104 157	Nombres premiers Arithmétique dans $\mathbb{Z}$.	Décomposition en facteurs premiers.	Monier Algèbre MPSI.

(Wikipedia) En mathématiques et plus précisément en arithmétique modulaire, la ***décomposition en produit de facteurs premiers****, aussi connue comme la* ***factorisation entière en nombres premiers****, consiste à chercher à écrire un entier supérieur ou égal à 2 sous forme d'un produit de nombres premiers. Par exemple, si le nombre donné est 45, la factorisation en nombres premiers est : $3^2 \times 5$, soit 3 x 3 x 5.*
Le facteur trivial « 1 » n'est pas mentionné.
La factorisation est toujours unique, en accord avec le théorème fondamental de l'arithmétique.
L'écriture des nombres entiers en produits de facteurs premiers en facilite la manipulation dans des problèmes de divisibilité, de fraction ou de racine carrée.
La recherche d'algorithmes de décomposition est d'une importance considérable par exemple en cryptologie.

Th.4: **Décomposition en facteurs premiers**.
Tout élément de $\mathbb{N}$-{0;1} admet une décomposition en facteurs premiers, unique à l'ordre des facteurs près.

Exemples: $9100=2^2.5^2.7.13$, et $1848=2^3.3.7.11$.

I. Prérequis (p.108,111):

Prop.4: $\begin{cases} a \wedge b = 1 \\ c \mid b \end{cases} \Rightarrow a \wedge c = 1.$

Preuve: Supp $a \wedge b = 1$ et c|b. Alors $\forall d \in \mathbb{N}^*$, (d|a et d|c) ⇒ d|a et d|b ⇒ d=1.
Ainsi le seul diviseur commun à a et c est 1, i.e. $a \wedge c = 1$.

Prop.5: $\left(\forall i, a \wedge x_i = 1\right) \Leftrightarrow a \wedge \left(\prod_i x_i\right) = 1.$

Preuve: Utilise la Prop.4.
1)⇒ Récurrence sur n.
Pour n=1, la prop. est évidente.
Pour n=2: Supposons $a \wedge x_1 = 1$ et $a \wedge x_2 = 1$. Bézout → $\exists u_1, u_2, v_1, v_2$ t.q. $au_1 + x_1 v_1 = 1$ et $au_2 + x_2 v_2 = 1$.

Alors $1 = (au_1 + x_1 v_1)(au_2 + x_2 v_2) = a(au_1 u_2 + x_1 v_1 u_2 + u_1 x_2 v_2) + (x_1 x_2)(v_1 v_2)$

et $au_1 u_2 + x_1 v_1 u_2 + u_1 x_2 v_2 \in \mathbb{Z}$, $v_1 v_2 \in \mathbb{Z}$, donc (Bézout) $a \wedge (x_1 x_2) = 1$.

Pour n≥2. Supposons la pté vraie pour un certain n≥2. Pout n+1 il vient:

Soient $x_1, \ldots, x_{n+1} \in \mathbb{Z}^*$ tels que: $\forall i \in [\![1; n+1]\!], a \wedge x_i = 1.$

Alors $\forall i \in [\![1; n]\!], a \wedge x_i = 1.$ D'après HR, alors $a \wedge \left(\prod_{i=1}^{n} x_i\right) = 1.$

Par suite, $a \wedge \left(\prod_{i=1}^{n+1} x_i\right) = a \wedge \left(\left(\prod_{i=1}^{n} x_i\right) x_{n+1}\right)$. Comme par hypothèse $a \wedge x_{n+1}$, d'après l'étude du cas n=2

il vient: $a \wedge \left(\prod_{i=1}^{n+1} x_i\right) = 1.$

2) ⇐ D'après la Prop.4 ci-dessus.

II. Développement.

A. Lemme 1 (p.117).

Lemme 1: Soient p premier et a∈$\mathbb{Z}^*$, On a: $p \mid a$ ou $p \wedge a = 1.$

Preuve: $p \wedge a \mid p \Rightarrow \begin{cases} p \wedge a = 1 \\ \text{ou} \\ p \wedge a = p \text{ i.e. } p \mid a \end{cases}.$

B. Lemme 2 (p.117).

Lemme 2: Soient p premier et n∈ℤ*, $x_1,...,x_n \in \mathbb{Z}^*$. On a: $p \mid \prod_i x_i \Leftrightarrow \exists i : p \mid x_i$

Preuve:

$\Rightarrow$ Supp. $p \mid \prod_i x_i$. Raisonnons par l'absurde en supposant que $\forall i, p \nmid x_i$.

D'après le Lemme 1, $\forall i, p \wedge x_i$.

D'après la Prop.5, $p \wedge \left(\prod_i x_i \right) = 1$. Or par hypothèse $p \mid \prod_i x_i$, donc p=1, ce qui est exclu par le définition de p premier.

$\Leftarrow$ Montrons que $\forall c,\ a \mid b \Rightarrow a \mid bc$. Supposons a|b; ∃d∈ℤ* tq b=da. Alors bc=dac=a(dc), et par suite a|bc.

Supposons par exemple que $p|x_1$. Alors $p \mid x_1 \times \prod_{i=2}^{n} x_i$ i.e. $p \mid \prod_{i=1}^{n} x_i$, ce qui achève la démonstration.

C. Théorème fondamental de l'arithmétique (p.119).

Th.4: **Décomposition en facteurs premiers**.
Tout élément de ℕ-{0;1} admet une décomposition en facteurs premiers, unique à l'ordre des facteurs près.

Exemples: $9100=2^2.5^2.7.13$, et $1848=2^3.3.7.11$.

Preuve:

1) <u>Existence de la décomposition</u>.

On raisonne par récurrence forte* sur n.

Pour n=2, la pté est vraie car 2 est premier.

Soit n≥2. Supposons que tout entier de $[\![1,n]\!]$ se décompose en produit de facteurs premiers.

→ Si n+1 est premier, n+1 se décompose en produit de facteurs premiers: lui-même.

→ Si n+1 est composé, alors $\exists a,b \in \mathbb{N}^*$ tq n+1=ab, avec a,b∈$[\![2,n]\!]$.

D'après HR, a et b admettent une décomposition en facteurs premiers, et le produit de ces deux décompositions est encore un produit de facteurs premiers, égal à n+1. On a donc trouvé une décomposition de n+1.

2) <u>Unicité de la décomposition.</u>

On raisonne par récurrence forte* sur n.

<u>Pour n=2</u>, la propriété est vrai.

<u>Soit n≥2</u>. Supposons que tout entier de $[\![1,n]\!]$ se décompose de façon unique à l'ordre des facteurs près en produit de facteurs premiers

<u>Considérons n+1</u>, et supposons qu'il admette deux décompositions en produit de facteurs premiers, $p_1...p_N$ et $q_1...q_{N'}$ avec $N, N' \in \mathbb{N}^*$. Alors $n+1 = p_1...p_N = q_1...q_{N'}$.

p_1 est premier, et $p_1 \mid q_1...q_{N'}$ donc d'après le Lemme 2, $\exists i_1 \in [\![1,N']\!] : p_1 \mid q_{i_1}$.

Mais q_{i_1} est premier, donc $p_1=1$ (exclu par définition de q_{i_1} premier) ou $p_1 = q_{i_1}$.

En réordonnant les q_i, on peut donc supposer que $p_1=q_1$.

Alors $p_2...p_N = q_2...q_{N'} \leq n$, donc par HR, N=N', et $\forall i \in [\![1,N]\!], p_i = q_i$ quitte à réordonner les facteurs,

ce qui achève la démonstration.

*Récurrence forte: {P(0), et $HR \equiv (\forall k \leq n, P(n))$} ⇒ P(n+1).