Devoir Libre $N°$ 2

n Arithmétiques dans $\mathbb{Z}$ m

PCSI

Exercice 1

Résoudre dans $\mathbb{Z}^2$ l'équation : $\quad 26x + 14y = 6$.

PROBLÈME

Première partie
Une démonstration du théorème de Bézout

Le but de cette partie est de démontrer le théorème de Bézout : Si $a, b \in \mathbb{Z}$, et $d = a \wedge b$, alors ils existent $u, v \in \mathbb{Z}$ tels que $au + bv = d$.
On considère deux entiers $a, b \in \mathbb{Z}$ non nuls et notons $d = a \wedge b$. On pose $H = \{an + bm \,/\, n, m \in \mathbb{Z}\}$.

1. Montrer que si $x \in H$, alors $-x \in H$.
2. Montrer que si $x, y \in H$, alors $x + y \in H$, en déduire que si $x \in H$ et $k \in \mathbb{Z}$, alors $kx \in H$.
3. Montrer que si $x, y \in H$, alors $x - y \in H$.
   Dans la suite de cette partie , on pose $H^+ = H \cap \mathbb{N}^*$.
4. Justifier que H^+ est non vide, en déduire que H^+ admet un plus petit élément δ.
5. Montrer que d divise δ, en déduire que $d \leq \delta$.
6. Notons r le reste de la division euclidienne de a par δ de sorte que $a = k\delta + r$. Montrer que $r \in H$, en déduire que $r = 0$.
7. Montrer que δ divise b.
8. En déduire que $\delta = d$.
9. Conclusion.

Deuxième partie
Inverse modulo n

Soient $a, b \in \mathbb{Z}$, on dit que a est congrue à b modulo n et on note $a \equiv b\ [n]$, si $n|(b - a)$ (n divise $b - a$).

10. Montrer que la relation $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$.
11. Montrer que si $a \equiv b[n]$ et $k \in \mathbb{Z}$, alors $ka \equiv kb[n]$.
12. Montre que si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors $a + a' \equiv b + b'[n]$ et $aa' \equiv bb'[n]$.
13. Montrer que si r est le reste de la division euclidienne de a par n, alors $a \equiv r[n]$.
14. Soit $(a, n) \in \mathbb{Z}^2$ avec n non nul. On dit que a est inversible modulo n, s'il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv 1[n]$.
    - 14.1 On suppose que a admet un inverse a' modulo n i.e $aa' = 1[n]$. Montrer qu'il existe $b \in \mathbb{Z}$ tel que $aa' + bn = 1$. En déduire que a et n sont premiers entre eux.
    - 14.2 Montrer que si a et n sont premiers entre eux, alors a est inversible modulo n.

END