HLMA304, Arithmétique
Examen, Première session, janvier 2018

— Durée : 2h —
Documents, calculatrices et téléphones portables sont interdits durant l'examen.
Les exercices pourront être traités dans n'importe quel ordre. On pourra admettre le résultat d'une question pour aborder les suivantes.

Exercice 1. *(Cours)* Énoncer le petit théorème de Fermat.

Correction : Soit p un nombre premier et $n \in \mathbb{Z}$. On a : $n^p \equiv n\ [p]$.
Si, de plus, $n \wedge p = 1$, alors $n^{p-1} \equiv 1\ [p]$.

Exercice 2.

(1) Déterminer l'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que :

$$6a - 11b = 6$$

Correction : Cherchons d'abord l'ensemble des couples de $\mathbb{Z}^2$ vérifiant cette relation.
On observe que $\text{pgcd}(6, 11) = 1$ divise le second membre, il y aura donc des solutions entières.
Cherchons d'abord une solution particulière.
On cherche une relation de Bezout entre 6 et 11, par exemple la relation $6 \times 2 - 11 \times 1 = 1$, puis on multiplie tout par 6, pour obtenir la solution particulière $(a_0, b_0) = (12, 6)$. La méthode habituelle montre alors que :

$$\{(a, b) \in \mathbb{Z}^2,\ 6a - 11b = 6\} = \{(12 + 11k, 6 + 6k),\ k \in \mathbb{Z}\}$$

On cherche maintenant les couples d'entiers naturels. On a :

$$12 + 11k \geq 0 \iff k \geq -1, \qquad 6 + 6k \geq 0 \iff k \geq -1$$

L'ensemble recherché est donc $\{(12 + 11k, 6 + 6k),\ k \geq -1, k \in \mathbb{Z}\} = \{(1 + 11k, 6k),\ k \in \mathbb{N}\}$

Remarque : on pouvait aussi prendre comme solution particulière la solution évidente $(a_0, b_0) = (1, 0)$.

(1) Déterminer l'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que :

$$6a - 12b = 5$$

Correction : Puisque $\text{pgcd}(6, 12) = 6$ ne divise pas le second membre, l'ensemble des solutions est vide.

Exercice 3. Soit a, b, c, d des entiers naturels non nuls. On suppose que $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$ et que

$$\frac{a}{b} + \frac{c}{d}$$

est entier. Montrer que $b = d$.

CORRECTION : Posons $n = \frac{a}{b} + \frac{c}{d}$, $n \in \mathbb{N}$.
On a : $nbd = ad + bc$, donc $d(nb - a) = bc$ et $d|bc$. Puisque $d \wedge c = 1$, le lemme de gauss montre que $d|b$.
De même, $b(nd - c) = ad$, et $a \wedge b = 1$, donc $b|d$.
Puisque d et b sont des entiers positifs, $d|b$ et $b|d$ implique $d = b$.

Exercice 4. Montrer que pour tout entier naturel n,

$$7|(3^{2n+1} + 2^{n+2})$$

CORRECTION : On peut procéder par récurrence ou modulo 7.
Par récurrence : Hypothèse de récurrence H_n : $7|(3^{2n+1} + 2^{n+2})$.
Pour $n = 0$, on a : $3^1 + 2^2 = 7$ qui divise 7 ; donc H_0 est vraie.
Supposons H_n vraie. On sait que $3^{2n+1} + 2^{n+2} = 7k,\ k \in \mathbb{N}$. On a :

$$\begin{aligned} 3^{2(n+1)+1} + 2^{(n+1)+2} &= 3^2.3^{2n+1} + 2.2^{n+2} = 9(7k - 2^{n+2}) + 2.2^{n+2} \\ &= 7.9k + 2^{n+2}(2 - 9) = 7.(9k - 2^{n+2}) \end{aligned}$$

qui est bien divisible par 7.
Dans $\mathbb{Z}/7\mathbb{Z}$: La barre désigne la classe d'équivalence dans $\mathbb{Z}/7\mathbb{Z}$:

$$\overline{3^{2n+1} + 2^{n+2}} = \overline{3^2}^n.\overline{3} + \overline{2}^n.\overline{2^2} = \overline{3}(\overline{9}^n - \overline{2}^n) = \overline{3}(\overline{2}^n - \overline{2}^n) = \overline{0}.$$

Exercice 5.

(1) Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair est 1.

CORRECTION : Dans $\mathbb{Z}/8\mathbb{Z}$, les classes des nombres impairs sont : $\overline{1}, \overline{3}, \overline{5} = -\overline{3}, \overline{7} = -\overline{1}$. Tous leurs carrés valent $\overline{1}$.

(1) Montrer de même que tout nombre pair vérifie $x^2 \equiv 0\ [8]$ ou $x^2 \equiv 4\ [8]$.

CORRECTION : Dans $\mathbb{Z}/8\mathbb{Z}$, les classes des nombres pairs sont : $\overline{0}, \overline{2}, \overline{4}, \overline{6} = -\overline{2}$. Leurs carrés respectifs sont : $\overline{0}, \overline{4}, \overline{0}, \overline{4}$.

(1) Soient a, b, c trois entiers impairs. Déterminer le reste modulo 8 de $a^2 + b^2 + c^2$ et celui de $2(ab + bc + ca)$.

Correction : Puisque a, b et c sont impairs, d'après la question 1, on a dans $\mathbb{Z}/8\mathbb{Z}$:

$$\overline{a^2+b^2+c^2} = \overline{a}^2 + \overline{b}^2 + \overline{c}^2 = \overline{1}+\overline{1}+\overline{1} = \overline{3}$$

Le reste modulo 8 vaut donc 3.
Puisque $a+b+c$ est aussi impair, on a aussi :

$$\begin{aligned} \overline{1} = \overline{(a+b+c)^2} &= \overline{a^2+b^2+c^2} + \overline{2ab+2bc+2cd} \\ \Longrightarrow \overline{2(ab+bc+cd)} &= \overline{1} - \overline{a^2+b^2+c^2} = \overline{1}-\overline{3} = \overline{-2} = \overline{6} \end{aligned}$$

Le reste modulo 8 vaut donc 6.

(1) En déduire que les nombres $a^2+b^2+c^2$ et $2(ab+bc+ca)$ ne sont pas des carrés ; puis que $ab+bc+ca$ n'est pas un carré non plus.

Correction : Si c'étaient des carrés, leur restes modulo 8 vaudraient $1, 0$ ou 4 d'après les deux premières questions, or ils valent respectivement 3 et 6.
Si $(ab+bc+cd)$ était un carré, sa classe dans $\mathbb{Z}/8\mathbb{Z}$ vaudrait $\overline{0}, \overline{1}$ ou $\overline{4}$. On aurait donc ; $\overline{2(ab+bc+cd)} \in \{\overline{0}, \overline{2}\}$, or $\overline{2(ab+bc+cd)} = \overline{6}$.

Exercice 6.

Une vieille fermière s'en allant au marché voit ses œufs écrasés par un cheval. Le cavalier voulant la rembourser lui demande combien d'œufs elle avait. Tout ce dont elle se souvient est qu'en les rangeant par 2, il en restait un, et de même en les rangeant par 3, 4, 5 ou 6 ; toutefois, en les rangeant par 7, il n'en restait pas. Combien d'œufs, au moins, avait-elle ?

Correction : L'énoncé puis se traduire de la manière suivante. Soit n le nombre d'oeufs ; n est le plus petit entier positif tel que :

$$\begin{aligned} &(n-1) \text{ est divisible par } 2,3,4,5,6 \text{ et } n \text{ est divisible par } 7 \\ \Longleftrightarrow &(n-1) \text{ est divisible par } 60 \text{ et } n \text{ est divisible par } 7. \end{aligned}$$

Ainsi n est le plus petit entier naturel solution du système de congruence :

$$\begin{cases} n & \equiv 1 \quad [60] \\ n & \equiv 0 \quad [7] \end{cases}$$

Pour résoudre ce système, on commence par trouver une relation de Bezout entre 60 et 7 à l'aide de l'algorithme d'Euclide augmenté : $60 = 8\times 7 + 4$, $7 = 1\times 4 + 3$, $4 = 1\times 3 + 1$ d'où on déduit :

$$1 = 4-3, \quad = 4-(7-4) = 2\times 4 - 7 = 2\times(60-8\times 7) - 7 = 2\times 60 - 17\times 7$$

D'après le cours, une solution particulière du système est : $n_0 = 0\times 2\times 60 - 1\times 17\times 7 = -119$, et l'ensemble des solutions du système est : $\{n_0 + 7\times 60k,\ k\in\mathbb{Z}\} = \{-119+420k,\ k\in\mathbb{Z}\}$ Le nombre d'oeufs recherché est le plus petit entier positif de cet ensemble, soit $301 = -119+420$.

Exercice 7. Un code de sécurité sociale est formé de 13 chiffres (entre 0 et 9) suivis d'une clef de deux chiffres. Si N est l'entier formé par les 13 chiffres et c la clef, la contrainte de vérification est la relation

$$N + c \equiv 0 \ [97]$$

Par exemple, la clé du numéro $N = 2\ 43\ 07\ 35\ 231\ 584$ est $c = 19$ (un calcul montre que $N = 97 \times 25059126099 - 19$).

(1) Montrer que 97 est un nombre premier.

CORRECTION : La racine carré de 97 est comprise entre 9 et 10. Il suffit donc de tester la divisibilité de 97 par les nombres premiers inférieurs à 10 : $2, 3, 5, 7$.
Puisque 97 ne se termine pas par un chiffre pair, il n'est pas divisible par 2.
Puisque la sommes des chiffres de 97 ($9 + 7 = 16$) n'est pas un multiple de 3, 97 n'est pas divisible par 3.
Puisque 97 ne se termine pas par 0 ou 5, il n'est pas divisible par 5.
Enfin, la division euclidienne de 97 par 7 s'écrit : $97 = 13 \times 7 + 6$. Le reste n'est pas nul, donc 97 n'est pas divisible par 7.

(1) Montrer que tous les nombres 10^k sont inversibles dans $\mathbb{Z}/97\mathbb{Z}$.

CORRECTION : Puisque 97 est premier, tous les nombres premiers à 97 sont inversibles dans $\mathbb{Z}/97\mathbb{Z}$. Puisque $0 < 10 < 97$, $10 \wedge 97 = 1$ et $\overline{10}$ est inversible dans $\mathbb{Z}/97\mathbb{Z}$, de même que toutes ses puissances.

(1) On considère un numéro de sécurité sociale dont un connait tous les chiffres sauf un, qui est illisible (on connait seulement sa position). Montrer que la clé permet de retrouver le chiffre manquant.

CORRECTION : Supposons que le nombre n s'écrive :

$$n = a_{12}a_{12} \cdots a_2 a_1 a_0$$

où les a_i sont des chiffres, et que le chiffres a_k soit illisible. Considérons le nombre :

$$m = a_{12}a_{12} \cdots a_{k+1} 0 a_{k-1} a_2 a_1 a_0$$

où on a remplacé le chiffre illisible par 0. On a : $n - m = a_k 0 \cdots 0 = 10^k a_k$ et donc, modulo 97 :

$$\overline{n} - \overline{m} = \overline{10^k}\overline{a_k} \quad \Longrightarrow \quad \overline{a_k} = \overline{10^{-k}}(\overline{c} - \overline{m})$$

(d'après la question précédente, 10^k est inversible dans $\mathbb{Z}/97\mathbb{Z}$). Ceci permet de calculer a_k modulo 97, et donc a_k puisque $0 \leq a_k \leq 9$.

(1) Montrer, en revanche, que si deux chiffres successifs sont illisibles, ils ne peuvent pas toujours être retrouvés.

CORRECTION : Voici un contre-exemple : Les nombres 1111111111100 et 1111111111197 ont même reste modulo 97 mais leurs deux derniers chiffres sont différents.