que ceux de certains de ses successeurs qui reprendront le même problème à partir de ses écrits.

Laissons la conclusion à al-Haytham, qui ne semble pas juger que son résultat mérite une aussi longue postérité.

> Ce que nous venons de mentionner englobe les réponses à tous les problèmes de ce genre, et que Dieu nous assiste. La réponse au problème numérique est achevée. Louange à Dieu Seigneur du Monde ; Béni soit Son Prophète Mohammed, l'Élu, et tous les siens.

3.8 Diophante et Hypathie, tous deux d'Alexandrie

Immédiatement après les Éléments d'Euclide, peu de livres ont eu autant d'influence sur l'histoire des mathématiques que les Arithmétiques de Diophante. Pourtant, pratiquement rien n'est connu de façon certaine sur son auteur, dont on pense qu'il aurait vécu au III^e^ siècle ap. J.C. C'est une collection de problèmes particuliers portant tous sur des équations polynomiales à coefficients rationnels dont on cherche des solutions rationnelles (ces équations s'appellent depuis « équations diophantiennes »). Sur les 13 chapitres, 6 nous sont parvenus. Quatre autres ont été retrouvés au siècle dernier en Iran dans une traduction arabe, mais il n'est pas certain qu'ils aient fait partie de l'ouvrage original. Diophante serait mort à 84 ans, si on en croit cette épitaphe sous forme d'équation diophantienne, parue au moins un siècle après sa mort.

> Voici la tombe qui renferme les cendres de Diophante ; elle est merveilleuse car, en utilisant un artifice arithmétique, elle apprend toute sa vie. Il resta enfant pendant le sixième de sa vie ; après un autre douzième ses joues se couvrirent de barbe ; après un septième, il alluma le flambeau du mariage ; cinq ans après, il lui naquit un fils ; mais celui-ci, enfant malheureux, quoique passionnément aimé, mourut arrivé à peine à la moitié de l'âge atteint par son père. Diophante vécut encore quatre ans, adoucissant sa douleur par des recherches sur la science des nombres.

Avant l'imprimerie, les livres devaient être copiés à la main. Mais cela n'effrayait pas les savants : il est difficile d'imaginer l'ampleur qu'a pu prendre dans l'antiquité la célèbre bibliothèque d'Alexandrie. Ou plutôt les bibiothèques successives puisqu'elle fut plusieurs fois détruite, dont la première fois par César (accidentellement prétendit-il). On raconte que chaque navire qui accostait à Alexandrie devait confier immédiatement tout écrit qui se trouvait à son bord à la bibliothèque où il était copié puis restitué à son propriétaire avant le départ du navire. À Alexandrie, les rouleaux de papyrus se comptaient par centaines de milliers. Autour de la bibliothèque s'était créé ce que nous appellerions maintenant un centre de recherche et d'enseignement, bref une université, qui attirait les savants de tout le monde ancien ; de sorte qu'il est impossible de savoir si Diophante « d'Alexandrie » en était vraiment originaire.

Il était d'usage que certaines copies soient des « commentaires » dont l'auteur ajoutait au texte initial ses propres solutions aux problèmes posés, voire insérait des problèmes de son cru. Parmi ces commentateurs figure un certain Théon (toujours d'Alexandrie), professeur de mathématiques et d'astronomie, qui décida vers 350 d'éduquer sa fille Hypathie de façon plutôt originale pour l'époque : il lui apprit à penser ! Cela fit d'elle une professeure reconnue de mathématiques et de philosophie et une femme très écoutée et admirée ; mais aussi considérée par certains comme dangereuse : elle mourut assassinée en 415. Sa mort en « martyre de la libre-pensée » a été tellement instrumentalisée par les idéologies successives, qu'il est impossible de savoir ce qui s'est réellement passé. Aucun écrit d'elle ne nous est parvenu, mais il est possible que l'Arithmétique de Diophante telle qu'elle a été traduite plus tard par les Arabes puis

encore plus tard les Européens, ait été en fait un de ses « commentaires ». Finalement la seule chose certaine à propos d'Hypathie est qu'elle est la première femme a avoir laissé un nom dans l'histoire des mathématiques.

L'édition europénne la plus célèbre de l'Arithmétique de Diophante est une traduction latine datée de 1621, due à Gaspard Bachet de Méziriac, natif de Bourg-en-Bresse. À part cette traduction, Bachet de Méziriac est aussi connu pour un ouvrage intitulé « Problèmes plaisans et délectables qui se font par les nombres », et pour être le premier découvreur (européen) de l'identité de Bézout. Pourquoi cette édition de 1621 est-elle si célèbre ? Parce que Pierre de Fermat en possédait une copie, dont il griffonnait les marges de ses réflexions. Le livre fut plus tard réédité par son fils Samuel en incluant les remarques du père, dont celle-ci :

> Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eius-dem nominis fas est dividere cuius rei demontrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Mmh ... « aucune puissance jusqu'à l'infini »... « j'en ai découvert une démonstration merveilleuse »... « Cette marge est trop étroite pour la contenir »... hein ? Voici ce qu'en pensait Legendre en 1825.

> Les dernières paroles de cette note autorisent à croire que la démonstration dont parle Fermat, n'aurait occupé qu'un petit nombre de pages, s'il les avait eues à sa disposition. Cette démonstration était donc beaucoup plus simple que celle dont nous nous servons dans cet écrit pour prouver seulement que la solution, s'il y en avait une dans quelque cas, ne pourrait être donnée que par des nombres d'une grandeur prodigieuse. Mais ne poussons pas trop loin des observations qui nous induiraient à penser que Fermat a pu se méprendre sur l'exactitude ou la généralité de sa solution.

La « merveilleuse démonstration » de Fermat est un élément tellement central de l'histoire des mathématiques des trois derniers siècles qu'elle mérite bien qu'on lui consacre quelques sections, non ?

3.9 Le Dernier Théorème de Fermat

Les *triplets Pythagoriciens* sont les triplets d'entiers positifs (x, y, z) vérifiant $x^2 + y^2 = z^2$. Observons que si (x, y, z) répond à la question, alors il en est de même de (kx, ky, kz) et (ky, kx, kz), pour tout entier k. On peut donc se ramener à l'étude des triplets avec $x < y$ et tels que (x, y, z) n'aient pas de diviseur commun. Le triplet pythagoricien le plus simple est $(3, 4, 5)$, mais bien d'autres exemples sont connus depuis l'antiquité. Certains pensent que la tablette d'argile dite Plimpton 322, gravée en caractères cunéiformes vers 1800 av. J.C. doit être interprétée comme une liste de triplets pythagoriciens. Ce qui est avéré en tout cas, c'est l'utilisation par les architectes depuis l'Égypte ancienne, de la *corde à treize nœuds*, qui délimite 12 intervalles égaux,

et permet de tracer toutes sortes de figures géométriques dont un triangle rectangle de côtés 3, 4 et 5 intervalles. Vers 800 av. J.C., le mathématicien indien Baudhayana connaissait $(3,4,5)$, $(5,12,13)$, $(8,15,17)$, $(7,24,25)$ et $(12,35,37)$. Pythagore (569–475 av. J.C.) est bien le premier à avoir donné une formule permettant d'en produire à volonté. D'autres formules furent données par Platon (428–347 av. J.C.), puis par Euclide (325–265 av. J.C.). Voici ces formules (en langage actuel).

- Pythagore : $\forall n \in \mathbb{N}$, $(2n+1\,,\, 2n^2+2n\,,\, 2n^2+2n+1)$ est un triplet pythagoricien,
- Platon : $\forall n \in \mathbb{N}$, $(2n\,,\, n^2-1\,,\, n^2+1)$ est un triplet pythagoricien,
- Euclide : $\forall a \geqslant b \in \mathbb{N}$, $(2ab\,,\, a^2-b^2\,,\, a^2+b^2)$ est un triplet pythagoricien.

Euclide démontre que sa formule permet en fait de les obtenir tous. Peut-être s'était-il posé la même question pour la puissance 3 : existe-t-il des triplets d'entiers (x,y,z) tels que $x^3+y^3=z^3$? On n'en a pas de trace, pas plus que chez Diophante. Par contre les mathématiciens arabes, grands exégètes des grecs, y avaient répondu par la négative dès le Xe siècle, mais sans apporter de démonstration convaincante. Voici ce qu'écrit al-Khasin, dans son « Épître à al-Hasib ». [3]

> J'ai déjà démontré que ce qu'avance Abu Mohammed al-Khujandi – que Dieu soit miséricordieux avec lui – dans sa démonstration que la somme de deux nombres cubiques n'est pas un cube, est défectueux et incorrect.

Pourquoi al-Khazin donne-t-il lui aussi une démonstration incomplète ? Cela reste un mystère. Un peu plus tard ibn Sina (plus connu comme médecin que comme mathématicien, sous le nom d'Avicenne) affirme lui aussi le résultat et précise qu'il n'a pas été démontré, puis ibn al-Khawam au XIe siècle affirme sans non plus la démontrer l'impossibilité du cas $n=4$.

Quelques siècles passent avant Pierre de Fermat (1601–1665). Il est né à Beaumont de Lomagne d'un père négociant en cuir, assez riche pour que Pierre fasse des études de droit à l'Université, puis achète une charge de conseiller au parlement de Toulouse. Amateur de sciences et de mathématiques en particulier, il entretient une relation épistolaire suivie avec les plus grands savants de son temps : Descartes, Pascal, Mersenne, Roberval, Toricelli... L'image qu'il a laissé est celle d'un amateur génial, avec des intuitions certes fulgurantes, mais très peu de faits établis [4]. Voici un extrait de sa lettre d'août 1640 à Frénicle :

> Je suis quasi-persuadé que $2^{2^n}+1$ est premier quel que soit n. Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières qui éclairent ma pensée, que j'aurais peine à me dédire.

3. R. Rashed : l'analyse diophantienne au Xe siècle : l'exemple d'al-Khasin, *Revue d'Histoire des Sciences, 32(3) pp. 193-222 (1979).*

4. C. Goldstein : l'arithmétique de Pierre de Fermat dans le contexte de la correspondance de Mersenne : une approche microsociale. *Annales de la Faculté des Sciences de Toulouse XVIII, pp. 25–57 (2009)*

Il l'avait sans doute vérifié jusqu'à $n = 4$. C'est malheureusement faux dès $n = 5$ et au moins jusqu'à $n = 32$. Sa soi-disant « merveilleuse démonstration » de l'impossibilité de trouver trois entiers strictement positifs tels que $x^n + y^n = z^n$ pour $n > 2$ a fait beaucoup pour sa réputation. Il avait tout de même résolu le cas $n = 4$ et nous allons voir comment.

Fermat commence par affirmer qu'il n'existe pas de triangle rectangle à côtés entiers dont l'aire soit un carré d'entier. Voici ce que qu'il écrit ensuite dans la marge des Arithmétiques de Diophante. La traduction du latin est due à C. Henri et P. Tannery ; nous avons ajouté la numérotation.

1. Si l'aire d'un triangle était un carré, il y aurait deux bicarrés dont la différence serait un carré ;
2. il s'ensuit qu'on aurait également deux carrés dont la somme et la différence seraient des carrés.
3. Par conséquent, on aurait un nombre carré, somme d'un carré et du double d'un carré, avec la condition que la somme des deux carrés qui servent à le composer soit également un carré.
4. Mais si un nombre carré est somme d'un carré et du double d'un carré, sa racine est également somme d'un carré et du double d'un carré, ce que je puis prouver sans difficulté. On conclura de là que cette racine est la somme des deux côtés de l'angle droit d'un triangle rectangle dont l'un des carrés composant formera la base et le double de l'autre carré la hauteur.
5. Ce triangle rectangle sera donc formé par deux nombres carrés dont la somme et la différence seront des carrés.
6. Mais on prouvera que la somme de ces deux carrés est plus petite que celle des deux carrés, dont on a également supposé que la somme et la différence soient des carrés. Donc, si on donne deux carrés dont la somme et la différence soient deux carrés, on donne par là-même en nombres entiers, deux carrés jouissant de la même propriété et dont la somme est inférieure.
7. Par le même raisonnement, on aura ensuite une somme plus petite que celle déduite de la première et en continuant indéfiniment on trouvera toujours des nombres entiers de plus en plus petits satisfaisant aux mêmes conditions. Mais cela est impossible, puisque, un nombre entier étant donné, il ne peut y avoir une infinité de nombres entiers qui soient plus petits.
8. La marge est trop étroite pour recevoir la démonstration complète avec tous ses développements.

Re-voilà le gag de la marge trop étroite, mais cette fois-ci tout est juste. Par contre, il faut quand même travailler beaucoup pour arriver à la « démonstration complète ».

Pour commencer, les différentes affirmations méritent une traduction mathématique. Les problèmes successifs évoqués par Fermat sont les suivants.

$$\exists (a,b,c,d) \in \mathbb{N}^*\ , \quad \left\{ \begin{array}{rcl} a^2+b^2 & = & c^2 \\ ab/2 & = & d^2 \end{array} \right. \tag{P1}$$

$$\exists (a,b,c) \in \mathbb{N}^*\ , \quad a^4 - b^4 = c^2 \tag{P2}$$

$$\exists (a,b,c,d) \in \mathbb{N}^*\ , \quad \left\{ \begin{array}{rcl} a^2+b^2 & = & c^2 \\ a^2-b^2 & = & d^2 \end{array} \right. \tag{P3}$$

$$\exists (a,b,c,d) \in \mathbb{N}^*\ , \quad \left\{ \begin{array}{rcl} a^2+2b^2 & = & c^2 \\ a^2+b^2 & = & d^2 \end{array} \right. \tag{P4}$$

$$\exists (a,b,c,d) \in \mathbb{N}^*\ , \quad \left\{ \begin{array}{rcl} a^2+2b^2 & = & c^2 \\ (a^2)^2+(2b^2)^2 & = & d^2 \end{array} \right. \tag{P5}$$

Observez que si $a^4 - b^4 = c^2$ n'a pas de solution (problème (P2)), alors $x^4 + y^4 = z^4$ n'en a pas non plus. Les cinq premières affirmations disent respectivement :

1. (P1) $\Longrightarrow$ (P2)
2. (P2) $\Longrightarrow$ (P3)
3. (P3) $\Longrightarrow$ (P4)
4. (P4) $\Longrightarrow$ (P5)
5. (P5) $\Longrightarrow$ (P3)

Vous pouvez chercher vous-mêmes les démonstrations de ces implications, qui ne sont pas immédiates. Les deux principaux ingrédients sont :

1. la caractérisation d'Euclide des triplets pythagoriciens,
2. le fait que si le produit de deux nombres premiers entre eux est un carré, chacun des deux nombres est lui-même un carré (commencez par le démontrer).

Au fil des arguments revenant de (P3) à (P3) en passant par (P4) et (P5), les sommes d'entiers concernés diminuent strictement (affirmation 6). Arrive alors l'argument massue de la « descente infinie » (affirmation 7) : si partant de 4 entiers a, b, c, d solution d'un problème donné, on construit 4 autres entiers (a', b', c', d') solution du même problème et vérifiant $a'+b'+c'+d' < a+b+c+d$, alors le problème n'a pas de solution. Pas convaincu ? Démontrez rigoureusement par récurrence sur n qu'il n'existe pas de solution vérifiant $a+b+c+d \leqslant n$, pour tout n. Fermat n'a pas inventé cet argument que l'on trouve déjà chez Euclide. Mais il en a fait un usage tellement intensif et astucieux qu'on l'a baptisé depuis « descente infinie de Fermat ». En 1654 il avait promis à Pascal un traité rassemblant tous ses résultats basés sur la descente infinie ; il n'écrira finalement cette compilation qu'en 1659. Rappelons que Pascal est le premier à avoir formalisé le raisonnement par récurrence... en 1654.

Les affirmations péremptoires de Fermat ont occupé beaucoup de mathématiciens après lui. Mais à la mort d'Euler en 1783 tous les énoncés de Fermat avaient été soit démontrés soit infirmés. Tous sauf un : le Dernier Théorème de Fermat.

3.10 Quatre siècles avant Fermat

Le livre le plus profond et le plus abouti de Fibonacci, le Liber Quadratorum [5], ou « Livre des carrés », écrit en 1225, n'a été retrouvé et traduit qu'en 1851. Sur différents problèmes arithmétiques, Fibonacci y élabore des solutions astucieuses, et son approche est du même niveau que les recherches mathématiques arabes de l'époque, sans qu'il soit possible de démontrer qu'il en ait eu connaissance : certes, il s'était fait l'ardent propagandiste de la numération de position qu'il avait apprise dans sa jeunesse auprès des commerçants de Béjaïa, mais rien n'indique qu'il ait étudié des travaux plus avancés. Dans la dédicace, Fibonacci raconte qu'il a été présenté à la cour de l'Empereur à Pise, et que Magister Johannes de Palermo lui avait proposé un problème pour tester ses capacités. Il s'agissait de trouver un nombre carré, qui augmenté ou diminué de 5 donnerait encore des nombres carrés. Plus généralement, Fibonacci cherche à trouver trois carrés $x^2 < y^2 < z^2$ en progression arithmétique, c'est-à-dire tels que $x^2+z^2 = 2y^2$. Voici en gros son raisonnement. Si $x^2 + z^2$ est pair, alors x et z ont la même parité, donc $x+z = 2p$ et $z-x = 2q$ sont pairs. Écrivons $x = p-q$, $z = p+q$. On arrive ainsi à $x^2 + z^2 = 2p^2 + 2q^2 = 2y^2$. Donc (p, q, y) est un triplet pythagoricien. En utilisant la caractérisation d'Euclide, on peut se ramener au cas où il existe deux entiers m et m tels que :

$$p = m^2 - n^2 \ , \quad q = 2mn \ , \quad y = m^2 + n^2 \ .$$

On obtient alors :

$$y^2 - x^2 = z^2 - y^2 = 4mn(m + n)(m - n) \ .$$

Vérifiez le calcul et ayez une pensée admirative pour Fibonacci qui ne raisonnait que sur des rapports de surfaces et de longueurs, sans utiliser notre notation littérale. Fibonacci appelle *congruum* les nombres de la forme $4mn(m + n)(m - n)$, et étudie leurs propriétés. Il démontre en particulier qu'ils sont forcément divisibles par 24. Plus loin dans le même ouvrage, il démontre que si $x > y$, le rapport $(x + y)/(x - y)$ n'est jamais égal au rapport x/y (vérifiez-le vous-mêmes). De là, dit Fibonacci, on peut démontrer qu'aucun nombre carré ne peut être un congruum. Dommage qu'il n'ait pas dit pourquoi ! Car si un congruum n'est jamais un carré, alors avoir à la fois $y^2-c^2 = x^2$ et $y^2 + c^2 = z^2$ est impossible : la somme et la différence de deux carrés ne peuvent pas être toutes deux des carrés. C'est le problème (P3) de la section précédente, dont nous avons vu qu'il menait au cas $n = 4$ du Dernier Théorème de Fermat. Fibonacci n'en était pas loin... plus de quatre siècles avant Fermat.

5. R. B. McClenon : *Leonardo of Pisa and his Liber Quadratorum, Amer. Math. Monthly, 26(1) (1919)*

3.11 Le grand plan de Sophie Germain

Après la démonstration du cas $n = 4$ par Fermat lui-même, il n'y eut pas beaucoup de progrès jusqu'à Euler, qui annonce avoir démontré le cas $n = 3$ dans une lettre à Goldbach de 1753. Sa démonstration contenait une erreur, laquelle pouvait être corrigée par d'autres méthodes également dues à Euler ; de sorte que l'on s'accorde à lui en faire crédit : après tout, c'était le mathématicien le plus prolifique de tous les temps.

Vient ensuite Sophie Germain. En 1789 elle a 13 ans, elle vit à Paris, et deux événements ont pu l'impressionner durablement cette année-là. La Révolution Française est l'un d'entre eux : son père, d'une famille bourgeoise de commerçants était député du tiers-état. L'autre événement est sa lecture dans une histoire des mathématiques de la mort tragique d'Archimède. Elle se met à étudier les mathématiques avec passion, au point que ses parents lui confisquent bougies et couvertures pour qu'elle ne passe plus ses nuits à travailler. Devant la détermination de la jeune fille, ils finissent par lui laisser le champ libre : elle continue son apprentissage, mais sans jamais suivre le moindre cours. En 1794, l'École Polytechnique nouvellement créée compte parmi ses professeurs un des plus grands mathématiciens du moment, Joseph-Louis Lagrange. Sans que l'on sache comment, Sophie Germain réussit à se procurer les notes de cours de Lagrange et les étudie à fond. Elle a alors l'idée d'écrire à l'auteur sous le nom emprunté d'un élève de l'école. Lagrange, intrigué par la justesse et la profondeur des remarques qu'il reçoit, demande à rencontrer ce « Monsieur Le Blanc » qui a si bien compris ses cours. Face à la jeune fille de 19 ans, il est impressionné : il devient son ami et son mentor en sciences. Quatre ans plus tard, Adrien-Marie Legendre (1752–1833) publie une synthèse de nombreux résultats nouveaux d'arithmétique obtenus par Euler, Lagrange et lui-même. Sophie Germain étudie cet « Essai sur la théorie des nombres » avec passion, et entame une correspondance avec son auteur. Plusieurs autres éditions complétées suivront, dont un « second supplément » en 1825, portant « sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat ». Voici ce qu'on y lit, dans une note de bas de page.

> Cette démonstration qu'on trouvera sans doute très ingénieuse, est due à Mlle Sophie Germain, qui cultive avec succès les sciences physiques et mathématiques, comme le prouve le prix qu'elle a remporté à l'Académie sur les vibrations des lames élastiques. On lui doit encore la proposition de l'art. 13 et celle qui concerne la forme particulière des diviseurs premiers de α, donnée dans l'art. 11.

Et voilà Sophie Germain adoubée pour les siècles à venir : un théorème (d'ailleurs souvent cité de façon erronée) porte désormais son nom. Elle est l'auteur, certes d'autant plus remarquable qu'elle est une femme, d'un résultat accessoire qui a conduit à la résolution de quelques cas particuliers, méritant une note de bas de page. Est-ce vraiment tout ? Récemment, des chercheurs [6] ont pris la peine de lire les manuscrits de Sophie

6. R. Laubenbacher, D. Pengelley : « Voici ce que j'ai trouvé » Sophie Germain's grand plan to

Germain qui nous sont parvenus. Il ressort de leur étude que Sophie Germain avait un plan d'attaque sur le théorème de Fermat bien plus ambitieux que ne le laisse croire la place marginale à laquelle elle a été reléguée. Elle comptait, en procédant par l'absurde, démontrer que s'il y avait une solution, alors nécessairement les trois nombres x, y, z vérifiant $x^p + y^p = z^p$ devraient être arbitrairement grands. Dans le mémoire de Legendre on lit un plan analogue, mais avec des méthodes de démonstration complètement différentes. Pourtant, autant Legendre que Sophie Germain connaissaient les raisons pour lesquelles leurs plans ne suffiraient pas à démontrer le théorème dans toute sa généralité. Celui de Legendre a permis de régler de nombreux cas. Qu'en aurait-il été si tous les travaux de Sophie Germain avaient été publiés ? On ne le saura jamais, mais certaines de ses techniques n'ont été redécouvertes qu'au siècle suivant. Voici ce qu'elle en dit.

> Je n'ai jamais pu arriver à l'infini, quoique j'aie reculé bien loin les limites par une méthode de tâtonnement trop longue pour qu'il me soit possible de l'exposer ici. Je n'oserais même pas affirmer qu'il n'existe pas une limite au-delà de laquelle tous les nombres de la forme $2Np + 1$ auraient deux résidus p-ièmes placés de suite dans la série des nombres naturels. C'est le cas qui intéresse l'équation de Fermat.
>
> Vous concevrez aisément, Monsieur, que j'ai dû parvenir à prouver que cette équation ne serait possible qu'en nombres dont la grandeur effraie l'imagination. Car elle est encore assujettie à bien d'autres conditions que je n'ai pas le temps d'énumérer à cause des détails nécessaires pour en établir [la véracité (?)]. Mais tout cela n'est encore rien, car il faut l'infini et non pas le très grand.

La lettre dont ce passage est extrait date de 1819 et est adressée à Gauss. Il avait un an de moins qu'elle, mais était devenu célèbre très vite. En 1801 (à 24 ans) il publie « Disquisitiones Arithmeticae », un livre très moderne dans sa manière d'aborder l'arithmétique, que Sophie Germain étudie soigneusement. Elle écrit alors à l'auteur pour lui faire part de ses découvertes en utilisant le même stratagème qu'avec Lagrange quelques années plus tôt. On trouve dans la correspondance de Gauss des traces de ce « Monsieur Leblanc » de Paris qu'il tient en haute estime. Mais à l'automne 1806, les troupes de Napoléon envahissent la Prusse où réside Gauss. Sophie Germain, se souvenant peut-être du sort d'Archimède lors du siège de Syracuse, avertit un ami de la famille, le général Pernety, qu'il convient de protéger à tout prix ce grand savant. Pernety s'acquitte de sa mission, rencontre Gauss, et lui dit à qui il doit sa recommandation. Sophie Germain écrit alors à Gauss sous son vrai nom et dévoile la supercherie. Dans la réponse (en français alors qu'il n'écrivait qu'en latin ou en allemand) que Gauss envoie en remerciement à Sophie Germain le 30 avril 1807, on sent au-delà des formules de politesse, une réelle admiration : le grand Gauss, connu pour son exigence et son caractère difficile, est clairement impressionné. Voici le début de cette lettre (orthographe

prove Fermat's Last Theorem, (2010)

de Gauss).

> Votre lettre du 20 février, mais qui ne m'est parvenue que le 12 mars, a été pour moi la source d'autant de plaisir que de surprise. Combien l'acquisition d'une amitié aussi flateuse et précieuse est-elle douce à mon cœur ! L'intérêt vif, que vous avez pris à mon sort pendant cette guerre funeste, mérite la plus sincère reconnaissance. Assurément, votre lettre au général Pernety m'eût été fort utile, si j'avais été dans le cas d'avoir recours à une protection spécielle de la part du gouvernement françois. Heureusement les evenements et les suites de la guerre ne m'ont pas touché de trop près jusqu'ici, bien que je sois persuadé qu'elles auront une grande influence sur le plan futur de ma vie. Mais comment vous décrire mon admiration et mon étonnement, en voïant se metamorphoser mon correspondant estimé M. Leblanc en cette illustre personnage, qui donne un exemple aussi brillant de ce que j'aurois peine de croire. Le goût pour les sciences abstraites en général et surtoût pour les mysteres des nombres est fort rare : on ne s'en étonne pas ; les charmes enchanteurs de cette sublime science ne se decelent dans toute leur beauté qu'à ceux qui ont le courage de l'approfondir. Mais lorsqu'une personne de ce sexe, qui, par nos mœurs et par nos préjugés, doit rencontrer infiniment plus d'obstacles et de difficultés, que les hommes, à se familiariser avec ces recherches epineuses, sait neansmoins franchir ces entraves et penétrer ce qu'elles ont de plus caché, il faut sans doute, qu'elle ait le plus noble courage, des talens tout à fait extraordinaires, le génie supérieur. En effet, rien ne pourroit me prouver d'une manière plus flatteuse et moins équivoque, que les attraits de cette science, qui ont embelli ma vie de tant de jouissances, ne sont pas chimériques, que la predilection, dont vous l'avez honorée.
>
> Les notes savantes, dont toutes vos lettres sont si richement remplies, m'ont donné mille plaisirs. Je les ai étudiées avec attention, et j'admire la facilité avec laquelle vous avez pénétré toutes les branches de l'Arithmetique, et la sagacité avec laquelle vous les avez su généraliser et perfectionner.

Comment les lettres et les manuscrits de Sophie Germain nous sont-ils parvenus, alors qu'elle-même n'a jamais rien publié de ses résultats arithmétiques ? Grâce à Guillaume Libri, qui a lui-même publié ses propres réflexions sur le théorème de Fermat, mais qui est surtout resté dans l'histoire pour s'être constitué à force de vols dans les bibliothèques publiques, une collection personnelle phénoménale. Il avait lié connaissance avec Sophie Germain lors d'une année sabbatique passée à Paris en 1824 et se disait son ami. La renommée mathématique de Sophie Germain était alors bien établie, et elle siégait (comme auditrice, n'exagérons rien tout de même) à l'Académie des Sciences, que Libri fréquentait assidument. Aujourd'hui les manuscrits de Sophie Germain sont partagés entre la Bibliothèque Nationale à Paris et la Biblioteca Moreniana, à Florence.

3.12 Le Théorème de Fermat-Wiles

Il faudra encore 350 ans après l'énoncé de Fermat pour que l'on démontre vraiment que $x^n + y^n = z^n$ n'a pas de solution entière pour $n > 2$. Courbes elliptiques, fonctions modulaires, groupes de Galois absolus, la construction mathématique qui a abouti au succès d'Andrew Wiles s'appuie sur des notions qui vont très au-delà des mathématiques du temps de Fermat, et qui ont pour l'essentiel été élaborées au XX^{e} siècle. Wiles s'est appuyé sur de nombreux travaux de ses prédécesseurs, prolongés en une construction impressionnante qu'il a bâtie secrètement pendant 7 ans, avant de l'annoncer en juin 1993. Une « petite » erreur dans cet immense édifice lui a encore coûté un an d'efforts avant que sa démontration soit vraiment complète. Au bilan, le théorème qui porte désormais le nom de Fermat-Wiles n'est plus qu'un petit cas particulier de la théorie qu'il a suscitée.

Avant Wiles, de nombreux mathématiciens ont cru de bonne foi avoir réussi, avant que l'on ne découvre une faille dans leur démonstration : parmi les plus célèbres, Lamé, Cauchy, Lindemann, Kummer... Il est impossible de citer tous les mathématiciens qui ont apporté leur contribution avant Wiles, et encore moins tous ceux qui ont tenté de le faire. Il faut dire que ce résultat était devenu plus que toute autre conjecture, le Saint-Graal des mathématiques. C'est en partie dû au fait que son énoncé soit si simple ; Wiles lui-même raconte que vers l'âge de 10 ans il avait été frappé par le fait qu'il soit capable de le comprendre bien que personne ne l'aie encore démontré.

C'est aussi dû aux nombreux prix dont le résultat a fait l'objet. Un des plus célèbres est le prix Wolfskhel [7]. Héritier d'une famille de banquiers, Paul Wolfskhel avait une formation de médecin mais, atteint de sclérose, il avait compris très vite qu'il ne pourrait pas exercer. Il s'était alors tourné vers les mathématiques, et avait étudié auprès de Kummer, grand spécialiste du Théorème de Fermat. À son décès en 1906, il laissait par testament un prix de 100 000 Deutsche Marks (de l'ordre d'un million et demi d'euros d'aujourd'hui). Du fait des dévaluations successives, ce ne sont que 75 000 DM (environ 38 000 euros) que Wiles a reçu en 1997. Ne croyez pas les histoires qui circulent sur le fait que Wolfskhel aurait été sauvé par l'arithmétique d'une tentative de suicide suite à un chagrin d'amour, ni qu'il aurait voulu écarter de sa succession une épouse acariâtre et avide ; rien n'est avéré, à part le fait que les mathématiques ont adouci une vie par ailleurs bien difficile. Ce qui est certain en revanche, c'est qu'à compter de 1908, l'Institut de Mathématiques de Göttingen a eu la charge d'examiner chacun des manuscrits sur le Théorème de Fermat qui lui parvenaient, de détecter l'erreur, d'écrire à l'auteur pour la lui signaler, de recevoir ses protestations parfois véhémentes etc. L'année suivant l'annonce du prix, 621 manuscrits sont parvenus à Göttingen. En tout des milliers de textes, provenant de tous les pays, auront été écrits sur le Théorème de Fermat ; et ce n'est sans doute pas fini : certains sont toujours en quête de la fameuse « démonstration merveilleuse ». Au vu de l'énorme édifice que

7. K. Barner : Paul Wolfskhel and the Wolfskhel prize, *Notices of the A.M.S. 44(10) p. 1294–1303 (1997)*

représente la démonstration de Wiles, et n'en déplaise à Boris Vian, il est difficile de croire qu'un bricoleur puisse faire en amateur des bombes atomiques.

Mais que cela ne vous empêche pas de réfléchir : il reste de nombreuses conjectures non démontrées en arithmétique. La plus ancienne et l'une des plus simples est la conjecture de Goldbach (1742) : tout entier pair strictement supérieur à 2 est somme de deux nombres premiers. Cela a été vérifié par ordinateur jusqu'au-delà de 10^{18}, mais pas encore *démontré*. À moins qu'au fin fond de l'Amazonie, un perroquet bavard... [8]

3.13 Le code RSA

Le plus célèbre des codes à clé publique est dû à Ron Rivest, Adi Shamir et Leonard Adleman du MIT. La clé publique est connue de tous et est utilisée pour coder les messages. Par contre un message codé par la clé publique ne peut être décodé que par quelqu'un qui connaît la clé privée. Les clés sont constituées de la façon suivante.

1. Choisir deux (grands) nombres premiers p et q.
2. Calculer $n = pq$: les opérations s'effectueront modulo n.
3. Calculer $\varphi(n) = (p-1)(q-1)$.
4. Choisir un entier e inférieur à $\varphi(n)$ et premier avec $\varphi(n)$: c'est l'exposant de la clé publique.
5. Calculer l'inverse d de e pour la multiplication modulo $\varphi(n)$ (il existe et est unique puisque e et $\phi(n)$ sont premiers entre eux : calcul par l'algorithme d'Euclide). L'entier d est l'exposant de la clé privée.

La clé publique se compose de l'entier n et de l'exposant e, connus de tous. La clé privée est l'exposant d qui doit être tenu secret. Évidemment, quelqu'un qui connaît n peut théoriquement retrouver ses deux facteurs premiers p et q et donc calculer $\varphi(n)$ puis d connaissant e. La sécurité du système repose sur le fait que la décomposition d'un nombre en produit de facteurs premiers est très coûteuse en temps de calcul : il est virtuellement impossible de décomposer un nombre produit de deux très grands facteurs premiers. Cela n'empêche pas les utilisateurs de changer assez souvent de clé par mesure de sécurité.

Voici comment fonctionnent le codage et le décodage. Le message à transmettre est d'abord transformé en un entier (par exemple par concaténation des codes ascii des caractères qui le composent). Notons m cet entier qui est censé être inférieur à n. Le codage le transforme en $c = m^e$ modulo n. Pour décoder, il faut connaître d et calculer c^d modulo n. Miracle, on retrouve m. Vous pouvez nous croire sur parole, mais ce serait dommage, car la démonstration est parfaitement à votre portée.

Définition 9. *On appelle* caractéristique d'Euler *la fonction qui à un entier n fait correspondre le nombre d'entiers premiers avec n, compris entre 1 et n. On note cette fonction φ.*

8. D. Guedj : Le théorème du perroquet, Éditions du Seuil, Paris (1998)

Si p est premier, alors $\varphi(p) = p-1$, puisque tout entier strictement inférieur à p est premier avec p. Si $n = pq$ est le produit des 2 nombres premiers p et q, alors $\varphi(n) = (p-1)(q-1)$. Pourquoi ? Vous pouvez trouver tout seul : comptez les multiples de p puis les multiples de q, entre 1 et pq (ne comptez pas pq deux fois). Voici maintenant la généralisation du petit théorème de Fermat, que nous vous avons posé en exercice.

Théorème 9. *Soit n un entier et a un entier premier avec n. Alors $a^{\varphi(n)} \equiv 1\ [n]$.*

Cela aussi, vous pouvez le démontrer vous-mêmes : considérez le sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$, noté P, constitué des $\varphi(n)$ entiers premiers avec n compris entre 1 et n. Montrez ensuite que l'application qui à $r \in P$ associe ar modulo n est une bijection de P sur lui-même (raisonnez par l'absurde et utilisez le lemme de Gauss). Cela signifie que $\{ar\,[n]\,,\ r \in P\}$ est égal à P. Maintenant faites le produit modulo n de tous les éléments de chacun des deux ensembles :

$$\prod_{r\in P} ar = a^{\varphi(n)} \prod_{r\in P} r \equiv \prod_{r\in P} r\ [n]\ .$$

Allez, vous y êtes presque : un dernier coup de lemme de Gauss peut-être ?

Après un tel effort, vérifier que le codage RSA fonctionne, c'est presque du repos : Puisque $ed \equiv 1\ [\varphi(n)]$, il existe un entier k tel que $ed = k(p-1)(q-1)+1$. Alors : $(m^e)^d = m^{ed} = m\,(m^k)^{\varphi(n)} \equiv m\ [n]$.

Euh... à condition que m soit premier avec n, pour pouvoir appliquer le théorème ci-dessus à m^k. Si m n'est pas premier avec n, il est divisible par p ou par q, mais pas les deux (car il est inférieur à pq). Supposons qu'il soit divisible par p et écrivons : $m = p^\alpha h$, où h est premier avec p et avec q. Allez, vous allez encore devoir travailler : montrez d'abord que $p^{\alpha ed} \equiv p^\alpha\ [p]$, puis que $p^{\alpha ed} \equiv p^\alpha\ [q]$. Maintenant, vous pouvez en déduire que $p^{\alpha ed} \equiv p^\alpha\ [n]$. Recollez les morceaux : $m^{ed} = p^{\alpha ed} h^{ed} \equiv p^\alpha h\ [n]$. Vous y êtes, le message est bien décodé ! Par pure bonté d'âme, nous vous dispensons de recommencer ce qui précède si m est multiple de q : merci qui ?

3.14 La course aux nombres premiers

Comme vous l'avez vu pour le codage RSA, la cryptographie est grande consommatrice de nombres premiers, les plus imposants possibles évidemment. Un moyen de trouver de grands nombres premiers est de les chercher parmi les nombres dits « de Mersenne », autrement dit sous la forme $2^k - 1$. Pourquoi ? Parce qu'il existe un test de primalité extrêmement simple pour de tels nombres : le test de Lucas-Lehmer. Considérons la suite définie par $a_0 = 4$ et pour $k > 0$, $a_k = a_{k-1}^2 - 2$. Il se trouve que pour $k > 2$, le nombre $2^k - 1$ est premier si et seulement si il divise a_{k-2}. Essayez pour les premiers termes :

- $2^3 - 1 = 7$ divise $a_1 = 14$
- $2^4 - 1 = 15$ ne divise pas $a_2 = 194$
- $2^5 - 1 = 31$ divise $a_3 = 37634$

... étonnant non ? Avec un peu d'astuce, le test peut être implémenté en $O(p^2 \ln(p) \ln(\ln(p)))$ opérations pour un nombre de p bits, ce qui est bien plus rapide que tous les algorithmes généraux connus. Un gigantesque effort collaboratif de calcul distribué (Great Internet Mersenne Prime Search) vise à trouver des nombres de Mersenne premiers les plus grands possibles. Le plus grand connu à ce jour est $2^{43112609} - 1$ qui a plus de 12 millions de chiffres en écriture décimale. Rien de vous empêche de participer en offrant le temps de calcul de votre ordinateur. Vous ferez progresser le calcul distribué, mais pas la cryptographie : les nombres de Mersenne sont trop connus pour offrir un niveau de sécurité suffisant. S'il suffisait de tester quelques nombres de Mersenne pour décomposer une clé publique en deux facteurs premiers, le code RSA perdrait beaucoup de son intérêt.

Gauss écrivait :

> Le problème de distinguer les nombres premiers des nombres composés, et de décomposer ces derniers en facteurs premiers est connu pour être un des plus importants et des plus utiles en arithmétique. Il a engagé l'industrie et la sagesse des géomètres anciens et modernes à un tel point que la dignité de la science elle-même requiert que tous les moyens possibles soient explorés pour la résolution d'un problème si important et si célèbre.

La véritable difficulté est de tester des nombres *quelconques*, et donc de disposer d'un algorithme permettant de décider de façon certaine si un nombre est premier ou non. Ératosthène (276–194 av. J.C.) savait déjà comment énumérer tous les nombres premiers inférieurs à un nombre n donné. L'algorithme, qui porte le nom de « Crible d'Ératosthène », est bien connu : 2 est le plus petit nombre premier. On peut éliminer tous les multiples de 2. On itère ensuite en conservant le plus petit entier qui n'a pas encore été éliminé et en éliminant tous ses multiples. Mais pour décider si n est premier en utilisant cet algorithme, le nombre d'opérations est gigantesque, beaucoup trop grand pour la pratique. Une autre manière de tester la primalité est d'utiliser le théorème de Wilson : n est premier si et seulement si $(n-1)!$ est congru à -1 modulo n. Cela requiert de l'ordre de n multiplications modulo n, ce qui est encore beaucoup trop lent.

Quand en 2002 Agrawal, Kayal et Saxena ont annoncé « PRIMES is in P », la nouvelle a fait sensation. Enfin un test de primalité, dont on peut démontrer qu'il décide de façon certaine si n est premier, en un nombre d'opérations polynomial en $\ln(n)$. L'article original était théorique, mais très vite des implémentations ont suivi, avec des raffinements et des améliorations. Les algorithmes AKS sont maintenant toute une famille et sont couramment utilisés. Deux points méritent d'être soulignés dans cette histoire. Le premier est que l'algorithme utilise un résultat d'arithmétique vieux de deux siècles élaboré dans la quête du Dernier Théorème de Fermat, précisément celui qui porte le nom de Sophie Germain. L'autre est que Neeraj Kayal et Nitin Saxena, à l'époque de leur découverte, étaient deux étudiants en Btech (équivalent d'un Master Professionnel) d'Informatique à l'Indian Institute of Technology de Kampur, effectuant

leur mémoire sous la direction de Manindra Agrawal.

3.15 La répartition des nombres premiers

Il suffit d'observer un crible d'Érathostène rempli pour réaliser que les nombres premiers sont relativement rares parmi les entiers. Vers la fin du XVIII^{e} siècle, Gauss et Legendre avaient examiné de près la répartition expérimentale des nombres premiers et proposé chacun une fonction pour ajuster cette répartition. Les deux avaient en commun leur comportement asymptotique. Si $\pi(n)$ désigne le nombre d'entiers premiers inférieurs ou égaux à n, alors :

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1 \ .$$

Il faudra un siècle d'efforts après Legendre et Gauss pour démontrer ce résultat, mais la même année 1896, deux mathématiciens y parviennent indépendamment : Charles-Jean de la Vallée Poussin (1866–1962) et Jacques Hadamard (1865–1965). Le second est un des plus grands mathématiciens français [9]. Élève brillant, il avait été classé premier aux deux concours de l'École Normale Supérieure et de l'École Polytechnique, avec une moyenne record de 18.34 au second. D'une longévité scientifique exceptionnelle, il écrivit son dernier livre sur les équations aux dérivées partielles à plus de 90 ans. On dit qu'il a inspiré le personnage du « Savant Cosinus » (mais on le dit aussi d'Émile Picard). Ce qui est sûr c'est que sa distraction a plus d'une fois fait trembler ses proches. À l'occasion de vacances dans les Alpes en 1882, il était allé au glacier des Bossons avec sa petite sœur Germaine, alors âgée de sept ans, ramasser des plantes pour son herbier. De retour à la maison, sa mère lui demanda ce qu'il avait fait de Germaine. Il avoua qu'il l'avait oubliée et il courut pour la retrouver. Le début de sa carrière d'enseignant ne fut pas particulièrement facile. En 1892, le Vice-Recteur de l'Académie de Paris en appelle au Ministre [10].

> Le dernier rapport bimensuel de M. le Proviseur du Lycée Buffon contient au sujet de M. Hadamard la note suivante.
>
> « Les classes de M. Hadamard laissent de plus en plus à désirer. Aucun souci des intérêts moraux des élèves petits et grands. Aucune autorité sur eux. Une discipline cassante et capricieuse. Des plaintes continuelles et des demandes de punition faciles à éviter avec un peu de fermeté et de bonté sérieuse. Nulle préparation pratique des classes. M. Hadamard se croit dispensé de tout par ses remarquables aptitudes mathématiques. Plus nous allons, plus nous sacrifions le bien public aux convenances personnelles de ce jeune savant ».

9. V.G. Maz'ia, T. Shaposhnikova : Jacques Hadamard, un mathématicien universel, *EDP Sciences, 2005*

10. Cette lettre m'a été aimablement communiquée par Claudine Schwartz, petite-nièce de Jacques Hadamard

> J'invite M. l'Inspecteur d'Académie Piéron à voir la classe de M. Hadamard. J'aurai l'honneur de vous rendre compte.
>
> Je suis avec respect, M. le Ministre, votre très humble et très obéissant serviteur.

Comme le dit Paul Montel,

> Heureusement, une admirable compagne veillait sur lui. Madame Hadamard avait tout de suite compris le rôle qu'elle pouvait jouer auprès d'un homme de génie. Avec une générosité constante, elle a su protéger son travail. D'une grande intelligence, la Mathématique agissait sur elle comme par induction.

Qualifiée par Mittag-Leffler de « secrétaire admirable et infatigable », elle débarrassa son mari de toute contingence matérielle, et se chargea de sa correspondance et de ses écrits. Hadamard lui dictait en sténo ses lettres et ses articles, lui indiquant simplement les espaces qu'elle devait laisser pour les formules mathématiques. La vie n'a pourtant pas épargné le couple. Leurs deux fils aînés étaient morts à quelques semaines d'intervalle à Verdun en 1916. Leur troisième fils devait mourir durant la seconde guerre mondiale. Ni la célébrité du père, ni le sacrifice des fils n'empêchèrent la famille d'être victime des persécutions anti-juives de Vichy, et de devoir s'exiler en 1941. À son arrivée aux États-Unis, Hadamard est d'abord nommé sur un poste de professeur invité à l'Université de Columbia à New-York. Mais la guerre se prolonge et Hadamard doit chercher un travail pour nourrir sa famille. Il a beau être célèbre, il a tout de même 77 ans et les scientifiques européens sont nombreux à chercher du travail. Son neveu Laurent Schwartz rapporte l'anecdote suivante.

> Il arriva dans une petite université et fut reçu par le directeur du département de mathématiques. Il expliqua qui il était et remit son Curriculum Vitæ. Le directeur lui dit : « Nos possibilités sont limitées et je ne peux pas vous promettre de vous prendre ».
>
> Hadamard remarqua que parmi les portraits accrochés au mur figurait le sien. « C'est moi » dit-il. « Bien, revenez la semaine prochaine ». Lorsqu'il se présenta, la réponse était négative et son portrait avait été enlevé.