Savoir A. 2: Congruences

Exercice 8 : Congruences, les bases

1) Compléter les tableaux :

Division euclidienne $a = bq + r$	Congruence $a \equiv r\ [b]$
$34 = 6 \times 5 + 4$	$34 \equiv \cdots\ [5]$
$17 = 2 \times 7 + 3$	$17 \equiv \cdots \bmod (7)$
$23 = \cdots \times 4 + \cdots$	$23 \equiv 3\ [4]$
$27 =$	$27 \equiv 0\ [9]$

Expressions $y - x = kn$	Congruences $y \equiv x\ [n]$
$34 - 19 = 3 \times 5$	$34 \equiv \cdots\ [5]$
$17 - (-4) = 3 \times 7$	$17 \equiv \cdots\ [7]$
$23 - \cdots = \cdots \times \ldots$	$23 \equiv -5 \bmod (4)$
$27 - \cdots$	$27 \equiv 18\ [9]$

2) *Exemple* **:** *On a* $35 \equiv 5\ [6]$ $\Rightarrow$ *on a aussi :* $35 \equiv 11\ [6]$ *ou :* $35 \equiv -1\ [6]$
En suivant l'exemple, donner dans chaque cas les 2 congruences les plus proches de celle donnée :celle d'après et celle d'avant.

a) $16 \equiv 2\ [7]$ **b)** $11 \equiv 5 \bmod (3)$ **c)** $25 \equiv -3\ [7]$ **d)** $43 \equiv -7\ [10]$ **e)** $33 \equiv 17 \bmod (8)$

3) Compléter les congruences $y \equiv x[n]$ avec $x \in [0; n-1]$

a) $18 \equiv \cdots\ [4]$ **b)** $41 \equiv \cdots \bmod(3)$ **c)** $27 \equiv \cdots [12]$ **d)** $50 \equiv \cdots\ [25]$ **e)** $61 \equiv \cdots mod(7)$

4) a) Les entiers 128 et 15 sont-ils congrus modulo 11 ? **b)** 214 et 25 sont-ils congrus modulo 9 ?

5) Vrai ou faux ? **a)** $132 \equiv 47\ [15]$ **b)** $1\,214 \equiv -8\ [44]$ **c)** $899 \equiv -1 \bmod (45)$

Exercice 9 : Réfléchir sur les congruences

1) On sait que $2015 \equiv r\ [7]$.
Déterminer r dans chaque cas : **a)** $r \in [0; 6]$ **b)** $r \in [15; 21]$ **c)** $r \in [-10;\ -4]$

2) a) Déterminer le plus petit entier positif r tel que $2017 \equiv r\ [10]$
b) Déterminer le plus petit entier en valeur absolue k tel que $2017 \equiv k\ [10]$

3) Effectuer la division euclidienne de 49 par 5, et traduire le résultat à l'aide d'une congruence.
Même chose pour la division euclidienne de 75 par 8 et celle de 610 par 9.

4) Un entier n vérifie $n \equiv 100 \bmod(11)$. Quel est le reste de la division euclidienne de n par 11 ?

5) Déterminer les entiers naturels n tels que $27 \equiv 5\ [n]$

6) a) Est-il vrai que tout nombre entier est congru modulo 3 à l'un des entiers 7 ; 8 ou 9 ?
b) Est-il vrai que tout nombre entier est congru modulo 3 à l'un des entiers -3 ; 28 ou 137 ?

7) Déterminer tous les entiers n compris entre 0 et 50 tels que $n \equiv 7\ [11]$

Exercice 10 : Opérations et congruences

1) a. Compléter le tableau de congruence ci-dessous

$x \equiv \cdots [6]$	0	1	2	3	4	5
$4x$						
$4x \equiv \cdots\ [6]$						

b. Utiliser ce tableau pour déterminer quels sont les restes possibles dans la division euclidienne de $4x$ par 6

c. Utiliser ce tableau pour déterminer si le nombre 4×39 est divisible par 6.

2) a. Compléter le tableau de congruence ci-dessous

$x \equiv \cdots [4]$	0	1	2	3
x^2				
$x^2 \equiv \cdots\ [4]$				

b. Quels sont les carrés divisibles par 4 ?

3) a. Compléter le tableau de congruence ci-dessous

$x \equiv \cdots [5]$	0	1	2	3	4
$4x - 9$					
$4x - 9 \equiv \cdots\ [5]$					

b. Sans la calculer, l'image de 16 par la fonction affine $f(x) = 4x - 9$ est-elle un multiple de 5 ?

4) a. Compléter ces tables d'additions et de multiplication modulo 5

$x + y \equiv \cdots [5]$		$x \equiv \cdots [5]$				
		0	1	2	3	4
$y \equiv \cdots [5]$	0					
	1					
	2					
	3					
	4					

$xy \equiv \cdots [5]$		$x \equiv \cdots [5]$				
		0	1	2	3	4
$y \equiv \cdots [5]$	0					
	1					
	2					
	3					
	4					

b. En déduire, sans les calculer, les restes dans la division euclidienne par 5, des nombres :
$A = 23 + 78$ $\quad B = 217 + 411$ $\quad C = 14 \times 76$ $\quad D = 852 \times 753$

Exercice 11 : Pareil en plus dur

1) $n \in \mathbb{N}^*$. Démontrer à l'aide d'un tableau de restes, que $n(n^2 - 4)$ est divisible par 3

2) Démontrer que, pour tout entier naturel n, le nombre $A = n(2n + 1)(n + 1)$ est divisible par 6.

Exercice 12 : Inverses modulo n

Définition : Soit $x \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

On dit que $\boldsymbol{x}$ **est inversible modulo** $\boldsymbol{n}$ quand il existe un entier y tel que : $\boldsymbol{xy \equiv 1\ [n]}$

* Attention il n'existe pas qu'un seul « inverse » modulo n, quand il en existe un, mais une infinité. Et il peut très bien ne pas en exister du tout.

1) Déterminer un inverse modulo 5 du nombre $x = 7$

2) a. En regardant le tableau de congruence de l'exercice 10 (1), pensez-vous qu'il soit possible de trouver un inverse modulo 6 pour le nombre 4 ?

b. En appliquant cette méthode, déterminer l'ensemble des inverses de 11 modulo 3.

3) On sait que $5^3 \equiv 1\ [31]$. En déduire un inverse de 5 modulo 31.