Chapitre 5: Problèmes de chiffrement I

1 Généralités sur le PGCD et le PPCM

Définition:
Soit a et b des entiers naturels non-nuls. Le plus grand élément de $D(a) \cap D(b)$, ensemble des diviseurs positifs communs de a et de b, est le plus grand diviseur commun de a et b, ou encore $PGCD$ de a et b.

Remarque:
Le $PGCD$ de deux entiers naturels est un entier au moins égal à 1

Propriété:
Soit a et b des entiers naturels au moins égaux à 2. Le plus grand diviseur commun de a et b est égal au produit des facteurs communs de a et b, avec pour chacun d'eux, l'exposant le plus petit de ceux qu'il a dans a et dans b

Exemple:
$6600 = 2^3 \times 3 \times 5^2 \times 11$ *et* $1188 = 2^2 \times 3^3 \times 11$ *donc* $PGCD(6600; 1188) = 2^2 \times 3 \times 11 = 132$

Propriété:
Soit a et b des entiers naturels non-nuls. Le plus grand diviseur commun de a et b est le dernier reste non-nul de la suite des divisons de l'algorithme d'Euclide.

Exemple:
$6600 = 1188 \times 5 + 660$ *;* $1188 = 660 \times 1 + 528$ *;* $660 = 528 \times 1 + 132$ *et* $528 = 132 \times 4 + 0$ *donc* $PGCD(6600; 1188) = 132$ *et les diviseurs communs de* 6600 *et* 1188 *sont les douze diviseurs de* 132 *soit* $D(132) = \{1; 2; 3; 4; 6; 11; 12; 22; 33; 44; 66; 132\}$

Définition:
Le plus petit multiple commun des entiers naturels non-nuls a et b est le plus petit élément de l'ensemble des multiples communs strictement positifs de a et de b. On l'appelle aussi $PPCM$ de a et b.

Remarque:
Le $PPCM$ de deux entiers naturels non-nul est un entier au moins égal à 1.

Propriété:
Soit a et b des entiers naturels au moins égaux à 2. Le plus petit commun multiple de a et b est égal au produit des facteurs communs de a et b, avec pour chacun d'eux, l'exposant le plus grand de ceux qu'il a dans a et dans b

Exemple:
$6600 = 2^3 \times 3 \times 5^2 \times 11$ *et* $1188 = 2^2 \times 3^3 \times 11$ *donc* $PPCM(6600; 1188) = 2^3 \times 3^3 \times 5^2 \times 11 = 59400$

Remarque:
$PGCD(a; b) \times PPCM(a; b) = a \times b$

2 Nombres premiers entre-eux

Définition:
Deux entiers sont premiers entre-eux lorsque leur $PGCD$ est égal à 1.

Exemple:
8 *et* 3 *sont premiers entre-eux tout comme* 12 *et* 35. *Attention, les nombres premiers entre-eux n'ont pas de lien direct avec les nombres premiers.*

3 Théorème de Bézout

Théorème: (Théorème de Bézout)
Deux entiers a et b sont premiers entre-eux, si et seulement si, il existe deux entiers u et v tels que $au + bv = 1$

Exemple:
8 *et* 3 *sont premiers entre-eux donc d'après le théorème de Bézout, il existe des solutions entières à l'équation* $8x + 3y = 1$. *Par exemple* $x = -1$ *et* $y = 3$.

Théorème: (Corollaire du théorème de Bézout)
Si d est le PGCD de deux entiers a et b alors il existe deux entiers u et v tels que $au + bv = d$

Exemple:
$PGCD(6600; 1188) = 132$ *donc il existe des entiers tels que* $6600u + 1188v = 132$. *Par exemple* $u = 2$ *et* $v = -11$.