8.2 Le ppcm

Déf : soient $a, b \geqslant 1$ entiers. On appelle **ppcm de a et b** le plus petit de leurs multiples communs. On le note $\text{ppcm}(a,b)$.

Rem - la restriction $a,b \geqslant 1$ n'est pas nécessaire ; on peut en fait définir $\text{ppcm}(a,b)$ pour $a,b \in \mathbb{Z}$.

- ab est un multiple commun de a et b donc $\text{ppcm}(a,b) \leqslant ab$.

Prop : $a,b \geqslant 1$. Soient $d = \text{pgcd}(a,b)$ et $m = \text{ppcm}(a,b)$. On a alors : $ab = md$.

Dém: On sait qu'il existe a', d' tels que $\begin{cases} a = da' \\ b = db' \\ \text{pgcd}(a',b') = 1 \end{cases}$

On a donc $ab = d^2 a'b' = d \times (da'b')$ et il suffit de montrer que $da'b'$ est le ppcm de a et b.

1) montrons que $da'b'$ est un multiple commun de a et b :
c'est clair car $da'b' = (da').b' = ab'$
$= a'.(db') = a'b$

2) montrons que c'est le plus petit : soit n un multiple commun de a et b, on va mq $da'b' \leqslant n$.
Par hyp. sur n il existe u, v entiers tq $n = ua = vb$.
Alors $ua = vb = uda' = vdb'$, donc en simplifiant par d :

$$ua' = vb'.$$

Comme $\text{pgcd}(a',b') = 1$, d'après le th. (ou lemme) de Gauss on a $a' | v$ donc il existe $\begin{cases} k \in \mathbb{Z} \\ k \geqslant 1 \end{cases}$ tel que $v = ka'$.
Alors $n = vb = ka'b = kda'b' \geqslant n$. Ceci conclut ⊠

Exemple : $a = 585 \quad b = 247$

$\text{pgcd}(a,b) = 13 \quad \text{ppcm}(a,b) = 585 \times 19$

Prop soient $a, b \geq 1$ entiers écrits comme produits de nombres premiers avec les mêmes premiers qui apparaissent : $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$.

Alors $\begin{cases} \text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_r^{\min(\alpha_r,\beta_r)} \\ \text{et} \\ \text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_r^{\max(\alpha_r,\beta_r)} \end{cases}$

Dém C'est une conséquence facile de la proposition qui décrit la divisibilité d'un nombre de la forme $p_1^{n_1} \cdots p_r^{n_r}$ par un autre de la même forme ⊠

Ex : $a = 21 \quad b = 14$ on écrit les DFP : $a = 3 \times 7$, $b = 2 \times 7$

on complète pour faire apparaître les mêmes facteurs 2, 3 et 7 : $a = 2^0 \times 3^1 \times 7^1$ et $b = 2^1 \times 3^0 \times 7^1$

La prop dit que $\text{pgcd} = 7$ et $\text{ppcm} = 2 \times 3 \times 7 = 42$

9. Deux équations célèbres avec des congruences

9.1. Le théorème des restes chinois

Th soient $n, m \geq 2$ premiers entre eux. Alors pour tous $a, b \in \mathbb{Z}$ il existe $x \in \mathbb{Z}$ tel que $\begin{cases} x \equiv a \ (n) \\ x \equiv b \ (m) \end{cases}$

Dém : Soit (u,v) un couple de Bézout pour n et m :

$un + vm = 1$. En particulier on a :

(1) $\quad vm \equiv 1 \mod n$

(2) $\quad un \equiv 1 \mod m$

Posons maintenant $x = aum + bun$. On calcule :

$$x = aum + bun \equiv aum \mod n$$
$$\equiv a \mod n \quad \text{d'après (1)}$$

$$x = aum + bun \equiv bun \mod m$$
$$\equiv b \mod m \quad \text{d'après (2).} \ \boxtimes$$

Ex Trouver x tel que $x \equiv 1\ (5)$ et $x \equiv 2\ (7)$

Ici $n=5$, $m=7$ qui sont bien premiers entre eux avec couple de Bézout $u=3$ $v=-2$ $(3\times 5+(2)\times 7=1)$

De plus $a=1$ et $b=2$. On pose :

$x = aum + bun = 1.(-2).7 + 2.3.5 = -14+30 = 16$

9.2. Le petit théorème de Fermat

Th Soit p un nombre premier. Alors :

1) $\forall x \in \mathbb{Z}$, $x^p \equiv x \mod p$

2) Si de plus $p \nmid x$, alors $x^{p-1} \equiv 1 \mod p$.

Dém 1) Cas $x \geq 0$ récurrence sur $x \geq 0$

Initialisation : $0 \equiv 0\ (p)$ donc propriété vraie.

Hérédité : on suppose que pour un $x \geq 0$ on a $x^p \equiv x \mod p$. Alors, par la formule du binôme de Newton :

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k = 1 + \binom{p}{1}x + \dots + \binom{p}{p-1}x^{p-1} + x^p$$

↑ ↑ on a vu que ces coefs binômiaux sont divisibles par p (conséquence du lemme d'Euclide)

Donc $(x+1)^p \equiv 1 + x^p \mod p$.

Par hyp. de récurrence $x^p \equiv x \ (p)$

donc $(x+1)^p \equiv 1 + x^p \equiv 1 + x \mod p$ comme désiré.

Cas 1:0 on utilisera le fait suivant :

$$(-1)^p = \left\{ \begin{array}{l} -1 \text{ si } p \text{ impair} \\ 1 \text{ si } p \text{ pair : } p = 2 \end{array} \right\} \equiv -1 \mod p$$

en observant que lorsque $p=2$ on a $1 \equiv -1 \ (2)$!

On calcule maintenant :

$$x^p = (-(-x))^p = (-1)^p (-x)^p \equiv (-1)\cdot(-x) \mod p$$

d'après le fait ci-dessus et le cas précédent appliqué à $-x \neq 0$

Donc $x^p \equiv x \mod p$, ce qui conclut.

2) D'après 1) on a $p \mid x^p - x = x(x^{p-1} - 1)$.

Si $p \nmid x$, par Euclide (le lemme d'Euclide, pas l'algorithme !) on déduit que $p \mid x^{p-1} - 1$.

Donc $x^{p-1} \equiv 1 \mod p$. ☒

Ex d'utilisation trouver le reste de la DE de 143^{2016} par 7. On observe d'abord que

$143 \equiv 3 \mod 7$ donc $143^{2016} \equiv 3^{2016} \mod 7$.

Ensuite, le th de Fermat pour $x=3$ et $p=7$ nous dit que $3^6 \equiv 1 \ (7)$ donc le calcul des puissances sera périodique :

n	1	2	3	4	5	6	7	8	9	10	11	...
3^n	3	2	6	4	5	1	3	2	6	4	5	...

En faisant la DE de 2016 par 6 : $2016 = \cancel{3 \times 672} = 6 \times 336$

on trouve $143^{2016} \equiv 3^{2016} \equiv (3^6)^{336} \equiv 1^{336} \equiv 1 \mod 7$.