Nombres premiers

Définition : Soit n un nombre entier différent de 0 et de 1. On dit que n est un nombre premier si l'ensemble de ses diviseurs est $\{-1, 1, n, -n\}$.

Exemple : 2, 3, 5, 7, 11, 13, 17, ... sont des nombres premiers.

Proposition : Tout entier naturel $n \geq 2$ admet au moins un diviseur premier.

Preuve : Notons $D^+(n)$ l'ensemble des diviseurs de n plus grands que 2. Nous avons $n \in D^+(n)$, donc $D^+(n) \neq \emptyset$.
De plus, $D^+(n) \subseteq \mathbb{N}$. Donc $D^+(n)$ admet un plus petit élément que l'on note m.
Montrons que m est premier.
Raisonnons par l'absurde : si d divise m alors d divise n.
Maintenant si m n'est pas premier, on peut choisir $2 \leq d < m$
Donc $d \in D^+(n)$ ce qui contradit la minimalité de m.

■

Proposition : L'ensemble des nombres premiers est infini.

Preuve : Raisonnons par l'absurde et supposons que l'ensemble des nombres premiers est fini. On le note donc par

$$\mathcal{P} = \{p_1, p_2, \dots, p_n\}$$

Alors $n = p_1 \dots p_n + 1 \notin \mathcal{P}$, il admet donc un diviseur premier $p \in \mathcal{P}$ d'après la proposition précédente. Mais le reste de la division euclidienne de n par p est 1 : contradiction! ∎

Lemme de Gauss et conséquences

Théorème (Lemme de Gauss),
Si des entiers a, b et c sont tels que a divise bc et a est premier avec b, alors a divise c.

Preuve :
Comme a est premier avec b, on peut écrire $au + bv = 1$ pour des entiers u et v. Ainsi $auc + bvc = c$. Comme a divise auc et a divise bvc (car a divise c) alors a divise c ∎

Lemme : Si un nombre premier p divise un produit $a_1 \dots a_n$, alors il divise l'un des a_i.

Preuve : Supposons que p divise aucun des a_i. Comme les seuls diviseurs positifs de p sont 1 et p, les nombres p et a_n sont

premiers entre eux. On en déduit par le lemme de Gauss que p divise $a_2, \dots, a_n$ (puisque p est premier avec a_1). Ensuite p divise $a_3, \dots, a_n$. Puis en itérant il divise $a_3, a_4, \dots$ et a_n ce qui contredit notre supposition. ∎

Voici une autre conséquence importante du lemme de Gauss :

Proposition : Si deux entiers premiers entre eux a et b divisent n, alors leur produit ab divise n.

Preuve :

Comme a divise n, on peut écrire $n = ak$ pour $k \in \mathbb{Z}$. Mais alors b divise ak et comme il est premier avec a, il divise k. Ainsi $k = bk'$ pour un entier k' et puis $n = abk'$, ce qui prouve que ab divise n. ∎

⚠ **Exercice important** :

Soient a et b deux entiers et soit $d = \text{pgcd}(a,b)$ leur pgcd. Trouver tous les couples u et v tels que

$$au + bv = c$$

pour un entier c.

Comme d divise a et b alors il doit diviser $au+bv=c$.
Ainsi si c n'est pas un multiple de d, l'équation n'admet pas de solutions.
On suppose donc que $c = kd$, avec $k \in \mathbb{Z}$.
D'après le lemme de Bézout, il existe $(u_0, v_0) \in \mathbb{Z}^2$ tels que

$$a u_0 + b v_0 = d$$

en multipliant par k, on obtient :

$$a u_0 k + b v_0 k = dk = c$$

Ainsi le couple (ku_0, kv_0) est une solution.
Soit (u,v) une autre solution, alors on a

$$au + bv = a k u_0 + b k v_0 = c$$

donc en faisant la différence, on obtient :

$$a(u - ku_0) = b(kv_0 - v)$$

en divisant par d, on obtient

$$\frac{a}{d}(u - ku_0) = \frac{b}{d}(kv_0 - v)$$

avec $\frac{a}{d}$ et $\frac{b}{d}$ deux entiers premiers entre eux.
On en déduit que $\frac{a}{d}$ divise $\frac{b}{d}(kv_0 - v)$ et comme il est premier avec $\frac{b}{d}$, par le lemme de Gauss $\frac{a}{d}$ divise $(v - kv_0)$
ainsi il existe $m \in \mathbb{Z}$ tels que

$$kv_0 - v = m \frac{a}{d}$$

Ainsi $\frac{a}{d}(u - ku_0) = \frac{b}{d} m \cdot \frac{a}{d}$

donc $u - \frac{u_0}{k} = m\frac{b}{d}$

donc $(u,v) = (ku_0 + m\frac{b}{d}, kv_0 - m\frac{a}{d})$

Réciproquement, si $(u,v) = (ku_0 + m\frac{b}{d}, kv_0 - m\frac{a}{d})$ pour $m \in \mathbb{Z}$ alors

$$\begin{aligned} au + bv &= a(ku_0 + m\tfrac{b}{d}) + b(kv_0 - m\tfrac{a}{d}) \\ &= akv_0 + m\frac{ab}{d} + bkv_0 - m\frac{ab}{d} \\ &= akv_0 + bkv_0 = c \end{aligned}$$

Donc les solutions sont les couples $(ku_0 + m\frac{b}{d}, kv_0 - m\frac{a}{d})$ pour $m \in \mathbb{Z}$.

Théorème : (Décomposition en facteurs premiers)

Tout entier naturel $n \geq 2$ peut s'écrire comme produit fini de nombres premiers. De plus, cette décomposition est unique, à l'ordre des facteurs près.

Preuve :

Raisonnons par récurrence sur n.

Pour $n=2$, nous avons $2=2$ donc l'affirmation est vraie.

On suppose que le résultat est vrai pour tout entier appartenant à $\{1,\dots,n\}$. Considérons $n+1$. Si $n+1$ est premier, il n'y a rien à montrer. Sinon, on sait qu'il existe un premier p qui divise $n+1$. Mais $p \geq 2$, donc $\frac{n+1}{p} \leq n$. L'hypothèse de récurrence s'applique

pour $\frac{n+1}{p}$. Donc $\frac{n+1}{p} = p_1 \cdots p_k$ avec p_i premier

ainsi $n+1 = p \cdot p_1 \cdots p_k$.

Montrons maintenant l'unicité. Supposons qu'on a deux écritures $n = p_1 \cdots p_m = q_1 \cdots q_s$

alors p_1 divise $q_1 \cdots q_s$, par le lemme de Gauss p_1 divise l'un des q_i, supposons que c'est q_1, alors comme il est premier, on doit avoir que $q_1 = p_1$, on peut donc simplifier des deux côtés, et on continue ainsi de suite ∎

Proposition : Si $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ $\alpha_i \geq 0$

$b = p_1^{\beta_1} \cdots p_n^{\alpha_n}$ $\beta_i \geq 0$

p_i premiers, alors

$$\text{ppcm}(a,b) = p_2^{\max(\alpha_1,\beta_1)} \cdots p_n^{\max(\alpha_n,\beta_n)}$$

$$\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_n^{\min(\alpha_n,\beta_n)}$$

Valuation p-adique :

Définition : Si p est un nombre premier et n un entier non-nul, la valuation p-adique de n est le plus grand entier k tel que p^k divise n. On le note $v_p(n)$.

Si $n = 0$, on convient que $v_p(0) = +\infty$.

Proposition :

1) Si n est non-nul et se décompose sous la forme

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

alors $v_{p_i}(n) = \alpha_i$ pour tout $1 \leq i \leq k$ et $v_p(n) = 0$ pour p distinct des p_i.

2) Si m et n sont deux entiers alors m divise n si et seulement si $v_p(m) \leq v_p(n)$ pour tout nombre premier p.

3) Si a et b sont des entiers non-nuls, alors

$$v_p(\text{pgcd}(a,b)) = \min(v_p(a), v_p(b))$$

$$v_p(\text{ppcm}(a,b)) = \max(v_p(a), v_p(b))$$

et si a

$$v_p(ab) = v_p(a) + v_p(b)$$

$$v_p(a+b) \geq \min(v_p(a), v_p(b)).$$

La dernière inégalité est une égalité si $v_p(a) \neq v_p(b)$.