Nombres premiers

Définition : Soit p un entier naturel différent de 1. p est dit premier si et seulement si il n'est divisible que par 1 et lui-même.

Exemple : Les premiers nombres premiers sont : $1, 3, 5, 7, 9, 11, 13, 17, 19, 23$ ….

Théorème : Tout entier naturel supérieur ou égal à 2 peut se décomposer en produit de nombres premiers et cette décomposition est unique.

Preuve

Montrons l'existence d'une décomposition par récurrence :

- Initialisation : 2 est un nombre premier donc c'est un produit de nombres premiers.
- Hérédité : Soit $n \geq 2$. Supposons que tous les entiers compris entre 2 et n puissent s'ecrirent comme produit de nombres premiers.
  Considérons $n+1$:
  Si $n+1$ est premier alors $n+1$ peut s'écrire comme le produit de nombres premiers.
  Si $n+1$ n'est pas premier alors $n+1 = pq$ avec p et q supérieurs ou égaux à 2. Le fait que p et q soient ≥ 2 implique que $p \leq n$ et $q \leq n$. L'hypothèse de récurrence s'applique à p et q.
  $p = \prod {p_i}^{\alpha_i}$ (tous les p_i étant premiers. Les α_i sont des entiers naturels et désignent les puissances de p_i)
  $q = \prod {q_i}^{\beta_i}$ (tous les q_i étant premiers. Les β_i sont des entiers naturels et désignent les puissances de q_i)
  Donc $n+1 = pq = \prod {p_i}^{\alpha_i} \prod {q_i}^{\beta_i}$; $n+1$ est donc aussi le produit de facteurs premiers.

Montrons maintenant l'unicité.
Supposons que $n = \prod_{i=0}^{m} {p_i}^{\alpha_i} = \prod_{j=0}^{l} {q_j}^{\beta_j}$, les p_i et les q_j étant tous premiers.
Prenons un p_i quelconque dans la première décomposition de n et supposons qu'il ne se retrouve pas dans la deuxième décomposition.
$p_i \mid \prod_{j=0}^{l} {q_j}^{\beta_j}$ et $\forall j, p_i \Lambda {q_j}^{\beta_j} = 1$ (puisque p_i et les q_j sont premiers) donc d'après le théorème de Gauss nous sommes arrivés à une contradiction.
Tous les p_i sont donc dans la deuxième décomposition et tous les q_j sont dans la première.

$$n = \prod_{i=0}^{m} {p_i}^{\alpha_i} = \prod_{i=0}^{m} {p_i}^{\beta_i}$$

Supposons qu'il existe l tel que $\alpha_l \neq \beta_l$. On peut supposer $\alpha_l < \beta_l$.

$$n = {p_l}^{\alpha_l} \prod_{\substack{i=0 \\ (i \neq l)}}^{m} {p_i}^{\alpha_i} = {p_l}^{\beta_l} \prod_{\substack{i=0 \\ (i \neq l)}}^{m} {p_i}^{\beta_i}$$

$$\frac{n}{{p_l}^{\alpha_l}} = \prod_{\substack{i=0 \\ (i \neq l)}}^{m} {p_i}^{\alpha_i} = {p_l}^{\beta_l - \alpha_l} \prod_{\substack{i=0 \\ (i \neq l)}}^{m} {p_i}^{\beta_i}$$

Donc ${p_l}^{\beta_l - \alpha_l} \mid \prod_{\substack{i=0 \\ (i \neq l)}}^{m} {p_i}^{\alpha_i}$ ce qui est impossible puisque p_l est premier avec tous les ${p_i}^{\alpha_i} (i \neq l)$. Nous sommes donc arrivés à une contradiction. Il vient $\forall l, \alpha_l = \beta_l$ et donc la décomposition en facteurs premiers est unique.

Exemple : $252 = 2^2 \times 3^2 \times 7.$

Définition : Soit p un nombre premier et n un entier quelconque.
La valuation p −adique d'un nombre n notée $v_p(n)$ est définie par :

$$\begin{cases} v_p(n) = \max\{k \in \mathbb{N} \; tel \; que \; p^k | n\} \; si \; n \neq 0 \\ +\infty \; si \; n = 0 \end{cases}$$

Remarque : La valuation p −adique d'un nombre n est donc la puissance maximale de p qui peut diviser n. Elle apparait donc dans la décomposition de n en facteurs premiers.

Exemple : D'après la décomposition précédente nous avons : $v_2(252) = 2$, $v_3(252) = 2$, $v_7(252) = 1$.

Propriété : Soit p un nombre premier et n un entier quelconque. $p \mid n \; ssi \; v_p(n) \geq 1$

Preuve

$v_p(n) \geq 1 \Longrightarrow p^{v_p(n)} | n$ Or $p \mid p^{v_p(n)}$ donc $p \mid n$.
Réciproquement si $p \mid n$ alors d'après la définition de $v_p(n)$, nous avons $v_p(n) \geq 1$

Remarque : Soit n un entier naturel non nul. Soit $n = \prod_{i=0}^{m} {p_i}^{\beta_i}$ sa décomposition en facteurs premiers.
Alors $v_{p_i}(n) = \beta_i$. On peut donc écrire $n = \prod_{i=0}^{m} {p_i}^{v_{p_i}(n)}$

Propriété	Soit p un nombre premier et n et m deux entiers quelconques. $$v_p(mn) = v_p(m) + v_p(n)$$

Preuve

Soient $\begin{cases} m = p^{v_p(m)} \prod_{i=0}^{j} {p_i}^{\alpha_i} \ pour\ 0 \le i \le j \ \ p_i \neq p \\ n = p^{v_p(n)} \prod_{k=0}^{l} {p_k}^{\beta_k} \ pour\ 0 \le k \le l \ \ p_k \neq p \end{cases}$ les deux décompositions en facteurs premiers de m et n.

Alors $mn = \ p^{v_p(m)+v_p(n)} \prod_{i=0}^{j} {p_i}^{\alpha_i} \prod_{k=0}^{l} {p_k}^{\beta_k} \Leftrightarrow v_p(mn) = v_p(m) + v_p(n)$

Propriété	Soit m et n deux entiers naturels. Soient $\prod_{i=0}^{j} {p_i}^{v_{p_i}(m)}$ et $\prod_{k=0}^{l} {p_k}^{v_{p_k}(n)}$ leurs décompositions en facteur premiers. Alors $m\Lambda n = \ \prod_{r=0}^{s} {p_r}^{Min\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$. Les p_r étant les nombres premiers se retrouvant à la fois dans les décompositions de m et de n.

Preuve

$\prod_{r=0}^{s} {p_r}^{Min\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$ divise m et n donc $\prod_{r=0}^{s} {p_r}^{Min\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)} \mid m\Lambda n.\ (div(m) \cap div(n) = div(m\Lambda n)\,)$

$$\exists K \in \mathbb{N}\ et\ K \ge 1\ tel\ que\ m\Lambda n = K \prod_{r=0}^{s} {p_r}^{Min\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$$

Supposons qu'il existe un nombre premier p tel que $p \mid K$ mais p n'est pas dans la liste des p_r.

$p \mid K \Longrightarrow p \mid m\Lambda n \Longrightarrow p \mid m$ et $p \mid n$. Or p ne peut apparaitre à la fois dans la décomposition de m et celle de n. Nous avons donc une contradiction.

Tous les nombres premiers divisant K apparaissent donc dans la liste des p_r .

Soit p un nombre premier apparaissant dans la liste des diviseurs de K et dans la liste des p_r

${p}^{Min\,(\,v_p(m)\,,\,v_p(n)\,)+1}$ divise $m\Lambda n$. Cela implique ${p}^{Min\,(\,v_p(m)\,,\,v_p(n)\,)+1} \mid m$ et ${p}^{Min\,(\,v_p(m)\,,\,v_p(n)\,)+1} \mid n$

Supposons $v_p(n) \ge v_p(m)$. Nous avons ${p}^{\,v_p(m)+1} \mid m$ ce qui remet en question la définition de $v_p(m)$.

Bien entendu nous serions arrivés à un résultat similaire si $v_p(n) \le v_p(m)$.

Nous sommes donc là encore arrivés à une contradiction. Nous en déduisons :

$$p = 1 \Longrightarrow K = 1 \Longrightarrow m\Lambda n = \prod_{r=0}^{s} {p_r}^{Min\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$$

Exemple	$120 = 2^3 * 3 * 5$ et $3920 = 2^4 * 5 * 7^2$ donc $120\ \Lambda\ 3920 = 2^3 * 5$
Propriété	Soit m et n deux entiers naturels. Soient $\prod_{i=0}^{j} {p_i}^{v_{p_i}(m)}$ et $\prod_{k=0}^{l} {p_k}^{v_{p_k}(n)}$ leurs décompositions en facteur premiers. Alors $m \vee n = \ \prod_{r=0}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$. Les p_r désignant les nombres premiers se retrouvant dans la réunion des décompositions de m et de n en facteurs premiers.

Preuve

$\prod_{r=0}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$ est un multiple de m et de n. Donc $\prod_{r=0}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$ est un multiple de $m \vee n$.

$$\exists K \in \mathbb{N}\ et\ K \ge 1\ tel\ que \prod_{r=0}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)} = K(m \vee n)$$

Supposons qu'il existe un nombre premier p_l tel que $p_l \mid K$ mais p_l n'est pas dans la liste des p_r.

$p_l \mid \prod_{r=0}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)}$ ce qui est impossible car p_l n'est pas dans la liste des p_r.

Donc p_l est dans la liste des p_r. Soit α la puissance de p_l dans la décomposition de K $(\alpha > 1)$

Supposons $v_{p_l}(n) \ge v_{p_l}(m)$ nous avons ${p_l}^{v_{p_l}(n)} \prod_{\substack{r=0 \\ (r \neq l)}}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)} = {p_l}^{\alpha} \left(\frac{K}{{p_l}^{\alpha}}\right)(m \vee n)$

$$ {p_l}^{v_{p_l}(n)-\alpha} \prod_{\substack{r=0 \\ (r \neq l)}}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)} = \left(\frac{K}{{p_l}^{\alpha}}\right)(m \vee n)$$

Nous avons donc $v_{p_l}(m \vee n) = \ v_{p_l}(n) - \alpha$. Or $m \vee n$ est un multiple de n. Nous devrions donc avoir $v_{p_l}(m \vee n) \ge \ v_{p_l}(n)$ Nous sommes donc arrivés à une contradiction et en déduisons que $K = 1$.

Nous avons donc $\prod_{r=0}^{s} {p_r}^{Max\,(\,v_{p_r}(m)\,,\,v_{p_r}(n)\,)} = (m \vee n)$

Théorème	L'ensemble des nombres premiers noté P est un ensemble infini

Preuve

Supposons qu'il soit fini. $P = \{n_1, n_2, n_3 \ \dots \ n_m\}$

Construisons le nombre $n = n_1 * n_2 * \dots . n_m + 1$

Il n'est pas premier. Il se décompose donc en produit de facteurs premiers.

$n = \prod_{i=0}^{m} {n_i}^{\alpha_i}$

Soit n_j un nombre premier différent de 1 présent dans la décomposition de n .

On aurait alors $n_1 * n_2 * \dots . n_m + 1 = kn_j$ or $n_1 * n_2 * \dots . n_m = k'\, n_j$ car n_j apparaît forcément dans la liste de gauche.

Il vient $n_j k' + 1 = \ kn_j \Longrightarrow 1 = n_j(k - k')$ ce qui impliquerait que n_j divise 1. C'est impossible. Nous sommes donc arrivés à une contradiction. P n'est donc pas fini.