Thème 3: Problèmes de chiffrement

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 commun diviseur de a et b, ou encore $PGCD$ de a et b.

Remarque:
Soit a un entier non-nul, alors $PGCD(a;a) = a$, $PGCD(1;a) = 1$ et $PGCD(0;a) = a$ donc 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 tels que b ne divise pas a. 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. De plus, l'ensemble des diviseurs communs de a et b est l'ensemble des diviseurs de leur $PGCD$.

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 commun multiple 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:
Soit a un entier non-nul, alors $PPCM(a;a) = a$, $PPCM(1;a) = a$ et $PPCM(0;a) = 0$. Le $PPCM$ de deux entiers naturels non-nul est un entier au moins égal à 1. De plus, l'ensemble des multiples communs de a et b est l'ensemble des multiples de leur $PGCD$.

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

2 Théorème de Bézout

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.*

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* $v = -11$.

3 Théorème de Gauss et applications

Théorème: (Théorème de Gauss)
Soit a, b et c trois entiers. Si a divise le produit bc et si a est premier avec b alors a divise c.

Exemple:
Soit a et b deux entiers tels que $3a = 5b$. 3 divise $5b$ et 3 est premier avec 5 donc 3 divise b.

Théorème:
- *Si un entier est divisible par des entiers a et b premiers entre-eux alors il est divisible par le produit ab.*
- *Si un entier premier divise un produit de facteurs ab alors il divise au moins l'un des facteurs a ou b.*
- *Si un entier premier p divise un produit de facteurs premiers alors il est égal à l'un d'eux.*
- *Un entier p est premier avec les entiers a et b si et seulement si p est premier avec le produit ab.*

Exemple:
36 *est divisible par* 2 *et* 9 *qui sont premiers entre-eux donc* 36 *est divisible par* $2 \times 9 = 18$. *Par contre,* 36 *est divisible par* 4 *et* 6 *qui ne sont pas premiers entre-eux et* 36 *n'est pas divisible par* $4 \times 6 = 24$.

4 Petit théorème de Fermat

Théorème: (petit théorème de Fermat)
Soit n un entier. Si p est un nombre premier ne divisant pas n, alors $n^{p-1} \equiv 1\,(p)$

Théorème: (Corollaire du petit théorème de Fermat)
Soit n un entier et p est un nombre premier, alors $n^p \equiv n\,(p)$