Eléments d'arithmétique

I. Les nombres premiers

Pour cette partie, on se place dans $\mathbb{N}$.

1. Définition

Déf : tout nombre entier supérieur ou égal à 2 est premier s'il admet exactement 2 diviseurs :1 et lui-même.

2. Le crible d'Erathostène

Algorithme de recherche des nombres premiers inférieurs à un certain N :
Les nombres premiers inférieurs ou égaux à 100 sont :
2, 3, 5, 7, 11, 13, 17,19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

3. Décomposition en nombres premiers.

Prop : Tout nombre entier positif peut s'écrire comme produit de puissances de nombres premiers. Cette décomposition est unique.

Ex : $6776 = 2^3 \times 7 \times 11^2$

II. Pgcd de deux nombres

1. Définition

Déf 1 : Soient A et B deux entiers naturels, alors Pgcd(A ; B) est le plus commun diviseur à A et à B.
Déf 2 : A et B sont premiers entre eux, si Pgcd (A ; B) = 1.

2. Algorithme d'Euclide

Algorithme de recherche du Pgcd de deux nombres entiers naturels non nuls : dernier reste non nul dans la suite des divisions euclidienne de A par B puis de B par R … etc …

III. Notions de congruences

Déf : Soit a et n deux entiers naturels ($n \neq 0$), alors $a \equiv b$ (n) ou $a \equiv b$ [n] ou $a \equiv b$ mod (n) signifie qu'il existe $q \in \mathbb{N}$ tel que : $a = q \times n + b$. On peut dire aussi que b est le reste de la division de a par n.

Prop : Modulo n, les multiples de a sont les multiples de Pgcd (a ; n).