CHAPITRE 7

LES NOMBRES PREMIERS

Ératosthène de Cyrène, Grec, a vécu aux alentours de -276/-196
Mathématicien, astronome, géographe et philosophe du III^{e} siècle avant Jésus-Christ, il établit le crible d'Ératosthène, méthode qui permet de déterminer par exclusion tous les nombres premiers. Il travailla sur le problème de la duplication du cube et imagina le mésolabe, instrument propre à connaître les moyennes proportionnelles.

Pierre Simon de Fermat, français, 1601/1608-1665
Philologue, parlant couramment l'italien, l'espagnol, le grec et le latin (indispensable à l'époque pour tout érudit en lettres ou sciences), Fermat fut administrateur au Parlement de Toulouse (l'équivalent d'une cour de justice) puis Conseiller du Roi (1648) à Castres. Ce serviteur de l'État qui assuma les devoirs de sa charge avec rigueur et compétence et quoique mathématicien amateur autodidacte, restera dans la mémoire des hommes comme un des plus grands mathématiciens du XVII^{e} siècle. Il fut un des artisans fondateurs de l'Académie des sciences qui vit officiellement le jour un an après sa mort.
Reprenant les travaux de Diophante d'Alexandrie, traduits et complétés par Bachet de Méziriac, il redora le blason de l'arithmétique en créant la théorie des nombres. Il est connu pour le petit théorème de Fermat (vu dans ce chapitre) et le théorème de Fermat (conjecturé par Fermat et démontré par Wiles).

Les contenus du chapitre
▷ Nombres premiers. Leur ensemble est infini.
▷ Existence et unicité de la décomposition d'un entier en produits de facteurs premiers.
▷ Petit théorème de Fermat.

Les capacités attendues du chapitre
▷ Etablir et utiliser le test de primalité de certains nombres.
▷ Décomposer des nombres entiers en produits de facteurs premiers.

Cours

1. Définition

Définition 1 – Nombre premier

On note $a \in \mathbb{N}$.
On dit que a est **un nombre premier** s'il admet exactement deux diviseurs dans $\mathbb{N}$, 1 et lui-même.

Exemples :
▷ 2, 3, 5, 7, 11, 13 sont des nombres premiers.
▷ 1 n'est pas premier car il admet un seul diviseur entier naturel.
▷ 14 n'est pas premier car il admet 1, 2, 7 et 14 comme diviseurs entiers naturels.

⚠ On note P l'ensemble des nombres premiers.

$$P = \{n \in \mathbb{N} \text{ tels que } n \text{ est un nombre premier}\}$$

Méthode 1 – Trouver tous les nombres premiers inférieurs à 100

Cette méthode se nomme **le crible d'*Ératosthène***.
On écrit tous les nombres entiers naturels de 0 jusqu'à 100.
▷ On commence par barrer le 0 et le 1 qui ne sont pas premiers.
▷ On entoure le 2 qui est premier puis on barre tous les mutliples de 2.
▷ On entoure le 3 puis on barre tous les multiples de 3.
▷ On entoure le 5 puis on barre tous les multiples de 5.
▷ On entoure le 7 puis on barre tous les multiples de 7.
On obtient alors tous les nombres premiers inférieurs 100.

~~0~~	~~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~~

Remarque : Si n est un nombre premier avec $n > 2$ alors n est impair.

Propriété 1 – Diviseur premier

Tout entier naturel n distinct de 1 admet au moins un diviseur premier.

Démonstration

Propriété 2 – Infinité des nombres premiers

L'ensemble P des nombres premiers est infini.

Démonstration

2. Décomposition des nombres entiers

Propriété 3 – Décomposition des entiers en produits de nombres premiers

Tout entier naturel non nul m distinct de 1 se décompose de façon unique sous la forme :

$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_n^{\alpha_n}$$

avec p_i des nombres premiers tels que $0 < p_1 < p_2 < ... < p_n$ et $\alpha_i \in \mathbb{N}^*$

Démonstration

► Existence de la décomposition :
On va faire une récurrence forte sur m (au lieu de supposer la propriété vraie au rang k on suppose qu'elle est vraie à tous les rangs jusqu'à k).
On note $\mathbf{P}_m$ la propriété : "Tout entier naturel k $(2 \leq k \leq m)$ admet une décomposition de la forme $p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_n^{\alpha_n}$."
Initialisation : (Pour $m = 2$)
$2 = 2^1$ donc $\mathbf{P}_2$ est vraie.
Hérédité : on suppose que $\mathbf{P}_k$ est vraie pour tous les rangs inférieur ou égaux à k, montrons que dans ce cas $\mathbf{P}_{k+1}$ l'est aussi.
▷ Si $k+1 \in P$ alors $k+1 = (k+1)^1$ donc $\mathbf{P}_{k+1}$ est vraie.
▷ Si $k+1 \notin P$:
D'après la propriété précédente, $k+1$ admet un diviseur premier p et $k+1 = pq$ avec $q \in \mathbb{N}$ et $2 \leq q \leq k$.

On a $q \neq 0$ car $k+1 \neq 0$ et $q \neq 1$ car $k+1 \in P$.
On applique donc l'hypothèse de récurrence sur q et donc $\mathbf{P}_{k+1}$ est vraie.
Conclusion :
$\left.\begin{array}{l}\mathbf{P}_2 \text{ est vraie} \\ \mathbf{P}_k \text{ implique } \mathbf{P}_{k+1}\end{array}\right\}$ donc tout entier naturel m ($m \geq 2$) admet une décomposition de la forme :

$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n}$$

► Unicité de la décomposition :
D'après le théorème de Gauss, les seuls nombres premiers divisant m sont les p_1, p_2, ..., p_n.
Pour tout $i \in \{1;2;\ldots;n\}$, $p_i^{\alpha_i}$ divise m mais $p_i^{\alpha_i+1}$ ne divise pas m.
En effet, si $p_i^{\alpha_i+1}$ divise m alors il existe $q \in \mathbb{N}$ tel que $m = p_i^{\alpha_i+1} \times q$ et en simplifiant on aurait :
$p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_{i-1}^{\alpha_{i-1}} \times p_{i+1}^{\alpha_{i+1}} \times \ldots \times p_n^{\alpha_n} = p_i \times q$
On aurait donc $p_i = p_k$ avec $k \in \{1;2;\ldots;i-1;i+1;\ldots;n\}$ mais ce n'est pas le cas.
Les α_i sont les exposants des plus grandes puissances de p_i, divisant m.
La décomposition est unique car nous n'avons pas le choix des p_i et des α_i.

Méthode 2 – Décomposer des entiers avec les nombres premiers

Tous les entiers peuvent s'exprimer sous la forme de multiplications de nombres premiers.
Exemple
▷ On veut décomposer le nombre 360 à l'aide des nombres premiers :
360 est divisible par 2 donc $360 = 2 \times 180$
180 est divisible par 2 donc $360 = 2 \times 2 \times 90$
90 est divisible par 2 donc $360 = 2 \times 2 \times 2 \times 45$
45 est divisible par 3 donc $360 = 2^3 \times 3 \times 15$
15 est divisible par 3 donc $360 = 2^3 \times 3^2 \times 5$
Conclusion : $360 = 2^3 \times 3^2 \times 5$

Propriété 4 – Diviseurs et nombres de diviseurs

On note m un entier donc la décomposition en facteurs premiers est

$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n}$$

Les diviseurs positifs de m sont les entiers de la forme

$$m = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_n^{\beta_n}$$

avec pour tout $i \in \{1;2;\ldots;n\}$, $0 \leq \beta_i \leq \alpha_i$.

De plus, le nombre de diviseurs de m est

$$\prod_{i=1}^{n} (\alpha_i + 1) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_n + 1).$$

Démonstration

Il y a deux choses à démontrer :
► Si un nombre positif d divise m alors $d = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_n^{\beta_n}$ avec pour tout $i \in \{1;2;...;n\}$, $0 \leq \beta_i \leq \alpha_i$.

► Si un nombre positif d est égal à $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_n^{\beta_n}$ avec pour tout $i \in \{1;2;...;n\}$, $0 \leq \beta_i \leq \alpha_i$ alors d divise m.

▷ Soit d un diviseur de m supérieur ou égal à 2.
$d \geq 2$ donc d admet un diviseur premier p et donc $p|m$.
Par unicité de la décomposition en produit de facteurs premiers de m, il existe un entier $i \in \{1;2;..;r\}$ tel que $p = p_i$.
Ainsi tout diviseur premier de d est l'un des p_i de la décomposition en produit de facteurs premiers de m. La décomposition en facteurs premiers de d s'écrit donc $d = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_n^{\beta_n}$ avec pour tout $i \in \{1;2;...;n\}$, $0 \leq \beta_i \leq \alpha_i$.

▷ Réciproquement :
Puisque $0 \leq \beta_i \leq \alpha_i$ alors $\alpha_i - \beta_i \geq 0$,
on peut donc écrire :

$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_n^{\alpha_n} = \left(\underbrace{p_1^{\alpha_1-\beta_1} \times p_2^{\alpha_2-\beta_2} \times ... \times p_n^{\alpha_n-\beta_n}}_{\in \mathbb{N}} \right) \times p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_n^{\beta_n}$$

donc $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_n^{\beta_n}$ divise m.

Compte tenu de l'écriture des diviseurs de $m = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_n^{\beta_n}$, pour obtenir un de ces diviseurs, on choisit pour chaque p_i une puissance comprise entre 0 et α_i. Ainsi pour chaque p_i, il y a $(\alpha_i + 1)$ choix possibles, ce qui donne bien $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_n + 1)$ diviseurs de m.

Méthode 3 – Trouver tous les diviseurs d'un nombre

▷ $1960 = 2^3 \times 5 \times 7^2$
1960 admet donc $(3+1)(1+1)(2+1) = 24$ diviseurs qui sont :

1	2	$2^2 = 4$	$2^3 = 8$
$1 \times 5 = 5$	$2 \times 5 = 10$	$2^2 \times 5 = 20$	$2^3 \times 5 = 40$
$1 \times 7 = 7$	$2 \times 7 = 14$	$2^2 \times 7 = 28$	$2^3 \times 7 = 56$
$1 \times 5 \times 7 = 35$	$2 \times 5 \times 7 = 70$	$2^2 \times 5 \times 7 = 140$	$2^3 \times 5 \times 7 = 280$
$1 \times 5 \times 7^2 = 245$	$2 \times 5 \times 7^2 = 490$	$2^2 \times 5 \times 7^2 = 980$	$2^3 \times 5 \times 7^2 = 1960$
$1 \times 7^2 = 49$	$2 \times 7^2 = 98$	$2^2 \times 7^2 = 196$	$2^3 \times 7^2 = 392$

Propriété 5 – Existence d'un diviseur premier

Tout entier naturel, $n \geq 2$ non premier, admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$.

Démonstration

Cette propriété permet de définir un critère de primalité des nombres entiers.
▷ Si aucun des nombres premiers dans $[2;\sqrt{n}]$ ne divise n alors n est premier.

Exemple :
▷ On souhaite savoir si 191 est premier.
$\sqrt{191} \approx 13,82$ on teste donc la divisibilité de 191 avec tous les nombres premiers jusqu'à 13.
Comme 191 n'est pas divisible par 2, 3, 5, 7, 11 et 13 alors 191 est un nombre premier.

3. Petit théorème de Fermat

Propriété 6 – Petit théorème de Fermat

Soit p un nombre premier et a un entier naturel non divisible par p, alors $a^{p-1}-1$ est divisible par p donc

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

Démonstration

p est premier donc il ne divise aucun des nombres de $\{1;2;..;p-1\}$ et comme il ne divise pas a alors p ne divise aucun nombre de $\{a;2a;..;(p-1)a\}$

Démontrons par l'absurde que les restes possibles de la division de a, $2a$, ..., $(p-1)a$ par p sont tous différents.
Supposons que les restes de deux de ces nombres (par division par p) soient identiques alors il existe k et k' dans $\{1;2;...;(p-1)\}$ tel que $ka \equiv r\ [p]$ et $k'a \equiv r\ [p]$

Par différence on obtient que ..... et donc que $(k-k')a$ est divisible par .....
Or $k-k' \in \{.....\}$ ce n'est donc pas possible et la supposition est fausse.
Les restes des divisions de a, $2a$, ...,$(p-1)a$ par p sont tous différents.

Comme les restes possibles de la division de a, $2a$, ..., $(p-1)a$ par p sont tous différents et que a, $2a$, ..., $(p-1)a$ représentent $p-1$ nombres alors les restes sont $1, 2, ..., p-1$.
De plus $a \times 2a \times ... \times (p-1)a = a^{p-1} \times 1 \times 2 \times ... \times (p-1)$
et $a \times 2a \times ... \times (p-1)a \equiv 1 \times 2 \times ... \times (p-1)\ [p]$.
On a donc $a^{p-1} \times 1 \times 2 \times ... \times (p-1) \equiv 1 \times 2 \times ... \times (p-1)\ [p]$.
et donc

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

Propriété 7 – Corollaire du petit théorème de Fermat

Si p est un nombre premier et a un entier naturel quelconque alors $a^p - a$ est divisible par p ou $a^p \equiv a\ [p]$

Démonstration

Raisonnons par disjonction des cas sur a :

▷ Si a est divisible par p alors .....

▷ Si a n'est pas divisible par p, d'après le petit théorème de Fermat, $a^{p-1} \equiv ..... \ [p]$ donc en multipliant par a on obtient $a^p \equiv ..... \ [p]$.

Dans les deux cas, comme $a^p \equiv a\ [p] \Leftrightarrow a^p - a \equiv 0\ [p]$ alors $a^p - a$ est divisible par p.

Propriété 8

Si p est un nombre premier et a un entier naturel alors p divise a ou p et a sont premiers entre eux.

Démonstration

Si p est un nombre premier et a un entier naturel, alors :
▷ Soit $\text{PGCD}(p;a) = 1$ et a et p sont premiers entre eux.

▷ Soit $\text{PGCD}(p;a) \neq 1$ et comme p est premier alors $\text{PGCD}(p;a) = p$ donc $p|a$.

Propriété 9

Si p est un nombre premier et a et b deux entiers alors si $p|ab$ on a $p|a$ ou $p|b$.

Démonstration

On suppose l'existence d'un nombre premier p et d'entiers naturels a et b non divisibles par p tels que $p|ab$.

▷ Pour p et a fixés, on choisit parmi toutes les possibilités de b, la plus petite. On a donc $0 < b < p$ car autrement on peut remplacer b par le reste modulo p. De plus $b \neq 1$ car a n'est pas divisible par p.

▷ On note r le reste de la division euclidienne de p par b donc $r \neq 0$ car p est premier.
On a donc $p = mb + r$ donc $ar = ap - mab$ est un multiple de p. Or $0 < r < p$ donc ar n'est pas un multiple de p et donc il y a une contradiction avec l'hypothèse de départ.

On a donc $p|a$ ou $p|b$.