ARITHMÉTIQUE

$(\mathbb{Z},+,\times)$ *est un anneau commutatif totalement ordonné, discret, intègre d'éléments inversibles* $\mathbb{U}(\mathbb{Z})=\{+1,-1\}$ *; tout sous-ensemble non vide et majoré de* $\mathbb{Z}$ *admet un plus grand élément.*
Définition de la divisibilité $a \mid b$ *et règles d'usage.*

1 - Division Euclidienne :
- $\forall\,(a,b)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})\quad \exists!\,(q,r)\in\mathbb{Z}^2\quad a=bq+r\ \ \mathsf{ET}\ \ 0\le r<|b|$
- démonstration de l'unicité,
- preuve de l'existence à partir de $\max\left\{p\in\mathbb{Z}\ \middle/\ bp\le a\right\}$ pour $b>0$.

Définition du pgcd *par l'algorithme d'Euclide.*

2 - Algorithme d'Euclide :
- énoncé et démonstration du lemme d'Euclide,
- description de l'algorithme d'Euclide, nombre fini d'étapes,
- démonstration que son résultat est un diviseur commun à a et à b,
- preuve que ce diviseur est le plus grand, cas particulier $a=b=0$,
- propriété fondamentale du pgcd : $d\mid a\ \mathsf{ET}\ d\mid b\iff d\mid \mathrm{pgcd}(a,b)$

3 - Théorèmes de Bezout et de Gauss
- théorème de Bezout : $\mathrm{pgcd}(a,b)=1\iff\exists\,(u,v)\in\mathbb{Z}^2\quad au+bv=1$,
- démonstration à partir de l'algorithme d'Euclide, par remontée,
- conséquence : $\mathrm{pgcd}(a,b)=1\,\mathsf{ET}\,\mathrm{pgcd}(a,c)=1\Longrightarrow\mathrm{pgcd}(a,bc)=1$,
- théorème de Gauss : $\mathrm{pgcd}(a,b)=1\ \mathsf{ET}\ a\mid bc\Longrightarrow a\mid c$
- démonstration à partir de l'équation de Bezout par produit par c,
- conséquence : $\mathrm{pgcd}(a,b)=1\ \mathsf{ET}\ a\mid c\ \mathsf{ET}\ b\mid c\Longrightarrow ab\mid c$

Définition du $\mathrm{ppcm}(a,b)=\min\left\{m\in\mathbb{N}^*\ \middle/\ a\mid m\ \mathsf{ET}\ b\mid m\right\}$,
Cas particulier $a=0$ *ou* $b=0$,
Propriété fondamentale : $a\mid m\ \mathsf{ET}\ b\mid m\iff\mathrm{ppcm}(a,b)\mid m$.

4 - Démonstration de ces propriétés par les propriétés fondamentales :

$$\mathrm{pgcd}(ca,cb)=|c|\ \mathrm{pgcd}(a,b)\qquad \mathrm{pgcd}(a,b)=|a|\iff a\mid b$$
$$\mathrm{ppcm}(ca,cb)=|c|\ \mathrm{ppcm}(a,b)\qquad \mathrm{ppcm}(a,b)=|b|\iff a\mid b$$
$$\mathrm{pgcd}(a,b)\ \mathrm{ppcm}(a,b)=|ab|$$

Extension du pgcd *et du* ppcm *à plusieurs entiers.*

Définition des nombres premiers p *dont l'ensemble est infini.*

$$\mathrm{pgcd}(a,p)\neq 1\iff p\mid a\iff\mathrm{pgcd}(a,p)=p$$

Factorisation des entiers, et conséquences sur le pgcd *et le* ppcm.

---

5 - Exemple de résolution du lemme chinois par l'équation de Bezout :
- Donner une solution à l'équation de Bezout (E) : $101a+1003b=1$,
- déterminer toutes les solutions de (E) par le théorème de Gauss,
- construire les ensembles solutions entières de ces trois systèmes :

$$\begin{cases} x\equiv 1 \mod[1003]\\ x\equiv 0 \mod[101]\end{cases}\quad\begin{cases} x\equiv 0 \mod[1003]\\ x\equiv 1 \mod[101]\end{cases}\quad\begin{cases} x\equiv 8 \mod[1003]\\ x\equiv 15 \mod[101]\end{cases}$$

6 - (m_i), (n_i), (q_i), (r_i), (u_i) et (v_i) sont définies ainsi :
$m_0=m\ge 2\quad n_0=n\ge 2\quad u_0=0\quad v_0=1\quad u_1=1\quad v_1=-q_0$
$m_{k+1}=n_k\quad n_{k+1}=r_k\quad u_{k+2}=u_k-u_{k+1}q_{k+1}\quad v_{k+2}=v_k-v_{k+1}q_{k+1}$
Pour tout $k\in\mathbb{N}$ tel que $n_k\neq 0$, q_k et r_k sont respectivement le quotient et le reste de la division euclidienne de m_k par n_k.
- justifier que ces suites ne comportent qu'un nombre fini p de termes, c'est-à-dire $n_p=0$, préciser les termes égaux à $\mathrm{pgcd}(m,n)$,
- montrer pour tout $k\in[\![0,p]\!]$ l'égalité $r_k=u_{k+1}m+v_{k+1}n$; en déduire une expression de $\mathrm{pgcd}(m,n)$ en fonction de u_k et v_k,
- donner une solution de l'équation $7u+19v=1$, par ces suites.

7 -
- Démontrer ces égalités puis prouver cette implication

$$\mathrm{pgcd}(a,b)=\mathrm{pgcd}(a,a+b)=\mathrm{pgcd}(b,a+b)\qquad\text{avec }(a,b)\in\mathbb{N}^2$$
$$\mathrm{pgcd}(a,b)=1\Longrightarrow\mathrm{pgcd}(a+b,ab)=1$$

- calculer de même $\mathrm{pgcd}(a+1,2a+1)$ et $\mathrm{pgcd}(a^2+a,2a+1)$.

8 - Petit théorème de Fermat, p est un nombre premier et $k\in[\![1,p-1]\!]$:
- Montrer que $p\mid\binom{p}{k}$ en exprimant $\binom{p}{k}$ en fonction de $\binom{p-1}{k-1}$,
- montrer que p divise $(1+1)^p-2$ par la formule du binôme,
- prouver par récurrence que p divise a^p-a quand $a\in\mathbb{Z}$,
- démontrer le *petit théorème de Fermat* qui énonce que si a n'est pas un multiple de p, alors $p\mid a^{p-1}-1$, c'est-à-dire $a^{p-1}\equiv 1 \mod[p]$,
- calculer le reste de la division par p de $\displaystyle\sum_{k=1}^{p-1}k^{p-1}$,
- montrer sur des exemples numériques qu'il est nécessaire que l'entier p soit premier pour que les propriétés précédentes soient vraies.