L2 informatique
HAI306X Arithmétique

PGCD et PPCM

Exercice 1. Soient a et b deux entiers. Démontrer la proposition du cours qui annonce :

$$a \wedge b \times a \vee b = a \times b$$

Exercice 2. Quelques calculs de PGCD par l'algorithme d'Euclide :

- $96 \wedge 81$;
- $126 \wedge 71$;
- $231 \wedge 35$;

Exercice 3. Quelques calculs de PGCD par décomposition en facteurs premiers :

- $231 \wedge 35$;
- $728 \wedge 28$;
- $231 \wedge 35$;
- $1800 \wedge 494$;

Exercice 4. Quelques calculs de PPCM par décomposition en facteurs premiers :

- $231 \wedge 35$;
- $728 \wedge 28$;
- $231 \wedge 35$;
- $1800 \wedge 494$;

Exercice 5. Montrer que si $d = a \wedge b$ et si le couple $(u_0, v_0) \in \mathbb{Z}^2$ vérifie $au_0 + bv_0 = d$, les autres couples (u, v) vérifiant $au + bv = d$ sont les couples (u_k, v_k) définis pour chaque $k \in \mathbb{Z}^*$ par :

$$\begin{cases} u_k = u_0 + kb_1, \\ v_k = v_0 - ka_1 \end{cases}$$

où a_1 at b_1 sont définis par $a = da_1$ et $b = db_1$.

Exercice 6. Algorithme d'Euclide étendu : Soient a et b deux entiers.

1. Rappeler le théorème de Bézout.
2. Montrer que l'algorithme d'Euclide calcule une suite définie par récurrence de la forme :

$$a_{n-1} = q_n a_n + a_{n+1}$$

   On explicitera l'initialisation.

3. Montrer qu'on peut définir deux suites u_n et v_n telles que :

$$a_n = u_n a + v_n b$$

   On explicitera les conditions initiales sur u_n et v_n.

4. Proposer un algorithme récursif, nommé **Euclide étendu** qui calcule $a \wedge b$ et les coefficients de Bézout.

Exercice 7. Déterminer la plus petite solution positive du système :

$$\begin{cases} x & \equiv 9[14] \\ x & \equiv 13[31] \end{cases}$$

Exercice 8.

- Quels sont les restes des division de 10^{100} par 13 et par 19 ?
- Quel est le reste de la division de 10^{100} par $247 = 13 \times 19$? En déduire que $10^{99} + 1$ est multiple de 247.

Exercice 9. Soient $p, q \in \mathbb{N} \setminus \{0, 1, 2\}$ tels que $p \wedge q = 1$. Montrer que $x^2 = \overline{1}$ a bien une solution mod pq autre que $\overline{1}$ et $-\overline{1}$