Chapitre 17

Arithmétique

Plan du chapitre

1 Relation de divisibilité

Définition 17.1 – Relation "divise"

On définit sur $\mathbb{Z}$ une relation binaire, notée $|$, de la manière suivante : pour tous $a, b \in \mathbb{Z}$,

$$b \mid a \iff \exists k \in \mathbb{Z} \quad a = bk$$

On dit que b divise a, ou encore que a est un multiple de b. L'ensemble des entiers qui divisent a se note :

$$\mathrm{div}(a) := \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \quad a = bk\}$$

L'ensemble $b\mathbb{Z} := \{bk \mid k \in \mathbb{Z}\}$ correspond à l'ensemble des multiples de b.

Exemple 1. $\text{div}(5) = \ldots\ldots\ldots\ldots\ldots\ldots$

Exemple 2. Quelques propriétés "immédiates" des ensembles de diviseurs :

1. $\text{div}(0) = \mathbb{Z}$
2. $\text{div}(1) = \text{div}(-1) = \{-1, 1\}$.
3. $\forall a \in \mathbb{Z} \quad -1 \in \text{div}(a) \quad \text{et} \quad 1 \in \text{div}(a)$
4. $\forall a \in \mathbb{Z} \quad \text{div}(a) = \text{div}(-a)$.
5. $\forall a \in \mathbb{Z}^* \quad \text{div}(a) \subset [\![-a, a]\!]$
6. $\forall a \in \mathbb{Z}^* \quad 0 \notin \text{div}(a)$. Par contre, $0 \in \text{div}(0)$.

La relation "divise" sur $\mathbb{Z}$ est réflexive et transitive. Toutefois, elle n'est pas symétrique ($1 \mid 2$ mais $2 \nmid 1$) ni antisymétrique, cf résultat ci-dessous :

Théorème 17.2 – "Pseudo-antisymétrie" de la division sur $\mathbb{Z}$

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

$$(a \mid b \quad \text{et} \quad b \mid a) \iff |a| = |b|$$

Dans ce cas, les entiers a et b sont dits associés.

Remarque. Ainsi "divise" définie sur $\mathbb{Z}$ n'est ni une relation d'équivalence, ni une relation d'ordre. En revanche, la relation "divise" définie sur $\mathbb{N}$ est une relation d'ordre.

Théorème 17.3

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

1. $(d \mid a \quad \text{et} \quad d \mid b) \implies \forall u, v \in \mathbb{Z} \quad d \mid (au + bv)$
2. $a \mid b \implies a \mid bc$
3. $(a \mid b \quad \text{et} \quad c \mid d) \implies ac \mid bd$
4. En particulier, $a \mid b \implies ac \mid bc$
5. Si $c \neq 0$, alors $ac \mid bc \implies a \mid b$

Démonstration. Montrons la première propriété.

Les preuves des autres assertions sont assez immédiates et laissées en exercice. □

2 Division euclidienne dans $\mathbb{Z}$

Lemme 17.4 – Semi-officiel

Soit (x_n) une suite à valeurs dans $\mathbb{Z}$. Alors (x_n) est convergente si et seulement si (x_n) est stationnaire.

Démonstration. Si (x_n) est stationnaire, elle est constante à partir d'un certain rang, donc est évidemment convergente. Réciproquement, supposons que (x_n) est convergente et montrons qu'elle est stationnaire.
Notons $\ell = \lim x_n \in \mathbb{R}$. Par la définition de la limite, si on prend $\varepsilon = 1/3$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$

$$|x_n - \ell| \leq \frac{1}{3} = \varepsilon \qquad \text{donc} \qquad x_n \in \left[\ell - \frac{1}{3}, \ell + \frac{1}{3}\right]$$

Posons $J := \left[\ell - \frac{1}{3}, \ell + \frac{1}{3}\right]$. J contient un entier car $x_N \in \mathbb{Z} \cap J$. Or, J est de longueur $\frac{2}{3}$ donc J contient au plus un entier. Ainsi, $J \cap \mathbb{Z} = \{x_N\}$. Or, pour tout $n \geq N$, on a $x_n \in \mathbb{Z} \cap J$, si bien que $x_n = x_N$. Ainsi, x_n est stationnaire (et en particulier $\ell = x_N$). □

Théorème 17.5 – Semi-officiel

Toute partie de $\mathbb{Z}$ non vide et majorée admet un maximum.

Démonstration. Soit $X \subset \mathbb{Z}$ une partie non vide et majorée. Comme $X \subset \mathbb{R}$, X admet une borne supérieure, qu'on note M. Pour conclure, il suffit de montrer que $M \in X$. Par caractérisation de la borne supérieure, il existe une suite $(x_n) \in X^{\mathbb{N}}$ telle que $x_n \to M$. En particulier, on a pour tout $n \in \mathbb{N}$, $x_n \in X \subset \mathbb{Z}$. Par le Lemme 17.4, on en déduit que (x_n) est stationnaire. Ainsi, $x_n = M$ à partir d'un certain rang. On en déduit que $M \in X$. □

Théorème 17.6 – Division euclidienne

Soit $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors il existe un ***unique*** couple $(q, r) \in \mathbb{Z}^2$ tel que

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

- q est appelé le quotient de la division euclidienne de a par b.
- r est appelé le reste de la division euclidienne de a par b.

Existence – On pose $X := b\mathbb{Z} \cap \left]-\infty, a\right]$. Comme $b \neq 0$, on montre facilement que X est non vide (par exemple si $b > 0$, alors $bk \in X$ avec $k = \left\lfloor \frac{a}{b} \right\rfloor$). De plus $X \subset \mathbb{Z}$ et X est majorée par a. Par conséquent, X admet un plus grand élément par le Théorème 17.5. On pose $M := \max X$. Comme $M \in X$, il existe $q \in \mathbb{Z}$ tel que $M = bq$ et $M \leq a$. On pose

$$r := a - bq \in \mathbb{Z}$$

Comme $bq = M \leq a$, il est clair que $r \geq 0$. Pour conclure, il suffit de montrer que $r < |b|$. Supposons par l'absurde que $r \geq |b|$. Alors

$$a = bq + r \geq bq + |b|$$

Comme $bq + |b| \in b\mathbb{Z}$, on en déduit que $bq + |b| \in X$. Or, $M = bq < bq + |b|$, ce qui contredit le fait que M majore X. Ainsi, $r < |b|$ et l'existence d'un tel couple (q, r) est vérifiée. □

Exemple 3. Calculer la division euclidienne de 539 par 17.

Exemple 4. Quelle est la division euclidienne de 17 par 539 ?

Théorème 17.7

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

Remarque. En langage Python, les instructions `a//b` et `a%b` renvoient respectivement le quotient et le reste de la division euclidienne.

3 PGCD

3.1 PGCD dans $\mathbb{N}$

Définition 17.8 – PGCD

Soit $a, b \in \mathbb{N}$ tels que $(a, b) \neq (0, 0)$. **Le** PGCD de a et b est le plus grand entier qui divise à la fois a et b. Il est noté $a \wedge b$.

L'ensemble des diviseurs communs positifs à a et b est $\text{div}(a) \cap \text{div}(b)$. Autrement dit,

$$a \wedge b := \max\left(\text{div}(a) \cap \text{div}(b)\right)$$

En particulier, par unicité du maximum, on en déduit que **le** PGCD est unique.

Justifions que cette définition a un sens. Il suffit pour cela de montrer que l'ensemble noté $X := \text{div}(a) \cap \text{div}(b) \cap \mathbb{N}$ admet un maximum.

- Il est clair que $X \subset \mathbb{Z}$ par définition de $\text{div}(a)$ et de $\text{div}(b)$.
- De plus, $1 \mid a$ et $1 \mid b$ donc $1 \in X$. En particulier, X est non vide.
- Enfin, montrons que X est majoré. Comme $(a,b) \neq (0,0)$, on a $a \neq 0$ ou $b \neq 0$. Supposons par exemple que $a \neq 0$. Alors $\text{div}(a) \subset [\![-a,a]\!]$. Comme $X \subset \text{div}(a)$, on en déduit que $X \subset [\![-a,a]\!]$. Donc X est majoré. La preuve est similaire dans le cas $b \neq 0$.

Ainsi, X est une partie non vide et majorée de $\mathbb{Z}$, donc X admet un maximum par le Théorème 17.5.

Exemple 5. Le PGCD de 12 et de 18 est 6. En effet (on omet les diviseurs négatifs) : $\text{div}(12) = \{\cdots, 1, 2, 3, 4, 6, 12\}$ et $\text{div}(18) = \{\cdots, 1, 2, 3, 6, 9, 18\}$. Ainsi, $\text{div}(12) \cap \text{div}(18) = \{\cdots, 1, 2, 3, 6\}$ et donc $12 \wedge 18 = 6$.

Remarque (Convention $0 \wedge 0 = 0$)**.** On pose par convention [1] $0 \wedge 0 = 0$. Ainsi, $a \wedge b$ a un sens pour tous $a, b \in \mathbb{N}$ (et même $a, b \in \mathbb{Z}$ comme on le verra plus loin).

Exemple 6. Soit $a, b \in \mathbb{N}$.

1. $a \wedge 1 =$ .....
2. $a \wedge 0 =$ .....
3. $a \wedge b = b \wedge a$
4. Si $(a,b) \neq (0,0)$, alors $a \wedge b \geq 1$
5. $a \wedge b = b \iff b \mid a$

Lemme 17.9

Soit $a, b \in \mathbb{N}$. Soit $q, r \in \mathbb{N}$ tels que $a = bq + r$. Alors

$$\text{div}(a) \cap \text{div}(b) = \text{div}(b) \cap \text{div}(r) \qquad \text{et} \qquad a \wedge b = b \wedge r$$

□

Théorème 17.10

Soit $a, b \in \mathbb{N}$. Les diviseurs communs à a et b sont exactement les diviseurs de $a \wedge b$:

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

ou encore : $\forall n \in \mathbb{Z} \quad (n \mid a \quad \text{et} \quad n \mid b) \iff n \mid (a \wedge b)$

De plus $a \wedge b$ est le seul entier positif qui vérifie les assertions ci-dessus.

1. Techniquement, le PGCD de 0 et 0 n'a pas de sens car $\text{div}(0) \cap \text{div}(0) = \mathbb{Z} \cap \mathbb{Z} = \mathbb{Z}$ et $\mathbb{Z}$ n'admet pas de maximum. Cependant, on peut aussi définir $a \wedge b$ comme étant le maximum de $\text{div}(a) \cap \text{div}(b) \cap \mathbb{N}$ *pour la relation d'ordre "divise" sur* $\mathbb{N}$. Dans ce cas, $\text{div}(0) \cap \text{div}(0) \cap \mathbb{N} = \mathbb{N}$ et 0 est bien le maximum de $\mathbb{N}$ car 0 majore tous les entiers naturels pour la relation "divise" (tout entier naturel divise 0). Cette nouvelle définition est cohérente avec la définition classique du PGCD de deux entiers a et b tels que $(a,b) \neq (0,0)$: dans l'exemple ci-dessus, on a $\text{div}(12) \cap \text{div}(18) \cap \mathbb{N} = \{1, 2, 3, 6\}$ et 6 est bien le plus grand élément de cet ensemble pour la relation "divise".

3.2 Algorithme d'Euclide

L'algorithme d'Euclide permet de calculer un PGCD en effectuant des divisions euclidiennes successives. Le calcul de $a \wedge b$ est immédiat si a ou b vaut 0, c'est pourquoi on suppose $a, b \in \mathbb{N}^*$ dans la méthode.

Méthode – Algorithme d'Euclide

Soit $a, b \in \mathbb{N}^*$. Quitte à échanger a et b, on suppose $b \leq a$.

1. On fait la division euclidienne de a par b : on trouve un reste r_1.
2. Puis on fait la division euclidienne de b par r_1 : on trouve un reste r_2.
3. Puis on fait la division euclidienne de r_1 par r_2 : on trouve un reste r_3, etc.
4. (...)
5. On s'arrête dès qu'on trouve un reste nul : $r_k = 0$ avec $k \geq 1$.
6. Alors, le PGCD de a et b est le *dernier reste non nul qu'on a obtenu,* à savoir :

$$r_{k-1} = a \wedge b \qquad \text{(avec la convention } r_0 = b\text{)}$$

Démonstration. En effet, on a $\mathrm{div}(r_k) = \mathrm{div}(0) = \mathbb{Z}$, donc, par le lemme 17.9

$$\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(b) \cap \mathrm{div}(r_1) = \ldots = \mathrm{div}(r_{k-1}) \cap \mathrm{div}(r_k) = \mathrm{div}(r_{k-1}) \cap \mathbb{Z} = \mathrm{div}(r_{k-1})$$

si bien que $r_{k-1} = a \wedge b$ par le Théorème 17.10. □

Exemple 7. Calculer le PGCD de 195 et 247.

L'algorithme d'Euclide est un grand classique qu'il faut savoir coder en Python !

```
def euclide(a,b):
    """Calcule le PGCD de deux entiers naturels a et b."""
    while b!=0:
        a, b = b, a%b
        # (a,b) --> (b,r1) --> (r1,r2) --> (r2,r3) --> ... --> (PGCD,0)
    return a
```

3.3 PGCD de deux entiers relatifs

Définition 17.11

Soit $a, b \in \mathbb{Z}$. On définit le PGCD de a et b par :

$$a \wedge b := |a| \wedge |b|$$

et on a de même $\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(a \wedge b)$.

Ainsi, il est suffisant de savoir calculer le PGCD de deux entiers naturels pour traiter le cas général.

3.4 Relation de Bézout / Théorème de Bézout–Bachet

Théorème 17.12 – Relation de Bézout / Théorème de Bézout–Bachet

Soit $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = a \wedge b$$

Les entiers u et v sont appelés des coefficients de Bézout de a et b.

Démonstration. Montrons d'abord la propriété pour tous $a, b \in \mathbb{N}$. Il suffit de montrer l'assertion suivante pour tout $b \in \mathbb{N}$:

$$H_b : \qquad \forall a \in \mathbb{N} \quad \exists u, v \in \mathbb{Z} \qquad au + bv = a \wedge b$$

On procède par récurrence **forte** sur $b \in \mathbb{N}$.

On a ainsi montré le théorème de Bézout-Bachet dans le cas $a, b \in \mathbb{N}$. Maintenant, montrons-le pour tous $a, b \in \mathbb{Z}$. Comme $|a|$ et $|b|$ sont des entiers positifs, par ce qui précède, il existe $u, v \in \mathbb{Z}$ tels que $|a|u + |b|v = a \wedge b$.

- Si $a \leq 0$ et $b \geq 0$, comme $|a| = -a$, on a

  $$au' + bv = a \wedge b \qquad \text{avec } u' := -u \in \mathbb{Z}$$

  On en déduit le résultat voulu.
- Les autres cas selon le signe de a et/ou b peuvent être traités par les mêmes arguments.

Finalement, la propriété est vérifiée pour tous $a, b \in \mathbb{Z}$. □

Remarque. Les coefficients u et v ne sont pas uniques : si $au+bv=1$, alors pour tout $k\in\mathbb{Z}$, on vérifie que $a(u+bk)+b(v-ak)=1$, donc $u+bk$ et $v-ak$ sont aussi des coefficients de Bézout de a et b.

Méthode – Algorithme d'Euclide étendu

On peut calculer les coefficients de Bézout avec l'algorithme d'Euclide étendu, cf exemple ci-dessous.

Exemple 8. Calculer $247\wedge 195$ puis trouver un couple $(u,v)\in\mathbb{Z}$ tel que $247u+195v=247\wedge 195$.

Méthode

Pour montrer que deux entiers *positifs* x et y sont égaux, on peut montrer que $x\mid y$ et $y\mid x$ (ce qui conclut car "divise" est une relation d'ordre sur $\mathbb{N}$).

Théorème 17.13 – Factorisation dans le PGCD

Soit $a,b\in\mathbb{Z}$ et $c\in\mathbb{N}^*$. Alors $(ca)\wedge(cb)=c(a\wedge b)$.

□

4 Entiers premiers entre eux

4.1 Définition et théorème de Bézout

Définition 17.14 – Entiers premiers entre eux

Soit $a, b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Autrement dit, a et b sont premiers entre eux si les seuls diviseurs communs à a et b sont -1 et 1.

Théorème 17.15 – Théorème de Bézout

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

$$a \wedge b = 1 \quad \Longleftrightarrow \quad \exists u, v \in \mathbb{Z} \quad au + bv = 1$$

Rappel : le théorème de Bézout-Bachet (Théorème 17.12) affirme que, pour tous $a, b, d \in \mathbb{Z}$:

$$d = a \wedge b \quad \Longrightarrow \quad \exists u, v \in \mathbb{Z} \quad au + bv = d$$

Le théorème de Bézout ci-dessus affirme donc que si $d = 1$, alors le sens réciproque est vrai également.

Démonstration. Le sens direct est une conséquence immédiate du théorème de Bézout-Bachet.

□

Exemple 9. Soit $a \in \mathbb{Z}$. Montrer que a et $a+1$ sont premiers entre eux.

Théorème 17.16 – Se ramener à des entiers premiers entre eux

Soit $a, b \in \mathbb{Z}$ tels que $(a, b) \neq (0, 0)$. Si on pose $a' = \dfrac{a}{a \wedge b} \in \mathbb{Z}$ et $b' = \dfrac{b}{a \wedge b} \in \mathbb{Z}$, alors a' et b' sont premiers entre eux.

En définitive, les entiers $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont toujours premiers entre eux.

Démonstration. On pose $d = a \wedge b$. Comme $d \mid a$ et $d \mid b$, il est clair que a' et b' sont entiers. Ensuite, par le théorème de Bézout-Bachet, il existe $u, v \in \mathbb{Z}$ tels que

$$\begin{aligned} & au + bv = d \\ \Longrightarrow\ & da'u + db'v = d \\ \Longrightarrow\ & a'u + b'v = 1 \end{aligned}$$

donc $a' \wedge b' = 1$ par le théorème de Bézout. □

Définition 17.17

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. On dit que $\dfrac{a}{b}$ est une fraction irréductible si $a \wedge b = 1$.

Toute fraction admet deux formes irréductibles, qui se déduisent l'une de l'autre en multipliant par -1 le numérateur et le dénominateur. Par exemple $-24/16$ a pour formes irréductibles $-3/2$ et $3/(-2)$. En particulier, toute fraction admet une unique écriture de la forme $\dfrac{a}{b}$ avec $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ et $a \wedge b = 1$.

Remarque. Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ (avec a,b non nécessairement premiers entre eux). Alors, par le Théorème qui précède, une forme irréductible de $\dfrac{a}{b}$ est la fraction $\dfrac{a'}{b'}$ avec $a' = \dfrac{a}{a \wedge b}$ et $b' = \dfrac{b}{a \wedge b}$.

Exemple 10. On a vu que $195 \wedge 247 = 13$ donc la forme irréductible de $\dfrac{195}{247}$ est $\dfrac{\frac{195}{13}}{\frac{247}{13}} = \dfrac{15}{19}$

4.2 Trois corollaires du théorème de Bézout

Corollaire 17.18 – Lemme de Gauss

Soit $a,b,c \in \mathbb{Z}$. Si a divise bc et si a est premier avec b, alors a divise c.

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

□

Corollaire 17.19

Soit $a_1, a_2, b \in \mathbb{Z}$. Si a_1 et a_2 sont premiers avec b, alors le produit $a_1 a_2$ est premier avec b.

Autrement dit : $\begin{cases} a_1 \wedge b = 1 \\ a_2 \wedge b = 1 \end{cases} \implies (a_1 a_2) \wedge b = 1$

□

Corollaire 17.20

Soit $a,b,c \in \mathbb{Z}$. Si a divise c, si b divise c et si a et b sont premiers entre eux alors ab divise c.

Autrement dit : $\begin{cases} a \mid c \\ b \mid c \\ a \wedge b = 1 \end{cases} \implies ab \mid c$

□

Exemple 11. Soit $n \in \mathbb{Z}$. Puisque 2 et 3 sont premiers entre eux, on a $(2 \mid n \quad \text{et} \quad 3 \mid n) \implies 6 \mid n$, et c'est même une équivalence.

4.3 PGCD de plusieurs entiers

Définition 17.21

Soit $a_1, \cdots, a_n \in \mathbb{Z}$. Le PGCD des entiers $a_1, \cdots, a_n$ est l'entier qui est leur plus grand diviseur commun. On le note

$$\bigwedge_{i=1}^{n} a_i := a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

avec la convention $0 \wedge 0 \wedge \ldots \wedge 0 = 0$.

La notation est cohérente car on peut montrer que $\wedge$ est associative :

$$a_1 \wedge (a_2 \wedge a_3) = (a_1 \wedge a_2) \wedge a_3$$

donc on peut enlever les parenthèses sans ambiguité. De plus, on peut changer l'ordre des entiers $a_1, \cdots, a_n$ du PGCD comme on le souhaite.

Exemple 12. $195 \wedge 247 \wedge 18 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

Remarque. Si $a_1 = 0$, on a en particulier :

$$a_1 \wedge a_2 \wedge \ldots \wedge a_n = 0 \wedge (a_2 \wedge \ldots \wedge a_n) = a_2 \wedge \ldots \wedge a_n$$

Sur le même principe, lorsqu'on calcule le PGCD de $a_1 \wedge \ldots \wedge a_n$, on peut exclure du calcul tous les termes a_i qui sont nuls.

Définition 17.22

Soit $a_1, \cdots, a_n \in \mathbb{Z}$. On dit que $a_1, \cdots, a_n$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_n = 1$.

On dit que $a_1, \cdots, a_n$ sont premiers entre eux deux à deux si pour tous $i, j \in [\![1, n]\!]$, si $i \neq j$, alors $a_i \wedge a_j = 1$.

Si $a_1, \cdots, a_n$ sont premiers entre eux deux à deux alors ils le sont dans leur ensemble. La réciproque est fausse :

$$2 \wedge 3 \wedge 6 = 1 \qquad \text{mais} \qquad 6 \wedge 3 = 3 \neq 1$$

On peut généraliser à n entiers la plupart des résultats vus pour deux entiers. Les plus utiles (et au programme) sont les théorèmes de Bézout et de Bézout-Bachet :

Théorème 17.23 – Bézout-Bachet généralisé

Soit $a_1, \cdots, a_n \in \mathbb{Z}$. Il existe $u_1, \cdots, u_n \in \mathbb{Z}$ tels que

$$a_1u_1 + a_2u_2 + \ldots + a_nu_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

Théorème 17.24 – Bézout généralisé

Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Les entiers $a_1, a_2, \cdots, a_n$ sont premiers entre eux dans leur ensemble si et seulement si

$$\exists u_1, u_2, \cdots, u_n \in \mathbb{Z} \qquad a_1u_1 + a_2u_2 + \ldots + a_nu_n = 1$$

Les preuves reposent entièrement sur une récurrence : l'exemple ci-dessous permet de mieux comprendre l'idée de la preuve.

Méthode

Pour calculer le PGCD de n entiers $a_1, \cdots, a_n$ ainsi que leurs coefficients de Bézout, on se ramène à des calculs successifs de PGCD et des coefficients pour deux entiers à la fois : d'abord entre a_1 et a_2, ensuite entre $a_1 \wedge a_2$ et a_3, etc. Cf exemple ci-dessous.

Exemple 13. Montrer que 5, 195 et 247 sont premiers dans leur ensemble, puis trouver $u, v, w \in \mathbb{Z}$ tels que $5u + 195v + 247w = 1$.

5 PPCM

Définition 17.25 – PPCM

Soit $a,b \in \mathbb{N}^*$. **Le** PPCM de a et b, noté $a \vee b$, est le plus petit des multiples communs *strictement positifs* à a et b.

Pour $a,b \in \mathbb{Z}^*$, on définit le PPCM de a et b par $a \vee b := |a| \vee |b|$.

L'ensemble des multiples communs strictement positifs à a et b est $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$. Autrement dit,

$$a \vee b := \min\left(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*\right)$$

En particulier, par unicité du minimum, **le** PPCM est unique. Justifions que la définition de $a \vee b$ a un sens. L'ensemble $X := a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ est une partie non vide (car $|ab| \in X$) et minorée de $\mathbb{Z}$. Ainsi, X admet un minimum.

Exemple 14. Le PPCM de 12 et de 18 est 36. En effet (on omet les multiples négatifs) : $12\mathbb{Z} = \{\cdots, 12, 24, 36, 48, 60, 72, \cdots\}$ et $18\mathbb{Z} = \{\cdots, 18, 36, 54, 72, \cdots\}$. Ainsi, $12\mathbb{Z} \cap 18\mathbb{Z} \cap \mathbb{N}^* = \{\cdots, 36, 72\}$ et donc $12 \wedge 18 = 36$.

Remarque (Convention $a \vee 0 = 0$)**.** Pour tout $a \in \mathbb{Z}$, on pose par convention[2] $a \vee 0 = 0$. Ainsi, $a \vee b$ a un sens pour tous $a,b \in \mathbb{Z}$.

Exemple 15. Soit $a,b \in \mathbb{N}$

1. $a \vee 1 = \ldots\ldots$
2. $a \vee 0 = 0$
3. $a \vee b = b \vee a$
4. Si $(a,b) \neq (0,0)$, $\quad a \vee b \geq 1$
5. $a \vee b \leq ab$
6. $a \vee b = b \iff a \mid b$

Théorème 17.26

Soit $a,b \in \mathbb{Z}$. Alors les multiples communs à a et b sont exactement les multiplies de $a \vee b$:

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

ou encore :

$$\forall n \in \mathbb{Z} \qquad (a \mid n \quad \text{et} \quad b \mid n) \iff (a \vee b) \mid n$$

2. Comme pour le PGCD, $a \vee 0$ a un sens si on modifie la définition de $a \vee b$ comme étant le minimum de $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}$ *pour la relation d'ordre "divise" de* $\mathbb{N}$. Dans ce cas, $a\mathbb{Z} \cap 0\mathbb{Z} \cap \mathbb{N} = \{0\}$ et donc 0 est bien le minimum de cet ensemble (car $0 \mid 0$). Cette nouvelle définition est cohérente avec la définition classique du PPCM de deux entiers a et b tels que $(a,b) \neq (0,0)$: dans l'exemple ci-dessus, on a $12\mathbb{Z} \cap 18\mathbb{Z} \cap \mathbb{N} = \{0, 36, 72, \cdots\} = 36\mathbb{N}$ et 36 est bien le plus petit élément de cet ensemble pour la relation "divise".

Théorème 17.27

Soit $a,b \in \mathbb{Z}$. Alors
$$(a \vee b) \times (a \wedge b) = |ab|$$

Ainsi, pour calculer $a \vee b$, on peut calculer $a \wedge b$ puis $\dfrac{|ab|}{a \wedge b}$.

Démonstration. Par définition du PGCD et du PPCM, il suffit de regarder le cas $a,b \in \mathbb{N}$. L'égalité est évidente si $a = 0$ ou $b = 0$. On suppose donc $a,b \in \mathbb{N}^*$.

- Supposons d'abord que $a \wedge b = 1$. Il suffit donc de montrer que $a \vee b = ab$. Tout d'abord, ab est un multiple commun à a et b, donc par définition, $(a \vee b) \mid ab$. Ensuite,
$$a \mid (a \vee b) \qquad \text{et} \qquad b \mid (a \vee b) \qquad \text{et} \qquad a \wedge b = 1$$
donc on en déduit (Théorème 17.20) que $ab \mid (a \vee b)$. Donc ab et $a \vee b$ sont associés. Comme ab et $a \vee b$ sont positifs, on obtient $a \vee b = ab$.

□

Exemple 16. Calculer le PPCM de 195 et de 247.

Théorème 17.28 – Factorisation dans un PPCM

Soit $a,b \in \mathbb{Z}$ et $c \in \mathbb{N}^*$. Alors $(ca) \vee (cb) = c(a \vee b)$.

Démonstration. L'égalité est évidente si $(a,b) = (0,0)$. Supposons à présent $(a,b) \neq (0,0)$. Par le Théorème précédent, on a
$$(ca) \vee (cb) = \frac{|cacb|}{(ca) \wedge (cb)} = \frac{c^2|ab|}{c(a \wedge b)} = c \times \frac{|ab|}{a \wedge b} = c(a \vee b)$$

□

6 Nombres premiers

6.1 Définitions et lemmes préliminaires

Définition 17.29

On appelle nombre premier tout entier $p \geq 2$ tel que les seuls diviseurs positifs de p sont 1 et p.
Autrement dit, p est premier si $\text{div}(p) \cap \mathbb{N} = \{1, p\}$.

Un nombre qui n'est pas premier est appelé un nombre composé.

Exemple 17. 1 n'est pas un nombre premier. 2 est l'unique nombre premier pair, tous les autres sont impairs.

Remarque. Si $n \geq 2$ est composé (i.e. non premier), alors il existe $a, b \in [\![2, n-1]\!]$ tel que $n = ab$.
En effet, $\text{div}(n) \cap \mathbb{N} \neq \{1, n\}$, donc il existe $a \in [\![2, n-1]\!]$ tel que $a \mid n$. En particulier, il existe $b \in \mathbb{Z}$ tel que $n = ab$. On montre alors facilement que, comme $1 < a < n$, on a aussi $1 < b < n$.

Lemme 17.30

Soit $a \in \mathbb{Z}$ et p un nombre premier. Ou bien $p \mid a$, ou bien $p \wedge a = 1$.

En particulier, p est premier avec tout entier qu'il ne divise pas.

Démonstration. On a $p \wedge a \in \text{div}(p) \cap \mathbb{N} = \{1, p\}$, donc deux cas sont possibles : ou bien $p \wedge a = 1$, ou bien $p \wedge a = p$. Or, on a vu (exemple 6) que $p \wedge a = p \iff p \mid a$. D'où le résultat. □

Théorème 17.31 – Lemme d'Euclide

Soit $a, b \in \mathbb{Z}$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (ou inclusif !).

Par une récurrence immédiate, si p divise un produit $a_1 \times \cdots \times a_r$, alors p divise (au moins) un des a_i.

Démonstration. Supposons que $p \mid ab$. Si $p \mid a$, alors c'est terminé. Supposons que p ne divise pas a. Par le lemme précédent, on a alors $p \wedge a = 1$. Donc par le lemme de Gauss, comme $p \mid ab$, on en déduit que $p \mid b$. □

Lemme 17.32

Soit p_1, p_2 deux nombres premiers. Si $p_1 \mid p_2$, alors $p_1 = p_2$.

Démonstration. Comme $p_1 \mid p_2$, on a $p_1 \in \text{div}(p_2) \cap \mathbb{N}$, i.e. $p_1 \in \{1, p_2\}$. Comme p_1 est premier, on a $p_1 \geq 2$, donc $p_1 = p_2$. □

6.2 Décomposition en PFP – Existence

Le but de cette section et de la suivante est d'établir la décomposition de tout entier $n \geq 2$ en produits de facteurs premiers. Dans un premier temps, on établit un résultat qui permet de déduire l'existence de cette décomposition.

Lemme 17.33

Tout entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers (non nécessairement distincts).

Démonstration. On procède par récurrence forte sur n.

- Initialisation : si $n = 2$, alors n est premier. Sa décomposition en PFP est lui-même !
- Hérédité : soit $n \in \mathbb{N}$. On suppose que tout entier $k \in [\![2, n]\!]$ peut s'écrire comme un produit de nombres premiers. Montrons qu'il en est de même pour $n+1$.
  - Si $n+1$ est premier, alors là encore, il est sa propre décomposition.
  - Si $n+1$ n'est pas premier, alors il est composé : il existe donc $a, b \in [\![2, n]\!]$ tels que $n+1 = ab$. Par hypothèse de récurrence, a et b peuvent s'écrire comme un produit de nombres premiers, donc $n+1$ aussi.
- Finalement, tout entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers.

□

Corollaire 17.34

Tout nombre entier $n \geq 2$ admet (au moins) un diviseur premier.

Soit $n \geq 2$ un entier. Par le Lemme 17.33, il existe $N \geq 1$ nombres premiers $q_1 \leq \ldots \leq q_N$ (non nécessairement distincts) tels que

$$n = q_1 \times q_2 \times \cdots \times q_N$$

Cependant, on modifier cette écriture en rassemblant les nombres premiers qui sont égaux : il existe donc $r \geq 1$ nombres premiers distincts $p_1 < p_2 < \ldots < p_r$ tels que

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r} \qquad \text{avec } \alpha_1, \alpha_2, \cdots, \alpha_r \in \mathbb{N}^*$$

C'est la forme générale de la décomposition en produits de facteurs premiers.

6.3 Décomposition en PFP – Unicité

Théorème 17.35

Soit $n \geq 2$ un entier. Il existe un entier $r \geq 1$, des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des entiers $\alpha_1, \alpha_2, \cdots, \alpha_r \geq 1$ tels que

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

De plus, les entiers $(p_i)_{1 \leq i \leq r}$ et $(\alpha_i)_{1 \leq i \leq r}$ sont uniques. Les nombres premiers $p_1, \cdots, p_r$ sont appelés les facteurs premiers de n.

Démonstration. L'existence découle du Lemme 17.33. Montrons l'unicité de cette décomposition. Supposons qu'un entier $n \geq 2$ admette les deux décompositions ci-dessous et montrons qu'elles coïncident :

$$n \quad = \quad p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \quad = \quad q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$$

donc il faut montrer que $r = s$, et que $\forall k \in [\![1, r]\!] \quad p_k = q_k \quad$ et $\alpha_k = \beta_k$.

- Soit $i \in [\![1,r]\!]$. Montrons qu'il existe $j \in [\![1,s]\!]$ tel que $p_i \mid q_j$. Comme $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$, par le lemme d'Euclide, il existe $j \in [\![1,s]\!]$ tel que $p_i \mid q_j^{\beta_j}$. Ainsi, p_i divise le produit $\underbrace{q_j \cdots q_j}_{\beta_j \text{ fois}}$. En appliquant à nouveau le lemme d'Euclide, on a $p_i \mid q_j$.
- Comme $p_i \mid q_j$ et que q_j est premier, on en déduit que (lemme 17.32) $p_i = q_j$. Ainsi, chaque p_i est égal à un q_j et un seul (car les q_j sont tous distincts). Réciproquement, chaque q_j est égal à un et un seul p_i. On en déduit que $r = s$. De plus, comme les familles (p_i) et (q_j) sont strictement croissantes, on a nécessairement $p_1 = q_1$, $p_2 = q_2$, $\cdots$, $p_r = q_r$.
- Par ce qui précède, on a donc

$$(n \quad =) \quad p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad = \quad p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

Supposons par l'absurde que $\alpha_1 \neq \beta_1$, par exemple $\alpha_1 < \beta_1$. Alors en divisant l'égalité par $p_1^{\alpha_1}$, on trouve que :

$$\begin{aligned} p_2^{\alpha_2} \dots p_r^{\alpha_r} &= p_1^{\beta_1 - \alpha_1} \times \left(p_2^{\beta_2} \dots p_r^{\beta_r} \right) \\ &= p_1 \times \underbrace{\left(p_1^{\beta_1 - \alpha_1 - 1} p_2^{\beta_2} \dots p_r^{\beta_r} \right)}_{\in \mathbb{Z}} \end{aligned}$$

Donc p_1 divise $p_2^{\alpha_2} \dots p_r^{\alpha_r}$. Comme à la première étape de la preuve, cela entraine qu'il existe $j \geq 2$ tel que $p_1 \mid p_j$. Comme p_1, p_j sont premiers, on a $p_1 = p_j$. Or, c'est impossible puisque $j \geq 2$ et que les nombres $p_1, \cdots, p_r$ sont distincts. Contradiction. Donc $\alpha_1 = \beta_1$. En divisant l'égalité par $p_1^{\alpha_1}$, on obtient donc :

$$p_2^{\alpha_2} \dots p_r^{\alpha_r} = p_2^{\beta_2} \dots p_r^{\beta_r}$$

et on montre de même que $\alpha_2 = \beta_2$, etc. En réitérant le processus, on en conclut que $(\alpha_1, \cdots, \alpha_r) = (\beta_1, \cdots, \beta_r)$.

Finalement, $r = s$ et $\forall k \in [\![1,r]\!] \quad p_k = q_k$ et $\alpha_k = \beta_k$. Les deux décompositions sont donc bien égales. □

Exemple 18. Décomposer 1400 en produits de facteurs premiers.

Corollaire 17.36

Il existe une infinité de nombres premiers.

Démonstration. Supposons par l'absurde qu'il n'existe qu'un nombre fini n de nombres premiers distincts, notés $p_1, \cdots, p_n$. Notons que $n \geq 1$ car (par exemple) 2 est premier. On pose

$$N := p_1 p_2 \cdots p_n + 1$$

Comme $n \geq 1$, on a $N \geq 2$, donc N admet un diviseur premier qui est forcément parmi $p_1, \cdots, p_n$. Supposons que ce diviseur soit p_1 (la preuve sera identique dans les autres cas). Ainsi, $p_1 \mid N$ et par ailleurs $p_1 \mid p_1 p_2 \cdots p_n$. Donc p_1 divise $N - p_1 p_2 \cdots p_n$, c'est-à-dire 1. D'où $p_1 \in \{-1, 1\}$, ce qui est absurde. Ainsi, l'ensemble des nombres premiers est infini. □

6.4 Valuation p-adique

Définition 17.37

Soit p un nombre premier. Pour tout entier $n \in \mathbb{N}^*$, on appelle valuation p-adique de n, un nombre noté $v_p(n)$, défini comme le plus grand entier $k \in \mathbb{N}$ tel que

$$p^k \mid n \qquad \text{et} \qquad p^{k+1} \nmid n$$

Autrement dit

$$v_p(n) := \max\left\{k \in \mathbb{N} \quad | \quad p^k \mid n\right\}$$

Exemple 19.

- $v_2(8) = 3$ car $2^3 \mid 8$ mais $2^4 \nmid 8$.
- $v_5(100) = \ldots$
- $v_3(4) = \ldots$
- Si p est un nombre premier et $\alpha \in \mathbb{N}$, $v_p(p^\alpha) = \ldots$

Définition 17.38 – Décomposition généralisée

Soit $n \in \mathbb{N}^*$. Soit $\mathbb{P}$ l'ensemble des nombres premiers. Pour tout $p \in \mathbb{P}$, il existe un unique $\alpha_p \in \mathbb{N}$ tel que

$$n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$$

et dans ce cas, $\alpha_p = v_p(n) \in \mathbb{N}$.

La décomposition généralisée est donc un produit infini (car $\mathbb{P}$ est infini), mais en pratique seul un nombre fini de termes du produit sont différents de 1. Cette décomposition est là encore unique, et on peut "lire" les valuations de n directement.

Exemple 20. La décomposition généralisée de 12 est

$$12 = 2^2 \times 3^1 \times 5^0 \times 7^0 \times \ldots$$

et donc $v_2(12) = 2$, $v_3(12) = 1$, $v_p(12) = 0$ pour tout nombre premier $p \geq 5$.

Théorème 17.39

Soit $a, b \in \mathbb{N}^*$.

1. $a \mid b$ si et seulement si $\forall p \in \mathbb{P} \quad v_p(a) \leq v_p(b)$.
2. $a = b$ si et seulement si $\forall p \in \mathbb{P} \quad v_p(a) = v_p(b)$.

De plus, pour tout nombre premier p,

3. $v_p(ab) = v_p(a) + v_p(b)$
4. $v_p(a \wedge b) = \min(v_p(a), v_p(b))$
5. $v_p(a \vee b) = \max(v_p(a), v_p(b))$

Démonstration. On ne prouve que les points 3 et 4. Pour tout $p \in \mathbb{P}$, on pose $\alpha_p = v_p(a)$ et $\beta_p = v_p(b)$. Par la décomposition généralisée,

$$a = \prod_{p \in \mathbb{P}} p^{\alpha_p} \qquad b = \prod_{p \in \mathbb{P}} p^{\beta_p}$$

donc par associativité du produit :

$$ab = \left(\prod_{p\in\mathbb{P}} p^{\alpha_p}\right)\left(\prod_{p\in\mathbb{P}} p^{\beta_p}\right) = \prod_{p\in\mathbb{P}} p^{\alpha_p+\beta_p}$$

On en déduit que pour tout $p \in \mathbb{P}$, $v_p(ab) = \alpha_p + \beta_p = v_p(a) + v_p(b)$. Donc l'assertion 3 est vraie.
Maintenant, montrons 4. Pour tout $p \in \mathbb{P}$, on pose $\gamma_p := \min(\alpha_p, \beta_p)$ et

$$d := \prod_{p\in\mathbb{P}} p^{\gamma_p}$$

on va montrer que $d = a \wedge b$. Comme $\forall p \in \mathbb{P} \quad \gamma_p \leq \alpha_p$, on a $d \mid a$. De même $d \mid b$. Ainsi, $d \mid (a \wedge b)$. En particulier, pour tout $p \in \mathbb{P}$, on a $\gamma_p \leq v_p(a \wedge b)$. Supposons par l'absurde qu'il existe $q \in \mathbb{P}$ tel que $\gamma_q < v_q(a \wedge b)$. Quitte à échanger a et b, on peut par exemple supposer que $\gamma_q = \alpha_q$. Comme $\alpha_q + 1 \leq v_q(a \wedge b)$, on en déduit que $q^{\alpha_q+1} \mid (a \wedge b)$, donc que $q^{\alpha_q+1} \mid a$. Ainsi,

$$v_q\left(q^{\alpha_q+1}\right) \leq v_q(a) \qquad \text{d'où} \qquad \alpha_q + 1 \leq \alpha_q$$

Contradiction. Donc pour tout $p \in \mathbb{P}$, on a $v_p(d) = v_p(a \wedge b)$. On en déduit que $d = a \wedge b$. □

Méthode

On peut calculer un PGCD et un PPCM à partir de la décomposition en produits de facteurs premiers, cf exemple ci-dessous.

Exemple 21. Calculer le PGCD et le PPCM de 360 et 315.

Exemple 22. Combien 1400 a-t-il de diviseurs positifs ? Et de diviseurs de signe quelconque ?

6.5 Vérifier rapidement si un nombre est premier

Soit un entier $n \geq 2$ dont on veut savoir s'il est premier.

- Méthode longue : vérifier si pour tout $k \in [\![2, n-1]\!]$ on a bien $k \nmid n$, donc de vérifier que $\text{div}(n) \cap \mathbb{N} = \{1, n\}$.
- Méthode moins longue : vérifier si pour tout nombre premier $p \leq n-1$, on a bien $p \nmid n$.
- Méthode optimale : vérifier si pour tout nombre premier $p \leq \sqrt{n}$, on a bien $p \nmid n$.

Exemple 23. Est-ce que 89 est un nombre premier ?

7 Congruences

7.1 Définition et relation d'équivalence

Définition 17.40 – Congruences

Soit un entier $n \geq 2$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n si $n \mid (a-b)$. On note alors

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

Certains auteurs notent parfois $a \equiv b \pmod{n}$. Voici plusieurs caractérisations de cette définition :

$$\begin{aligned} a \equiv b \ [n] &\iff \exists k \in \mathbb{Z} \quad a - b = kn \\ &\iff \exists k \in \mathbb{Z} \quad a = b + kn \end{aligned}$$

Exemple 24.
- $a \equiv 0 \ [n]$ si et seulement si a est divisible par n. Par exemple $a \equiv 0 \ [2]$ ssi a est pair.
- $10 \equiv 3 \equiv -4 \ [7]$.
- Résoudre l'équation $x \equiv 2 \ [7]$.

Théorème 17.41 – Relation "congru modulo n"

Soit $a, b \in \mathbb{Z}$ et un entier $n \geq 2$.

1. La relation "congru modulo n" est une relation d'équivalence :
   - $a \equiv a \ [n]$
   - si $a \equiv b \ [n]$, alors $b \equiv a \ [n]$.
   - si $a \equiv b \ [n]$ et $b \equiv c \ [n]$, alors $a \equiv c \ [n]$.
2. $a \equiv b \ [n]$ si et seulement si a et b ont le même reste quand on réalise leur division euclidienne par n.
3. Il y a donc n classes d'équivalence pour la relation "congru modulo n" :

$$\overline{0}, \overline{1}, \cdots, \overline{n-1}$$

(Une classe pour chaque reste possible)

7.2 Opérations et congruences

Théorème 17.42 – Opérations sur les congruences

Soit $a,b,c,d \in \mathbb{Z}$ et un entier $n \geq 2$.

1. On peut additionner, soustraire ou multiplier les congruences :

$$\begin{cases} a \equiv b \ [n] \\ c \equiv d \ [n] \end{cases} \implies \begin{cases} a+c \equiv b+d \ [n] \\ a-c \equiv b-d \ [n] \\ ac \equiv bd \ [n] \end{cases}$$

2. On peut ajouter / retrancher autant de fois n que l'on souhaite dans une congruence :

$$a \equiv b \ [n] \quad \implies \quad \forall k \in \mathbb{Z} \quad a+kn \equiv b \ [n]$$

La première assertion entraine notamment (par somme, différence ou produit de $a \equiv b \ [n]$ avec lui-même) :

$$a \equiv b \ [n] \quad \implies \quad \begin{cases} \forall k \in \mathbb{Z} & ka \equiv kb \ [n] \\ \forall k \in \mathbb{N} & a^k \equiv b^k \ [n] \end{cases} \quad \text{avec la convention } 0^0 = 1$$

Démonstration. On ne montre que le premier point, pour la somme et le produit :

$$\begin{aligned} \begin{cases} a \equiv b \ [n] \\ c \equiv d \ [n] \end{cases} &\implies \begin{cases} n \mid a-b \\ n \mid c-d \end{cases} \\ &\implies \begin{cases} n \mid (a-b)+(c-d) \\ n \mid (a-b) \times d + (c-d) \times a \end{cases} \\ &\implies \begin{cases} n \mid (a+c)-(b+d) \\ n \mid ac-bd \end{cases} \\ &\implies \begin{cases} (a+c) \equiv (b+d) \ [n] \\ ac \equiv bd \ [n] \end{cases} \end{aligned}$$

□

Exemple 25. Montrer que $9^{2025} \equiv -1 \ [10]$.

Il est souvent utile de "simplifier" une congruence, càd trouver un entier r "simple" tel que $a \equiv r \ [n]$.

Méthode

Lorsque $a \wedge n = 1$, on peut simplifier la congruence "$a^m \equiv \ldots \ [n]$" de la manière suivante :

1. Calculer à quoi est congru a, a^2, a^3, etc. jusqu'à trouver un entier $k \geq 1$ tel que $a^k \equiv 1 \ [n]$ ou $a^k \equiv -1 \ [n]$.
2. Par la division euclidienne $m = qk + r$ avec $0 \leq r < k$, déduire que $a^m \equiv (a^k)^q a^r \equiv (\pm 1)^q a^r \ [n]$ et simplifier cette dernière congruence.

Exemple 26. Déterminer le reste de la division euclidienne de 7^{2019} par 22.

Remarque. Si $a \wedge n \neq 1$, alors pour tout $k \geq 1$, on a $a^k \not\equiv \pm 1 \ [n]$, et cette méthode échoue. Mais les valeurs "simples" qu'on trouve forment un cycle, par exemple, $4 \wedge 14 \neq 1$ et on trouve un cycle, comme le montre le tableau de congruence suivant :

k	1	2	3	4	5	6	$\cdots$
$4^k \equiv \ldots \ [14]$							$\cdots$

7.3 Congruence et "division"

Attention la division dans une congruence n'est pas autorisée en général : $9 \equiv 3 \ [6]$ mais $\frac{9}{3} \not\equiv \frac{3}{3} \ [6]$. Par contre, si a, b, n sont tous divisibles par un entier $d \in \mathbb{N}^*$, alors la division est possible :

Théorème 17.43 – Division – crochet inclus

Soit $x, y \in \mathbb{Z}$, $a \in \mathbb{Z}^*$ et $n \geq 2$ un entier. On a $ax \equiv ay \ [an] \iff x \equiv y \ [n]$.

Par exemple $9 \equiv 3 \ [6] \implies 3 \equiv 1 \ [2]$.

Cette division est possible seulement si le facteur a est déjà présent dans le crochet et dans les deux membres, ce qui est assez restrictif. Par exemple, si on souhaite résoudre $5x \equiv 2 \ [7]$, on ne peut pas "diviser par 5" cette équation. Il faut donc faire autrement. Plutôt que de diviser par 5, on va multiplier... par l'inverse de 5 ! Mais un inverse modulo n, cf ci-dessous.

Définition 17.44 – Inverse modulo n

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$. On dit que a admet un inverse modulo n s'il existe $c \in \mathbb{Z}$ tel que $ac \equiv 1 \ [n]$.
Un tel entier c est appelé **un** inverse de a modulo n.

Il n'y a pas unicité de l'inverse : si $ac \equiv 1 \ [n]$, alors pour tout $k \in \mathbb{Z}$ $\quad a(c+kn) \equiv 1 \ [n]$

Théorème 17.45 – Passage à l'inverse dans une congruence

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$. Alors a admet un inverse modulo n si et seulement si $a \wedge n = 1$.
Dans ce cas, si on note c cet inverse, alors

$$\forall x, b \in \mathbb{Z} \qquad ax \equiv b \ [n] \iff x \equiv bc \ [n]$$

Méthode – Trouver un inverse modulo n

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$ tels que $a \wedge n = 1$. Pour trouver un inverse de a modulo n, on peut :

- Chercher un inverse "évident"
- Calculer un couple de coefficients de Bézout (u, v) tels que $\quad au + nv = 1$. Dans ce cas, $au \equiv 1 \ [n]$, donc u est un inverse de a modulo n.

Exercice 1. Résoudre (dans $\mathbb{Z}$) l'équation $5x \equiv 2 \ [7]$.

Corollaire 17.46 – Division – crochet exclu

Soit $x, y, a \in \mathbb{Z}$ et $n \geq 2$ un entier. Si $\boxed{a \wedge n = 1}$, alors $\quad ax \equiv ay \ [n] \iff x \equiv y \ [n]$.

Démonstration. Comme $a \wedge n = 1$, l'entier a admet un inverse modulo n, qu'on note c. On a donc $ac \equiv 1 \ [n]$, donc en particulier $c \neq 0$. Alors

$$ax \equiv ay \ [n] \iff cax \equiv cay \ [n] \iff x \equiv y \ [n] \qquad \text{car } ca \equiv 1 \ [n]$$

□

Méthode – Résoudre une équation sur les congruences

Étant donné $A, B, N \in \mathbb{Z}$, on cherche à résoudre $Ax \equiv B \ [n]$ d'inconnue $x \in \mathbb{Z}$.

1. On détermine $d := A \wedge N$.
   - Si d ne divise pas B, il n'y a pas de solution. En effet, s'il existait une solution $x \in \mathbb{Z}$, alors il existerait $k \in \mathbb{Z}$ tel que $Ax = B + kN$. Or, $d \mid A$ et $d \mid N$ donc $d \mid (Ax - kN)$, càd $d \mid B$. Contradiction.
2. Si $d \mid B$, on pose
$$a := \frac{A}{d} \in \mathbb{Z} \qquad b := \frac{B}{d} \in \mathbb{Z} \qquad n := \frac{N}{d} \in \mathbb{Z}$$
et on divise la congruence (crochet inclus) par d. Ainsi : $Ax \equiv B \ [N] \iff ax \equiv b \ [n]$.
3. Par construction de a et n, nécessairement $a \wedge n = 1$. On détermine un inverse de a modulo n : on le notera (ici) c.
$$ax \equiv b \ [n] \iff x \equiv cb \ [n] \iff \exists k \in \mathbb{Z} \quad x = cb + kn$$
donc $\mathcal{S} = \{cb + kn \mid k \in \mathbb{Z}\}$.

Exercice 2. Soit $m \in \mathbb{Z}$. Résoudre l'équation $15x \equiv m \ [21]$ d'inconnue $x \in \mathbb{Z}$.

7.4 Petit théorème de Fermat

Lemme 17.47

Soit p un nombre premier.
$$\forall a, b \in \mathbb{Z} \qquad (a+b)^p \equiv a^p + b^p \ [p]$$

Démonstration. Par la formule du binôme, on a
$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$
On va montrer que pour tout $k \in [\![1, p-1]\!]$, on a $p \mid \binom{p}{k}$. Si on prouve cela, alors on aura
$$p \left| \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} \right. \qquad \text{et donc} \quad (a+b)^p \equiv a^p + b^p \ [p]$$

□

Théorème 17.48 – Petit théorème de Fermat

Si p est un nombre premier et $a \in \mathbb{Z}$, alors

$$a^p \equiv a \ [p]$$

De plus, si $a \wedge p = 1$, alors

$$a^{p-1} \equiv 1 \ [p]$$

Démonstration. Si $a^p \equiv a \ [p]$ et $a \wedge p = 1$, alors on peut diviser par a dans la congruence (crochet exclu) et en déduire que $a^{p-1} \equiv 1 \ [p]$. Il suffit donc de montrer que $a^p \equiv a \ [p]$.

On fait d'abord la preuve pour $a \in \mathbb{N}$, par récurrence sur a.

- Si $a = 0$, alors $0^p = 0$ donc $0^p \equiv 0 \ [p]$. La propriété est vraie au rang 0.
- Supposons que $a^p \equiv a \ [p]$ pour un $a \in \mathbb{N}$, et montrons que $(a+1)^p \equiv a+1 \ [p]$. Par le lemme ci-dessus, comme p est premier,

$$\begin{aligned} (a+1)^p &\equiv a^p + 1^p \ [p] \\ &\equiv a + 1^p \ [p] \qquad \text{par hypothèse de récurrence} \\ &\equiv a+1 \ [p] \end{aligned}$$

  Donc la propriété est vraie au rang $a+1$.
- Finalement, pour tout $a \in \mathbb{N}$, $a^p \equiv a \ [p]$.

Faisons enfin la preuve pour $a \in \mathbb{Z} \setminus \mathbb{N}$. Comme $p \geq 2$, il existe $k \in \mathbb{N}$ (assez grand) tel que $a + kp \geq 0$. On pose alors $a' := a + kp$. Par construction, $a' \equiv a \ [p]$ et donc $(a')^p \equiv a^p \ [p]$. De plus, comme $a' \geq 0$, on a montré que $(a')^p \equiv a' \ [p]$. Ainsi, $\quad a^p \equiv (a')^p \equiv a' \equiv a \ [p]$. □

Exemple 27. Quel est le reste de la division euclidienne de 14^{2024} par 11 ?

8 Équations diophantiennes

Définition 17.49 – Équation diophantienne

On appelle équation diophantienne une équation dont la ou les inconnues sont des entiers relatifs.

Exemple 28. L'équation $2x+7y=3$ d'inconnues $x,y\in\mathbb{Z}$.
L'équation $x^2+y^2=z^2$ d'inconnues $x,y,z\in\mathbb{Z}$.
La résolution de ces équations est souvent non triviale. Néanmoins, il y a un cas particulier d'équation qu'il faut savoir traiter sans indication : les équations diophantiennes du premier ordre à deux inconnues :

Méthode – Résolution d'une équation diophantienne du type $Ax+By=C$

Soit $A,B,C\in\mathbb{Z}$. On cherche à résoudre l'équation $Ax+By=C$ d'inconnues $x,y\in\mathbb{Z}$.

1. On détermine $d=A\wedge B$.
   - Si $d\nmid C$, alors il n'y a pas de solution. En effet, on a toujours $d\mid(Ax+By)$.
2. Si $d\mid C$, on pose $a=\dfrac{A}{d}$, $b=\dfrac{B}{d}$, $c=\dfrac{C}{d}$, et on résoud l'équation équivalente $ax+by=c$.
3. On cherche une solution particulière (x_0,y_0). Ou bien on trouve une solution évidente, ou bien :
   (a) Par construction, $a\wedge b=1$. On détermine $u,v\in\mathbb{Z}$ tels que $au+bv=1$
   (b) En multipliant par c cette équation, on obtient une solution particulière $(x_0,y_0)=(uc,vc)$.
4. On écrit $\begin{cases}ax+by=c\\ax_0+by_0=c\end{cases}$ et donc par soustraction $a(x-x_0)+b(y-y_0)=0$. On résout cette équation de manière spécifique, par lemme de Gauss et substitution, cf exemple ci-dessous.

Exemple 29. Résoudre $10x+6y=8$.

Liens entre équations diophantiennes et équations de congruences. On remarquera que les méthodes pour résoudre $ax \equiv b \ [n]$ et les équations diophantiennes se ressemblent beaucoup. Mais les notations sont trompeuses. L'équation diophantienne associée à $ax \equiv b \ [n]$ est en fait $ax+ny=b$. En voici une explication :

$$\begin{aligned} & ax \equiv b \ [n] \\ \iff & \exists k \in \mathbb{Z} \quad ax = b+nk \\ \iff & \exists k \in \mathbb{Z} \quad ax - nk = b \\ \iff & \exists y \in \mathbb{Z} \quad ax + ny = b \qquad (\text{en posant } y = -k) \end{aligned}$$

Dit autrement, x est solution de $ax \equiv b \ [n]$ si et seulement s'il existe $y \in \mathbb{Z}$ tel que (x,y) soit solution de $ax+ny=b$. On comprend aussi pourquoi, dans les deux cas, il faut que $a \wedge n$ divise b pour qu'il y ait une solution.

9 Méthodes pour les exercices

Méthode

Pour montrer que deux entiers a et b sont premiers entre eux, on peut :

- Poser $d = a \wedge b$ et montrer que d divise 1.
- Utiliser le théorème de Bézout.
- Supposer par l'absurde que $a \wedge b \neq 1$. Alors il existe un nombre premier p qui divise $a \wedge b$, donc qui divise a et b. En déduire une contradiction.

Méthode

Pour calculer le PGCD de deux entiers a et b, on peut :

- Appliquer l'algorithme d'Euclide.
- Si on connait $a \vee b$, utiliser la formule $(a \wedge b)(a \vee b) = \ldots$
- Décomposer a et b en produits de facteurs premiers.
- Si on estime que a et b sont premiers entre eux, on peut utiliser la méthode précédente.

Cette méthode s'adapte également au calcul de PPCM.

Il faut connaitre les méthodes pour résoudre une équation de congruence (forme $ax \equiv b \ [n]$), une équation diophantienne (forme $ax + by = c$) sans les confondre !