بِسمِ اللهِ الرَّحمٰنِ الرَّحِيمِ

Devoir Surveillé $N°$ 3

Il sera tenu compte, dans l'appréciation des copies, de la précision des raisonnements ainsi que la clarté de la rédation.

PCSI

Questions de Cours

Cours

Exercice 1

$$\left\{\begin{array}{rcl} x+y+z & = & 0 \\ 2x+y+z & = & 1 \\ 3x+y-z & = & 0 \end{array}\right. \underset{L_3\leftarrow L_3-3L_1}{\overset{L_2\leftarrow L_2-2L_1}{\Rightarrow}} \left\{\begin{array}{rcl} x+y+z & = & 0 \\ -y-z & = & 1 \\ -2y-4z & = & 0 \end{array}\right. \underset{L_3\leftarrow L_3-2L_2}{\Rightarrow} \left\{\begin{array}{rcl} x+y+z & = & 0 \\ -y-z & = & 1 \\ -2z & = & -2 \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} x & = & -y-z=-1 \\ y & = & -1-z=2 \\ z & = & 1 \end{array}\right.$$

$S=\{(-1,2,1)\}$.

Exercice 2

$$\left\{\begin{array}{rcl} x+2y+3z+2t+s & = & 1 \\ 2x+y+z+t+s & = & 2 \end{array}\right. \underset{L_2\leftarrow L_2-2L_1}{\Rightarrow} \left\{\begin{array}{rcl} x+2y+3z+2t+s & = & 1 \\ -3y-5z-3t-s & = & 0 \end{array}\right.$$

Les inconnues principales sont : x et y.

Les inconnues secondaires sont : z, t et s.

On obtient, $\left\{\begin{array}{rcl} x & = & -2y-3z-2t-s+1 \\ y & = & -\frac{5}{3}z-t-\frac{1}{3}s \end{array}\right.$ et donc $\left\{\begin{array}{rcl} x & = & \frac{1}{3}z-\frac{1}{3}s+1 \\ y & = & -\frac{5}{3}z-t-\frac{1}{3}s \end{array}\right.$

$S=\{(\frac{1}{3}z-\frac{1}{3}s+1,-\frac{5}{3}z-t-\frac{1}{3}s,z,t,s)\in\mathbb{R}^5 \ / z,t,s\in\mathbb{R}\}$

Exercice 3

1. $34x+26y=15 \Leftrightarrow 2(17x+13)=15$. Puisque 2 n'est pas un diviseur de 15, $S=\emptyset$.
2. L'équation $14x+3y=2$ (pour cette équation $14\wedge 3=1$ divise 2).
   Recherche d'une solution particulière par l'algorithme d'Euclide :
   La division euclidienne de 14 par 3 : $14=3\times 4+2$
   La division euclidienne de 3 par 2 : $3=2\times 1+1$ (le reste est le pgcd).
   On remonte les calcules : $1=3+(-1)2=3+(-1)(14+3(-4))=3\times 5+14\times(-1)$, on multiplie par 2, il vient que $2=14\times(-2)+3\times 10$. Une solution particulière est donnée par $(x_0,y_0)=(-2,10)$.
   Les solutions générales :soit $(x,y)\in\mathbb{Z}^2$ une solution de l'équation
   $14x+3y=2=14x_0+3y_0$, donc $14(x-x_0)=3(y_0-y)$, en particulier 14 divise $3(y_0-y)$ et comme 14 et 3 sont premier entre eux, par l' théorème de Gauss , 14 divise y_0-y, il existe alors $k\in\mathbb{Z}$ tel que $y_0-y=14k$ i.e $y=y_0-14k$. Maintenant on remplace y par sont expression dans l'équation on obtient, $14(x_-x_0)=3\times 14k$, ou encore $x-x_0=3k$, on a donc $x=x_0+3k$. Ainsi

$(x,y) = (x_0+3k, y_0-14k) = (-2+3k, 10-14k)$, on vérifie facilement qu'un élément de cette forme est solution de l'équation.
$S = \{(-2+3k, 10-14k) \in \mathbb{Z}^2 \ / \ k \in \mathbb{Z}\}$

3. Notons $d = n \wedge (n+1)$. On a donc $d|n$ et $d|n+1$ donc $d|(n+1)-n = 1$, d'où $d = 1$.

PROBLÈME

Autour des congruences

Soit $n \in \mathbb{Z}$, et $a, b \in \mathbb{Z}$. On dit que a est congrue à b modulo n et on note $a \equiv b[n]$, si n divise $b-a$.
Ainsi $a \equiv b[n]$ si, et seulement si, $\exists k \in \mathbb{Z}$ tel que $b-a = kn$.

Première partie : Questions préliminaires

1. Réflexive : Soit $a \in \mathbb{Z}$, on a $n|0 = a-a$, donc $a \equiv a[n]$.
Symétrique : Si $a \equiv b[n]$, alors $n|b-a$, et donc $n|a-b$, d'où $b \equiv a[n]$.
Transitive : Si $a \equiv b[n]$ et $b \equiv c[n]$, alors $n|b-a$ et $n|c-b$, donc $n|(c-b)+(b-a) = c-a$, d'où $a \equiv c[n]$.
Il s'agit bien d'une relation d'équivalence.

2. $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$.Il existent $l, l' \in \mathbb{Z}$ tels que $b-a = ln$ et $b'-a' = l'n$, donc $(b+b')-(a+a') = (l+l')n$, d'où $a+a' \equiv b+b'[n]$.
Si de plus $k \in \mathbb{Z}$, alors $kb-ka = kln$, et donc $ka \equiv kb[n]$.

3. $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$. Il existent $l, l' \in \mathbb{Z}$ tels que $b-a = ln$ et $b'-a' = l'n$, ou encore $b = a+ln$ et $b' = a'+l'n$, on a donc $bb' = aa'+(al'+a'l+ll'n)n$ c'est-à-dire $bb'-aa' = (al'+a'l+ll'n)n$, d'où $aa' \equiv bb'[n]$.
Pour le reste de cette question on peut raisonner par récurrence sur k :
Pour $k = 0$: $a^0 = 1 \equiv 1 = b^0$ (la relation est réflexive).
Soit $k \in \mathbb{N}$, et on suppose que $a^k \equiv b^k[n]$. On a $a \equiv b[n]$ et $a^k \equiv b^k[n]$, par le premier résultat de cette question on a $a^{k+1} = a^k a \equiv b^k b = b^{k+1}[n]$. D'où le résultat.

4. Soit $a \in \mathbb{Z}$ et r le reste de la division euclidienne de a par n. a s'écrit sous la forme $a = qn+r$ (q le quotient et r le reste), donc $a-r = qn$, puis $a \equiv r[n]$.
Si n divise a alors $r = 0$, et donc $a \equiv 0[n]$.
Réciproquement, si $a \equiv 0[n]$, alors n divise $a-0 = a$.

5. Une application : Soit $n \in \mathbb{N}$. Il s'agit de montrer que $4^{2n+1}+3^{n+2} \equiv 0[13]$ ou encore $4^{2n+1} \equiv -3^{n+2}[13]$.
On a $4^{2n+1} = 4 \times 16^n$ et $3^{n+2} = 9 \times 3^n$.
D'autre par $4 \equiv -9[13]$ (car 13 divise $3-(-9) = 13$). Et $16 \equiv 3[13]$ donc $16^n \equiv 3^n[13]$, d'où $4 \times 16^n \equiv -9 \times 3^n[n]$, il vient alors que $4^{2n+1} \equiv -3^{n+2}[13]$

Deuxième partie : Théorème chinois

Dans *cette partie* on fixe deux entiers n et m **premier entre eux**.

6. n et m sont premier entre eux, donc par le théorème de Bézout, il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que $nu+mv = 1$.

7. $nu+mv = 1$, donc $1-nu = vm$ (multiple de m), d'où $nu \equiv 1[m]$.
$nu+mv = 1$, donc $1-mv = un$ (multiple de n), d'où $mv \equiv 1[n]$.

8. Soit maintenant $(a,b) \in \mathbb{Z}^2$.
On pose $x_0 = nua+mvb$.

8.1 Modulo m : $x_0 \equiv nua + mvb \equiv nua \equiv a[m]$ (car $nu \equiv 1[m]$).
Modulo n : $x_0 \equiv nua + mvb \equiv mvb \equiv b[m]$ (car $mv \equiv 1[n]$).

8.2 On a $x \equiv a[m]$ et $x_0 \equiv a[m]$, donc $x \equiv x_0[m]$, ainsi m divise $x - x_0$.

8.3 On a $x \equiv b[n]$ et $x_0 \equiv b[n]$, donc $x \equiv x_0[n]$, ainsi n divise $x - x_0$.

8.4 On a n divise $x - x_0$ et n divise $x - x_0$ et puisque n et m sont premiers entre eux, alors nm divise $x - x_0$ (Par le théorème d'Euclide).

8.5 nm divise $x - x_0$, il existe alors $k \in \mathbb{Z}$ tel que $x - x_0 = kmn$, c'est-à-dire $x = x_0 + knm$.

Troisième partie : Vers le théorème de Wilson

Dans cette partie p est un **nombre premier** ≥ 2.
Pour $n \in \mathbb{Z}$, on note $f(n)$ le reste de la division euclidienne de n par p.

9. $n \equiv f(n)\ [p]$ par le résultat de la question 4.

10. On a $n = f(n)[p]$ et $m = f(m)[p]$, donc (par le résultat de la question 3) $nm \equiv f(n)f(m)\ [p]$.
On a $nm \equiv f(nm)\ [p]$ et $nm \equiv f(n)f(m)[p]$ donc (par transitivité) $f(nm) = f(n)f(m)[p]$.

11. Soit $n \in \{1, \ldots, p-1\}$.

11.1 Puisque $1 \leq n < p$, donc p ne divise pas n et comme p et premier, alors n et p sont premiers entre eux.

11.2 p et n sont premiers entre eux, d'après le théorème de Bézout, il existe $(l, l') \in \mathbb{Z}^2$ tel que $nl + l'p = 1$ c'est-à-dire $1 - ln = l'p$, et donc $ln \equiv 1[p]$.

11.3 En effectuant la division euclidienne de l par p, il existe $(q, n') \in \mathbb{Z} \times \mathbb{N}$ tel que $l = qp + n'$ avec $0 \leq n' \leq p-1$, donc $nn' = n(l - qp) = nl - qp$, d'où $nn' \equiv nl \equiv 1[p]$ (car $qp = 0[p]$). De plus $n' \neq 0$: car si $n' = 0$, alors $1 \equiv nn' \equiv 0[p]$, et dans ce cas p divise 1 ce qui est impossible.
Conclusion : Il existe $n' \in \{1, \ldots, p-1\}$ tel que $nn' \equiv 1[p]$.

12. Si $n^2 \equiv 1[p]$ alors $p | n^2 - 1 = (n-1)(n+1)$, comme p premier, alors $p | n-1$ ou $p | n+1$ et donc $n \equiv 1[p]$ ou $n \equiv -1[p]$

END