Chapitre 18

Arithmétique

Plan du chapitre

1 Relation de divisibilité

Définition 18.1 – Relation "divise"

On définit sur $\mathbb{Z}$ une relation binaire, notée $\mid$, 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. $\mathrm{div}(5) = \ldots\ldots\ldots\ldots\ldots\ldots$

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

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

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 ci-dessous). Ce n'est donc ni une relation d'équivalence, ni une relation d'ordre.

Théorème 18.2 – "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. En revanche, la relation "divise" définie sur $\mathbb{N}$ est une relation d'ordre.

Théorème 18.3

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. Si $c \neq 0$, alors $a \mid b \iff ac \mid bc$ (division par c non nul de part et d'autre du "divise")

Démonstration. Montrons la première propriété.

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

2 Division euclidienne dans $\mathbb{Z}$

Lemme 18.4

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 18.5

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

Toute partie non vide et minorée de $\boxed{\mathbb{Z}}$ admet un minimum.

Démonstration. On ne prouve que la première assertion. 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) à valeurs dans X telle que $x_n \to M$. En particulier, (x_n) est à valeurs dans $\mathbb{Z}$. Par le Lemme 18.4, 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 18.6 – 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.

Démonstration.

Existence – On pose $X := b\mathbb{Z} \cap]-\infty, a]$. Comme $b \neq 0$, on montre facilement que X est non vide. De plus $X \subset \mathbb{Z}$ et X est majorée par a. Par conséquent, X admet un plus grand élément par le Théorème 18.5. 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.

□

Remarque. On peut montrer que si $b > 0$, le quotient q de la division euclidienne est donné par $q = \left\lfloor \frac{a}{b} \right\rfloor$.

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

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

Théorème 18.7

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 de a par b.

3 PGCD

3.1 PGCD dans $\mathbb{N}$

Soit $a, b \in \mathbb{N}$ tels que $(a,b) \neq (0,0)$. On souhaite définir le PGCD de a et b comme étant le plus grand diviseur commun à a et à b. Or, l'ensemble des diviseurs communs à a et b est l'ensemble

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

Le PGCD de a et b sera le maximum de X. Mais il faut s'assurer que ce maximum existe !

- Puisque $\text{div}(a)$ et $\text{div}(b)$ sont des parties de $\mathbb{Z}$, il en va de même pour X.
- De plus, $1 \mid a$ et $1 \mid b$ donc $1 \in X$. On en déduit que 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 (par a). 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 18.5. On en déduit que la définition suivante a un sens.

Définition 18.8 – PGCD

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

On notera que, par unicité du maximum, **le** PGCD est unique.

Exemple 5. Le PGCD de 12 et de 18 est 6. En effet (on omet les diviseurs négatifs) :

$$\text{div}(12) = \{\cdots, 1, 2, 3, 4, 6, 12\} \qquad \text{div}(18) = \{\cdots, 1, 2, 3, 6, 9, 18\}$$

$$\text{Ainsi,} \quad \text{div}(12) \cap \text{div}(18) = \{\cdots, 1, 2, 3, 6\}$$

si bien que $12 \wedge 18 = 6$.

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. $a \wedge b = b \iff b \mid a$

Théorème 18.9

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

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

Démonstration.

□

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 $X = \text{div}(a) \cap \text{div}(b) \cap \mathbb{N}$ *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 $\mathbb{N}$ pour "divise" 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".

Théorème 18.10

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

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

ou encore, de manière équivalente :

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

De plus $a \wedge b$ est le seul entier positif qui vérifie l'une des assertions ci-dessus.

Démonstration. On va montrer l'assertion suivante pour tout $b \in \mathbb{N}$:

$$H_b : \qquad \forall a \in \mathbb{N} \qquad \operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}(a \wedge b)$$

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

- Initialisation : Si $b = 0$, alors d'une part $\operatorname{div}(a) \cap \operatorname{div}(b) = \operatorname{div}(a) \cap \mathbb{Z} = \operatorname{div}(a)$ et d'autre part $a = a \wedge b$ donc $\operatorname{div}(a \wedge b) = \operatorname{div}(a)$. Donc H_0 est vraie.
- Hérédité : Soit $b_0 \in \mathbb{N}$. On suppose que pour tout $b \leq b_0$, l'assertion H_b est vraie. Montrons que H_{b_0+1} est vraie. Pour simplifier, on pose $B = b_0 + 1$. Soit $a \in \mathbb{N}$. Montrons que $\operatorname{div}(a) \cap \operatorname{div}(B) = \operatorname{div}(a \wedge B)$. De par la division euclidienne de a par B (possible car $B \neq 0$), il existe $q, r \in \mathbb{Z}$ tels que

  $$a = Bq + r \qquad \text{et} \qquad 0 \leq r < |B| = B$$

  Or, par le lemme précédent, on a $a \wedge B = B \wedge r$ et

  $$\operatorname{div}(a) \cap \operatorname{div}(B) = \operatorname{div}(B) \cap \operatorname{div}(r) \qquad (*)$$

  Or, comme $r < B$, on a $r \leq b_0$ donc par hypothèse de récurrence, l'assertion H_r est vraie :

  $$\forall a' \in \mathbb{N} \qquad \operatorname{div}(a') \cap \operatorname{div}(r) = \operatorname{div}(a' \wedge r)$$

  En particulier, (pour $a' = B$), on en déduit que $\operatorname{div}(B) \cap \operatorname{div}(r) = \operatorname{div}(B \wedge r)$. On en déduit avec $(*)$ que

  $$\begin{aligned} \operatorname{div}(a) \cap \operatorname{div}(B) &= \operatorname{div}(B \wedge r) \\ &= \operatorname{div}(a \wedge B) \qquad \text{car } a \wedge B = B \wedge r \end{aligned}$$

  Par arbitraire sur a, on a montré que H_B est vraie, i.e. que H_{b_0+1} est vraie.
- Conclusion : la propriété H_b est vraie pour tout $b \in \mathbb{N}$.

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 $\operatorname{div}(r_k) = \operatorname{div}(0) = \mathbb{Z}$, donc, par le Théorème 18.9

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

si bien que $r_{k-1} = a \wedge b$ par le Théorème 18.10. □

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 18.11

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 18.12 – 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 $b \in \mathbb{N}$:

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

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

- Initialisation : si $b = 0$, alors pour tout $a \in \mathbb{N}$, on a $a \wedge b = a$, donc le couple $(u,v) = (1,0)$ convient. Ainsi, H_0 est vraie.
- Hérédité : soit $b_0 \in \mathbb{N}$. On suppose que H_b est vraie pour tout $b \leq b_0$. Montrons H_{b_0+1}. Pour simplifier on pose $B = b_0 + 1$. Soit $a \in \mathbb{N}$. De par la division euclidienne de a par B (qui est bien non nul), il existe $q,r \in \mathbb{Z}$ tels que

  $$a = Bq + r \qquad \text{et} \qquad 0 \leq r < B$$

  On a alors $a \wedge B = B \wedge r$. De plus, comme $r < B$, on a $r \leq b_0$ donc l'assertion H_r est vraie, à savoir

  $$\forall a' \in \mathbb{N}^* \quad \exists u',v' \in \mathbb{Z} \qquad a'u' + rv' = a' \wedge r$$

  En particulier, (avec $a' = B$), il existe $u',v' \in \mathbb{Z}$ tels que

  $$\begin{aligned} Bu' + rv' = B \wedge r &\implies Bu' + (a - Bq)v' = a \wedge B \\ &\implies av' + B\left(u' - qv'\right) = a \wedge B \end{aligned}$$

  si bien que le couple $(u,v) := (v', u' - qv')$ convient. Finalement H_B est vraie.

Ainsi, H_b est vraie pour tout $b \in \mathbb{N}$. On a donc 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

  $$a(-u) + bv = |a|u + |b|v = a \wedge b$$

  On en déduit que $-u$ et v sont des coefficients de Bézout de a et b.

- Les autres cas selon les signes 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 $au+bv = a\wedge b$, alors pour tout $k\in\mathbb{Z}$, on vérifie que $a(u+bk)+b(v-ak) = a\wedge b$, 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 $(u,v)\in\mathbb{Z}^2$ tel que $247u+195v = 247\wedge 195$.

Méthode

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

Théorème 18.13 – Factorisation par un entier dans le PGCD

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

Démonstration.

□

4 Entiers premiers entre eux

4.1 Définition et théorème de Bézout

Définition 18.14 – 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 18.15 – Théorème de Bézout

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

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

Il ne faut pas confondre la relation de Bézout (Théorème 18.12) et le Théorème de Bézout. Pour tous $a, b, d \in \mathbb{Z}$:

$$\text{Relation de Bézout :} \quad d = a \wedge b \quad \boxed{\Longrightarrow} \quad \exists u, v \in \mathbb{Z} \quad au + bv = d$$

$$\text{Théorème de Bézout :} \quad 1 = a \wedge b \quad \boxed{\Longleftrightarrow} \quad \exists u, v \in \mathbb{Z} \quad au + bv = 1$$

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 18.16 – 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.

□

Définition 18.17

On dit qu'une fraction est irréductible si son numérateur et son dénominateur sont premiers entre eux.
On ne peut alors plus la "simplifier".

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 écriture irréductible de $\frac{a}{b}$ est la fraction $\frac{a'}{b'}$ avec $a' = \frac{a}{a \wedge b}$ et $b' = \frac{b}{a \wedge b}$.

Exemple 10. Comme $(-195) \wedge 247 = 13$, la fraction $\frac{-195}{247}$ se simplifie en une fraction irréductible : $\frac{\frac{-195}{13}}{\frac{247}{13}} = \frac{-15}{19}$.

Remarque. Dans l'exemple ci-dessus, la fraction $\frac{15}{-19}$ est également irréductible, mais en général on prend un dénominateur positif, ce qui garantit l'unicité.

4.2 Trois corollaires du théorème de Bézout

Corollaire 18.18 – 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 : $\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies a \mid c$

Démonstration.

□

Corollaire 18.19

Soit $a,b_1,b_2 \in \mathbb{Z}$. Si a est premier avec les entiers b_1 et b_2, alors a est premier avec leur produit $b_1 b_2$.

Autrement dit : $\begin{cases} a \wedge b_1 = 1 \\ a \wedge b_2 = 1 \end{cases} \implies a \wedge (b_1 b_2) = 1$

Démonstration.

□

Corollaire 18.20

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

Démonstration.

□

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.

5 Congruences

5.1 Définition et relation d'équivalence

Définition 18.21 – 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 12.
- $10 \equiv 3 \equiv -4 \ [7]$.
- $a \equiv 0 \ [n]$ si et seulement si a est divisible par n. Par exemple $a \equiv 0 \ [2]$ ssi a est pair.
- Résoudre l'équation $x \equiv 2 \ [7]$.

Théorème 18.22 – 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)

5.2 Opérations et congruences

Théorème 18.23 – 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 :

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

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

$$a \equiv b \ [n] \implies \begin{cases} \forall k \in \mathbb{Z} & ka \equiv kb \ [n] \\ \forall k \in \mathbb{N}^* & a^k \equiv b^k \ [n] \end{cases}$$

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

$$\begin{cases} a \equiv b \ [n] \\ c \equiv d \ [n] \end{cases} \quad \begin{cases} n \mid a-b \\ n \mid c-d \end{cases}$$

$$\begin{cases} n \mid (a-b)+(c-d) \\ n \mid (a-b) \times d + (c-d) \times a \end{cases}$$

$$\begin{cases} n \mid (a+c)-(b+d) \\ n \mid ac-bd \end{cases}$$

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

□

Exemple 13. Montrer que $9^{2025} \equiv -1 \ [10]$.

Définition 18.24 – Tableaux de congruence

Soit $a \in \mathbb{Z}$ et un entier $n \geq 2$. On appelle tableau de congruence de a modulo n une table de la forme :

k	1	2	3	$\cdots$
$a^k \equiv \ldots \ [n]$				

où, pour chaque valeur de k, on remplit la case vide par une valeur de $[\![0, n-1]\!]$ qui est congrue à a^k modulo n.

Théorème 18.25 – Cyclicité du tableau de congruence

Les valeurs (de la seconde ligne) du tableau de congruence forment un cycle. De plus, si $a \wedge n = 1$, l'une de ces valeurs est 1.

Démonstration. Admise en MPSI, démontrée en MP. □

Méthode

Pour déterminer à quoi est congru a^m modulo n pour de grandes valeurs de m, on peut remplir un tableau de congruence :

1. Si $a \wedge n = 1$, on peut s'arrêter dès qu'on a trouvé k tel que $a^k \equiv 1 \ [n]$ ou $a^k \equiv n-1 \equiv -1 \ [n]$, cf ci-dessous.
2. Sinon, on peut exploiter le caractère cyclique du tableau.

Exemple 14. Déterminer le reste de la division euclidienne de 7^{2019} par 22.

5.3 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 et n sont tous divisibles par un entier $d \in \mathbb{N}^*$, alors la division est possible :

Théorème 18.26 – 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 18.27 – 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 $k \in \mathbb{Z}$ $a(c+kn) \equiv 1\ [n]$

Théorème 18.28 – 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 de a 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", parmi les entiers de $[\![1, n-1]\!]$.
- Calculer un couple de coefficients de Bézout (u, v) tels que $au + nv = 1$. 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 18.29 – 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 $d := A \wedge N$ et on tente de diviser la congruence crochet inclus par d :
   - Si d ne divise pas B, il n'y a pas de solution.
   - Si $d \mid B$, on pose
   $$a := \frac{A}{d} \in \mathbb{Z} \qquad b := \frac{B}{d} \in \mathbb{Z} \qquad n := \frac{N}{d} \in \mathbb{Z}$$
   On peut alors diviser la congruence par d : $\quad Ax \equiv B \ [N] \iff ax \equiv b \ [n]$. De plus $a \wedge n = 1$.
2. On détermine un inverse de a modulo n : on le notera (ici) c. On a donc :
   $$ax \equiv b \ [n] \iff x \equiv cb \ [n]$$
   et l'équation est résolue.

Justifions que si d ne divise pas B, alors il n'y a pas de solution. En effet, on a $Ax = B + kN$ avec un certain $k \in \mathbb{Z}$. Comme d divise A et N, il divise $Ax - kN$, donc B. Contradiction.

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

6 Équations diophantiennes

6.1 Définition

Définition 18.30 – Équation diophantienne

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

Exemple 15. Les équations suivantes sont des équations diophantiennes :

- L'équation $3x^2 + xy = 11$ d'inconnues $x, y \in \mathbb{Z}$.
- L'équation $\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$ 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. On peut invoquer des propriétés sur les nombres premiers, on peut aussi regarder ce que donne l'égalité mise au modulo n pour un n bien choisi.

Exemple 16. Montrer que l'équation $x^2 + y^2 = 4003$ n'admet pas de solution dans $\mathbb{Z}^2$.

6.2 Équation de la forme $ax + by = c$

Il y a un cas particulier d'équation qu'il faut savoir traiter sans indication : les équations diophantiennes de la forme $ax + by = c$ avec $a, b, c \in \mathbb{Z}$.

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 $d=A\wedge B$ et on tente de diviser l'équation par d :
   - Si $d\nmid C$, alors il n'y a pas de solution.
   - Si $d\mid C$, on pose
   $$a:=\frac{A}{d}\in\mathbb{Z}\qquad b:=\frac{B}{d}\in\mathbb{Z}\qquad c=\frac{C}{d}\in\mathbb{Z}$$
   On peut alors diviser l'équation par d : $\quad Ax+By=C\quad\Longleftrightarrow\quad ax+by=c$. De plus $a\wedge b=1$.
2. On passe l'équation au modulo b, on obtient : $\quad ax\equiv c\ [b]$, que l'on résout. On trouve que x est de la forme $x(k)=x_0+bk$ avec $x_0\in\mathbb{Z}$ fixé et $k\in\mathbb{Z}$ quelconque.
3. On injecte cette valeur $x(k)$ dans l'équation $ax+by=c$ et on trouve la valeur $y(k)$ correspondante. L'ensemble des solutions est alors $\{(x_k,y_k)\mid k\in\mathbb{Z}\}$.

Exemple 17. Résoudre $10x+6y=8$.

7 PPCM et extension du PGCD

7.1 PPCM

Soit $a,b\in\mathbb{N}^*$. On souhaite définir le PPCM de a et b comme étantle plus petit des multiples communs strictement positifs de a et b. Or, l'ensemble des multiples communs strictement positifs à a et b est l'ensemble

$$X=a\mathbb{Z}\cap b\mathbb{Z}\cap\mathbb{N}^*$$

Le PPCM de a et b sera le minimum de X. Mais il faut s'assurer que ce minimum existe !

- Il est clair que X est une partie de $\mathbb{Z}$.
- De plus, on a clairement $ab\in X$. On en déduit que X est non vide.
- Enfin, X est minoré par 0.

Ainsi, X est une partie non vide et minorée de $\mathbb{Z}$, donc X admet un minimum par le Théorème 18.5. On en déduit que la définition suivante a un sens.

Définition 18.31 – PPCM

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

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

Exemple 18. Le PPCM de 12 et de 18 est 36. En effet (on omet les multiples négatifs) :

$$12\mathbb{Z} = \{\cdots, 12, 24, 36, 48, 60, 72, \cdots\} \qquad 18\mathbb{Z} = \{\cdots, 18, 36, 54, 72, \cdots\}$$

Ainsi, $12\mathbb{Z} \cap 18\mathbb{Z} \cap \mathbb{N}^* = \{36, 72, \cdots\}$ et donc $12 \vee 18 = 36$.

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 19. 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 18.32

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

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

ou encore, de manière équivalente :

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

Théorème 18.33 – Factorisation dans un PPCM

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

Démonstration. Pour montrer l'égalité de ces deux entiers (positifs), il suffit de montrer que chacun divise l'autre.

- Montrons que $(ca) \vee (cb) \mid c(a \vee b)$. Tout d'abord, $a \mid a \vee b$ donc $ca \mid c(a \vee b)$. De même on montre que $cb \mid c(a \vee b)$. On en déduit par le Théorème 18.32 que $(ca) \vee (cb) \mid c(a \vee b)$.
- On pose $m = (ca) \vee (cb)$. Montrons que $c(a \vee b) \mid m$. On sait que $ca \mid m$, donc en particulier $c \mid m$. Ainsi, il existe $m' \in \mathbb{Z}$ tel que $m = cm'$. Comme $ca \mid m$, on a donc $ca \mid cm'$, d'où $a \mid m'$. On montre de même que $b \mid m'$. Ainsi, par le Théorème 18.32, on a $a \vee b \mid m'$. D'où $c(a \vee b) \mid cm'$, i.e. $c(a \vee b) \mid m$.

□

Théorème 18.34

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

$$(a \vee b) \times (a \wedge b) = |ab|$$

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" car il divise tous les autres élements de cet ensemble.

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

□

Méthode

Pour calculer le PPCM $a \vee b$, on peut donc calculer le PGCD $a \wedge b$ puis calculer $\dfrac{|ab|}{a \wedge b}$.

Exemple 20. Calculer le PPCM de 195 et de 247.

7.2 PGCD de plusieurs entiers

Définition 18.35

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 21. $195 \wedge 247 \wedge 18 =$ .....

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 18.36

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 18.37 – Relation de Bézout généralisée

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

$$a_1 u_1 + a_2 u_2 + \ldots + a_n u_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

Théorème 18.38 – Théorème de Bézout généralisé

Soit $a_1, \ldots, a_n \in \mathbb{Z}$.

$$a_1 \wedge \cdots \wedge a_n = 1 \iff \exists u_1, \cdots, u_n \in \mathbb{Z} \qquad a_1 u_1 + \ldots + a_n u_n = 1$$

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

8 Nombres premiers

8.1 Définitions et lemmes préliminaires

Définition 18.39

On appelle nombre premier tout entier $p \geq 2$ tel que les seuls diviseurs positifs de p sont 1 et p.
On note $\mathbb{P}$ l'ensemble des nombres premiers.

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 23. 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 18.40

Soit $a \in \mathbb{Z}$ et $p \in \mathbb{P}$. 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 18.41 – Lemme d'Euclide

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

Corollaire immédiat : si p divise un produit $a_1 \times \cdots \times a_N$, alors p divise (au moins) un des entiers $a_1, \cdots, a_N$.

Démonstration. Supposons que $p \mid ab$. Si $p \mid a$, alors on a le résultat voulu. Supposons que p ne divise pas a. Par le Lemme 18.40 ci-dessus, 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 18.42

Soit $p_1, p_2 \in \mathbb{P}$. 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 $p_1 = p_2$. □

8.2 DPFP – Existence

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

Lemme 18.43

Tout entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers (non nécessairement distincts). Autrement dit, il existe $N \in \mathbb{N}^*$ et $q_1, \cdots, q_N \in \mathbb{P}$ tels que

$$n = q_1 \times \ldots \times q_N$$

Démonstration. On procède par récurrence forte sur n.

- Initialisation : si $n = 2$, alors $n = q_1$ avec $q_1 = 2 \in \mathbb{P}$. 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 18.44

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

Soit $n \geq 2$ un entier. Par le Lemme 18.43, n admet une DPFP : on a donc

$$n = q_1 \times q_2 \times \cdots \times q_N \qquad \text{avec } n \in \mathbb{N}^*, \quad q_1, \cdots, q_N \in \mathbb{P}$$

De plus, quitte à réindexer les entiers $q_1, \cdots, q_N$, on peut imposer que $q_1 \leq \ldots \leq q_N$. 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

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

Ceci est la forme générale de la décomposition en produits de facteurs premiers. On a obtenu l'existence

8.3 DPFP – Unicité

Théorème 18.45

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 $\alpha_1, \alpha_2, \cdots, \alpha_r \in \mathbb{N}^*$ tels que

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

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 18.43. Montrons l'unicité de cette décomposition. Supposons qu'un entier $n \geq 2$ admette les deux décompositions ci-dessous et montrons qu'elles coïncident :

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

donc il faut montrer que $r = s$, et que $\forall k \in [\![1, r]\!]$ $p_k = q_k$ 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 18.42) $p_i = q_j$. 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

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

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

Exemple 24. Décomposer 1400 en produits de facteurs premiers.

Corollaire 18.46

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. □

8.4 Valuation p-adique

Définition 18.47

Soit $p \in \mathbb{P}$. Pour tout entier $n \in \mathbb{N}^*$, on appelle valuation p-adique de n, la puissance de l'entier p qui apparait dans la DPFP de n, et on la note $v_p(n)$.
Si p n'apparait pas dans la DPFP de n, on pose $v_p(n) = 0$.

Alternativement, $v_p(n)$ peut être défini comme le plus grand entier $k \in \mathbb{N}$ tel que

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

On a toujours $v_p(n) \in \mathbb{N}$.

Définition 18.48 – Décomposition généralisée

Pour tout $n \in \mathbb{N}^*$, on a :

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

On appelle cela la DPFP généralisée de n.

Exemple 25.
- Comme $90 = 2^1 \times 3^2 \times 5^1$, on a $v_2(90) = v_5(90) = 1$ et $v_3(90) = 2$. Les autres valuations sont nulles.
- Si p est un nombre premier et $\alpha \in \mathbb{N}$, $v_p(p^\alpha) = \ldots$

Remarque. La décomposition généralisée de n est 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.

Théorème 18.49

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

$$a \mid b \iff \forall p \in \mathbb{P} \quad v_p(a) \leq v_p(b)$$
$$a = b \iff \forall p \in \mathbb{P} \quad v_p(a) = v_p(b)$$

De plus, pour tout nombre premier p,

1. $v_p(ab) = v_p(a) + v_p(b)$ et en particulier $v_p(a^n) = n v_p(a)$ pour tout $n \in \mathbb{N}^*$.
2. $v_p(a \wedge b) = \min(v_p(a), v_p(b))$
3. $v_p(a \vee b) = \max(v_p(a), v_p(b))$

Démonstration. On ne prouve que l'assertion 1.

□

Méthode

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

Exemple 26. Calculer le PGCD et le PPCM de 360 et 315.

Exemple 27. Combien 1400 a-t-il de diviseurs positifs ? Et de diviseurs de signe quelconque ?

Exemple 28. Soit $a, b \in \mathbb{N}^*$. Montrer que $a^3 \wedge b^3 = (a \wedge b)^3$.

8.5 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 29. Est-ce que 89 est un nombre premier ?

8.6 Petit théorème de Fermat

Lemme 18.50

Soit p un nombre premier. Pour tout $k \in [\![1, p-1]\!]$, on a

$$p \mid \binom{p}{k}$$

Démonstration.

□

Corollaire 18.51

Pour tous $a, b \in \mathbb{Z}$, on a :

$$(a+b)^p \equiv a^p + b^p \ [p]$$

Démonstration. Par la formule du binôme, on a

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

Puisque $p \mid \binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$, en passant modulo p dans l'équation, on a bien $(a+b)^p \equiv a^p + b^p \ [p]$. □

Théorème 18.52 – 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, $a^p \equiv (a')^p \equiv a' \equiv a \ [p]$. □

Exemple 30. Quel est le reste de la division euclidienne de 14^{2024} par 11 ?

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.
- 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, et on peut par ailleurs utiliser la formule $(a \wedge b)(a \vee b) = \ldots$

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 !