Chapitre 1

Divisibilité et primalité

1.1 Introduction historique

Μονας εστι, καθ νη εκαστον των οντων εν λεγεται.

(L'unité est selon quoi tout ce qui existe est dit un.)
Euclide - Éléments L.VII (300 av. J.C.)

1.1.1 Des éléments d'Euclide...

Vers 290 av. J.C., **Euclide**, à Alexandrie, rassemble en un vaste traité formé de 13 livres et appelé les Éléments ($\Sigma\tau o\iota\kappa\epsilon\iota\alpha$) l'essentiel des connaissances mathématiques de son temps. Non seulement il fait oeuvre encyclopédique en accumulant dans un seul ouvrage tout le savoir arithmétique et géométrique des Grecs, mais surtout il ordonne ce savoir selon un enchainement logique, en distinguant définitions, postulats et axiomes, et propositions, donnant ainsi aux mathématiques l'apparence logique qu'on lui connaît aujourd'hui.

Dans les livres VII à X, Euclide démontre que tout nombre peut être égalé au produit de ses facteurs premiers, autrement appelé le théorème fondamental de l'arithmétique. En s'appuyant sur ce résultat, il démontre également qu'il existe une infinité de nombre premiers. Ses livres seront utilisé pour l'enseignement des mathématiques jusque dans la seconde moitié du XXème siècle (comme l'Organon d'Aristote pour la Logique).

1.1.2 ... au passe-temps de Fermat

Né au début du XVIIème siècle, **Pierre de Fermat** est un magistrat français qui a sans doute découvert les mathématiques en étudiant les Éléments d'Euclide. Profil particulier de notre histoire scientifique, ce dernier aura dévoué sa vie au droit mais correspond avec de nombreux mathématiciens de son époque, jusqu'à publier quelques unes de ses trouvailles et donner son nom à de nombreux théorème d'arithmétique, dont le petit théorème de Fermat qui sera étudié cette année.

Son grand théorème est particulièrement connu pour avoir été énoncé en 1621 par Fermat, non démontré alors que selon lui il avait une « démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir », et demandera ensuite 3 siècles de travail pour finalement être prouvé en 1995. De nombreux problèmes persistent encore dans ce domaine ouvert par Euclide, qui aura offert une richesse de résultats remarquable.

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

1.2 Divisibilité dans $\mathbb{Z}$

Définition : Soient a et b deux entiers relatifs.
On dit que a **divise** b, noté $a|b$, si et seulement si il existe $k \in \mathbb{Z}$ tel que :

$$b = ka$$

Ainsi, on dit que a est un **diviseur** de b, ou que b est un **multiple** de a.

ex : On peut voir par exemple que :

$$7|63 \quad car : \ 63 = 7 \times 9$$

Ou bien :

$$\forall n \in \mathbb{N}, \ 3|6n + 9n^2 \quad car : \ 6n + 9n^2 = 3 \times (2n + 3n^2)$$

♡ **Remarque :** On sait que les entiers pairs sont divisibles par 2 et les impairs divisibles par 2 si on leur ajoute 1, on en déduit :

$$n \in \mathbb{Z} \text{ est pair} \Leftrightarrow \exists k \in \mathbb{Z}, \ n = 2k$$
$$n \in \mathbb{Z} \text{ est impair} \Leftrightarrow \exists k \in \mathbb{Z}, \ n = 2k + 1$$

Proposition 1 : Soient a, b et c trois entiers relatifs. On a alors :
- Si $a|b$ et $b|c$, alors $a|c$.
- Si $a|b$ et $a|c$, alors pour tout u et v entiers relatifs, $a|(ub + vc)$.
- Si $a|b$, alors $a|(a + b)$ et $a|(a - b)$.

∘ Démonstration :

— Supposons que $a|b$ et $b|c$. Alors il existe k et k' deux entiers relatifs tels que :

$$b = ka \ \text{ et : } \ c = k'b$$

donc $c = (k'k) \times a$, ce qui justifie que $a|c$.

— Supposons que $a|b$ et $a|c$. Alors il existe k et k' deux entiers relatifs tels que :

$$b = ka \ \text{ et : } c = k'a$$

Ainsi pour tout u et v entiers relatifs, on constate que :

$$\begin{aligned} ub + vc &= uka + vk'a \\ &= (uk + vk') \times a \end{aligned}$$

donc $a|(ub + vc)$.

— On applique la propriété précédente avec $c = a$, $u = -1$ ou $u = 1$, et $v = 1$.

1.3 Division euclidienne

Théorème 1 : Division Euclidienne dans $\mathbb{Z}$:
Soient a un entier relatif et b un entier naturel tels que $b \neq 0$. Alors il existe un unique couple d'entiers (q, r) (où $q \in \mathbb{Z}$ et $r \in \mathbb{N}$) tel que :

$$a = bq + r \text{ où : } \ 0 \leqslant r < b$$

On appelle q **quotient de la division euclidenne de** a **par** b et r **reste de la division euclidienne de** a **par** b. On appelle également a **dividende** et b **diviseur** de cette divison euclidienne.

∘ Démonstration : On s'intéresse premièrement au cas où $a \geqslant 0$.

— **Existence**
On appelle partie entière d'un réel x l'entier n tel que : $n \leqslant x < n+1$. On la note $n = E(x)$.
Posons alors :

$$q = E(\frac{a}{b})$$

On sait que $\frac{a}{b} \geqslant 0$ donc $E(\frac{a}{b}) \geqslant 0$. Ainsi :

$$0 \leqslant q \leqslant \frac{a}{b} < q+1$$

Or b étant strictement positif, on en déduit que :

$$qb \leqslant a < qb + b$$

et vient :

$$0 \leqslant a - qb < b$$

Ainsi, si on pose $r = a - qb$, on constate que $0 \leqslant r < b$ et que :

$$a = qb + r$$

— **Unicité**
Supposons qu'il existe deux couples (q, r) et (q', r') satisfaisant les conditions de la division euclidienne, autrement dit :

$$\begin{cases} a = bq + r \text{ et : } 0 \leqslant r < b \\ a = bq' + r' \text{ et : } 0 \leqslant r' < b \end{cases}$$

On constate alors que :

$$\begin{aligned} bq + r &= bq' + r' \\ \Rightarrow b(q - q') &= r' - r \\ \Rightarrow b|(r' - r) & \end{aligned}$$

et de plus nécessairement $r' - r < b$, ce qui n'est possible que si $r' - r = 0$, donc $r' = r$. Sachant alors que b est non nul, on en déduit que $q = q'$, ce qui prouve l'unicité.

Dans le cas où $a < 0$, on pose simplement :

$$a' = a(1-b) > 0 \text{ car } b \text{ est un entier naturel non nul}$$

Ainsi on applique le théorème à a' afin d'obtenir un unique couple (q', r) où :

$$a' = q'b + r \text{ et : } 0 \leqslant r < b$$

Autrement dit :

$$\begin{aligned} a(1-b) &= q'b + r \\ a &= ab + q'b + r \\ &= (a + q')b + r \end{aligned}$$

On pose alors $q = q' + a$ et par unicité de q' on a l'unicité de q.

□

1.4 Primalité

Définition : On appelle **nombre premier** tout entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

ex : On peut déterminer les nombres premiers parmi les 100 premiers entiers naturels à l'aide du crible d'Eratosthène : en partant de 2, on élimine successivement les multiples des nombres premiers que l'on trouve (voir l'image en introduction). On en déduit la liste des nombres premiers jusqu'à 100 :

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

Proposition 2 :
Tout entier n supérieur ou égal à 2 admet un diviseur premier. En particulier, si n n'est pas premier il admet un diviseur premier inférieur ou égal à $\sqrt{n}$.

∘ Démonstration : On procède par récurrence sur n. Pour tout $n \in \mathbb{N}$ avec $n \geqslant 2$, on note :

$$P_n \ : \ \text{« Tout entier naturel compris entre 2 et } n \text{ admet un diviseur premier. »}$$

— **Initialisation :** On constate que 2 est divisble par 2 qui est premier, donc P_2 est vraie.

— **Hérédité :** Soit $k \geqslant 2$ un entier. Supposons que P_k est vraie. On considère alors le nombre $k+1$, selon deux cas de figure :

— Si $k+1$ est premier, alors il est divisible par $k+1$ qui est premier.

— Si $k+1$ n'est pas premier, alors il admet au moins deux diviseurs qu'on notera a et b, tels que $k+1 = ab$. On remarque premièrement que a ou b est inférieur ou égal à $\sqrt{k+1}$, car sinon :

$$k+1 = ab > \sqrt{k+1} \times \sqrt{k+1} = k+1$$

ce qui est absurde.
Or a étant inférieur ou égal à k, et P_k étant vraie, il existe p premier inférieur ou égal à a (donc à $k+1$) qui divise $k+1$. Ainsi P_{k+1} est vraie. On peut choisir a ou b pour avoir $p \leqslant \sqrt{k+1}$.

— **Conclusion :** Pour tout entier naturel n supérieur ou égal à 2, les entiers naturels compris entre 2 et n admettent un diviseur premier. En particulier si ces entiers naturels sont non premiers ils admettent un diviseur premier inférieur ou égal à leur racine carrée.

□

Proposition 3 :

Il existe une infinité de nombres premiers.

∘ Démonstration :
On procède par l'absurde. Supposons qu'il existe un nombre fini de nombre premiers, on note alors p le plus grand d'entre eux. On pose :

$$N = 2 \times 3 \times ... \times p + 1$$

Autrement dit $N-1$ est le produit de tous les nombres premiers qui existent. On a alors deux possibilités :

— Si N est premier, alors c'est un nombre premier supérieur à p ce qui est absurde.

— Si N n'est pas premier, alors il est divisible par un nombre x premier. Or si x est plus petit que p, alors il apparait dans le produit $2 \times 3 \times ... \times p$ et donc le reste de la division euclidienne de N par x est nécessairement 1, ce qui est impossible car N est divisible par x. On en déduit donc que x est un nombre premier supérieur à p, ce qui est absurde.

p ne peut donc pas être le plus grand des nombres premier, on en déduit enfin que l'ensemble des nombres premiers est infini.

□

Lemme d'Euclide :

Soient a, b et p trois entiers tels que p est premier.

Si p divise ab, alors p divise a ou p divise b.

∘ Démonstration : On procède par l'absurde :
Supposons que p divise ab, mais que p ne divise pas a et p ne divise pas b.
Ainsi, la division euclidienne de a et b par p implique l'existence de q, $q' \in \mathbb{N}^*$ et α, $\beta \in \mathbb{N}^*$ tels que $0 < \alpha < p$ et $0 < \beta < p$ et :

$$\begin{cases} a = pq + \alpha \\ b = pq' + \beta \end{cases}$$

On constate alors que $\alpha\beta$ est divisible par p, car :

$$\begin{aligned} ab &= (pq+\alpha)(pq'+\beta) \\ &= p(pqq' + q\beta + q'\alpha) + \alpha\beta \\ \text{d'où : } \alpha\beta &= ab - p(pqq' + q\beta + q'\alpha) \end{aligned}$$

puis on applique la proposition 1.
Sachant ceci, pour un α fixé, on sait donc qu'il existe un $\beta < p$ tel que p divise $\alpha\beta$. L'ensemble des β

qui admettent cette propriété admet donc forcément **un plus petit élément**, qu'on note β_0. β_0 étant plus petit que p, la division euclidienne de p par β_0 implique l'existence de m et r deux entiers tels que $r < \beta_0$, où r est non nul car p est premier (il n'est divisible que par 1 ou par lui-même) et :

$$p = \beta_0 m + r$$

Ainsi :

$$\begin{aligned} r &= p - \beta_0 m \\ \Rightarrow\ \alpha r &= \alpha p - \alpha\beta_0 m \end{aligned}$$

Or $\alpha\beta_0$ est divisible par p donc d'après la proposition 1 αr est divible par p, ce qui est absurde car $r < \beta_0$.

La supposition initiale est donc fausse, ce qui prouve que p divise a ou p divise b.

□

Théorème fondamental de l'arithmétique :

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

Autrement dit, pour tout entier $N \geqslant 2$, il existe $k \in \mathbb{N}$ nombres premiers p_i (où $i \in [\![1; k]\!]$) et k entiers naturels α_i (où $i \in [\![1; k]\!]$) tels que :

$$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k}$$

On sait par ailleurs que N admet précisément $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$ diviseurs.

∘ Démonstration : On démontre tout d'abord l'existence de la décomposition puis son unicité.

— **Existence :**

On procède par récurrence forte en considérant pour tout $n \geqslant 2$ la propriété :

$$P_n : \text{« L'entier admet une décomposition en facteurs premiers. »}$$

Initialisation : On a immédiatement $2 = 2^1$ donc 2 est admet une décomposition.
Hérédité : Soit $k \geqslant 2$ un entier. On suppose que P_i est vraie pour tout $i \in [\![1; k]\!]$.
On considère alors l'entier $k + 1$:

- Si $k + 1$ est premier, alors il a pour décomposition $k + 1 = (k + 1)^1$.
- Si $k + 1$ n'est pas premier, alors il admet deux diviseurs différents de 1 ou de $k + 1$, qu'on notera a et b tels que :

$$k + 1 = ab$$

Or a et b sont inférieurs ou égaux à k, ils admettent donc tous les deux une décomposition en facteurs premiers, et leur produit reste une décomposition en facteurs premiers. D'où la décomposition pour $k + 1$.

Conclusion : Tout entier supérieur ou égal à 2 admet une décomposition en facteurs premiers.

— **Unicité :**

Soit n un entier supérieur ou égal à 2 tel que n admet deux décompositions différentes selon les hypothèses de l'énoncé :

$$\begin{aligned} n &= p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k} \\ \text{ou : } n &= q_1^{\beta_1} \times q_2^{\beta_2} \times ... \times q_{k'}^{\beta_{k'}} \end{aligned}$$

Pour tout premier p_i (où $i \in [\![1; k]\!]$) issu de la première décomposition de n, ce p_i divise n et divise alors la seconde décomposition. Or selon le lemme d'Euclide, il existe donc au moins un q_j (où $j \in [\![1; k']\!]$) tel que p_i divise q_j.

Les deux étant premiers, on a donc forcément $p_i = q_j$.

En procédant de la même façon pour tout i on en déduit que $k = k'$, et que la décomposition est constituée des mêmes nombres premiers, la seule différence pouvant être les exposants. Autrement dit :

$$\begin{aligned} n &= p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k} \\ \text{ou : } n &= p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_k^{\beta_k} \end{aligned}$$

Supposons maintenant que pour un même p_i (où $i \in [\![1;k]\!]$), on a $\alpha_i < \beta_i$. Ainsi :

$$\begin{aligned}\frac{n}{p_i^{\alpha_i}} &= p_1^{\alpha_1} \times ... \times p_{i-1}^{\alpha_{i-1}} \times p_{i+1}^{\alpha_{i+1}} \times ... \times p_k^{\alpha_k} \\ &= p_1^{\beta_1} \times ... \times p_{i-1}^{\beta_{i-1}} \times p_i^{\beta_i - \alpha_i} \times p_{i+1}^{\beta_{i+1}} \times ... \times p_k^{\beta_k}\end{aligned}$$

On constate qu'il n'y a plus de p_i lorsqu'on utilise la première décomposition de n, tandis qu'il y en a encore selon la deuxième.

Autrement dit la deuxième décomposition implique que p_i divise $\frac{n}{p_i^{\alpha_i}}$, ce qui d'après le lemme d'Euclide et la première décomposition implique que p_i divise au moins un nombre premier différent de lui-même, ce qui est absurde.

En procédant de la même façon pour $\alpha_i > \beta_i$, on en déduit donc que $\alpha_i = \beta_i$. Ainsi la décomposition est la même, elle est donc nécessairement unique.

Pour ce qui est du nombre de diviseurs, on le déduit simplement du fait que pour chaque puissance de p_i on a le choix des entiers allant de 0 à α_i, donc $(\alpha_i + 1)$ possibilités, et on conclut sur la formule par dénombrement.

□

<u>ex :</u> *Cette décomposition permet de faire apparaître tous les diviseurs d'un nombre :*

$$84 = 2^2 \times 3 \times 7$$

Ici chaque diviseur de 84 *autre que* 1 *sera une combinaison des facteurs premiers présents dans sa décomposition, on sait également qu'il en existe :*

$$(2+1) \times (1+1) \times (1+1) = 12$$

donc 1, 2, 3, 7, $2^2 = 4$, $2 \times 3 = 6$, $2 \times 7 = 14$, $3 \times 7 = 21$, $2 \times 3 \times 7 = 42$, $2^2 \times 3 = 12$, $2^2 \times 7 = 28$ *et* $2^2 \times 3 \times 7 = 84$.
Cette décomposition est particulièrement pratique pour trouver des facteurs communs dans deux nombres différents, donc simplifier des fractions, factoriser, etc.