Arithmétique suite - 1 SIO

Nombres premiers

Un *nombre premier* est un nombre entier positif qui a exactement deux diviseurs (1 et lui-même). Un nombre non premier différent de 0 et de 1 est dit *composé*.

Propriété (utile pour optimiser les algorithmes de test)

Si un nombre n est composé, alors il admet un diviseur strict d tel que $d \leq \sqrt{n}$.

Démonstration **:** Soit n un nombre composé. On note d_1 et d_2 des diviseurs stricts de n (peut-être égaux), tels que $n = d_1 \times d_2$ (on parlera de diviseurs *associés*).

On suppose par l'absurde que $d_1 > \sqrt{n}$ et $d_2 > \sqrt{n}$. On a la chaîne d'égalités et d'inégalités suivante : $n = d_1 \times d_2 > \sqrt{n} \times \sqrt{n} = n$, ce qui est impossible.

En bref : sur les deux diviseurs associés, s'il y a un grand, alors il y a un petit.

Décomposition en facteurs premiers

Tout nombre entier positif strictement supérieur à 1 s'écrit
$N = p^a \, . \, q^b \, ... \, s^d$ où p, q, …, s sont des nombres premiers.
Cette décomposition est unique.

Nombre de diviseurs

Soit N un nombre entier positif strictement supérieur à 1.
Si $N = p^a \, . \, q^b \, ... \, s^d$, (décomposition en facteurs premiers),
alors le nombre de diviseurs de N est $(a+1)(b+1)...(d+1)$.

PGCD

Soit deux entiers a et b. On note $D(a)$ et $D(b)$ les ensembles de diviseurs de a et de b respectivement. Le plus grand élément commun à ces deux ensembles est appelé *le plus grand diviseur commun* de a et de b (*greatest common divisor* en anglais), et est noté $PGCD(a,b)$ ou $GCD(a,b)$, voire $a \wedge b$.

Connaissant la décomposition en facteurs premiers de deux nombres, on peut trouver leur PGCD en gardant la plus petite des deux puissances pour chaque facteur.

Arithmétique suite - 1 SIO

Nombres premiers

Un *nombre premier* est un nombre entier positif qui a exactement deux diviseurs (1 et lui-même). Un nombre non premier différent de 0 et de 1 est dit *composé*.

Propriété (utile pour optimiser les algorithmes de test)

Si un nombre n est composé, alors il admet un diviseur strict d tel que $d \leq \sqrt{n}$.

Démonstration **:** Soit n un nombre composé. On note d_1 et d_2 des diviseurs stricts de n (peut-être égaux), tels que $n = d_1 \times d_2$ (on parlera de diviseurs *associés*).

On suppose par l'absurde que $d_1 > \sqrt{n}$ et $d_2 > \sqrt{n}$. On a la chaîne d'égalités et d'inégalités suivante : $n = d_1 \times d_2 > \sqrt{n} \times \sqrt{n} = n$, ce qui est impossible.

En bref : sur les deux diviseurs associés, s'il y a un grand, alors il y a un petit.

Décomposition en facteurs premiers

Tout nombre entier positif strictement supérieur à 1 s'écrit
$N = p^a \, . \, q^b \, ... \, s^d$ où p, q, …, s sont des nombres premiers.
Cette décomposition est unique.

Nombre de diviseurs

Soit N un nombre entier positif strictement supérieur à 1.
Si $N = p^a \, . \, q^b \, ... \, s^d$, (décomposition en facteurs premiers),
alors le nombre de diviseurs de N est $(a+1)(b+1)...(d+1)$.

PGCD

Soit deux entiers a et b. On note $D(a)$ et $D(b)$ les ensembles de diviseurs de a et de b respectivement. Le plus grand élément commun à ces deux ensembles est appelé *le plus grand diviseur commun* de a et de b (*greatest common divisor* en anglais), et est noté $PGCD(a,b)$ ou $GCD(a,b)$, voire $a \wedge b$.

Connaissant la décomposition en facteurs premiers de deux nombres, on peut trouver leur PGCD en gardant la plus petite des deux puissances pour chaque facteur.