Nombres premiers; existence et unicité de la décomposition d'un nombre en facteurs premiers, infinitude de l'ensemble des nombres premiers. Exemples d'algorithmes de recherche des nombres premiers.

Cadre: Les entiers naturels.

Pré-requis:
- ◇ Notion de nombres premiers entre eux.
- ◇ Théorème de Gauss.

0.1 Nombres premiers.

Définition 0.1.1.
Un nombre est dit premier s'il est distinct de 1 et n'a pas d'autre diviseur que 1 et lui-même.

Ainsi, par exemple, 0 n'est pas premier, mais 2 l'est. L'ensemble des nombres premiers est donc non vide: nous le noterons $\mathcal{P}$.

Exemples:

- ◇
$$2, 3, 5, 7 \in \mathcal{P}.$$
- ◇
$$F_n = 2^{2^n} + 1 \in \mathcal{P} \text{ pour } n = 0, 1, 2, 3, 4 \text{ mais pas } 5.$$

0.2 Décomposition en facteurs premiers.

Afin d'établir l'existence et l'unicité "essentielle" de la décomposition en facteurs premiers d'un nombre, nous avons besoin du:

Lemme 0.2.1.
Soit $a \in \mathbb{N} \setminus \{0, 1\}$, alors le plus petit diviseur supérieur ou égal à deux de a est un nombre premier.

Démonstration. Soit $E = \{q \geq 2 : q|a\} \subset \mathbb{N}$. E est non vide car il contient a donc E possède un plus petit élément: notons le p.

Soit q un diviseur positif de p ($q \leq p$). Puisque $q|p$, alors $q|a$; on a donc deux possibilités:
- $q = 1$
- $q \in E$ et donc $q \geq p$, ce qui implique que $p = q$.

Donc p est premier. ■

Théorème 0.2.2.

Soit n un entier naturel non nul. Il existe une et une seule application de $\mathcal{P}$ dans $\mathbb{N}$ à support fini, que nous noterons v_n, telle que:

$$n = \prod_{p \in \mathcal{P}} p^{v_n(p)}.$$

Remarquons que cette écriture a bien un sens puisque v_n est à support fini.

Démonstration. Pour $n = 1$, seul $v_n(p) = 0$ pour tout $p \in \mathcal{P}$ convient.

Pour $n \geq 2$, si n est premier c'est terminé ($v_n(n) = 1$ et $v_n(p) = 0$ pour tout autre nombre premier p). Sinon, $n = p_1 n_1$ où p_1 est le plus petit diviseur de n supérieur ou égal à 2, d'après notre lemme p_1 est premier et $n_1 < n$.

Si n_1 est premier c'est terminé. Sinon, $n_1 = p_2 n_2$ où p_2 est le plus petit diviseur premier de n_1 et $n_2 < n_1$.

On construit alors par récurrence une suite d'entiers $n_1 > n_2 > \ldots > n_k$ telle que $n = p_1 \cdot p_2 \cdots p_j \cdot n_j$. On a alors une suite d'entiers supérieurs ou égal à 1 strictement décroissante donc pour un certain rang k, $n_k = 1$ et

$$n = p_1 \cdot p_2 \cdots p_k.$$

Montrons maintenant l'unicité de cette décomposition: Supposons que pour $n \geq 2$,

$$n = p_1^{v_n(p_1)} p_2^{v_n(p_2)} \cdots p_k^{v_n(p_k)} = q_1^{\widetilde{v_n}(q_1)} q_2^{\widetilde{v_n}(q_2)} \cdots q_r^{\widetilde{v_n}(q_r)}$$

où v_n et $\widetilde{v_n}$ sont deux applications de $\mathcal{P}$ dans $\mathbb{N}$ à support fini distinctes, les p_i sont premiers deux à deux distincts et les q_j sont aussi premiers deux à deux distincts.

$p_1 | n$ donc $p_1 | q_1 q_2 \cdots q_r$ donc d'après le théorème de Gauss il existe $j \in [\![1, r]\!]$ tel que $p_1 | q_j$ et donc $p_1 = q_j$. De la même manière on a:

$$\forall i \in [\![1, k]\!],\ \exists j \in [\![1, r]\!] \text{ tel que } p_i = q_j$$

et

$$\forall j \in [\![1, r]\!],\ \exists i \in [\![1, k]\!] \text{ tel que } q_j = p_i$$

donc

$$k = r \text{ et } \{p_1, p_2, \ldots, p_k\} = \{q_1, q_2, \ldots, q_k\}.$$

Ainsi

$$n = p_1^{v_n(p_1)} p_2^{v_n(p_2)} \cdots p_k^{v_n(p_k)} = p_1^{\widetilde{v_n}(p_1)} p_2^{\widetilde{v_n}(p_2)} \cdots p_k^{\widetilde{v_n}(p_k)}.$$

Supposons que $\widetilde{v_n}(p_1) \leq v_n(p_1)$, alors $v_n(p_1) = \widetilde{v_n}(p_1) + c_1$ où $c_1 \geq 0$. Donc

$$p_1^{\widetilde{v_n}(p_1)} p_1^{c_1} p_2^{v_n(p_2)} \cdots p_k^{v_n(p_k)} = p_1^{\widetilde{v_n}(p_1)} p_2^{\widetilde{v_n}(p_2)} \cdots p_k^{\widetilde{v_n}(p_k)},$$

ainsi $p_1^{c_1} | p_2 p_3 \cdots p_k$ donc d'après le théorème de Gauss $p_1^{c_1}$ divise p_2 ou p_3 ou $\ldots$ ou p_k, or $\forall i \in [\![2, k]\!]$, $(p_1, p_i) = 1$ donc $p_1^{c_1} = 1$ d'où $c_1 = 0$ et par conséquent $\widetilde{v_n}(p_1) = v_n(p_1)$. De façon analogue, on obtient que $\widetilde{v_n}(p_i) = v_n(p_i)$ pour tout i. ■

Propriétés 0.2.3.
Soient m et n deux entiers naturels non nuls. On a:

1. $\forall p \in \mathcal{P}$,
$$v_{mn}(p) = v_m(p) + v_n(p).$$
2. $\forall p \in \mathcal{P}$,
$$m|n \Rightarrow v_m(p) \leq v_n(p).$$
3. $\forall p \in \mathcal{P}$,
$$v_{\text{pgcd}(m,n)} = \min\left(v_m(p), v_n(p)\right)$$
et
$$v_{\text{ppcm}(m,n)} = \max\left(v_m(p), v_n(p)\right)$$

Remarque: Le nombre $v_n(p)$ apparaît comme le plus grand entier α tel que $p^\alpha | n$, il est appelé p-valuation de n.

0.3 Infinitude de l'ensemble des nombres premiers.

Théorème 0.3.1.
L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Démonstration. Il suffit d'observer que pour tout entier naturel n, il existe un entier premier p supérieur à n. C'est le cas, par exemple, du plus petit diviseur autre que 1 de $n! + 1$. ■

Remarques:

- Observons que pour tout $n \geq 2$, l'intervalle $[\![n! + 2, n! + n]\!]$ est sans nombres premiers; il existe donc des intervalles d'entiers de longueur arbitrairement grande ne contenant aucun nombres premier.
- Pour la répartition des nombres premiers on a démontré indépendamment l'un de l'autre en 1896 par *Hadamard* et *De la Vallée Poussin* le théorème des nombres premiers qui donne une évaluation asymptotique de nombre $\pi(n)$ de nombres premiers inférieurs ou égal à n:
$$\pi(n) \sim \frac{n}{\ln n}.$$
- Cependant il reste un grand nombre de questions sur les nombres premiers:
  - $(3, 5)$, $(29, 31)$, $(101, 103)$ sont des couples de nombres premiers de la forme $(n, n+2)$ (nombres premiers jumeaux); Existe-t-il une infinité de tels couples?
  - Conjecture de Goldbach: Tout nombre pair supérieur à 3 est la somme de deux nombres premiers.

0.4 Exemples d'algorithmes de recherche de nombres premiers.

Le but est de déterminer si un nombre supérieur ou égal à 2 est premier ou non.

◇ L'algorithme qui suit repose sur la définition d'un nombre premier et sur le fait que si un nombre $n \geq 2$ n'est pas premier, il admet un diviseur strict de carré inférieur ou égal à n.

lire n
$k := 2$
tant que $k^2 \leq n$ faire
  si k divise n, imprimer: n est non premier
  sinon, $k := k + 1$
imprimer: n est premier.

On peut vérifier à l'aide de la calculatrice que F_5 n'est pas premier.

◇ Soit $k \in \mathbb{N}^*$ et supposons établie la liste des k premiers nombres premiers: $p_1, p_2, \ldots, p_k$. La remarque précédente nous dit que tout nombre de $[\![p_k + 1, p_k^2]\!]$ est premier si, et seulement si il n'est divisible par aucun des p_i, $i \in [\![1, k]\!]$.
Sur ce principe, voici le crible d'*Erasthostène* qui donne la liste de tous les nombres premiers inférieurs à un nombre donné n:

a. Se donner un entier naturel $n \geq 2$ et écrire la liste de tous les entiers naturels de 2 à n.
b. Soit $p = 2$.
c. Entourer p.
d. Si $p^2 \leq n$, barrer tous les multiples de p supérieurs ou égaux à p^2, appeler p le premier nombre de la liste non barré et non déjà entouré, aller en c.. Sinon, sortir la liste de tous les nombres entourés et de tous les nombres non barrés.