Nombres premiers

Définition

Dire qu'un entier naturel est premier signifie qu'il admet exactement **deux diviseurs** dans $\mathbb{N}$: **un** et **lui-même**.

Zéro **n'est pas premier** car il admet une infinité de diviseurs dans $\mathbb{N}$. Un **n'est pas premier** car il n'admet qu'un seul diviseur dans $\mathbb{N}$: lui-même. Deux est **le seul** nombre pair qui est premier.

Propriétés

Tout entier naturel **non premier**, distinct de un, admet au **moins un diviseur premier**. Un entier naturel non premier est alors appelé **nombre composé**.

Soit n un nombre entier naturel supérieur ou égal à deux.
Si le nombre n n'est divisible par aucun entier p tel que $2 \leq p \leq \sqrt{n}$ alors le nombre n est **premier**.

Le crible d'Eratosthène

Il s'agit d'une méthode permettant de déterminer tous les nombres premiers inférieurs à un nombre donné. On raye tous les multiples de deux supérieurs à deux, puis tous les multiples de trois supérieurs à trois, les multiples de cinq supérieurs à cinq, les multiples de sept supérieurs à sept.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Par ce procédé, on obtient dans les cases non rayées du tableau **tous** les nombres premiers **inférieurs à cent**.

Théorème

Il existe **une infinité** de nombres premiers. La preuve de ce théorème est à connaître.

Critère de primalité

Soit n un entier naturel supérieur ou égal à deux.

Si n n'est pas premier alors il existe un nombre premier $p \leq \sqrt{n}$ qui divise n.

Limiter les essais

Soit n un entier naturel supérieur ou égal à deux. La propriété proposée ci-dessous permet de **limiter le nombre d'opérations** dans la détermination du caractère premier d'un entier.

Si n n'est divisible par aucun nombre premier p inférieur à $\sqrt{n}$ alors n est **premier**.

Décomposition en produit de facteurs premiers

Théorème

Soit n un nombre entier naturel supérieur ou égal à deux.

Ce nombre peut se décomposer sous la forme $\boxed{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k}}$.

Dans cette décomposition les nombres p_1, p_2, … , p_k sont des nombres premiers tels que $p_1 < p_2 < ... < p_k$ et les nombres α_1, α_2, … , α_k sont des entiers naturels non nuls. Cette décomposition est **unique**.

Propriété

Soit n un nombre entier naturel supérieur ou égal à deux dont le décomposition est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k}$.

L'ensemble des **diviseurs** de n est l'ensemble des entiers d s'écrivant sous la forme $d = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_k^{\beta_k}$ où les nombres β_1, β_2, … , β_k sont des entiers naturels tels que $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, … , $0 \le \beta_k \le \alpha_k$.

Le **nombre de diviseurs naturels** de n est $(\alpha_1 + 1) \times (\alpha_2 + 1) \times ... \times (\alpha_k + 1)$ car tout diviseur peut s'écrire sous la forme $d = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_k^{\beta_k}$ et chaque nombre β_i peut prendre les $(\alpha_i + 1)$ valeurs entières de 0 à βi.

Plus petit commun multiple

Définition

L'ensemble des multiples strictement positifs communs à deux entiers naturels non nuls **n'est pas vide** puisque leur produit en fait partie. Par conséquent il existe dans cet ensemble un multiple commun à ces deux nombres **plus petit** que les autres. Ce nombre est appelé le plus petit commun multiple de a et de b et sera noté $PPCM(a;b)$.

Propriétés

$$PPCM(a;b) = PPCM(b;a)$$

$$PPCM(a;1) = a$$

$$PPCM(a;a) = a$$

Si b est un multiple de a alors $PPCM(a;b) = b$

Homogénéité

Si on multiplie deux entiers naturels non nuls a et b par un **même entier naturel** k non nul alors leur PPCM est lui aussi multiplié par k. On a donc l'égalité suivante : $\boxed{PPCM(k \times a; k \times b) = k \times PPCM(a;b)}$.

PGCD, PPCM et décomposition en facteurs premiers

Théorème

Soit a et b deux entiers naturels supérieurs ou égaux à deux.

Le PGCD de a et b est égal au produit **des facteurs premiers communs** aux décompositions de a et b, chacun d'eux étant affectés **du plus petit exposant** avec lequel il figure dans la décomposition de a et b.

Le PPCM de a et b est égal au produit **de tous les facteurs premiers** présents dans **l'une ou l'autre** des décompositions de a et b, chacun d'eux étant affectés **du plus grand exposant** avec lequel il figure dans la décomposition de a et b.

Ainsi, si $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k}$ et si $b = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_k^{\beta_k}$ où p_1, p_2, … , p_k sont des nombres premiers, où α_1, α_2, … , α_k ainsi que β_1, β_2, … , β_k sont des entiers naturels **éventuellement nuls**, on a :

- $PGCD(a;b) = p_1^{\delta_1} \times p_2^{\delta_2} \times ... \times p_k^{\delta_k}$ avec $\delta_i = \min(\alpha_i;\beta_i)$ pour tout $1 \le i \le k$
- $PPCM(a;b) = p_1^{\gamma_1} \times p_2^{\gamma_2} \times ... \times p_k^{\gamma_k}$ avec $\gamma_i = \max(\alpha_i;\beta_i)$ pour tout $1 \le i \le k$

Propriété

Le **produit de deux entiers** naturels non nuls est égal au **produit de leur PGCD et de leur PPCM**. Cette relation s'écrit de la façon suivante : $PGCD(a;b) \times PPCM(a;b) = a \times b$.

Conséquence

Si a et b sont **premiers entre eu**x alors $PPCM(a;b) = a \times b$. Cette propriété est immédiate puisque la définition de deux nombres premiers entre eux est $PGCD(a;b) = 1$.