Licence 2 - 2018/2019

HLMA304 : Arithmétique

Thierry Mignon

Juin 2019

Examen de deuxième session

Durée : 2h – Documents, calculatrices et téléphones interdits

Exercice 1. *(Cours)*

(1) Soit G un sous-groupe de $\mathbb{Z}$, montrer qu'il existe un unique entier naturel d tel que $G = d\mathbb{Z}$.

> Correction : *cf.* cours. Si $\mathbb{N}^* \cap G = \emptyset$, d vaut 0. Sinon d est le plus petit élément de $\mathbb{N}^* \cap G$. On le démontre par division euclidienne.

(1) Soit $(a, b) \in \mathbb{Z}^2$. Donner la définition du pgcd de (a, b). Montrer que $\text{pgcd}(a, b)$ est le générateur de $a\mathbb{Z} + b\mathbb{Z}$.

> Correction : Le pgcdde (a, b) est l'unique entier positif ou nul divisant a et b et tel que si $d' \in \mathbb{Z}$ divise a et b, alors d' divise d.
> Voir le cours pour la deuxième partie.

Exercice 2. Déterminer les entiers relatifs n tels que $n - 4$ divise $3n - 17$.

> Correction : On a : $3n - 17 = 3(n - 4) - 5$. Donc, $(n - 4)$ divise $3n - 17$ si et seulement si $n - 4$ divise 5, c'est à dire si $(n - 4) \in \{-5, -1, 1, 5\}$, ou encore $n \in \{-1, 3, 5, 9\}$.

Exercice 3. Déterminer le le reste de la division euclidienne de $5^{2019} + 7772$ par 7.

> Correction : On se place dans $\mathbb{Z}/7\mathbb{Z}$, où $\overline{7772} = \overline{2}$. On applique le petit théorème de Fermat : dans $\mathbb{Z}/7\mathbb{Z}$, si x est non nul, $x^6 = \overline{1}$. Il faut donc connaître 2019 modulo 6 :
>
> $$2019 = 6.336 + 3.$$
>
> On obtient :
>
> $$\overline{5^{2019} + 7772} = \left(\overline{5}^6\right)^{336}.\overline{5}^3 + \overline{7772} = \overline{1}^{336}\overline{(-2)}^3 + \overline{2} = \overline{-8} + \overline{2} = \overline{1}.$$
>
> Le reste de la division euclidienne est 1.

Exercice 4. Un phare émet un signal jaune toutes les 15 secondes et un signal rouge toutes les 28 secondes. On aperçoit le signal jaune 2 secondes après minuit et le rouge 8

secondes après minuit. A quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?

CORRECTION : Soit x le nombre de seconde écoulées à partir de minuit où l'on voit les deux signaux en même temps. Vu la description du signal jaune, il existe un entier k tel que $x = 2+15k$. Vu la description du signal rouge, il existe un entier k' tel que $x = 8 + 28k'$. Autrement dit, x est solution du système de congruence :

$$\begin{cases} x \equiv 2 \ [15] \\ x \equiv 8 \ [28] \end{cases} \tag{0.1}$$

Puisque 15 et 28 sont premier entre eux, se système possède une solution d'après le théorème des restes chinois. Pour l'obtenir, on commence par chercher une relation de Bezout entre 15 et 28 à l'aide de l'algorithme d'Euclide augmenté :

$$28 = 1.15 + 13, \qquad 15 = 1.13 + 2, \qquad 13 = 6.2 + 1$$
$$\text{donc } 1 = 13 - 6.2 = 13 - 6(15 - 13) = (-6).15 + 7.13 = (-6).15 + 7(28 - 15) = 7.28 + (-13).15$$

Le théorème des restes chinois nous assure que l'entier :

$$x_0 = 7.2.28 + (-13).8.15 = 392 - 1560 = -1168$$

est une solution particulière du système. Les solutions sont connues modulo $28 \times 15 = 420$. L'ensemble des solutions du système (0.1) est alors :

$$S = \{-1168 + 420k, k \in \mathbb{Z}\}.$$

Le plus petite solution positive est obtenue pour $k = 3$. On obtient : $x = 92$ secondes.

Exercice 5. Le but de l'exercice est de montrer que : si $(a, b) \in \mathbb{N}^*$ est un couple d'entier positifs tel que $ab + 1$ divise $a^2 + b^2$, alors le quotient

$$k = \frac{a^2 + b^2}{ab + 1}$$

est un carré parfait (le carré d'un nombre entier).

(1) Vérifier cette propriété pour $(a, b) = (1, 1)$.

CORRECTION : $\frac{1^2+1^2}{1\times1+1} = 1$, qui est le carré de 1.

(1) Montrer que si $a = b \neq 1$ alors $ab + 1$ ne divise pas $a^2 + b^2$.

CORRECTION : Soit $a \in \mathbb{N}$, $a \geq 2$. Supposons que $(a^2 + 1)$ divise $2a^2$. Il existe $k \in \mathbb{Z}$ tel que : $k(a^2 + 1) = 2a^2$. Puisque $a \geq 2$, cet entier k est nécessairement strictement positif et, si $k \geq 2$, alors $k(a^2 + 1) \geq 2(a^2 + 1) > 2a^2$. C'est impossible.
On a donc forcément $k = 1$, donc $a^2 + 1 = 2a^2$ ce qui fournit le cas précédent, $a = 1$, que l'on a exclu par hypothèse.

Dans la suite On pose :

$$S = \{(a, b) \in \mathbb{N}^*, a < b, (ab + 1)|(a^2 + b^2)\}$$

(1) Montrer que S est non vide.

CORRECTION : La propriété est symétrique en a et b. On peut supposer $a < b$. On va écrire les couples $(ab+1, a^2+b^2)$ pour les petites valeurs de (a,b) avec $a<b$:

$a\backslash b$	1	2	3	4	5	6	7	8
1	×	$(3,5)$	$(4,10)$	$(5,17)$	$(6,26)$	$(7,37)$	$(8,50)$	$(9,65)$
2	×	×	$(7,13)$	$(9,20)$	$(11,29)$	$(13,40)$	$(15,53)$	$(17,68)$

On observe que $68/17 = 4$. Le couple $(a,b) = (2,8)$ est donc un élément de S.

On souhaite prouver la propriété par contraposée. Dans la suite on note (a,b) un élément de S tel que

$$b = \min\left\{ y \in \mathbb{N}^*,\ \exists x \in \mathbb{N}^*, (x,y) \in S,\ \text{et } \frac{x^2+y^2}{xy+1} \text{ n'est pas un carré} \right\}$$

(1) Posons $k = \frac{a^2+b^2}{ab+1}$ Montrer que b est racine du polynôme :

$$P = X^2 - akX + (a^2 - k)$$

CORRECTION : On a :

$$k = \frac{a^2+b^2}{ab+1} \iff k(ab+1) = a^2+b^2 \iff b^2 - akb + (a^2-k) = 0 \iff P(b) = 0.$$

Soit b' la deuxième racine de ce polynôme.

(1) En considérant les relations coefficients/racines pour P, montrer que b' est un entier relatif.

CORRECTION : Les relations coefficients/racines pour P s'écrivent :

$$\begin{cases} b + b' &= ak \\ bb' &= a^2 - k \end{cases} \tag{0.2}$$

En particulier $b' = ak - b$ est dans $\mathbb{Z}$ puisque b et k le sont par hypothèse.

(1) Montrer qu'on a : $k = \frac{a^2+b'^2}{ab'+1}$, puis :

CORRECTION : Montrons tout d'abord que l'on ne peut avoir $ab'+1 = 0$. Si c'était le cas, puisque $a \geq 1$, on aurait nécessairement $a = 1, b' = -1$. Les relations coefficients racines donnent alors : $b = 1+k$, $-b = 1-k$ ce qui n'est pas possible.
La même suite d'équivalence qu'à la question (4) montre que $P(b') = 0 \iff k = \frac{a^2+b'^2}{ab'+1}$.

a. Si $b' = 0$, montrer que k est un carré.

CORRECTION : Si $b' = 0$, $k = a^2/1$ est un carré d'après la question (6).

b. Si $b' < 0$, montrer que $k < 0$.

CORRECTION : On a vu que le cas $ab' + 1 = 0$ était impossible. Puisque $a \geq 1$ et $b' \leq -1$, on a donc nécessairement $ab' + 1 < 0$, et par suite : $k = (a^2 + b'^2)(ab' + 1) < 0$.

c. Si $b' > 0$, montrer que $b' < a$, et que le couple $(b', a) \in S$.

CORRECTION : Puisque $a < b$ et $a, b \geq 0$ on sait que :

$$k = \frac{a^2 + b^2}{ab + 1} < \frac{b^2 + b^2}{ab} = 2\frac{b}{a}$$

La relation coefficient racine $b + b' = ak$ donne donc :

$$b + b' < a\frac{2b}{a} = 2b, \quad \text{ou encore : } b' < b.$$

(1) Conclure.

CORRECTION :
L'entier k est strictement positif par hypothèse. Le cas $b' < 0$ est donc impossible.
Si $b' > 0$, pusique $b' < a$ on a trouvé un nouveau couple (b', a) qui est élément de S. Mais on a $a < b$, or b était le plus petit élément possible parmi les "deuxièmes-coefficients" des éléments de S. Ce cas est donc impossible.
Le seul cas possible est donc $b' = 0$, et k est bien un carré parfait.