Chapitre 18. Arithmétique dans $\mathbb{Z}$

Plan du chapitre

1 Divisibilité dans $\mathbb{Z}$

1.1 Définitions

Définition 1.

1) Soient a et b deux entiers relatifs tels que $a \neq 0$.
On dit que a **divise** b ou que a est un **diviseur de** b si et seulement si il existe un entier relatif q tel que $b = qa$.
Il revient au même de dire que a divise b ou que b est **divisible par** a.
Quand a divise b, on écrit $a|b$ et quand a ne divise pas b, on écrit $a \nmid b$.

2) Soient a et b deux entiers relatifs.
b est un **multiple de** a si et seulement si il existe un entier relatif q tel que $b = qa$.
Si de plus, $a \neq 0$, b est multiple de a si et seulement si a divise b.

Notation. Si a est un entier relatif, l'ensemble des multiples de a est l'ensemble des nombres de la forme qa où q est un entier relatif. Il se note $a\mathbb{Z}$:

$$a\mathbb{Z} = \{qa,\ q \in \mathbb{Z}\} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}.$$

De même, l'ensemble des diviseurs de a se note $\mathrm{div}(a)$ ou $\mathcal{D}(a)$.

Exemples. 2 divise 6 car $6 = 3 \times 2$ avec 3 entier relatif. 4 divise -4 car $4 = (-1) \times (-4)$ avec -1 entier relatif. 1 divise 5 car $5 = 5 \times 1$ avec 5 entier relatif. 1 divise 0 car $0 = 0 \times 1$ avec 0 entier relatif. ❑

1.2 Propriétés de la divisibilité

Théorème 1.

1) $\forall a \in \mathbb{Z}^*$, $a|(-a)$ et $(-a)|a$. $\forall a \in \mathbb{Z}$, $-a$ est un multiple de a et a est un multiple de $-a$.

2) $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, $b|a \Leftrightarrow (-b)|a \Leftrightarrow b|(-a) \Leftrightarrow (-b)|(-a)$.

Démonstration.

1) Soit a un entier relatif non nul. $-a = a \times (-1)$ avec $-1 \in \mathbb{Z}$. Donc, $a|(-a)$. Ensuite, en appliquant le résultat précédent à l'entier $-a$, on a aussi $-a|a$.

2) Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Si $b|a$, il existe $q \in \mathbb{Z}$ tel que $a = bq$. Mais alors, $a = (-b)(-q)$ avec $-q \in \mathbb{Z}$ et donc $-b$ divise a. Ensuite, en appliquant à l'entier relatif non nul $-b$, on a aussi le fait que si $-b|a$, alors $b|a$.
Enfin, en appliquant aux entiers $\pm a$ et/ou $\pm b$, on obtient les deux autres équivalences.

❑

Théorème 2.

1) $\forall a \in \mathbb{Z}$, les diviseurs de a sont les diviseurs de $|a|$.

2) $\forall a \in \mathbb{Z}$, les multiples de a sont les multiples de $|a|$.

Démonstration.

1) Soit $a \in \mathbb{Z}$. D'après le théorème 1, si b est un entier relatif divisant a, alors b divise a et $-a$ et donc b divise $|a|$. Inversement, si b est un entier relatif divisant $|a|$, b divise a qui est l'un des deux entiers $|a|$ ou $-|a|$.

2) Soit $a \in \mathbb{Z}$. Si $b = qa$, $q \in \mathbb{Z}$, alors $b = (\mathrm{sgn}(a)q)|a|$ avec $\mathrm{sgn}(a)q \in \mathbb{Z}$ et si $b = q|a|$, $q \in \mathbb{Z}$, alors $b = (\mathrm{sgn}(a)q)a$.

❑

Dans le théorème qui suit, $\leqslant$ désigne la relation d'ordre usuelle dans $\mathbb{N}^*$ ou $\mathbb{Z}^*$.

Théorème 3.

Soit $a \in \mathbb{N}^*$. $\forall b \in \mathbb{N}^*$, $(b|a \Rightarrow b \leqslant a)$ (tout diviseur de a dans $\mathbb{N}^*$ est inférieur ou égal à a).
Soit $a \in \mathbb{N}^*$. $\forall b \in \mathbb{Z}^*$, $(b|a \Rightarrow b \leqslant a)$ (tout diviseur de a dans $\mathbb{Z}^*$ est inférieur ou égal à a).
Soit $a \in \mathbb{Z}^*$. $\forall b \in \mathbb{Z}^*$, $(b|a \Rightarrow |b| \leqslant |a|)$.

Soit $a \in \mathbb{N}^*$. Tout multiple strictement positif de a est supérieur ou égal à a.

Démonstration. Soit $(a,b) \in (\mathbb{N}^*)^2$. Si b divise a, alors il existe $q \in \mathbb{N}^*$ tel que $a = qb$. On en déduit que

$$a = qb \geqslant 1 \times b = b.$$

Si maintenant b est strictement négatif, alors $b \leqslant 0 < a$ et en particulier $b \leqslant a$.

Enfin, si $(a,b) \in (\mathbb{Z}^*)^2$, b est un diviseur de $|a|$ et donc $b \leqslant |a|$. $-b$ est aussi un diviseur de $|a|$ et donc $-b \leqslant a$. Finalement, $|b| \leqslant |a|$.

❑

Théorème 4. $\forall (a,b) \in \mathbb{Z}^* \times \mathbb{Z}$, $a|b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$.

Démonstration. Soit $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}$.

• Supposons que $a|b$. Il existe $q \in \mathbb{Z}$ tel que $b = qa$. Soit alors $k \in \mathbb{Z}$.

$$kb = kqa = (kq)a \in a\mathbb{Z}.$$

Donc, $b\mathbb{Z} \subset a\mathbb{Z}$.

• Supposons que $b\mathbb{Z} \subset a\mathbb{Z}$. En particulier, puisque $b = 1 \times b \in b\mathbb{Z}$, on en déduit que $b \in a\mathbb{Z}$ et donc il existe $q \in \mathbb{Z}$ tel que $b = aq$. Mais alors, $a|b$.

❑

⇨ **Commentaire.** *Le théorème précédent dit que si un entier non nul a divise un entier b, alors l'ensemble des multiples de b est contenu dans l'ensemble des multiples de a. Par exemple, l'entier 3 divise l'entier 6 et donc tout multiple de 6 est en particulier un multiple de 3.*

Théorème 5.

1) Pour tout $a \in \mathbb{Z}^*$, $a|0$. Pour tout $a \in \mathbb{Z}$, 0 est multiple de a.

2) Pour tout $a \in \mathbb{Z}$, $1|a$. Pour tout $a \in \mathbb{Z}$, a est multiple de 1.

Démonstration.

1) Soit $a \in \mathbb{Z}^*$. $0\mathbb{Z} = \{0\} \subset a\mathbb{Z}$ et donc a divise 0 ou encore 0 est multiple de a. Cette dernière affirmation reste claire quand $a = 0$.

2) Soit $a \in \mathbb{Z}$. $a\mathbb{Z} \subset \mathbb{Z} = 1\mathbb{Z}$ et donc $1|a$ ou encore a est multiple de 1.

❑

Théorème 6.

1) $\forall a \in \mathbb{Z}^*$, $a|a$ (la relation de divisibilité dans $\mathbb{Z}^*$ ou dans $\mathbb{N}^*$ est réflexive).

2) a) $\forall (a,b) \in (\mathbb{N}^*)^2$, ($a|b$ et $b|a$) $\Leftrightarrow a = b$ (la relation de divisibilité dans $\mathbb{N}^*$ est anti-symétrique).

b) $\forall (a,b) \in (\mathbb{Z}^*)^2$, ($a|b$ et $b|a$) $\Leftrightarrow b = a$ ou $b = -a$.

3) $\forall (a,b,c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$, ($a|b$ et $b|c$) $\Rightarrow a|c$ (et en particulier, la relation de divisibilité dans $\mathbb{Z}^*$ ou dans $\mathbb{N}^*$ est transitive).

La relation de divisibilité est une relation d'ordre sur $\mathbb{N}^*$ et n'est pas une relation d'ordre sur $\mathbb{Z}^*$.

Démonstration.

1) Soit $a \in \mathbb{Z}^*$. $a = 1 \times a$ avec $1 \in \mathbb{Z}$ et donc $a|a$ (ou aussi $a\mathbb{Z} \subset a\mathbb{Z}$ et donc $a|a$).

2) a) Soit $(a,b) \in (\mathbb{N}^*)^2$. Si a divise b et b divise a, alors d'après le théorème 3, $b \leqslant a$ et $a \leqslant b$ et finalement $a = b$. Réciproquement, si $a = b$, alors $a|b$ et $b|a$.

b) Soit $(a,b) \in (\mathbb{Z}^*)^2$. Si a divise b et b divise a, alors $|a|$ divise $|b|$ et $|b|$ divise $|a|$ puis $|a| = |b|$ d'après ci-dessus. Ainsi, $b = a$ ou $b = -a$. Réciproquement, si $b = a$ ou $b = -a$, alors a divise b et b divise a d'après le théorème 1.

3) Soient $(a,b,c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$. Si a divise b et b divise c, alors il existe deux entiers relatifs q et q' tels que $b = qa$ et $c = q'b$. Mais alors, $c = (qq')\,a$ avec $qq' \in \mathbb{Z}$ et donc a divise c.

❑

Les couples d'entiers relatifs non nuls tels que $a|b$ et $b|a$ sont appelés *couples d'entiers associés*. Le théorème 6 dit que les couples d'entiers associés sont les couples de la forme (a,a), $a \in \mathbb{Z}^*$, et les couples de la forme $(a,-a)$, $a \in \mathbb{Z}^*$.

Théorème 7. Soit $(a,b,c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}^*$.

$(c|a$ et $c|b) \Rightarrow \forall (u,v) \in \mathbb{Z}^2,\ c|(au+bv)$.

Démonstration. Soient $(a,b,c)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}^*$. Soit $(u,v)\in\mathbb{Z}^2$. Si c divise a et c divise b, alors il existe deux entiers relatifs q et q' tels que $a=qc$ et $b=q'c$. Mais alors $au+bv=(uq+vq')c$ avec $uq+vq'\in\mathbb{Z}^2$ et donc c divise $au+bv$.

❑

⇨ **Commentaire.**

◇ *Le théorème précédent peut se réexprimer en terme d'ensembles de multiples : si $a\mathbb{Z}\subset c\mathbb{Z}$ et $b\mathbb{Z}\subset c\mathbb{Z}$, alors $(au+bv)\mathbb{Z}\subset c\mathbb{Z}$ ou encore si a et b sont des multiples commun de c, alors tout nombre de la forme $au+bv$ où u et v sont des entiers relatifs, est un multiple de c ou aussi si c est un diviseur commun à a et b, alors c divise tout nombre de la forme $au+bv$, $(u,v)\in\mathbb{Z}^2$.*

◇ *Ce dernier résultat est très utilisé dans la pratique. Un exemple d'utilisation est fourni par l'exercice suivant.*

Exercice 1. Trouver tous les entiers naturels n tels que $2n+3$ divise $3n+7$.

Solution 1. Soit $n\in\mathbb{N}$ tel que $2n+3$ divise $3n+7$. Alors, puisque $2n+3$ divise à la fois $2n+3$ et $3n+7$, $2n+3$ divise encore $2(3n+7)-3(2n+3)=5$. Puisque $2n+3$ est un entier naturel, on a donc nécessairement $2n+3=1$ ou $2n+3=5$ puis $n=-1$ ou $n=1$ puis $n=1$ car n est un entier naturel.

Réciproquement, si $n=1$, alors $2n+3=5$ et $3n+7=10=2\times5$. Donc, si $n=1$, $2n+3$ divise effectivement $3n+7$.

Il existe un et un seul entier naturel n tel que $2n+3$ divise $3n+7$ à savoir $n=1$.

---

2 Division euclidienne dans $\mathbb{Z}$

On commence par le cas où on divise par un entier naturel non nul.

Théorème 8. Soit $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$. Il existe un couple (q,r) d'entiers relatifs et un seul tels que

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

q s'appelle le **quotient** de la division euclidienne de l'entier relatif a par l'entier naturel non nul b et r s'appelle le **reste** de la division euclidienne de a par b.

Démonstration.

Existence. Soit $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$. Soient $q=\left\lfloor\frac{a}{b}\right\rfloor$ (où $\lfloor x\rfloor$ désigne la partie entière du réel x) puis $r=a-bq$. q et r sont deux entiers relatifs tels que $a=bq+r$. De plus,

$$\begin{aligned}q=\left\lfloor\frac{a}{b}\right\rfloor &\Rightarrow q\leqslant\frac{a}{b}<q+1\\ &\Rightarrow qb\leqslant a<qb+b \text{ (car } b>0)\\ &\Rightarrow 0\leqslant a-bq<b\\ &\Rightarrow 0\leqslant r<b.\end{aligned}$$

Donc, le couple (q,r) convient.

Unicité. Soit $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$. Soit $(q,q',r,r')\in\mathbb{Z}^4$ tels que $a=bq+r=bq'+r'$ et $0\leqslant r<b$ et $0\leqslant r'<b$. Alors, $bq+r=bq'+r'$ puis $b(q-q')=r'-r$ puis $|r'-r|=b|q-q'|$.
Puisque $0\leqslant r<b$ et $0\leqslant r'<b$, on a encore $-b<r-r'<b$ et aussi $-b<r'-r<b$ et donc $|r-r'|<b$. Si $q\neq q'$, alors $|q-q'|\geqslant1$ puis $|r'-r|=b|q-q'|\geqslant b$ ce qui est faux. Donc, $q=q'$ puis $r=r'$. Ceci montre l'unicité du couple (q,r).

❑

⇨ **Commentaire.**

◇ *La division euclidienne est la division où « on ne poursuit pas après la virgule ». Elle se présente dans les petites classes sous la forme*

50	13
11	3

De manière générale, elle s'écrit

a	b
r	q

◇ *Si* $x = \dfrac{a}{b}$ *est un rationnel non nul avec* $a \in \mathbb{Z}^*$ *et* $b \in \mathbb{N}^*$*, la division euclidienne de* a *par* b *permet de décomposer* x *en somme de sa partie entière et de « sa partie décimale ». Plus précisément, si* $a = bq + r$ *abec* $0 \leqslant r < b$ *(et* q *et* r *entiers relatifs), alors*

$$x = \frac{a}{b} = q + \frac{r}{b}$$

où cette fois-ci $0 \leqslant \dfrac{r}{b} < 1$*. Par exemple*

$$\frac{50}{13} = 3 + \frac{11}{13}.$$

Théorème 9. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un couple (q, r) d'entiers relatifs et un seul tels que

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

Démonstration .

Existence. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Le résultat est déjà connu si $b > 0$. Soient donc a et b deux entiers relatifs tels que $b < 0$. Soit $b' = -b$.
La division euclidienne de $-a$ par b' fournit un couple (q', r') d'entiers relatifs tel que $-a = q'b' + r'$ et $0 \leqslant r' < b'$. Ceci s'écrit encore $a = q'b - r'$ avec $0 \leqslant r' < -b = |b|$. Si $r' = 0$, le couple $(q, r) = (q', 0)$ convient. Sinon, on a $0 < r' < -b$ puis $b < -r' < 0$. On pose alors $r = -r' - b$ de sorte que $0 < r = -r' - b < -b = |b|$. On pose ensuite $q = q' + 1 \in \mathbb{Z}$ et on a

$$bq + r = b\left(q' + 1\right) - r' - b = bq' - r' = a.$$

Le couple $(q, r) = (q' + 1, -r' - b)$ convient.

Unicité. La démonstration du théorème précédent peut être reproduite quasiment à l'identique en remplaçant b par $|b|$. ❑

⇨ **Commentaire** . *Par exemple, la division euclidienne de* 7 *par* -3 *s'écrit* $7 = (-2) \times (-3) + 1$ *(le quotient est* -2 *qui n'est pas la partie entière de* $\dfrac{7}{-3}$*) et la division euclidienne de* -11 *par* -4 *s'écrit* $-11 = 3 \times (-4) + 1$ *(le quotient est* 3 *qui n'est pas la partie entière de* $\dfrac{-11}{-4}$*).*

Exercice 2. Pour $n \in \mathbb{N}^*$, on pose $M_n = 2^n - 1$ (nombres de Mersenne). Effectuer la division euclidienne de M_p par M_n pour n et p entiers naturels non nuls tels que $p > n$.

Solution 2. Soit $(n, p) \in (\mathbb{N}^*)^2$ tel que $n < p$. La division euclidienne de p par n s'écrit $p = nq + r$ où $q \in \mathbb{N}^*$ et $r \in [\![0, n-1]\!]$.

$$\begin{aligned} M_p = 2^p - 1 = 2^{qn+r} - 1 &= (2^n)^q \times 2^r - 1 = \left((2^n)^q - 1\right) 2^r + (2^r - 1) \\ &= (2^n - 1)\left(1 + 2^n + (2^n)^2 + \ldots + (2^n)^{q-1}\right) 2^r + (2^r - 1) \text{ (on rappelle que } q \in \mathbb{N}^*) \\ &= QM_n + R \end{aligned}$$

où $Q = \left(1 + 2^n + (2^n)^2 + \ldots + (2^n)^{q-1}\right) 2^r$ est un entier (car $q \in \mathbb{N}^*$) et $R = 2^r - 1 = M_r$ est un entier. De plus,

$$0 \leqslant r < n \Rightarrow 1 \leqslant 2^r < 2^n \Rightarrow 0 \leqslant 2^r - 1 < 2^n - 1 \Rightarrow 0 \leqslant M_r < M_n.$$

Le quotient de la division euclidienne de M_p par M_n est $\left(1 + 2^n + (2^n)^2 + \ldots + (2^n)^{q-1}\right) 2^r$ et le reste est M_r où q et r sont le quotient et le reste de la division euclidienne de p par n.

Sinon, un résultat évident mais qui doit être énoncé explicitement est :

Théorème 10. Soit $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$. b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Démonstration. Soit $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$. Si b divise a, il existe un entier relatif q tel que $a=bq$. Mais alors, $a=bq+r$ avec $r=0\in[\![0,b-1]\!]$. Le reste de la division euclidienne de a par b est donc 0.
Réciproquement, si le reste de la division euclidienne de a par b est nul, cette division euclidienne s'écrit $a=bq$ où q est un entier relatif et donc b divise a.

❑

3 PGCD - PPCM

Dans tout ce qui suit, nous aurons besoin du résultat intuitif suivant que l'on admet et qui est une conséquence de l'axiome de récurrence :

Théorème 11. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

3.1 PGCD

3.1.1 Définition du PGCD

Théorème 12. Soient a et b deux entiers relatifs tous deux non nuls. Il existe un entier naturel et un seul qui est un diviseur commun à a et à b et qui est plus grand (au sens de la relation d'ordre usuelle $\leqslant$) que tout diviseur commun à a et à b dans $\mathbb{Z}$.

Démonstration. Soit $(a,b)\in(\mathbb{Z}^*)^2$.

Existence. Soit $\mathcal{E}=\{d\in\mathbb{N}^*/\ d|a \text{ et } d|b\}$. $\mathcal{E}$ est une partie non vide de $\mathbb{N}$ car 1 est un entier naturel non nul qui est un diviseur commun à a et à b et donc $1\in\mathcal{E}$. D'autre part, tout diviseur commun à a et b dans $\mathbb{N}^*$ est majoré par $\text{Min}\{|a|,|b|\}$ d'après le théorème 3.
$\mathcal{E}$ admet donc un plus grand élément qui est par définition un entier naturel non nul, diviseur commun à a et à b et plus grand que tout diviseur commun à a et à b qui est strictement positif. Mais alors, $\text{Max}(\mathcal{E})$ est plus grand que tout diviseur commun à a et à b dans $\mathbb{Z}$ car $\text{Max}(\mathcal{E})>0$.

Unicité. Un diviseur commun à a et à b et plus grand que tout diviseur commun à a et à b est nécessairement le maximum de $\mathcal{E}$ et on sait qu'un maximum est unique.

❑

Définition 2. Soient a et b deux entiers relatifs non nuls.

Le plus grand diviseur commun à a et à b se note $\text{PGCD}(a,b)$ ou aussi $a\wedge b$.

On a défini le PGCD de deux entiers relatifs non nuls. On peut élargir cette définition au cas où l'un des deux entiers relatifs a ou b est nul sans que l'autre ne le soit : si $a>0$, tout entier non nul divise 0 et donc, il existe un et un seul entier naturel non nul divisant à la fois a et $b=0$ et plus grand que tous les autres à savoir a lui-même. Donc $a\wedge 0=a$. Plus généralement, si $a\in\mathbb{Z}^*$, $a\wedge 0=|a|$.
Par contre, on ne peut pas élargir encore au cas où $a=b=0$ car dans ce cas, tout entier naturel non nul divise à la fois a et b et il n'y a donc pas de plus grand diviseur commun.

En raison de ces complications, nous donnerons la plupart des résultats sur le PGCD en excluant le cas où l'un des deux nombres a ou b est nul.

Un premier résultat, qui permet de se ramener au cas où $a>0$ et $b>0$, est :

Théorème 13. $\forall(a,b)\in(\mathbb{Z}^*)^2$, $a\wedge b=|a|\wedge|b|$.

Démonstration. Soit $(a,b)\in(\mathbb{Z}^*)^2$. D'après le théorème 2, les diviseurs communs à a et à b sont encore les diviseurs communs à $|a|$ et $|b|$ et en particulier, $a\wedge b=|a|\wedge|b|$.

❑

3.1.2 L'algorithme d'Euclide

On commence par le « lemme d'Euclide » :

Théorème 14. Soient $(a, b, q, r) \in \mathbb{Z}^4$ tel que $a \neq 0$, $b \neq 0$, $r \neq 0$ et $a = bq + r$.

Alors $a \wedge b = b \wedge r$.

Démonstration. Soit d un entier relatif non nul. Si d divise a et b, alors d divise b et $a - bq = r$ d'après le théorème 7 et si d divise b et r, alors d divise b et d divise $bq + r = a$.
Donc, $\text{div}(a) \cap \text{div}(b) = \text{div}(b) \cap \text{div}(r)$. En particulier, $\text{Max}(\text{div}(a) \cap \text{div}(b)) = \text{Max}(\text{div}(b) \cap \text{div}(r))$ ou encore $a \wedge b = b \wedge r$.

❑

Nous allons maintenant utiliser ce résultat pour déterminer de manière algorithmique le PGCD de deux entiers. L'algorithme ci-dessous s'appelle l'algorithme d'Euclide.

Commençons par un exemple. Déterminons le PGCD de $a = 1386$ et $b = 270$. La division euclidienne de a par b s'écrit

$$1386 = 5 \times 270 + 36$$

et le théorème 14 nous permet alors d'affirmer que $1386 \wedge 270 = 270 \wedge 36$. La division euclidienne de 270 par 36 s'écrit

$$270 = 7 \times 36 + 18$$

et donc $1386 \wedge 270 = 270 \wedge 36 = 36 \wedge 18$. Maintenant, puisque $36 = 2 \times 18$, 18 divise 36 et donc le plus grand diviseur commun à 18 et 36 est 18. Finalement

$$1386 \wedge 270 = 270 \wedge 36 = 36 \wedge 18 = 18.$$

Passons au cas général. On se donne deux entiers naturels non nuls a et b tels que $a > b$. Posons $r_0 = a$ et $r_1 = b$. On a donc $r_1 < r_0$.

- La division euclidienne de $r_0 = a$ par $r_1 = b$ s'écrit

$$r_0 = r_1 \times q_0 + r_2 \quad \text{avec} \quad 0 \leqslant r_2 < r_1.$$

Si $r_2 = 0$, $r_1 = b$ divise $r_0 = a$. Le plus grand diviseur commun à a et b est donc $r_1 = b$.
Sinon, $1 \leqslant r_2 < r_1$ et d'après le théorème 13, $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2$.

- On pose alors la division euclidienne de r_1 par r_2 qui s'écrit

$$r_1 = r_2 \times q_1 + r_3 \quad \text{avec} \quad 0 \leqslant r_3 < r_2.$$

Si $r_3 = 0$, r_2 divise r_1 et donc $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = r_2$.
Sinon, $1 \leqslant r_3 < r_2$ et on pose la division euclidienne de r_2 par r_3.

- De manière générale, pour $k \in \mathbb{N}$ tel que les restes $r_0, \ldots, r_{k+1}$ ne soient pas nuls, on pose la division euclidienne de r_k par r_{k+1}. Elle fournit un quotient $q_k \in \mathbb{N}$ et un reste $r_{k+2} \in \mathbb{N}$ tels que

$$r_k = r_{k+1} \times q_k + r_{k+2} \quad \text{avec} \quad 0 \leqslant r_{k+2} < r_{k+1}.$$

On a alors $a \wedge b = r_1 \wedge r_2 = \ldots = r_k \wedge r_{k+1}$ avec $r_0 > r_1 > \ldots > r_k > r_{k+1}$.

- S'il n'existe aucun reste nul, on obtient une suite de reste $(r_k)_{k\in\mathbb{N}}$ qui est une suite d'entiers naturels strictement décroissante. Mais une telle suite n'existe pas car dans le cas contraire, pour tout $k \in \mathbb{N}$, $r_{k+1} \leqslant r_k - 1$ puis, par récurrence, pour tout $k \in \mathbb{N}$, $r_k \leqslant r_0 - k$, ce qui entraine $\lim\limits_{k\to+\infty} r_k = -\infty$ et est absurde (puisque $\forall k \in \mathbb{N}$, $r_k \geqslant 0$).
Donc, il existe un reste qui est nul ou encore l'algorithme que l'on vient de mettre en place, s'arrête.
Soit r_{k_0+2}, $k_0 \in \mathbb{N}$, ce premier reste nul. On a $r_{k_0} = r_{k_0+1} \times q_{k_0}$ et donc r_{k_0+1} divise r_{k_0} puis $r_{k_0} \wedge r_{k_0+1} = r_{k_0+1}$.
Mais alors,

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{k_0} \wedge r_{k_0+1} = r_{k_0+1}.$$

Ainsi, le PGCD de a et b est le **dernier reste non nul** dans l'algorithme d'Euclide. On peut énoncer :

Théorème 15. Soient $(a, b) \in (\mathbb{N}^*)^2$ tel que $a > b$. On pose $r_0 = a$, $r_1 = b$ puis pour $k \in \mathbb{N}$, tant que $r_{k+1} \neq 0$, on pose $r_k = q_k r_{k+1} + r_{k+2}$ où $(q_k, r_{k+2}) \in (\mathbb{N}^*)^2$ et $0 \leqslant r_{k+2} < r_{k+1}$.

- il existe un premier reste nul
- le PGCD de a et de b est le dernier reste non nul.

Exercice 3. Déterminer le PGCD de 273 et 455

Solution 3. Déterminons PGCD(455, 273) par l'algorithme d'Euclide.

$$455 = 1 \times 273 + 182$$
$$273 = 1 \times 182 + 91$$
$$182 = 2 \times 91 + 0.$$

Le dernier reste non nul dans l'algorithme d'Euclide est 91 et donc

$$\mathrm{PGCD}(455, 273) = 91.$$

On doit noter que, étape après étape, un reste donné « descend en diagonale » de la droite vers la gauche (comme le reste 182 par exemple).

Exercice 4. Pour $n \in \mathbb{N}^*$, on pose $M_n = 2^n - 1$. Montrer que

$$\forall (n, p) \in (\mathbb{N}^*)^2,\ M_p \wedge M_p = M_{n \wedge p}.$$

Solution 4. Soit $(n, p) \in (\mathbb{N}^*)^2$ tel que $n < p$. La division euclidienne de p par n s'écrit $p = nq + r$ où q et r sont deux entiers naturels. D'après l'exercice n° 2, la division euclidienne de M_p par M_n s'écrit

$$M_p = QM_n + M_r \quad (*)$$

où Q est un entier naturel et $0 \leqslant M_r < M_n$. De plus,

$$M_r = 0 \Leftrightarrow 2^r = 1 \Leftrightarrow r = 0 \quad (**).$$

Posons $r_0 = p$, $r_1 = n$ puis pour $k \in \mathbb{N}$, tant que $r_{k+1} \neq 0$, posons $r_k = r_{k+1}q_k + r_{k+2}$ où q_k et r_k sont des entiers naturels tels que $0 \leqslant r_{k+2} < r_{k+1}$. Posons encore $R_0 = M_p$, $R_1 = M_n$ puis pour $k \in \mathbb{N}$, tant que $R_{k+1} \neq 0$, posons $R_k = R_{k+1}Q_k + R_{k+2}$ où Q_k et R_k sont des entiers naturels tels que $0 \leqslant R_{k+2} < R_{k+1}$.

$(*)$ et $(**)$ montrent que les deux algorithmes s'effectuent en parallèle : pour tout $k \in \mathbb{N}$, tant que $r_{k+1} \neq 0$, on a encore $R_{k+1} \neq 0$ et $R_{k+2} = M_{r_{k+2}}$.
Le dernier reste non nul dans l'algorithme d'Euclide appliqué à p et n est alors $r_{k_0+1} = n \wedge p$ et le dernier reste non nul dans l'algorithme d'Euclide appliqué à M_p et M_n est $R_{k_0+1} = M_{r_{k_0+1}} = M_{n \wedge p}$.

Ceci montre que $M_n \wedge M_p = M_{n \wedge p}$.

A partir, de l'algorithme d'Euclide, on obtient une propriété importante du PGCD.

Théorème 16. Soit $(a, b) \in (\mathbb{Z}^*)^2$.

Il existe $(u, v) \in \mathbb{Z}^2$ tel que $a \wedge b = au + bv$.

Démonstration .

• Commençons par supposer que $(a, b) \in (\mathbb{N}^*)^2$ et $b \leqslant a$. Si b divise a, alors il existe $q \in \mathbb{Z}$ tel que $a = bq$. Dans ce cas, $a \wedge b = b = 0 \times a + 1 \times b$ et il existe donc des entiers relatifs u et v tels que $a \wedge b = au + bv$.

Sinon, b ne divise pas a et l'entier k_0 de l'algorithme d'Euclide appliqué à a et à b est supérieur ou égal à 1. Cet algorithme s'écrit : $\forall k \in [\![0, k_0]\!]$, $r_k = r_{k+1}q_k + r_{k+2}$ avec $0 \leqslant r_{k+2} < r_{k+1}$ (et $r_{k_0+2} = 0$). On sait alors que $a \wedge b = r_{k_0+1}$.
A partir de l'égalité $r_{k_0-1} = r_{k_0}q_{k_0} + r_{k_0+1}$, on exprime $a \wedge b = r_{k_0+1}$ sous la forme

$$a \wedge b = r_{k_0+1} = r_{k_0-1}u_{k_0-1} + r_{k_0}v_{k_0-1}$$

où $u_{k_0-1} = 1$ et $v_{k_0-1} = -q_{k_0}$ sont des entiers relatifs. Puis en remontant dans l'algorithme, par récurrence, on peut écrire $a \wedge b$ sous la forme

$$a \wedge b = r_k u_k + r_{k+1}v_k$$

où $k \in [\![0, k_0 - 1]\!]$ et u_k et v_k sont des entiers relatifs. En particulier, il existe deux entiers relatifs u et v tels que

$$a \wedge b = r_0 u + r_1 v = au + bv.$$

Le résultat reste clair si $b > a$ en échangeant les rôles de a et b. Enfin, si $(a, b) \in (\mathbb{Z}^*)^2$, on dispose d'entiers relatifs u' et v' tels que

$$a \wedge b = |a| \wedge |b| = |a|u' + |b|v' = a(\pm u') + b(\pm v')$$

et on obtient encore une fois des entiers relatifs u et v tel que $a \wedge b = au + bv$.

❑

3.1.3 Propriétés du PGCD

Théorème 17.

$\forall a \in \mathbb{N}^*$, $a \wedge a = a$.
$\forall a \in \mathbb{Z}^*$, $a \wedge a = |a|$.

Démonstration. Soit $a \in \mathbb{N}^*$. a est un diviseur commun à a et à a et tout diviseur commun à a et à a est inférieur ou égal à a d'après le théorème 3. Donc, $a \wedge a = a$.

Si $a \in \mathbb{Z}^*$, $a \wedge a = |a| \wedge |a| = |a|$.

❑

Théorème 18. Soit $(a, b) \in (\mathbb{Z}^*)^2$. Les diviseurs communs à a et à b sont les diviseurs communs de leur PGCD.

Démonstration. Soit $(a, b) \in (\mathbb{Z}^*)^2$. $a \wedge b$ est un diviseur commun à a et b. Par transitivité, un diviseur de $a \wedge b$ est encore un diviseur commun à a et b.

Réciproquement, posons $d = a \wedge b \in \mathbb{N}^*$. D'après le théorème 16, il existe deux entiers relatifs u et v tels que $d = au + bv$.
Soit alors d' un diviseur commun à a et b. d' divise $au + bv$ d'après le théorème 7 ou encore d' divise d.

On a montré que les diviseurs communs à a et à b sont les diviseurs de $a \wedge b$.

❑

⇨ **Commentaire.** *Le résultat du théorème 18 s'écrit de manière plus condensée : div$(a) \cap$ div$(b) =$ div$(a \wedge b)$.*

Ensuite, l'application $\begin{array}{ccc}(\mathbb{N}^*)^2 & \to & \mathbb{N}^* \\ (a, b) & \mapsto & a \wedge b\end{array}$ est une loi de composition interne sur $\mathbb{N}^*$. Le théorème suivant détaille les propriétés de cette loi.

Théorème 19.

1) $\forall (a, b) \in (\mathbb{N}^*)^2$, $a \wedge b = b \wedge a$ (commutativité du PGCD).

2) $\forall (a, b, c) \in (\mathbb{N}^*)^3$, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ (associativité du PGCD).

3) $\forall a \in \mathbb{N}^*$, $a \wedge 1 = 1$ (1 est absorbant).

Démonstration.

1) Soit $\forall (a, b) \in (\mathbb{N}^*)^2$. div$(a) \cap$ div$(b) =$ div$(b) \cap$ div(a) et en particulier, $a \wedge b = b \wedge a$.

2) Soit $(a, b, c) \in (\mathbb{N}^*)^3$. D'après le théorème 18,

$$\text{div}(a \wedge b) \cap \text{div}(c) = (\text{div}(a) \cap \text{div}(b)) \cap \text{div}(c) = \text{div}(a) \cap \text{div}(b) \cap \text{div}(c),$$

puis par symétrie des rôles, on a aussi div$(a) \cap$ div$(b \wedge c) =$ div$(a) \cap$ div$(b) \cap$ div(c).
Donc, $(a \wedge b) \wedge c = \text{Max}(\text{div}(a) \cap \text{div}(b) \cap \text{div}(c)) = a \wedge (b \wedge c)$.

3) Soit $a \in \mathbb{N}^*$. $a \wedge 1$ est en particulier un diviseur de 1 dans $\mathbb{N}^*$ et donc $a \wedge 1 = 1$.

❑

⇨ **Commentaire.** *Puisque le PGCD est associatif, on peut écrire chacune des deux expressions $(a \wedge b) \wedge c$ et $a \wedge (b \wedge c)$ sans parenthèses : $a \wedge b \wedge c$. $a \wedge b \wedge c$ est alors le plus grand diviseur commun à a, b et c.*

Par exemple, $6 \wedge 10 \wedge 15 = (6 \wedge 10) \wedge 15 = 2 \wedge 15 = 1$.

Plus généralement, si $a_1, \ldots, a_n$, sont n entiers relatifs non nuls, $n \geqslant 2$, l'expression $a_1 \wedge \ldots \wedge a_n$ a un sens : c'est le plus grand diviseur commun à $a_1, \ldots, a_n$.

Théorème 20. $\forall (a,b,c) \in (\mathbb{N}^*)^3$, $(ca) \wedge (cb) = c(a \wedge b)$.

Démonstration. Soit $(a,b,c) \in (\mathbb{N}^*)^3$.

• c divise ca et cb et donc c divise $(ca) \wedge (cb)$. Donc, il existe $q \in \mathbb{N}^*$ tel que $(ca) \wedge (cb) = qc$ $(*)$.
On va montrer que $q = a \wedge b$. On pose $d = a \wedge b$.

• qc divise ca et donc il existe $k \in \mathbb{N}^*$ tel que $ca = kqc$ puis $a = kq$. Mais alors q divise a et de même q divise b puis q divise d.

• Il existe $k \in \mathbb{N}^*$ tel que $a = kd$ puis $ca = kdc$. Donc, dc divise ca et de même dc divise cb puis dc divise $(ca) \wedge (cb) = qc$. Il existe donc $k \in \mathbb{N}^*$ tel que $qc = kdc$ puis $q = kd$. Par suite, d divise q.

• En résumé, d divise q et q divise d. Donc, $d = q$ (car $d > 0$ et $q > 0$). L'égalité $(*)$ s'écrit alors $(ca) \wedge (cb) = c(a \wedge b)$.

❑

Ainsi, par exemple, $24 \wedge 36 = (2 \times 12) \wedge (3 \times 12) = 12(2 \wedge 3) = 12$.

Une conséquence importante est le

Théorème 21. Soit $(a,b) \in (\mathbb{N}^*)^2$. Soit $d = a \wedge b$. Il existe deux entiers naturels non nuls a' et b' tels que $a = da'$ et $b = db'$ et $a' \wedge b' = 1$.

Démonstration. d divise a et b. Donc, il existe deux entiers naturels non nuls a' et b' tels que $a = da'$ et $b = db'$. De plus,

$$d = a \wedge b = (da') \wedge (db') = d(a' \wedge b').$$

Puisque $d \neq 0$, on obtient $a' \wedge b' = 1$ après simplification.

❑

3.2 PPCM

3.2.1 Définition du PPCM

Théorème 22. Soient a et b deux entiers relatifs tous deux non nuls. Il existe un entier naturel et un seul qui est un multiple commun à a et à b et qui est plus petit (au sens de la relation d'ordre usuelle $\leqslant$) que tout diviseur multiple commun à a et à b dans $\mathbb{N}^*$.

Démonstration. Soit $(a,b) \in (\mathbb{Z}^*)^2$.

Existence. Soit $\mathcal{E} = \{m \in \mathbb{N}^* / \ a|m \text{ et } b|m\}$. $\mathcal{E}$ est une partie non vide de $\mathbb{N}$ car $|ab|$ est un entier naturel non nul qui est un multiple commun à a et à b et donc $|ab| \in \mathcal{E}$.
$\mathcal{E}$ admet donc un plus petit élément qui est par définition un entier naturel non nul, multiple commun à a et à b et plus petit que tout multiple commun à a et à b qui est strictement positif.

Unicité. Un multiple commun à a et à b et plus petit que tout multiple commun strictement positif à a et à b, est nécessairement le minimum de $\mathcal{E}$ et on sait qu'un minimum est unique.

❑

Définition 3. Soient a et b deux entiers relatifs non nuls.

Le plus petit multiple commun à a et à b se note PPCM(a,b) ou aussi $a \vee b$.

Par exemple, $4 \vee 6 = 12$ car les nombres 5, 6, ..., 11 ne sont pas divisibles par 4 ou par 6 et 12 est divisible par 4 et par 6 (il faudra bien sûr améliorer les techniques de calcul d'un PPCM, ce qui se fera petit à petit).
On peut et on doit utiliser le PPCM pour réduire correctement au même dénominateur une somme de fractions. Par exemple,

$$\frac{7}{4} + \frac{5}{6} = \frac{7 \times 3}{4 \times 3} + \frac{5 \times 2}{6 \times 2} = \frac{31}{12}$$

et non pas

$$\frac{7}{4} + \frac{5}{6} = \frac{42}{24} + \frac{20}{24} = \frac{62}{24} = \frac{31}{12}.$$

Le meilleur dénominateur commun est bien $12 = 4 \vee 6$ et pas 24.

3.2.2 Propriétés du PPCM

On a immédiatement

Théorème 23.

1) $\forall a \in \mathbb{N}^*,\ a \vee a = a$.

2) $\forall a \in \mathbb{Z}^*,\ a \vee a = |a|$.

et aussi

Théorème 24. $\forall (a,b) \in (\mathbb{Z}^*)^2,\ a \vee b = |a| \vee |b|$.

On a vu que les diviseurs communs à deux entiers relatifs non nuls sont les diviseurs de leur PGCD. De même,

Théorème 25. Soit $(a,b) \in (\mathbb{Z}^*)^2$. Les multiples communs à a et à b sont les multiples de leur PPCM.

Démonstration. Soit $(a,b) \in (\mathbb{Z}^*)^2$. $a \vee b \in \mathbb{N}^*$ est un multiple commun à a et à b.
Soit $m \in \mathbb{Z}$. Si m est un multiple de $a \vee b$ (ou encore si $a \vee b$ divise m), par transitivité, m est un multiple commun à a et à b.
Réciproquement, soit m un multiple commun à a et à b. La division euclidienne de m par $a \vee b$ s'écrit $m = q(a \vee b) + r$ avec $(q,r) \in \mathbb{Z}^2$ et $0 \leqslant r < a \vee b$. m est un multiple de a et $q(a \vee b)$ est un multiple de a. Donc, $r = m - q(a \vee b)$ est un multiple de a. De même, r est un multiple de b. Finalement, r est un multiple commun à a et à b vérifiant de plus $0 \leqslant r < a \vee b$. Par définition de $a \vee b$, on en déduit que $r = 0$ puis que m est un multiple de $a \vee b$.

On a montré que pour tout $m \in \mathbb{Z}$, m est un multiple commun à a et b si et seulement si m est un multiple de $a \vee b$.

❑

⇨ **Commentaire.** *Le résultat du théorème 25 peut être écrit de manière plus condensée :* $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Théorème 26.

1) $\forall (a,b) \in (\mathbb{N}^*)^2,\ a \vee b = b \vee a$ (commutativité du PPCM).

2) $\forall (a,b,c) \in (\mathbb{N}^*)^3,\ (a \vee b) \vee c = a \vee (b \vee c)$ (associativité du PPCM).

3) $\forall a \in \mathbb{N}^*,\ 1 \vee a = a$ (1 est élément neutre pour le PPCM dans $\mathbb{N}^*$).

Démonstration.

1) Immédiat.

2) Soit $(a,b,c) \in (\mathbb{N}^*)^3$.

$$(a \vee b)\mathbb{Z} \cap c\mathbb{Z} = (a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z} = a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z}) = a\mathbb{Z} \cap (b \vee c)\mathbb{Z}.$$

Ainsi, l'ensemble des multiples communs à $a \vee b$ et c est aussi l'ensemble des multiples communs à a et $b \vee c$ (c'est l'ensemble des multiples communs à a, b et c). En particulier, $(a \vee b) \vee c = a \vee (b \vee c)$.

3) Immédiat.

❑

4 Nombres premiers entre eux. Théorèmes de Bézout et Gauss

4.1 Nombres premiers entre eux

Définition 4. Soit $(a,b) \in (\mathbb{Z}^*)^2$. a et b sont **premiers entre eux** si et seulement si $a \wedge b = 1$.

Par exemple, 5 et 6 sont premiers entre eux car le seul diviseur commun strictement positif à 5 et à 6 est 1 et 4 et 6 ne sont pas premiers entre eux car $4 \wedge 6 = 2 > 1$.

Exercice 5. Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (nombres de Fermat).

Montrer que les nombres de Fermat sont deux à deux premiers entre eux.

Solution 5. Soit $(n,m) \in \mathbb{N}^2$ tel que $m > n$. Posons $p = m - n$ de sorte que $m = n + p$ et $p > 0$.

$$\begin{aligned}
F_m &= 2^{2^m}+1 = 2^{2^n\times 2^p}+1 = \left(2^{2^n}\right)^{2^p}+1 = (F_n-1)^{2^p}+1\\
&= \sum_{k=0}^{2^p}\binom{2^p}{k}(-1)^{2^p-k}F_n^k+1 \text{ (d'après la formule du binôme de Newton)}\\
&= (-1)^{2^p}+\sum_{k=1}^{2^p}\binom{2^p}{k}(-1)^{2^p-k}F_n^k+1 \text{ (car } p>0 \text{ et donc } 2^p\geqslant 1)\\
&= 2+\sum_{k=1}^{2^p}\binom{2^p}{k}(-1)^{2^p-k}F_n^k \text{ (car } p>0 \text{ et donc } 2^p \text{ est pair)}\\
&= 2+F_n\sum_{k=1}^{2^p}\binom{2^p}{k}(-1)^{2^p-k}F_n^{k-1}.
\end{aligned}$$

Ainsi, il existe un entier relatif Q (à savoir $Q=\sum_{k=1}^{2^p}\binom{2^p}{k}(-1)^{2^p-k}F_n^{k-1}$) tel que $F_m = QF_n+2$.

D'après le lemme d'Euclide, on sait que $F_m\wedge F_n = F_n\wedge 2$. En particulier, le PGCD de F_n et F_m est un diviseur de 2 et est donc égal à 1 ou 2. Enfin, puisque $n\in\mathbb{N}$, $2^n\geqslant 1$ puis 2^{2^n} est pair et finalement F_n est impair. Donc, 2 ne divise pas F_n et il ne reste que

$$F_n\wedge F_m = 1.$$

On généralise maintenant la définition d'entiers premiers entre eux au cas de n entiers $n\geqslant 2$:

Définition 5. Soient $n\geqslant 2$ puis $(a_1,\dots,a_n)\in(\mathbb{Z}^*)^n$.

$a_1,\dots,a_n$ sont **premiers entre eux** (on dit aussi : premiers entre eux dans leur ensemble) si et seulement si

$$a_1\wedge a_2\wedge\dots\wedge a_n = 1.$$

$a_1,\dots,a_n$ sont **deux à deux premiers entre eux** si et seulement si

$$\forall(i,j)\in[\![1,n]\!]^2,\ (i\neq j\Rightarrow a_i\wedge a_j = 1).$$

Théorème 27. Soient $n\geqslant 2$ puis $(a_1,\dots,a_n)\in(\mathbb{Z}^*)^n$.

Si $a_1,\dots,a_n$ sont deux à deux premiers entre eux, alors $a_1,\dots,a_n$ sont premiers entre eux.

Démonstration. Soient $n\geqslant 2$ puis $(a_1,\dots,a_n)\in(\mathbb{Z}^*)^n$. Supposons que $a_1,\dots,a_n$ soient deux à deux premiers entre eux. Un diviseur commun à $a_1,\dots,a_n$ est en particulier un diviseur commun à a_1 et a_2 et est donc égal à 1.
Ceci montre que $a_1\wedge a_2\wedge\dots\wedge a_n = 1$.

❑

La réciproque du résultat précédent est fausse : si $a_1,\dots,a_n$ sont premiers entre eux, ils ne sont pas nécessairement deux à deux premiers entre eux. Par exemple $6\wedge 10 = 2$, $6\wedge 15 = 3$, et $10\wedge 15 = 5$ mais $6\wedge 10\wedge 15 = 1$.

4.2 Théorème de Bézout

Théorème 28. (théorème de Bézout).

Soit $(a,b)\in(\mathbb{Z}^*)^2$.

$$a\wedge b = 1 \Leftrightarrow \exists(u,v)\in\mathbb{Z}^2/\ au+bv = 1.$$

Plus généralement, soient $n\geqslant 2$ puis $(a_1,\dots,a_n)\in(\mathbb{Z}^*)^n$.

$$a_1\wedge\dots\wedge a_n = 1 \Leftrightarrow \exists\,(u_1,\dots,u_n)\in(\mathbb{Z}^*)^n\ /\ a_1u_1+\dots+a_nu_n = 1.$$

Démonstration.

• Soit $(a,b)\in(\mathbb{Z}^*)^2$.
Si a et b sont premiers entre eux, alors $a\wedge b=1$ et donc, d'après le théorème 16, page 8, il existe deux entiers relatifs u et v tels que $au+bv=1$.
S'il existe deux entiers relatifs u et v tels que $au+bv=1$, l'entier $d=a\wedge b$ divise a et b et donc d divise $au+bv=1$ d'après le théorème 7, page 3. On en déduit que $d=1$.

• Passons au cas général. Soit $(a_1,\dots,a_n)\in(\mathbb{Z}^*)^n$.
Supposons qu'il existe $(u_1,\dots,u_n)\in\mathbb{Z}^n$ tel que $a_1u_1+\dots+a_nu_n=1$. L'entier $d=a_1\wedge\dots\wedge a_n$ divise $a_1,\dots,a_n$ et donc d divise $a_1u_1+\dots+a_nu_n=1$. On en déduit que $d=1$.

Pour la réciproque, montrons par récurrence que pour tout $n\geqslant 2$, pour tout $(a_1,\dots,a_n)\in(\mathbb{Z}^*)^n$, il existe $(u_1,\dots,u_n)\in\mathbb{Z}^n$ tel que $a_1\wedge\dots\wedge a_n=a_1u_1+\dots+a_nu_n$.

- Le résultat est déjà connu pour $n=2$.
- Soit $n\geqslant 2$. Supposons le résultat pour n. Soit $(a_1,\dots,a_{n+1})\in(\mathbb{Z}^*)^{n+1}$. Il existe deux entiers relatifs u et u_{n+1} tels que

$$u(a_1\wedge\dots\wedge a_n)+a_{n+1}u_{n+1}=(a_1\wedge\dots\wedge a_n)\wedge a_{n+1}=a_1\wedge\dots\wedge a_n\wedge a_{n+1}.$$

Ensuite, par hypothèse de récurrence, il existe $(v_1,\dots,v_n)\in\mathbb{Z}^n$ tel que $a_1\wedge\dots\wedge a_n=a_1v_1+\dots+a_nv_n$ et on en déduit que

$$a_1\wedge\dots\wedge a_n\wedge a_{n+1}=u(a_1v_1+\dots+a_nv_n)+a_{n+1}v_{n+1}=uv_1a_1+\dots+uv_na_n+u_{n+1}a_{n+1}.$$

Le résultat est démontré par récurrence. En particulier, si $a_1,\dots,a_n$ sont n entiers relatifs non nuls et premiers entre eux, il existe $(u_1,\dots,u_n)\in\mathbb{Z}^n$ tel que $a_1u_1+\dots+a_nu_n=1$.

❑

Ainsi, par exemple, 21 et 10 sont premiers entre eux car $1\times 21+(-2)\times 10=1$. Deux entiers consécutifs non nuls n et $n+1$ sont toujours premiers entre eux car $1\times(n+1)+(-1)\times n=1$. 6, 10 et 15 sont premiers entre eux car $1\times 6+1\times 10+(-1)\times 15=1$.

Dans certaines situations, la question se pose de fournir explicitement des entiers u et v tels que $au+bv=1$. L'algorithme d'Euclide fournit un procédé d'obtention d'un tel couple comme le montre l'exercice suivant :

Exercice 6. Déterminer deux entiers relatifs u et v tels que $337u+241v=1$.

Solution 6. L'algorithme d'Euclide appliqué à 337 et 241 s'écrit

$$\begin{aligned}
337&=1\times 241+96\\
241&=2\times 96+49\\
96&=1\times 49+47\\
49&=1\times 47+2\\
47&=23\times 2+1\\
2&=2\times 1+0.
\end{aligned}$$

Le dernier reste non nul dans l'algorithme d'Euclide est 1 et donc $337\wedge 241=1$. D'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $337u+241v=1$. Déterminons explicitement un tel couple. En remontant dans l'algorithme d'Euclide, on obtient

$$\begin{aligned}
1&=47-23\times 2\\
&=47-23(49-1\times 47)=-23\times 49+24\times 47\\
&=-23\times 49+24(96-1\times 49)=24\times 96-47\times 49\\
&=24\times 96-47(241-2\times 96)=-47\times 241+118\times 96\\
&=-47\times 241+118(337-1\times 241)=118\times 337-165\times 241.
\end{aligned}$$

Le couple $(u,v)=(118,-165)$ est un couple d'entiers relatifs vérifiant $337u+241v=1$.

On peut présenter les calculs précédents d'une autre façon en descendant dans l'algorithme d'Euclide cette fois-ci. On obtient l'**algorithme d'Euclide étendu**. On veut deux entiers u et v tels que $au+bv=1$. On suppose que $b<a$ et que b ne divise pas a. On dispose de l'algorithme d'Euclide :

$$r_0=a,\ r_1=b \text{ et tant que } r_{k+1}\neq 0,\ r_k=q_kr_{k+1}+r_{k+2}.$$

On note r_{k_0+1} le dernier reste non nul de sorte que r_{k_0+1} est le PGCD de a et b. On veut deux entiers u et v tels que $r_{k_0+1}=au+bv$.
Au départ, on a $r_0=a=1\times a+0\times b=u_0a+v_0b$ avec $(u_0,v_0)=(1,0)$ et $r_1=b=0\times a+1\times b=u_1a+v_1b$ avec $(u_1,v_1)=(0,1)$. L'idée est alors simple : si $r_k=u_ka+v_kb$ et $r_{k+1}=u_{k+1}a+v_{k+1}b$, alors

$$r_{k+2} = r_k - q_k r_{k+1} = (u_k a + v_k b) - q_k (u_{k+1} a + v_{k+1} b) = (u_k - q_k u_{k+1}) a + (v_k - q_k v_{k+1}) b$$

On pose donc

$$(u_0, v_0) = (1, 0) \text{ et } (u_1, v_1) = (0, 1) \text{ puis, tant que } r_{k+1} \neq 0,\ (u_{k+2}, v_{k+2}) = (u_k - q_k u_{k+1}, v_k - q_k v_{k+1}).$$

A tout instant, on a $u_k a + v_k b = r_k$ et en particulier, on a $a \wedge b = r_{k_0+1} = u_{k_0+1} a + v_{k_0+1} b$. On a ainsi obtenu deux entiers relatifs u et b tels que $au + bv = a \wedge b$.

A titre d'exemple, reprenons les calculs de l'exercice 6 :

$337 = 1 \times 241 + 96$ $\quad r_0 = 337,\ q_0 = 1$
$241 = 2 \times 96 + 49$ $\quad r_1 = 241,\ q_1 = 2$
$96 = 1 \times 49 + 47$ $\quad r_2 = 96,\ q_2 = 1$
$49 = 1 \times 47 + 2$ $\quad r_3 = 49,\ q_3 = 1$
$47 = 23 \times 2 + 1$ $\quad r_4 = 47,\ q_4 = 23$
$2 = 2 \times 1 + 0$ $\quad r_5 = 2,\ q_5 = 21$ puis $r_6 = 1$

Présentons les résultats dans un tableau :

k	r_k	q_k
0	337	1
1	241	2
2	96	1
3	49	1
4	47	23
5	2	1
6	1	

L'algorithme d'Euclide étendu s'écrit alors (la dernière colonne est donnée à titre de vérification) (on rappelle que pour tout k $u_{k+2} = u_k - q_k u_{k+1}$ et $v_{k+2} = v_k - q_k v_{k+1}$)

k	r_k	q_k	u_k	v_k	$337u_k + 241v_k = r_k$
0	337	1	1	0	$1 \times 337 + 0 \times 241 = 337$
1	241	2	0	1	$0 \times 337 + 1 \times 241 = 241$
2	96	1	1	-1	$1 \times 337 + (-1) \times 241 = 96$
3	49	1	-2	3	$(-2) \times 337 + 3 \times 241 = 49$
4	47	23	3	-4	$3 \times 337 + (-4) \times 241 = 47$
5	2	1	-5	7	$(-5) \times 337 + 7 \times 241 = 2$
6	1		118	-165	$118 \times 337 + (-165) \times 241 = 1$

Un couple (u, v) tel que $337u + 241v = 1$ est donc $(118, -165)$.

4.3 Lemme de Gauss

Théorème 29. (lemme de Gauss).

Soient a, b et c trois entiers relatifs tels que $a \neq 0$ et $b \neq 0$.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration. Soient a, b et c trois entiers relatifs tels que $a \neq 0$ et $b \neq 0$ et a divise bc et a et b sont premiers entre eux. Il existe $q \in \mathbb{Z}$ tels que $bc = qa$ et d'autre part, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $au + bv = 1$.
On multiplie les deux membres de cette dernière égalité par c et on obtient

$$c = acu + bcv = acu + qav = a(cu + qv)$$

où $cu + qv$ est un entier relatif. Donc, a divise c.

❑

Il ne faut pas croire que si un entier a divise un produit bc, a divise automatiquement l'un des deux entiers b ou c. Par exemple, 8 divise $24 = 4 \times 6$ mais 8 ne divise ni 4, ni 6. Le théorème de Gauss dit que si de plus, a est premier avec un des deux entiers, alors a divise l'autre entier. Par exemple, 4 divise $24 = 3 \times 8$ et 4 est premier à 3 et de fait, 4 divise 8.

4.4 Quelques conséquences des théorèmes de Bézout et Gauss

Théorème 30. Soit $(a, b) \in (\mathbb{N}^*)^2$. On pose $m = a \vee b$ et $d = a \wedge b$. Alors,

$$md = ab.$$

Démonstration. Soit $(a, b) \in (\mathbb{N}^*)^2$. D'après le théorème 21, page 10, il existe deux entiers naturels non nuls a' et b' tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$. On a alors

$$ab = d(da'b') \quad (*).$$

Montrons que $m = da'b'$. $da'b' = ab' = a'b$ et donc $da'b'$ est un multiple commun à a et à b. D'après le théorème 25, page 11, $da'b'$ est un multiple de m ou encore m divise $da'b'$.
Inversement, m est un multiple de a et b. Posons donc $m = ka = lb$ où $(k, l) \in (\mathbb{N}^*)^2$. Puisque $ka = lb$, on a encore $kda' = ldb'$ puis $ka' = lb'$. b' divise $lb' = ka'$ et b' est premier à a'. D'après le théorème de Gauss, b' divise k. On peut donc poser $k = k'b'$ où $k' \in \mathbb{N}^*$. On obtient $m = ka = k'da'b'$ et donc $da'b'$ divise m.

En résumé, m divise $da'b'$ et $da'b'$ divise m. Puisque m et $da'b'$ sont des entiers naturels non nuls, on en déduit que $m = da'b'$. L'égalité $(*)$ s'écrit alors $ab = md$.

❑

Dans la démonstration précédente, on a obtenu plusieurs procédés équivalents pour calculer le PPCM de deux entiers quand on connaît leur PGCD. Prenons par exemple $a = 24 = 2 \times 12$ et $b = 36 = 3 \times 12$. Puisque $2 \wedge 3 = 1$, on a $d = 12$, $a' = 2$ et $b' = 3$. On en déduit que $m = da'b' = 12 \times 2 \times 3 = 72$ ou bien directement $m = \dfrac{ab}{d} = \dfrac{24 \times 36}{12} = 72$.

Théorème 31. Soient $n \geqslant 2$ puis $(a, b_1, \dots, b_n) \in (\mathbb{Z}^*)^{n+1}$.
(Pour tout $i \in [\![1, n]\!]$, $a \wedge b_i = 1$) $\Leftrightarrow a \wedge \left(\prod_{i=1}^{n} b_i\right) = 1$.

Démonstration. Pour chaque $i \in [\![1, n]\!]$, il existe $(u_i, v_i) \in \mathbb{Z}^2$ tel que $au_i + b_iv_i = 1$. On multiplie membre à membre toutes ces égalités : $\prod_{i=1}^{n}(au_i + b_iv_i) = 1$. En développant, on obtient une égalité de la forme $Ua + V\left(\prod_{i=1}^{n} b_i\right) = 1$ où U et V sont deux entiers relatifs (par exemple, $V = \prod_{i=1}^{n} v_i$). D'après le théorème de Bézout, a et $\prod_{i=1}^{n} b_i$ sont premiers entre eux.

Inversement, si a et $\prod_{i=1}^{n} b_i$ sont premiers entre eux, d'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $ua + v\prod_{i=1}^{n} b_i = 1$. Mais alors, pour chaque $i \in [\![1, n]\!]$,

$$ua + v\left(\prod_{j \neq i} b_j\right) b_i = 1$$

et donc, pour chaque $i \in [\![1, n]\!]$, il existe deux entiers relatifs u et v_i tels que $au + bv_i = 1$. On en déduit que a est premier à chaque b_i.

❑

Un corollaire immédiat au théorème 31 est :

Théorème 32. Soit $(a, b) \in (\mathbb{Z}^*)^2$. $a \wedge b = 1 \Leftrightarrow \forall (n, m) \in \mathbb{N}^2,\ a^n \wedge b^m = 1$.

Théorème 33. Soient $n \geqslant 2$ puis $(a, b_1, \dots, b_n) \in (\mathbb{Z}^*)^{n+1}$.

Si pour tout $i \in [\![1, n]\!]$, b_i divise a et si les b_i, $1 \leqslant i \leqslant n$, sont deux à deux premiers entre eux, alors $\prod_{i=1}^{n} b_i$ divise a.

Démonstration. Montrons le résultat par récurrence.

• Soient a, b_1 et b_2 trois entiers relatifs non nuls tels que b_1 et b_2 divisent a et $b_1 \wedge b_2 = 1$.
Il existe $k \in \mathbb{Z}$ tel que $a = kb_1$. b_2 divise $a = kb_1$ et $b_2 \wedge b_1 = 1$. D'après le théorème de Gauss, b_2 divise k. Donc, il existe $k' \in \mathbb{Z}$ tel que $k = k'b_2$ puis $a = k'b_1b_2$. Ceci montre que b_1b_2 divise a.

• Soit $n \geqslant 2$. Supposons le résultat pour n. Soient a, b_1, …, b_{n+1}, $n+2$ entiers relatifs non nuls tels que pour tout $i \in [\![1, n+1]\!]$, b_i divise a et b_1, …, b_{n+1} sont deux à deux premiers entre eux.

Par hypothèse de récurrence, $\prod_{i=1}^{n} b_i$ divise a. D'après le théorème 31, $\prod_{i=1}^{n} b_i$ et b_{n+1} sont premiers entre eux. D'après le cas $n = 2$, $\prod_{i=1}^{n+1} b_i$ divise a.

Le résultat est démontré par récurrence.

❑

Une autre application des théorèmes de Bézout et Gauss est la forme irréductible d'un nombre rationnel :

Théorème 34. Pour tout rationnel strictement positif r, il existe un couple $(a, b) \in (\mathbb{N}^*)^2$ et un seul tel que $r = \frac{a}{b}$ et $a \wedge b = 1$.

Démonstration.

Existence. Soit $r \in \mathbb{Q}^{+*}$. Il existe deux entiers naturels non nuls p et q tels que $r = \frac{p}{q}$. On sait que l'on peut écrire $p = da$ et $q = db$ où $d = p \wedge q$ et a et b sont deux entiers naturels non nuls premiers entre eux. On a alors

$$r = \frac{p}{q} = \frac{da}{db} = \frac{a}{b}$$

où cette fois-ci a et b sont premiers entre eux.

Unicité. Soit $(a_1, a_2, b_1, b_2) \in (\mathbb{N}^*)^4$ tel que $a_1 \wedge b_1 = 1$, $a_2 \wedge b_2 = 1$ et $\frac{a_1}{b_1} = \frac{a_2}{b_2}$. Alors, $a_1b_2 = a_2b_1$. a_2 divise $a_2b_1 = a_1b_2$ et $a_2 \wedge b_2 = 1$. Donc, a_2 divise a_1 d'après le théorème de Gauss. De même, a_1 divise a_2 et finalement $a_1 = a_2$ puis $b_1 = b_2$.

❑

Définition 6. L'écriture d'un rationnel strictement positif r sous la forme $r = \frac{a}{b}$ avec $a \wedge b = 1$ s'appelle la **forme irréductible** du rationnel r.

4.5 Résolution dans $\mathbb{Z}^2$ de l'équation $ax + by = c$

On se donne trois entiers relatifs a, b et c tels que $a \neq 0$ et $b \neq 0$. On veut résoudre dans $\mathbb{Z}^2$ l'équation

$$ax + by = c \quad (E),$$

d'inconnue $(x, y) \in \mathbb{Z}^2$.

• Posons $d = a \wedge b$. Pour tout couple d'entiers relatifs (x, y), d divise $ax + by$. Si de plus $ax + by = c$, alors d doit diviser c. Donc, si d ne divise pas c, l'équation (E) n'a pas de solution dans $\mathbb{Z}^2$. C'est par exemple le cas de l'équation $2x + 4y = 3$: $2x + 4y$ est toujours un nombre relatif pair, alors que 3 est un nombre impair. Cette équation n'a pas de solution dans $\mathbb{Z}^2$.

Supposons maintenant que d divise c. On peut écrire $a = da'$, $b = db'$ et $c = dc'$ où a' et b' dont deux entiers relatifs premiers entre eux et c' est un entier relatif. Après simplification par d, l'équation (E) s'écrit

$$a'x + b'y = c',$$

où cette fois-ci a' et b' sont premiers entre eux.

• Soient donc a et b deux entiers relatifs non nuls et premiers entre eux. Soit (E_0) l'équation

$$ax + by = 1.$$

D'après le théorème de Bézout, il existe au moins une solution (x_0', y_0') de cette équation dans $\mathbb{Z}^2$. On rappelle qu'une telle solution peut par exemple être obtenue en remontant l'algorithme d'Euclide ou grâce à l'algorithme d'Euclide étendu.
Par définition, $ax_0' + by_0' = 1$. En multipliant les deux membres de cette égalité par c, on obtient $a(cx_0') + b(xy_0') = c$. Le couple $(x_0, y_0) = (cx_0', cy_0')$ est une solution particulière dans $\mathbb{Z}^2$ de l'équation (E).
Par exemple, le couple $(x_0', y_0') = (-1, 2)$ est une solution particulière de l'équation $7x + 4y = 1$ et donc le couple $(x_0, y_0) = (-3, 6)$ est une solution particulière de l'équation $7x + 4y = 3$.
On a ainsi montré que quand $a \wedge b = 1$, pour tout $c \in \mathbb{Z}$, l'équation $ax + by = c$ admet toujours au moins une solution (x_0, y_0) dans $\mathbb{Z}^2$.

• On peut maintenant résoudre complètement l'équation (E). Soit $(a, b) \in (\mathbb{Z}^*)^2$ tel que $a \wedge b = 1$. Soient $c \in \mathbb{Z}$ puis (x_0, y_0) une solution particulière dans $\mathbb{Z}^2$ de l'équation (E) : $ax + by = c$.

Soit $(x, y) \in \mathbb{Z}^2$.

$$\begin{aligned}(x, y) \text{ solution de (E)} &\Leftrightarrow ax + by = c \Leftrightarrow ax + by = ax_0 + by_0\\ &\Leftrightarrow a(x_0 - x) = b(y - y_0).\end{aligned}$$

Si (x, y) est solution de (E), nécessairement b divise $b(y - y_0) = a(x_0 - x)$. Puisque $a \wedge b = 1$, le théorème de Gauss permet d'affirmer que b divise $x_0 - x$ et donc il existe $k \in \mathbb{Z}$ tel que $x_0 - x = kb$ ou encore $x = x_0 - kb$. De même, a divise $y - y_0$ et donc il existe $k' \in \mathbb{Z}^2$ tel que $y - y_0 = k'a$ ou encore $y = y_0 + k'a$.

Réciproquement, soient $(k, k') \in \mathbb{Z}^2$ puis $(x, y) = (x_0 - kb, y_0 + k'a)$.

$$\begin{aligned}(x, y) \text{ solution de (E)} &\Leftrightarrow a(x_0 - x) = b(y - y_0) \Leftrightarrow a(kb) = b(k'a)\\ &\Leftrightarrow (k - k')ab = 0\\ &\Leftrightarrow k = k' \text{ (car } ab \neq 0).\end{aligned}$$

Les solutions de (E) dans $\mathbb{Z}^2$ sont les couples de la forme $(x_0 - kb, y_0 + ka)$, $k \in \mathbb{Z}$. On peut résumer tout ce qui précède dans un théorème :

Théorème 35.

1) Soient a, b et c trois entiers relatifs tels que $a \neq 0$, $b \neq 0$. L'équation (E) : $ax + by = c$ admet au moins une solution dans $\mathbb{Z}^2$ si et seulement si $a \wedge b$ divise c. Dans ce cas, quite à diviser les deux membres de (E) par $a \wedge b$, on se ramène à la situation où $a \wedge b = 1$.

2) Soient a, b et c trois entiers relatifs tels que $a \neq 0$, $b \neq 0$ et $a \wedge b = 1$. Les solutions de (E) dans $\mathbb{Z}^2$ sont les couples de la forme

$$(x, y) = (x_0 - kb, y_0 + ka),\ k \in \mathbb{Z}$$

où (x_0, y_0) est une solution particulière de (E) dans $\mathbb{Z}^2$.

Exercice 7. Résoudre dans $\mathbb{Z}^2$ l'équation (E) : $12x + 7y = 2$.

Solution 1. L'algorithme d'Euclide appliqué à 7 et 12 s'écrit

$12 = 1 \times 7 + 5$
$7 = 1 \times 5 + 2$
$5 = 2 \times 2 + 1$

(En particulier, $7 \wedge 12 = 1$). Donc,

$$\begin{aligned}1 &= 5 - 2 \times 2\\ &= 5 - 2(7 - 1 \times 5) = 3 \times 5 - 2 \times 7\\ &= 3(12 - 1 \times 7) - 2 \times 7 = 3 \times 12 - 5 \times 7.\end{aligned}$$

En multipliant les deux membres de l'égalité par 2, on obtient $6 \times 12 - 10 \times 7 = 2$. Le couple $(x_0, y_0) = (6, -10)$ est une solution particulière de (E) dans $\mathbb{Z}^2$.

Soit $(x,y)\in\mathbb{Z}^2$.

$$\begin{aligned}(x,y)\text{ solution de }(E)&\Leftrightarrow 12x+7y=2\Leftrightarrow 12x+7y=12x_0+7y_0\\&\Leftrightarrow 12(x-x_0)=7(y_0-y).\end{aligned}$$

Si (x,y) est solution de (E), nécessairement 7 divise $7(y_0-y)=12(x-x_0)$. Puisque $7\wedge 12=1$, le théorème de Gauss permet d'affirmer que 7 divise $x-x_0$ et donc il existe $k\in\mathbb{Z}$ tel que $x-x_0=7k$ ou encore $x=x_0+7k$. De même, 12 divise y_0-y et donc il existe $k'\in\mathbb{Z}^2$ tel que $y_0-y=12k'$ ou encore $y=y_0-12k'$.

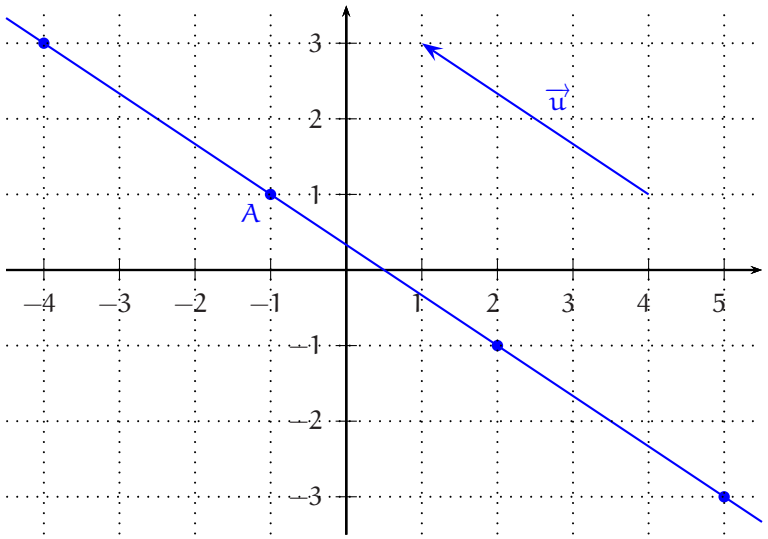
Réciproquement, soient $(k,k')\in\mathbb{Z}^2$ puis $(x,y)=(x_0+7k,y_0-12k')$.

$$\begin{aligned}(x,y)\text{ solution de }(E)&\Leftrightarrow 12(x-x_0)=7(y_0-y)\Leftrightarrow 12\times 7\times k=7\times 12\times k'\\&\Leftrightarrow k=k'.\end{aligned}$$

Les solutions de (E) : $12x+7y=2$ dans $\mathbb{Z}^2$ sont les couples de la forme $(6+7k,-10-12k)$, $k\in\mathbb{Z}$.

La résolution dans $\mathbb{Z}^2$ de l'équation $ax+by=c$ a bien sûr une interprétation géométrique. Si le plan est rapporté à un repère $\mathcal{R}$, l'ensemble $\mathcal{D}$ des points M du plan de coordonnées $(x,y)\in\mathbb{R}^2$ est une droite. Résoudre dans $\mathbb{Z}^2$ l'équation $ax+by=c$, c'est déterminer les points de cette droite à **coordonnées entières**.

Par exemple, les points à coordonnées entières de la droite d'équation $2x+3y=1$ sont les points de coordonnées $(-1-3k,1+2k)$. Ces coordonnées peuvent se lire sous la forme $(-1,1)+k(-3,2)$, $k\in\mathbb{Z}$. Le vecteur $\vec{u}$ de coordonnées $(-3,2)$ est un vecteur directeur directeur particulier de cette droite à coordonnées entières et le point A de coordonnées $(-1,1)$ est un point particulier de cette droite à coordonnées entières. Les points solutions s'écrivent alors $A+k\vec{u}$, $k\in\mathbb{Z}$.



5 Nombres premiers. Décomposition primaire

5.1 Définition des nombres premiers

Définition 7. Soit n un entier naturel supérieur ou égal à 2.

n est **premier** si et seulement si n admet exactement deux diviseurs strictement positifs, à savoir 1 et lui-même. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Un entier supérieur ou égal à 2 non premier est dit **composé**.

◇ Les premiers nombres premiers sont

$$2\quad 3\quad 5\quad 7\quad 11\quad 13\quad 17\quad 19\quad \ldots$$

◇ $6=2\times 3$ n'est pas premier ou encore 6 est composé car 6 est divisible par au moins un autre nombre que 1 et 6 comme par exemple 2.

◇ 1 ne fait pas partie de la liste des nombres premiers. Nous démontrerons plus loin que tout entier supérieur ou égal à 2 se décompose de manière unique à l'ordre près des facteurs en produit de nombres premiers. Par exemple, $72 = 2^3 \times 3^2$ avec unicité de cette décomposition et en particulier unicité des exposants écrits. Si on décidait maintenant que 1 est un nombre premier, on perdrait cette unicité : par exemple, $72 = 1^3 \times 2^3 \times 3^2 = 1^5 \times 2^3 \times 3^2$.

◇ Rien ne dit à priori qu'il existe une infinité de nombres premiers. Nous le démontrerons plus loin.

Si un nombre entier n supérieur ou égal à 2 est premier, n n'admet pas d'autre diviseur que 1 et n et si n est composé, n admet au moins un diviseur qui n'est ni 1, ni n. Donc,

Théorème 36. Soient n un entier naturel supérieur ou égal à 2.

n est composé si et seulement si il existe $(a, b) \in (\mathbb{N}^*)^2$ tel que $1 < a < n$, $1 < b < n$ et $n = ab$.
n est premier si et seulement si pour tout $(a, b) \in (\mathbb{N}^*)^2$, $(n = ab \Rightarrow a = 1 \text{ ou } b = 1)$.

5.2 Quelques propriétés des nombres premiers

Théorème 37. Soient n un entier naturel supérieur ou égal à 2 et p un nombre premier.

Si p divise n, alors $n \wedge p = p$ et si p ne divise pas n, alors $n \wedge p = 1$.

Démonstration. Soit $d = n \wedge p$. d est en particulier un diviseur de p et donc $d = 1$ ou $d = p$.
Si p divise n, immédiatement $d = p$ et si p ne divise pas n, on ne peut avoir $d = p$ et il ne reste que $d = 1$.

❑

⇨ **Commentaire.** *Si on considère deux entiers naturels non nuls a et b, trois situations sont possibles : l'un des deux entiers divise l'autre (par exemple, $a = 4$ et $b = 8$), les deux entiers sont premiers entre eux (par exemple $a = 4$ et $b = 9$) ou ni l'un, ni l'autre (par exemple $a = 4$ et $b = 6$). Quand l'un des deux entiers a ou b est un nombre premier, il n'y a plus que deux situations possibles, les deux situations du théorème 37.*

Théorème 38. Deux nombres premiers distincts sont premiers entre eux.

Plus généralement, si p et q sont des nombres premiers distincts, alors pour tout $(\alpha, \beta) \in \mathbb{N}^2$, $p^\alpha \wedge q^\beta = 1$.

Démonstration. Soient p et q deux nombres premiers distincts. Les diviseurs strictement positifs de p sont 1 et p et les diviseurs strictement positifs de q sont 1 et q. Puisque $p \neq q$, le seul diviseur strictement positif commun à p et q est 1. Ceci montre que $p \wedge q = 1$.

Mais alors, le théorème 32, page 15, montre que pour tout $(\alpha, \beta) \in \mathbb{N}^2$, $p^\alpha \wedge q^\beta = 1$. ❑

Théorème 39. Tout nombre entier $n \geqslant 2$ admet au moins un diviseur qui est un nombre premier.

Démonstration. On montre le résultat par récurrence forte.

- Si $n = 2$, n admet au moins un diviseur premier à savoir 2.
- Soit $n \geqslant 2$. Supposons que pour tout $k \in [\![2, n]\!]$, k admet au moins un diviseur qui est un nombre premier. Si $n+1$ est premier, $n+1$ admet au moins un diviseur qui est un nombre premier. Sinon, $n+1$ n'est pas premier et admet donc au moins un diviseur k qui n'est ni 1, ni $n+1$. Ce diviseur k vérifie donc $2 \leqslant k \leqslant n$. Par hypothèse de récurrence, k admet au moins un diviseur premier p. p divise k et k divise $n+1$. Donc, par transitivité, p est un nombre premier divisant $n+1$.

Le résultat est démontré par récurrence.

❑

Théorème 40. Soient p un nombre premier et $a_1, \ldots, a_n$, n entiers naturels non nuls, $n \geqslant 2$. Si p divise $a_1 \times \ldots \times a_n$ alors p divise l'un des a_i, $1 \leqslant i \leqslant n$.

Démonstration. Si p ne divise aucun des a_i, $1 \leqslant i \leqslant n$, alors pour tout $i \in [\![1, n]\!]$, $p \wedge a_i = 1$ d'après le théorème 37 puis $p \wedge \left(\prod_{i=1}^{n} a_i\right) = 1$ d'après le théorème 31, page 15. Par contraposition, si p divise $\prod_{i=1}^{n} a_i$, alors il existe $i \in [\![1, n]\!]$ tel que p divise a_i.

❑

5.3 Le théorème fondamental de l'arithmétique

Théorème 41. (théorème fondamental de l'arithmétique)

Tout entier naturel supérieur ou égal à 2 se décompose de manière unique, à l'ordre près des facteurs, en produit de facteurs premiers.

Démonstration .

Existence. Soit $n \geqslant 2$. D'après le théorème 39, n est divisible par au moins un nombre premier et d'autre part, tout nombre premier p divisant n vérifie $2 \leqslant p \leqslant n$. Il y a donc un nombre fini $k \in [\![1, n-1]\!] \subset \mathbb{N}^*$ de nombres premiers divisant n. Notons p_1, ..., p_k les k nombres premiers deux à deux distincts divisant n.

Soit $i \in [\![1, k]\!]$. Soit $\mathcal{E}_i = \{\alpha \in \mathbb{N}^* / \ p_i^\alpha | n\}$. Puisque p_i est un nombre premier divisant n, $1 \in \mathcal{E}_i$ et donc $\mathcal{E}_i$ est une partie non vide de $\mathbb{N}$ (et même de $\mathbb{N}^*$). Vérifions que $\mathcal{E}_i$ est une partie majorée de $\mathbb{N}$. Soit $\alpha \in \mathbb{N}^*$.

$$\begin{aligned} \alpha \in \mathcal{E}_i &\Rightarrow p_i^\alpha | n \Rightarrow p_i^\alpha \leqslant n \Rightarrow \ln(p_i^\alpha) \leqslant \ln(n) \\ &\Rightarrow \alpha \leqslant \frac{\ln(n)}{\ln(p_i)} \text{ (car } p_i \geqslant 2 \Rightarrow \ln(p_i) > 0). \end{aligned}$$

Ainsi, $\mathcal{E}_i$ est une partie de $\mathbb{N}$ non vide (car $1 \in \mathcal{E}_i$) et majorée (par $\frac{\ln(n)}{\ln(p_i)}$). $\mathcal{E}_i$ admet donc un plus grand élément.

Soit $\alpha_i = \text{Max}\{\alpha \in \mathbb{N}^* / \ p^\alpha | n\}$. Par définition, $p_i^{\alpha_i}$ divise n et $p_i^{\alpha_i+1}$ ne divise pas n.

Ainsi, chacun des entiers $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ divise n et $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ sont deux à deux premiers entre eux d'après le théorème 38. D'après le théorème 33, n est divisible par $p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}$. Donc, il existe un entier naturel non nul q tel que

$$n = q \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Supposons par l'absurde que $q \geqslant 2$. q est divisible par au moins un nombre premier p. Puisque p divise q et que q divise n, p divise n et donc p est l'un des nombres premiers p_1, ..., p_k. Si $i \in [\![1, k]\!]$ est tel que $p = p_i$, n est divisible par $p_i \times p_i^{\alpha_i} = p_i^{\alpha_i+1}$, ce qui contredit le caractère maximal de α_i. Donc, $q = 1$ puis

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

On a décomposé n en un produit de nombres premiers.

Unicité. p_1, ..., p_k, $k \in \mathbb{N}^*$, désignent toujours les nombres premiers deux à deux distincts divisant n. Supposons que

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{k} p_i^{\beta_i}$$

où $(\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k) \in (\mathbb{N}^*)^{2k}$. Soit $i \in [\![1, k]\!]$. $p_i^{\beta_i}$ divise $\prod_{j=1}^{k} p_j^{\beta_j} = \prod_{j=1}^{k} p_j^{\alpha_j}$ et $p_i^{\beta_i} \wedge \left(\prod_{j \neq i} p_j^{\alpha_j} \right) = 1$ (car les p_i sont des nombres premiers deux à deux distincts et d'après les théorèmes 38 et 31). D'après le théorème de Gauss, $p_i^{\beta_i}$ divise $p_i^{\alpha_i}$. En particulier, $p_i^{\beta_i} \leqslant p_i^{\alpha_i}$ puis $\beta_i \leqslant \alpha_i$. De même, $\alpha_i \leqslant \beta_i$ et finalement $\alpha_i = \beta_i$.

On a montré l'unicité de la décomposition.

❑

Définition 8. Soit n un entier naturel supérieur ou égal à 2.

L'écriture $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, où les p_i sont des nombres premiers deux à deux distincts et les α_i sont des entiers naturels non nuls, s'appelle la **décomposition primaire** de n.

Ainsi, par exemple, la décomposition primaire de 72 est $72 = 2^3 \times 3^2$. L'unicité de cette décomposition assure par exemple que $2^2 \times 3^3 \neq 72$, sans plus faire aucun calcul.

DÉFINITION 9. Soient n un entier naturel supérieur ou égal à 2 et p un nombre premier.

La **valuation p-adique de** n, notée $v_p(n)$ est

$$v_p(n) = \text{Max}\{\alpha \in \mathbb{N} / \ p^\alpha | n\}.$$

La décomposition primaire d'un entier n supérieur ou égal à 2 s'écrit alors

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

où $\mathcal{P}$ désigne l'ensemble des nombres premiers.

Ainsi, $v_2(72) = 3$, $v_3(72) = 2$ et $v_5(72) = 0$. De manière générale, si p n'est pas un facteur premier de n, on a $v_p(n) = 0$ et donc $p^{v_p(n)} = 1$.
Si p est un facteur premier de n (c'est-à-dire un nombre premier divisant n),
- pour $0 \leqslant \alpha \leqslant v_p(n)$, p^α divise $p^{v_p(n)}$ et $p^{v_p(n)}$ divise n et donc p^α divise n,
- pour $\alpha > v_p(n)$, p^α ne divise pas n,
- pour $\alpha = v_p(n)$, p^α divise n et $p^{\alpha+1}$ ne divise pas n. Cette condition caractérise entièrement $v_p(n)$.

On verra plus loin que l'ensemble $\mathcal{P}$ des nombres premiers est infini. Le produit $\prod_{p \in \mathcal{P}} p^{v_p(n)}$ contient donc une infinité de facteurs. Mais seul un nombre fini de ces facteurs est différent de 1 de sorte que le produit est totalement défini et peut se réécrire en n'utilisant qu'un nombre fini de facteurs.

5.4 Infinité de l'ensemble des nombres premiers

Théorème 42. Il existe une infinité de nombres premiers.

DÉMONSTRATION. Montrons par récurrence que pour tout entier naturel non nul n, il existe n nombres premiers.

- $p_1 = 2$ est premier. Donc, le résultat est vrai quand $n = 1$.
- Soit $n \geqslant 1$. Supposons qu'il existe n nombres premiers deux à deux distincts $p_1, \ldots, p_n$.

  Soit $N = 1 + \prod_{i=1}^{n} p_i$. N est un entier naturel supérieur ou égal à 2 car $N \geqslant 1 + p_1 \geqslant 1 + 2 \geqslant 2$. N admet donc au moins diviseur premier que l'on note p_{n+1}. Montrons que p_{n+1} est distinct de chacun des p_i, $1 \leqslant i \leqslant n$.

  Supposons par l'absurde, il existe $i_0 \in [\![1, n]\!]$ tel que $p_{n+1} = p_{i_0}$, alors p_{n+1} divise $\prod_{i=1}^{n} p_i$ et p_{n+1} divise N. Donc, p_{n+1} divise $N - \prod_{i=1}^{n} p_i = 1$ ce qui est faux. Donc, p_{n+1} est distinct de chacun des p_i, $1 \leqslant i \leqslant n$, et on a montré qu'il existe $n+1$ nombres premiers deux à deux distincts.

Le résultat est démontré par récurrence.

❑

⇨ **Commentaire**. *Le procédé ci-dessus fournit des nombres premiers deux à deux distincts. Il n'y a par contre aucune raison pour que ce procédé fournissent tous les nombres premiers ou même une infinité de nombres obtenus dans l'ordre croissant.*
Ainsi, si on prend $p_1 = 2$. *Alors,* $x_1 = p_1 + 1 = 3$ *fournit* $p_2 = 3$. $x_2 = p_1p_2 + 1 = 7$ *fournit* $p_3 = 7$. $x_3 = p_1p_2p_3 + 1 = 43$ *fournit* $p_4 = 43$. $x_5 = p_1p_2p_3p_4 + 1 = 1807 = 13 \times 139$ *fournit par exemple* $p_5 = 13$.

5.5 Tester si un nombre est premier. Le crible d'ERATOSTHÈNE

5.5.1 Tester si un nombre est premier

On commence par un résultat utile pour réduire le nombre de vérifications.

Théorème 43. Soit n un entier naturel supérieur ou égal à 2.

Si n n'est pas premier, n est divisible par au moins un nombre premier p tel que $p \leqslant \sqrt{N}$.
Si n n'est divisible par aucun un nombre premier p tel que $p \leqslant \sqrt{N}$, alors n est premier.

Démonstration. Soit n un entier naturel supérieur ou égal à 2. Supposons n non premier, il existe donc deux entiers naturels non nuls a et b tels que $n = ab$ et $2 \leqslant a \leqslant n-1$ et $2 \leqslant b \leqslant n-1$. Si $a > \sqrt{n}$ et $b > \sqrt{n}$, alors $ab > \sqrt{n} \times \sqrt{n} = n$ ce qui est faux. Donc, $a \leqslant \sqrt{n}$ ou $b \leqslant \sqrt{n}$.

Si par exemple $a \leqslant \sqrt{n}$, puisque $a \geqslant 2$, a est divisible par au moins un nombre premier p tel que $p \leqslant a \leqslant \sqrt{n}$. Ainsi, si n n'est pas premier, n est divisible par au moins un nombre premier inférieur ou égal à sa racine.

Par contraposition, si n n'est divisible par aucun nombre premier p tel que $p \leqslant \sqrt{N}$, alors n est premier.

❑

A titre d'exemple, testons si 71 et 899 sont premiers.

$64 \leqslant 71 \leqslant 81$ et donc $E\left(\sqrt{71}\right) = 8$. Les nombres premiers inférieurs ou égaux à $\sqrt{71}$ sont 2, 3, 5 et 7. 71 n'est divisible ni par 2 ($71 = 2 \times 35 + 1$), ni par 3 ($71 = 3 \times 23 + 2$), ni par 5 ($71 = 5 \times 14 + 1$), ni par 7 ($71 = 7 \times 10 + 1$). Donc, 71 est un nombre premier.

$E\left(\sqrt{899}\right) = 29$ (car $30^2 = 900$). Les nombres premiers inférieurs ou égaux à $\sqrt{899}$ sont 2, 3, 5, 7, 11, 13, 17, 19, 23 et 29. 899 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, ni par 11, ni par 13, ni par 17, ni par 19, ni par 23. Mais au dernier moment $899 = 29 \times 31$. 899 n'est donc pas un nombre premier. (De manière générale, les entiers supérieurs ou égaux à 8 qui précèdent un carré parfait ne sont jamais premier car pour $n \geqslant 3$, $n^2 - 1 = (n-1)(n+1)$ avec $n + 1 \geqslant n - 1 \geqslant 2$).

5.5.2 Le crible d'Eratosthène

On veut systématiser la démarche précédente pour obtenir avec un minimum de calcul la liste des nombres premiers inférieurs ou égaux à 100 par exemple et ceci de manière algorithmique. Puisque $\sqrt{100} = 10$, un entier n compris au sens large entre 2 et 100 est un nombre premier si et seulement si n n'est divisible par aucun nombre premier inférieur ou égaux à 10.

On écrit les entiers de 1 à 100 dans un tableau carré, on barre 1 qui n'est pas premier et on entoure 2 qui est premier. On barre ensuite tous les multiples de 2 sauf 2 qui ne sont pas des nombres premiers.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

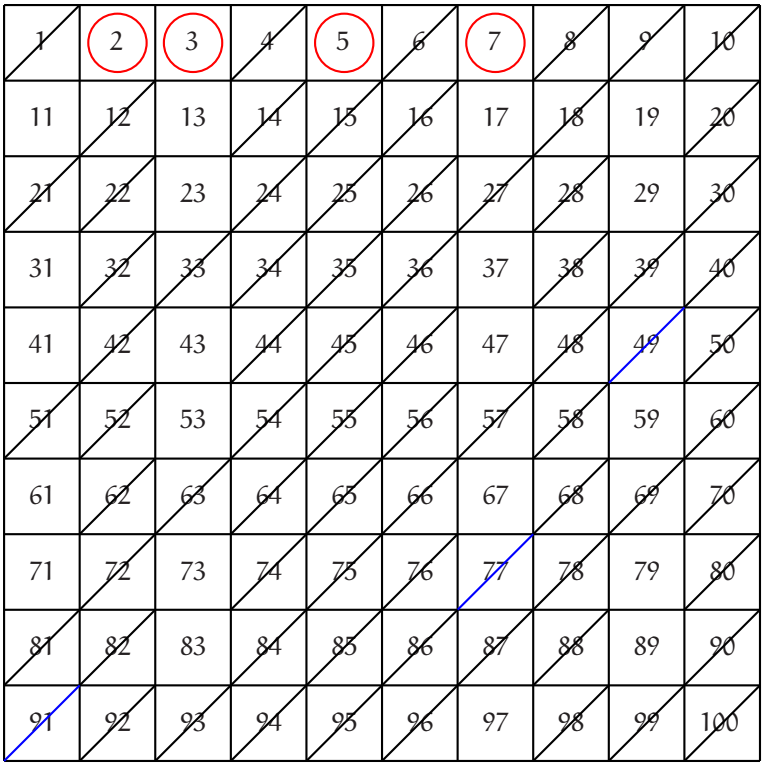
Le premier entier non barré après 2 est 3. 3 n'est donc multiple d'aucun nombre premier le précédant et par suite, 3 est premier. On entoure 3 puis on barre tous les multiples de 3 sauf 3 qui n'ont pas encore été barrés.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

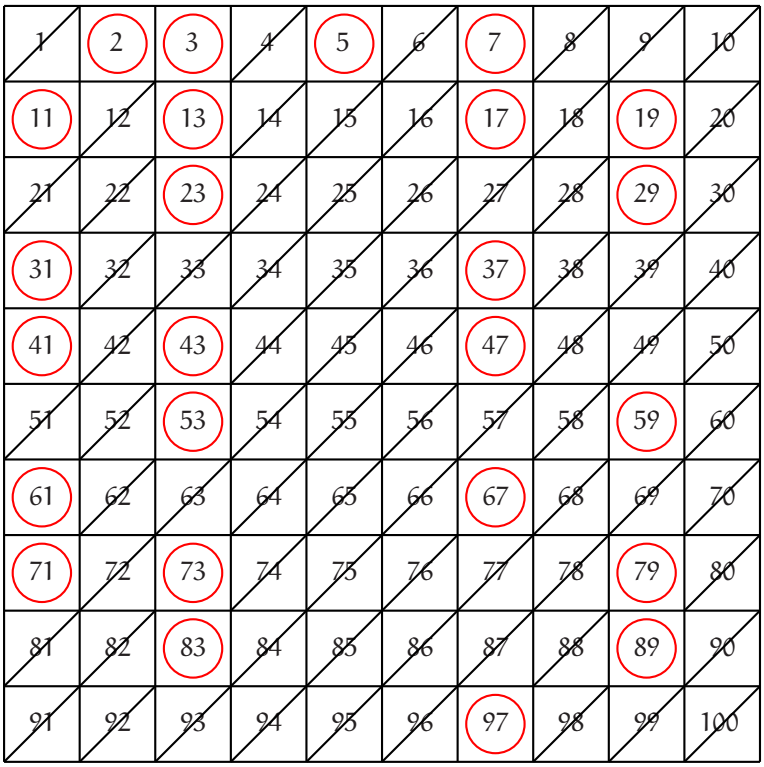
Le premier entier non barré après 3 est 5. 5 n'est donc multiple d'aucun nombre premier le précédant et par suite, 5 est premier. On entoure 5 puis on barre tous les multiples de 5 sauf 5 qui n'ont pas encore été barrés.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Le premier entier non barré après 5 est 7. 7 est premier. On entoure 7 puis on barre tous les multiples de 7 sauf 7 qui n'ont pas encore été barrés.



Les nombres non barrés ne sont multiples d'aucun nombre premier de la première ligne et donc ne sont multiples d'aucun nombre premier inférieur ou égal à leur racine carrée. L'algorithme s'achève : les nombres non barrés sont les nombres premiers inférieurs ou égaux à 100.



Les nombres premiers inférieurs ou égaux à 100 sont

2 3 5 7 11 13 17 19 23 29 31 37 41
43 47 53 59 61 67 71 73 79 83 89 97

5.6 Décomposer un entier en produit de facteurs premiers

Soit n un entier naturel supérieur ou égal à 2. On veut la décomposition primaire de n. On procède de manière systématique. On commence par le nombre premier 2 et on cherche la plus grande puissance de 2 divisant n. On obtient $n = 2^\alpha n'$ où

n' n'est plus divisible par 2. On passe au nombre premier 3 et on écrit $n = 2^\alpha 3^\beta n''$ où n'' n'est divisible ni par 2, ni par 3. On passe ensuite au nombre premier 5 ...

Par exemple,

$$\begin{aligned} 792\,792 &= 2 \times 396\,396 = 2^2 \times 198\,198 = 2^3 \times 99\,099 \\ &= 2^3 \times 3 \times 33\,033 = 2^2 \times 3^2 \times 11\,011 \\ &= 2^2 \times 3^2 \times 7 \times 1573 \\ &= 2^2 \times 3^2 \times 7 \times 11 \times 143 = 2^2 \times 3^2 \times 7 \times 11^2 \times 13. \end{aligned}$$

5.7 Quelques applications du théorème fondamental de l'arithmétique

Théorème 44. Soient a et b deux entiers supérieurs ou égaux à 2.

a et b sont premiers entre eux si et seulement si a et b n'ont pas de facteur premier commun.

Démonstration. Soit $d = a \wedge b$.
Si $d = 1$, a et b n'admettent pas de diviseur commun supérieur ou égal à 2 et en particulier n'admettent pas de facteur premier commun.
Si $d \geqslant 2$, d est divisible par au moins un nombre premier p qui est un diviseur commun à a et à b.

❑

Par exemple, $21 = 3 \times 7$ et $26 = 2 \times 13$ sont premiers entre eux.

Théorème 45. Soit n un entier supérieur ou égal à 2. On suppose que la décomposition primaire de n s'écrit

$$n = p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}.$$

Les diviseurs de n sont les entiers de la forme $p_1^{\beta_1} \times \ldots \times p_k^{\beta_k}$ où, pour tout $i \in [\![1, k]\!]$, $0 \leqslant \beta_i \leqslant \alpha_i$.

Le nombre des diviseurs de n est $\prod_{i=1}^{k} (\alpha_i + 1)$.

⇨ **Commentaire.**

Le théorème précédent peut aussi s'exprimer sous la forme : pour tous entiers n et m supérieurs ou égaux à 2,

$$m \textit{ divise } n \Leftrightarrow \forall p \in \mathcal{P},\ v_p(m) \leqslant v_p(n).$$

Démonstration. Soit n un entier supérieur ou égal à 2. Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la décomposition primaire de n. Soit $(\beta_1, \ldots, \beta_k) \in \prod_{i=1}^{k} [\![0, \alpha_i]\!]$. Alors, pour tout $i \in [\![1, k]\!]$, $\alpha_i - \beta_i \geqslant 0$ puis

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \left(\prod_{i=1}^{k} p_i^{\beta_i} \right) \left(\prod_{i=1}^{k} p_i^{\alpha_i - \beta_i} \right).$$

Ceci montre que $\prod_{i=1}^{k} p_i^{\beta_i}$ est un diviseur de n.

Réciproquement, soit d un diviseur de n.
Si $d = 1$, $d = p_1^0 \times \ldots \times p_k^0$.
Sinon, $d \geqslant 2$. Soit p un facteur premier de d. Puisque p divise d et d divise n, p divise n puis $p \wedge n = p$. Si p n'est aucun des p_i, p est premier à chaque p_i puis p est premier à $\prod_{i=1}^{k} p_i^{\alpha_i} = n$ ce qui contredit $p \wedge n = p$. Donc, p est l'un des p_i. Par suite, on peut poser $d = \prod_{i=1}^{k} p_i^{\beta_i}$ où les β_i, $1 \leqslant i \leqslant k$, sont des entiers naturels.

Soit $i \in [\![1, k]\!]$. $p_i^{\beta_i}$ divise d et d divise n. Donc, $p_i^{\beta_i}$ divise $n = \prod_{j=1}^{k} p_j^{\alpha_j}$. D'autre part, $p_i^{\beta_i}$ est premier à $\prod_{j \neq i} p_j^{\alpha_j}$. D'après le théorème de Gauss, $p_i^{\beta_i}$ divise $p_i^{\alpha_i}$ et en particulier, $\beta_i \leqslant \alpha_i$.

On a montré que les diviseurs de n sont les entiers de la forme $d = p_1^{\beta_1} \times \ldots \times p_k^{\beta_k}$ où, pour tout $i \in [\![1,k]\!]$, $0 \leqslant \beta_i \leqslant \alpha_i$.

Soit $\mathcal{D}$ l'ensemble des diviseurs de n. Soit $f : \prod_{i=1}^{k} [\![0,\alpha_i]\!] \to \mathcal{D}$. f est une application surjective d'après ce qui précède

$$(\beta_1,\ldots,\beta_k) \mapsto \prod_{i=1}^{k} p_i^{\beta_i}$$

et injective d'après le théorème fondamental de l'arithmétique (et en tenant compte du fait que le seul k-uplet d'image 1 est le k-uplet $(0,\ldots,0)$). f est donc une bijection et en particulier (voir chapitre « Dénombrements »)

$$\text{card}(\mathcal{D}) = \text{card}\left(\prod_{i=1}^{k} [\![0,\alpha_i]\!]\right) = \prod_{i=1}^{k} (\alpha_i+1).$$

❑

Par exemple, puisque $72 = 2^3 \times 3^2$, 72 admet $(3+1)(2+1) = 12$ diviseurs. Les diviseurs de 72 sont les nombres

$$\begin{array}{llll} 2^0\times 3^0 = 1 & 2^1\times 3^0 = 2 & 2^2\times 3^0 = 4 & 2^3\times 3^0 = 8 \\ 2^0\times 3^1 = 3 & 2^1\times 3^1 = 6 & 2^2\times 3^1 = 12 & 2^3\times 3^1 = 24 \\ 2^0\times 3^2 = 9 & 2^1\times 3^2 = 18 & 2^2\times 3^2 = 36 & 2^3\times 3^2 = 72 \end{array}$$

Exercice 8. Soit n un entier supérieur ou égal à 2. On suppose que la décomposition primaire de n s'écrit $n = p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}$.

Calculer la somme des diviseurs de n.

Solution 8. Soit n un entier supérieur ou égal à 2. Notons $S(n)$ la somme des diviseurs de n.

$$\begin{aligned} S(n) &= \sum_{(\beta_1,\ldots,\beta_k)\in[\![0,\alpha_1]\!]\times\ldots\times[\![0,\alpha_k]\!]} p_1^{\beta_1}\times\ldots\times p_k^{\beta_k} \\ &= \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right)\times\ldots\times\left(\sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k}\right) \\ &= \frac{p_1^{\alpha_1+1}-1}{p_1-1}\times\ldots\times\frac{p_k^{\alpha_k+1}-1}{p_k-1}. \end{aligned}$$

Ainsi, par exemple, $S(72) = \dfrac{2^4-1}{2-1}\times\dfrac{3^3-1}{3-1} = \dfrac{15\times 26}{2} = 195$ (et de fait 1+2+3+4+6+8+9+12+18+24+36+72 = 195).

Théorème 46. Soient a et b deux entiers naturels non nuls.

On suppose que $a = p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \times \ldots \times p_k^{\beta_k}$ où $k \in \mathbb{N}^*$, p_1, …, p_k, sont des nombres premiers deux à deux distincts et α_1, …, α_k, β_1, …, β_k, sont des entiers naturels.

Alors, $a \wedge b = p_1^{\text{Min}(\alpha_1,\beta_1)} \times \ldots \times p_k^{\text{Min}(\alpha_k,\beta_k)}$ et $a \vee b = p_1^{\text{Max}(\alpha_1,\beta_1)} \times \ldots \times p_k^{\text{Max}(\alpha_k,\beta_k)}$.

Démonstration. La résultat est clair si $a = 1$ ou $b = 1$. Dorénavant, on suppose $a \geqslant 2$ et $b \geqslant 2$. D'après le théorème précédent, un diviseur commun à a et à b est nécessairement de la forme $p_1^{\gamma_1} \times \ldots \times p_k^{\gamma_k}$ où pour tout $i \in [\![1,k]\!]$, $\gamma_i \leqslant \text{Min}(\alpha_i,\beta_i)$ (en adaptant le théorème précédent quand l'un des α_i ou l'un des β_i est nul) et est donc un diviseur de $p_1^{\text{Min}(\alpha_1,\beta_1)} \times \ldots \times p_k^{\text{Min}(\alpha_k,\beta_k)}$. D'autre part, $p_1^{\text{Min}(\alpha_1,\beta_1)} \times \ldots \times p_k^{\text{Min}(\alpha_k,\beta_k)}$ divise a et b et on a donc montré que

$$a \wedge b = p_1^{\text{Min}(\alpha_1,\beta_1)} \times \ldots \times p_k^{\text{Min}(\alpha_k,\beta_k)}.$$

Soit $m = a \vee b$. Pour $i \in [\![1,k]\!]$, m est un multiple de a et donc de $p_i^{\alpha_i}$ et un multiple de b et donc de $p_i^{\beta_i}$. Par suite, pour tout $i \in [\![1,k]\!]$, m est un multiple de $p_i^{\text{Max}(\alpha_i,\beta_i)}$. Maintenant, les entiers $p_i^{\text{Max}(\alpha_i,\beta_i)}$, $1 \leqslant i \leqslant k$, sont deux à deux premiers entre eux et donc m est un multiple de $p_1^{\text{Max}(\alpha_1,\beta_1)}\times\ldots\times p_k^{\text{Max}(\alpha_k,\beta_k)}$ d'après le théorème 33. Puisque d'autre part, $p_1^{\text{Max}(\alpha_1,\beta_1)}\times\ldots\times p_k^{\text{Max}(\alpha_k,\beta_k)}$ est un multiple commun à a et à b, on a montré que

$$a \vee b = p_1^{\text{Max}(\alpha_1,\beta_1)} \times \ldots \times p_k^{\text{Max}(\alpha_k,\beta_k)}.$$

❑

⇨ **Commentaire.** *On note que le théorème 46 peut aussi s'écrire sous la forme :* $\forall p \in \mathcal{P}$, $v_p(a \wedge b) = Min\{v_p(a), v_p(b)\}$ *et* $v_p(a \vee b) = Max\{v_p(a), v_p(b)\}$.

Exemple. $120 = 2^3 \times 3^1 \times 5^1 \times 7^0$ et $252 = 2^2 \times 3^2 \times 5^0 \times 7^1$. Donc $120 \wedge 252 = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$ et $120 \vee 252 = 2^3 \times 3^2 \times 5^1 \times 7^1 = 2520$.

⇨ **Commentaire.** *Pour tout* $(\alpha, \beta) \in \mathbb{N}^2$, $Min(\alpha, \beta) + Max(\alpha, \beta) = \alpha + \beta$ *et donc, on retrouve l'égalité*

$$(a \wedge b)(a \vee b) = \left(\prod_{i=1}^{k} p_i^{Min(\alpha_i, \beta_i)}\right)\left(\prod_{i=1}^{k} p_i^{Max(\alpha_i, \beta_i)}\right) = \prod_{i=1}^{k} p_i^{Min(\alpha_i, \beta_i) + Max(\alpha_i, \beta_i)} = \prod_{i=1}^{k} p_i^{\alpha_i + \beta_i} = ab.$$

6 Congruences

6.1 Définition

DÉFINITION 10. Soit n un entier naturel. Soient a et b deux entiers relatifs.

b est congru à a modulo n si et seulement si $b - a$ est un multiple de n ou encore si et seulement si il existe $q \in \mathbb{Z}$ tel que $b = a + qn$.

La phrase « b est congru à a modulo n » se note $a \equiv b\ [n]$ ou aussi $a \equiv b\ (\text{mod } n)$.

Remarques.

• $a \equiv b\ [0] \Leftrightarrow \exists q \in \mathbb{Z} /\ b = a + q \times 0 \Leftrightarrow a = b$. La congruence modulo 0 est donc tout simplement l'égalité.

• $a \equiv b\ [1] \Leftrightarrow b - a$ multiple de $1 \Leftrightarrow b - a \in \mathbb{Z}$. Cette dernière phrase est toujours vraie et donc tout entier est congru à tout entier modulo 1.

• $a \equiv 0\ [2]$ signifie que a est pair et $a \equiv 1\ [2]$ signifie que a est impair. Plus généralement, $a \equiv b\ [2] \Leftrightarrow b - a$ multiple de 2. Ceci équivaut à dire que les entiers a et b ont même parité (ils sont tous les deux pairs ou tous les deux impairs).

• Les entiers relatifs a vérifiant $a \equiv 0\ [n]$ sont les multiples de n : $\{a \in \mathbb{Z} /\ a \equiv 0\ [n]\} = n\mathbb{Z}$. ❑

Exemples.

Puisque $24 = 9 + 3 \times 5$, on a encore $24 - 9 \in 5\mathbb{Z}$ et donc $9 \equiv 24\ [5]$. La congruence modulo 5 a pour effet d'« effacer tout multiple de 5 » dans une somme.
Puisque $-3 = 11 - 2 \times 7$, on a $11 \equiv -3\ [7]$. ❑

Un résultat immédiat est :

Théorème 47. Soit n un entier naturel non nul. Soit a un entier relatif. Soit r le reste de la division euclidienne de a par n. Alors, $a \equiv r\ [n]$

Une des premières propriétés de la congruence modulo n est qu'elle se comporte comme l'égalité. Plus précisément,

Théorème 48. Soit n un entier naturel.

La congruence modulo n est une relation d'équivalence.

DÉMONSTRATION. Soit $n \in \mathbb{N}$. La congruence modulo n est une relation binaire sur $\mathbb{Z}$.

Réflexivité. Soit $a \in \mathbb{Z}$. $a - a = 0 = 0 \times n$ et donc $a \equiv a\ [n]$. Ainsi,

$$\forall a \in \mathbb{Z},\ a \equiv a\ [n]$$

et donc la congruence modulo n est réflexive.

Symétrie. Soit $(a, b) \in \mathbb{Z}^2$ tel que $a \equiv b\ [n]$. Donc, il existe $q \in \mathbb{Z}$ tel que $b = a + qn$. Mais alors, $a = b + (-q)n$ où $-q$ est un entier relatif et donc $b \equiv a\ [n]$. Ainsi,

$$\forall (a, b) \in \mathbb{Z}^2,\ (a \equiv b\ [n] \Rightarrow b \equiv a\ [n])$$

et donc la congruence modulo n est symétrique.

Transitivité. Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a \equiv b\ [n]$ et $b \equiv c\ [n]$. Alors, il existe $(q, q') \in \mathbb{Z}^2$ tel que $b = a + qn$ et $c = b + q'n$. On en déduit que $c = a + qn + q'n = a + (q + q')n$ avec $q + q' \in \mathbb{Z}$ et donc $a \equiv c\ [n]$. Ainsi,

$$\forall (a, b, c) \in \mathbb{Z}^2,\ (a \equiv b\ [n] \text{ et } b \equiv c\ [n] \Rightarrow a \equiv c\ [n])$$

et donc la congruence modulo n est transitive.

On a montré que la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

❑

Ainsi, la congruence $2 \equiv 7\ [5]$ peut tout aussi bien se lire $7 \equiv 2\ [5]$.

6.2 Calculs avec des congruences

Nous allons maintenant apprendre à calculer avec des congruences.

Théorème 49. (compatibilité avec l'addition). Soit n un entier naturel.

1) $\forall (a,b,c) \in \mathbb{Z}^3$, $(a \equiv b\ [n] \Rightarrow a+c \equiv b+c\ [n])$.

2) $\forall (a,b,c,d) \in \mathbb{Z}^4$, $(a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow a+c \equiv b+d\ [n])$.

Démonstration .

1) Soit $(a,b,c) \in \mathbb{Z}^3$.

$$a \equiv b\ [n] \Rightarrow \exists q \in \mathbb{Z}/\ b = a+qn \Rightarrow \exists q \in \mathbb{Z}/\ b+c = a+c+qn \Rightarrow a+c \equiv b+c\ [n].$$

2) Soit $(a,b,c,d) \in \mathbb{Z}^4$.

$$a \equiv b\ [n] \text{ et } c \equiv d\ [n] \Rightarrow a+c \equiv b+c\ [n] \text{ et } b+c \equiv b+d\ [n] \Rightarrow a+c \equiv b+d\ [n] \text{ (par transitivité).}$$

❑

Ainsi, on peut additionner membre à membre des congruences.

Théorème 50. (compatibilité avec la multiplication). Soit n un entier naturel.

1) $\forall (a,b,c) \in \mathbb{Z}^3$, $(a \equiv b\ [n] \Rightarrow ac \equiv bc\ [n])$.

2) $\forall (a,b,c,d) \in \mathbb{Z}^4$, $(a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow ac \equiv bd\ [n])$.

3) $\forall (a,b) \in \mathbb{Z}^2$, $\forall k \in \mathbb{N}$, $(a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n])$.

Démonstration .

1) Soit $(a,b,c) \in \mathbb{Z}^3$.

$$a \equiv b\ [n] \Rightarrow \exists q \in \mathbb{Z}/\ b = a+qn \Rightarrow \exists q \in \mathbb{Z}/\ bc = ac+(qc)n \Rightarrow ac \equiv bc\ [n].$$

2) Soit $(a,b,c,d) \in \mathbb{Z}^4$.

$$a \equiv b\ [n] \text{ et } c \equiv d\ [n] \Rightarrow ac \equiv bc\ [n] \text{ et } bc \equiv bd\ [n] \Rightarrow ac \equiv bd\ [n] \text{ (par transitivité).}$$

3) Soit $(a,b) \in \mathbb{Z}^2$ tel que $a \equiv b\ [n]$. Par récurrence (et d'après b)), pour tout $k \in \mathbb{N}$, $a^k \equiv b^k\ [n]$.

❑

Ainsi, on peut multiplier membre à membre des congruences.

On va maintenant analyser le principal problème des congruences : la possibilité de simplifier un même nombre de part et d'autre d'une congruence. On va voir que simplifier pour l'addition ne pose aucun problème mais que la simplification pour la multiplication en pose.

Théorème 51. (simplifications). Soit n un entier naturel non nul.

1) $\forall (a,b,c) \in \mathbb{Z}^3$, $a+c \equiv b+c\ [n] \Rightarrow a \equiv b\ [n]$ (tout entier relatif est simplifiable pour l'addition).

2) a) $\forall (a,b) \in \mathbb{Z}^2$, $\forall c \in \mathbb{Z}^*$, $(ac \equiv bc\ [n]$ et $c \wedge n = 1) \Rightarrow a \equiv b\ [n]$.
b) Si $n \geqslant 2$, les entiers relatifs simplifiables modulo n sont les entiers non nuls et premiers à n.

Démonstration . Soit n un entier naturel non nul.

1) Soit $(a,b,c) \in \mathbb{Z}^3$.

$$a+c \equiv b+c\ [n] \Rightarrow a+c+(-c) \equiv b+c+(-c)\ [n] \Rightarrow a \equiv b\ [n].$$

2) a) Soit $(a,b) \in \mathbb{Z}^2$. Soit $c \in \mathbb{Z}^*$ tel que $c \wedge n = 1$. D'après le théorème de Bézout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $cu+vn = 1$. Mais alors, $cu \equiv 1\ [n]$. On en déduit que

$$ac \equiv bc\ [n] \Rightarrow acu \equiv bcu\ [n] \Rightarrow a \times 1 \equiv b \times 1\ [n]\ (*)$$
$$\Rightarrow a \equiv b\ [n].$$

L'implication $(*)$ se détaille de la façon suivante : $cu \equiv 1\ [n] \Rightarrow acu \equiv a \times 1\ [n]$ par compatibilité avec la multiplication et de même $bcu \equiv b \times 1\ [n]$. Mais alors, par transitivité, puisque $a \equiv acu\ [n]$, $acu \equiv bcu\ [n]$ et $bcu \equiv b\ [n]$, on en déduit que $a \equiv b\ [n]$.

b) Soit $n \geqslant 2$. D'après ce qui précède, les entiers relatifs non nuls et premiers à n sont simplifiables pour la multiplication.

Si $c = 0$, $c \times 0 = 0 \equiv 0 = c \times 1\ [n]$ mais $0 \not\equiv 1\ [n]$ (car $n \geqslant 2$). Donc, 0 n'est pas simplifiable pour la congruence modulo n.

Si $c \neq 0$ et $c \wedge n \neq 1$, soit p un facteur premier de $c \wedge n$. p est un facteur premier de n et donc il existe $q \in [\![2, n-1]\!]$ tel que $n = pq$. Puisque d'autre part p divise c, il existe un entier c' tel que $c = pc'$. Mais alors $qc = qpc' = nc'$ et donc $qc \equiv 0\ [n]$.
Ainsi, il existe q vérifiant $1 < q < n$ et $qc \equiv 0\ [n]$ ou encore $qc \equiv 0c\ [n]$. Mais puisque $1 < q < n$, on a $q \not\equiv 0\ [n]$ et on ne peut donc pas simplifier c dans la congruence $qc \equiv 0c\ [n]$.

On a montré que les entiers relatifs simplifiables modulo n sont les entiers non nuls et premiers à n.

❑

En résumé, si $n \geqslant 2$, pour tout $(a, b, c) \in \mathbb{Z}^3$, $a + c \equiv b + c\ [n] \Leftrightarrow a \equiv b\ [n]$ et pour tout $(a, b) \in \mathbb{Z}^2$, si c est un entier relatif non nul premier à n, $ac \equiv bc\ [n] \Leftrightarrow a \equiv b\ [n]$. Ces résultats sont essentiels pour résoudre des congruences :

Exercice 9. Résoudre dans $\mathbb{Z}$ les congruences :

1) $3x + 5 \equiv 4\ [7]$.

2) a) $6x + 5 \equiv 2\ [9]$.
b) $6x + 5 \equiv 1\ [9]$.

Solution 9. Dans les deux questions, on note $\mathcal{S}$ l'ensemble des solutions de la congruence proposée.

1) Soit $x \in \mathbb{Z}$.

$$\begin{aligned} 3x + 5 \equiv 4\ [7] &\Leftrightarrow 3x + 5 + (-5) \equiv 4 + (-5)\ [7] \Leftrightarrow 3x \equiv -1\ [7] \\ &\Leftrightarrow 5 \times 3x \equiv 5 \times (-1)\ [7]\ (\text{car } 5 \wedge 7 = 1) \\ &\Leftrightarrow x \equiv -5\ [7] \Leftrightarrow x \equiv 2\ [7]. \end{aligned}$$

Ainsi, $\mathcal{S} = \{2 + 7k,\ k \in \mathbb{Z}\} = 2 + 7\mathbb{Z}$.

2) a) Soit $x \in \mathbb{Z}$.

$$\begin{aligned} 6x + 5 \equiv 2\ [9] &\Leftrightarrow 6x = -3\ [9] \Leftrightarrow \exists k \in \mathbb{Z} / \ 6x = -3 + 9k \Leftrightarrow \exists k \in \mathbb{Z} / \ 2x = -1 + 3k \\ &\Leftrightarrow 2x \equiv -1\ [3] \Leftrightarrow 2 \times 2x \equiv 2 \times (-1)\ [3]\ (\text{car } 2 \wedge 3 = 1) \\ &\Leftrightarrow x \equiv -2\ [3] \Leftrightarrow x \equiv 1\ [3]. \end{aligned}$$

Ainsi, $\mathcal{S} = \{1 + 3k,\ k \in \mathbb{Z}\} = 1 + 3\mathbb{Z}$.

b) Soit $x \in \mathbb{Z}$.

$$6x + 5 \equiv 1\ [9] \Leftrightarrow 6x = -4\ [9] \Leftrightarrow \exists k \in \mathbb{Z} / \ 6x - 9k = -4.$$

Maintenant, l'équation $6x - 9k = -4$ n'a pas de solution dans $\mathbb{Z}$ car $6x - 9k$ est un entier divisible par 3 alors que -4 n'est un entier divisible par 3. Ainsi, $\mathcal{S} = \varnothing$.

Exercice 10. Résoudre dans $\mathbb{Z}^2$ le système de congruence

$$\begin{cases} 3x - 2y \equiv 1\ [7] \\ 4x + 5y \equiv 3\ [7] \end{cases}$$

Solution 10. On note $\mathcal{S}$ l'ensemble des solutions du sytème proposé. Soit $(x, y) \in \mathbb{Z}^2$.

$$\left\{\begin{array}{l} 3x-2y\equiv 1\ [7] \\ 4x+5y\equiv 3\ [7] \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} 3x\equiv 1+2y\ [7] \\ 4x+5y\equiv 3\ [7] \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} 5\times 3x\equiv 5(1+2y)\ [7] \\ 4x+5y\equiv 3\ [7] \end{array}\right. \quad (\text{car } 5\wedge 7=1)$$
$$\Leftrightarrow \left\{\begin{array}{l} x\equiv 5+10y\ [7] \\ 4x+5y\equiv 3\ [7] \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x\equiv -2+3y\ [7] \\ 4(-2+3y)+5y\equiv 3\ [7] \end{array}\right.$$
$$\Leftrightarrow \left\{\begin{array}{l} x\equiv -2+3y\ [7] \\ 17y\equiv 11\ [7] \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} 3y\equiv -3\ [7] \\ x\equiv -2+3y\ [7] \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} y\equiv -1\ [7] \\ x\equiv -2+3(-1)\ [7] \end{array}\right. \quad (\text{car } 3\wedge 7=1)$$
$$\Leftrightarrow \left\{\begin{array}{l} y\equiv -1\ [7] \\ x\equiv -5\ [7] \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} y\equiv -1\ [7] \\ x\equiv 2\ [7] \end{array}\right. .$$

Donc, $\mathcal{S}=\left\{(2+7k,-1+7k'),\ (k,k')\in\mathbb{Z}^2\right\}=(2+7\mathbb{Z})\times(-1+7\mathbb{Z})$.

6.3 Le petit théorème de Fermat

Théorème 52. (petit théorème de Fermat). Soit p un nombre premier.

1) Pour tout $a\in\mathbb{N}$, $a^p\equiv a\ [p]$.

2) Pour tout $a\in\mathbb{N}^*$, $(a\wedge p=1\Rightarrow a^{p-1}\equiv 1\ [p])$.

Démonstration. On va démontrer le 1) par récurrence après avoir établi un

Lemme. Pour tout nombre premier p et tout $k\in[\![1,p-1]\!]$, p divise $\binom{p}{k}$.

Démonstration du lemme. Soit p un nombre premier. Donc $p\geqslant 2$. Soit $k\in[\![1,p-1]\!]$. On sait que $k\binom{p}{k}=p\binom{p-1}{k-1}$. Ainsi, p divise $p\binom{p-1}{k-1}=k\binom{p}{k}$. D'autre part, puisque p est premier et que $1\leqslant k\leqslant p-1<p$, on a $p\wedge k=1$. D'après le théorème de Gauss, p divise $\binom{p}{k}$. Le lemme est démontré.

On peut maintenant établir le théorème. Montrons par récurrence que pour tout $a\in\mathbb{N}$, $a^p\equiv a\ [p]$.

- $0^p\equiv 0\ [p]$ et donc le résultat est vrai pour $a=0$.
- Soit $a\geqslant 0$. Supposons que $a^p\equiv a\ [p]$. D'après la formule du binôme de Newton,

$$\begin{aligned}(a+1)^p=\sum_{k=0}^{p}\binom{p}{k}a^k&=1+\sum_{k=1}^{p-1}\binom{p}{k}a^k+a^p\\ &\equiv 1+0+a^p\ [p]\ (\text{d'après le lemme})\\ &\equiv a+1\ [p]\ (\text{par hypothèse de récurrence}).\end{aligned}$$

On a montré par récurrence que pour tout $a\in\mathbb{N}$, $a^p\equiv a\ [p]$.

Montrons maintenant 2). Soit $a\in\mathbb{N}^*$ tel que $a\wedge p=1$. On a vu dans la démonstration du théorème 51 qu'il existe $a'\in\mathbb{N}^*$ tel que $aa'\equiv 1\ [p]$. Mais alors

$$a^p\equiv a\ [p]\Rightarrow a'\times a^p\equiv a'a\ [p]\Rightarrow a^{p-1}\equiv 1\ [p].$$

❑

⇨ **Commentaire.** *La congruence $a^p\equiv a\ [p]$ est valable pour tout $a\in\mathbb{Z}$. En effet, si $a<0$, $a^p=(-1)^p(-a)^p\equiv(-1)^{p+1}a\ [p]$. Si p est un nombre premier supérieur ou égal à 3, $p+1$ est pair et donc $(-1)^p=1$ puis $a^p\equiv a\ [p]$ et si $p=2$, $(-1)^{p+1}=-1\equiv 1\ [2]$ et encore une fois $a^p\equiv a\ [p]$.*
De même, la congruence $a^{p-1}\equiv 1\ [p]$, valable quand $a\in\mathbb{N}^*$ et $a\wedge p=1$, reste valable quand $a\in\mathbb{Z}^*$ et $a\wedge p=1$.

Exercice 11. Montrer que pour tout $(m,n)\in(\mathbb{N}^*)^2$, $mn\left(m^{36}-n^{36}\right)$ est divisible par 25 935.

Solution 11. $25\,935 = 3 \times 8\,645 = 3 \times 5 \times 1729 = 3 \times 5 \times 7 \times 247 = 3 \times 5 \times 7 \times 13 \times 19$ où 3, 5, 7, 13 et 19 sont des nombres premiers.

Soit $(m, n) \in (\mathbb{N}^*)^2$. Posons $N = mn\left(m^{36} - n^{36}\right)$.

• Si m ou n est divisible par 3, alors N est divisible par 3. Sinon, $m \wedge 3 = 1$ et $n \wedge 3 = 1$ et d'après le petit théorème de Fermat, $m^2 \equiv 1\ [3]$ et $n^2 \equiv 1\ [3]$ puis

$$\begin{aligned} N &= mn\left(\left(m^2\right)^{18} - \left(n^2\right)^{18}\right) \\ &\equiv mn\left((1)^{18} - (1)^{18}\right)\ [3] \\ &\equiv 0\ [3]. \end{aligned}$$

et encore une fois N est divisible par 3. Dans tous les cas, N est divisible par 3.

• Si m ou n est divisible par 5, alors N est divisible par 5. Sinon, $m \wedge 5 = 1$ et $n \wedge 5 = 1$ et d'après le petit théorème de Fermat, $m^4 \equiv 1\ [5]$ et $n^4 \equiv 1\ [5]$ puis

$$\begin{aligned} N &= mn\left(\left(m^4\right)^9 - \left(n^4\right)^9\right) \\ &\equiv mn\left((1)^9 - (1)^9\right)\ [5] \\ &\equiv 0\ [5]. \end{aligned}$$

et encore une fois N est divisible par 5. Dans tous les cas, N est divisible par 5.

• Si m ou n est divisible par 7, alors N est divisible par 7. Sinon, $m \wedge 7 = 1$ et $n \wedge 7 = 1$ et d'après le petit théorème de Fermat, $m^6 \equiv 1\ [7]$ et $n^6 \equiv 1\ [7]$ puis

$$\begin{aligned} N &= mn\left(\left(m^6\right)^6 - \left(n^6\right)^6\right) \\ &\equiv mn\left((1)^6 - (1)^6\right)\ [7] \\ &\equiv 0\ [7]. \end{aligned}$$

et encore une fois N est divisible par 7. Dans tous les cas, N est divisible par 7.

• Si m ou n est divisible par 13, alors N est divisible par 13. Sinon, $m \wedge 13 = 1$ et $n \wedge 13 = 1$ et d'après le petit théorème de Fermat, $m^{12} \equiv 1\ [13]$ et $n^{12} \equiv 1\ [13]$ puis

$$\begin{aligned} N &= mn\left(\left(m^{12}\right)^3 - \left(n^{12}\right)^3\right) \\ &\equiv mn\left((1)^3 - (1)^3\right)\ [13] \\ &\equiv 0\ [13]. \end{aligned}$$

et encore une fois N est divisible par 13. Dans tous les cas, N est divisible par 13.

• Si m ou n est divisible par 19, alors N est divisible par 19. Sinon, $m \wedge 19 = 1$ et $n \wedge 19 = 1$ et d'après le petit théorème de Fermat, $m^{18} \equiv 1\ [19]$ et $n^{18} \equiv 1\ [19]$ puis

$$\begin{aligned} N &= mn\left(\left(m^{18}\right)^2 - \left(n^{18}\right)^2\right) \\ &\equiv mn\left((1)^2 - (1)^2\right)\ [19] \\ &\equiv 0\ [19]. \end{aligned}$$

et encore une fois N est divisible par 19. Dans tous les cas, N est divisible par 19.

En résumé, dans tous les cas, N est divisible par les nombres premiers 3, 5, 7, 13 et 19 et finalement N est divisible par $3 \times 5 \times 7 \times 13 \times 19 = 25\,935$.

6.4 Quelques critères de divisibilité

On écrit un entier naturel non nul n en base 10 :

$$n = c_p 10^p + c_{p-1} 10^{p-1} + \ldots + c_1 10 + c_0$$

où, pour tout $i \in [\![0, p]\!]$, $c_i \in [\![0, 9]\!]$ et $c_p \neq 0$ (les c_i sont les chiffres de n en base 10). On cherche une condition nécessaire et suffisante sur les chiffres de n pour que n soit divisible par certains entiers.

Critère de divisibilité par 9. On part d'une remarque simple : $10 \equiv 1\ [9]$. On en déduit que

$$n \equiv c_p + c_{p-1} + \ldots + c_1 + c_0\ [9].$$

Ainsi, modulo 9, un entier est congru à la somme de ses chiffres (en base 10). En particulier, en notant $S(n)$ la somme des chiffres (en base 10) de n,

$$n \text{ est divisible par } 9 \Leftrightarrow n \equiv 0\ [9] \Leftrightarrow S(n) \equiv 0\ [9] \Leftrightarrow S(n) \text{ est divisible par } 9.$$

Ainsi, un entier est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

Par exemple, modulo 9, 2844 est congru à $2 + 8 + 4 + 4 = 18$ qui est divisible par 9 et donc 2844 est divisible par 9. Modulo 9, de 541968 est $5 + 4 + 1 + 9 + 6 + 8 = 33$ puis à $3 + 3 = 6$. Donc, le reste de la division euclidienne de 541968 par 9 est 6.

Critère de divisibilité par 3. De même, $10 \equiv 1\ [3]$ et donc, modulo 3, un entier est congru à la somme de ses chiffres. En particulier, un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Critère de divisibilité par 11. C'est presque la même idée : $10 \equiv -1\ [11]$ et donc

$$n = \sum_{k=0}^{p} c_k 10^k \equiv \sum_{k=0}^{p} (-1)^k c_k\ [11]$$

ou encore, modulo 11, un entier est congru à la somme alternée de ses chiffres. En particulier, un entier est divisible par 11 si et seulement si la somme alternée $c_0 - c_1 + c_2 - \ldots + (-1)^p c_p$ de ses chiffres est divisible par 11.

Par exemple, la somme alternée des chiffres de 3 141 567 est $7 - 6 + 5 - 1 + 4 - 1 + 3 = 11$. Donc, 3 141 567 est divisible par 11. De fait, $3\,141\,567 = 11 \times 285\,597$.

On rappelle aussi que les nombres divisibles par 2 sont les nombres pairs et que les nombres divisibles par 4 sont les nombres tels que le nombre formé par leur deux derniers chiffres (à droite) est lui-même divisible par 4. En effet, soit $n = c_p c_{p-1} \ldots c_2 c_1 c_0$ (les c_i sont les chiffres de n en base 10 et l'écriture précédente désigne une juxtaposition de chiffres et non pas un produit). Puisque 100 est divisible par 4,

$$n = \sum_{k=0}^{p} c_k 10^k = c_0 + 10c_1 + 100 \sum_{k=2}^{p} 10^{k-2} c_k \equiv c_0 + 10c_1\ [4].$$

Par suite, $n \equiv 0\ [4] \Leftrightarrow c_1 c_0 \equiv 0\ [4]$.