Devoir Surveillé N° 3

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

PCSI

Questions de cours

1. Rappeler la définition d'un nombre premier.
2. Rappeler la définition de deux entiers premiers entre eux.
3. Enoncer le théorème de la division euclidienne.
   Soit $f : E \to F$ une application, A une partie de E et B une partie de F.
4. Rappeler la définition de $f(A)$.
5. Rappeler la définition de $f^{-1}(B)$.

Exercice 1

Résoudre, en indiquant les opérations élémentaires, le système linéaire suivant :

$$\begin{cases} x + 2y + z + t &= 1 \\ x + y - z - t &= 2 \\ 2x + 4y + z + 2t &= 3 \end{cases}$$

Exercice 2

Résoudre dans $\mathbb{Z}^2$ les deux équations suivantes :

1. $15x + 12y = 3$.
2. $55x + 22y = 40$.

Exercice 3

Soit n un entier impair. Montrer que les deux entiers n et $n+2$ sont premiers entre eux.

Exercice 4

Soient a et b deux entiers premiers entre eux.

1. Vérifier que a^2 et b^2 sont premiers entre eux.
2. Montrer que $a+b$ et ab sont premiers entre eux.

PROBLÈME

Petit théorème de Fermat

Dans tout le problème p désigne un entier premier ≥ 2.

Questions préliminaires

1. Soient $a_1, \dots, a_n \in \mathbb{Z}$. Montrer que si p divise le produit $a_1 \dots a_n$ alors p divise l'un des entiers a_i. Indication : on pourra raisonner par récurrence.
2. Montrer que p et $(p-1)!$ sont premiers entre eux. Indication : utiliser le résultat de la question précédente.
3. Soit $n \in \mathbb{Z}$ et r le reste de la division euclidienne de n par p. Justifier que p divise $n-r$.
4. Soient k, k' deux entiers tels que $1 \leq k, k' \leq p-1$. Montrer que si p divise $k-k'$ alors $k = k'$. Indication : justifier d'abord que $|k-k'| < p$.
5. Soient $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z}$ tels que pour tout $1 \leq i \leq n$, p divise $a_i - b_i$. Montrer que p divise $\prod_{i=1}^{n} a_i - \prod_{i=1}^{n} b_i$. Indication : on pourra raisonner par récurrence sur n.

Première partie : Petit théorème de Fermat

Dans cette partie A désigne l'ensemble $A = \{1, 2, \dots, p-1\}$ et $a \in \mathbb{Z}$. Pour $k \in A$, on note r_k le reste de la division euclidienne de ka par p.

6. Montrer que si p n'est pas premier avec a alors p divise $a^p - a$.
On suppose, jusqu'à la fin de cette partie, que a et p sont premiers entre eux.
7. Justifier, pour $k \in A$, que $r_k \in A$ et que p divise $ka - r_k$.
8. En déduire que p divise $(p-1)!a^{p-1} - \prod_{k=1}^{p-1} r_k$. Indication : utiliser le résultat de la question 5.
9. Soient $k, k' \in A$. Montrer que si $r_k = r_{k'}$ alors $k = k'$. En déduire que $A = \{r_1, r_2, \dots, r_{p-1}\}$.
10. Montrer que $\prod_{k=1}^{p-1} r_k = (p-1)!$. Indication : utiliser le résultat de la question précédente.
11. Montrer que p divise $a^{p-1} - 1$, puis que p divise $a^p - a$. Indication : exploiter les résultats des questions 2. et 8..

Deuxième partie : Une application

Soient p et q deux entiers premiers positifs distincts ($p \neq q$) et $m = pq$.

12. Justifier que $p \wedge q = 1$.
13. Soit $a \in \mathbb{Z}$. Montrer que a est premier avec m si, et seulement si, a est premier avec p et q.
On suppose, dans la suite de cette partie, que a est premier avec m.
14. Montrer que $a^{p-1} - 1$ et $a^{q-1} - 1$ divisent $a^{(p-1)(q-1)} - 1$.
15. En déduire que p et q divisent $a^{(p-1)(q-1)} - 1$
16. Montrer que m divise $a^{(p-1)(q-1)} - 1$.