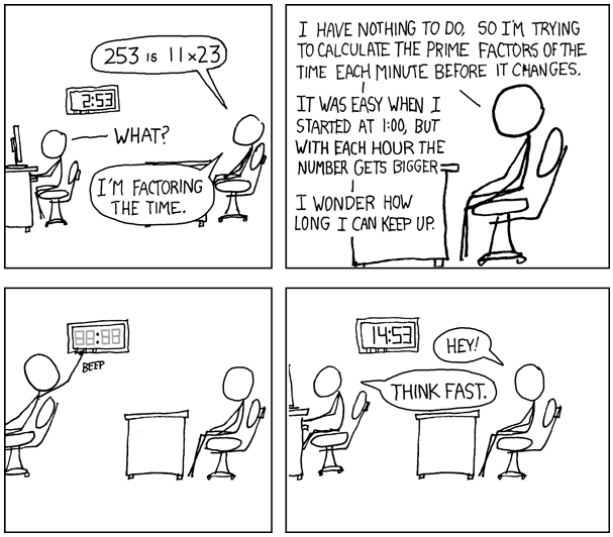
Lycée Loges

Chapitre 14
Arithmétique

Simon Dauguet
simon.dauguet@gmail.com

6 janvier 2026



Le but de ce chapitre est d'étudier plus précisément l'anneau $\mathbb{Z}$ des entiers.

L'arithmétique est probablement la branche des mathématiques la plus vieille. C'est aussi l'une des plus développées et l'une des plus fondamentales (au sens fondateur donc importante, et au sens abstraction). Il arrive très régulièrement que des questions d'arithmétique fasses irruptions dans des domaines ou des problèmes où on ne les attendait a priori pas. Mais comme *tout est nombre* (cf Pythagore) et que l'étude des nombres, c'est le but de l'arithmétique,

L'arithmétique est particulièrement difficile pour ces raisons là. Les questions posées sont souvent élémentaires et on a alors peu d'outils à notre disposition. Il faut alors développer des trésors d'ingéniosité et de contorsions intellectuelles pour résoudre le problème. Étant un domaine fondateur et élémentaire (au sens peu d'outil sont nécessaires), les choses sont très sensibles d'un point de vue logique. L'arithmétique foisonne de petites propriétés contre intuitive dont les réciproques sont fausses mais tentantes. C'est donc un domaine exigeant et ingrat pour l'intuition. Mais très formateur intellectuellement.

> Disons qu'en mathématique, il y a deux sources inépuisables de phénomènes à l'état brut qui sont, d'un côté l'arithmétique, et, d'un autre, la physique.
>
> *Alain Connes*

Table des matières

1 Divisibilté

On rappelle que $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre dont le groupe des inversibles est $\{-1, 1\}$.

1.1 Divisibilité, Diviseurs, multiples

Définition 1.1 (Divisibilité) :
Soit $a, b \in \mathbb{Z}$. On dit que a *divise* b (ou que b *est divisible par* a) si $\exists c \in \mathbb{Z}$ tel que $b = ac$. Et on note $a|b$.

Remarque :
Attention, la définition n'est pas si simple. La définition de la divisibilité se fait un peu "à l'envers". On a pas de définition directe.

Remarque :
0 est le seul entier qui est divisible par par tous les entiers. Autrement dit si $n \in \mathbb{Z}$, alors $n = 0 \iff \forall p \in \mathbb{Z},\ p|n$.

Proposition 1.1 (Relation d'ordre de la divisibilité sur $\mathbb{N}$) :
La relation de divisibilité est une relation d'ordre partielle sur $\mathbb{N}$ mais la divisibilité n'est pas antisymétrique sur $\mathbb{Z}$ (donc elle n'est que réflexive et antisymétrique sur $\mathbb{Z}$).

Autrement dit, la relation $|$ est une relation binaire, réflexive, antisymétrique, transitive sur $\mathbb{N}$. Et on a $-2|2$ et $2|-2$ mais $2 \neq -2$. Donc il n'y a pas d'antisymétrie sur $\mathbb{Z}$.

Remarque :
Si $a \neq 0$ et si $b|a$, alors $|b| \leq |a|$. En effet, si $b|a$, alors $|b|||a|$. Et donc $\exists k \in \mathbb{N}^*$ tel que $|a| = k|b|$ car $a \neq 0$. Donc $k \geq 1$ et d'où le résultat.

Définition 1.2 (Entiers associés) :
Soit $a, b \in \mathbb{Z}$.
a et b sont dit *associés* si $a|b$ et $b|a$.

Remarque :
On notera que a et b associés entraîne $ab \neq 0$ ou bien $a = b = 0$. Mais on ne peut pas avoir un seul des deux nuls.

Proposition 1.2 (Caractérisation des entiers associés) :
Soit $a, b \in \mathbb{Z}$.
a et b sont associés si, et seulement si, $a = \pm b$.

Démonstration :
Le sens indirecte est évident. Il sont multiples l'un de l'autre en multipliant par -1 (qui est son propre inverse dans $\mathbb{Z}$).

Réciproquement, supposons a et b associés. Si $a = 0$, alors $b = 0$ car b est un multiple de a. Si $a \neq 0$, alors $\exists p, q \in \mathbb{Z}$ tels que $a = pb = pqa$. Comme $\mathbb{Z}$ est intègre, on en déduit $pq = 1$. Donc $p, q \in \mathbb{Z}^\times = \{-1, 1\}$. D'où l'on déduit $a = \pm b$. □

Proposition 1.3 (Propriétés algébriques de la divisibilité) :
Soit $a, b, c, d \in \mathbb{Z}$. Alors :

(i) $a|b \iff |a|||b|$

(ii) Si $a|b$, alors $\forall p \in \mathbb{Z}$, $a|pb$.

(iii) Si $c|a$ et $c|b$, alors $\forall u, v \in \mathbb{Z}$, $c|(au + bv)$.

(iv) Si $a|b$ et $c|d$, alors $ac|bd$.

(v) Si $d \neq 0$, alors $a|b \iff ad|bd$.

Démonstration :

(i) C'est évident. Mais il faut le dire au moins une fois.

(ii) Il suffit décrire la définition. C'est évident.

(iii) Par définition, $\exists p, q \in \mathbb{Z}$ tels que $a = pc$ et $b = qc$. Alors $\forall u, v \in \mathbb{Z}$, $au + bv = (pu + qv)c$ et donc le résultat.

(iv) Par définition, $\exists p, q \in \mathbb{Z}$ tels que $b = ap$ et $d = qc$. Alors $bd = pqac$ et donc $ac|bd$.

(v) On fait les deux sens d'un coup :

$$a|b \iff \exists p \in \mathbb{Z},\ b = ap \iff \exists p \in \mathbb{Z},\ bd = adp \iff ad|bd$$

□

Remarque :
En effectuant une petite récurrence, on a aussi $a|b \implies \forall n \in \mathbb{N},\ a^n|b^n$.

Proposition 1.4 (Caractérisation de la divisibilité en terme de sous-groupe de $\mathbb{Z}$) :
Soit $a, b \in \mathbb{Z}$. Alors

$$a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$$

Démonstration :
Il suffit d'écrire les définitions : $a|b \iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z}$. □

Définition 1.3 (Diviseurs, multiples) :
Soit $n, p \in \mathbb{Z}$.
On dit que n est un *diviseur* de p si $n|p$.
On dit que n est *multiple* de p si $p|n$.

Remarque :
Dans une relation $b = ap$, la notion de diviseur et multiple est une question de référentiel, de point de vue, de ce qui nous intéresse. Pour b, a et p sont des diviseurs. Pour a et p, b est un multiple. Mais dans les deux cas, on parle de la même relation. On ne se focalise simplement pas sur la même chose. Le sujet n'est pas le même. Un peu comme le passage d'une phrase sous la forme active à sa forme passive.

Exemple 1.1 :
Les diviseurs de 15 sont $\{-15, -5, -3, -1, 1, 3, 5, 15\}$.

⚠ Attention à ne pas oublier les diviseurs négatifs. On a tendance naturellement à ne raisonner que dans $\mathbb{N}$ et donc oublier les diviseurs négatifs. Sans précision, ils doivent être pris en compte. Ce qui change beaucoup, par exemple, le nombre de diviseurs d'un entier.

Remarque :
C'est évident, mais tout de même, il faut le remarquer. Évidemment, $\forall n \in \mathbb{Z}$, $\forall a \in \mathbb{Z}^*$, $n|a \implies |n| \leq |a|$.

Définition 1.4 (Diviseurs triviaux) :
Soit $n \in \mathbb{Z}$. Alors $-n$, -1, 1 et n sont des diviseurs de n. Ce sont les *diviseurs triviaux* de n.

Proposition 1.5 (Ensemble des multiples) :
Soit $n \in \mathbb{Z}$.
L'ensemble des multiples de n est $n\mathbb{Z}$.

Démonstration :
C'est évident. □

Remarque :
En particulier, l'ensemble des multiples est un sous-groupes de $\mathbb{Z}$.

Notation (Ensemble des diviseurs) :
Soit $n \in \mathbb{Z}$. On notera $\mathrm{Div}(n)$ l'ensemble des diviseurs de n, *i.e.*

$$\mathrm{Div}(n) := \{p \in \mathbb{Z},\ p|n\}.$$

Attention, cette notation n'est pas canonique. C'est un choix de ma part. Elle doit être redéfinie à chaque nouvelle utilisation.
On notera $\mathrm{Div}_+(n)$ l'ensemble des diviseurs positifs de n. Donc $\mathrm{Div}_+(n) = \mathrm{Div}(n) \cap \mathbb{N}$.

Proposition 1.6 (Ensemble de diviseurs) :
Soit $n \in \mathbb{Z}$.
$\mathrm{Div}(n)$ est un ensemble fini si, et seulement si, $n \neq 0$.

Démonstration :
On sait que si $n \neq 0$, alors $a|n \implies |a| \leq |n|$. Donc l'ensemble des diviseurs de n est borné par $|n|$. Comme c'est un sous-ensemble de $\mathbb{Z}$ et il est fini si $n \neq 0$.
Et si $n = 0$, alors par définition, $\mathrm{Div}(0) = \mathbb{Z}$ qui est infini. □

Remarque :
En particulier, par contraposition, on a $n = 0$ ssi il est divisible par une infinité d'entier. C'est assez pratique. C'est ce qu'on utilise par exemple dans la démonstration classique de l'irrationalité de $\sqrt{2}$.

1.2 Division euclidienne

Définition-Propriété 1.5 (Division euclidienne) :
Soit $a, b \in \mathbb{Z}$ et $b \neq 0$. Alors $\exists!(q, r) \in \mathbb{Z}$ tels que :

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

q s'appelle le *quotient*, r le *reste*, a le *dividende* et b le *diviseur* de *la division euclidienne de a par b*.

Démonstration :
On pose $q = \lfloor a/b \rfloor$. Alors, par caractérisation de la partie entière, $a/b - 1 < q \leq a/b$. Et donc $a - b < bq \leq a$. On pose $r = a - bq$. Alors $q, r \in \mathbb{Z}$ et $0 \leq r < b$. D'où l'existence.

Supposons $\exists q, r, s, t \in \mathbb{Z}$ tel que $a = bq + r = bs + t$ et $0 \leq r, t < b$. Alors $b(q - s) = t - r \in]\!]-b, b[\![$. donc $b(q - s) = 0$. Et $\mathbb{Z}$ étant intègre, on en déduit $q = s$. Puis immédiatement $r = t$. D'où l'unicité. □

Remarque :
Une autre preuve classique consiste à faire une récurrence forte sur a. C'est ce que nous ferons dans le chapitre sur les polynômes. Pour diversifier les méthodes, j'ai proposé une autre démo dans le cadre des entiers qui utilise des outils qui ne sont disponibles que dans le cadre des entiers.

Proposition 1.7 (Caractérisation de la division par la division euclidienne) :
Soit $a, b \in \mathbb{Z}$ et $a \neq 0$.
Alors $a|b \iff$ le reste de la division euclidienne de b par a est 0.

Démonstration :
Il suffit de l'écrire. Si le reste de la division euclidienne de b par a est 0, alors, par définition de la division euclidienne, $\exists p \in \mathbb{Z}$ tel que $b = ap + 0 = ap$ et donc $a|b$.

Réciproquement, si $a|b$, alors $\exists p \in \mathbb{Z}$ tel que $b = ap$. Et donc on peut écrire $b = ap + 0$ avec $0 \leq 0 < a$. Donc, par unicité de la division euclidienne, $b = ap + 0$ est la division euclidienne de b par a et le reste est 0. □

1.3 Congruence

Définition 1.6 (Congruence) :
Soit $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

On dit que a *est congrue à* b *modulo* n, et on note $a \equiv b\ [n]$, si a et b ont le même reste dans la division euclidienne par n, *i.e.*

$$a \equiv b\ [n] \overset{\text{def}}{\iff} \exists p, q, r \in \mathbb{Z},\ a = pn + r,\ b = qn + r,\ 0 \leq r < n$$

Remarque :
On note parfois aussi $a \equiv b \mod n$ pour la relation de congruence modulo n, avec éventuellement des parenthèses en plus. Mais le programme impose la notation donnée dans la définition.

Proposition 1.8 (Caractérisation des congruences par les divisibilités) :
Soit $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$.

Alors

$$a \equiv b\ [n] \iff n | (b - a)$$

Démonstration :
Il suffit d'utiliser la définition avec la caractérisation de la division euclidienne par la division. □

Remarque :
En particulier, $n|a \iff a \equiv 0\ [n]$.

Proposition 1.9 (Reformulation des congruences) :
Soit $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Alors

$$a \equiv b\ [n] \iff \exists k \in \mathbb{Z},\ a = b + nk$$

Démonstration :
D'après la caractérisation précédente $a \equiv b\ [n] \iff n|(b - a) \iff \exists k \in \mathbb{Z},\ b - a = nk \iff \exists k \in \mathbb{Z},\ a = b + nk$. □

Définition 1.7 (Extension des congruences dans $\mathbb{R}$) :
Soit $x, y, z \in \mathbb{R}$ et $z \neq 0$.
On dira que x *est congrue à* y *modulo* z, et on écrira $x \equiv y\ [z]$ si $\exists k \in \mathbb{Z}$ tel que $x = y + kz$.

Exemple 1.2 :
D'où les notations des congruences en trigonométrie. Donc, par exemple, $\theta \equiv \frac{\pi}{4}\ [\pi] \iff \exists k \in \mathbb{Z},\ \theta = \frac{\pi}{4} + k\pi$.

Proposition 1.10 ($\equiv \mod n$ est une relation d'équivalence) :
Soit $n \in \mathbb{N}^*$.
La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Démonstration :
La relation $\equiv\ [n]$ est évidemment une relation binaire. Elle est également réflexive car $n|0$ donc $\forall x \in \mathbb{Z},\ n|(x - x)$.

De plus, $\forall x, y \in \mathbb{Z},\ x \equiv y\ [n] \iff n|(y - x) \iff n|(x - y) \iff y \equiv x\ [n]$. Donc la relation est symétrique.

Et enfin elle est transitive facilement : si $x, y, z \in \mathbb{Z}$ tels que $x \equiv y\ [n]$ et $y \equiv z\ [n]$, alors $n|((y - x) - (y - z))$ et donc $x \equiv z\ [n]$ □

Remarque (HP) :
Comme on vient de voir que la relation d'équivalence modulo n est une relation d'équivalence sur $\mathbb{Z}$, on peut étudier l'ensemble des classes d'équivalence par rapport à cette relation d'équivalence. On note

$$\forall x \in \mathbb{Z},\ \overline{x} = \mathrm{Cl}(x) = \{y \in \mathbb{Z},\ x \equiv y\ [n]\}.$$

Et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences.

Alors on peut munir $\mathbb{Z}/n\mathbb{Z}$ d'un addition est d'une multiplication telles que :

$$\forall n, m \in \mathbb{Z},\ \overline{n} + \overline{m} = \overline{n + m} \qquad \text{et} \qquad \overline{n} \times \overline{m} = \overline{nm}$$

On peut alors montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif fini composé de n éléments. Cela revient un peu à compter en rond. Au bout de la chaîne, on revient à 0.

L'étude plus poussée de cette anneau est au programme de MP (pour étudier les conditions pour qu'il soit intègre, un corps etc).

Proposition 1.11 (Propriétés algébriques de la relation de congruence) :
Soit $n \in \mathbb{N}^*$. Soit $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors

(i) $a + c \equiv b + d\ [n]$

(ii) $ac \equiv bd\ [n]$

(iii) $\forall k \in \mathbb{N}$, $a^k \equiv b^k\ [n]$

(iv) Si $\lambda \in \mathbb{Z}^*$, alors $a \equiv b[n] \iff \lambda a \equiv \lambda b\ [\lambda n]$

Démonstration :

(i) Il suffit de voir que $n|(b + d - a - c)$.

(ii) Alors $\exists p, q \in \mathbb{Z}$ tel que $a = b + np$ et $c = nq + d$. Alors $ac = bd + n(npq + d + b)$. Donc $ac \equiv bd\ [n]$.

(iii) Pour $k = 0$, c'est assez évident. Et il suffit ensuite de faire un récurrence en utilisant le point précédent.

(iv) Si $\exists k \in \mathbb{Z}$ tel que $a = b + nk$, alors $\lambda a = \lambda b + \lambda nk$. Et la réciproque est évidente puisque $\lambda \neq 0$ et $\mathbb{Z}$ est intègre.

□

Remarque :
On notera que dans le dernier point, le sens directe est encore vraie avec $\lambda = 0$. Mais c'est la réciproque qui n'est plus vraie.

Ces résultats sont également vraies avec les congruences dans $\mathbb{R}$.

!!! ATTENTION !!!

⚠ Ce ne sont que des implications. Les réciproques sont fausses.

Par exemple, $2 + 3 \equiv 1 + 4\ [5]$ mais $2 \not\equiv 1\ [5]$ et $2 \not\equiv 4\ [5]$. De même, $2 \times 3 \equiv 1 \times 0\ [6]$ mais ni 2 ni 3 ne sont congrues à 1 ou 0 mod 6. Et $\forall n \geq 2$, $2^n \equiv 0\ [4]$ mais bien entendu, $2 \not\equiv 0\ [4]$.

Exemple 1.3 :
Résoudre $\cos(2x)\sin(2x) = \frac{\sqrt{2}}{4}$.

Exemple 1.4 :
Montrer que $\forall n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2} \in 7\mathbb{Z}$.

Exemple 1.5 :
Résoudre dans $\mathbb{Z}$ l'équation $x^2 + 5y^2 = 3$.

2 PGCD et PPCM

2.1 PGCD

Définition-Propriété 2.1 (PGCD dans $\mathbb{N}$) :
Soit $a, b \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$. On appelle *plus grand commun diviseurs de a et b*, ou pgcd de a et b, le plus grand entier naturel qui divise à la fois a et b. On le note $a \wedge b$ ou $\mathrm{pgcd}(a, b)$. Donc

$$\mathrm{pgcd}(a, b) := a \wedge b := \max\{n \in \mathbb{N},\ n|a,\ n|b\}.$$

Démonstration :
On considère $\mathrm{Div}_+(a, b) := \{n \in \mathbb{N},\ n|a,\ n|b\} = \mathrm{Div}_+(a) \cap \mathrm{Div}_+(b)$. Alors $1 \in \mathrm{Div}_+(a, b)$. Donc $\mathrm{Div}(a, b) \neq \emptyset$. On a $(a, b) \neq (0, 0)$. Sans perte de généralité, on peut suppose $a \neq 0$. Et $\forall n \in \mathrm{Div}(a, b)$, $n|a$, donc $n \leq a$. Donc $\mathrm{Div}(a, b)$ est majoré par a. Et donc $\max \mathrm{Div}(a, b)$ existe car $\mathrm{Div}(a, b) \subset \mathbb{N}$. □

Remarque :
Tous les entiers sont des diviseurs de 0 car $\forall n \in \mathbb{Z}$, $0 = n \times 0$. On en déduit alors que $\forall n \in \mathbb{Z}^*$, $\mathrm{pgcd}(n, 0) = |n|$.

On pourrait alors choisir la convention $\mathrm{pgcd}(0, 0) = 0$ par soucis de cohérence avec cette remarque et avec les formules qui vont suivre. Mais cette convention n'est officiellement pas au programme. Le programme demande de se contenter du pgcd d'un couple non nul d'entier.

Proposition 2.1 ($\wedge$ est une LCI commutative) :
La loi $\wedge$ est commutative. Autrement dit, $\forall a, b \in \mathbb{Z}$ tels que $(a, b) \neq (0, 0)$, $a \wedge b = b \wedge a$.

Démonstration :
La commutativité provient de la commutativité de la conjonction logique. □

Proposition 2.2 (Caractérisation de la divisibilité par le pgcd) :
Soit $a, b \in \mathbb{Z}$, $a \neq 0$. Alors

$$a|b \iff a \wedge b = |a|$$

Démonstration :
Si $a|b$, alors $a \in \mathrm{Div}(a, b)$. Et donc $|a| \leq \max(\mathrm{Div}(a, b)) = a \wedge b$. Et bien sûr $(a \wedge b)|a$ donc $(a \wedge b) \leq |a|$. Et donc, $|a| = a \wedge b$.

Réciproquement, si $a \wedge b = |a|$, alors automatiquement, $|a| = a \wedge b|b$. □

2.2 Algorithme d' Euclide

Théorème 2.3 (Théorème d'Euclide) :
Soit $a, b, q, r \in \mathbb{Z}^*$. Alors

$$a = bq + r \implies a \wedge b = b \wedge r.$$

Démonstration :
Si d est un diviseur commun à a et b, alors $d|r$ car d divise toute combinaison linéaire de a et b (en particulier $a - bq$). Donc d divise b et r, donc d est un diviseur commun à b et r.

D'autre part, si d est un diviseurs commun de b et r, alors $d|a$ car d divise toute combinaison linéaire de b et r. Donc d divise a et b. Donc d est un diviseurs commun de a et b.

On en déduit que (a, b) et (b, r) ont les mêmes diviseurs communs. Et donc, en particulier, $a \wedge b = b \wedge r$. □

Théorème 2.4 (Algorithme d'Euclide) :
Soit $(a,b) \in \mathbb{Z}^2$ avec $b \neq 0$. On pose $r_0 = a$, $r_1 = b$ et $\forall n \in \mathbb{N}^*$, si $r_n \neq 0$, on définit r_{n+1} comme le reste de la division euclidienne de r_{n-1} par r_n.

Alors $\exists N \in \mathbb{N}$ tel que $r_N = 0$ et $r_{N-1} \neq 0$. De plus $(r_n)_{0 \leq n \leq N}$ est strictement décroissante et $r_{N-1} = a \wedge b$.

Donc le pgcd de a et b est le dernier reste non nul dans la suite des divisions euclidienne.

Démonstration :
Si $b = 0$, alors $a \wedge b = a = r_0$ et $r_1 = b = 0$.

Si $b \neq 0$, alors $r_1 \neq 0$. Alors $\exists q_1 \in \mathbb{N}$ tel que $r_0 = r_1 q_1 + r_2$ et $r_2 < r_1$. A chaque étape, tant que l'on peut définir la suite, on a $r_{n+1} < r_n$ par définition de la division euclidienne. Donc la suite, tant qu'elle est définie, est strictement décroissante. Or c'est une suite d'entier, donc elle est stationnaire en 0. Soit $N \in \mathbb{N}$ tel que $r_N = 0$ et $r_{N-1} = 0$.

De plus, $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{n-1} \wedge r_n = \cdots = r_{N-1} \wedge r_N$ par récurrence. Or $r_N = 0$, donc $r_{N-1} \wedge r_N = r_{N-1}$. Et donc $r_{N-1} = a \wedge b$. □

L'algorithme d'Euclide peut très bien s'écrire en python. Voir avec le prof d'info pour les détails.

Théorème 2.5 (Relation de Bézout) :
Soit $a, b \in \mathbb{Z}$ avec $(a,b) \neq (0,0)$. Alors

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

Démonstration :
Sans perte de généralités, on peut suppose $b \geq 0$, quitte à multiplier par -1.

On va opérer une récurrence forte sur b. Si $b = 0$, alors $a \times 1 + 0 = a = a \wedge 0$.

Supposons $b \neq 0$ et suppose que $\forall r \in \{0, \ldots, b-1\}$, $\forall a \in \mathbb{N}$, $\exists u, v \in \mathbb{Z}$ tels que $au + rv = a \wedge r$. Soit $a \in \mathbb{N}$. On effectue la division euclidienne de a par b. Donc $\exists q, r \in \mathbb{N}$ tels que $a = bq + r$ et $0 \leq r < b$. Alors $a \wedge b = b \wedge r$. Et par hypothèse de récurrence, $\exists u, v \in \mathbb{Z}$ tels que $a \wedge b = au + rv$.

Alors $a \wedge b = au + v(a - bq) = a(u+v) - bqv$ et $u + v \in \mathbb{Z}$, $-qv \in \mathbb{Z}$. □

Remarque :
On en déduit une méthode à partir de l'algorithme d'Euclide pour trouver les coefficients de Bézout :

- On effectue les divisions euclidiennes successives de a par b de l'algorithme d'Euclide.
- On remonte chaque étapes pour obtenir à chaque fois les le pgcd comme combinaison linéaire de r_k et r_{k-1}.

Exemple 2.1 :
Déterminons un couple de Bézout pour $(302, 112)$.

$$\begin{array}{rcl} 302 &=& 112 \times 2 + 78 \\ 112 &=& 78 \times 1 + 34 \\ 78 &=& 34 \times 2 + 10 \\ 34 &=& 10 \times 3 + 4 \\ 10 &=& 4 \times 2 + 2 \end{array} \qquad \begin{array}{rcl} 2 &=& 23\left(302 - 112 \times 2\right) - 16 \times 112 = 23 \times 302 - 62 \times 112 \\ 2 &=& 7 \times 78 - 16\left(112 - 78 \times 1\right) = 23 \times 78 - 16 \times 112 \\ 2 &=& 7\left(78 - 34 \times 2\right) - 2 \times 34 = 7 \times 78 - 16 \times 34 \\ 2 &=& 10 - 2\left(34 - 10 \times 3\right) = 7 \times 10 - 2 \times 34 \\ 2 &=& 10 - 2 \times 4 \end{array}$$

!!! ATTENTION !!!

⚠ Il n'y a pas unicité des coefficients de Bézout ! En fait, il y a même une infinité de coefficients possibles. C'est ce qu'on montre dans le cas de la résolution d'équations diophantienne.

Mais pour s'en convaincre tout de suite, on peut prendre $3 \times 1 - 2 \times 1 = 1 = 3 \times 3 - 2 \times 4$ ou encore $6 \times 1 - 4 \times 1 = 2 = 6 \times 3 - 4 \times 4$.

Proposition 2.6 (Sous-groupe et PGCD) :
Soit $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$.

Alors

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}.$$

Démonstration :
Par définition du pgcd, $(a \wedge b)|a$ et $(a \wedge b)|b$. Donc, d'après 1.4 (caractérisation de la divisibilité par

les sous-groupes), $a\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$ et $b\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$. Donc $a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\mathbb{Z}$ (par structure de groupe).

Par la relation de Bézout, $\exists u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$. Donc $(a \wedge b)\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$. □

Remarque :
En fait, c'est une caractérisation des pgcd, que l'on pourrait prendre comme définition, et qui a l'avantage de redonner très facilement la relation de Bézout. Mais ce n'est pas l'orientation du programme. Donc en fait, on a même $d = a \wedge b \iff a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Proposition 2.7 (Caractérisation du pgcd) :
Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $d \in \mathbb{N}$. Alors

$$d = a \wedge b \iff \begin{cases} d|a \text{ et } d|b \\ \forall \delta \in \mathbb{Z},\ \delta|a \text{ et } \delta|b \implies \delta|d \end{cases}$$

Autrement dit, $a \wedge b$ est le plus petit diviseur commun pour la relation d'ordre partielle $|$ sur $\mathbb{N}$.

Démonstration :
Supposons $d = a \wedge b$. Alors, d'après la relation de Bézout, $\exists u, v \in \mathbb{Z}$ tel que $au + bv = d$. Donc, si $\delta \in \mathbb{Z}$ divise a et b, alors δ divise toute combinaison linéaire et donc en particulier divise d.

Réciproquement, toujours par Bézout, $\exists u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$. Donc si $d|a$ et $d|b$, alors $d|a \wedge b$. Mais, par définition, $a \wedge b$ est un diviseur commun de a et b. Donc, par définition de d, $(a \wedge b)|d$. Donc d et $a \wedge b$ sont associés. Or ils sont positif par définition, et donc $d = a \wedge b$. □

Remarque :
On notera que dans $\mathbb{N}$, 0 est un maximum pour la relation $|$. En effet : $\forall n \in \mathbb{N}$, $n|0$. Donc la caractérisation du pgcd précédente est cohérente avec la convention $0 \wedge 0 = 0$ (le plus grand diviseur commun au sens de la divisibilité).

Remarque :
On vient d'utiliser un lemme tiré de la relation de Bézout : $d \in \mathrm{Div}(a, b) \iff d|(a \wedge b)$. On le reformule un peu différemment :

Corollaire 2.8 (Ensemble des diviseurs communs) :
Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. On note $\mathrm{Div}(a, b)$ les diviseurs communs de a et b. Alors

$$\mathrm{Div}(a, b) = \mathrm{Div}(a \wedge b)$$

Démonstration :
La démonstration est essentiellement contenu dans la remarque précédente. □

Proposition 2.9 (Propriété algébrique de $\wedge$) :
Soit $a, b, c \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$. Alors

(i) Si $c \neq 0$, alors $(ac) \wedge (bc) = |c|(a \wedge b)$.

(ii) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ [*associativité*]

Démonstration :

(i) D'après la relation de Bézout, $\exists u, v \in \mathbb{Z}$ tels que $(ac) \wedge (bc) = acu + bcv = c(au + bv)$. Alors $|c|(a \wedge b)|((ac) \wedge (bc))$. Et de même, par Bézout, $\exists n, m \in \mathbb{Z}$ tels que $an + bm = (a \wedge b)$. Donc $c(a \wedge b) = acn + bcm$. Donc $(ac) \wedge (bc)|(|c|(a \wedge b))$. Donc $(ac) \wedge (bc)$ et $|c|(a \wedge b)$ sont associés. Comme ils sont tous les deux positifs, on en déduit $(ac) \wedge (bc) = |c|(a \wedge b)$.

(ii) Soit $d \in \mathbb{Z}$ tel que $d|(a \wedge b)$ et $d|c$. Alors $d|a$ et $d|b$ et $d|c$. Par associativité de la conjonction logique, on a aussi $d|a$ et $d|(b \wedge c)$. Donc $\mathrm{Div}(a \wedge b, c) = \mathrm{Div}(a, b \wedge c)$ et donc en particulier les pgcd sont égaux (car ce sont les $\max$ de ces ensembles).

□

Définition 2.2 (PGCD de plusieurs entiers) :
Soit $a_1, \ldots, a_n \in \mathbb{Z}$. On définit le pgcd de $a_1, \ldots, a_n$ comme le plus grand diviseurs communs à $a_1, \ldots, a_n$. On le note $\bigwedge_{i=1}^{n} a_i$ et donc $\bigwedge_{i=1}^{n} a_i = \left(\bigwedge_{i=1}^{n-1} a_i\right) \wedge a_n$.

Proposition 2.10 (Généralisation de la relation de Bézout) :
Soit $n \in \geq 2$ et $a_1, \ldots, a_n \in \mathbb{Z}^*$. Alors

$$\exists u_1, \ldots, u_n \in \mathbb{Z},\ \sum_{k=1}^{n} a_k u_k = \bigwedge_{k=1}^{n} a_k.$$

Démonstration :
Il suffit de faire une récurrence. On sait que c'est vrai pour $n = 2$ par Bézout.

Par Bézout, $\exists u, v \in \mathbb{Z}$ tel que $u(a \wedge b) + cv = a \wedge b \wedge c$. Et $\exists n, m \in \mathbb{Z}$ tels que $a \wedge b = an + bm$. Donc $aun + bum + cv = a \wedge b \wedge c$. Et on continue. □

Remarque :
La loi $\wedge$ est donc presque une LCI sur $\mathbb{Z}$. Il y a le problème de 0. Avec la convention $0 \wedge 0 = 0$, $\wedge$ devient une LCI sur $\mathbb{Z}$ commutative associative ayant 0 comme élément neutre. Mais elle n'est pas symétrisable. Ce qui l'empêche de munir $\mathbb{Z}$ d'une structure de groupe pour le pgcd.

2.3 Entiers premiers entre eux

Définition 2.3 (Nombres premiers entre eux) :
Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

On dit que a et b sont *premiers entre eux* si $a \wedge b = 1$, c'est-à-dire s'ils n'ont pas de diviseurs communs positifs autre que 1.

Exemple 2.2 :
35 et 24 sont premiers entre eux.

Exemple 2.3 ([✓]) :
Montrer que $\forall n \in \mathbb{Z}$, n et $n + 1$ sont premiers entre eux.

Proposition 2.11 (Transmission de la primalité relative aux diviseurs) :
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

Si a et b sont premiers entre eux, alors $\forall d \in \mathrm{Div}(a)$, $\forall \delta \in \mathrm{Div}(b)$, d et δ sont premiers entre eux.

Démonstration :
Soit $d \in \mathrm{Div}(a)$ et $\delta \in \mathrm{Div}(b)$. Soit $n = d \wedge \delta$. Alors $n|a$ et $n|b$ par transitivité de la divisibilité. Et donc $n|1$. Donc $n = 1$ car $n \geq 0$. □

Théorème 2.12 (Théorème de Bézout) :
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Alors

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

Démonstration :
Le sens directe est la relation de Bézout qu'on a tiré de l'algorithme d'Euclide.

Réciproquement, si $\exists u, v \in \mathbb{Z}$ tel que $au + bv = 1$. Alors $(a \wedge b)|1$ et donc $a \wedge b = 1$ car $a \wedge b \geq 0$. □

!!! ATTENTION !!!

Le théorème de Bézout n'est valable que pour les entiers premiers entre eux. C'est faux avec un pgcd qui n'est pas 1 ! En général, si $au + bv = d$, alors $(a \wedge b)|d$. et on ne peux pas dire mieux. Mais dans le cas où $d = 1$, il n'y a plus le choix.

Contre-exemple :
On $6 \wedge 4 = 2$ et $3 \times 6 + (-1) \times 4 = 12 \neq 2$. Mais on a bien $2|12$.

Proposition 2.13 (Caractérisation du pgcd par des entiers premiers entre eux) :
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ et $d \in \mathbb{N}$. Alors

$$d = a \wedge b \iff \exists a', b' \in \mathbb{Z},\ a = da',\ b = db',\ a' \wedge b' = 1.$$

Démonstration :
Si $d = a \wedge b$. Alors $\exists u, v \in \mathbb{Z}$ tel que $da'u + db'v = d$. Comme $\mathbb{Z}$ est intègre et $d \neq 0$, on en déduit $a'u + b'v = 1$. Et donc $a' \wedge b' = 1$ par le théorème de Bézout. Ou alors $d = (da') \wedge (b'd) = d(a' \wedge b')$.

Réciproquement, si $\exists a', b' \in \mathbb{Z}$, $a' \wedge b' = 1$ et $a = da'$ et $b = db'$. Alors d est un diviseur commun de a et b. Donc $d|(a \wedge b)$. De plus, par Bézout, $\exists u, v \in \mathbb{Z}$ tels que $a'u + b'v = 1$. Donc $au + bv = d$. Et donc $(a \wedge b)|d$. Par positivité, on en déduit $d = a \wedge b$. □

Proposition 2.14 ("Transmission de la primalité relative") :
Soit $a, b, c \in \mathbb{Z}$, $a \neq 0$. Alors

$$a \wedge (bc) = 1 \iff \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases}$$

Démonstration :
Si $a \wedge (bc) = 1$, alors $\exists u, v \in \mathbb{Z}$ tels que $au + bcv = 1$ par Bézout. Et donc $a \wedge b|1$ donc $a \wedge b = 1$. De même pour $a \wedge c$.

Si $a \wedge b = 1 = a \wedge c$. Alors $\exists u, v, n, m \in \mathbb{Z}$ tels que $au + bv = 1 = an + cm$. Alors

$$1 = (au + bv)(an + cm) = a(anu + cmu + bvn) + bcvm$$

Donc, par théorème de Bézout, $a \wedge (bc) = 1$. □

Théorème 2.15 (Lemme de Gauss) :
Soit $a, b, c \in \mathbb{Z}$, $a \neq 0$.
Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.

Démonstration :
Par Bézout, $\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Donc $acu + bcv = c$. Et donc $a|c$. □

Remarque :
Lemme de Gauss est une sorte de réciproque partielle au point (ii) de la propriété 1.3 des propriétés algébriques de la divisibilité page 4.

Proposition 2.16 :
Soit $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}^*$ et $n \in \mathbb{N}^*$ tels que $c \wedge n = 1$. Alors

$$ac \equiv bc\ [n] \implies a \equiv b\ [n].$$

Démonstration :
En écrivant la définition, $\exists k \in \mathbb{Z}$ tel que $ac = bc + nk$. Donc $c|nk$. Or $n \wedge c = 1$. Donc, par lemme de Gauss, $c|k$. Et donc $\exists p \in \mathbb{Z}$ tel que $a = b + np$. Donc $a \equiv b\ [n]$. □

Proposition 2.17 :
Soit $a, b, c \in \mathbb{Z}$.
Si $a \wedge b = 1$ et $a|c$ et $b|c$, alors $ab|c$.

Démonstration :

Par définition, $\exists k, \ell \in \mathbb{Z}$ tels que $ak = c = b\ell$. Mais $a \wedge b = 1$. Donc, d'après le lemme de Gauss, $a|\ell$. Et donc $ab|c$. □

L'hypothèse de primalité relative entre a et b est essentielle !

Contre-exemple :
On a $4|12$ et $6|12$ mais $24 \nmid 12$.

Théorème 2.18 (Fractions irréductibles) :
Tout rationnel s'écrit de façon unique comme une fraction irréductible, *i.e.*

$$\forall r \in \mathbb{Q},\ \exists!(p,q) \in \mathbb{Z} \times \mathbb{N}^*,\ p \wedge q = 1,\ r = \frac{p}{q}.$$

Démonstration :
Soit $r \in \mathbb{Q}^*$. Alors $\exists a, b \in \mathbb{Z}$ tels que $b \neq 0$ et $r = \frac{a}{b}$. En simplifiant par le pgcd de a et b, alors $\exists a', b' \in \mathbb{Z}$ tels que $r = a'/b'$ et $a' \wedge b' = 1$. Donc sans perte de généralité, $\exists (a', b') \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = a'/b'$ et $a' \wedge b' = 1$.

Si $r = 0$, alors $r = 0/1$ et $0 \wedge 1 = 1$.

Si on a $(a, b), (p, q) \in \mathbb{Z}^* \times \mathbb{N}^*$ tels que $a \wedge b = 1 = p \wedge q$ et $a/b = p/q$, alors $aq = bp$. Donc $q|bp$. Mais $q \wedge p = 1$, donc, par lemme de Gauss, $q|b$. De même, $b|aq$ et $b \wedge a = 1$, donc $b|q$. Or $b, q \geq 0$ et $|$ étant une relation d'ordre sur $\mathbb{N}$, par antisymétrie, $b = q$. Et on a donc immédiatement $a = p$. Dans le cas où $a = 0$, on a automatiquement $b = 1$ et aussi $p = 0$ et $q = 1$. □

Proposition 2.19 (PGCD pour plus que 2 entiers (Rappel)) :
Soit $a, b, c \in \mathbb{Z}^*$. Alors

$$a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c).$$

Démonstration :
Soit d diviseur de a, b, c. En particulier, $d|a$ et $d|b$, donc $d|a \wedge b$. Et $d|c$, donc $d|((a \wedge b) \wedge c)$. D'où la première égalité. Et de même pour la seconde. □

Définition 2.4 (Entiers premiers dans leurs ensembles, Entiers deux à deux premiers) :
Soit $n \geq 2$ et $a_1, \ldots, a_n \in \mathbb{Z}$.

On dit que $a_1, \ldots, a_n$ sont *premiers dans leur ensemble* si $\bigwedge_{k=1}^{n} a_k = 1$, *i.e.* si le seul diviseur commun à tous les a_i est 1.

On dit que $a_1, \ldots, a_n$ sont *premiers entre eux deux à deux* si $\forall i, j \in \{1, \ldots, n\}$, $i \neq j$, $a_i \wedge a_j = 1$.

Il est plus difficile d'être deux à deux premiers entre eux pour des entiers que d'être premier dans leur ensemble. Donc "premier deux à deux $\implies$ premier dans leur ensemble".

Contre-exemple :
$(6, 10, 15)$ sont premiers dans leur ensemble mais pas premiers deux à deux. $(6, 7, 10)$ également.

Proposition 2.20 (Généralisation du théorème de Bézout) :
Soit $a_1, \ldots, a_n \in \mathbb{Z}$.

$a_1, \ldots, a_n$ sont premiers dans leur ensemble si, et seulement si, $\exists u_1, \ldots, u_n \in \mathbb{Z}$ tels que $\sum_{k=1}^{n} a_k u_k = 1$.

Démonstration :
Le sens direct a été vu dans la généralisation de la relation de Bézout.

Réciproquement, si $\sum_{k=1}^{n} a_k u_k = 1$, alors le pgcd divise 1 et donc c'est 1. □

2.4 Équations diophantienne

Diophante d'Alexandrie était un mathématicien de l'antiquité qui a vécu entre le 4eme et le 1er siècle avant JC. Il s'est beaucoup intéressé à l'arithmétique et aux résolutions d'équations à coefficients entiers. On appelle plus généralement équation diophantienne toute équation dans les entiers. Dans le cadre du programme, on ne s'intéressera pas à toutes les équations diophantiennes.

Définition 2.5 (Équation diophantienne (au programme)) :
On appelle *équation diophantienne (au programme)* toute équation de la forme

$$ax + by = c$$

avec $a, b, c \in \mathbb{Z}$.
On s'intéresse aux solutions entières de cette équation (donc aux solutions dans $\mathbb{Z}^2$).

Proposition 2.21 (Existence de solutions) :
Soit $a, b, c \in \mathbb{Z}$.
L'équation diophantienne $ax + by = c$ a des solutions entières si, et seulement si, $(a \wedge b)|c$.

Démonstration :
Soit $d \in \mathbb{Z}$ tel que $c = d(a \wedge b)$. Par Bézout, $\exists u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$. Donc $adu + bvd = c$. Donc (du, dv) est une solution entière de l'équation diophantienne $ax + by = c$.

Réciproquement, si l'équation diophantienne $ax + by = c$ a une solution (entière) et qu'on considère (u, v) une telle solution (donc $u, v \in \mathbb{Z}$ tels que $au + bv = c$), alors $(a \wedge b)|(au + bv)$ et donc $(a \wedge b)|c$. □

Méthode de résolution des équations diophantienne :
On considère l'équation diophantienne $ax + by = c$, avec $a, b, c \in \mathbb{Z}$. On suppose $(a \wedge b)|c$ (pour qu'il existe des solutions).

- On trouve une solution particulière $(x_0, y_0) \in \mathbb{Z}^2$ (en utilisant l'algorithme d'Euclide par exemple).
- On se ramène à une équation diophantienne dont les coefficients sont premiers entre eux en utilisant la solution particulière (*i.e.* on se ramène à $a'(x - x_0) = b'(y_0 - y)$).
- On résout en utilisant le lemme de Gauss.
- Les solutions sont les $\{(x_0 + b'k, y_0 - a'k),\ k \in \mathbb{Z}\}$.

Exemple 2.4 :
Résoudre l'équation $6x + 9y = 12$.

En simplifiant par $3 = 6 \wedge 9$, on a $\forall x, y \in \mathbb{Z}$, $(6x + 9y = 12 \iff 2x + 3y = 4)$.
On a facilement $3 - 2 = 1$. Donc $3 \times 4 + 2 \times (-4) = 4$. Et donc $(-4, 4)$ est une solution de l'équation.
Soit $(x, y) \in \mathbb{Z}^2$ telle que $2x + 3y = 4$. Alors

$$2x + 3y = 4 \iff 2x + 3y = 3 \times 4 - 2 \times 4 \iff 2(x + 4) = 3(4 - y)$$

Donc $2|3(4-y)$. Or 2 et 3 sont premiers entre eux. Donc par lemme de Gauss, $2|4-y$. Donc $\exists k \in \mathbb{Z}$, tel que $4-y=2k$, *i.e.* $\exists k \in \mathbb{Z}$ tel que $y=4-2k$. Alors

$$\begin{aligned} 2x+3y=4 &\iff \exists k \in \mathbb{Z},\ y=4-2k \text{ et } 2(x+4)=3(4-y) \\ &\iff \exists k \in \mathbb{Z},\ \begin{cases} y=4-2k \\ 2(x+4)=6k \end{cases} \\ &\iff \exists k \in \mathbb{Z},\ \begin{cases} y=4-2k \\ x=3k-4 \end{cases} \end{aligned}$$

On peut vérifier : $\forall k \in \mathbb{Z}$, $2(3k-4)+3(4-2k)=-2\times 4+3\times 4=4$.

Donc l'ensemble des solutions entières de l'équation $6x+9y=12$ est

$$\{(3k-4, 4-2k),\ k \in \mathbb{Z}\}$$

Exemple 2.5 :
Résoudre l'équation $12x+14y=6$.

Remarque :
On pourrait formuler un théorème pour donner directement l'ensemble des solutions d'une équation diophantienne. Mais ce qui est attendu c'est la méthode de résolution, donc la démonstration dudit théorème. Il faut donc refaire la démonstration à chaque fois.

La démonstration permet également de pouvoir l'adapter à d'autres situations un peu différentes, ce que ne permet pas d'appliquer une "boîte noire".

Exemple 2.6 :
Résoudre dans $\mathbb{Z}$ l'équation $6xy+4x=3y+5$.

2.5 PPCM

Définition-Propriété 2.6 (PPCM) :
Soit $(a,b) \in \mathbb{Z} \setminus \{(0,0)\}$.

Si $a, b \in \mathbb{Z}^*$, alors l'ensemble des multiples communs de a et b non nuls $\{p \in \mathbb{N}^*,\ a|p,\ b|p\}$ a un minimum pour la relation $\leq$. On appelle alors *plus petit commun multiple de a et b*, noté $\mathrm{ppcm}(a,b)$ ou $a \vee b$, ce minimum, *i.e.*

$$a \vee b = \min\{n \in \mathbb{N}^*,\ a|n,\ b|n\}.$$

Par convention, $a \vee 0 = 0$.

Démonstration :
L'ensemble $\{p \in \mathbb{N}^*,\ a|p,\ b|p\}$ est non vide car $|ab|$ est dedans. C'est un sous-ensemble de $\mathbb{N}^*$. Donc il admet un minimum pour la relation $\leq$. □

Proposition 2.22 (La loi $\vee$ est commutative) :
La loi $\vee$ est une LCI commutative sur $\mathbb{N}$ dont 1 est élément neutre.

Démonstration :
Ça provient de la commutativité de la conjonction logique. Comme pour le pgcd. □

⚠ Le ppcm est le plus petit commun multiple **strictement positif** ! Ne pas oublier que 0 est toujours un multiple commun. Mais précisément comme il est toujours là, il ne donne pas beaucoup d'informations sur a et b.

Ne pas l'oublier toutefois en considérant **les** multiples.

Proposition 2.23 (Caractérisation du ppcm) :
Soit $a, b \in \mathbb{Z}^*$ et $p \in \mathbb{N}^*$. Alors

$$p = a \vee b \iff \begin{cases} a|p \text{ et } b|p \\ \forall m \in \mathbb{Z},\ a|m \text{ et } b|m \implies p|m \end{cases}$$

Démonstration :
Si $p = a \vee b$, alors par définition, $a|p$ et $b|p$. Soit $m \in \mathbb{Z}$ tel que $a|m$ et $b|m$. Alors m est un multiple commun de a et b. Si $m = 0$, on a $p|m$. Supposons $m \neq 0$. Alors $|m|$ est aussi un multiple commun positif de a et b. Alors, par définition de p qui est le plus d'entre eux strictement positif, $p \leq |m|$. En utilisant la division euclidienne, $\exists!(q, r) \in \mathbb{N}^2$ tel que $|m| = pq + r$ et $0 \leq r < p$. Mais $a|m$ et $a|p$, donc $a|r$. De même, $b|r$. Donc r est un multiple commun positif de a et b. Donc, par définition de p, on a $r = 0$ et donc, par caractérisation de la divisibilité par la division euclidienne, $p|m$.

Réciproquement, on a $a \vee b \leq p$ par définition du minimum. Et par définition de p, comme $a \vee b$ est un multiple commun de a et b, on a $p|(a \vee b)$. Mais comme ils sont tous les deux positifs, on en déduit $p \leq a \vee b$. D'où l'égalité par antisymétrie de la relation $\leq$. □

Remarque :
Donc le ppcm est le plus petit des multiples communs au sens de la divisibilité.

Proposition 2.24 (Ensemble des multiples communs par les sous-groupes) :
Soit $a, b \in \mathbb{Z}$. Alors

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

Autrement dit, les multiples communs de a et b sont les multiples de $a \vee b$.

Démonstration :
L'ensemble des multiples de a est $a\mathbb{Z}$ par définition. Donc l'ensemble des multiples commun est $a\mathbb{Z} \cap b\mathbb{Z}$. Mais $a\mathbb{Z} \cap b\mathbb{Z}$ est donc un sous-groupe de $(\mathbb{Z}, +)$. Alors $\exists p \in \mathbb{Z}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = p\mathbb{Z}$. Alors $a \vee b \in p\mathbb{Z}$. Et par définition du minimum, on en déduit $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. □

Remarque :
On peut même en faire une caractérisation du ppcm : $m = a \vee b \iff a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Proposition 2.25 (Propriété algébrique du ppcm) :
Soit $a, b, c \in \mathbb{Z}^*$. Alors

$$(ca) \vee (cb) = |c|(a \vee b)$$

Démonstration :
Sans perte de généralité on peut raisonner sur des entiers naturels, et multiplier par les signes après. $(a \vee b)$ est un multiple commun de a et b, donc $c(a \vee b)$ est un multiple commun de ca et cb. Donc $(ca) \vee (cb) | (c(a \vee b))$.

Réciproquement, si $ca|m$ et $cb|m$, alors $c|m$ et donc $\exists k \in \mathbb{Z}$ tel que $m = ck$. Alors $a|k$ et $b|k$. Donc $a \vee b|k$. Et donc $c(a \vee b)|m$. D'où, par caractérisation, $(ca) \vee (cb) = c(a \vee b)$. □

Proposition 2.26 (Lien entre pgcd et ppcm) :
Soit $a, b \in \mathbb{Z}^*$.

Si $a \wedge b = 1$, alors $a \vee b = |ab|$. Plus généralement :

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

Démonstration :
Supposons $a \wedge b = 1$. Or $a|(a \vee b)$ et $b|(a \vee b)$, donc $|ab||(a \vee b)$. Mais par ailleurs, ab est multiple commun de a et b, donc $(a \vee b)||ab|$. Et donc, par positivité, $|ab| = a \vee b$.

Soit $d = a \wedge b$. Soit $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$ et $a' \wedge b' = 1$. Alors $(a \vee b)(a \wedge b) = d((da') \vee (db')) = d^2(a' \vee b') = d^2 a'b' = ab$. □

3 Les nombres premiers

3.1 L'ensemble des nombres premiers

Définition 3.1 (Nombre premier) :
Un nombre premier est nombre $p \geq 2$ dont les seuls diviseurs sont ses diviseurs triviaux, c'est à dire 1 et lui même. Autrement dit, $p \geq 2$ est premier si $\mathrm{Div}(p) = \{-p, -1, 1, p\}$.

On notera $\mathcal{P}$ l'ensemble des nombres premiers.

!!! ATTENTION !!!

⚠ En dépit de l'opinion populaire, 1 n'est pas un nombre premier. Il est nécessaire d'imposer $p \geq 2$ dans la définition précisément pour ne pas considérer 1 comme un nombre premier. Autoriser 1 a être un nombre premier entraînerait beaucoup d'inconvénients fâcheux. En particulier, certaines unicité disparaîtraient.

Les nombres premiers sont les briques élémentaires qui constituent les entiers. Tous les théorèmes que nous avons vu dans ce chapitre peuvent se redémontrer "facilement" (au pris d'une manipulation un peu fastidieuse de quantificateurs tout de même) une fois le théorème fondamental de l'arithmétique prouvé.

On pourrait avoir envie de commencer par le théorème fondamental de l'arithmétique. Mais la démonstration de ce dernier se fait à partir de toute la mécanique que l'on vient de mettre en place. En commençant par le théorème fondamental de l'arithmétique, on se retrouverait alors avec un argument circulaire. D'où la nécessité de l'étude de la mécanique.

De plus, c'est cette mécanique qu'on utilise en pratique. Et pas la lourdeur du théorème fondamental.

Toutefois, on pourrait, une fois la théorie construite, reprendre et reprouvé tous les théorèmes a posteriori.

!!! ATTENTION !!!

⚠ Le seul nombre premier pair est 2.

Remarque :
On notera que les diviseurs d'un entier vont toujours par pair. Si $d|n$, alors $(n/d)|n$ et $n = d(n/d)$. Bien sûr. Mais lorsque l'on fait parcourir à d les diviseurs de n, n/d va les parcourir également "dans l'autre sens". Autrement dit, lorsque d croît, n/d va décroître.

Il est donc inutile de faire parcourir à d *tous* les diviseurs de n. Seul la première "moitié" suffit, n/d parcourant l'autre moitié. On peut donc imposer à d de parcourir les diviseurs de n tant que son homologues reste plus grand, *i.e.* $d \leq n/d$. Ce qui impose $d^2 \leq n$.

Autrement dit, pour étudier les diviseurs d'un entier, il suffit de se restreindre au diviseurs $\leq \sqrt{n}$.

Ce qui donne naissance à plusieurs tests de primalité. En particulier, il suffit de chercher un diviseurs inférieur à $\sqrt{n}$.

Les tests de primalité ont une importance toute particulière en informatique. Les nombres premiers sont la base (voir entièrement) des cryptage informatique. Les codes bancaires et toutes les informations sensibles sont codées à partir des nombres premiers. Et plus précisément, à partir de la difficulté de trouver les facteur premier d'un entier.

Avec des ressources infinies et un temps illimités, on peut toujours factoriser un entier. La méthode est simple. On test. Si on a le temps, pas de problème. Mais c'est là qu'intervient la complexité informatique. Faire des opérations, ça prend du temps. Pas beaucoup (en fonction de la puissance de l'ordinateur qu'on utilise, mais un petit peu). Plus il y a de tests à faire, plus la factorisation sera donc longue.

Évidemment, et c'est un sujet de recherche très actif, on peut gagner un peu de temps en optimisant les algorithme ou même en choisissant des langages informations spécialement conçus pour et donc plus performant que d'autres (python n'est pas très performant en calculs, ce n'est pas son domaine de prédilection).

Mais la factorisation prend du temps. Avec des nombres suffisamment grand, elle ne peut pas s'effectuer dans un temps raisonnable par rapport à une vie humaine, même avec des super-ordinateur à disposition. C'est ce qui rend les cryptages informatiques sur. La méthode est connue, mais on a pas le temps.

Et c'est aussi ce qui rend la recherche d'outil informatique toujours plus puissant aussi vivace.

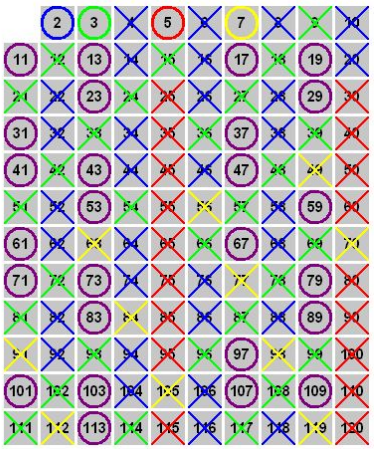
Test de primalité "naïf" :

```python
def est_premier(n) :
    """test de primalité de n """
    if n<2 :
        return False
    k=2
    premier = True
    while k**2<=n and premier : # teste que les entiers <sqrt(n) comme diviseurs potentiels
        premier = (n%k!=0) # devient False si n est divisible par k
        k += 1
    return(premier)
```

Ce test de primalité n'est pas très bon. Sa complexité est assez mauvaise (on $O(\sqrt{n})$ ce qui est assez mauvais).

Crible d'Ératosthène

Le crible d'Ératosthène est un algorithme de recherche de nombre premier. Il consiste à prendre une liste d'entier et d'enlever successivement les multiples de chacun des entier. Les éléments qui restent sont des nombres premiers (s'ils restent, c'est qu'ils ne sont multiples d'aucun entier plus petit qu'eux, et donc ils sont premiers).



Prime numbers

2	3	5	7
11	13	17	19
23	29	31	37
41	43	47	53
59	61	67	71
73	79	83	89
97	101	103	107
109	113		

```python
def Crible(N) :
    """Liste des nombres premiers <= N."""
    estPremier = [True]*(N+1)
    estPremier[0:2]=[False,False] # 0 et 1 ne sont pas premiers
    # A la fin de l'algorithme, on veut que k soit premier ssi estPremier[k]=True
    k=2
    while k<=N :
        m=k
        while m<= N :
            estPremier[m]=False
            m=m+k
        while estPremier[k]==False :
            k=k+1

    while k**2<=N :
        if estPremier[k] : # Si k est premier
            m=k**2 # premier "nouveau" multiple
            while m<=N : # supprime les multiples de k après k
                estPremier[m]=False
                m+=k # passe au multiple de k suivant
        k+=1
    return([k for k in range(1,N+1) if estPremier[k]]
```

Proposition 3.1 (Existence de diviseur premier) :
Soit $n \in \mathbb{Z}$.
Si $|n| \geq 2$, alors n a un diviseur premier.

Démonstration :
Sans perte de généralité, on peut suppose $n \in \mathbb{N}$. Si n est premier, c'est évident.

Supposons que n n'est pas premier. On note $\mathrm{Div}_+(n)$ l'ensemble des diviseurs positifs de n. Alors $\mathrm{Div}_+(n) \setminus \{1, n\}$ n'est pas vide. C'est un sous-ensemble de $\mathbb{N}$. On note $p = \min(\mathrm{Div}_+(n) \setminus \{1, n\})$.

Soit $d \in \mathbb{N}$ tel que $d|p$. Alors, par transitivité, $d|n$. Donc $d \in \mathrm{Div}_+(n)$. Supposons $d \neq 1$. Alors $d \in \mathrm{Div}_+(n) \setminus \{1, n\}$ (car $d \leq p < n$). Et donc $p \leq d$ car p est le minimum. Mais $d|p$, donc $d \leq p$ car $p, d \in \mathbb{N}$. D'où $p = d$. Et donc les seuls diviseurs de p sont 1 ou p. Donc par définition, p est premier. □

Corollaire 3.2 (Caractérisation des entiers premiers entre eux par leurs diviseurs premiers) :
Soit $a, b \in \mathbb{Z}$.

a et b sont premiers entre eux si, et seulement si, ils n'ont pas de diviseurs communs premiers.

Démonstration :
C'est assez évident. Si a est b sont premiers entre eux, alors $a \wedge b = 1$ et donc ils n'ont pas de diviseurs premiers en communs.

Si a et b n'ont pas de diviseurs premiers en communs, alors $a \wedge b$ n'est divisible par aucun nombre premier et donc $a \wedge b = 1$. □

Théorème 3.3 (Infinité des nombres premiers [✓]) :
Il y a une infinité de nombres premiers.

Démonstration :
Raisonnons par l'absurde. Supposons que $\mathcal{P}$ soit fini. On pose $N = 1 + \prod_{p \in \mathcal{P}} p$. Alors $N \geq 2$ car $\forall p \in \mathcal{P}$, $p \geq 1$. Donc, d'après la propriété précédente, N a un diviseur premiers $p \in \mathcal{P}$. Donc $p|N$. Et donc $p|1$. ☠. Donc $\mathcal{P}$ n'est pas fini. □

Proposition 3.4 :
Soit $n \in \mathbb{Z}$ et $p \in \mathcal{P}$.

Alors $p|n$ ou $p \wedge n = 1$.

Démonstration :
On pose $d = n \wedge p$. Alors $d|p$. Donc $d \in \{1, p\}$. □

Proposition 3.5 (Lemme d'Euclide) :
Soit $p \in \mathcal{P}$ et $a, b \in \mathbb{Z}$.
Si $p|ab$, alors $p|a$ ou $p|b$.

Démonstration :
Si $p \not| a$, alors $p \wedge a = 1$, et donc, par lemme de Gauss, $p|b$. □

!!! ATTENTION !!!

C'est faux si p n'est pas premier : $6|4 \times 3$ et $6 \not| 4$ et $6 \not| 3$.

Remarque :
En particulier, si $p|n^2$, alors $p|n$.

Exemple 3.1 :
Montrer que $7|x$ et $7|y \iff 7|x^2 + y^2$.

Proposition 3.6 :
Soit $p \in \mathcal{P}$ et $a_1, \ldots, a_n \in \mathbb{Z}$. Alors

$$p \left| \prod_{k=1}^{n} a_k \iff \exists k \in \{1, \ldots, n\},\ p|a_k \right.$$

Démonstration :
Le sens indirecte est évident. Pour le sens direct, on va raisonner par contraposée. On va donc montrer que si $\forall k \in \{1, \dots, n\},\ p \nmid\ a_k$, alors $p \nmid\ \prod_{k=1}^{n} a_k$.

p étant premier, si $\forall k \in \{1, \dots, n\},\ p \nmid\ a_k$, alors $\forall k \in \{1, \dots, n\},\ p \wedge a_k = 1$. Et donc $p \wedge \prod_{k=1}^{n} a_k = 1$. Comme p est premier, on a donc $p \nmid\ \prod_{k=1}^{n} a_k$. □

Remarque :
Autrement dit, les nombres premiers sont les briques élémentaires qui constituent les entiers. On ne peut les séparés en petit morceaux éparpillés à droite ou à gauche. Par exemple, $6|(4 \times 9)$ mais $6 \nmid\ 4$ et $6 \nmid\ 9$. Parce que 6 peut être décomposés en briques élémentaires et qu'elles sont réarrangées à l'intérieur de 4 et 9.

3.2 Théorèmes de Fermat

Lemme 3.7 (Diviseur des coefficients binomiaux) :
Soit p un nombre premier. Alors

$$\forall k \in \{1, \dots, p-1\},\ p \left| \binom{p}{k} \right. .$$

Démonstration :
Soit $k \in \{1, \dots, p-1\}$. Alors (formule du pion)

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Donc $p \left| k\binom{p}{k} \right.$. Mais $k \in \{1, \dots, p-1\}$, donc $k \wedge p = 1$. Sinon p ne serait pas premier. Et donc, par le lemme de Gauss, le résultat. □

Théorème 3.8 (Petit théorème de Fermat) :
Soit p un nombre premier. Alors

$$\forall a \in \mathbb{Z},\ a^p \equiv a\ [p].$$

Démonstration :
On va donner une preuve relativement élémentaire.

On a déjà $1^p \equiv 1[p]$ et $0^p \equiv 0\ [p]$. Supposons qu'il existe $a \in \mathbb{N}$ tel que $a^p \equiv a\ [p]$. Alors, par Newton,

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

D'où le théorème par récurrence.

Il est facile d'étendre le résultat pour $a < 0$: si $a < 0$, on a $-a \in \mathbb{N}$. Donc $a^p \equiv (-1)^p(-a)^p \equiv (-1)^p(-a) \equiv a\ [p]$ car p premier et en utilisant le cas positif au-dessus. De plus, si p est pair, alors $-1 \equiv 1\ [p]$ et donc $(-1)^p(-a) \equiv -a \equiv a\ [p]$. Et si p n'est pas pair, alors $(-1)^p \equiv -1\ [p]$. Et donc le résultat. □

Théorème 3.9 (Petit théorème de Fermat (autre formulation)) :
Soit p un nombre premier et $a \in \mathbb{Z}$. Alors

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

Démonstration :
Cet énoncé est une reformulation exacte de l'énoncé précédent. Autrement dit, il est équivalent au précédent.

En effet, si on suppose 3.8 et si on considère $a \in \mathbb{Z}$ tel que $p \nmid a$, alors $p|a(a^{p-1}-1)$ et $p \wedge a = 1$. Donc par le lemme de Gauss, $p|(a^{p-1}-1)$ et donc 3.9.

Réciproquement, si on suppose 3.9 et qu'on considère $a \in \mathbb{Z}$, alors soit $p|a$ et dans ce cas, $p|a^p$ et donc $a^p \equiv 0 \equiv a\ [p]$; soit $p \nmid a$ et donc $p|(a^{p-1}-1)$ donc $p|(a(a^{p-1}-1))$ et donc 3.8. □

Remarque :
Il existe beaucoup de preuves du petit théorème de Fermat. Certaines utilisant des arguments plus élémentaires que d'autres. Certaines plus savantes que d'autres.

Exemple 3.2 :
Déterminer le reste de la division euclidienne de 2173^{217} par 5.

Exemple 3.3 :
Montrer que si $p \in \mathbb{N}$ est premier, alors $p | 1 + \sum_{k=1}^{p-1} k^{p-1}$.

Théorème (HP) 3.10 (*Dernier (Grand) théorème de Fermat*)

L'équation diophantienne

$$x^n + y^n = z^n$$

n'a pas de solution autre que $(0,0,0)$ *dès que* $n \geq 3$.

Remarque :
Ce théorème a été énoncé par Pierre de Fermat dans la marge d'un de ses livres. Il a écrit précisément :

> *"J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir."* *(Pierre de Fermat – 1665)*

Cette citation est très connue dans le monde des mathématiques. En partie parce que la démonstration a résisté aux assauts des mathématiciens pendant 3 siècles et n'a été prouvé qu'en 1994 par Andrew Wiles.

Ce théorème est très connu à cause de la simplicité de son énoncé assez élémentaire qui peut être compris même par des collégiens, malgré une démonstration très complexe.

La démonstration d'Andrew Wiles utilise les courbes elliptiques définies sur le corps $\mathbb{Q}$. Il faut donc des outils de mathématiques avancées pour démontrer ce résultat élémentaire. Cette confrontation entre un énoncé d'apparence simple et une preuve sophistiquée est assez courante en théorie des nombres et en arithmétique, ce qui en fait à la fois un domaine fascinant et difficile d'accès.

3.3 Théorème fondamental de l'arithmétique

Théorème 3.11 (Théorème fondamental de l'arithmétique) :
Soit $n \geq 2$. Alors $\exists! r \in \mathbb{N}$, $\exists!(p_1, \ldots, p_r) \in \mathcal{P}^r$ tel que $p_1 < p_2 < \cdots < p_r$ et $\exists!(\alpha_1, \ldots, \alpha_r) \in (\mathbb{N}^*)^r$ tels que

$$n = \prod_{k=1}^{r} p_k^{\alpha_k}$$

Autrement dit, tout entier non nul se décompose de manière unique (à l'ordre des facteurs près) comme un produit de nombres premiers.

Démonstration (Esquisse) *:*
On va faire une récurrence forte.

C'est vrai pour $n = 2$ avec $r = 1$, $p_1 = 2$ et $\alpha_1 = 1$.

Supposons qu'il existe un entier $n \in \mathbb{N}^*$ tel que la proposition soit vraie pour tout entier $m \leq n$. Alors $n+1 \geq 2$ a donc un diviseur premier p. Alors $n+1 = pn'$. Et $p \geq 2$, donc $n' \leq (n+1)/2 < n+1$. Donc $n' \leq n$. On applique l'hypothèse de récurrence à n'. Puis on multiplie par p pour avoir la forme annoncée.

On vient donc de démontrer la décomposition en produit de facteurs premiers par récurrence forte.

Reste l'unicité. Supposons qu'il y ait deux écritures. Alors tous les nombres premiers d'une écriture divisent l'autre écriture. Et par primalité, on en déduit que l'ensemble des premiers des deux écritures sont les mêmes. Ce qui impose en particulier qu'il y a autant de nombres premiers qui apparaissent. On a donc l'unicité de r et des nombres premiers. Il reste les puissances. Mais $\alpha_k = \max\{j \in \mathbb{N},\ p_k^j | n\}$ est unique. □

Remarque :
Dans l'énoncé précédent, on est pas obligé d'imposer $p_1 < p_2 < \cdots < p_n$ pour demander simplement à ce que les premiers soient deux à deux distincts. On aboutit à la même forme, toujours unique à ordre des facteurs près, à cause de la commutativité du produit.

Mais comme sur $\mathbb{Z}$ on a une relation d'ordre totale avec l'inégalité, on peut donc imposer l'ordre des facteurs. Ce qui permet d'avoir une écriture unique.

Exemple 3.4 :
$\overline{2025 = 3^4 \times 5^2}$.

Ce théorème est très important. Il permet de mieux "voir" ce qu'est un nombre entier.

On peut alors reformuler beaucoup plus simplement tous ce qui a été vu plus haut, notamment le pgcd et le ppcm.

3.4 Valuation p-adique

Définition-Propriété 3.2 (Valuation p-adique) :
Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}^*$.

On appelle *valuation p-adique* de n, la plus grande puissance de p qui divise n, *i.e.*

$$v_p(n) := \max\{k \in \mathbb{N},\ p^k | n\} \in \mathbb{N}$$

Démonstration :
On a $0 \in \{k \in \mathbb{N},\ p^k | n\}$ donc cet ensemble est non vide. C'est un sous-ensemble de $\mathbb{N}$ par définition et il est majoré par $\left\lfloor \frac{\ln(n)}{\ln(p)} \right\rfloor$. Donc il a un maximum. □

Remarque :
On peut donner une expression de la valuation p-adique :

$$v_p(n) = \log_p(n)$$

mais ce n'est pas très pratique. Il n'est pas dit ce que soit effectivement un entier.

Proposition 3.12 (Reformulation du théorème fondamental à l'aide des valuations) :
Soit $n \in \mathbb{N}^*$. Alors

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

Démonstration :
On utilise le théorème fondamental. Soit $r \in \mathbb{N}$, $p_1, \ldots, p_r \in \mathcal{P}$ avec $p_1 < p_2 < \cdots < p_r$, $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ tel que

$$n = \prod_{k=1}^{r} p_k^{\alpha_k}.$$

Alors, par définition, $\forall k \in \{1, \ldots, r\}$, $v_{p_k}(n) = \alpha_k$. Et pour $p \in \mathcal{P}$, $p|n \iff p \in \{p_1, \ldots, p_r\}$. D'où l'écriture.

De plus, si $p \nmid n$, alors $v_p(n) = 0$. Et donc la deuxième écriture. □

Proposition 3.13 (Propriété algébrique de la valuation) :
Soit $n, m \in \mathbb{Z}^*$ et $p \in \mathcal{P}$.

(i) $v_p(n) \neq 0 \iff p|n$

(ii) $v_p(nm) = v_p(n) + v_p(m)$

(iii) $n|m \iff \forall q \in \mathcal{P},\ v_q(n) \leq v_q(m)$

(iv) $v_p(n \wedge m) = \min(v_p(n), v_p(m))$ et $v_p(n \vee m) = \max(v_p(n), v_p(m))$.

Démonstration :

(i) Évident

(ii) On a $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$ et $m = \prod_{p\in\mathcal{P}} p^{v_p(m)}$. Alors $nm = \prod_{p\in\mathcal{P}} p^{v_p(n)+v_p(m)}$ (car c'est en réalité un produit fini). Puis l'unicité dans le théorème fondamental fourni l'égalité voulue.

(iii) Si $\forall q \in \mathcal{P}$, $v_q(n) \leq v_q(m)$, alors, en utilisant le théorème fondamental, $n = \prod_{q\in\mathcal{P}} q^{v_q(n)} | \prod_{q\in\mathcal{P}} q^{v_q(m)} = m$.

Et si $n|m$, alors $\exists k \in \mathbb{Z}$ tel que $m = nk$. Alors $\forall q \in \mathcal{P}$, $v_q(m) = v_q(n) + v_q(k) \geq v_q(n)$ en utilisant le point précédent.

(iv) $n \wedge m$ est un diviseur commun de n et m. Donc d'après le point précédent, $v_p(n \wedge m) \leq v_p(n)$ et $v_p(n \wedge m) \leq v_p(m)$. Donc, $v_p(n \wedge m) \leq \min(v_p(n), v_p(m))$. De plus, $\min(v_p(n), v_p(m)) \leq v_p(n)$ donc $p^{\min(v_p(n),v_p(m)}$ est un diviseur de $p^{v_p(n)}$ et donc aussi de n. De même $p^{\min(v_p(n),v_p(m))}$ est un diviseur de m. Donc $p^{\min(v_p(n),v_p(m))}$ est un diviseur de $n \wedge m$. Donc, d'après le point précédent, $\min(v_p(n), v_p(m)) \leq v_p(n \wedge m)$. D'où légalité.

On peut procéder de façon similaire pour le ppcm, ou alors, en écrivant $(n \wedge m)(n \vee m) = |nm|$ et en utilisant le point (ii) et le fait que $\min(a, b) + \max(a, b) = a + b$.

□

Exemple 3.5 :

1. Montrer que si $p \in \mathcal{P}$, alors $\sqrt{p} \notin \mathbb{Q}$.
2. Montrer que si $n \in \mathbb{N}$, alors $\sqrt{n} \in \mathbb{Q}$ si, et seulement si, n est un carré parfait.

3.5 Retour sur les diviseurs

Proposition 3.14 (Nombre de diviseurs) :
Soit $n \in \mathbb{N}^*$.

Le nombre de diviseurs positifs de n est

$$\prod_{\substack{p\in\mathcal{P}\\ p|n}} (1 + v_p(n)).$$

Démonstration :
Pour fabriquer un diviseur de n, il faut et il suffit de choisir des puissances dans les facteurs premiers de n. Or $m|n \iff \forall p \in \mathcal{P},\ v_p(m) \leq v_p(n)$. Donc, pour chaque premier p divisant n, on peut choisir une valuation entre 0 et $v_p(n)$. D'où le résultat. □

Autrement dit, $\mathrm{Card}(\mathrm{Div}_+(n)) = \prod_{\substack{p\in\mathcal{P}\\ p|n}} (1 + v_p(n))$.

Remarque :
On peut enlever la condition $p|n$ dans le produit. En effet, si $p \nmid n$, alors $v_p(n) = 0$ et donc on multiplie par 1. Donc enlevant cette condition, on se retrouve avec un produit en apparence infini, mais qui est, en fait, fini puisqu'il y aura un nombre fini de facteur qui ne seront pas des 1 (pour les premiers divisant n).

Exemple 3.6 :
Trouver le nombre de facteur non-premiers de 1200.

Proposition 3.15 (Somme des diviseurs positifs) :
Soit $n \in \mathbb{Z}^*$.

La somme $\sigma(n)$ des diviseurs positifs de n est

$$\sigma(n) := \sum_{d\in\mathrm{Div}_+(n)} d = \prod_{\substack{p\in\mathcal{P}\\ p|n}} \frac{p^{v_p(n)+1} - 1}{p - 1}.$$

Démonstration :
Soit $p_1, \dots, p_N \in \mathcal{P}$ les diviseurs premiers de n. Alors, par théorème fondamental de l'arihmétique, $\forall d \in \mathrm{Div}_+(n)$, $\forall k \in \{1, \dots, N\}$, $\exists \alpha_k \in \{0, \dots, v_{p_k}(n)\}$ tels que

$$d = \prod_{k=1}^{N} p_k^{\alpha_k}.$$

Et donc

$$\begin{aligned}
\sigma(n) &= \sum_{\alpha_1=0}^{v_{p_1}(n)} \sum_{\alpha_2=0}^{v_{p_2}(n)} \cdots \sum_{\alpha_N=0}^{v_{p_N}(n)} p_2^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N} \\
&= \left(\sum_{\alpha_1=0}^{v_{p_1}(n)} p_1^{\alpha_1} \right) \left(\sum_{\alpha_2=0}^{v_{p_2}(n)} p_2^{\alpha_2} \right) \cdots \left(\sum_{\alpha_N=0}^{v_{p_N}(n)} p_N^{\alpha_N} \right) \\
&= \prod_{k=1}^{N} \frac{p_k^{v_{p_k}(n)+1} - 1}{p_k - 1}.
\end{aligned}$$

D'où la formule annoncée. □

Proposition 3.16 (Expression à l'aide de la valuation du ppcm et pgcd) :
Soit $n, m \in \mathbb{Z}^*$. Alors

$$n \wedge m = \prod_{p \in \mathcal{P}} p^{\min(v_p(n), v_p(m))} \qquad \text{et} \qquad n \vee m = \prod_{p \in \mathcal{P}} p^{\max(v_p(n), v_p(m))}$$

Exemple 3.7 :
Si $a = 2520 = 2^3 \times 3^2 \times 5 \times 7$ et $b = 882 = 2 \times 3^2 \times 7^2$, alors $a \wedge b = 126 = 2 \times 3^2 \times 7$ et $a \vee b = 17640 = 2^3 \times 3^2 \times 5 \times 7^2$.