DIVISISIBILITE DANS $\mathbb{Z}$ ET CONGRUENCES

Term - ME

I Divisibilité dans $\mathbb{Z}$

1.1 Multiples et diviseurs d'un nombre entier relatif

Définition

Vocabulaire

Exemples

Conséquences immédiates

Exemple

1.2 Propriétés de la divisibilité

Propriété *Transitivité*

Démonstration

Exemple

Propriété *Combinaison linéaire*

Démonstration

Vocabulaire

Conséquence

Exemple

Exercice 1

Soit n un entier impair. Démontrer que 8 divise n^2-1.

II <u>Division euclidienne</u>

Théorème et définition

Démonstration

• **Existence du couple $(q\,;r)$**

La suite des multiples de b est :

$$\ldots;-kb\,;\ldots;-2b\,;-b\,;0\,;b\,;2b\,;\ldots kb\,;\ldots \text{ avec } k\in\mathbb{N}.$$

<u>1^er^ cas</u> : a est un multiple de b.

Alors a est l'un des termes de la suite ci-dessus et il existe un nombre entier relatif q tel que $a=bq$.

<u>2^e^ cas</u> : a n'est pas un multiple de b.

Il existe des multiples de b inférieurs à a et d'autres supérieurs à a.

On peut écrire $bq<a<b(q+1)$ où $b(q+1)$ est le plus petit multiple de b supérieur à a.

Finalement, pour tout $a\in\mathbb{Z}$, il existe un entier relatif q tel que $bq\leqslant a<b(q+1)$,

c'est-à-dire $0\leqslant a-bq<b$.

On pose $r=a-bq$, on obtient $a=bq+r$ et $0\leqslant r<b$.

• **Unicité du couple $(q\,;r)$**

On suppose qu'il existe deux couples de nombres entiers relatifs $(q\,;r)$ et $(q'\,;r')$ tels que $a=bq+r$, $a=bq'+r'$ et $0\leqslant r<b$, $0\leqslant r'<b$.

Alors, par différence $0=b(q-q')+r-r'$, soit $r-r'=b(q'-q)$, donc $r-r'$ est un multiple de b.

De plus, $0\leqslant r<b$ et $-b<-r'\leqslant 0$, donc $-b<r-r'<b$.

Or, 0 est le seul multiple de b strictement compris entre $-b$ et b, donc $r-r'=0$, soit $r=r'$.

On en déduit que $b(q'-q)=0$; comme $b\neq 0$, $q'-q=0$, soit $q=q'$.

L'unicité du couple $(q\,;r)$ est ainsi prouvée.

Conséquence

Exemples

III Congruences

3.1 Définition et propriétés

Définition

Exemple

Propriété fondamentale

Démonstration

Exemples

Remarque

Propriétés

Démonstrations en exercice

Vocabulaire

Exemple

Définition

Exemple

3.2 Compatibilité avec les opérations

Propriétés

Démonstrations de (i), (ii) et (iii) en exercice

Démonstration de (iv)

Exemples

Exercice 2

Dans cette partie, on se propose de déterminer les couples $(n,\ m)$ d'entiers naturels non nuls vérifiant la relation :

$$7^n - 3 \times 2^m = 1 \quad \text{(F)}.$$

1. On suppose $m \leqslant 4$.
Montrer qu'il y a exactement deux couples solutions.

2. On suppose maintenant que $m \geqslant 5$.

a. Montrer que si le couple $(n,\ m)$ vérifie la relation (F) alors $7^n \equiv 1 \pmod{32}$.

b. En étudiant les restes de la division par 32 des puissances de 7, montrer que si le couple $(n,\ m)$ vérifie la relation (F) alors n est divisible par 4.

c. En déduire que si le couple $(n,\ m)$ vérifie la relation (F) alors $7^n \equiv 1 \pmod{5}$.

d. Pour $m \geqslant 5$, existe-t-il des couples $(n,\ m)$ d'entiers naturels vérifiant la relation (F) ?

3. Conclure, c'est-à-dire déterminer l'ensemble des couples d'entiers naturels non nuls vérifiant la relation (F).

D'après un sujet de BAC