Arithmétique

I Divisibilité dans $\mathbb{Z}$ 2
Diviseurs, multiples
Division euclidienne sur $\mathbb{Z}$

II Définition du pgcd et du ppcm 5
pgcd
ppcm

III Algorithme d'Euclide 7

IV Nombres premiers. 8
Premières propriétés
Décomposition en facteurs premiers
Conséquences de la DFP

V Caractérisation du pgcd et du ppcm (HP) 13

VI Conséquences multiples! (HP). 14
pgcd et constante multiplicative
Le lemme de Gauss et ses corollaires
Démonstration de l'unicité de la DFP

VII Bézout and Cie (HP) 16
Le théorème de Bézout
Nouvelles preuves des résultats précédents
Obtention du pgcd et des coefficients de Bézout
Encore des conséquences de Bézout

VIII Congruences (HP) 18

I. Divisibilité dans $\mathbb{Z}$

Diviseurs, multiples

1 **Définition.** Soit $a, b \in \mathbb{Z}$.
On dit que b *divise* a, et l'on note $b \mid a$, s'il existe $k \in \mathbb{Z}$ tel que $a = kb$.
On dit aussi que b est un *diviseur* de a, ou que a est un *multiple* de b.

- L'ensemble des diviseurs de $a \in \mathbb{Z}$ sera noté $\mathscr{D}(a)$.
- L'ensemble des multiples de $b \in \mathbb{Z}$ sera noté $b\mathbb{Z} = \{bq\}_{q\in\mathbb{Z}}$.
- 1 et -1 divisent tous les entiers, mais ne sont divisibles que par 1 et -1.
- Tout nombre est un multiple de 1 et de lui-même (car $n = n \times 1$) et est un diviseur de 0, car $0 = n \times 0$.
- Pour tout ce qui concerne la divisibilité, on peut se limiter à $\mathbb{N}$ puisqu'un entier a les mêmes diviseurs et les mêmes multiples que son opposé.
- La relation de divisibilité sur $\mathbb{N}^*$ est liée à l'ordre naturel de $\mathbb{N}^*$ par la relation :

$$a \mid b \implies a \leqslant b.$$

Ce résultat est faux dans $\mathbb{N}$ puisque, par exemple, $1 \mid 0$.
Ce résultat est faux dans $\mathbb{Z}$ puisque, par exemple, $3 \mid -6$.

2 **Proposition (diviseurs d'un entier).**
Soit $a \in \mathbb{N}$.

— Si $a \in \mathbb{N}^*$, alors $\mathscr{D}(a)$ est inclus dans $[\![-a, a]\!]$. Autrement dit, si $d \mid a$, alors $-a \leqslant d \leqslant a$.

— Si $a = 0$, alors $\mathscr{D}(0)$ est égal à $\mathbb{Z}$.

- **Preuve.** Si $d \mid a$, alors $a = kd$. Comme $a \neq 0$, on a $|k| \geqslant 1$. En multipliant par $|d|$, on obtient $a \geqslant |d|$.
- Si $a \in \mathbb{Z}^*$, alors $\mathscr{D}(a)$ est inclus dans $[\![-|a|, |a|]\!]$.
- Les diviseurs d'un entier *non nul* sont donc en nombre fini.
  En revanche, les diviseurs de 0 sont en nombre infini puisque tous les entiers divisent 0.
- **Multiples d'un entier.**

— Si $a \neq 0$, alors $a\mathbb{Z}$ est infini, contient 0, est symétrique par rapport à 0, stable par addition.

— Si $a = 0$, alors $a\mathbb{Z} = \{0\}$.

3 **Proposition (inclusion diviseurs/multiples).** Soit $a, b \in \mathbb{Z}$.
On a $\quad b \mid a \iff a\mathbb{Z} \subset b\mathbb{Z}$
On a $\quad b \mid a \iff \mathscr{D}(b) \subset \mathscr{D}(a)$

- Grâce à cette proposition, on obtient les égalités : $a\mathbb{Z} = (-a)\mathbb{Z}$ et $\mathscr{D}(a) = \mathscr{D}(-a)$.

4 **Proposition.** Soit $a, b, c, d, a', b', u, v \in \mathbb{Z}$.

i) **Transitivité.** Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

ii) **Égalité au signe près.** On a $\quad a \mid b$ et $b \mid a \iff |a| = |b| \iff a = \pm b$

iii) **Combinaison $\mathbb{Z}$-linéaire.** Si $d \mid a$ et $d \mid b$, alors $d \mid au + bv$.

iv) **Produit.** Si $b \mid a$ et $b' \mid a'$, alors $bb' \mid aa'$.

v) **Puissance $k \in \mathbb{N}$.** Si $b \mid a$, alors $b^k \mid a^k$.

Division euclidienne sur $\mathbb{Z}$

5 **Théorème.**
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ *non nul.*
Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $\begin{cases} a = bq + r \\ 0 \leqslant r < b. \end{cases}$

— q est appelé *quotient de la division euclidienne* de a par b,

— r est appelé *reste de la division euclidienne* de a par b.

- **Retour à l'école primaire.**
Effectuons la division euclidienne de 7342 par 31.
On a :

$$\begin{array}{rcll} 73 & = & 31 \times 2 & + \ 11 \\ 734 & = & 31 \times 20 & + \ \underbrace{114}_{31\times 3+21} \\ & = & 31 \times 23 & + \ 21 \\ 7342 & = & 31 \times 230 & + \ \underbrace{212}_{31\times 6+26} \\ & = & 31 \times 236 & + \ 26 \end{array}$$

- **Remarque.** On a $\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$ d'où $\begin{cases} \dfrac{a}{b} = q + \dfrac{r}{b} \\ 0 \leqslant \dfrac{r}{b} < 1 \end{cases}$. Ainsi, $\dfrac{a}{b} = \underbrace{q}_{\in\mathbb{Z}} + \underbrace{\gamma}_{\in[0,1[}$. D'où $q = \lfloor \frac{a}{b} \rfloor$.

- **Autre remarque importante.** Si $a \in \mathbb{N}$, alors le quotient est également dans $\mathbb{N}$.
En effet, on a $r < b$, d'où $a - bq < q$. Ainsi, $a < b(q+1)$.
Comme $a \in \mathbb{N}$ et que l'inégalité stricte précédente ne fait intervenir que des entiers, on a $1 \leqslant b(q+1)$.
Or $b \geqslant 1$ (car $b \in \mathbb{N}^*$), d'où $q + 1 \geqslant 1$. Donc $q \in \mathbb{N}$.

- **Première preuve.** Posons $E = \{k \in \mathbb{Z} \mid bk \leqslant a\}$.

Analyse. Soit $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leqslant r < b$.
Alors $0 \leqslant a - bq < b$, d'où

$$bq \leqslant a \qquad \text{et} \qquad a < b(q+1)$$

ce qui prouve d'une part que $q \in E$, et que d'autre part pour tout $k > q$, on a $a < bk$, donc $k \notin E$.
Ainsi q apparaît comme étant le maximum de E.
Et r est nécessairement égal à $a - bq$.

Synthèse. L'ensemble E est une partie de $\mathbb{Z}$ non vide et majorée.

— E est non vide.
En effet, $\begin{cases} b0 \leqslant a & \text{si } a \geqslant 0 \\ ba \leqslant a & \text{si } a \leqslant -1 \text{ (car } b \geqslant 1) \end{cases}$ donc $\begin{cases} 0 \in E & \text{si } a \geqslant 0 \\ a \in E & \text{si } a \leqslant -1 \end{cases}$.
Sans disjonction de cas : comme $b \geqslant 1$, on a $b(-|a|) \leqslant -|a| \leqslant a$, donc E contient $-|a|$.

— E est majorée. En effet, $\begin{cases} b(a+1) > a & \text{si } a \geqslant 0 \text{ (car } b \geqslant 1) \\ b0 > a & \text{si } a \leqslant -1 \end{cases}$ donc E est majorée par $\begin{cases} a+1 & \text{si } a \geqslant 0 \\ 0 & \text{si } a \leqslant -1 \end{cases}$.
Sans disjonction de cas : comme $b \geqslant 1$, on a $b(|a|+1) > b|a| \geqslant |a| \geqslant a$, donc E est majorée par $|a|+1$.

Donc E admet un plus grand élément.
Posons $q = \max E$ et $r = a - bq$.
On a alors :

— $bq \leqslant a$, car $q \in E$.

— $a < b(q+1)$, car $q + 1 \notin E$.

D'où $bq \leqslant a < b(q+1)$.
En ajoutant $-bq$, on obtient $0 \leqslant a - bq < b$.
D'où $0 \leqslant r < b$.

- **Deuxième preuve.**

Unicité. Soit $(q_1, r_1) \in \mathbb{Z}^2$ et $(q_2, r_2) \in \mathbb{Z}^2$ tels que $\begin{cases} a = bq_1 + r_1 \\ 0 \leqslant r_1 < b \end{cases}$ et $\begin{cases} a = bq_2 + r_2 \\ 0 \leqslant r_2 < b. \end{cases}$

Par différence, on a $b(q_1 - q_2) + (r_1 - r_2) = 0$.
Donc $r_1 - r_2 \in b\mathbb{Z}$.
Or $r_1 - r_2 \in]\!]-b, b[\!]$.
On en déduit que $r_1 - r_2 = 0$.
Or $b \neq 0$, donc $q_1 - q_2 = 0$.

Existence.

— **Premier cas :** $a \in \mathbb{N}$
Considérons $E = \{a - kb\}_{k\in\mathbb{N}} \cap \mathbb{N}$.
L'ensemble E est une partie de $\mathbb{N}$ non vide (car $a \in E$).
Donc E admet un plus petit élément.
Posons $r = \min E$.
Comme $r \in E$, l'entier r s'écrit $r = a - bq$ pour un certain $q \in \mathbb{N}$.
On a déjà $r \geqslant 0$. Reste à montrer que $r < b$.
Si on avait $r \geqslant b$, on aurait simultanément $\begin{cases} r - b = a - (q+1)b \\ r - b \in \mathbb{N} \end{cases}$, donc $r - b$ serait dans E.
Or $r - b < r$ (car $b \in \mathbb{N}^*$), et cela contredit la définition de r.

— **Deuxième cas :** $a \in \mathbb{Z} \setminus \mathbb{N}$
On a alors $-a \in \mathbb{N}$.
On applique alors le premier cas. Il existe $(q, r) \in \mathbb{Z}^2$ tel que

$$\begin{cases} (-a) = bq + r \\ 0 \leqslant r < b. \end{cases} \quad \text{c'est-à-dire tel que} \quad \begin{cases} a = b(-q) + (-r) \\ -b < -r \leqslant 0. \end{cases}$$

Si $r = 0$, alors le couple $(-q, 0)$ convient
Si $r \neq 0$, alors $0 < -r + b < b$ et le couple $(-q-1, -r+b)$ convient.

6 preuve

Proposition.
Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.
On a l'équivalence :

$$b \text{ divise } a \iff \text{le reste de la division euclidienne de } a \text{ par } b \text{ est nul}$$

7 sol → 20

Question.
Soit $u \in \mathbb{C}^{\mathbb{N}}$ une suite périodique, c'est-à-dire telle qu'il existe $a \in \mathbb{N}^*$ tel que $\forall n \in \mathbb{N},\ u_{n+a} = u_n$.
On note $\mathscr{P}_u$ l'ensemble des périodes de u :

$$\mathscr{P}_u = \left\{ p \in \mathbb{N}^* \mid \forall n \in \mathbb{N}, u_{n+p} = u_n \right\}$$

Justifier que $p_0 = \min \mathscr{P}_u$ est bien défini, puis montrer que $\mathscr{P}_u = p_0\mathbb{N}^*$.
On aura besoin de la remarque importante suivante sur la division euclidienne.
Si $a \in \mathbb{N}$, alors le quotient dans la division euclidienne de a par b est également dans $\mathbb{N}$.
En effet, on a $r < b$, d'où $a - bq < q$. Ainsi, $a < b(q+1)$.
Comme $a \in \mathbb{N}$ et que l'inégalité stricte précédente ne fait intervenir que des entiers, on a $1 \leqslant b(q+1)$.
Or $b \geqslant 1$ (car $b \in \mathbb{N}^*$), d'où $q + 1 \geqslant 1$. Donc $q \in \mathbb{N}$.

II. Définition du pgcd et du ppcm

pgcd

Soit $a, b \in \mathbb{Z}$. Considérons l'ensemble $\mathscr{D}(a) \cap \mathscr{D}(b)$ des diviseurs communs à a et b.

— si $a = 0$ et $b = 0$;
alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(0) \cap \mathscr{D}(0) = \mathbb{Z} \cap \mathbb{Z} = \mathbb{Z}$.

— sinon (a, b *non tous les deux nuls*) ;
alors $\mathscr{D}(a) \cap \mathscr{D}(b)$ est une partie de $\mathbb{Z}$
  — non vide (car contient 1)
  — majorée (par $|a|$ si $a \neq 0$; par $|b|$ si $b \neq 0$)

Ainsi, $\mathscr{D}(a) \cap \mathscr{D}(b)$ possède un plus grand élément, supérieur ou égal à 1.

8 **Définition.** Soit $a, b \in \mathbb{Z}$. On définit le pgcd de a et b de la façon suivante.

— Si $a = 0$ et $b = 0$,
alors le pgcd de a et b est 0.

— Sinon (a et b *non tous les deux nuls*),
le pgcd de a et b est le plus grand des diviseurs communs à a et b.

Le pgcd est noté $\text{pgcd}(a, b)$ ou encore $a \wedge b$.

- On peut retenir en particulier que
  ⋆ $\text{pgcd}(0, 0) = 0$
  ⋆ sinon, $\text{pgcd}(a, b) \geqslant 1$
- Soit $a, b \in \mathbb{Z}$. On a les **petites formules** :
$$\text{pgcd}(a, 0) = |a| \qquad \text{pgcd}(a, 1) = 1 \qquad \text{si } b \mid a, \quad \text{pgcd}(a, b) = |b|$$
- **Exemple.** On a $\mathscr{D}(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ et $\mathscr{D}(15) = \{\pm1, \pm3, \pm5, \pm15\}$.
Donc $\text{pgcd}(12, 15) = 3$.
On remarque que l'on peut se limiter aux diviseurs *positifs* pour déterminer le pgcd.
- Il n'est pas très restrictif de se **limiter à** $a, b \in \mathbb{N}$, car pour $a, b \in \mathbb{Z}$, on a $\text{pgcd}(a, b) = \text{pgcd}\big(|a|, |b|\big)$.
Montrons par exemple $\text{pgcd}(a, b) = \text{pgcd}(a, -b)$ où $a, b \in \mathbb{Z}$.
Il n'y a rien à montrer si $b = 0$. Supposons désormais $b \neq 0$.
Comme $\mathscr{D}(b) = \mathscr{D}(-b)$, on a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a) \cap \mathscr{D}(-b)$.
Donc le plus grand élément de l'intersection de gauche, qui vaut $\text{pgcd}(a, b)$ est égal au plus grand élément de l'intersection de droite, qui vaut $\text{pgcd}(a, -b)$.
Ce qui s'écrit $\text{pgcd}(a, b) = \text{pgcd}(a, -b)$.
- **Ordre naturel VERSUS divisibilité.** Par définition, on a :
Soit $a, b \in \mathbb{Z}$ non tous les deux nuls et $\delta \in \mathbb{Z}$.
$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \forall\, d \in \mathscr{D}(a) \cap \mathscr{D}(b),\ d \leqslant \delta \end{cases} \iff \delta = \text{pgcd}(a, b)$$
Il existe le même genre de résultat en remplaçant « plus petit que $\leqslant$ » par « divise $\mid$ ».
Pour l'instant, seule l'implication $\Longrightarrow$ est facile à justifier :
Soit $a, b \in \mathbb{Z}$. Soit $\delta \in \mathbb{N}$.
On a :
$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \forall\, d \in \mathscr{D}(a) \cap \mathscr{D}(b),\ d \mid \delta \end{cases} \Longrightarrow \delta = \text{pgcd}(a, b)$$
  — Les deux conditions de gauche sont invariantes par $\delta \leftrightarrow -\delta$, d'où le besoin d'imposer $\delta \in \mathbb{N}$.
  — On remarque que cette caractérisation englobe le cas où a et b sont nuls tous les deux.
  En effet, dans ce cas, la deuxième condition s'écrit $\forall\, d \in \mathbb{Z},\ d \mid \delta$. Elle implique $\delta = 0$ (prendre $d = 0$).
- pgcd = 1 Pour démontrer que deux entiers a et b sont *premiers entre eux*, c'est-à-dire $\text{pgcd}(a, b) = 1$, il suffit de prendre d un diviseur commun à a et b, et de montrer que $d \mid 1$ (ou, faute de mieux, $d \leqslant 1$).

9 **Question.** Montrer que deux entiers consécutifs sont premiers entre eux.

10 **Question.** Soit $a, b \in \mathbb{Z}$. On pose $\delta = \text{pgcd}(a,b)$.
Montrer qu'il existe $a', b' \in \mathbb{Z}$ premiers entre eux tels que $a = \delta a'$ et $b = \delta b'$.
sol → 21

ppcm

Soit $a, b \in \mathbb{Z}$. Considérons l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs à a et b.

— si $a = 0$ ou $b = 0$;
alors $a\mathbb{Z} \cap b\mathbb{Z} = \{0\}$.

— sinon (a, b *tous les deux nons nuls*) ;
alors $a\mathbb{Z} \cap b\mathbb{Z}$ est une partie de $\mathbb{Z}$.
Son intersection avec $\mathbb{N}^*$ est une partie de $\mathbb{N}$ non vide (car contient $|a||b|$).
Ainsi, $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ possède un plus petit élément, supérieur ou égal à 1.

11 **Définition.** Soit $a, b \in \mathbb{Z}$. On définit le ppcm de a et b de la façon suivante.

— Si $a = 0$ ou $b = 0$,
alors le ppcm de a et b est 0.

— Sinon (a et b *tous les deux non nuls*),
le ppcm de a et b est le plus petit des multiples *strictement positifs* communs à a et b.

Le ppcm est noté $\text{ppcm}(a,b)$ ou encore $a \vee b$.

- On peut retenir en particulier que
  ⋆ si $ab = 0$, $\text{ppcm}(a,b) = 0$
  ⋆ sinon, $a \neq 0$ et $b \neq 0$, $\text{ppcm}(a,b) \geqslant 1$
- Soit $a, b \in \mathbb{Z}$. On a les **petites formules** :

$$\text{ppcm}(a,0) = 0 \qquad \text{ppcm}(a,1) = |a| \qquad \text{si } b \mid a, \quad \text{pgcd}(a,b) = |a|$$

- **Exemple.** On a $12\mathbb{Z} \cap \mathbb{N}^* = \{12, 24, 36, 48, 60, 72, \ldots\}$ et $15\mathbb{Z} \cap \mathbb{N}^* = \{15, 30, 45, 60, 75, \ldots\}$.
  Donc $\text{ppcm}(12,15) = 60$.
- Il n'est pas très restrictif de se **limiter à** $a, b \in \mathbb{N}$, car pour $a, b \in \mathbb{Z}$, on a $\text{ppcm}(a,b) = \text{ppcm}\big(|a|,|b|\big)$.
- **Ordre naturel VERSUS divisibilité.** Par définition, on a :

  Soit $a, b \in \mathbb{Z}$ tous les deux non nuls et $\mu \in \mathbb{Z}$.

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^* \\ \forall\, m \in a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*,\ m \geqslant \mu \end{cases} \iff \mu = \text{ppcm}(a,b)$$

  Il existe le même genre de résultat en remplaçant l'ordre naturel par la relation de divisibilité.
  Pour l'instant, seule l'implication $\Longrightarrow$ est facile à justifier :

  Soit $a, b \in \mathbb{Z}$. Soit $\mu \in \mathbb{N}$.
  On a :

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ \forall\, m \in a\mathbb{Z} \cap b\mathbb{Z},\ m \in \mu\mathbb{Z} \end{cases} \Longrightarrow \mu = \text{ppcm}(a,b)$$

  — Les deux conditions de gauche sont invariantes par $\mu \leftrightarrow -\mu$, d'où le besoin d'imposer $\mu \in \mathbb{N}$.
  — On remarque que cette caractérisation englobe le cas où a et b sont nuls tous les deux.
  En effet, dans ce cas, la première condition s'écrit $\mu \in 0\mathbb{Z} \cap 0\mathbb{Z}$; d'où $\mu = 0$.

- Quand on fait la somme de deux fractions comme $\frac{3}{16} + \frac{5}{12}$, on les réduit au même dénominateur, c'est-à-dire qu'on les écrit comme des fractions dont le dénominateur est égal au ppcm des dénominateurs originaux. Comme $\text{ppcm}(16,12) = 48$, on a

$$\frac{3}{16} + \frac{5}{12} = \frac{9}{48} + \frac{20}{48} = \frac{29}{48}$$

III. Algorithme d'Euclide

12 **Le lemme des informaticiens.**
Il n'existe pas de suite strictement décroissante d'entiers naturels.
Autrement dit, une suite strictement décroissante d'entiers naturels est toujours finie.

13 **Le lemme fondamental du cours d'arithmétique de PCSI.**
Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$. On suppose $a = bq + r$, avec $q, r \in \mathbb{Z}$.
Alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$.
En particulier, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

- Dans ce lemme, l'égalité $a = bq + r$ n'est *pas* supposée être la division euclidienne de a par b.
  La seule hypothèse est $b \neq 0$.
- **Algorithme d'Euclide**
  Avec ce lemme, on a un moyen pour calculer le pgcd de a et b.
  - Si $b = 0$, alors $\text{pgcd}(a, b) = |a|$.
  - Si $b \neq 0$, alors on écrit la division euclidienne de a par b, disons $a = bq + r$, puis on recommence en remplaçant (a, b) par (b, r).
    On obtient une suite de restes strictement décroissante, qui est une suite de $\mathbb{N}$.
    D'après le lemme des informaticiens, la suite est *finie*.
    Le pgcd de a et b est alors le dernier reste non nul.
- **Exemple 1.** Soit $a = 19$ et $b = 7$. On a les divisions euclidiennes successives suivantes :

$$\begin{array}{rcrcrl} a & = & bq_1 & + & c & \text{avec } q_1 = 2 \text{ et } c = 5 \\ b & = & cq_2 & + & d & \text{avec } q_2 = 1 \text{ et } d = 2 \\ c & = & dq_3 & + & e & \text{avec } q_3 = 2 \text{ et } e = 1 \\ d & = & eq_4 & + & 0 & \text{avec } q_4 = d \end{array}$$

  On en déduit
$$a \wedge b = b \wedge c = c \wedge d = d \wedge e = e \wedge 0 = e$$
  Donc le pgcd de 19 et 7 est 1.
- **Exemple 2.** Soit $a = 782$ et $b = 221$. On a les divisions euclidiennes successives suivantes :

$$\begin{array}{rcrcrl} a & = & bq_1 & + & c & \text{avec } q_1 = 3 \text{ et } c = 119 \\ b & = & cq_2 & + & d & \text{avec } q_2 = 1 \text{ et } d = 102 \\ c & = & dq_3 & + & e & \text{avec } q_3 = 1 \text{ et } e = 17 \\ d & = & eq_4 & + & 0 & \text{avec } q_4 = 6 \end{array}$$

  On en déduit
$$a \wedge b = b \wedge c = c \wedge d = d \wedge e = e \wedge 0 = e$$
  Donc le pgcd de 782 et 221 est 17.
- **Remarque anecdotique.** Dans l'algorithme d'Euclide, si $a < b$, alors la première division donne a pour reste et l'algorithme commence donc par échanger a et b (WHY?).

IV. Nombres premiers

Premières propriétés

14 **Définition.**
On appelle *nombre premier* tout entier naturel différent de 1 n'admettant pour diviseurs *positifs* que 1 et lui-même.

- Les entiers 2, 3, 5, 7, 11, …, 65 537, …, 314 159, …, 2 718 281, … sont premiers.
- Un entier $n \geqslant 2$ est non premier si et seulement si il existe $a, b \in [\![2, n-1]\!]$, $n = ab$.
- Soit p un nombre premier et $a, b \in \mathbb{Z}$ tels que $p = ab$. Alors $a = \pm 1$ ou $b = \pm 1$.

15 **Question.** Soit $a \geqslant 3$ et $n \geqslant 2$. Montrer que $a^n - 1$ n'est pas premier.

16 preuve **Proposition.**
— Tout entier $n \geqslant 2$ admet un diviseur premier.
— Si $n \geqslant 2$ n'est pas premier, il admet un diviseur premier inférieur ou égal à $\sqrt{n}$.

- Pour savoir si un nombre n est premier, on effectue la division euclidienne de n par les nombres premiers $p \leqslant \sqrt{n}$. Si aucun ne divise n, c'est que n est premier.
- Par exemple, pour savoir si un nombre $p \leqslant 100$ est premier, il suffit de vérifier qu'il n'est ni multiple de 2, ni multiple de 3, ni multiple de 5, ni multiple de 7 (les seuls multiples de 7 à connaître au-delà de la table usuelle sont 77 et 91).
- Mettons en œuvre cette idée. C'est le crible d'Ératosthène :

	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

17 **Proposition.** L'ensemble des nombres premiers est infini.

- **Première preuve.** Montrons que $\mathscr{P}$ est infini en raisonnant par l'absurde.
  Supposons $\mathscr{P}$ fini.
  Considérons l'entier $N = \prod_{p \in \mathscr{P}} p + 1$, qui est $\geqslant 2$.
  L'entier N admet un diviseur premier $q \in \mathscr{P}$ (WHY ?).
  On a (WHY ?) $q \mid 1$.
  C'est absurde (WHY ?).
- **Deuxième preuve.** Montrons que l'ensemble des nombres premiers est non majoré.
  Soit $n \in \mathbb{N}$. Montrons qu'il existe un nombre premier $p > n$.
  Considérons l'entier $N = n! + 1$ qui est $\geqslant 2$.
  L'entier N admet un diviseur premier p.
  Si on avait $p \leqslant n$, alors p diviserait $n!$. Comme p divise N, alors p diviserait leur différence à savoir 1. Ce qui est impossible.
  Donc $p > n$.

Décomposition en facteurs premiers

18 **Théorème (Décomposition en Facteurs Premiers)**
Tout entier $\geqslant 2$ s'écrit de manière unique, à l'ordre près des facteurs, comme un produit de nombres premiers.

Soit $n \geqslant 2$.
Il existe une unique partie $\{p_1, \dots, p_r\}$ de $\mathscr{P}$, un unique r-uplet $(\alpha_1, \dots, \alpha_r) \in \mathbb{N}^*$ d'exposants strictement positifs tels que :

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Exemples. On a

$$15 = \dots \qquad 225 = \dots \qquad 84 = \dots$$

Remarques importantes.

- Les nombres premiers $p_1, \dots, p_r$ sont appelés les *facteurs premiers* de n.
- Si $\{p_1, \dots, p_s\}$ est une partie de nombres premiers *contenant tous les facteurs premiers de n*, on peut aussi écrire :
$$n = p_1^{\beta_1} \cdots p_s^{\beta_s},$$
en prenant $\beta_i = 0$ si p_i n'est pas un diviseur de n.
- Avec cette convention, $n = 1$ peut s'écrire sous cette forme en prenant tous les β_i nuls.
- Soit $a, b \in \mathbb{N}^*$. On peut écrire les décompositions de a et b en utilisant les *mêmes* nombres premiers :
$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r}$$
pourvu de prendre α_i et β_i dans $\mathbb{N}$.
- Parfois, seule l'**existence** de la DFP est utilisée.
  — Une façon de le raconter :
  Tout entier $n \geqslant 1$ est un produit de puissances de nombres premiers distincts.
  On peut englober le cas $n = 1$ en prenant des exposants nuls.
  — Une autre façon de le raconter :
  Tout entier $n \geqslant 1$ est un produit de nombres premiers non nécessairement distincts.
  On peut englober le cas $n = 1$ en convenant que 1 est un produit *vide* de nombres premiers.
- Voici une autre décomposition utile de temps en temps :
  Tout nombre $n \geqslant 1$ peut s'écrire comme produit d'une puissance de 2 et d'un nombre impair : il existe $\alpha \in \mathbb{N}$ et q impair tels que $n = 2^\alpha q$.

Deux preuves de l'existence de la DFP

- **Par récurrence forte.**

  Pour tout $n \geqslant 2$, notons $\mathscr{H}_n$ la propriété « n est un produit de nombres premiers ».

  Initialisation. 2 est un nombre premier, donc un produit de nombres premiers.

  Donc $\mathscr{H}_2$ est vraie.

  Hérédité. Soit $n \geqslant 2$.

  On suppose $\mathscr{H}_2, \mathscr{H}_3, \ldots, \mathscr{H}_n$.

  Montrons $\mathscr{H}_{n+1}$.

  Distinguons deux cas.

  — Si $n+1$ est premier, il est en particulier un produit de nombres premiers.

  — Si $n+1$ n'est pas premier, on peut trouver deux entiers a et b, appartenant à $[\![2, n]\!]$, tels que $n+1 = ab$.

  D'après l'hypothèse de récurrence, $\mathscr{H}_a$ et $\mathscr{H}_b$ sont vraies.

  Donc a et b sont produits de nombres premiers.

  On peut donc trouver des nombres premiers $p_1, \ldots, p_r$ et $q_1, \ldots, q_s$ (pas nécessairement distincts) tels que

  $$a = p_1 \cdots p_r \qquad \text{et} \qquad b = q_1 \cdots q_s$$

  En effectuant le produit, on a alors $ab = p_1 \cdots p_r q_1 \cdots q_s$, ce qui démontre que $n+1$ est un produit de nombres premiers.

  Dans les deux cas, $n+1$ est un produit de nombres premiers, ce qui démontre $\mathscr{H}_{n+1}$.

- **Par absurde-minimalité.**

  Raisonnons par l'absurde et supposons qu'il existe des entiers $\geqslant 2$ qui ne soit pas produit de nombres premiers. Notons E l'ensemble de ces nombres.

  Alors E est une partie de $\mathbb{N}$ non vide (WHY ?).

  Donc E admet un plus petit élément. Posons $m = \min E$.

  Alors m n'est pas premier (WHY ?).

  Donc il existe $a, b \in [\![2, m-1]\!]$ tel que $m = ab$.

  Par minimalité de m, les entiers a et b ne sont pas dans E (WHY ?).

  Donc a et b sont des produits de nombres premiers.

  Mais alors leur produit, à savoir m, est également un produit de nombres premiers.

  D'où la contradiction.

Conséquences de la DFP

19 **Proposition (diviseurs).** Soit $n \in \mathbb{N}^*$ dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
Alors, les diviseurs positifs de n sont les entiers d qui s'écrivent :

$$d = p_1^{\delta_1} \cdots p_r^{\delta_r} \quad \text{où } \forall\, i \in [\![1, r]\!],\ 0 \leqslant \delta_i \leqslant \alpha_i$$

- **Preuve.** Soit $d \in \mathbb{N}^*$ un diviseur de n. Écrivons $n = dc$ avec $c \in \mathbb{N}^*$.
  Les décompositions en facteurs premiers de n, d et c peuvent s'écrire

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad d = p_1^{\delta_1} \cdots p_s^{\delta_s} \text{ et } c = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$$

  où $p_{r+1}, \ldots, p_s$ des nombres premiers distincts, et distincts de $p_1, \ldots, p_r$.
  De l'égalité $n = dc$ et par unicité de la décomposition en facteurs premiers, on a :
  — pour tout $i \in [\![1, r]\!]$, $\alpha_i = \delta_i + \gamma_i$, d'où $\delta_i \in [\![0, \alpha_i]\!]$;
  — pour tout $i \in [\![r+1, s]\!]$, $0 = \delta_i + \gamma_i$, d'où, par positivité, $\delta_i = 0$ (et $\gamma_i = 0$).
  On en déduit que $d = p_1^{\delta_1} \cdots p_r^{\delta_r}$.
- **Conséquence.** Soit $a, b \in \mathbb{N}^*$ que l'on écrit

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

  où $p_1, \ldots, p_r$ sont des nombres premiers distincts et $\alpha_i, \beta_i \in \mathbb{N}$.
  On a l'équivalence :

$$a \mid b \iff \forall\, i \in [\![1, r]\!],\ \alpha_i \leqslant \beta_i$$

20 **Question.** Soit $a, b \in \mathbb{N}^*$ tel que $a^2 \mid b^2$. Montrer que $a \mid b$.

21 preuve **Proposition (pgcd et ppcm).**
Soit $a, b \in \mathbb{N}^*$ que l'on écrit

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

où $p_1, \ldots, p_r$ sont des nombres premiers distincts et $\alpha_i, \beta_i \in \mathbb{N}$.
Alors on a :

$$\operatorname{pgcd}(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)} \quad \text{et} \quad \operatorname{ppcm}(a, b) = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

- Pour déterminer le pgcd de deux entiers, nous disposons donc de deux méthodes : l'algorithme d'Euclide, et la décomposition en facteurs premiers.
- Calculons le pgcd de $a = 201387$ et $b = 3000$.
  La décomposition en facteurs premiers de b est immédiate $3000 = 2^3 \times 3 \times 5^3$.
  Le pgcd recherché est donc de la forme $2^\alpha \times 3^\beta \times 5^\gamma$, avec $\alpha \leqslant 3$, $\beta \leqslant 1$ et $\gamma \leqslant 3$.
  Comme ni 2 ni 5 ne divisent a mais que 3 le divise (la somme des chiffres est un multiple de 3), on en déduit $\operatorname{pgcd}(a, b) = 3$.

22 **Proposition.** Soit $a, b \in \mathbb{Z}$. On a l'égalité

$$\text{pgcd}(a,b) \times \text{ppcm}(a,b) = |a||b|$$

- Il suffit de prouver cette formule pour $a, b \in \mathbb{N}$.

  Cette formule est invariante par $a \leftrightarrow b$. Elle est aussi invariante par $a \leftrightarrow -a$ (et donc par $b \leftrightarrow -b$).

- **Preuve.**
  - Le cas $\big(a = 0 \text{ ou } b = 0\big)$ est facile et résulte du fait que dans ce cas $\text{ppcm}(a,b) = 0$.
  - Le cas où $a, b \in \mathbb{N}^*$ repose sur la proposition précédente et le fait que $\min(\alpha,\beta)+\max(\alpha,\beta) = \alpha+\beta$. On a

$$\begin{aligned}
\text{pgcd}(a,b) \times \text{ppcm}(a,b) &= \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)} \times \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)} \\
&= \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)} \\
&= \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i} \\
&= \prod_{i=1}^{r} p_i^{\alpha_i} \times \prod_{i=1}^{r} p_i^{\beta_i} \\
&= ab
\end{aligned}$$

V. Caractérisation du pgcd et du ppcm (HP)

23 preuve

Proposition. Soit $a, b \in \mathbb{Z}$.

— On a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$.

— Soit $\delta \in \mathbb{N}$. On a :

$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \forall\, d \in \mathscr{D}(a) \cap \mathscr{D}(b),\ d \mid \delta \end{cases} \iff \delta = \text{pgcd}(a, b)$$

- L'inclusion $\mathscr{D}(a) \cap \mathscr{D}(b) \subset \mathscr{D}(a \wedge b)$ n'est pas du tout évidente (l'autre est gratuite ou presque).
  Elle s'énonce :

  Tout diviseur de a et b est un diviseur de pgcd(a, b).

  Autrement dit, pgcd(a, b) est le plus grand élément de $\mathscr{D}(a) \cap \mathscr{D}(b)$ *pour la relation de divisibilité* sur $\mathbb{N}$.
- L'équivalence se réécrit :

$$\begin{cases} \delta \in \mathscr{D}(a) \cap \mathscr{D}(b) \\ \mathscr{D}(a) \cap \mathscr{D}(b) \subset \mathscr{D}(\delta) \end{cases} \iff \delta = \text{pgcd}(a, b)$$

  ou encore

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(\delta) \iff \delta = \text{pgcd}(a, b)$$

  Ainsi, cette équivalence montre que le pgcd est le seul entier naturel δ à vérifier $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(\delta)$.

24

Proposition. Soit $a, b \in \mathbb{Z}$.

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

— Soit $\mu \in \mathbb{N}$. On a :

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ \forall\, m \in a\mathbb{Z} \cap b\mathbb{Z},\ m \in \mu\mathbb{Z} \end{cases} \iff \mu = \text{ppcm}(a, b)$$

- L'inclusion $a\mathbb{Z} \cap b\mathbb{Z} \subset (a \vee b)\mathbb{Z}$ n'est pas du tout évidente (l'autre est gratuite ou presque).
  Elle s'énonce :

  Tout multiple de a et b est un multiple de ppcm(a, b).

  Autrement dit, ppcm(a, b) est le plus petit élément de $a\mathbb{Z} \cap b\mathbb{Z}$ *pour la relation de divisibilité* sur $\mathbb{N}$.
- L'équivalence se réécrit :

$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ a\mathbb{Z} \cap b\mathbb{Z} \subset \mu\mathbb{Z} \end{cases} \iff \mu = \text{ppcm}(a, b)$$

  ou encore

$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z} \iff \mu = \text{ppcm}(a, b)$$

  Ainsi, cette équivalence montre que le ppcm est le seul entier naturel μ à vérifier $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$.

VI. Conséquences multiples ! (HP)

pgcd et constante multiplicative

25 preuve

Proposition. Soit $a, b \in \mathbb{Z}$. Soit $k \in \mathbb{N}$. Alors

$$\text{pgcd}(ka, kb) = k\,\text{pgcd}(a, b)$$

- On en déduit facilement (WHY ?) :

  Soit $a, b, a', b' \in \mathbb{Z}$ et $d \in \mathbb{N}$ tels que $a = da'$ et $b = db'$.
  Si $\text{pgcd}(a', b') = 1$, alors $d = \text{pgcd}(a, b)$.

- On a le même type d'énoncé avec le ppcm.

Le lemme de Gauss et ses corollaires

26 preuve

Lemme de Gauss. Soit $a, b, c \in \mathbb{Z}$.

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$$

27

Lemme d'Euclide. Soit $a, b \in \mathbb{Z}$ et $p \in \mathscr{P}$.

$$p \mid ab \implies \Big(p \mid a \quad \text{ou} \quad p \mid b \Big)$$

- C'est un corollaire du lemme de Gauss, car il est équivalent à (WHY ?)

$$\begin{cases} p \mid ab \\ p \wedge a = 1 \end{cases} \implies p \mid b$$

- Au passage, on peut retenir que pour un nombre premier $p \in \mathscr{P}$, on a $p \nmid a \implies p \wedge a = 1$.
- On a la généralisation suivante.

  Soit $a_1, \ldots, a_r \in \mathbb{Z}$ et $p \in \mathscr{P}$.
  Si $p \mid a_1 \cdots a_r$, alors il existe $i \in [\![1, r]\!]$ tel que $p \mid a_i$.

Démonstration de l'unicité de la DFP

Soit $n \geqslant 2$ que l'on écrit de deux façons

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \qquad \text{et} \qquad n = q_1^{\beta_1} \cdots q_s^{\beta_s}$$

où les $p_i \in \mathscr{P}$ sont deux à deux distincts et $\alpha_i \in \mathbb{N}^*$ (idem pour les q_j et β_j).

— Montrons d'abord $\{p_1, \ldots, p_r\} \subset \{q_1, \ldots, q_s\}$.
Soit $i \in [\![1, r]\!]$.
On a $p_i \mid n$, donc $p_i \mid q_1^{\beta_1} \cdots q_s^{\beta_s}$.
Comme $p_i \in \mathscr{P}$, le résultat précédent (lequel ?) implique qu'il existe $k \in [\![1, s]\!]$ tel que $p_i \mid q_k$.
Comme $q_k \in \mathscr{P}$, on a nécessairement $p_i = 1$ ou $p_i = q_k$.
Mais $p_i \neq 1$, donc $p_i = q_k$.
Donc $p_i \in \{q_1, \ldots, q_s\}$.

— On en déduit que $r = s$. Puis, quitte à réordonner, on obtient $\forall\, i,\ p_i = q_i$.

— Montrons que $\forall\, i,\ \alpha_i = \beta_i$.
Supposons par l'absurde qu'il existe i_0 tel que $\alpha_{i_0} \neq \beta_{i_0}$.
Quitte à échanger les rôles, on peut supposer que $\alpha_{i_0} > \beta_{i_0}$.
On a

$$\left(\prod_{k \neq i_0} p_k^{\alpha_k} \right) \times p_{i_0}^{\alpha_{i_0} - \beta_{i_0}} = \left(\prod_{k \neq i_0} p_k^{\beta_k} \right)$$

Comme $\alpha_{i_0} > \beta_{i_0} \geqslant 1$, on a $p_{i_0} \mid \left(\prod_{k \neq i_0} p_k^{\beta_k} \right)$.
Comme p_{i_0} est premier, il existe $k \neq i_0$ tel que $p_{i_0} \mid p_k$, ce qui est impossible.

VII. Bézout and Cie (HP)

Le théorème de Bézout

28 preuve

Théorème de Bézout. Soit $a, b \in \mathbb{Z}$.
Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.

- La preuve peut se faire par récurrence forte, en commençant par le cas $b \in \mathbb{N}$ et en considérant $\mathscr{H}_b$ la propriété « Pour tout $a \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = \text{pgcd}(a, b)$ ».
- Attention, il n'y a pas d'unicité du couple (u, v).
  Pire, si on a un couple, on en a nécessairement une infinité.
  En effet, si (u, v) est un couple de Bézout, alors $(u - mb, v + ma)$ en est un aussi pour tout $m \in \mathbb{Z}$, car $au + bv = a(u - mb) + b(v + ma)$.
- Si a et b sont positifs, u et v ne peuvent pas être tous les deux positifs (WHY ?).
- Attention, si on a $au + bv = d$, alors cela n'implique pas que d est égal au $\text{pgcd}(a, b)$.
  Par exemple, exhiber $u, v \in \mathbb{Z}$ tels que $3u + 2v = 2023$.
- En revanche, si on a une relation du type $au + bv = d$, alors $\text{pgcd}(a, b) \mid d$ (WHY ?).

29

Proposition (Bézout dans le cas pgcd = 1**).** Soit $a, b \in \mathbb{Z}$.
Les entiers a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Nouvelles preuves des résultats précédents

- Avec une relation de Bézout, on peut redémontrer l'inclusion difficile $\mathscr{D}(a) \cap \mathscr{D}(b) \subset \mathscr{D}(a \wedge b)$.
  Allons-y. Considérons une relation de Bézout du type $au + bv = a \wedge b$.
  Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors $d \mid au + bv$. Autrement dit, $d \mid a \wedge b$, c'est-à-dire $d \in \mathscr{D}(a \wedge b)$.
- Avec une relation de Bézout, on peut redémontrer :

  Soit $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}$. On a $ka \wedge kb = k(a \wedge b)$.

  Allons-y. Montrons une double divisibilité, ce qui suffit car les deux entiers sont dans $\mathbb{N}$, on en déduit qu'ils sont égaux.
  - Considérons une relation de Bézout du type $au + bv = a \wedge b$.
    Alors $(ka)u + (kb) = k(a \wedge b)$.
    Ainsi (WHY ?), $ka \wedge kb \mid k(a \wedge b)$.
  - On a $a \wedge b \in \mathscr{D}(a) \cap \mathscr{D}(b)$.
    En multipliant par k, on a $k(a \wedge b) \in \mathscr{D}(ka) \cap \mathscr{D}(kb)$.
    D'où $k(a \wedge b) \mid ka \wedge kb$.
- Avec une relation de Bézout, on peut redémontrer :

  Soit $a, b \in \mathbb{Z}$ et $d = a \wedge b$.
  Alors il existe a', b' premiers entre eux tels que $a = da'$ et $b = db'$.
  - Si $(a, b) = (0, 0)$, alors $d = 0$. Les entiers $a' = 1$ et $b' = 1$ conviennent.
  - Si $(a, b) \neq (0, 0)$, alors $d \neq 0$.
    D'une part, comme d est un diviseur de a et b, il existe a', b' tels que $a = da'$ et $b = db'$.
    D'autre part, comme $d = \text{pgcd}(a, b)$, le théorème de Bézout fournit $u, v \in \mathbb{Z}$ tel que $au + bv = d$.
    En divisant par d, on obtient donc $a'u + b'v = 1$. Ce qui implique d'après le théorème de Bézout que $a' \wedge b' = 1$.
- Avec une relation de Bézout, on peut redémontrer le lemme de Gauss :

  Lemme de Gauss. *Soit $a, b, c \in \mathbb{Z}$.*

$$\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$$

Écrivons une relation de Bézout entre a et b, disons $au + bv = 1$.
Multiplions-la par c. On obtient $acu + bcv = c$.
Comme $a \mid bc$ (hypothèse), on en déduit que (WHY ?) $a \mid acu + bcv$, d'où $a \mid c$.

Obtention du pgcd et des coefficients de Bézout

Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$.
Supposons que les divisions euclidiennes successives soient les suivantes :

$$\begin{array}{rcrcl} a & = & bq_1 & + & c \\ b & = & cq_2 & + & d \\ c & = & dq_3 & + & e \\ d & = & eq_4 & + & 0 \end{array}$$

Le pgcd de a et b est donc e.
Comment obtenir **des** coefficients de Bézout, c'est-à-dire $u, v \in \mathbb{Z}$ tels que $au + bv = e$?
L'idée est la suivante. On part de l'avant-dernière égalité dont le reste est le pgcd e, puis on remonte.

$$\begin{array}{rcll} e & = & c - dq_3 & 3^{\text{ème}} \text{ égalité pour exprimer } e \\ & = & c - (b - cq_2)q_3 & 2^{\text{ème}} \text{ égalité pour exprimer } d \\ & = & b(-q_3) + c(1 + q_2q_3) & \text{calculs : on isole } b \text{ et } c \\ & = & b(-q_3) + (a - bq_1)(1 + q_2q_3) & 1^{\text{ère}} \text{ égalité pour exprimer } c \\ & = & a(1 + q_2q_3) + b\big(-q_1(1 + q_2q_3) - q_3\big) & \text{calculs : on isole } a \text{ et } b \end{array}$$

30 **Question.** Déterminer le pgcd de 19 et 7, ainsi que des coefficients de Bézout.

Encore des conséquences de Bézout

31 **Proposition (nombres premiers entre eux et produit).**
Soit $a, b, c \in \mathbb{Z}$. On a l'implication

$$\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \implies a \wedge bc = 1$$

- C'est même une équivalence, mais le sens $\impliedby$ est facile, donc presque sans intérêt. Démontrons-le.
  Supposons $a \wedge bc = 1$ et montrons $a \wedge b = 1$ (l'autre égalité est analogue).
  Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors a fortiori, $d \in \mathscr{D}(a) \cap \mathscr{D}(bc)$, donc $d \mid a \wedge bc = 1$.
- En français : « *Si a est premier avec deux entiers, alors a est premier avec leur produit* ».
- Évidemment, on peut généraliser :

$$\begin{cases} a \wedge b_1 = 1 \\ \quad \vdots \\ a \wedge b_r = 1 \end{cases} \implies a \wedge b_1 \cdots b_r = 1$$

- On a également le corollaire suivant :

$$a \wedge b = 1 \implies \forall \alpha, \beta \in \mathbb{N},\ a^\alpha \wedge b^\beta = 1$$

VIII. Congruences (HP)

32 **Définition.**
Soit $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
On dit que a est congru à b modulo n lorsque $n \mid a-b$.
On écrit $a \equiv b \mod n$.

- Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
  Alors, en notant r le reste de la division euclidienne de a par n, on a $a \equiv r \mod n$.
- Tout nombre $a \in \mathbb{Z}$ est congru modulo $n \in \mathbb{N}^*$ à un unique entier de $\{0, 1, \dots, n-1\}$.
  Par exemple, on a $2023 \equiv ? \mod 3$.
- L'entier a est divisible par n si et seulement si $a \equiv 0 \mod n$.

33 **Proposition.**
Soit $n \in \mathbb{N}^*$.
La relation « est congru modulo n » est réflexive, symétrique, transitive.

— Soit $a \in \mathbb{Z}$. On a $a \equiv a \mod n$.

— Soit $a, b \in \mathbb{Z}$ tel que $a \equiv b \mod n$.
Alors $b \equiv a \mod n$.

— Soit $a, b, c \in \mathbb{Z}$ tel que $a \equiv b \mod n$ et $b \equiv c \mod n$.
Alors $a \equiv c \mod n$.

34 **Proposition.**
L'addition et la multiplication de $\mathbb{Z}$ sont compatibles avec la relation de congruence modulo n :

$$\forall a, b, c, d \in \mathbb{Z}, \quad \begin{cases} a \equiv b \mod n \\ c \equiv d \mod n \end{cases} \implies \Big(a + c \equiv b + d \mod n \quad \text{et} \quad ac \equiv bd \mod n \Big)$$

35 **Proposition (critère de divisibilité de l'école primaire).**
Soit $a \in \mathbb{N}$.

— L'entier a est divisible par 2 si et seulement si son chiffre des unités est 0, 2, 4, 6 ou 8.

— L'entier a est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

— L'entier a est divisible par 4 si et seulement si le nombre obtenu en gardant ses deux derniers chiffres est divisible par 4.

— L'entier a est divisible par 5 si et seulement si son chiffre des unités vaut 0 ou 5.

— L'entier a est divisible par 8 si et seulement si le nombre obtenu en gardant ses trois derniers chiffres est divisible par 8.

— L'entier a est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

— L'entier a est divisible par 10 si et seulement si son chiffre des unités vaut 0.

— L'entier a est divisible par 11 si et seulement si la somme alternée de ses chiffres l'est.

36 **Question.**
Obtenir (à la main !) la décomposition en facteurs premiers de 14 652.

Arithmétique

preuve et éléments de correction

6

$\boxed{\Longrightarrow}$ Supposons $b \mid a$. Alors il existe $k \in \mathbb{Z}$ tel que $a = bk$.

On a alors :

$$\begin{cases} a = bk + 0 \\ 0 \leqslant 0 < b. \end{cases}$$

Il s'agit donc de la division euclidienne de a par b.

Par unicité de cette division, on en déduit que le reste est nul.

$\boxed{\Longleftarrow}$ Supposons que le reste de la division euclidienne de a par b est nul. Alors la division euclidienne s'écrit $a = bq$. Donc $b \mid a$.

7

• L'ensemble $\mathscr{P}_u$ est une partie de $\mathbb{N}$ (facile), non vide (car u est supposée périodique).
Ainsi, $\mathscr{P}_u$ admet un minimum.
Donc $p_0 = \min \mathscr{P}_u$ est bien défini.

• Montrons l'égalité $\mathscr{P}_u = p_0\mathbb{N}^*$ par double inclusion.
$\boxed{\supset}$ Commençons par cette inclusion (c'est important de commencer par celle-là).
Pour cela, montrons que $\forall\, k \in \mathbb{N}^*,\ p_0 k \in \mathscr{P}_u$.
Procédons par récurrence et pour tout $k \in \mathbb{N}^*$, notons $\mathscr{H}_k$ l'assertion « $p_0 k \in \mathscr{P}_u$ ».

Initialisation. On a $p_0 \in \mathscr{P}_u$, d'où $\mathscr{H}_1$.

Hérédité. Soit $k \in \mathbb{N}^*$ tel que $\mathscr{H}_k$.

Montrons $\mathscr{H}_{k+1}$, c'est-à-dire montrons $\forall\, n \in \mathbb{N},\ u_{n+p_0(k+1)} = u_n$.

Fixons $n \in \mathbb{N}$. On a

$$\begin{array}{rcll} u_{n+p_0(k+1)} & = & u_{(n+p_0k)+p_0} & \text{où } n + p_0k \in \mathbb{N} \\ & = & u_{n+p_0k} & \text{car } p_0 \in \mathscr{P}_u \\ & = & u_n & \text{d'après } \mathscr{H}_k \end{array}$$

D'où $\mathscr{H}_{k+1}$.

$\boxed{\subset}$ Soit $a \in \mathscr{P}_u$. Montrons que $a \in p_0\mathbb{N}^*$.
Écrivons la division euclidienne de a par p_0 (licite car $p_0 \in \mathbb{N}^*$) :
il existe $q, r \in \mathbb{Z}$ tel que $\begin{cases} a = p_0 q + r \\ 0 \leqslant r < p_0 \end{cases}$
Comme $a \in \mathbb{N}$, on en déduit, d'après la remarque importante écrite en rose à la page 3 et même à la page 4, que le quotient q est dans $\mathbb{N}$.
On veut montrer que $r = 0$.
Pour cela raisonnons par l'absurde en supposant $r \neq 0$.
On a alors $r \in \mathbb{N}^*$ et montrons que $\forall\, n \in \mathbb{N},\ u_{n+r} = u_n$; ce qui impliquera que $r \in \mathscr{P}_u$.

Soit $n \in \mathbb{N}$.

On a

$$\begin{array}{rcll} u_n & = & u_{n+a} & \\ & = & u_{n+p_0q+r} & \\ & = & u_{(n+r)+p_0q} & \\ & = & u_{n+r} & \text{facile si } q = 0, \text{ et si } q \in \mathbb{N}^*, \text{ on utilise l'inclusion } \supset \text{ qui dit que } p_0 q \in \mathscr{P}_u \end{array}$$

On a donc montré que $r \in \mathscr{P}_u$. Or $r < p_0$ (division euclidienne) et $p_0 = \min \mathscr{P}_u$. D'où la contradiction.
On a alors $r = 0$.
Puis $a = p_0 q$.
Comme $a \neq 0$, on en déduit que $q \in \mathbb{N}^*$.
Bilan : $a \in p_0\mathbb{N}^*$.

10

— Si $(a,b)=(0,0)$, alors $\delta=0$. Les entiers $a'=1$ et $b'=1$ conviennent.

— Sinon, on a en particulier $\delta \geqslant 1$.
Comme δ est un diviseur de a et b, il existe a' et b' tels que $a=\delta a'$ et $b=\delta b'$.
Comme a et b sont non tous les deux nuls, il en est de même de a' et b'.
Montrons que $\text{pgcd}(a',b')=1$ en montrant que

$$\forall\, d \in \mathscr{D}(a)\cap\mathscr{D}(b),\ d \leqslant 1$$

Soit $d \in \mathscr{D}(a')\cap\mathscr{D}(b')$.
En multipliant par δ, on obtient $d\delta \in \mathscr{D}(a)\cap\mathscr{D}(b)$. Hélas, on ne sait pas encore que $d\delta \mid a\wedge b=\delta$
Par définition du pgcd (en tant que plus grand élément de …), on obtient $d\delta \leqslant a\wedge b=\delta$.
En divisant par δ (licite car $\delta \geqslant 1$), on obtient $d \leqslant 1$.

16

— Soit $E=\{d\in[\![2,n]\!] \text{ tel que } d\mid n\}=\mathscr{D}(n)\cap[\![2,+\infty[\![$.
L'ensemble E est une partie de $\mathbb{N}$, non vide ($n\in E$), donc admet un plus petit élément.
Notons $p=\min E$.
Montrons que p est premier en montrant que $\begin{cases} p\neq 1 \\ \mathscr{D}(p)\cap\mathbb{N}=\{1,p\}\end{cases}$
Soit d un diviseur *positif* de p.
Alors par transitivité, on a $d\mid n$.
Ou bien $d=1$.
Ou bien $d\geqslant 2$ et alors $d\in E$. Par définition du minimum de E, on a nécessairement $d\geqslant p$. Et comme $d\mid p$, on a nécessairement $d=p$.

— Soit $n\geqslant 2$ non premier.
Alors il existe $a,b\in[\![2,n-1]\!]$ tel que $n=ab$.
On peut supposer que $a\leqslant b$. Ainsi, $a^2\leqslant n$.
Considérons un nombre premier p divisant a (il divise donc aussi n). Alors $p^2\leqslant n$. D'où $p\leqslant\sqrt{n}$.
On vient de montrer que n possède un diviseur premier p qui est $\leqslant\sqrt{n}$.

21

Posons $d=\prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$.
Il s'agit de montrer que d est le plus grand élément de $\mathscr{D}(a)\cap\mathscr{D}(b)$.
Tout d'abord, d est un diviseur commun à a et b.
Soit $d'\in\mathscr{D}(a)\cap\mathscr{D}(b)$. Montrons que $d'\leqslant d$.
D'après la proposition précédente, d' a une décomposition du type $d'=p_1^{\delta_1}\cdots p_r^{\delta_r}$ avec

$$\forall\, i\in[\![1,r]\!],\ \delta_i\in[\![0,\min(\alpha_i,\beta_i)]\!]$$

On a alors directement $d'\leqslant d$.

23

• Commençons par le cas $b\in\mathbb{N}$.
Par récurrence. Notons $\mathscr{H}_b$ la propriété « Pour tout $a\in\mathbb{Z}$, on a $\mathscr{D}(a)\cap\mathscr{D}(b)=\mathscr{D}(a\wedge b)$ ».

Initialisation.

Soit $a \in \mathbb{Z}$.

D'une part, on a $\mathscr{D}(a) \cap \mathscr{D}(0) = \mathscr{D}(a) \cap \mathbb{Z} = \mathscr{D}(a)$; d'autre part, $a \wedge b = a \wedge 0 = a$.

D'où $\mathscr{H}_0$.

Hérédité. Soit $b \in \mathbb{N}^*$. On suppose que $\mathscr{H}_r$ est vraie pour tout $r \in [\![0, b[\![$.

Montrons $\mathscr{H}_b$.

Soit $a \in \mathbb{Z}$. Écrivons la division euclidienne $a = bq + r$.

D'après $\mathscr{H}_r$ (la $\forall$-assertion est appliquée à b), on a $\mathscr{D}(b) \cap \mathscr{D}(r) = \mathscr{D}(b \wedge r)$.

D'après le lemme fondamental (nécessitant $b \neq 0$), on a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$ et $a \wedge b = b \wedge r$.

Il n'y a plus qu'à remplacer : on obtient $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$.

D'où $\mathscr{H}_b$.

• Traitons le cas $b \in \mathbb{Z} \setminus \mathbb{N}$.

Alors $-b \in \mathbb{N}$. Donc d'après le cas précédent, il existe $u, v \in \mathbb{Z}$ tel que $au + (-b)v = a \wedge (-b)$.

Comme $a \wedge (-b) = a \wedge b$, l'égalité précédente se réécrit $au + b(-v) = a \wedge b$.

25

Montrons que k divise $\text{pgcd}(ka, kb)$ et identifions le cofacteur.

On a $k \in \mathscr{D}(ka) \cap \mathscr{D}(kb)$. Donc $k \mid ka \wedge kb$.

Ainsi, il existe d tel que $ka \wedge kb = kd$.

Reste à montrer que $d = a \wedge b$: on procède par double divisibilité ce qui suffit car d et $a \wedge b$ sont positifs.

On a $kd \in \mathscr{D}(ka) \cap \mathscr{D}(kb)$, donc $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$, donc $d \mid a \wedge b$.

On a $a \wedge b \in \mathscr{D}(a) \cap \mathscr{D}(b)$, donc $k(a \wedge b) \in \mathscr{D}(ka) \cap \mathscr{D}(kb)$, donc $k(a \wedge b) \mid ka \wedge kb = kd$. D'où $a \wedge b \mid d$.

26

On a toujours $a \in \mathscr{D}(ac)$.

Par hypothèse, on a $a \in \mathscr{D}(bc)$.

Ainsi, $a \in \mathscr{D}(ac) \cap \mathscr{D}(bc)$.

D'où $a \in \mathscr{D}(ac \wedge bc)$. Or d'après la proposition précédente, on a $ac \wedge bc = c(a \wedge b)$. L'hypothèse $a \wedge b = 1$ fournit donc $ac \times bc = c$.

D'où $a \in \mathscr{D}(c)$.

28

• Commençons par le cas $b \in \mathbb{N}$.

Par récurrence. Notons $\mathscr{H}_b$ la propriété « Pour tout $a \in \mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tel que $au + bv = a \wedge b$ ».

Initialisation.

Soit $a \in \mathbb{Z}$.

D'une part, on a $a \times 1 + b \times 0 = a$; d'autre part, $a \wedge b = a \wedge 0 = a$.

D'où $\mathscr{H}_0$.

Hérédité. Soit $b \in \mathbb{N}^*$. On suppose que $\mathscr{H}_r$ est vraie pour tout $r \in [\![0, b[\![$.

Montrons $\mathscr{H}_b$.

Soit $a \in \mathbb{Z}$. Écrivons la division euclidienne $a = bq + r$.

D'après $\mathscr{H}_r$ (la $\forall$-assertion est appliquée à b), il existe $u, v \in \mathbb{Z}$ tel que $bu + rv = b \wedge r$.

D'après le lemme fondamental (nécessitant $b \neq 0$), on a $b \wedge r = a \wedge b$.

Il n'y a plus qu'à remplacer tous les (b, r) par (a, b) : on obtient $bu + (a - bq)v = a \wedge b$.

En réagençant, on obtient $av + b(u - qv) = a \wedge b$.

D'où $\mathscr{H}_b$.

• Traitons le cas $b \in \mathbb{Z} \setminus \mathbb{N}$.
Alors $-b \in \mathbb{N}^*$. Donc d'après le cas précédent, on a $\mathscr{D}(a) \cap \mathscr{D}(-b) = \mathscr{D}(a \wedge -b)$.
D'autre part, on a $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a) \cap \mathscr{D}(-b)$ et $a \wedge b = a \wedge -b$.
Ainsi, $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$.

Pour la deuxième partie.
$\boxed{\Longrightarrow}$ C'est un cas particulier du point précédent.
$\boxed{\Longleftarrow}$ Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors $d \mid au + bv$, donc $d \mid 1$. Donc $a \wedge b = 1$.