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

Corrigé

Questions de cours

Cours

Exercice 1

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

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

On effectuant les deux opérations élémentaires $L_2 \leftarrow L_2 - L_1$ et $L_2 \leftarrow L_3 - 2L_1$, on obtient le système équivalent suivant

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

Ce dernier est échelonné avec t comme paramètre (secondaire). On a donc $z = -1$, $y = -2z-2t-1 = 1-2t$ et $x = 1-2y-z-t = 3t$. D'où

$$S = \{(3t, 1-2t, -1, t) \ / \ t \in \mathbb{K}\}$$

Exercice 2

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

1. L'équation est équivalente à $5x+4y = 1$, pour cette dernière équation les coefficients sont premiers entre eux.
   Recherche d'une solution particulière : On a $5 = 4\times 1+1$, donc $1 = 5\times 1+4\times(-1)$, ainsi $(x_0, y_0) = (1,-1)$ est une solutions particulière.
   Résolution de l'équation : Soit (x,y) une solution de de l'équation. On a $5x+4y = 1 = 5x_0+4y_0$, donc $(\star)$ $5(x-x_0) = 4(y_0-y)$. il vient que 5 divise $4(y_0-y)$, or $5\wedge 4 = 1$, il s'en suit que 5 divise (y_0-y), il existe $k \in \mathbb{Z}$ tel que $y_0-y = 5k$ ou encore $y = y_0-5k$. On remplace dans $(\star)$ on obtient $5(x-x_0) = 4\times 5k$. Ainsi $x = 4k+x_0$. On vérifie facilement que $(4k+x_0, y_0-5k)$ est une solution de l'équation, d'où

$$S = \{(4k+1, -1-5k) \ / \ k \in \mathbb{Z}\}$$

2. L'équation est équivalente à $11(5x+2y)=40$, or 11 ne divise pas 40, l'équation n'admet pas de solution, d'où $S=\emptyset$.

Exercice 3

Posons $d=n\wedge(n+2)$. On a d divise n et $n+2$ donc d divise $(n+2)-n=2$, par suite $d=1$ ou $d=2$. Or n est impair, $d\neq 2$. D'où $d=1$.

Exercice 4

Soient a et b deux entiers premiers entre eux.

1. Posons $d=a^2\wedge b^2$ et supposons par l'absurde que $d\neq 1$. L'entier d admet au moins un diviseur premier p. On a p divise a^2 donc p divise a, de même p divise b. Il en résulte que p divise $a\wedge b=1$, ce qui est impossible. D'où $a^2\wedge b^2=1$.
2. Posons $d=(a+b)\wedge(ab)$ et supposons par l'absurde que $d\neq 1$. l'entier d admet au moins un diviseur premier p. On a p divise ab donc p divise a ou divise b. Si p divise a alors p divise $(a+b)-a=b$, par suite p divise a et b, donc divise $a\wedge b=1$, ce qui est impossible. Si p divise b, on démontre de même que p divise $a\wedge b=1$, ce qui est aussi impossible. Il vient alors que $d=1$.

PROBLÈME

Petit théorème de Fermat

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

Questions préliminaires

1. Par récurrence sur n. Le résultat est immédiat pour $n=1$. Supposons le résultat vrai pour un certain $n\geq 1$. Soient $a_1,\dots,a_n,a_{n+1}\in\mathbb{Z}$ tel que p divise $a_1\dots a_n a_{n+1}$. Puisque p est premier, p divise $a_1\dots a_n$ ou p divise a_{n+1}. Si p divise a_{n+1}, c'est fait (dans ce cas $i=n+1$). Si p divise le produit $a_1\dots a_n$, d'après l'hypothèse de récurrence p divise l'un des a_i pour $1\leq i\leq n$. D'où le résultat.
2. Si p et $(p-1)!$ ne sont pas premiers entre eux alors p divise $(p-1)!=1.2\dots(p-1)$ car p est premier. D'après le résultat de la question précédente, p divise l'un des termes du produit, c'est-à-dire divise k où $1\leq k\leq p-1<p$, ce qui impossible.
3. Il existe $q\in\mathbb{Z}$ tel que $n=pq+r$, donc $n-r=pd$ est divisible par p.
4. On a $1\leq k'\leq p-1$ donc $-p+1)\leq -k'\leq 1$, par suite $2-p\leq k-k'\leq p-2$, par suite $|k-k'|\leq p-2<p$. Or p divise $k-k'$, p divise aussi $|k-k'|$. D'où $|k-k'|=0$ c'est-à-dire $k=k'$.
5. Le résultat est immédiat pour $n=1$. Supposons le résultat vrai pour un certain $n\geq 1$. Soient $a_1,\dots,a_n,a_{n+1},b_1,\dots,b_n,b_{n+1}\in\mathbb{Z}$ tels que pour tout $1\leq i\leq n+1$, p divise a_i-b_i. D'après l'hypothèse de récurrence p divise $\prod_{i=1}^n a_i-\prod_{i=1}^n b_i$, il existe alors $s\in\mathbb{Z}$ tel que $\prod_{i=1}^n a_i-\prod_{i=1}^n b_i=sp$ ou encore $\prod_{i=1}^n a_i=\prod_{i=1}^n b_i+sp$. Or p divise $a_{n+1}-b_{n+1}$, il existe $t\in\mathbb{Z}$ tel que $a_{n+1}=b_{n+1}+tp$. En multipliant les égalités précédentes membre par membre, on obtient,

$$a_{n+1}\prod_{i=1}^n a_i=(\prod_{i=1}^n b_i+sp)(b_{n+1}+tp)=(\prod_{i=1}^n b_i)b_{n+1}+p(sb_{n+1}+t\prod_{i=1}^n b_i+stp)$$

Ainsi $\prod_{i=1}^{n+1} a_i-\prod_{i=1}^{n+1}=p(sb_{n+1}+t\prod_{i=1}^n b_i+stp)$. Il en résulte alors que p divise $\prod_{i=1}^{n+1} a_i-\prod_{i=1}^{n+1}$. La récurrence est achevée.

Première partie :
Petit théorème de Fermat

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

6. Si p n'est pas premier avec a alors p divise a car p est premier. Par suite p divise $a^p - a$.
On suppose, jusqu'à la fin de cette partie, que a et p sont premiers entre eux.

7. On sait que $0 \leq r_k \leq p-1$, il suffit alors de démontrer que $r_k \neq 0$. Supposons que $r_k = 0$, donc p divise ka. Or p est premier avec a, p divise k, ce qui est impossible car $1 \leq k < p$. On en déduit que $1 \leq r_k \leq p-1$ et donc $r_k \in A$. D'après le résultat de la question 3., p divise $ka - r_k$.

8. Pour $1 \leq k \leq p-1$, p divise $ka - r_k$, d'après le résultat de la question 4, p divise $\prod_{k=1}^{p-1} ka - \prod_{k=1}^{p-1} r_k k = a^{p-1} \prod_{k=1}^{p-1} k - \prod_{k=1}^{p-1} r_k = (p-1)!a^{p-1} - \prod_{k=1}^{p-1} r_k$.

9. Soient $k, k' \in A$ tels que $r_k = r_{k'}$. Ils existent $q, q' \in \mathbb{Z}$ tels que $ka = pq + r_k$ et $k'a = pq' + r_{k'}$, et donc $(k-k')a = p(q-q') + r_k - r_{k'} = p(q-q')$. Il s'en suit que p divise $(k-k')a$, or p et a sont premiers entre eux, p divise $k-k'$, il en résulte, par le résultat de la question 4., que $k = k'$. De plus l'ensemble A a exactement $p-1$ éléments, or $r_1, \ldots, r_{p-1}$ sont $p-1$ éléments deux à deux distincts de A, il découle que $A = \{r_1, \ldots, r_{p-1}\}$.

10. D'une part, le produit de tous les éléments de A est $1 \times \ldots \times (p-1) = (p-1)!$. D'autre par, puisque $A = \{r_1, \ldots, r_{p-1}\}$, le produit de tous les éléments de A vaut $\prod_{k=1}^{p-1} r_k$. D'où $\prod_{k=1}^{p-1} r_k = (p-1)!$.

11. D'après le résultat de la question 8., on a p divise $(p-1)!a^{p-1} - \prod_{k=1}^{p-1} r_k$, le résulte de la question précédente affirme que $(p-1)!a^{p-1} - \prod_{k=1}^{p-1} r_k = (p-1)!a^{p-1} - (p-1)! = (p-1)!\left(a^{p-1} - 1\right)$. Or, d'après le résultat de la question 2, p et $(p-1)!$ sont premiers entre eux, il vient que p divise $a^{p-1} - 1$. En particulier p divise $a(a^{p-1} - 1) = a^p - a$.

Deuxième partie :
Une application

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

12. L'entier q est premier différent de p, donc p n'est pas un diviseur de q. Or p est premier et ne divise pas q, on a donc $p \wedge q = 1$.

13. Supposons que a et m sont premiers entre eux. Par le théorème de Bézout, ils existent $u, v \in \mathbb{Z}$ tels que $au + mv = 1$, puis $au + p(qv) = au + q(pv) = 1$, donc a est premier avec p et q. Réciproquement, supposons que a et premier avec p et q. Par le théorème de Bézout, ils existent $(u, v), (u', v') \in \mathbb{Z}^2$ tels que $au + pv = 1$ et $au' + qv' = 1$. En multipliant les deux égalités précédentes membre par membre, on obtient

$$a(auu' + uqv' + u'pv) + m(vv') = 1$$

Donc a et m sont premiers entre eux.
On suppose, dans la suite de cette partie, que a est premier avec m.

14. Rappelons d'abord que $x^l - 1 = (x-1)(1 + x + \ldots + x^{l-1})$.
Par l'identité de factorisation on a

$$a^{(p-1)(q-1)} - 1 = (a^{p-1})^{q-1} - 1 = (a^{p-1} - 1)(1 + a^{p-1} + \ldots + (a^{p-1})^{q-2})$$

Donc $a^{p-1} - 1$ divise $a^{(p-1)(q-1)} - 1$. De même pour $a^{q-1} - 1$.

15. Puisque a est premier avec m, a est premier avec p et q. D'après le résultat de la question 11., p divise $a^{p-1}-1$, le résultat de la question précédente affirme que p divise $a^{(p-1)(q-1)}-1$. Par un même raisonnement, q divise $a^{(p-1)(q-1)}-1$.

16. Les deux entiers p et q divisent $a^{(p-1)(q-1)}-1$, or ces nombres sont premiers entre eux, il vient alors pq divise $a^{(p-1)(q-1)}-1$.