UNIVERSITÉ D'ANTANANARIVO

DOMAINE SCIENCES ET TECHNOLOGIES

MENTION MATHÉMATIQUES ET INFORMATIQUE

Année Universitaire 2023-2024

Semestre 5

Licence L3 - PAAC

ALGÈBRE ALGORITHMIQUE I

TD no. 3 - Divisibilité - nombres Premiers et TAF

Exercice 1. Soit $N \in \mathbb{N}$ avec $N \geqslant 2$. Montrer que N admet un diviseur inférieur à $\sqrt{N}$ si et seulement si N admet un diviseur supérieur à $\sqrt{N}$.

Exercice 2. Soient $a, b \in \mathbb{N}$ non tous nuls et $d \in \mathbb{N}^*$. Montrer que $d = \operatorname{pgcd}(a, b)$ et seulement si d est un diviseur commun à a et b et tout autre diviseur commun d' à a et b, divise d.

Exercice 3 (ppcm)**.** Soient $a, b \in \mathbb{N}^*$. Soit M l'ensemble des multiples communs à a et b, qui sont non nuls :

$$M = \{m \in \mathbb{N}^* \mid a|m \text{ et } b|m\} = \{m \in \mathbb{N}^* \mid (\exists k, l \in \mathbb{N})\ [m = ka = lb]\}.$$

(1) Montrer que M admet un plus petit élément. Ce plus petit élément est appelé le *plus petit commun multiple* de a et de b et noté $\operatorname{ppcm}(a, b)$.

(2) Donner l'équation qui définit $\operatorname{ppcm}(a, b)$ (sans utiliser l'ensemble M).

(3) Montrer que $m = \operatorname{ppcm}(a, b)$ si et seulement si m est un multiple commun à a et b tel que pour tout autre multiple commun m' à a et b, on a $m|m'$,

Exercice 4. Soient $a, b \in \mathbb{N}^*$ des entiers $\geqslant 2$ avec leurs décompositions en produits de facteurs premiers

$$a = \prod_{i=1}^{s} p_i^{r_i} \quad \text{et} \quad b = \prod_{j=1}^{t} q_j^{s_j}$$

où p_i (resp. q_j) sont premiers avec $p_1 < p_2 \ldots < p_s$ (resp. $q_1 < q_2 < \ldots q_t$).

(1) Montrer qu'on peut écrire

$$a = \prod_{k=1}^{n} u_k^{\alpha_k} \quad \text{et} \quad b = \prod_{k=1}^{n} u_k^{\alpha_k}$$

où $n \in \mathbb{N}$, u_k un nombre premier et $\alpha_k, \beta_k \in \mathbb{N}$ pour $k = 1, \ldots, n$.

(2) Montrer que

$$\operatorname{pgcd}(a, b) = \prod_{k=1}^{n} u_k^{\min(\alpha_k, \beta_k)} \quad \text{et} \quad \operatorname{ppcm}(a, b) = \prod_{k=1}^{n} u_k^{\max(\alpha_k, \beta_k)}.$$

Exercice 5. Soient $a, b \in \mathbb{N}$ avec $a > b > 0$. Montrer que $\operatorname{pgcd}(a, b) = \operatorname{pgcd}(b, r)$ où $r = a \mod b$.

Exercice 6. Soient a, b, u et $v \in \mathbb{Z}$.

(1) Montrer que

$$(au + bv)^2 = (a + b)(au^2 + bv^2) + ab(2uv - u^2 - v^2).$$

(2) En déduire que a et b sont premiers entre eux si et seulement si $a + b$ et ab sont premiers entre eux.

Exercice 7. Soient a, b des entiers naturels non nuls. Soit $d = \mathrm{pgcd}(a, b)$. Soient a', b' des entiers tels que $a = da'$ et $b = db'$. On pose $\eta = da'b'$.

(1) Montrer que a' et b' sont premiers entre eux.

(2) Montrer que η est un multiple commun à a et b.

(3) Soit M un autre multiple commun à a et b et $\alpha, \beta \in \mathbb{N}$ avec $M = \alpha a = \beta b$.

(a) Montrer que $a' | \beta$.

(b) Montrer que M est un multiple de η.

(c) Montrer que $\eta = \mathrm{ppcm}(a, b)$.

(d) Montrer que $\mathrm{pgcd}(a, b)\,\mathrm{ppcm}(a, b) = ab$.

Exercice 8. (1) Montrer que pour tout entier naturel n, les entiers $14n + 3$ et $5n + 1$ sont premiers entre eux.

(2) Montrer que si deux entiers a et b, premiers entre eux divisent un entier n, alors leur produit ab divise aussi n.

Exercice 9. Soient p un nombre premier et a et b deux entiers naturels.

(1) Montrer que si p ne divise pas a, alors p et a sont premiers entre eux.

(2) Montrer que si p divise a^2 alors p divise a.

(3) On suppose maintenant que a et b sont des nombres premiers. Montrer que si p divise le produit ab alors $p = a$ ou $p = b$.