HLMA304, Arithmétique
Examen, Deuxième session, avril 2017

— 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. Trouver l'ensemble des entiers x tels que :

$$\begin{cases} 9x \equiv 12 & [21] \\ x \equiv 2 & [3] \end{cases}$$

CORRECTION : On observe que $9x \equiv 12\ [21] \iff 3x \equiv 4\ [7]$. Quelques calculs montrent que l'inverse de 3 dans $\mathbb{Z}/7\mathbb{Z}$ est 5. Cette équations équivaut donc à $x \equiv 5 \times 4 \equiv 6[7]$.
Le système à résoudre est donc :

$$\begin{cases} x \equiv 6 & [7] \\ x \equiv 2 & [3] \end{cases}$$

Puisque $\text{pgcd}(7,3) = 1$, on peut utiliser le théorème des restes chinois (et sa preuve). On trouve par exemple une solution particulière x_0 en calculant les premiers nombres $6, 6+7 = 13, 6+2.7 = 20$; $20 = 3.6 + 2$ est bien une solution particulière. L'ensemble des solutions est donc :

$$S = \{20 + 21k, \quad k \in \mathbb{Z}\}$$

Exercice 2.

(1) Soient $(a, b) \in \mathbb{Z}^2$ montrer l'équivalence suivante :

$$a \equiv b\ [42] \iff \begin{cases} a \equiv b & [2] \\ a \equiv b & [3] \\ a \equiv b & [7] \end{cases}$$

CORRECTION : D'après un corollaire du lemme de Gauss, puisque $\text{pgcd}(2,3) = 1$, si $2|(a-b)$ et $3|(a-b)$, alors $6 = 2.3|(a-b)$. De même, si $6|(a-b)$ et $7|(a-b)$ alors $42 = 6.7|(a-b)$. Ceci montre l'implication $\Leftarrow$.
L'implication $\Rightarrow$ est immédiate.

(1) En déduire :

$$\forall n \in \mathbb{Z}, \qquad n^7 \equiv n\ [42]$$

CORRECTION : D'après le (1), il suffit de montrer que $n^7 \equiv n[2]$, $n^7 \equiv n[3]$ et $n^7 \equiv n[7]$.
Dans $\mathbb{Z}/2\mathbb{Z}$, $\overline{0}^7 = \overline{0}$ et $\overline{1}^7 = \overline{1}$.
Dans $\mathbb{Z}/3\mathbb{Z}$, $\overline{0}^7 = \overline{0}$, $\overline{1}^7 = \overline{1}$ et $(-\overline{1})^7 = (-\overline{1})$.
D'après le petit théorème de Fermat, si p est premier, $n^p \equiv n$ $[p]$, donc $n^7 \equiv n$ $[7]$.
Ceci prouve que $n^7 \equiv n[42]$.

Exercice 3.

Soit p un nombre premier impair, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments. Si $n \in \mathbb{Z}$, on note $\overline{n}$ la classe de n dans $\mathbb{F}_p$.

(1) Soient $a, b, c \in \mathbb{F}_p$; montrer que le polynôme

$$X^2 + bX + c \in \mathbb{F}_p[X]$$

possède une racine si et seulement si $\Delta = b^2 - \overline{4}c$ est un carré dans $\mathbb{F}_p$.

CORRECTION : Puisque $\mathbb{F}_p$ est un corps, on effectue les mêmes opérations que sur $\mathbb{R}$ ou $\mathbb{C}$:

$$X^2 + bX + c = \left(X + \frac{b}{2}\right)^2 + c - \left(\frac{b}{2}\right)^2 = \left(X + \frac{b}{2}\right)^2 - \frac{b^2 - 4c}{4} = \left(X + \frac{b}{2}\right)^2 - \frac{\Delta}{2^2}$$

Si $\Delta = \delta^2$ est un carré, le polynôme se factorise en : $\left(X + \frac{b}{2} - \frac{\delta}{2}\right).\left(X + \frac{b}{2} + \frac{\delta}{2}\right)$ et possède donc deux racines : $\frac{-b \pm \delta}{2}$ (une seule si $\delta = 0$).
Réciproquement, si x est une racine du polynôme, on a : $\left(x + \frac{b}{2}\right)^2 - \frac{\Delta}{2^2} = 0$, donc $\Delta = (2x + b)^2$ est un carré.

(1) Soit $x \in \mathbb{F}_p^*$. Montrer que, si x est un carré, alors $x^{\frac{p-1}{2}} = 1$.

CORRECTION : Si x est un carré, il existe $y \in \mathbb{F}_p^*$ tel que $x = y^2$. Alors $x^{\frac{p-1}{2}} = y^{p-1} = 1$ par le petit théorème de Fermat.

(1) En déduire qu'il n'existe pas de couple $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ tels que

$$a^2 + ab + b^2$$

est divisible par 7.

CORRECTION :
Le polynôme $X^2 + X + 1$ n'a pas de racine dans $\mathbb{F}_7$. Sinon, $\Delta = 1^2 - 4.1 = -3$ serait un carré et on aura donc :

$$\Delta^{\frac{7-1}{2}} = (-3)^3 = -27$$

Exercice 4.

(1) Déterminez le pgcd de 2873 et 1001, ainsi que deux entiers relatifs u et v tels que

$$2873u + 1001v = \text{pgcd}(2873, 1001).$$

CORRECTION : Effectuons la division euclidienne :

$$\begin{aligned} 2873 &= 2 \times 1001 + 871, & 1001 &= 1 \times 871 + 130 \\ 871 &= 6 \times 130 + 91, & 130 &= 1 \times 91 + 39 \\ 91 &= 2 \times 39 + 13, & 39 &= 3 \times 13 + 0 \end{aligned}$$

Le pgcd vaut donc 13.
Pour trouver u et v, on reprends les égalités ci-dessus en remontant :

$$\begin{aligned} 13 &= 91 - 2 \times 39 = 91 - 2 \times (130 - 91) = (-2).130 + (3).91 = (-2).130 + (3).(871 - 6 \times 130) \\ &= (3).871 + (-20).130 = (3).871 + (-20).(1001 - 871) = (-20).1001 + (23).871 \\ &= (-20).1001 + (23).(2873 - 2.1001) = (23).2873 + (-66).1001 \end{aligned}$$

En posant $u = 23$ et $v = -66$ on obtient bien :

$$2873u + 1001v = 13 = \text{pgcd}(2873, 1001)$$

(1) Décomposez 2873 et 1001 en facteurs premiers.

CORRECTION : On divise 2873 par 13 : $2873 = 221 \times 13$. La racine de 221 est inférieure à 15. Il suffit donc de tester la divisibilité de 221 par $2, 3, 5, 7, 11, 13$. On observe que $221 = 13 \times 17$.
On divise 1001 par 13 : $2873 = 221 \times 77 = 7 \times 11$. On a donc :

$$2873 = 13^2 \times 171001 = 7 \times 13 \times 11$$

(1) Quel est l'ensemble des couples d'entiers $(u, v) \in \mathbb{Z}^2$ tels que :

$$2873u + 1001v = 15?$$

CORRECTION : Cet ensemble est vide puisque 15 n'est pas un multiple du pgcd de 2873 et 1001.

Exercice 5. Vous demandez à un ami de multiplier par 13 le jour de sa naissance, de multiplier par 14 le mois de naissance, et d'additionner ces deux résultats pour former un nombre n qu'il vous communique.

Comment pouvez vous retrouver le jour et le mois de sa naissance ?

CORRECTION : Soit j le jour de naissance et m le mois de naissance, et $a = 13j + 14m$.
Modulo 13, on voit que $a \equiv m[13]$. De plus $0 \leq m < 13$. Donc m est le reste de la division euclidienne de a par 13.
On calcule ensuite $a - 14m$, que l'on divise par 13 pour obtenir j.