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

1. Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$, rappeler le théorème de division euclidienne de a par b.
2. Rappeler le théorème de Bézout.
3. Rappeler le théorème de Gauss.
4. Rappeler la définition d'un nombre premier.

Exercice 1

Résoudre le système linéaire suivant :

$$\begin{cases} x+y+z &= 0 \\ 2x+y+z &= 1 \\ 3x+y-z &= 0 \end{cases}$$

Exercice 2

Résoudre le système linéaire suivant :

$$\begin{cases} x+2y+3z+2t+s &= 1 \\ 2x+y+z+t+s &= 2 \end{cases}$$

Exercice 3

1. Résoudre dans $\mathbb{Z}^2$ l'équation $34x+26y=15$.
2. Résoudre dans $\mathbb{Z}^2$ l'équation $14x+3y=2$.
3. Soit $n \in \mathbb{N}$, montrer que $n \wedge (n+1) = 1$.

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. Montrer que $\equiv$ est une relation d'équivalence.(reflexive symétrique et transitive).
2. Soient $a, a', b, b' \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$.
   Montrer que $a + a' \equiv b + b'\ [n]$, et que pour tout $k \in \mathbb{Z}$, $ka \equiv kb\ [n]$.
3. Soient $a, a', b, b' \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$.
   Montrer que $aa' \equiv bb'\ [n]$, et que pour tout $k \in \mathbb{N}$, $a^k \equiv b^k\ [n]$.
4. Soit $a \in \mathbb{Z}$ et r le reste de la division euclidienne de a par n. Montrer que $a \equiv r\ [n]$.
5. Soit $a \in \mathbb{Z}$. Montrer que n divise a si, et seulement si, $a \equiv 0\ [n]$.
6. Une application : Soit $n \in \mathbb{N}$. Montrer que 13 divise $4^{2n+1} + 3^{n+2}$.

Deuxième partie : Théorème chinois

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

7. Vérifier l'existence d'un couple $(u, v) \in \mathbb{Z}^2$ tel que $nu + mv = 1$.
8. Montrer que $nu \equiv 1\ [m]$ et $mv = 1\ [n]$.
9. Soit maintenant $(a, b) \in \mathbb{Z}^2$.
   On pose $x_0 = nua + mvb$.
   - 9.1 Montrer que $x_0 \equiv a\ [m]$ et $x_0 \equiv b\ [n]$.
     Soit $x \in \mathbb{Z}$ tel que $x \equiv a\ [m]$ et $x \equiv b\ [n]$.
   - 9.2 Montrer que m divise $x - x_0$.
   - 9.3 Montrer que n divise $x - x_0$.
   - 9.4 En déduire que nm divise $x - x_0$.
   - 9.5 Montrer qu'il existe $k \in \mathbb{Z}$ tel que $x = x_0 + knm$.

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.

10. Vérifier que pour tout $n \in \mathbb{Z}$, $n \equiv f(n)\ \ [p]$
11. Montrer que pour tout $n, m \in \mathbb{Z}$, $nm \equiv f(n)f(m)\ \ [p]$.
    En déduire que $f(nm) \equiv f(n)f(m)\ \ [p]$.
12. Soit $n \in \{1, \ldots, p-1\}$.
    - 12.1 Vérifier que n et p sont premier entre eux.
    - 12.2 En déduire qu'il existe $l \in \mathbb{Z}$ tel que $nl \equiv 1\ \ [p]$.
    - 12.3 Montrer qu'il existe $n' \in \{1, \ldots, p-1\}$ tel que $nn' \equiv 1\ \ [p]$.
      Indication : On pourra effectuer la division euclidienne de l par p.
13. Soit $n \in \mathbb{Z}$ tel que $n^2 \equiv 1\ \ [p]$. Montrer que $n \equiv 1\ \ [p]$ ou $n \equiv -1\ \ [p]$

END