HLMA304, Arithmétique
Examen de première session, Janvier 2020

Durée : 2h

Téléphones, calculatrices et documents sont interdits

Exercice 1. *Cours*

Montrer le théorème de Wilson :

$$(p-1)! \equiv -1[p] \quad \Longleftrightarrow \quad p \text{ est premier.}$$

CORRECTION : Supposons que $(p-1)! \equiv -1[p]$. Si p n'est pas premier, on peut écrire $p = ab$ avec $1 < a, b < p$. Donc $a.(p-1)! = a.(2.\cdots \times b \times \cdots .(p-1)) = ab \times (...) \equiv 0[p]$. Mais, puisque $(p-1)! \equiv -1[p]$, alors $a.(p-1)! \equiv -a \not\equiv 0[p]$. Contradiction.

Supposons maintenant que p est premier. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc tous les éléments $1, 2, \ldots, p-1$ non nuls sont inversibles. Les seuls éléments qui sont leurs propres inverses sont les solutions du polynôme $X^2 - 1$, c'est à dire 1 et -1. Le produit $1 \times 2 \cdots \times (p-1)$ vaut donc -1 dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 2.

(1) Trouvez un couple $(u, v) \in \mathbb{Z}^2$ tel que $35u + 22v = 1$.

CORRECTION : Appliquons l'algorithme d'Euclide. On pose $r_{-1} = 35, r_0 = 22$, puis :

$$\begin{array}{rcrcrcll}
35 & = & 1 & \times & 22 & + & 13, & q_1 = 1, \quad r_1 = 13 \\
22 & = & 1 & \times & 13 & + & 9, & q_2 = 1, \quad r_2 = 9 \\
13 & = & 1 & \times & 9 & + & 4, & q_3 = 1, \quad r_3 = 4 \\
9 & = & 2 & \times & 4 & + & 1, & q_4 = 2, \quad r_4 = 1 \\
4 & = & 4 & \times & 1 & + & 0, & q_5 = 4, \quad \mathbf{r_5 = 0} : \text{Fin de l'algorithme.}
\end{array}$$

Le pgcd est le dernier reste non nul ; il vaut 1. En applique ensuite l'algorithme d'Euclide étendu (en "remontant" les calculs ci-dessus) et on obtient :

$$\begin{aligned}
1 &= 9 - 2.4 = 9 - 2(13 - 9) = (-2).13 + (3).9 = (-2).13 + (3)(22 - 13) \\
&= (3)22 + (-5).13 = (3)22 + (-5)(35 - 22) = (-5).35 + (8).22
\end{aligned}$$

On peut donc prendre –par exemple– $(u, v) = (-5, 8)$.

(1) Trouvez la plus petite solution positive de l'équation :

$$\begin{cases} x \equiv 10[22] \\ y \equiv 7[35] \end{cases}$$

Correction : D'après le théorème des restes chinois, une solution particulière de ce système est : $x_0 = 10.35u + 7.22v = 350.(-5) + 154.8 = -1750 + 1232 = -518$, et l'ensemble des solutions est :

$$\{-518 + k22.35 = -518 + k770, k \in \mathbb{Z}\}.$$

Le plus petit élément positif de cet ensemble est $-518 + 770 = 252$.

Exercice 3.

(1) Pour tout $k \in \mathbb{N}^*$, calculer le reste de la division euclidienne de 10^k modulo 6.
(*Indication : On pourra procéder par récurrence.*)

Correction : Travaillons dans l'anneau $\mathbb{Z}/6\mathbb{Z}$. Nous posons, pour tout $k \in \mathbb{N}^*$ l'hypothèse de récurrence :

$$H_k \ : \qquad \overline{10}^k = \overline{4}$$

Puisque $\overline{10}^1 = \overline{6} + \overline{4} = \overline{4}$, H_1 est vraie.
Supposons que H_k est vraie, alors $\overline{10}^{k+1} = \overline{10}^k\overline{10} = \overline{4}.\overline{4} = \overline{16} = \overline{2.6 + 4} = \overline{4}$. Donc H_{k+1} est vraie. Ainsi,

$$\forall k \in \mathbb{N}^*, \qquad 10^k \equiv 4[6]$$

(1) Montrer que

$$\sum_{k=1}^{10} 10^{10^k} \equiv 5[7].$$

Correction : Nous nous plaçons cette fois dans $\mathbb{Z}/7\mathbb{Z}$ (la barre au dessus des nombres entiers change donc de signification par rapport à la question précédente).
Puisque $\overline{10} \neq \overline{0}$, et que 7 est un nombre premier, le petit théorème de Fermat affirme que : $\overline{10}^6 = \overline{1}$.
Soit maintenant $k \in \mathbb{N}^*$. D'après la question précédente, on peut écrire : $10^k = 4 + 6r, r \in \mathbb{N}$. On en déduit :

$$\overline{10}^{10^k} = \overline{10}^{4+6r} = \overline{10}^4.\left(\overline{10}^6\right)^r = \overline{10}^4\overline{1}^r = \overline{10}^4 = \overline{3}^4 = \overline{9}^2 = \overline{2}^2 = \overline{4}$$

Il vient ensuite :

$$\overline{\sum_{k=1}^{10} 10^{10^k}} = \sum_{k=1}^{10} \overline{10}^{10^k} = \sum_{k=1}^{10} \overline{4} = 10.\overline{4} = \overline{3}.\overline{4} = \overline{12} = \overline{5}.$$

Exercice 4. Résoudre dans $(\mathbb{N}^*)^2$ le système :

$$\begin{cases} x \wedge y &= x - y \\ x \vee y &= 72 \end{cases}$$

Correction : Écrivons $d = x \wedge y$, $x = dx'$ et $y = dy'$. On sait que $x \vee y = dx'y'$ et le système devient :

$$\begin{cases} d & = dx' - dy' \\ dx'y' & = 72 \end{cases} \iff \begin{cases} y' & = x' - 1 \\ dx'(x'-1) & = 72 \end{cases}$$

Les diviseurs de 72 sont :

$$\mathcal{D}(72) = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$$

Puisque x' et $x' - 1$ divisent tous deux 72, on a forcément :

$$x' \in \{9, 4, 3, 2\}$$

Si $x' = 9$, $x' - 1 = 8$ et $d = 1$; donc $(x, y) = (9, 8)$.
Si $x' = 4$, $x' - 1 = 3$ et $d = 6$; donc $(x, y) = (24, 18)$.
Si $x' = 3$, $x' - 1 = 2$ et $d = 12$; donc $(x, y) = (36, 24)$.
Si $x' = 2$, $x' - 1 = 1$ et $d = 36$; donc $(x, y) = (72, 36)$.
L'ensemble des solutions (x, y) est : $\{72, 36), (36, 24), (24, 18), (9, 8)\}$.

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.