Chapitre 5
Les nombres premiers

I. Définition et existence

1) Nombre premier dans ℕ

Définition :
Dire qu'un **nombre entier naturel** est **premier** signifie qu'il admet exactement deux diviseurs dans ℕ : 1 et lui-même.

Exemples :
- 0 n'est pas premier car il admet une infinité de diviseurs dans ℕ.
- 1 n'est pas premier car il a un seul diviseur dans ℕ : lui-même.
- 2 est le plus petit nombre premier et le seul qui soit pair.

Remarque :
Un entier naturel n non premier (autre que 1 et 0) est un **nombre composé**.
Il admet au moins un diviseur d, autre que 1 et lui-même, qui vérifie $1<d<n$.
Un tel diviseur est dit **diviseur strict** de l'entier n.

2) Critère de primalité

Propriétés :
n désigne un nombre entier naturel supérieur ou égal à 2.
- n admet un diviseur premier.
- Si n n'est pas premier alors il admet un diviseur premier p inférieur ou égal à $\sqrt{n}$.

Démonstration :
- Soit n un entier naturel, $n \geqslant 2$. Si n est premier, il est un diviseur premier de lui-même.
- Si n n'est pas premier, il admet un diviseur positif autre que 1 et lui-même.
  L'ensemble E des diviseurs positifs, autre que 1 et n, est donc un ensemble d'entiers naturels non vide. Il a donc un plus petit élément que l'on note p.
  On raisonne par l'absurde.
  Si p n'était pas premier, il existerait un diviseur propre d de p qui serait plus petit que p ; comme d diviserait p avec p qui divise n, d diviserait n.
  Donc d serait un élément de E plus petit que p. C'est impossible.
  Donc p est premier et divise n ; par suite il existe un entier q tel que $n=pq$ avec $1<q<n$.
  Donc q est un diviseur propre de n et par conséquent $p \leqslant q$.
  On en déduit que $p^2 \leqslant pq$ soit $p^2 \leqslant n$ et donc $p \leqslant \sqrt{n}$.

Propriété (test de primalité) :
n désigne un nombre entier naturel $n \geqslant 2$.
Si n n'est divisible par aucun nombre premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, alors n est premier.

Démonstration :
Il s'agit de la contraposée de la propriété précédente.

Exemple :
Pour $n=157$, $\sqrt{n} \simeq 12{,}5$.
Les nombres premiers inférieurs à $\sqrt{157}$ sont 2 ; 3 ; 5 ; 7 ; 11.
157 n'est divisible par aucun de ces nombres.
Donc 157 est premier.

- **Calculatrice :**

Crible Ératosthène	Test de primalité	

```
PROGRAM:CRIBLE
:EffListe L1,L2
:Prompt N
:suite(K,K,2,N)→
L1
:2→I
:While I≤ent(√(N
))
:For(J,I,ent(N/I
))
:0→L1(I*J-1)
:End
:I+1→I
:End
:1→R
:For(P,1,N-1)
:If L1(P)≠0
:Then
:L1(P)→L2(R)
:R+1→R
:End
:End
:Disp L2
```

```
PROGRAM:TEST
:Prompt N
:0→T
:For(K,2,ent(√(N
)))
:If N/K=ent(N/K)
:Then
:1→T
:End
:End
:If T=1
:Then
:Disp "NON PREMI
ER"
:Else
:Disp "PREMIER"
:End
```

```
PROGRAM:TEST2
:prgmCRIBLE
:0→T
:1→I
:While L2(I)≤ent
(√(N))
:If N/L2(I)=ent(
N/L2(I))
:Then
:1→T
:End
:I+1→I
:End
:If T=0
:Then
:Disp "PREMIER"
:Else
:Disp "NON PREMI
ER"
:End
```

```
N=?7
        {2 3 5 7}
             Done
prgmCRIBLE
N=?15
 {2 3 5 7 11 13}
             Done
```

```
N=?100
NON PREMIER
             Done
prgmTEST
N=?103
PREMIER
             Done
```

```
prgmTEST2
N=?103
{2 3 5 7 11 13 …
PREMIER
             Done
```

3) Ensemble des nombres premiers

Propriété :
Il existe une **infinité** de nombres premiers.

Démonstration :
On raisonne par l'absurde.
On suppose qu'il existe un nombre fini de nombres premiers p_1, p_2, …, p_n.
On considère le nombre $a=p_1 p_2 \cdots p_n+1$. Ce nombre est supérieur ou égal à 2, il admet donc au moins un diviseur premier p_i parmi les nombres p_1, p_2, …, p_n. Cet entier p_i divise a et divise $p_1 p_2 \cdots p_n$, donc il divise la différence soit 1. C'est impossible.
Ainsi, il existe une infinité de nombres premiers.

4) Divisibilité d'un nombre premier

Propriété :
p est un **nombre premier** et a est un entier **non divisible par *p***.
Alors p et a sont **premiers entre eux**.

Démonstration :
p est un nombre premier donc ses seuls diviseurs sont 1 et p. a n'étant pas divisible par p, des deux diviseurs de p, seul 1 est un diviseur commun à a et p : a et p sont donc premiers entre eux.

Propriété :
p est un nombre **premier**.
- Si p divise le produit ab de deux entiers alors p divise a ou p divise b.
- Si p divise le produit ab de deux nombres premiers alors $p=a$ ou $p=b$.

Démonstrations :
- Si p divise a, le résultat est acquis.
  Si p ne divise pas a, alors d'après le théorème précédent, p est premier avec a. Il divise donc b d'après le théorème de Gauss.
- On a vu que p divise a ou p divise b qui n'admettent que deux diviseurs 1 et eux-mêmes. Comme p est différent de 1, $p=a$ ou $p=b$.

Cas particuliers :
- Si p (premier) divise a^2, alors p divise a et pour tout entier naturel non nul n, si p (premier) divise a^n, alors p divise a.
- Il résulte de cette propriété, par contraposition, qui si p (premier) ne divise pas a, alors p ne divise pas, par exemple a^p.

II. Décomposition en facteurs premiers

1) Existence et unicité d'une décomposition

Théorème fondamental :

Tout entier naturel n supérieur ou égal à 2 se **décompose** en un **produit** de **nombres premiers**.
Cette décomposition est **unique** à l'ordre des facteurs près.
On écrira $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ où $n \geqslant 2$, p_1 , p_2 , …, p_k sont des nombres premiers deux à deux distincts et α_1 , α_2 , …, α_k sont des entiers naturels non nuls.

Démonstration :

- Existence
  Soit n un entier, $n \geqslant 2$. On sait qu'il admet un diviseur premier p_1 . Alors $n = p_1 n_1$ où $1 \leqslant n_1 < n$.
  Si $n_1 = 1$ alors $n = p_1$ et la propriété est démontrée.
  Si $n_1 \neq 1$ alors n_1 admet un diviseur premier p_2 et on a donc $n = p_1 p_2 n_2$ où $1 \leqslant n_2 < n_1$.
  On continue de la même façon tant que le quotient n_i est supérieur à 1.
  On forme ainsi une liste d'entiers n_1 , n_2 , … strictement décroissante et minorée par 1.
  Elle est donc finie (principe de descente infinie), c'est-à-dire qu'à un certain rang on a $n_m = 1$ et donc $n = p_1 p_2 ... p_m$ où les p_i sont des nombres premiers, pas nécessairement distincts. En regroupant les facteurs égaux entre eux on obtient l'écriture $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
- Unicité
  On suppose qu'un certain nombre premier p apparaît avec l'exposant $\alpha \geqslant 1$ dans une décomposition de n, et l'exposant $\beta \geqslant 0$ dans une autre (on envisage $\beta = 0$ pour le cas où p ne figurerait pas dans la deuxième décomposition). On a alors $n = p^{\alpha} a = p^{\beta} b$, où a et b sont des produits de nombres premiers distincts de p. Si $\alpha > \beta$, $p^{\alpha-\beta} a = b$, ce qui contredit que p et b sont premiers entre eux.
  Si $\alpha < \beta$, $a = p^{\beta-\alpha} b$, ce qui contredit que p et a sont premiers entre eux. Donc $\alpha = \beta$.

Exemples :

- $300 = 2 \times 150 = 2 \times 15 \times 10 = 2 \times 3 \times 5 \times 2 \times 5 = 2^2 \times 3 \times 5^2$
- $36 = 2^2 \times 3^2$
- $92 = 2^2 \times 23$
- $210 = 2 \times 3 \times 5 \times 7$
- $125 = 5^3$

Calculatrice :

Décomposition en facteurs premiers

```
PROGRAM:CRIBLE
:EffListe L1,L2
:Prompt N
:suite(K,K,2,N)→
L1
:1→R
:For(I,1,N-1)
:If L1(I)≠0
:Then
:L1(I)→L2(R)
:If L2(R)≤ent(√(
N))
:Then
:For(J,L2(R),ent
(N/L2(R)))
:0→L1(L2(R)*J-1)

:End
:End
:R+1→R
:End
:End
:Disp L2
```

```
PROGRAM:DECOMP
:prgmCRIBLE
:EffListe L3,L4
:1→J
:For(I,1,dim(L2)
)
:If N/L2(I)=ent(
N/L2(I))
:Then
:L2(I)→L3(J)
:1→K
:While N/(L3(J)^
(K+1))=ent(N/(L3
(J)^(K+1))
:K+1→K
:End
:K→L4(J)
:J+1→J
:End
:End
:Disp L3,L4
```

```
PROGRAM:DECOMP2
:EffListe L1,L2
:Prompt N
:1→J
:For(I,2,N)
:If N/I=ent(N/I)

:Then
:I→L1(J)
:1→K
:While N/(I^(K+1
))=ent(N/(I^(K+1
))
:K+1→K
:End
:K→L2(J)
:J+1→J
:N/(I^K)→N
:End
:End
:Disp L1,L2█
```

```
prgmCRIBLE
N=?16
 {2 3 5 7 11 13}
            Done
```

```
prgmDECOMP
N=?900
{2 3 5 7 11 13 …
         {2 3 5}
         {2 2 2}
            Done
```

```
prgmDECOMP2
N=?254
        {2 127}
          {1 1}
           Done
█
```

```
prgmDECOMP
N=?168
{2 3 5 7 11 13 …
         {2 3 7}
         {3 1 1}
            Done
█
```

```
prgmDECOMP2
N=?48
          {2 3}
          {4 1}
           Done
```

2) Conséquences

Propriété :
Si l'entier naturel n, supérieur ou égal à 2, admet pour décomposition en produit de facteurs premiers $n=p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, les diviseurs positifs de n sont les entiers $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ où r_1, r_2, …, r_k sont des entiers naturels tels que $0 \leqslant r_i \leqslant \alpha_i$ pour $1 \leqslant i \leqslant k$.

Démonstration :

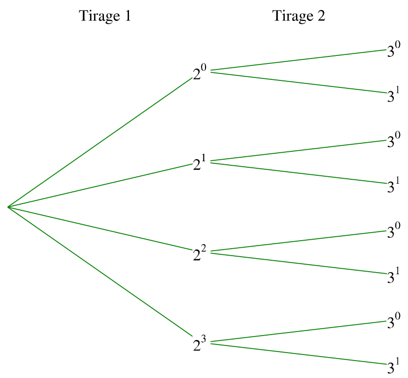
- Les nombres de la forme $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ où r_1, r_2, …, r_k sont des entiers tels que $0 \leqslant r_i \leqslant \alpha_i$ pour $1 \leqslant i \leqslant k$ sont clairement des diviseurs de $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
- Réciproquement, en notant d un diviseur de $n=p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, tout facteur premier de d divise n, donc appartient à la liste p_1, p_2, …, p_k. On en déduit que la décomposition en produit de facteurs premiers de d peut s'écrire par extension $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ avec $0 \leqslant r_i \leqslant \alpha_i$, le cas où $r_i=0$ correspondant à l'absence de facteur p_i.

Propriété :
a et b désignent deux nombres entiers naturels supérieurs ou égaux à 2.
Le PGCD de a et b est égal au produit des facteurs premiers communs aux décompositions de a et b, chacun d'eux étant affecté du plus petit exposant avec lequel il figure dans a et b.

Exemples :

- $300=2^2 \times 3^1 \times 5^2$ alors le nombre $2^1 \times 3^0 \times 5^2=50$ est un diviseur de 300.
- $24=2^3 \times 3^1$ donc 24 a pour diviseurs les entiers $2^\alpha \times 3^\beta$ avec $0 \leqslant \alpha \leqslant 3$ et $0 \leqslant \beta \leqslant 1$.
- $2^2 \times 3^1=12$ est donc le PGCD de 300 et 24.

On peut lister tous les diviseurs de 24 à l'aide d'un arbre.
Cet arbre possède 4×2 branches donc 24 a 8 diviseurs.



$2^0 \times 3^0=1$
$2^0 \times 3^1=3$
$2^1 \times 3^0=2$
$2^1 \times 3^1=6$
$2^2 \times 3^0=4$
$2^2 \times 3^1=12$
$2^3 \times 3^0=8$
$2^3 \times 3^1=24$

Propriété :
Si un entier n, $n \geqslant 2$, admet la décomposition en produit de facteurs premiers $n=p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, n admet $(\alpha_1+1)(\alpha_2+1) \times \dots \times (\alpha_k+1)$ diviseurs positifs.

Annexe : Théorèmes d'arithmétique

Petit théorème de Fermat

Petit théorème de Fermat :
Si p est un nombre premier et a est un en entier naturel non multiple de p alors $a^{p-1} \equiv 1 [p]$.

Démonstration :
Soit p un nombre premier et a un entier naturel non multiple de p. Les entiers a et p sont donc premiers entre eux.

- Considérons l'ensemble des multiples de a suivants :
$$\mathrm{A} = \{a ; 2a ; \ldots ; (p-1)a\}$$
Ce sont $p-1$ multiples non nuls de a. L'entier p ne divise aucun d'eux. En effet, si p divisait ka (avec k entier, $1 \leqslant k \leqslant p-1$), puisque p est premier avec a, il diviserait k d'après le théorème de Gauss, ce qui est impossible puisque $k < p$.
Donc leurs restes dans la division euclidienne par p sont non nuls et sont, par conséquent, des éléments de $\{1 ; 2 ; \ldots ; (p-1)\}$.
Ces restes sont tous distincts : en effet, si deux entiers k et k' appartenant à $\{1 ; 2 ; \ldots ; (p-1)\}$, avec $k > k'$, étaient tels que $ka \equiv k'a [p]$ alors p diviserait $(k-k')a$.
Or $1 \leqslant k-k' \leqslant p-2$ donc $(k-k')a$ est élément de A et aucun élément de A n'est divisible par p.
On a donc $p-1$ multiples de a dont les restes dans la division euclidienne par p sont exactement, à l'ordre près, les entiers $1 ; 2 ; \ldots ; p-1$.
- Considérons maintenant le produit P de ces multiples de a.
On a donc $\mathrm{P} \equiv 1 \times 2 \times \ldots \times (p-1) [p]$, c'est-à-dire $\mathrm{P} \equiv (p-1)! [p]$.
Donc p divise $\mathrm{P} - (p-1)!$.
Or en réordonnant les facteurs de P, on obtient $\mathrm{P} = (p-1)! \times a^{p-1}$.
Donc $\mathrm{P} - (p-1)! = (p-1)! \times a^{p-1} - (p-1)! = (p-1)! \times (a^{p-1} - 1)$.
p divise $(p-1)! \times (a^{p-1}-1)$. Or p est premier et ne divise aucun des facteurs de $(p-1)!$.
Il est donc premier avec $(p-1)!$.
Donc d'après le théorème de Gauss p divise $(a^{p-1}-1)$.

Propriété :
Si p est un nombre premier et a un entier naturel alors $a^p \equiv a [p]$.

Démonstration :
On remarque que $a^p - a = a \times (a^{p-1} - 1)$, donc $(a^{p-1}-1)$ divise $(a^p - p)$ et si a est non nul, a divise $(a^p - p)$.

- Si a n'est pas un multiple de p alors p divise $(a^{p-1}-1)$ et $(a^{p-1}-1)$ divise $(a^p - p)$ donc par transitivité p divise $(a^p - p)$
- Si a est un multiple non nul de p alors p divise a et a divise $(a^p - p)$ donc par transitivité p divise $(a^p - p)$. Si a est nul, le résultat est clairement vrai.

Remarque :
Le petit théorème de Fermat permet d'effectuer des tests de primalité.
On souhaite savoir si le nombre *n* est premier. On choisit un nombre *a* et si a^n et *a* n'ont pas le même reste dans la division euclidienne par *n* alors, d'après la contraposée, *n* n'est pas premier.
La réciproque n'est pas vraie : il existe des nombres composés *n* tels que $a^n \equiv a[n]$, mais ceux-ci sont « rares ». Ces nombres sont appelés des nombres pseudopremiers. Il y en a deux types :

- **Les nombres de Poulet**
  Pour une valeur de *a* (ou quelques valeurs de *a*) *n* vérifie $a^n \equiv a[n]$ et est composé. On dit alors que *n* est un nombre de Poulet ou un pseudopremier de base *a*.
- **Les nombres de Carmichaël**
  Pour toutes valeurs de *a* comprise entre 2 et $n-1$, *n* vérifie $a^n \equiv a[n]$ et est composé. On dit alors que *n* est un nombre de Carmichaël ou un pseudopremier absolu.

Le test de primalité consiste donc à choisir quelques valeurs de *a* et « teste » le nombre *n* en comparant les restes de a^n et *a* dans la division euclidienne par *n*. Si $a^n \equiv a[n]$ le test conclut que *n* est probablement premier.

Théorème de Wilson

Théorème de Wilson :
p est **premier** si et seulement si $(p-1)! \equiv -1[p]$.

Démonstration :

- Par contraposition : si $(p-1)! \equiv -1[p]$ alors *p* est premier.
  $(p-1)! \equiv -1[p] \Leftrightarrow (p-1)!+1 \equiv 0[p] \Leftrightarrow (p-1)!+1$ est divisible par *p*
  Si *p* n'est pas premier, il possède un diviseur *d* tel que $1<d<p$.
  Alors $(p-1)!+1$ n'est pas divisible par *d* (puisque $(p-1)!$ est divisible par *d*) ni par *p*.
- Réciproquement : si *p* est premier alors $(p-1)! \equiv -1[p]$
  - Soit *p* un nombre premier et *x* un entier naturel vérifiant $1 \leqslant x \leqslant p-1$.
    On considère les produits $x \times 1$, $x \times 2$, $x \times 3$, $x \times 4$, ..., $x \times (p-1)$.
    Puisque *p* est premier, le reste de ces produits dans la division par *p* est non nul (*p* ne divise aucun de ces produits).
  - Montrons que ces restes sont distincts (par l'absurde).
    Soit *a* et *b* entiers avec $1 \leqslant a<b<p$ et $ax \equiv bx[p]$. On aurait $(b-a)x \equiv 0[p]$, ce qui est impossible. Les restes sont dont deux à deux distincts.
  - Il y a $p-1$ restes distincts parmi $p-1$ valeurs. L'un d'entre eux est donc 1 et il est unique. Ainsi pour *x* compris entre 1 et $p-1$, il existe *y* unique entre 1 et $p-1$ tel que $xy \equiv 1[p]$.
  - $1 \times 1 \equiv 1[p]$ et $(p-1) \times (p-1) \equiv 1[p]$ donc pour $x=1$ et $x=p-1$, on a $x=y$ (puisque l'on sait que *y* est unique).
    Pour $1<x<p-1$, montrons (par l'absurde) que $x \neq y$.
    Si $x=y$ alors $x^2 \equiv 1[p]$. Donc il existe *k* tel que $x^2-1=kp$ soit $(x-1)(x+1)=kp$.
    Comme $x \neq 1$, $k \neq 0$ et *p* divise $(x+1)(x-1)$. *p* est premier et $x<p-1$. Donc c'est impossible. Ainsi si $1<x<p-1$ alors il existe un unique *y* ($x \neq y$) tel que $xy \equiv 1[p]$.
  - Si $p=2$, on a bien $1! \equiv -1[2]$. Donc la propriété est vérifiée pour $p=2$.
    Si *p* est premier et $p>2$, *p* est impair, il y a $(p-3)$ facteurs de $(p-1)!$ compris entre 1 et $(p-1)$ exclus et dont les produits sont congrus à 1 modulo *p*.
    On a donc $\prod_{i=2}^{p-2} i \equiv 1[p]$ et donc $\prod_{i=1}^{p-1} i \equiv p-1 \equiv -1[p]$. Ainsi on a bien $(p-1)! \equiv -1[p]$