# Arithmétique

En guise d'introduction rappelons que les *nombres* : un, deux, trois... sont utilisés pour compter les éléments d'un ensemble d'objets. Le zéro est utilisé pour désigner l'absence d'objet dans un ensemble. Il a été introduit (seulement) au V$^{\text{ème}}$ siècle après J.C. par les indiens : c'était un concept plus difficile à créer tout simplement parce qu'à l'époque on ne comptait pas les éléments d'ensembles qui n'en avaient pas. L'Arithmétique est l'étude des nombres entiers.

Rappelons aussi que les *chiffres* : 0,1,. . . ,9 sont les symboles des dix premiers nombres. Dans la notation décimale, ils servent à écrire tous les nombres.

## 1 Les entiers

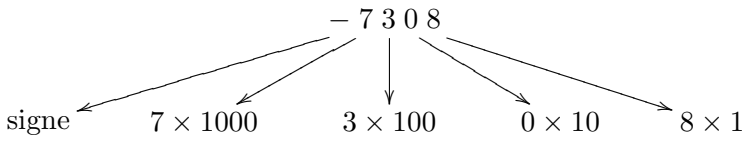
### 1.1 Entiers naturels et entiers relatifs

Les *entiers naturels* sont les nombres de l'ensemble

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

Les *entiers relatifs* sont les nombres de l'ensemble $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ c'est-à-dire les entiers naturels et leurs *opposés* ([1]).

La notation décimale d'un entier relatif utilise les symboles +,- et les chiffres de la façon suivante : « moins sept mille trois cent huit » est noté




### 1.2 Ordre et opérations sur les entiers

Il existe une relation d'*ordre* entre les entiers relatifs. On utilise la notation habituelle $m \leq n$ pour « $m$ est inférieur ou égal à $n$ » ainsi que les notations parentes $m < n$, $n \geq m$, $n > m$.

Les opérations de base sur les entiers sont l'*addition* et la *multiplication*. Soit $m$ et $n$ deux entiers relatifs avec $n > 0$. Une autre façon de voir le produit $mn$ est de dire que c'est le multiple $n$-uple de $m$ c'est-à-dire la répétition $n$ fois de l'addition, i.e. $mn = m + \cdots + m$ ($n$ termes). De même si on répète $n$ fois la multiplication de $m$ par lui-même on obtient

[1] On utilise les lettres $\mathbb{N}$ et $\mathbb{Z}$ pour les mots allemands *Nummer* et *Zahl*.

la *puissance* $n^{\text{ème}}$ *de* $m$ notée $m^n$ : $m^n = m \times \cdots \times m$ ($n$ termes). Cette opération a aussi un sens pour tout $m \in \mathbb{Z}$ ; enfin rappelons que par convention on pose $m^0 = 1$ si $m \neq 0$.

Nous supposons connues les propriétés élémentaires de ces opérations. Rappelons simplement une propriété essentielle qui est que ces opérations sont *compatibles* avec la relation d'ordre. Pour l'addition cela veut dire que pour tous entiers relatifs $m, n, p, q$ on a

$$(m \leq n \quad \text{et} \quad p \leq q) \quad \Rightarrow \quad m + p \leq n + q$$

On déduit facilement une compatiblité similaire pour la multiplication mais soyez méfiants car pour l'écrire correctement il faut tenir compte du signe des entiers.

**Exercice 1.2.1** Soient deux entiers $0 \leq k \leq n$. Le coefficient binômial $\mathrm{C}_n^k$ est défini [2] par

$$\mathrm{C}_n^k := \frac{n!}{k!(n-k)!}$$

(rappelons que $n! \stackrel{\text{déf}}{=} 1 \times 2 \times \cdots \times n$ est la *factorielle* de $n$). On verra plus loin que, même si ce n'est pas évident, c'est bien un nombre entier.

(a) Démontrez que $\mathrm{C}_n^{n-k} = \mathrm{C}_n^k$ et que si $1 \leq k \leq n$, on a $k\mathrm{C}_n^k = n\mathrm{C}_{n-1}^{k-1}$.

(b) Démontrez que si $0 \leq k \leq n-1$ on a $\mathrm{C}_n^k + \mathrm{C}_n^{k+1} = \mathrm{C}_{n+1}^{k+1}$.

## 1.3 Le principe de récurrence

L'ensemble des entiers naturels $\mathbb{N}$ possède une propriété très intuitive qui a deux énoncés équivalents, contenus dans les propositions 1.3.1 et 1.3.2 qui suivent. Nous ne les démontrons pas : ce sont notre point de départ intuitif pour raisonner sur les nombres entiers. (Le fait qu'elles sont équivalentes est démontré en exercice.)

**Proposition 1.3.1** *Tout ensemble non vide d'entiers naturels contient un entier inférieur ou égal à tous les autres.*

Cette popriété est équivalente à la suivante qui est le *principe de récurrence* :

**Proposition 1.3.2** *Soit $n_0 \geq 0$ un entier. Soit $P(n)$ une propriété dépendant d'un nombre entier $n \geq n_0$. Supposons que*

(i) *$P(n_0)$ est vraie ($P$ est initialisée), et*

(ii) *$P(n) \Rightarrow P(n+1)$ pour tout $n \geq n_0$ ($P$ est héréditaire).*

*Alors la propriété $P(n)$ est vraie pour tout $n \geq n_0$.*

Donnons des exemples d'application.

[2] Une remarque de notation : lorsqu'on utilise le signe « = » pour définir un objet mathématique il est préférable d'utiliser l'un des deux signes « := » ou « $\stackrel{\text{déf}}{=}$ » pour ne pas confondre avec le « = » utilisé pour noter une *égalité*.

**Exemple 1.3.3** Comme application de la proposition 1.3.1 démontrons que tout nombre entier $n \geq 2$ est divisible par un nombre premier (un nombre premier est un nombre $p \geq 2$ qui n'est divisible que par 1 et lui-même). Soit $E$ l'ensemble des entiers naturels $k \geq 2$ qui divisent $n$. On a $n \in E$ donc $E$ n'est pas vide : d'après la proposition 1.3.1 il possède donc un plus petit élément $p$. Ce nombre $p$ est forcément premier car si $r$ est un de ses diviseurs on a soit $r = 1$, soit $r \in E$. Or lorsque $r \in E$ on a $p \leq r$ (car $p$ est plus petit que tous les éléments de $E$) et $r \leq p$ (car $r$ divise $p$) donc $r = p$.

**Exercice 1.3.4** Montrer par récurrence que les coefficients binômiaux $\mathrm{C}_n^k$ sont entiers.
(*Indication* : prendre pour $P(n)$ : « pour tout $k$ tel que $0 \leq k \leq n$ on a $\mathrm{C}_n^k \in \mathbb{N}$ ».)

**Exemple 1.3.5** Démontrons par récurrence la formule du *binôme de Newton* : pour tout $n \geq 1$ et tout couple $(x, y)$ de nombres entiers, réels ou même complexes on a

$$(x+y)^n = \sum_{k=0}^{n} \mathrm{C}_n^k x^k y^{n-k}$$

(On rappelle que si on a des nombres $a_0, \ldots, a_n$ alors $\sum_{k=0}^{n} a_k$ désigne la somme $a_0 + a_1 + \cdots + a_n$.) Pour $n = 1$ l'égalité est claire. De plus si elle est vraie pour un entier $n \geq 1$ alors

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y)\sum_{k=0}^{n} \mathrm{C}_n^k x^k y^{n-k} \\
&= x(\mathrm{C}_n^0 x^0 y^n + \cdots + \mathrm{C}_n^n x^n y^0) + y(\mathrm{C}_n^0 x^0 y^n + \cdots + \mathrm{C}_n^n x^n y^0) \\
&= (0 + \mathrm{C}_n^0)x^0 y^{n+1} + \cdots + (\underbrace{\mathrm{C}_n^{k-1} + \mathrm{C}_n^k}_{\mathrm{C}_{n+1}^k})x^k y^{n+1-k} + \cdots + (\mathrm{C}_n^n + 0)x^{n+1} y^0 \\
&= \sum_{k=0}^{n+1} \mathrm{C}_{n+1}^k x^k y^{n+1-k}
\end{aligned}$$

La propriété est héréditaire donc elle est vraie pour tout $n \geq 1$.

# 2 La division euclidienne

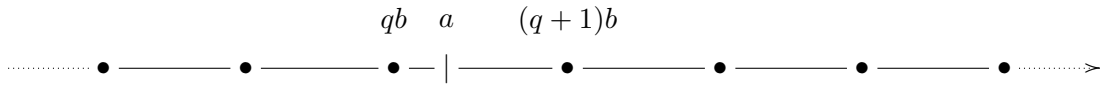
La division euclidienne est l'un des piliers de l'arithmétique. Comme nous allons le voir elle est à la base du système de numération en base dix utilisé aujourd'hui.

On sait peu de choses sur Euclide. Il vécut aux alentours de $-300$, enseigna et écrivit au Musée et à la Bibliothèque d'Alexandrie. Son traité *Les Éléments*, composé de treize *livres*, a un style et une profondeur qui en font l'un des textes mathématiques les plus importants de tous les temps. La division euclidienne (connue en fait bien avant Euclide) est démontrée dans le *Livre VII*.

## 2.1 Le théorème de division euclidienne

Soient $a$ et $b$ deux entiers naturels, avec $b \neq 0$. Si $a$ est un multiple de $b$ on a $a = bq$ pour un certain entier $q$. Si ce n'est pas le cas, on peut essayer d'approximer $a$ à l'aide de

multiples de $b$. Pour faire cela on place $a$ ainsi que tous les multiples de $b$ sur l'axe des nombres entiers, et on constate que $a$ est situé *entre deux de ces multiples, bien déterminés* :




(si $a$ est un multiple de $b$ on choisit l'intervalle qui est à sa droite). Ceci explique le théorème suivant :

**Théorème 2.1.1** *Soit $a, b \in \mathbb{N}$ deux entiers naturels avec $b > 0$. Alors, il existe un unique couple d'entiers $(q, r)$, tel que*

(i) $a = bq + r$

(ii) $0 \leq r < b$.

*L'écriture dans (i) s'appelle la* division euclidienne *de $a$ par $b$. On dit que $a$ est le* dividende*, $b$ le* diviseur*, $q$ le* quotient *et $r$ le* reste*.*

Pour démontrer cela l'idée est de chercher d'abord $q$, et pour cela de regarder l'ensemble de tous les multiples de $b$ qui sont plus grands que $a$. Précisément :

**Démonstration :** Soit $E := \{\, k \in \mathbb{N}\,,\; kb > a\,\}$. Cet ensemble est non vide, en effet, en utilisant le fait que $b \geq 1$ on voit que $a + 1 \in E$. Donc d'après 1.3.1 il possède un plus petit élément $u$. Soit $q = u - 1$. Comme $q \notin E$ et $q + 1 \in E$ on a $qb \leq a < (q + 1)b$. Donc $r = a - bq$ vérifie : $0 \leq r < b$.

Montrons maintenant que ce couple $(q, r)$ qui a les propriétés requises, est unique. Supposons qu'on ait deux écritures $a = bq + r = bq' + r'$ avec $0 \leq r, r' < b$. On a alors $|r' - r| < b$ et simultanément $r' - r$ est un multiple de $b$ car $r' - r = b(q - q')$. Donc nécessairement $r' - r = 0$ et par conséquent $q' - q = 0$ également. □

En fait, on peut facilement démontrer que si $a \in \mathbb{Z}$, le résultat du théorème reste vrai sous la forme suivante : il existe un unique couple $(q, r)$ avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$, tel que (i) $a = bq + r$ et (ii) $0 \leq r < b$.

**Exercice 2.1.2** Samy range 461 pots de yaourt dans des caisses. Il ne commence pas une caisse avant d'avoir fini la précédente. À la fin il a rangé les pots dans 14 caisses. Combien de pots contiennent les caisses pleines ? Combien de pots contient la dernière caisse ?

L'application la plus importante du théorème de division euclidienne (en abrégé DE) est l'écriture en base $b$ qui permet d'écrire tous les nombres avec un nombre fini de symboles.

## 2.2 Écriture d'un entier en base $b$

Regardons le cas de la base $b = 10$ qui nous est familier. On effectue successivement les DE par 10 de $a = 7308$ puis des quotients qui apparaissent :

$$\begin{array}{rcrll} 7308 & = & 730 \times 10 + 8 & \text{on pose} & a_1 := 730 \quad \text{(c'est le quotient)} \\ 730 & = & 73 \times 10 + 0 & \text{〃} & a_2 := 73 \\ 73 & = & 7 \times 10 + 3 & \text{〃} & a_3 := 7 \\ 7 & = & 0 \times 10 + 7 & \text{et on a} & a_4 := 0 \end{array}$$

On voit que les restes $r_0, r_1, r_2, r_3$ de ces DE donnent la suite des chiffres de l'écriture en base dix du nombre $a = 7308$ à savoir $7308 = 7 \times 10^3 + 3 \times 10^2 + 0 \times 10^1 + 8$. Plus généralement :

**Théorème 2.2.1** *Soit $b \geq 2$ un entier. Alors pour tout entier $a \geq 1$ il existe un unique $n$ et d'uniques entiers $r_0, \ldots, r_n$ tels que*

(i) $a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$ *avec* $r_n \neq 0$, *et*

(ii) $0 \leq r_i < b$ *pour tout* $i$.

*Cette écriture est appelée l'* écriture de $a$ en base $b$, *et les $r_i$ sont ses* chiffres.

**Démonstration :** Supposons qu'existe une écriture $a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$ avec la condition (ii). Alors $r_0$ est le reste de la DE de $a$ par $b$, qui est unique d'après le théorème de division euclidienne. Posons $a_0 := a$ et $a_1 := \frac{a_0 - r_0}{b}$ qui est égal à $r_n b^{n-1} + r_{n-1} b^{n-2} + \cdots + r_1$. Alors $r_1$ est le reste de la DE de $a_1$ par $b$. On continue en définissant par récurrence $a_i := \frac{a_{i-1} - r_{i-1}}{b}$. On voit que $a_i = r_n b^{n-i} + \cdots + r_i$ et donc $r_i$ est le reste de la DE de $a_i$ par $b$, unique donc. Enfin le nombre $n$ est bien déterminé comme étant le premier instant $i$ du processus où $a_i = r_i$. On a montré que les nombres $n$ et $r_0, \ldots, r_n$ s'ils existent, sont uniquement déterminés.

Partons maintenant de $a$ et $b$ et montrons qu'il y a en effet une telle écriture. D'après ce qu'on a fait avant on sait comment faire : on effectue des DE successives (en notant $a_i$ les quotients et $r_i$ les restes) :

$$\begin{array}{rcll} a & = & ba_1 + r_0 & (0 \leq r_0 < b) \\ a_1 & = & ba_2 + r_1 & (0 \leq r_1 < b) \\ & \vdots & & \\ a_k & = & ba_{k+1} + r_k & (0 \leq r_k < b) \\ & \vdots & & \end{array}$$

Comme $b \geq 2$, les $a_k$ sont de plus en plus petits : $a_{k+1} \leq \frac{1}{b} a_k < a_k$. Donc il vient un instant où $a_n < b$ c'est-à-dire $a_n = r_n$ et $a_{n+1} = 0$. En remplaçant successivement $a$, $a_1$, $a_2$... par leurs expressions ci-dessus on a

$$\begin{aligned} a &= a_1 b + r_0 = a_2 b^2 + r_1 b + r_0 = a_3 b^3 + r_2 b^2 + r_1 b + r_0 = \ldots \\ &= r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0 \end{aligned}$$

ce qui est l'écriture recherchée. □

Le nombre 0, quant à lui, s'écrit 0 dans toutes les bases (son écriture en base $b$ a cependant cela de particulier qu'elle ne vérifie pas la condition $r_n \neq 0$).

## 2.3 Notation de l'écriture en base $b$ et exemples de bases

Pour noter un nombre $a$ à l'aide de ses chiffres en base $b$ on écrira $a = \overline{r_n r_{n-1} \ldots r_0}_{(b)}$. Cela veut dire exactement que $a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$. Dans le cas de la base $b = 10$, quand ça ne risquera pas de prêter à confusion on notera comme d'habitude $r_n r_{n-1} \ldots r_0$ plutôt que $\overline{r_n r_{n-1} \ldots r_0}_{(\text{dix})}$.

**Exemple 2.3.1** Le théorème 2.2.1 nous apprend qu'on peut représenter tous les entiers déjà à l'aide de $b = 2$. On parle d'écriture *binaire*. Ce choix de base est particulièrement adapté aux ordinateurs : la tension aux bornes de leurs circuits physiques (des transistors utilisés comme interrupteurs) ne peut prendre que deux valeurs qu'on note 0 et 1. Toute information est codée dans un ordinateur à l'aide de 0 et de 1. Ce sont ces deux symboles qu'on utilise pour écrire les nombres en binaire. Par exemple le nombre $17 = 2^4 + 1$ s'écrit 10001 en binaire.

Avant d'envisager de noter les nombres ainsi il faut avoir fait un choix de $b$ symboles pour désigner $0, 1, \ldots, b$. Si $b > 10$ comme dans l'exemple suivant, on n'a pas de symbole évident à disposition !

**Exemple 2.3.2** Une autre base utilisée parfois est $b = 16$. On parle d'écriture *hexadécimale*. La raison de son utilisation est aussi liée à l'ordinateur et à la base 2. Ses chiffres sont $0, 1, \ldots, 9, A, B, C, D, E, F$ qui désignent les 16 premiers entiers ($A$ pour 10, etc). Ainsi, en hexadécimal $1B2$ représente le nombre $1 \times 16^2 + 11 \times 16 + 2 = 434$ (en base dix) et $\overline{45}_{(\text{dix})}$ s'écrit $2D$ en hexadécimal.

## 2.4 Repères historiques sur la numération

*À l'aube de l'Humanité.* La nécessité de compter s'est faite ressentir très tôt : par exemple un berger devait pouvoir compter les brebis de son troupeau, et clairement les mains ne suffisent pas très longtemps pour faire cela.

*Égyptiens et Babyloniens.* L'Homme a su compter avant de savoir écrire : dès -3000 les Égyptiens écrivirent les nombres en les notant sous forme de hiéroglyphes. Les Babyloniens écrivirent les nombres avec leur écriture cunéiforme ([3]). Pour les calculs les Babyloniens avaient déjà un système à base ; la base utilisée était 60 ce qui a laissé quelques traces dans les systèmes de numération que l'on utilise aujourd'hui (minutes, secondes).

*En Extrême-Orient.* Les Chinois et les Indiens aussi ont compté très tôt mais on a moins de traces de leurs mathématiques avant le Moyen-Âge. Les Chinois avaient des symboles pour les nombres de 1 à 9 et pour les puissances de 10. Faute de pouvoir manipuler des dessins chinois notons ♯ à la place du symbole que les chinois utilisaient pour 10 et ♠ pour 100 : le nombre 729 était noté 7♠2♯9. Observez que c'est très similaire à notre numération *parlée* : les puissances de dix n'ont de nom que jusqu'à une certaine taille, dans tous les langages ([4])...

*Les romains.* Ils avaient des symboles pour les puissances de 10 seulement (au début en tous cas) et ils les juxtaposaient pour écrire tous les nombres. C'est donc un système de numération additif. Les symboles de 1, 10, 100, 1000 sont I, X, C, M. Par la suite le système fut rafiné avec l'introduction d'un symbole pour 5 (V) et ses décuples 50 (L), 500 (D).

*Le système à base dix utilisée aujourd'hui.* Dans ce système les chiffres n'ont pas la même siginification selon leur place dans l'écriture du nombre (729 et 297 ne sont pas le même nombre !). Pour cette raison on dit que c'est un système de numération *positionnel à base dix*. Par opposition les systèmes tels que la numération romaine ou égyptienne sont dits *systèmes de numération non positionnels additifs*.

[3] Voir http://classes.bnf.fr/dossiecr/in-cunei.htm

[4] Voir http://perso.club-internet.fr/petrequin/mathema/traites/gnombres/gn_nombres.html

# 3 Divisibilité et congruences

## 3.1 Premières propriétés

Rappelons la définition :

**Définition 3.1.1** Soit $a, b \in \mathbb{Z}$.
On dit que $b$ *divise* $a$ lorsqu'il existe $q \in \mathbb{Z}$ tel que $a = qb$.
On note alors $b|a$. On dit aussi que $a$ *est multiple de* $b$, ou que $b$ *est un diviseur de* $a$.

Par exemple 1 divise tout entier; tout entier divise 0; et l'ensemble des diviseurs de 25 est $\{-25, -5, -1, 1, 5, 25\}$. Souvent on ne mentionnera que l'ensemble des diviseurs dans $\mathbb{N}$ ; pour 25 c'est $\{1, 5, 25\}$. Il est clair que si $a_1$ et $a_2$ sont multiples de $b$ alors il en est de même pour $a_1 + a_2$, $a_1 - a_2$ et aussi $na_1$ pour tout $n$.

**Définition 3.1.2** Soit $n > 0$ un entier naturel. On dit que deux entiers $a, b \in \mathbb{Z}$ sont *congrus entre eux modulo* $n$ lorsque $n$ divise $a - b$. Plusieurs notations sont utilisées :

$$a \equiv b \bmod n \quad \text{ou} \quad a \equiv b \,(\bmod n) \quad \text{ou parfois} \quad a \equiv b\,(n)$$

Un nombre $a > 0$ est congru modulo $n$ à exactement *un* entier compris entre 0 et $n-1$, qui n'est rien d'autre que le reste de la DE de $a$ par $n$. En particulier :

**Remarque 3.1.3 (cruciale)** C'est la même chose de dire « $n$ divise $a$ » ou « $a \equiv 0\,(n)$ ».

La relation de congruence modulo $n$ est vraiment très puissante du fait qu'elle se comporte comme une égalité à bien des égards :

**Proposition 3.1.4** *Soit $a, a', b, b', c \in \mathbb{Z}$ et $k \in \mathbb{N}$. Alors on a :*

| | | |
|---|---|---|
| (1) | $a \equiv a\,(n)$ | (réflexivité) |
| (2) | *si* $a \equiv b\,(n)$ *alors* $b \equiv a\,(n)$ | (symétrie) |
| (3) | *si* $a \equiv b\,(n)$ *et* $b \equiv c\,(n)$ *alors* $a \equiv c\,(n)$ | (transitivité) |
| (4) | *si* $a \equiv b\,(n)$ *et* $a' \equiv b'\,(n)$ *alors* $a + a' \equiv b + b'\,(n)$ | (compatibilité avec $+$) |
| (5) | *si* $a \equiv b\,(n)$ *alors* $-a \equiv -b\,(n)$ | (compatibilité avec $-$) |
| (6) | *si* $a \equiv b\,(n)$ *et* $a' \equiv b'\,(n)$ *alors* $aa' \equiv bb'\,(n)$ | (compatibilité avec $\times$) |
| (7) | *si* $a \equiv b\,(n)$ *alors* $a^k \equiv b^k\,(n)$ | (comp. avec les puissances) |

**Démonstration :** D'abord (1), (2) et (5) sont évidentes. Ensuite :

(3) découle du fait que si $a - b = nq_1$ et $b - c = nq_2$ alors $a - c = n(q_1 + q_2)$.

(4) découle du fait que si $a - a' = nq_1$ et $b - b' = nq_2$ alors $(a + a') - (b + b') = n(q_1 - q_2)$.

(6) découle du fait que si $a - b = nq_1$ et $a' - b' = nq_2$ alors

$$aa' - bb' = a(a' - b') + (a - b)b' = anq_2 + b'nq_1 = n(aq_2 + b'q_1)$$

(on fait apparaître « de force » les différences $a - b$ et $a' - b'$ qui nous intéressent).

(7) se déduit de (6) par récurrence, ou bien directement, car si $a - b = nq_1$ alors

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}) = nq_1(a^{k-1} + \cdots + b^{k-1})$$

□

En revanche, on se méfiera du fait que cela n'a pas de sens en général de vouloir utiliser la relation d'ordre avec les congruences. Par exemple on voit bien que l'inégalité $8 \leq 12$ ne « passe pas » modulo 5 puisque $8 \equiv 3\,(5)$ et $12 \equiv 2\,(5)$.

### 3.2 Critères de divisibilité

Une application immédiate de la notion de congruence est de démontrer les critères classiques de divisibilité ([5]). Soit $a$ un entier, écrit $r_n r_{n-1} \dots r_1 r_0$ en base dix. Les principaux critères à connaître sont les suivants :

2, 5 et 10

• $a$ est divisible par 2 si et seulement si son dernier chiffre $r_0$ est divisible par 2.

• $a$ est divisible par 5 si et seulement si son dernier chiffre $r_0$ est divisible par 5.

• $a$ est divisible par 10 si et seulement si son dernier chiffre $r_0$ est nul.

4 et 25

• $a$ est divisible par 4 si et seulement si le nombre $r_1 r_0$ (en base dix) formé par ses deux derniers chiffres, est divisible par 4.

• $a$ est divisible par 25 si et seulement si le nombre $r_1 r_0$ (en base dix) formé par ses deux derniers chiffres, est divisible par 25.

3 et 9

• $a$ est divisible par 3 si et seulement si la somme des chiffres de son écriture décimale $r_n + \cdots + r_0$ est divisible par 3.

• $a$ est divisible par 9 si et seulement si la somme des chiffres de son écriture décimale $r_n + \cdots + r_0$ est divisible par 9.

**Démonstration :** Démontrons seulement les critères de divisibilité par 2 et 9.

Étant donnée l'écriture en base dix $a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0$ on voit que $a \equiv r_0\,(2)$. Donc $a \equiv 0\,(2)$ si et seulement si $r_0 \equiv 0\,(2)$ qui est le critère recherché pour la divisibilité par 2.

Pour 9 il suffit de remarquer que $10 \equiv 1(9)$ donc $10^k \equiv 1^k \equiv 1(9)$ pour tout $k \geq 0$. Donc $a \equiv r_n + r_{n-1} + \cdots + r_1 + r_0 (9)$. Donc $a \equiv 0(9)$ si et seulement si $r_n + r_{n-1} + \cdots + r_1 + r_0 \equiv 0(9)$.

Prouvez les autres critères en exercice. □

## 4 Plus grand commun diviseur, plus petit commun multiple

### 4.1 Le pgcd

**Proposition et définition 4.1.1** *Soit $a, b \in \mathbb{N}$, non tous les deux nuls. L'ensemble des diviseurs communs de $a$ et $b$ dans $\mathbb{N}$ est fini et non vide. Il a un plus grand élément qu'on appelle leur* plus grand commun diviseur *noté* $\mathrm{pgcd}(a, b)$.

**Démonstration :** Par hypothèse $a$ ou $b$ est non nul, disons $a$. Alors les diviseurs de $a$ et $b$ dans $\mathbb{N}$ sont inférieurs à $a$, donc ils forment un ensemble fini, non vide car 1 en fait partie. Cet ensemble a donc un plus grand élément. □

[5] Un critère est une condition *suffisante*. Souvent le mot est utilisé aussi (c'est un léger abus) pour signifier une condition *nécessaire et suffisante*. C'est le cas ici.

**Définition 4.1.2** On dit que $a$ et $b$ sont *premiers entre eux* ssi $\text{pgcd}(a,b) = 1$.

Voici quelques exemples.

(a) Les diviseurs communs de 24 et 30 sont $1, 2, 3, 6$ et leur pgcd est donc 6.

(b) Le seul diviseur commun de 24 et 25 est 1 donc leur pgcd est 1.

(c) Si $b|a$ alors $\text{pgcd}(a,b) = b$. Par exemple $\text{pgcd}(a,1) = 1$.

## 4.2 Algorithme d'Euclide et théorème de Bézout

**Proposition 4.2.1** *Soit $a, b \in \mathbb{N}$, non tous les deux nuls. Effectuons la division euclidienne de $a$ par $b$, soit $a = bq + r$ avec $0 \leq r < b$. Alors les diviseurs communs de $a$ et $b$ sont les mêmes que ceux de $b$ et $r$, en particulier,* $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

**Démonstration :** Comme $r = a - bq$ il est clair qu'un diviseur commun de $a$ et $b$ divise $b$ et $r$. De même comme $a = bq + r$ un diviseur commun de $b$ et $r$ divise $a$ et $b$. □

Supposons que $b < a$. En changeant $a$ et $b$ par $b$ et $r$ on ne change pas le pgcd. Ce qui est très utile là-dedans, c'est que les nombres considérés maintenant sont moins grands et on peut itérer le processus : $b$ devient le nouveau dividende, $r$ devient le nouveau diviseur et on peut refaire une DE. Ainsi pour 490 et 154,

$$\begin{aligned} 490 &= 3 \times 154 + 28 \\ 154 &= 5 \times 28 + 14 \\ 28 &= 2 \times 14 + 0 \end{aligned}$$

Tant que les restes des DE effectuées sont non nuls ils sont strictement décroissants : $154 > 28 > 14 > \ldots$ Donc ils finissent par s'annuler, ce qui met fin au processus. À ce moment-là on calcule $\text{pgcd}(490, 154) = \text{pgcd}(154, 28) = \text{pgcd}(28, 14) = 14$. On voit que le pgcd est le dernier reste non nul du processus de divisions euclidiennes par les restes successifs.

Le résultat général est le suivant :

**Théorème 4.2.2 (Algorithme d'Euclide)** *Soit $a, b \in \mathbb{N}$ avec $b < a$. On pose $r_0 := a$ et $r_1 := b$. Par récurrence, tant que $r_k \neq 0$ on définit $r_{k+1}$ comme étant le reste de la DE de $r_{k-1}$ par $r_k$ :*

$$r_{k-1} = r_k q_k + r_{k+1} \qquad \text{avec} \quad 0 \leq r_{k+1} < r_k$$

*Le* pgcd *de $a$ et $b$ est le dernier reste non nul de cet algorithme.*

**Démonstration :** On a une suite strictement décroissante $r_0 > r_1 > r_2 > \ldots$ constituée par les restes non nuls successifs. Elle forme un sous-ensemble non vide de $\mathbb{N}$ donc elle a un plus petit élément (prop. 1.3.1) noté $r_n$. On a donc $r_{n+1} = 0$ (car sinon il serait strictement inférieur à $r_n$) c'est-à-dire $r_n | r_{n-1}$. D'après la proposition 4.2.1 on a :

$$\text{pgcd}(a,b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \cdots = \text{pgcd}(r_{n-1}, r_n) = r_n$$

c'est ce que l'on voulait. □

Le mot *algorithme* vient du nom d'un grand mathématicien arabe, Al-Khwārizmī (780-850). Le mot algèbre vient du mot arabe *al-jabr* que l'on peut traduire par *restaurer* (pour les mathématiciens arabes, *al-jabr* signifiait faire passer de l'autre côté d'une équation une quantité qui était « soustraite » pour la transformer en quantité « ajoutée »). Les mots *chiffre* et *zéro* dérivent tous les deux du mot arabe *sifr*, lui-même provenant du sanscrit *sūnyā* qui signifiait *vide*.

**Théorème 4.2.3 (Bézout)** *Soit $a, b \in \mathbb{N}$ non tous les deux nuls et soit $d = \text{pgcd}(a, b)$. Alors,*

(1) *Il existe $\lambda, \mu \in \mathbb{Z}$ tels que $d = \lambda a + \mu b$.*

(2) *$a$ et $b$ sont premiers entre eux si et seulement s'il existe $\lambda, \mu \in \mathbb{Z}$ tels que $1 = \lambda a + \mu b$.*

**Démonstration :** En fait la propriété (1) est vraie pour tous les restes de l'algorithme d'Euclide, pas seulement le dernier : pour tout $k \geq 0$ il existe $\lambda_k$, $\mu_k$ tels que $r_k = \lambda_k a + \mu_k b$. Pour $k = 0$ et $k = 1$ c'est clair car $r_0 = a$ (prendre $\lambda = 1$, $\mu = 0$) et $r_1 = b$ ($\lambda = 0$, $\mu = 1$). Par récurrence il suffit maintenant de prouver que cette propriété ([6]) est héréditaire. Or d'après la DE $r_{k-1} = r_k q_k + r_{k+1}$ on a

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k = (\lambda_{k-1} a + \mu_{k-1} b) - (\lambda_k a + \mu_k b) q_k \\ &= (\lambda_{k-1} - \lambda_k q_k) a + (\mu_{k-1} - \mu_k q_k) b \end{aligned}$$

d'où le résultat découle en posant $\lambda_{k+1} := \lambda_{k-1} - \lambda_k q_k$ et $\mu_{k+1} := \mu_{k-1} - \mu_k q_k$.

Passons à (2). Si $a$ et $b$ sont premiers entre eux on a $d = 1$ donc il existe $\lambda, \mu \in \mathbb{Z}$ tels que $1 = \lambda a + \mu b$ d'après (1). Réciproquement si $1 = \lambda a + \mu b$ alors soit $d$ un diviseur commun de $a$ et $b$ dans $\mathbb{N}$, il divise $\lambda a + \mu b$, donc divise 1, donc $d = 1$. □

Étienne Bézout (1730-1783) est un mathématicien français né à Nemours. Il laissa son nom au théorème qui est dans notre cours ainsi qu'à un théorème de Géométrie Algébrique qui compte le nombre de points d'intersection de deux courbes planes définies par des polynômes (en deux variables $x, y$) de degrés $m$ et $n$.

**Remarque 4.2.4** L'utilité du point (2) du théorème est inestimable. Retenez comme un refrain :

$$\text{« } a \text{ et } b \text{ premiers entre eux} \Leftrightarrow 1 = \lambda a + \mu b \text{ »}$$

L'algorithme d'Euclide donne un moyen de *déterminer pratiquement* (algorithmiquement) *une relation de Bézout*. La règle est la suivante. Les divisions euclidiennes de l'algorithme d'Euclide s'écrivent $r_{k-1} = r_k q_k + r_{k+1}$ (avec $0 \leq r_{k+1} < r_k$). On les « renverse » :

$$r_{k+1} = r_{k-1} - r_k q_k$$

et on remonte le calcul en partant du pgcd : $d = r_n = r_{n-2} - r_{n-1} q_{n-1} = \ldots$ en remplaçant successivement les restes.

[6] Quelle propriété $P(k)$ doit-on prendre exactement pour faire fonctionner la récurrence ?

**Exemple 4.2.5** Traitons en exemple $a = 1197$ et $b = 210$. L'algorithme d'Euclide donne

$$\begin{aligned} 1197 &= 5 \times 210 + 147 \\ 210 &= 1 \times 147 + 63 \\ 147 &= 2 \times 63 + 21 \\ 63 &= 3 \times 21 \end{aligned}$$

Donc $\text{pgcd}(1197, 210) = 21$ et en remontant les divisions :

$$\begin{aligned} 21 = &\ 147 - 2 \times 63 = 147 - 2 \times (210 - 147) = 3 \times 147 - 2 \times 210 \\ = &\ 3 \times (1197 - 5 \times 210) - 2 \times 210 = 3 \times 1197 - 17 \times 210 \end{aligned}$$

C'est une relation de Bézout.

**Exercice 4.2.6** (1) Soient $a, b, c \in \mathbb{N}$ non nuls. On suppose que $a$ est premier avec $b$ et premier avec avec $c$. Montrez qu'il est premier avec $bc$. (*Indic : écrire deux relations de Bézout et les multiplier entre elles*)

(2) Soient $a, b, m, n \in \mathbb{N}$ non nuls. Montrez que $a$ est premier avec $b$ ssi $a^m$ est premier avec $b^n$. (*Indic : un seul sens est difficile : écrire une relation de Bézout et l'élever à la puissance $m + n - 1$*)

## 4.3 Propriétés importantes du pgcd

**Lemme 4.3.1 (Lemme de Gauß)** *Soit $a, b, c$ des entiers naturels avec* $\text{pgcd}(a, b) = 1$. *Si $a|bc$ alors $a|c$.*

**Démonstration :** Soit $\lambda a + \mu b = 1$ une relation de Bézout. Si $a$ divise $bc$ alors $a$ divise $\lambda ac + \mu bc$ c'est-à-dire $c$. □

Karl Friedrich Gauß (1777-1855) est né dans une famille de paysans ruinés venus s'installer dans la ville de Brunswick. Son génie mathématique se manifesta très tôt : en 1791, le Duc de Brunswick lui donna une bourse pour recevoir le meilleur enseignement possible. Il publia à 24 ans ses travaux en Arithmétique, les *Disquisitiones Arithmeticæ*. En 1807 il obtint un poste à l'Université de Göttingen où il resta jusqu'à la fin de sa vie. Gauß publia peu car il n'était jamais entièrement satisfait de ce qu'il avait écrit. Ses travaux couvrent aussi l'astronomie, l'électricité, l'électromagnétisme...
Plus de détails sont sur http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Gauss.html

**Proposition 4.3.2** *Soit $a, b \in \mathbb{N}$, non tous les deux nuls et* $d = \text{pgcd}(a, b)$. *Tout diviseur commun de $a$ et $b$ divise $d$.*

**Démonstration :** Soit $\lambda a + \mu b = d$ une relation de Bézout. Si $e$ divise $a$ et $b$, il divise $\lambda a + \mu b$ c'est-à-dire $d$. □

**Proposition 4.3.3** *Soit $a, b \in \mathbb{N}$, non tous les deux nuls. Soit $d \in \mathbb{N}$. Alors* $d = \text{pgcd}(a, b)$ *si et seulement s'il existe $a', b' \in \mathbb{N}$ tels que $a = da'$, $b = db'$ avec* $\text{pgcd}(a', b') = 1$.

**Démonstration :** Si $d = \text{pgcd}(a, b)$ alors il existe $a', b' \in \mathbb{N}$ tels que $a = da'$ et $b = db'$. De plus, si $e$ est un diviseur commun de $a'$ et $b'$ alors $de$ divise $a$ et $b$ donc $de \leq \text{pgcd}(a, b) = d$, donc $e = 1$.

Réciproquement supposons que $a = da'$ et $b = db'$ avec $\text{pgcd}(a', b') = 1$. On a une relation de Bézout $\lambda a' + \mu b' = 1$ donc $\lambda a + \mu b = d$. Ceci montre que si $e$ est un diviseur commun de $a$ et $b$ il divise $d$. En particulier, $e \leq d$ donc $d = \text{pgcd}(a, b)$. □

**Remarque 4.3.4** L'utilité de cette proposition est inestimable. Retenez comme un refrain :

$$\text{« } d = \text{pgcd}(a, b) \Leftrightarrow \begin{cases} a = da' \\ b = db' \end{cases} \text{ avec } \text{pgcd}(a', b') = 1 \text{ »}$$

**Exercice 4.3.5** (1) Soient $a, b \in \mathbb{N}$ non nuls et $d := \text{pgcd}(a, b)$. Montrez que $\text{pgcd}(a^n, b^n) = d^n$. (*Indic : utilisez la proposition 4.3.3 et l'exercice 4.2.6(2)*)

(2) Soient $a, b, n \in \mathbb{N}$ non nuls. Montrez que $a^n | b^n$ si et seulement si $a | b$. (*Indic : utilisez le fait que* $x | y$ *ssi* $\text{pgcd}(x, y) = x$ *et la question précédente*)

## 4.4 Le ppcm

Le ppcm est le pendant du pgcd (pour les multiples au lieu des diviseurs). Étant donnés deux entiers naturels $a$ et $b$ non nuls, l'ensemble des multiples communs non nuls de $a$ et $b$ dans $\mathbb{N}$ est non vide car il contient $ab$. D'après la proposition 1.3.1 il contient un plus petit élément :

**Définition 4.4.1** Soit $a, b \in \mathbb{N}$ non nuls. L'ensemble des multiples communs non nuls de $a$ et $b$ dans $\mathbb{N}$ a un plus petit élément qu'on appelle leur *plus petit commun multiple* noté $\text{ppcm}(a, b)$. Si $a$ ou $b$ est nul on peut encore définir leur ppcm par $\text{ppcm}(a, b) = 0$.

**Exemples 4.4.2** Pour les exemples situés après la définition 4.1.2, vérifiez que les ppcm sont (a) 120 (b) 600 (c) $a$.

Le lien entre pgcd et ppcm peut être précisé comme suit :

**Proposition 4.4.3** *Soit* $a, b \in \mathbb{N}$ *non tous les deux nuls. Soit* $d = \text{pgcd}(a, b)$ *et* $m = \text{ppcm}(a, b)$. *Alors on a* $ab = dm$.

**Démonstration :** On écrit $a = da'$, $b = db'$ avec $\text{pgcd}(a', b') = 1$. On va montrer que $m = da'b'$. Tout d'abord il est clair que $da'b' = ab' = a'b$ est un multiple commun de $a$ et $b$. Étant donné un autre multiple commun $n$ on va montrer que $da'b' \leq n$, et même que $da'b' | n$. En effet, par hypothèse il existe $n_1, n_2$ tels que $n = an_1 = bn_2$. Divisant par $d$ on a : $a'n_1 = b'n_2$. En particulier $a' | b'n_2$ donc d'après le lemme de Gauß il existe $n_3$ tel que $n_2 = a'n_3$. Par conséquent $n = ba'n_3 = da'b'n_3$.

En conclusion $ab = da'db' = dm$. □

Remarquons que la démonstration a prouvé l'équivalent de la propriété de 4.3.2 pour le ppcm : *tout multiple commun de* $a$ *et* $b$ *est divisible par leur* ppcm. En particulier :

**Proposition 4.4.4** *Soit $a_1, \ldots, a_k$ des entiers strictement positifs et premiers entre eux deux à deux (c'est-à-dire* $\text{pgcd}(a_i, a_j) = 1$ *pour deux quelconques d'entre eux). Soit $n \in \mathbb{N}$. Si tous les $a_i$ divisent $n$ alors leur produit divise $n$.*

**Démonstration :** Pour $k = 2$ : soit $m = \text{ppcm}(a_1, a_2)$, d'après ce qui précède on a $m|n$, or $m = a_1 a_2$ par 4.4.3. Pour $k > 2$ c'est identique par récurrence sur $k$ (il faut utiliser le résultat de l'exercice 4.2.6(1)). □

# 5 Nombres premiers

## 5.1 Définition et propriétés importantes

**Définition 5.1.1** Soit un nombre entier $p \geq 2$. On dit que $p$ est un *nombre premier* si ses seuls diviseurs sont 1 et lui-même. Un nombre $n \geq 2$ qui n'est pas premier est dit *composé*.

**Remarques 5.1.2**

(i) Dire que $n$ est composé signifie que $n = rs$ avec $1 < r < n$ et $1 < s < n$.

(ii) Les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43...

(iii) Soit deux premiers distincts $p \neq q$, alors pour tous $m, n \geq 1$, $\text{pgcd}(p^m, q^n) = 1$.

Les nombres premiers sont à la fois des nombres fondamentaux et très mystérieux. Ils sont fondamentaux à cause du théorème suivant :

**Théorème 5.1.3** *Tout entier $n \geq 2$ s'écrit comme un produit de nombres premiers, de façon unique à l'ordre près des facteurs. Une telle écriture est donc de la forme*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$$

*avec $r \geq 1$ un entier déterminé, $p_1 < \cdots < p_r$ des premiers distincts, et $\alpha_1, \ldots, \alpha_r$ des exposants (entiers) $\geq 1$.*

**Démonstration :** Soit $E$ l'ensemble des nombres premiers qui divisent $n$. D'après l'exemple 1.3.3 il existe un tel nombre premier, c'est-à-dire que $E$ est non vide. Choisissons $N$ tel que $n < 2^N$ ([7]) et montrons que $E$ est fini avec moins de $N$ éléments. En effet, prenons des éléments distincts $p_1, \ldots, p_k$ dans $E$. Comme $p_1, \ldots, p_k$ sont premiers entre eux deux à deux on a $p_1 p_2 \ldots p_k \,|\, n$ d'après la proposition 4.4.4. En particulier, $2^k \leq p_1 p_2 \ldots p_k \leq n < 2^N$ donc $k < N$. Donc $E$ est fini et $E = \{p_1, \ldots, p_r\}$ avec $r < N$.

Pour chaque indice $i$ il y a un nombre $\alpha_i \geq 1$ maximal tel que $p_i^{\alpha_i}$ divise $n$. En appliquant encore 4.4.4 pour les nombres $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$ on obtient que $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ divise $n$. Si le quotient est strictement supérieur à 1 il a un facteur premier $p_u$ qui doit être dans $E$, pour un certain indice $u$. Donc $p_u \times p_u^{\alpha_u}$ divise $n$. C'est impossible car $\alpha_u$ a été choisi maximal, donc $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. □

Dans le reste du paragraphe, nous décrirons quelques faits qui montrent que les nombres premiers sont beaux et mystérieux.

[7] Par exemple on peut prendre $N$ égal au nombre de chiffres de l'écriture en base 2 de $n$ (vérifiez-le).

**Remarque 5.1.4** Plus ou moins par leur définition même, les entiers naturels s'obtiennent à partir du nombre 1 par des additions successives. Le théorème 5.1.3 nous dit que, si on veut obtenir tous les entiers par des *multiplications* successives, alors un seul nombre ne suffit pas mais l'ensemble des nombres premiers répond à la question. En d'autres termes, les nombres premiers sont les « atomes » de base de l'écriture multiplicative de tous les entiers.

Pour cette raison, on ne considère pas que 1 est un nombre premier : il est inutile dans les écritures multiplicatives ([8]).

On doit à Euclide (encore lui !) la démonstration du fait suivant :

**Proposition 5.1.5** *Il y a une infinité de nombres premiers.*

**Démonstration :** Supposons qu'il n'y ait qu'un nombre fini de nombres premiers $p_1, \ldots, p_r$. Considérons le nombre $N := p_1 \ldots p_r + 1$. Ce nombre est $> 1$ donc il admet un diviseur premier qui est donc l'un des $r$ nombres premiers, $p_u$ $(1 \leq u \leq r)$. Comme $p_u | N$ et $p_u | p_1 \ldots p_r$ on en déduit que $p_u$ divise 1 ce qui est absurde. Donc, il y a une infinité de nombres premiers. □

Comme on l'a écrit (remarque 5.1.2(ii)) les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53... et après ? On ne connaît pas de formule donnant tous les nombres premiers. Certes, connaissant les $r$ premiers, la proposition donne une façon d'en trouver un autre, en regardant un facteur premier de $N := p_1 \ldots p_r + 1$. Malheureusement, *primo* ces nombres grandissent trop vite, et *secundo* la méthode demande de savoir trouver des facteurs premiers d'un entier, ce qui est aussi compliqué que de trouver les nombres premiers eux-mêmes...

Un autre problème très difficile est de savoir si un nombre donné $n$ est premier. Pour cela il faut tester s'il est divisible par tous les nombres premiers $\leq n$, qu'en général on ne connaît pas très bien. Le mieux que l'on puisse faire dans cette idée est :

**Proposition 5.1.6** *Pour tester si $n$ est premier il suffit de tester s'il est divisible par les nombres premiers $p \leq \sqrt{n}$.*

**Démonstration :** Si $n$ n'est pas premier il s'écrit $n = ab$ avec $1 < a \leq b < n$. Donc $a^2 \leq n$ de sorte que si $p$ est un facteur premier de $a$, on a $p \leq \sqrt{n}$. □

## 5.2 Exemples de nombres premiers et composés

Aujourd'hui il faut dénormes ordinateurs pour trouver des grands nombres premiers (de temps en temps, le record du plus grand premier connu tombe). Souvent on en trouve parmi les nombres de Mersenne, nombres de la forme $2^p - 1$ avec $p$ premier. Fermat pensait que les nombres $F_k := 2^{2^k} + 1$ étaient tous premiers mais Euler a montré que ce n'était pas vrai pour $F_5$.

[8] Et, étant donné un nombre premier $p$, le nombre de facteurs premiers dans $p^k$ est $k$. Donc si $k = 0$ on a envie de dire qu'il n'y a aucun facteur premier dans $p^0 = 1$...

Marin Mersenne (1588-1648) voulait trouver une formule pour représenter tous les nombres premiers, ce que l'on ne connaît toujours pas. Il étudia les nombres de la forme $2^p - 1$ ($p$ premier) qu'il affirma premiers si $p = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127 et 257 et composés pour les 44 autres premiers inférieurs à 257. Par la suite on montra qu'il s'était trompé pour 67 et 257 ainsi que 61, 89, 107.
Leonhard Euler (1707-1783) est un génie mathématique de la taille de Gauß. Je n'ai pas le courage de résumer sa vie si intense ! Les curieux sont encouragés à aller voir sur le site :
http://www-gap.dcs.st-and.ac.uk/∼history/BiogIndex.html

Voici un nombre premier :

**Proposition 5.2.1** *Le plus grand nombre premier connu (en octobre 2004) est le nombre de Mersenne* $2^{24036583} - 1$. *Son écriture décimale a plus de 7,2 millions de chiffres.*

**Démonstration :** Il n'y a pas d'autre moyen que la vérification par ordinateur en utilisant la proposition 5.1.6 ! Le calcul a été fait début 2004 par l'américain Josh Findley en utilisant des ordinateurs en réseau; il a duré deux semaines. □

Voici des nombres composés :

**Proposition 5.2.2 (Euler)** *Le nombre de Fermat* $F_5 := 2^{32} + 1$ *est composé, plus précisément divisible par 641.*

**Démonstration :** L'astuce (double) est de voir que $641 = 640 + 1 = 5 \times 2^7 + 1$ et $641 = 625 + 16 = 5^4 + 2^4$. Modulo 641, la première relation donne $5 \times 2^7 \equiv -1$ donc $5^4 \times 2^{28} \equiv 1$. La deuxième donne $5^4 \equiv -2^4$. En remplaçant, on obtient $-2^4 \times 2^{28} \equiv 1$ c'est-à-dire que $2^{32} + 1 \equiv 0 \bmod 641$, ce que l'on voulait. □

Pierre Fermat (1601-1665), juriste de métier, était aussi mathématicien amateur et soumettait ses questions et découvertes à des grands mathématiciens. Il lut l'*Arithmetica* de Diophante où est résolue l'équation en nombres entiers $x^2 + y^2 = z^2$. Ceci le mena à s'intéresser à l'équation $x^n + y^n = z^n$ avec $n > 2$.
Le Dernier Théorème de Fermat affirme que cette équation n'a pas de solution avec $x, y, z$ entiers non nuls. C'est resté une énigme pour les mathématiciens pendant 350 ans, jusqu'en 1993, date à laquelle le britannique Andrew Wiles (1953- ) l'a démontré.

**Proposition 5.2.3** *Le nombre* $4^{545} + 545^4$ *est composé.*

**Démonstration :** La preuve repose sur l'égalité appelée *identité de Sophie Germain* : $n^4 + 4m^4 = (n^2 + 2mn + 2m^2)(n^2 - 2mn + 2m^2)$. (On la vérifie immédiatement.) Pour $n = 545$ et $m = 4^{136}$, on a

$$n^4 + 4m^4 = 545^4 + 4 \times (4^{136})^4 = 545^4 + 4^{545}$$

Donc l'identité de Sophie Germain dit que c'est aussi égal au produit de

$$n^2 + 2mn + 2m^2 = 545^2 + 2 \times 4^{136} \times 545 + 2 \times 4^{272}$$

$$\text{par} \qquad n^2 - 2mn + 2m^2 = 545^2 - 2 \times 4^{136} \times 545 + 2 \times 4^{272}$$

□

Sophie Germain (1776-1831) fit sa formation mathématique en grande partie seule, et contre l'avis de ses parents. Elle voulut entrer à l'École Polytechnique quand celle-ci fut créée en 1794 (pendant la Révolution Française), mais seuls les hommes y étaient admis. Elle maîtrisa très tôt les *Disquisitiones Arithmeticæ* de Gauß et correspondit ensuite longtemps avec lui. Elle contribua à certains progrès dans le Dernier Théorème de Fermat.

## 5.3 Application au pgcd et au ppcm

Soient deux entiers $a, b \in \mathbb{N}$ non nuls. Soit $r$ le nombre de facteurs premiers de $a$, et $s$ le nombre de facteurs premiers de $b$, voir théorème 5.1.3. Soient $p_1, \ldots, p_t$ les nombres premiers qui interviennent dans l'une ou l'autre des décompositions : on a donc $r \leq t$ et $s \leq t$. On peut alors écrire

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$$

quitte à mettre un exposant $\alpha_i = 0$ si le facteur $p_i$ n'apparaît pas dans la décomposition de $a$, c'est-à-dire si $p_i | b$ mais $p_i \not| a$. De même on écrit $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}$.

**Exemple 5.3.1** Soient $a = 12740$ et $b = 168$. On écrit

$$a = 2^2 \times 5^1 \times 7^2 \times 13^1 \qquad \text{et} \quad b = 2^3 \times 3^1 \times 7^1$$

En incluant dans les deux écritures les facteurs premiers $2, 3, 5, 7, 13$ on a :

$$a = 2^2 \times 3^0 \times 5^1 \times 7^2 \times 13^1 \qquad \text{et} \quad b = 2^3 \times 3^1 \times 5^0 \times 7^1$$

Étant donnés $a$ et $b$ avec une écriture comme ci-dessus, il est facile de vérifier que

(1) $a = b$ si et seulement si $\alpha_i = \beta_i$ pour tout $i$,

(2) $b$ divise $a$ si et seulement si $\beta_i \leq \alpha_i$ pour tout $i$.

On va utiliser ces deux faits pour démontrer :

**Proposition 5.3.2** *Soient $a, b \in \mathbb{N}$ non nuls, écrits comme ci-dessus :*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t} \qquad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}$$

*Soient $d = \mathrm{pgcd}(a, b)$ et $m = \mathrm{ppcm}(a, b)$. Alors on a*

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_t^{\gamma_t} \qquad \text{et} \quad m = p_1^{\delta_1} p_2^{\delta_2} \ldots p_t^{\delta_t}$$

*avec $\gamma_i := \min(\alpha_i, \beta_i)$ et $\delta_i := \max(\alpha_i, \beta_i)$.*

**Démonstration :** Soit $e := p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_t^{\gamma_t}$, et écrivons la décomposition en facteurs premiers de $d$ sous la forme $d = p_1^{\gamma'_1} p_2^{\gamma'_2} \ldots p_t^{\gamma'_t}$. On doit montrer que $e = d$.

Comme $\gamma_i \leq \alpha_i$ et $\gamma_i \leq \beta_i$ pour tout $i$, il est clair que $e$ divise $a$ et $b$. Donc il divise leur pgcd, $d$. Réciproquement, comme $d$ divise $a$ et $b$ on a $\gamma'_i \leq \alpha_i$ et $\gamma'_i \leq \beta_i$ pour tout $i$, donc $\gamma'_i \leq \min(\alpha_i, \beta_i) = \gamma_i$. C'est fini.

Pour le ppcm la démonstration est identique. On peut aussi donner une autre démonstration en utilisant le fait que $ab = dm$ et $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$. □

**Exemple 5.3.3** Calculons le pgcd de $a = 12740$ et $b = 168$. D'après l'écriture ci-dessus on trouve immédiatement $d = 2^2 \times 7 = 28$ et $m = 2^3 \times 3 \times 5 \times 7^2 \times 13 = 76440$.