103. Nombres premiers. Propriétés et applications.

I Définitions et propriétés.

Définition 1

Soit $n \in \mathbb{N}$.

Nous dirons que *n est premier* si et seulement si $n \geqslant 2$ et les seuls diviseurs positifs de n sont 1 et n.

Exemples.

1. 2 est un nombre premier.
2. 4 n'est pas premier puisqu'il admet 2 pour diviseur.
3. Les premiers nombres de Fermat (à détailler).

Remarques.

1. La méthode du crible d'Ératosthène permet de façon algorithmique d'obtenir la liste des nombres premiers jusqu'à une valeur maximale fixée.
2. Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19.
3. Un entier $n \geqslant 2$ qui n'est pas premier est dit composé.
4. Il est possible d'étendre la notion de nombre premier à un entier relatif n en considérant $|n|$.

Théorème 1 - théorème fondamental de l'arithmétique

Tout entier naturel supérieur ou égale à 2 s'écrit de façon unique (à l'ordre des facteurs près) comme un produit de nombres premiers.

Démonstration 1

* Existence démontrée par une récurrence forte.

- $n = 2$ est premier.
- Soit $n \geqslant 2$. Supposons que tous les entiers de $[\![2,n]\!]$ admettent une décomposition en facteurs premiers et montrons qu'alors c'est aussi le cas pour $n+1$. Si $n+1$ est premier c'est fini. Sinon il existe $(q_1,q_2) \in [\![2,n]\!]^2$ tels que $q_1 q_2 = n+1$. Comme d'après l'hypothèse de récurrence q_1 et q_2 s'écrivent comme des produits de nombres premiers, c'est encore le cas pour $n+1 = q_1 q_2$.

Nous avons démontré en usant d'une récurrence forte que tout nombre peut s'écrire comme un produit de nombre premiers.

* Unicité démontrée par une récurrence forte.

- La décomposition de $n = 2$ est unique ;
- Soit $n \in \mathbb{N}$, $n \geqslant 2$. Supposons que tout entier de $[\![2,n]\!]$ admet une décomposition en facteur premier unique à l'ordre des facteurs près, et démontrons qu'alors c'est aussi le cas pour $n+1$.
  Soit $p_1 \dots p_m$ et $q_1 \dots q_r$ deux décompositions en facteurs premiers de $n+1$.

  Puisque p_1 est premier :

  $$p_1 | q_1 \dots q_r \Rightarrow \exists i \in [\![1,r]\!],\ p_1 | q_i$$

  Et donc puisque q_i est également premier : $p_1 = q_i$.
  Nous en déduisons :

  $$p_2 \dots p_m = \prod_{k \in [\![1,r]\!] \setminus \{i\}} q_k.$$

  Par conséquent quitte à renuméroter les facteurs premiers nous avons maintenant : $p_1 \dots p_{m-1} = q_1 \dots q_{r-1} < n+1$. Et d'après l'hypothèse de récurrence ces deux décomposition sont à l'ordre des facteurs près les mêmes.

Nous avons démontré par une récurrence forte que la décomposition en facteurs premiers est unique à l'ordre des facteurs près.

Remarques.

1. Nous en déduisons que tout entier, hormis 0 -1 et 1, admet un diviseur premier.
2. Dans la démonstration de l'existence de la décomposition en facteurs premiers nous aurions pu prendre pour $q_1$le plus petit diviseur de $n+1$ supérieur ou égale à 2, car alors q_1 est une nombre premier et donc l'hypothèse de récurrence ne s'applique qu'à q_2.

Proposition 1 - infinitude de l'ensemble des nombres premiers

Soient :

. $\mathcal{P}$ l'ensemble des nombres premiers.

$\mathcal{P}$ est un ensemble infini dénombrable.

Démonstration 2

Évidemment $\mathcal{P}$ est au plus dénombrable puisque $\mathcal{P} \subset \mathbb{N}$.

Démontrons que $\mathcal{P}$ est fini en raisonnant par l'absurde.

Supposons que $\mathcal{P}$ est fini et démontrons que cela conduit à une contradiction.
Notons $\mathcal{P} = \{p_1, \ldots, p_n\}$ avec $n \in \mathbb{N}^*$.
$\mathcal{P}$ contient 2 donc $p_1 \ldots p_n + 1$ admet un diviseur premier p_i $(i \in [\![1,n]\!])$:

$$p_i | p_1 \ldots p_n + 1 \Rightarrow p_i | 1.$$

ce qui est impossible puisque p_i est premier.

Nous avons démontré par l'absurde que l'ensemble des nombres premiers est infini.

Remarques.

1. Ce résultat peut aussi se démontrer en utilisant une méthode de descente infinie.
2. Autre formulation.
   Soient $\mathcal{P}$ l'ensemble des nombres premiers, $n \in \mathbb{Z}^*$. Il existe un unique couple $(\varepsilon, (\alpha_p)_{p\in\mathcal{P}}) \in \{-1,1\} \times \mathbb{N}^{(\mathcal{P})}$ tel que :

$$n = \varepsilon \prod_{p\in\mathcal{P}} p^{\alpha_p}.$$

Définition 2

Soit $n \in \mathbb{N}^*$. Si p es un facteur premier de n alors l'unique entier $v_p(n)$ tel que $p^{v_p(n)} | n$ et $p^{v_p(n)+1} \nmid n$ est appelée la *p-valuation de n*.

II Théorèmes et trucs classiques.

Dans le Monier Algèbre
Théorèmes des restes chinois, de Fermat, de Euler.
Théorème des quatre carrés de Lagrange.
Résidus quadratiques symbole de Legendre loi de réciprocité quadratique de Gauss.

III Cryptographie.

IV Statistiques et nombres premiers.

V Fonctions multiplicatives.

une fonction complètement multiplicative est entièrement déterminée par les valeurs prises en les nombres premiers.

Exercice 40 page 128 et 75 page 131 algèbre Monier (somme des diviseurs et indicatrice d'Euler).

VI Prolongement vers d'autres arithmétiques polynômes et nombres algébriques.