ARITHMETIQUE - SOLUTIONS TD no. 3

Exercice 1. ($\Longrightarrow$) : Supposons que N admet un diviseur d tel que $d \leqslant \sqrt{N}$. Il existe $k \in \mathbb{N}^*$ tel que $N = dk$. On a alors

$$\begin{aligned} d &\leqslant \sqrt{N} \\ \frac{1}{\sqrt{N}} &\leqslant \frac{1}{d} \\ \sqrt{N} = \frac{N}{\sqrt{N}} &\leqslant \frac{N}{d} = k, . \end{aligned}$$

ainsi, k est un diviseur de N supérieur à $\sqrt{N}$.

($\Longleftarrow$) : Démonstration similaire.

Exercice 2. ($\Longleftarrow$) : Supposons que d divise a et de b et que pour tout autre diviseur commun d' de a et b, on a $d'|d$. Alors, forcément, $d' \leqslant d$. Donc d est le pgcd de a et de b.

($\Longrightarrow$) : La preuve utilise le théorème de Bézout. Supposons que $d = \mathrm{pgcd}(a, b)$ et soit d' un diviseur commun de a et b, i.e $a = d'k_1$ et $b = d'k_2$, avec $k_1 \in \mathbb{N}$ et $k_2 \in \mathbb{N}$. D'après le théorème de Bézout, il existe $u,\ v \in \mathbb{Z}$ tels que

$$au + bv = d.$$

Donc

$$\begin{aligned} d'k_1u + d'k_2v &= d \\ d'(k_1u + k_2v) &= d. \end{aligned}$$

D'où $d'|d$. □

Exercice 3. (1) On a $ab \in M$ donc $M \neq \emptyset$. Il admet donc un plus petit élément. Ainsi $\mathrm{ppcm}(a, b) = \min M$ existe.

(2) Si $\mu = \mathrm{ppcm}(a, b)$, alors

$$\mu \neq 0,\ a|\mu,\ b|\mu \text{ et si } m \in \mathbb{N}^* \text{ avec } a|m \text{ et } b|m \text{ alors } \mu \leqslant m.$$

(3) ($\Longrightarrow$) : Supposons que $m = \mathrm{ppcm}(a, b)$. Alors $m \neq 0$ et m est un multiple commun à a et b. Soit m' un autre multiple commun à a et b. Effectuons la division

euclidienne de m' par m : il existe $q, r \in \mathbb{N}$ tels que $m' = mq + r$ avec $o \leqslant r < m$. Alors $r = m' - mq$. Or il existe $k, k' \in \mathbb{N}$ tels que $m = k'a$ et $m = ka$. Ainsi,

$$r = a(k' - kaq),$$

donc r est multiple de a. De même, on montre que r est aussi un multiple de b. Si $r \neq 0$, alors r est un multiple commun à a et b qui est non nul avec $r < m$, ce contredit a minimalité de m. Donc, nécessairement, $r = 0$. Par suite, $m' = mq$, i.e. $m|m'$.

$(\Longleftarrow)$: Supposons que m est un multiple commun à a et b et que pour tout autre multiple commun m' à a et b, on a $m|m'$. Alors, nécessairement, $m \neq 0$, car il divise, par exemple ab qui est un multiple commun a et b. Puisque $m|m'$ pour tout autre multiple commun non nul m' à a et b, on a $m \leqslant m'$. Donc m est le plus petit des multiples communs a a et b, qui sont non nuls. D'où $m = \mathrm{ppcm}(a, b)$.

Exercice 4. (1) On pose

$$P = \{p_1, \ldots, p_s\} \bigcup \{q_1, \ldots, q_t\};$$

On pose card$(P) = n$; on a alors

$$P = \{u_1, \ldots, u_n\}$$

où u_k est un nombre premier, égal à l'un de p_i ou q_j, avec $u_1, \ldots, u_n$. De plus,

$$a = \prod_{k=1}^{n} u_k^{\alpha_k}$$

avec $\alpha_k = 0$ si u_k n'est égal à aucun des p_i et $\alpha_k = r_i$ si $u_k = p_i$; de même,

$$b = \prod_{k=1}^{n} u_k^{\alpha_k}.$$

avec $\beta_k = 0$ si u_k n'est égal à aucun des q_j et $\beta_k = s_j$ si $u_k = p_i$.

Formule pour $\mathrm{pgcd}(a, b)$**.** Soit d un diviseur commun à a et b . Soit p un nombre premier qui divise d ; alors $p|a$ et dans ce cas, d doit être égal à l'un des nombres p_i ; de même, puisque $p|b$, il doit être égal à l'un des nombre q_j. Finalement, p doit donc être égal à l'un des nombres u_k. La décomposition de d en un produit de facteurs premiers est donc de la forme

$$d = \prod_{k=1}^{n} u_k^{\delta_k}.$$

Puisque $d|a$, il existe $x \in \mathbb{N}$ tel que $dx = a$. Puisque $x|a$, par le même raisonnement pour d, la décomposition de x en facteurs premiers est de la forme

$$x = \prod_{k=1}^{n} u_k^{\gamma_k}.$$

Puisque

$$dx = (\prod_{k=1}^{n} u_k^{\delta_k})(\prod_{k=1}^{n} u_k^{\gamma_k}) = \prod_{k=1}^{n} u_k^{\delta_k+\gamma_k} = a = \prod_{k=1}^{n} u_k^{\alpha_k},$$

cela équivaut à $\delta_k + \gamma_k = \alpha_k$ pour $k = 1, \ldots, n$. Donc $\delta_k \leqslant \alpha_k$ pour $k = 1, \ldots, n$; on démontre de même que $\delta_k \leqslant \beta_k$. D'où $\delta_k \leqslant \min(\alpha, \delta_k)$. Pour que d soit le pgcd de a et b, il faut et il suffit que tous les δ_k soient maximum, i.e. $\delta_k = \min(\alpha_k, \beta_k)$. D'où la formule

$$\mathrm{pgcd}(a, b) = \prod_{k=1}^{n} u_k^{\min(\alpha_k, \beta_k)}.$$

Formule pour $\mathrm{ppcm}(a, b)$. Soit m un multiple commun à a et b. Puisque $u_k|a$ et $u_k|b$ pour $k = 1, \ldots, n$, on a $u_k|m$, donc u_k doit être facteur de m. Ainsi, la décomposition de m en facteurs premiers doit être de la forme

$$m = \prod_{k=1}^{n} u_k^{\mu_k} \prod_{h=1}^{l} v_h^{\rho_h}$$

où v_h est un nombre premier différent des u_k pour $h = 1, \ldots, l$ et $k = 1, \ldots, n$. On peut alors écrire

$$a = \prod_{k=1}^{n} u_k^{\gamma_k} \prod_{h=1}^{l} v_h^{\lambda_h}$$

avec $\lambda_h = 0$ pour $h = 1, \ldots, l$. Par un raisonnement analogue au précédent fait pour le pgcd, puisque $a|m$, la condition nécessaire et suffisante pour ceci est que $\alpha_k \leqslant \gamma_k$ et que $\lambda_k \leqslant_k$, mais cette dernière est déjà vérifiée car $\lambda_k = 0$. De même, la condition nécessaire et suffisante pour que $b|m$ est que $\beta_k \leqslant \gamma_k$. Ces conditions sont équivalentes à $\max(\alpha_k, \delta_k) \leqslant \gamma_k$ pour $k = 1, \ldots, n$. Pour que m soit égal à $\mathrm{ppcm}(a, b)$, il faut et il suffit que γ_k soit minimal et que $\prod_{h=1}^{l} v_h^{\rho_h}$ soit minimal aussi. Ces conditions sont équivalentes à $\gamma_k = \max(\alpha_k, \delta_k)$ et $\prod_{h=1}^{l} v_h^{\rho_h} = 1$; d'où la formule

$$\mathrm{ppcm}(a, b) = \prod_{k=1}^{n} u_k^{\max(\alpha_k, \beta_k)}.$$

Exercice 5. Soit $d = \mathrm{pgcd}(a, b)$. Il existe $k, l \in \mathbb{N}$ tels que $a = kd$ et $b = ld$. On a $a = bq + r$ avec $0 \leqslant r < b$, donc $r = a - bq = kd - ldq = d(k - lq)$. Ainsi $d|r$; donc d est

aussi un diviseur commun à b et r. Soit d' un autre diviseur commun à b et r ; il existe $u, v \in \mathbb{N}$ tel que $b = ud'$ et $r = vd'$. Ainsi, $a = bq + r = ud'q + vd' = d'(uq + v)$. Donc d' est aussi un diviseur commun à a et b ; il en résulte que $d' \leqslant d$. Tout diviseur commun à b et r est donc plus petit que d. Par suite, $d = \mathrm{pgcd}(b, r)$.

Exercice 6. (1) L'idée est d'écrire $(au+bv)^2$ comme une "combinaison" de $(a+b)$ ab avec des coefficients en a, b, u et v : d'où

$$\begin{aligned}(au + bv)^2 &= (au)^2 + 2(abuv) + (bv)^2 \\ &= a^2u^2 + b^2v^2 + 2abuv \\ &= (a + b)(au^2 + bv^2) - abu^2 - abv^2 + 2abvu \\ &= (a + b)(au^2 + bv^2) + ab(2uv - u^2 - v^2)\end{aligned}$$

($\Longrightarrow$) : Si a et b premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$; par l'équation ci-dessus, on a

$$(au + bv)^2 = 1 = (a + b)U + abV,$$

où $U = au^2 + bv^2 \in \mathbb{Z}$ et $V = 2uv - u^2 - v^2 \in \mathbb{Z}$. Donc $(a+b)$ et ab sont aussi premiers entre eux.
($\Longleftarrow$) : Supposons $(a + b)$ et ab premiers entre eux : il existe $x, y \in \mathbb{Z}$ tels que $(a + b)x + aby = 1$; or

$$(a + b)x + aby = 1 \Longrightarrow\ a(1 + by) + bx = 1,$$

donc on a $aX + bY = 1$ avec $X = 1 + by \in \mathbb{Z}$ et $Y = x \in \mathbb{Z}$. Donc a et b sont premiers entre eux.

Exercice 7. (1) Par l'identité de Bézout, il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = d = da'u + db'v = d.$$

Puisque $d \neq 0$, on peut simplifier par d, ce qui donne $a'u + b'v = 1$, donc a' et b' sont premiers entre eux.
(2) On a $\eta = da'b' = ab' = ba'$ donc c'est un multiple de a et de b.
(3) (a) On a $M = \alpha a = \beta b$. Donc $M = \alpha da' = \beta db'$. Ainsi, $\alpha a' = \beta b'$, donc $a' | \beta b'$;

mais puisque a' et b' sont premiers entre eux, d'après le lemme de Gauß, $a'|\beta$.

(b) Il existe donc un entier $k \in \mathbb{N}$ tel que $\beta = ka'$. On a alors $M = ka'b = k(\eta)$.

(c) D'après la question (2), $\eta \neq 0$ et c'est un multiple commun à a et b. De plus, on a vu d'après la question (b) ci-dessus que tout multiple commun à a et b est multiple de η. Cela signifie que $\eta = \mathrm{ppcm}(a, b)$ (Exercice 3).

(d) On donc, d'après la question (c) ci-dessus :

$$\begin{aligned} \eta = da'b' &= \mathrm{ppcm}(a, b) \\ dda'b' &= d\,\mathrm{ppcm}(a, b) \text{ (on multiplie par } d) \\ (da')(db') &= \mathrm{pgcd}(a, b)\,\mathrm{ppcm}(a, b) \\ ab &= \mathrm{pgcd}(a, b)\,\mathrm{ppcm}(a, b). \end{aligned}$$

Exercice 8. (1) On a

$$5(14n + 3) - 14(5n + 1) = 70n - 70n + 15 - 14 = 1,$$

donc ces deux nombres sont premiers entre eux ;

(2) Supposons que a et b sont premiers entre eux avec $a|n$ et $b|n$: il existe $k, l \in \mathbb{N}$ tels que $n = ka = lb$. Par hypothèse, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$; en multipliant par n, on a $nau + nbv = n$; en remplaçant n par ses expressions en fonction de b et de a, on a $lbau + kabv = n$, ce qui donne $ab(lu + kv) = n$, donc $ab|n$.

Exercice 9. (1) Supposons que p ne divise pas a. Soit $d = \mathrm{pgcd}(p, a)$; alors $d|p$ et $d|a$. Puisque p est premier, on a $d = 1$ ou $d = p$. Mais p ne divise pas a , on a $d = 1$, donc p et a sont premiers entre eux.
(2) Supposons que $p|a^2$, i.e. $p|a \cdot a$. D'après le lemme d'Euclide, $p|a$ ou $p|a$, donc $p|a$.
(3) Supposons a et b premiers et $p|ab$. D'après le lemme d'Euclide, $p|a$ ou $p|b$. Si $p|a$, pisque a est premier, on a $p = 1$ ou $p = a$; mais $p = 1$ est impossible, donc $p = a$; de même, si $p|b$, on a $p = b$.