Nombres premiers

1 Définition et existence

Définition :Un nombre entier est dit premier s'il admet exactement deux diviseurs : 1 et lui-même.

remarque : 1 possède un seul diviseur, il n'est pas premier.
Un entier naturel n non premier (différent de 1) est dit composé. Il admet au moins un diviseur d, autre que 1 et lui-même qui vérifie $1 < d < n$
Un tel diviseur est dit diviseur strict de l'entier n.

Théorème : Tout nombre entier a strictement supérieur à 1 admet un diviseur premier.

Démonstration (par disjonction de cas)

- si a est premier, alors le diviseur premier cherché est a
- si a n'est pas premier, alors, par définition, a admet au moins un diviseur strict. Notons $D(a)$ l'ensemble de ses diviseurs.
  $D(a) = \{1; d_1; d_2; ...; a\}$ avec $1 < d_1 < d_2 < ... < a$
  Prouvons par l'absurde que le plus petit diviseur strict de a, d_1, est un nombre premier.
  Supposons que d_1 est non premier. Alors, d_1 admet au moins un diviseur strict d tel que $1 < d < d_1$.
  Alors d divise d_1 et d_1 divise a, donc d est un diviseur strict de a strictement inférieur à d_1 ce qui est impossible. Donc d_1 est premier.

Théorème : Tout nombre entier a (a>1) non premier admet un diviseur strict inférieur ou égal à $\sqrt{a}$.

Démonstration
a n'est pas premier, donc il admet au moins un diviseur strict d et on peut écrire $a = d \times d'$. Dans cette écriture, d' est aussi un diviseur strict car :
* si $d' = 1$ alors $d = a$, ce qui est impossible car d est un diviseur strict de a.
* si $d' = a$ alors $d = 1$, ce qui est impossible pour la même raison.
Donc $1 < d' < a$ et d' est bien un diviseur strict de a.
Prouvons par l'absurde que l'un des deux diviseurs d ou d' est inférieur ou égal à $\sqrt{a}$.
C'est à dire prouvons que : $d \leq \sqrt{a}$ ou $d' \leq \sqrt{a}$
Supposons donc que : $d > \sqrt{a}$ et $d' > \sqrt{a}$
Alors, puisque d, d' et $\sqrt{a}$ sont positifs, $d \times d' > \sqrt{a} \times \sqrt{a}$ c'est à dire $a > a$ ce qui est absurde.
Donc $d \leq \sqrt{a}$ ou $d' \leq \sqrt{a}$.
Ainsi, a admet un diviseur strict inférieur ou égal à $\sqrt{a}$

Intérêt : Pour montrer qu'un nombre est premier, il suffit de vérifier qu'il n'a pas de diviseur strict inférieur ou égal à $\sqrt{a}$.

2 Ensemble des nombres premiers

Théorème : Il existe une infinité de nombres premiers

Démonstration (par l'absurde)
Supposons donc qu'il existe un nombre fini de nombres premiers : $2 < 3 < 5 < ... < p$
Posons $N = (2 \times 3 \times 5 \times ...p) + 1$
Le nombre N est strictement supérieur à 1. Il admet donc un diviseur premier d.
Comme les nombres 2,3,5,...,p sont les seuls nombres premiers, d est nécessairement l'un de ces nombres.
Le nombre d divise donc le produit $(2 \times 3 \times 5 \times ... \times p)$
Mais d divise également le nombre N. Donc il divise leur différence 1 , ce qui est impossible.
Il existe donc un infinité de nombres premiers.

3 Divisibilité par un nombre premier

p est un nombre premier et a est un entier non divisible par p.
Alors p et a sont premiers entre eux.

Démonstration : p est premier, donc ses seuls diviseurs sont 1 et p. a n'étant pas divisible par p, des deux diviseurs de p, seul 1 est diviseur commun à a et à p : donc $PGCD(a;p) = 1$

Théorème :
p est un nombre premier
1) Si p divise le produit ab de deux entiers, alors p divise a ou p divise b.
2) Si p divise le produit ab de deux nombres premiers, alors $p = a$ ou $p = b$

Démonstration :
1) si p divise a, le résultat est acquis
si p ne divise pas a, alors par le th précédent, p est premier avec a. Il divise donc b d'après le théorème de Gauss.
2) D'après 1), p divise a ou p divise b qui n'admettent que deux diviseurs 1 et eux-mêmes. Comme p est différent de 1, $p = a$ ou $p = b$.
Cas particulier :
Si p premier divise a^2, alors p divise a et pour tout entier naturel non nul, si p (premier) divise a^n, alors p divise a.
Il résulte de cette propriété, par contraposition, que si p premier ne divise pas a, alors p ne divise pas, par exemple a^p.

4 Décomposition en facteurs premiers

Théorème fondamental : Un nombre entier naturel (autre que 0 ou 1) est premier ou se décompose de manière unique, à l'ordre près, en produit de nombres premiers.

Démonstration :

- n est un entier naturel non premier. Il admet donc un diviseur strict premier p_1. Donc $n = p_1 \times q_1$, où q_1 est aussi un diviseur strict de n (sinon $p_1 = 1$ ou $p_1 = n$, ce qui est impossible). Ainsi $q_1 < n$
- Si q_1 est premier, alors n est le produit de deux nombres premiers : $n = p_1 \times q_1$
- Si q_1 n'est pas premier, alors il admet un diviseur strict premier p_2.
  Donc $p_1 = p_2 \times q_2$ où q_2 est un diviseur strict de q_1. Ainsi $q_2 < q_1 < n$.
  Si q_2 est premier, n est le produit de trois nombres premiers : $n = p_1 \times p_2 \times q_2$
- Tant que q_i n'est pas premier, on réitère ce processus. On construit ainsi une suite d'entiers naturels $1 \leq q_i < q_{i-1} < ... < q_3 < q_2 q_1$.
  Comme cette suite est finie, ce processus doit s'arrêter : il existe donc un diviseur q_k premier.
  Ainsi n est le produit de facteurs premiers $p_1 \times p_2 \times ... \times p_k \times q_k$

L'unicité de la décomposition est admise.

Décomposition canonique :
Certains des facteurs premiers peuvent être égaux et la décomposition peut s'écrire : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} ... p_k^{\alpha_k}$ (les p_i sont deux à deux distincts et les nombres α_i

4.1 Diviseurs d'un entier naturel non premier

Théorème :
Si n est un entier naturel non premier dont la décomposition en produit de facteurs premiers est $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$
Alors les diviseurs de n sont les nombres qui s'écrivent $p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$
avec $0 \leq \beta_1 \leq \alpha_1$, $0 \leq \beta_2 \leq \alpha_2$, ..., $0 \leq \beta_k \leq \alpha_k$

propriété : Si la décomposition en produits de facteurs premiers d'un entier naturel n est : $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, alors n admet $(\alpha_1 + 1)(\alpha_1 + 1)...(\alpha_2 + 1)$ diviseurs.

5 Petit théorème de Fermat

Théorème : Soit n un nombre premier
Si p est un nombre premier ne divisant pas n,alors $n^{p-1} \equiv 1 \pmod{p}$

Remarque : Ce théorème est un test de primalité.

Corollaire : Soit n un nombre entier et p un nombre premier
$n^p \equiv n \pmod{p}$