PGCD (1) : définition, algorithme d'Euclide

I) Questions de cours

1. Le PGCD de deux nombres entiers relatifs dont l'un au moins est non nul est par définition (d'après les initiales) ...?
   En utilisant uniquement cette définition, la méthode la plus « naïve » pour le déterminer serait : ...?
   Les propriétés qui suivent servent à améliorer cette méthode naïve.
2. Signe d'un PGCD : un PGCD est toujours ...?
3. Symétrie (commutativité) : $\text{PGCD}(a,b) =$ ...? (ordre de a et b)
4. Pour $b > 0$, dire que $\text{PGCD}(a,b) = b$ équivaut à dire que ...?
5. $\text{PGCD}(a,0) =$ ...?
6. Lemme d'Euclide : pour b non nul, $\text{PGCD}(a-kb,b) =$ ...? (autre PGCD)
   Cette propriété (utilisée « à l'envers ») sert à remplacer le calcul d'un PGCD par le calcul d'un autre PGCD plus simple. On l'appelle parfois propriété de réduction du PGCD. Cas particulier souvent pratique : $k = 1$
   « lemme » : propriété préliminaire utilisée pour démontrer ensuite un théorème plus important, ici le théorème 8. Mais ce lemme peut être utilisé pour lui-même
7. Lemme d'Euclide appliqué à la division euclidienne : si le reste de la division euclidienne de a par b est r, alors $\text{PGCD}(a,b) =$ ...? (autre PGCD).
8. Algorithme d'Euclide : énoncer l'algorithme d'Euclide pour calculer $\text{PGCD}(a,b)$ en utilisant les propriétés 7 et 5 *(un algorithme est un procédé de calcul systématique, assimilable à un programme d'ordinateur)* : ...?
   Dans cet algorithme, le résultat (PGCD) est finalement ...?

II) Exemples

1. Etablir les ensembles A et B des diviseurs de 8028 et de 10035 qui sont dans $[1;6]$. En déduire $\text{PGCD}(8028, 10035)$
   Avec les critères de divisibilité usuels, on trouve $A = \{1,2,3,4,6\}$ et $B = \{1,3,5\}$.
   Les ensembles des quotients correspondants sont $A' = \{8028, 4014, 2676, 2007, 1338\}$ et $B' = \{10035, 3345, 2007\}$.
   A' et B' sont donc les ensembles des diviseurs de 8028 et 10035 qui sont supérieurs ou égaux respectivement à $\frac{8028}{6} = 1338$ et à $\frac{10035}{6} = 1672,5$ (en effet, si $x = ab$ et si $1 \leqslant a \leqslant 6$, alors $b = \frac{x}{a} \geqslant \frac{x}{6}$ et réciproquement). Donc aucun diviseur commun à 8028 et 10035 ne peut être supérieur aux éléments de A' et de B'.
   Or $A' \cap B' = \{2007\}$. 2007 est donc un diviseur commun à 8028 et 10035 et c'est le plus grand des diviseurs communs . Donc $\text{PGCD}(8028, 10035) = 2007$
2. Calculer $\text{PGCD}(8028, 10035)$ en utilisant l'algorithme d'Euclide.
   La division euclidienne de 10035 par 8028 donne $10035 = 8028 \times 1 + 2007$.
   Donc (lemme d'Euclide) $\text{PGCD}(10035, 8028) = \text{PGCD}(8028, 2007)$.
   La division euclidienne de 8028 par 2007 donne : $8028 = 2007 \times 4 + 0$
   Donc (lemme d'Euclide) $\text{PGCD}(8028, 2007) = \text{PGCD}(2007, 0) = 2007$ d'après une propriété du PGCD. Donc par transitivité $\text{PGCD}(10035, 8028) = 2007$.
3. Déterminer l'ensemble des entiers naturels n tels que $\text{PGCD}(2n+3, n) = 3$.
   En déduire l'ensemble des entiers naturels n tels que $\text{PGCD}(2n+3, n) = 1$.
   D'après le lemme d'Euclide : $\text{PGCD}(2n+3, n) = \text{PGCD}((2n+3) - 2n, n) =$
   $= \text{PGCD}(3, n) = \text{PGCD}(n, 3)$ par commutativité.
   D'après un théorème, dire que $\text{PGCD}(n, 3) = 3$ équivaut à dire que n est divisible par 3. Donc l'ensemble des entiers naturels n tels que $\text{PGCD}(2n+3, n) = 3$ est l'ensemble des multiples de 3.
   D'autre part, par définition, $\text{PGCD}(n, 3)$ doit diviser à la fois n et 3. mais les seuls diviseurs de 3 sont 1 et 3. Donc $\text{PGCD}(n, 3)$ ne peut être égal qu'à 3 ou à 1. On a déterminé les cas où il était égal à 3, donc il est égal à 1 dans tous les autres cas.
   Conclusion : l'ensemble des entiers naturels n tels que $\text{PGCD}(2n+3, n) = 1$ est l'ensemble des nombres qui ne sont pas multiples de 3, c'est-à-dire l'ensemble des nombres de la forme $3k+1$ ou $3k+2$.
4. Calculer $\text{PGCD}(9p+4, 2p+1)$ pour p entier naturel.
   $\text{PGCD}(9p+4, 2p+1) = \text{PGCD}(9p+4-4(2p+1), 2p+1)$ (lemme d'Euclide).
   $= \text{PGCD}(p, 2p+1) = \text{PGCD}(2p+1, p) = \text{PGCD}(2p+1-2p, p) = \text{PGCD}(1, p)$ (lemme d'Euclide). Or le seul diviseur positif de 1 est 1, donc $\text{PGCD}(1, p) = 1$. Donc finalement $\text{PGCD}(9p+4, 2p+1) = 1$