بِسمِ اللّهِ الرَّحمٰنِ الرَّحِيمِ

Devoir Libre N°

Arithmétiques dans $\mathbb{Z}$

PCSI

Définition

Définition :

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

PROBLEM
A royal road to Fermat's little Theorem

First Part
Congruence modulo

Dans cette partie, on fixe un entier $n \in \mathbb{Z}$.

1. Soit $(a, b) \in \mathbb{Z}^2$. Démontrer que $a \equiv b\ [n]$ si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.
2. Montrer que la relation $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$.
3. Montrer que si $a \equiv b[n]$ et $k \in \mathbb{Z}$, alors $ka \equiv kb[n]$.
4. Montre que si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors $a + a' \equiv b + b'\ [n]$ et $aa' \equiv bb'\ [n]$.
5. Montrer que si r est le reste de la division euclidienne de a par n, alors $a \equiv r[n]$.
6. Soit $a \in \mathbb{Z}$. Montrer que n divise a si, et seulement si, $a = 0\ [n]$.

Second part
Fermat's little theorem

Dans cette partie, p est un nombre premier positif.

7. Montrer que si $k \in [\![2, p-1]\!]$, alors $kC_p^k = pC_{p-1}^{k-1}$, et en déduire que p divise C_p^k.
   Hint : Do you know Gauss ?
8. Montrer que pour tous $n, m \in \mathbb{Z}$, $(n+m)^p = n^p + m^p\ [p]$.
   Hint : Use the Newton's binomial formula
9. En déduire que pour tout $n \in \mathbb{Z}$, $(n+1)^p = n^p + 1\ [p]$.
10. En déduire, par récurrence, que pour tout $n \in \mathbb{N}$, $n^p = n\ [p]$.
11. Montrer le résultat de la question précédente, lorsque $n \in \mathbb{Z}$.
12. Soit $n \in \mathbb{Z}$ un entier premier avec p. Montrer que $n^{p-1} = 1\ [p]$.
    Hint : Write the result of the previous question without modulo,....