Licence 2 - 2016/2017

HLMA304 : Arithmétique

Thierry mignon

Octobre 2016

Contrôle continu

Durée : 1h30 – Documents, calculatrices et téléphones interdits

Exercice 1. (cours) Soit $n \in \mathbb{N}^*$. on note $\equiv_n$ la relation d'équivalence "congruence modulo n" dans $\mathbb{Z}$. Montrer que $\mathbb{Z}$ possède exactement n classes d'équivalences pour $\equiv_n$ qui sont : $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

CORRECTION : Montrons d'abord que les n classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sont distinctes : soient a, b tels que $0 \leq a, b \leq n-1$. Si $\overline{a} = \overline{b}$, alors $n|(b-a)$. Mais $|a-b| \leq n-1$ donc $a = b$.

Par ailleurs, soit $a \in \mathbb{Z}$. Notons r le reste de la division euclidienne de a par n. Alors $\overline{a} = \overline{r}$ et $r \in \{0, \ldots, n-1\}$, donc toute classe d'équivalence de $\equiv_n$ est élément de l'ensemble $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Exercice 2.

(1) (cours) Soit $(a, b, c) \in \mathbb{Z}$. On suppose qu'il existe $k \in \mathbb{Z}$ tel que

$$a + kb = c$$

Montrer que $a \wedge b = b \wedge c$.

CORRECTION : Posons $d = a \wedge b$ et $e = b \wedge c$. On a :

$$(d|a \text{ et } d|b) \Longrightarrow (d|b \text{ et } d|c = a + kb) \Longrightarrow d|e = b \wedge c$$
$$(e|b \text{ et } e|c) \Longrightarrow (e|a = c - kb \text{ et } e|b) \Longrightarrow e|d = a \wedge b$$

Ainsi, $d|e, e|b$ et les deux sont des entiers positifs ou nul. On en déduit : $d = e$.

(1) Calculer, en fonction de n, $(n-1) \wedge (n+1)$.

Correction : Puisque $2 = (n+1) + (-1).(n-1)$, la question précédente nous assure que :

$$(n-1) \wedge (n+1) = 2 \wedge (n+1)$$

On distingue alors deux cas : Si n est pair, on pose $n = 2k$ et

$$(n-1) \wedge (n+1) = 2 \wedge (n+1) = 2 \wedge ((2k+1) - k.2) = 2 \wedge 1 = 1$$

Si n est impair, on pose $n = 2k+1$ et

$$(n-1) \wedge (n+1) = 2 \wedge (n+1) = 2 \wedge ((2k+2) - k.2) = 2 \wedge 2 = 2$$

(1) En déduire, en fonction de n, $(2n^2 + 5n - 1) \wedge (n^2 + 2n - 1)$.

Correction : On a :

$$\begin{aligned}(2n^2 + 5n - 1) \wedge (n^2 + 2n - 1) &= ((2n^2 + 5n - 1) - 2.(n^2 + 2n - 1)) \wedge (n^2 + 2n - 1) \\ &= (n+1) \wedge (n^2 + 2n - 1) \\ &= (n+1) \wedge ((n^2 + 2n - 1) - n.(n+1)) = (n+1) \wedge (n-1) \\ &= 1 \text{ si } n \text{ est pair, et } 2 \text{ si } n \text{ est impair.}\end{aligned}$$

Exercice 3.

(1) Écrire la décomposition de 12! en facteurs premiers.

Correction : La décomposition de 12! est :

$$2.3.4.5.6.7.8.9.10.11.12 = 2.3.2^2.5.(2.3).7.2^3.3^2.(2.5).11.(2^2.3) = 2^{10}.3^5.5^2.7^1.11$$

(1) En déduire le nombre de diviseurs positifs de 12!.

Correction : Si $d = \prod_{p \in \mathcal{P}} p^{\alpha_p}$ est un nombre décomposé en facteur premier. C'est un diviseur de 12 si et seulement si : $0 \leq \alpha_2 \leq 10$, $0 \leq \alpha_3 \leq 5$, $0 \leq \alpha_5 \leq 2$, $0 \leq \alpha_7 \leq 1$, $0 \leq \alpha_{11} \leq 1$, et toutes les autres puissances α_p des nombres premiers p distincts de $2, 3, 5, 7, 11$ sont nulles.
Il y a donc 11 choix possibles pour α_2, 6 pour α_3, 3 pour α_5, 2 pour α_7 et 2 pour α_{11}.
Cela fait un total de $11 \times 6 \times 3 \times 2 \times 2 = 792$ diviseurs de 12!.

Exercice 4. Soit $a \in \mathbb{Z}$, montrer que $a^3 - a$ est divisible par 2 et par 3. En déduire que 6 divise $a^3 - a$.

CORRECTION : On peut, par exemple prouver que la classe d'équivalence de $a^3 - a$ est nul dans $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.
D'après le petit théorème de Fermat, tout x de $\mathbb{Z}/2\mathbb{Z}$ vérifie $x^2 = x$ (c'est un cas particulier très simple de ce théorème puisque $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$). On a donc :

$$\overline{a}^3 - \overline{a} = \overline{a}^2.\overline{a} - \overline{a} = \overline{a}.\overline{a} - \overline{a} = \overline{0}.$$

De même, tout x de $\mathbb{Z}/2\mathbb{Z}$ vérifie $x^3 = x$, donc, dans $\mathbb{Z}/3\mathbb{Z}$, $\overline{a}^3 - \overline{a} = \overline{0}$.
D'après un corollaire du lemme de Gauss vu en cours, puisque $2|(a^3 - a)$, $3|(a^3 - a)$ et $2 \wedge 3 = 1$, alors $2.3 = 6$ divise $a^3 - a$.

Exercice 5. Calculer $d = 650 \wedge 66$ et déterminer l'ensemble des couples $(u, v) \in \mathbb{Z}^2$ tels que :

$$650u + 66v = d.$$

Correction : On applique l'algorithme d'Euclide :

$$\begin{aligned} 650 &= 9.66 + 56 & \qquad 66 &= 1.56 + 10 \\ 56 &= 5.10 + 6 & \qquad 10 &= 1.6 + 4 \\ 6 &= 1.4 + 2 & \qquad 4 &= 2.2 + 0 \end{aligned}$$

Le pgcd est le dernier reste non nul : $650 \wedge 66 = 2$. Résoudre l'équation de l'énoncé revient à résoudre l'équation équivalente obtenue en divisant tous les termes par 2 :

$$325u + 33v = 1.$$

On cherche une solution particulière à l'aide l'algorithme d'Euclide étendu. On écrit d'abord l'algorithme d'Euclide pour cette équation réduite (ce qui revient à diviser toutes les égalités ci-dessus par 2) :

$$\begin{aligned} 325 &= 9.33 + 28 \\ 33 &= 1.28 + 5 \\ 28 &= 5.5 + 3 \\ 5 &= 1.3 + 2 \\ 3 &= 1.2 + 1 \end{aligned}$$

On remonte ensuite les égalités pour écrire :

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2.3 - 5 \\ &= 2.(28 - 5.5) - 5 = 2.28 - 11.5 \\ &= 2.28 - 11.(33 - 28) = 13.28 - 11.33 \\ &= 13.(325 - 9.33) - 11.33 = 13.325 - 128.33 \end{aligned}$$

Ainsi le couple $(u_0, v_0) = (13, -128)$ est une solution particulière.
Soit (u, v) une solution quelconque de l'équation. On a :

$$\begin{cases} 325u + 33v &= 1 \\ 325u_0 + 33v_0 &= 1 \end{cases} \Longrightarrow 325(u - u_0) = 33(v_0 - v)$$

Donc 33 divise $325(u - u_0)$ et, puisque $325 \wedge 33 = 1$, $33|(u - u_0)$ d'après le lemme de Gauss. Il existe donc $k \in \mathbb{Z}$ tel que $u - u_0 = 33k$. On a alors $325.33k = 33.(v_0 - v)$ donc $v_0 - v = 325k$. Ainsi, il existe k tel que $(u, v) = (u_0 + 33k, v_0 - 325k)$.
Réciproquement, on vérifie que tous ces couples sont bien des solutions.
L'ensemble des solutions est :

$$S = \{(u, v) = (13 + 33k, -128 - 325k), k \in \mathbb{Z}\}$$

Exercice 6. On suppose que, pour effectuer des achats, on ne dispose que de deux types de pièces de valeurs 3 € et 5 €. On cherche quelles sont les sommes pouvant

être payées si le vendeur ne peut pas nous rendre la monnaie. Ceci revient à chercher l'ensemble

$$S = \{3a + 5b, (a, b) \in \mathbb{N}^2\}.$$

(1) Montrer que si $n \geq 15$, $n \in S$.

CORRECTION : Soit $n \geq 15$. Puisque $5 \wedge 3 = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$3u + 5v = n.$$

Si u, v sont positifs ou nuls, c'est terminé. Sinon, puisque n est positif, il y a deux cas possibles :
Premier cas : Si $u \geq 0, v < 0$, on a :

$$3u + 5v = 3(u - 5) + 5(v + 3)$$

Si $u - 5 < 0$, alors $n = 3u + 5v \leq 3u < 15$ ce qui est exclu. On peut donc remplacer (u, v) par $(u - 5, v + 3)$ et on a encore $u - 5 \geq 0$. Si $v + 3 \geq 0$, on a terminé. Sinon, on recommence, jusqu'à ce que le coefficient de 5 soit positif.
Deuxième cas : Si $u < 0, v \geq 0$, on a :

$$3u + 5v = 3(u + 5) + 5(v - 3)$$

Si $v - 3 < 0$, alors $n = 3u + 5v \leq 5v < 15$ ce qui est exclu. On peut donc remplacer (u, v) par $(u + 5, v - 3)$ et on a encore $v - 3 \geq 0$. Si $u + 5 \geq 0$, on a terminé. Sinon, on recommence, jusqu'à ce que le coefficient de 3 soit positif.

(1) Trouver S.

CORRECTION : Après la question précédente, il suffit de considérer les sommes entre 0 et 14. On a :

$$0 = 0.3 + 0.5, 3 = 1.3, 5 = 1.5, 6 = 2.3, 8 = 3 + 5, 9 = 3.3,$$
$$10 = 2.5, 11 = 2.3 + 1.5, 12 = 4.3, 13 = 2.5 + 1.3, 14 = 3.3 + 1.5$$

Considérons les trois sommes restantes : $1, 2, 4$ et 7.
Si $(u, v) \neq (0, 0)$, on a : $3u + 5v \geq 3$. Donc 1 et 2 ne sont pas dans S.
Supposons que $4 = 3u + 5v$ avec $(u, v) \in \mathbb{N}^2$. Si $v \neq 0$, $3u + 5v \geq 5$, ce qui est impossible. Donc $4 = 3u$ et $3|4$, ce qui ne convient pas non plus. Ainsi, $4 \notin S$.
Supposons que $7 = 3u + 5v$ avec $(u, v) \in \mathbb{N}^2$. Comme ci-dessus, on a forcément $v \leq 1$. Si $v = 0$, 3 divise 7, ce qui n'est pas le cas. Si $v = 1$, alors $3u = 7 - 5 = 2$, donc 3 divise 2 ; c'est impossible. Ainsi :

$$S = \mathbb{N} \setminus \{1, 2, 4, 7\}$$