Correction devoir maison 1

Exercice 1

(a) Cela découle du théorème fondamental de l'arithmétique.

(b) On montre les deux implications :

($\Leftarrow$) si $\delta_i \leq \alpha_i$ pour tout i, alors $a = \pm dc$ avec $c = p_1^{\alpha_1-\delta_1} \cdots p_r^{\alpha_r-\delta_r}$, donc $c \in \mathbb{Z}$ puisque $\alpha_i - \delta_i \geq 0$ pour tout i, si bien que $d \mid a$.

($\Rightarrow$) Soit $c \in \mathbb{Z}$ tel que $a = dc$. Par unicité de la décomposition de $a = dc$ en produit de puissances de premiers, les facteurs premiers qui apparaissent dans la décomposition de c apparaissent forcément dans celle de a, donc on peut écrire $c = \prod_{i=1}^r p_i^{\gamma_i}$ avec $\gamma_i \geq 0$ pour tout i. On obtient :

$$\prod_{i=1}^r p_i^{\alpha_i} = \prod_{i=1}^r p_i^{\delta_i} \times \prod_{i=1}^r p_i^{\gamma_i} = \prod_{i=1}^r p_i^{\delta_i+\gamma_i} \ ,$$

d'où $\alpha_i = \delta_i + \gamma_i \geq \delta_i$ pour tout i.

(c) D'après la question précédente, il est clair que $d = \prod_{i=1}^r p_i^{\min(\alpha_i,\beta_i)}$ divise a et b et, si $c \in \mathbb{Z}$ est un diviseur commun à a et b, alors $c = \prod_{i=1}^r p_i^{\gamma_i}$ avec $0 \leq \gamma_i \leq \min(\alpha_i, \beta_i)$ pour tout i, donc $c \mid d$. Ceci entraîne que d est le pgcd de a et b.

De même, il est clair que a et b divisent $e = \prod_{i=1}^r p_i^{\max(\alpha_i,\beta_i)}$ et, si $f \in \mathbb{Z}$ est un multiple commun à a et b, alors $f = \prod_{i=1}^r p_i^{\phi_i}$ avec $\phi_i \geq \max(\alpha_i, \beta_i)$ pour tout i, donc $e \mid f$. Ceci entraîne que f est le ppcm de a et b.

(d) On a :

$$\mathrm{pgcd}(a,b)\mathrm{ppcm}(a,b) = \prod_{i=1}^r p_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)} = \prod_{i=1}^r p_i^{\alpha_i+\beta_i} = ab \ .$$

Exercice 2

(a) $d \mid a$ donc il existe $a' \in \mathbb{Z}$ tel que $a = da'$; de même pour b'. Soit c un diviseur commun à a' et b', alors cd divise a et b donc $cd \mid d$ donc $c = \pm 1$, si bien que $\mathrm{pgcd}(a, b) = 1$.

(b) On a :

$$\begin{aligned} a(u+s) + b(v+t) = d &\iff as + bt = 0 \\ &\iff a's + b't = 0 \\ &\iff a's = -b't \end{aligned}$$

Comme b' est premier à a', cette dernière égalité entraîne que b' divise s (par le théorème de Gauss), donc il existe $n \in \mathbb{Z}$ tel que $s = b'n$. On en tire $a'n = -t$ (car $b' \neq 0$) et donc $t = -a'n$. La réciproque est claire, d'où la deuxième équivalence demandée.

(c) On commence par chercher une relation de Bézout entre 15 et 51 à l'aide de l'algorithme d'Euclide :

$$\begin{aligned} 51 &= 15 \times 3 + 6 \ , \\ 15 &= 6 \times 2 + 3 \ , \\ 6 &= 3 \times 2 + 0 \ , \end{aligned}$$

d'où $\text{pgcd}(15, 51) = 3$ et

$$3 = 15 - 6 \times 2 = 15 - (51 - 15 \times 3) \times 2 = 15 \times 7 + 51 \times (-2) \ .$$

Le couple $(7, -2)$ est donc solution de l'équation. Toutes les solutions entières peuvent se mettre sous la forme $(7 + s, -2 + t)$, et on sait par la question précédente que $s = 17n$ (car $51 = 3 \times 17$) et $t = -5n$ ($15 = 3 \times 5$) pour un $n \in \mathbb{Z}$. L'ensemble des solutions est donc :

$$S = \{(x, y) \in \mathbb{Z}^2,\ 15x + 51y = 3\} = \{(7 + 17n, -2 - 5n),\ n \in \mathbb{Z}\} \ .$$

On est en quelque sorte passé de l'écriture cartésienne de l'ensemble S à son écriture paramétrique.

(d) Commençons par l'équation $3x + 4y = 1$: $(-1, 1)$ en est une solution évidente et toutes les autres sont de la forme $(-1 + 4n, 1 - 3n)$ avec $n \in \mathbb{Z}$.

Considérons maintenant l'équation $3x + 4y = 66$: $(-66, 66)$ en est une solution évidente et toutes les solutions peuvent se mettre sous la forme $(-66+s, 66+t)$ avec $s, t \in \mathbb{Z}$. En reprenant le raisonnement de la question précédente, on obtient $s = 4n$ et $t = -3n$ pour un $n \in \mathbb{Z}$, donc toutes les solutions s'écrivent $(-66 + 4n, 66 - 3n)$ avec $n \in \mathbb{Z}$. On veut de plus $-66 + 4n \geq 0$ et $66 - 3n \geq 0$, d'où $17 \leq n \leq 22$. L'ensemble des solutions entières positives est donc :

$$\{(2, 15), (6, 12), (10, 9), (14, 6), (18, 3), (22, 0)\} \ .$$

On retrouve bien le résultat de l'exercice 6 de la feuille de TD 1.

Exercice 3

(a) Soit $k \in \mathbb{Z}$ alors $k = 2m$ pour un entier m ou $k = 2m'+1$ pour un entier m' (k pair ou impair) ; dans le premier cas $k^2 = 4m^2 \equiv 0 \bmod 4$, dans le second cas $k^2 = 4m'^2 + 4m' + 1 \equiv 1 \bmod 4$, d'où le résultat.

(b) x n'est pas multiple de 3 donc $x \equiv 1$ ou $-1 \bmod 3$, c'est-à-dire $x = 3x' + \varepsilon$ avec $x' \in \mathbb{Z}$ et $\varepsilon \in \{-1, 1\}$, donc

$$x^3 = (3x' + \varepsilon)^3 = 27x'^3 + 27x'^2\varepsilon + 9x'\varepsilon^2 + \varepsilon^3 \equiv \varepsilon^3 \equiv \pm 1 \bmod 9 \ .$$

(c) On obtient de même que $y^3 \equiv \pm 1 \bmod 9$, d'où $x^3 + y^3 \equiv -2, 0$ ou $2 \bmod 9$, ce qui contredit $x^3 + y^3 = z^3$ puisque $z^3 \equiv \pm 1 \bmod 9$.

(d) On peut faire de même pour $n = 5$ en raisonnant modulo 25 : comme x n'est pas multiple de 5, on a $x = 5x' + \varepsilon$ avec $x' \in \mathbb{Z}$ et $\varepsilon \in \{\pm 1, \pm 2\}$, d'où l'on tire $x^5 \equiv \varepsilon^5 \bmod 25$. Or $\varepsilon^5 \equiv \pm 1$ ou $\pm 7 \bmod 25$. On en déduit que $x^5 + y^5 \equiv 0, \pm 2, \pm 6, \pm 8$ ou $\pm 14 \bmod 25$, ce qui contredit $x^5 + y^5 = z^5$.

Par contre, ça ne marche plus pour $n = 7$; en particulier, on peut vérifier la congruence :

$$1^7 + 30^7 \equiv 31^7 \bmod 49 \ .$$

L'hypothèse « (x, y, z) est une solution entière non triviale telle que xyz n'est pas divisible par n » s'appelle le *premier cas* du théorème de Fermat ; il est plus facile à traiter que le second cas : $n \mid xyz$. Pour $n = 3$, Fermat a traité le second cas ($3 \mid xyz$) en utilisant sa méthode de « descente infinie ».