Maths XP Contrôle $n°2$ Lundi 24/ 11/2025 Thiaude P. + Vermeulen G.
1h Calculatrice interdite

Carl Friedrich GAUSS

(1777 – 1855)

Mathématicien, astronome et physicien allemand.
Est à l'origine de la notion de congruence.
(image : source Wikipedia)

Exercice 1 **[4 pts]** Démontrer que : $\forall n \in \mathbb{N}, 7|23^n - 9^n + 133$.

Exercice 2 **[4 pts]** Déterminer le reste de la division euclidienne de 8^{173} par 5.

Exercice 3 **[4 pts]**

1. Montrer que 6 n'a pas d'inverse modulo 8.
2. Soient $a \in \mathbb{Z}, m \in \mathbb{N}^*$ tels qu'il existe $d \in \mathbb{Z} \setminus \{-1; 1\}$ vérifiant : $d|a$ et $d|m$. Montrer que a n'a pas d'inverse modulo m.

Exercice 4 **[4 pts]**

Les questions **1.** et **2.** sont indépendantes.

1. Quel est le chiffre des unités de 3^{2025} ?
2. Montrer que $3^{10} \equiv 49\ [100]$ puis déterminer les deux derniers chiffres de 3^{2025}.

Exercice 5 **[4 pts]**

Les questions **1.** et **2.** sont indépendantes.

Soient a, b et c trois entiers relatifs tels que : $a^2 + b^2 = c^2$.

1. **Dans cette question on se propose de démontrer que : $3|abc$.**
   - **a.** Montrer que, pour tout $x \in \mathbb{Z}$, $x^2 \equiv 0\ ou\ 1\ [3]$.
   - **b.** Montrer que : si $a \equiv 0\ [3]$ ou $b \equiv 0\ [3]$, alors : $3|abc$.
   - **c.** On suppose que : $a \not\equiv 0\ [3]$ et $b \not\equiv 0\ [3]$, justifier que $a^2 + b^2 \equiv 2\ [3]$ puis établir une contradiction.
   - **d.** Justifier que : $3|abc$.
2. **Etude de la divisibilité de abc par 5 dans un cas particulier.**
   Dans cette question, n est un entier relatif.
   - **a.** Vérifier que : $(n^2 - 1)^2 + (2n)^2 = (n^2 + 1)^2$.
   - **b.** On pose : $a = n^2 - 1$, $b = 2n$ et $c = n^2 + 1$; a-t-on : $5|abc$?

Corrigé

Exercice 1 **Démontrer que** : $\forall n \in \mathbb{N}, 7|23^n - 9^n + 133.$

Soit $n \in \mathbb{N}$.

Raisonnons modulo 7 :

$23 \equiv 23 - 3 \times 7 \equiv 23 - 21 \equiv 2\ [7]$

$9 \equiv 9 - 1 \times 7 \equiv 2\ [7]$

$133 \equiv 133 - 20 \times 7 \equiv 133 - 140 \equiv -7 \equiv -7 + 1 \times 7 \equiv 0\ [7]$

On en déduit que :

$23^n - 9^n + 133 \equiv 2^n - 2^n + 0 \equiv 0\ [11]$

On a : $23^n - 9^n + 133 \equiv 0\ [7]$, donc : $7|23^n - 9^n + 133$.

Conclusion : $\forall \boldsymbol{n} \in \mathbb{N}, \mathbf{17}|\mathbf{23^n - 9^n + 133}$.

Autre rédaction dite « accélérée »

Soit $n \in \mathbb{N}$, on a :

$23^n - 9^n + 133 \equiv (23 - 3 \times 7)^n - (9 - 7)^n + 133 - 19 \times 7 \equiv 2^n - 2^n + 0 \equiv 0\ [7]$

On a : $23^n - 9^n + 133 \equiv 0\ [7]$, autrement dit : $7|23^n - 9^n + 133$.

Conclusion : $\forall \boldsymbol{n} \in \mathbb{N}, \mathbf{17}|\mathbf{23^n - 9^n + 133}$.

Exercice 2 **Déterminer le reste de la division euclidienne de $\mathbf{8^{173}}$ par 5**

$8^1 = 8 \equiv 3\ [5]$

$8^2 \equiv 3^2 \equiv 9 \equiv 4\ [5]$

$8^3 = 8 \times 8^2 \equiv 3 \times 4 \equiv 12 \equiv 2\ [5]$

$8^4 = (8^2)^2 \equiv 4^2 \equiv 16 \equiv 1\ [5]$

Posons la division euclidienne de 173 par 4 :

1	7	3	4
−1	6		4 3
	1	3	
	−1	2	
		1	

Il en résulte que : $\mathbf{173 = 43 \times 4 + 1}$. On a :

$8^{173} = 8^{43 \times 4 + 1} = 8^{43 \times 4} \times 8^1 = (8^4)^{43} \times 8 \equiv 1^{43} \times 8 \equiv 1 \times 8 \equiv 8 \equiv 3\ [5]$

$8^{173} \equiv 3\ [5]$ avec $0 \leqslant 3 < 5$

Le reste de la division euclidienne de $\mathbf{8^{173}}$ par 5 est : 3.

Exercice 3

1. **Montrer que 6 n'a pas d'inverse modulo 8.**

   Montrons qu'il n'existe pas $n \in \mathbb{Z}$ tel que : $6n \equiv 1\ [8]$.

   Tableau de congruence modulo 8 :

$n \equiv$	0	1	2	3	4	5	6	7
$6n \equiv$	0 $\not\equiv 1$	6 $\not\equiv 1$	12 $\equiv 4$ $\not\equiv 1$	18 $\equiv 2$ $\not\equiv 1$	24 $\equiv 0$ $\not\equiv 1$	30 $\equiv 6$ $\not\equiv 1$	36 $\equiv 4$ $\not\equiv 1$	42 $\equiv 2$ $\not\equiv 1$

   Par disjonction de cas : $\forall n \in \mathbb{Z}, 6n \not\equiv 1\ [8]$ donc **6 n'a pas d'inverse modulo 8**.

2. **Soient $a \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ tels qu'il existe $d \in \mathbb{Z} \setminus \{-1; 1\}$ tel que : $d|a$ et $d|m$. Montrer que a n'a pas d'inverse modulo m.**

Supposons qu'il existe $b \in \mathbb{Z}$ vérifiant : $ab \equiv 1\ [m]$, c'est-à-dire tel qu'il existe $k \in \mathbb{Z}$ vérifiant : $ab = 1 + km$, qui s'écrit aussi : $ab - km = 1$.
On a $d|a$ et $d|m$ donc d divise toute combinaison linéaire de a et m, en particulier : $d|ab - km$, c'est-à-dire : $d|1$. Or les seuls diviseurs de 1 sont -1 et 1, donc $d = -1$ ou $d = 1$ ce qui est en contradiction avec l'hypothèse $d \in \mathbb{Z} \setminus \{-1; 1\}$, il faut donc rejeter la supposition d'existence de $b \in \mathbb{Z}$ vérifiant $ab \equiv 1\ [m]$ autrement dit a n'est pas inversible modulo m.

Conclusion : **a n'a pas d'inverse modulo m.**

Exercice 4 **Quel est le chiffre des unités de 3^{2025} ?**

1. **Raisonnons modulo 10.**
$3^1 \equiv 3\ [10]$
$3^2 = 9 \equiv 9 - 10 \equiv -1\ [10]$
On a :
$3^{2025} = 3^{2\times1012+1} = 3^{2\times1012} \times 3^1 = (3^2)^{1012} \times 3 \equiv (-1)^{1012} \times 3 \equiv 1 \times 3 = 3\ [10]$
$3^{2025} \equiv 3\ [10]$ avec $0 \leqslant 3 < 10$ donc le reste modulo 10 de 3^{2025} est 3 autrement dit **le chiffre des unités de 3^{2025} est 3.**

2. **Montrer que $3^{10} \equiv 49\ [100]$ puis déterminer les deux derniers chiffres de 3^{2025}.**
$3^1 \equiv 3\ [100]$
$3^2 \equiv 3^2 \equiv 9\ [100]$
$3^5 = 3 \times 3^2 \times 3^2 \equiv 3 \times 9 \times 9 \equiv 3 \times 81 \equiv 243 \equiv 43\ [100]$
$3^{10} = (3^5)^2 \equiv 43^2 \equiv 1849 \equiv 1849 - 18 \times 100 \equiv 1849 - 1800 \equiv 49\ [100]$
On a donc bien : $3^{10} \equiv 49\ [100]$.
On a : $3^{20} = (3^{10})^2 \equiv 49^2 \equiv 2401 \equiv 2401 - 24 \times 100 \equiv 1\ [100]$
On a : $3^{2025} = 3^{20\times101+5} = 3^{20\times101} \times 3^5 = (3^{20})^{101} \times 3^5 \equiv 1 \times 43 \equiv 43\ [100]$
$3^{2025} \equiv 43\ [100]$ avec $0 \leqslant 43 < 100$ donc le reste modulo 100 de 3^{2025} est 43 autrement dit : **les deux derniers chiffres de 3^{2025} sont 4 puis 3.**

Exercice 5

Soient a, b et c trois entiers relatifs tels que : $a^2 + b^2 = c^2$.

1. **Dans cette question on se propose de démontrer que : $3|abc$.**
   a. **Montrer que, pour tout $x \in \mathbb{Z}$, $x^2 \equiv 0$ *ou* $1\ [3]$.**

Tableau de congruence modulo 3

$x \equiv$	0	1	2
$x^2 \equiv$	0^2 $\equiv 0$	1^2 $\equiv 1$	2^2 $\equiv 4$ $\equiv 1$

Par disjonction de cas, la dernière ligne montre que : $\forall x \in \mathbb{Z}$, $x^2 \equiv 0$ *ou* $1\ [3]$.

   b. **Montrer que : si $a \equiv 0\ [3]$ ou $b \equiv 0\ [3]$, alors : $3|abc$.**
Supposons que $a \equiv 0\ [3]$ ou $b \equiv 0\ [3]$
− si $a \equiv 0\ [3]$, alors $3|a$ donc $3|abc$

$-$ si $b \equiv 0\ [3]$, alors $3|b$ donc $3|abc$.
Dans tous les cas on a bien : $\mathbf{3|abc}$.

c. On suppose que : $a \not\equiv 0\ [3]$ et $b \not\equiv 0\ [3]$, justifier que $a^2 + b^2 \equiv 2\ [3]$ puis établir une contradiction.

On suppose $a \not\equiv 0\ [3]$ et $b \not\equiv 0\ [3]$:
$a \not\equiv 0\ [3]$ revient à dire : $a \equiv 1\ ou\ 2\ [3]$, donc d'après **1.** cela revient à dire $a^2 \equiv 1\ [3]$,
$b \not\equiv 0\ [3]$ revient à dire : $b \equiv 1\ ou\ 2\ [3]$, donc d'après **1.** cela revient à dire $b^2 \equiv 1\ [3]$ Il vient alors : $a^2 + b^2 \equiv 1 + 1 \equiv 2\ [3]$.
Or, $a^2 + b^2 = c^2$, donc : $c^2 \equiv 2\ [3]$ ce qui est en contradiction avec **1.** : un carré est congru à 0 ou 1 modulo 3, jamais à 2.
Supposer $a \not\equiv 0\ [3]$ et $b \not\equiv 0\ [3]$ amène donc **une contradiction**.

d. Justifier que : $\mathbf{3|abc}$.

Remarquons que, d'après la question **c.**, il est impossible d'avoir simultanément $a \not\equiv 0\ [3]$ et $b \not\equiv 0\ [3]$ donc : $a \equiv 0\ [3]$ ou $b \equiv 0\ [3]$, puis d'après **b.** on en déduit que : $\mathbf{3|abc}$.

2. Etude de la divisibilité par 5 de abc dans un cas particulier.

Dans cette question, n est un entiers relatifs.

a. Vérifier que : $(n^2 - 1)^2 + (2n)^2 = (n^2 + 1)^2$.

On a :
$(n^2 - 1)^2 + (2n)^2 = (n^2)^2 - 2(n^2)(1) + (1)^2 + 4n^2 = n^4 - 2n^2 + 4n^2 + 1$
$= n^4 + 2n^2 + 1 = (n^2)^2 + 2(n^2)(1) + (1)^2 = (n^2 + 1)^2$

On a donc bien : $(n^2 - 1)^2 + (2n)^2 = (n^2 + 1)^2$.

b. On pose : $a = n^2 - 1$, $b = 2n$ et $c = n^2 + 1$; a-t-on : $5|abc$?

Il s'agit de savoir si : $5|(n^2 - 1)2n(n^2 + 1)$, c'est-à-dire si : $5|2n(n^4 - 1)$.

Tableau de congruence modulo 5

$n \equiv$	0	1	2	3	4
$2n \equiv$	0	2 $\equiv 1$	4 $\equiv -1$	6 $\equiv 1$	8 $\equiv 3$
$n^4 - 1 \equiv$	$0^4 - 1$ $\equiv -1$	$1^4 - 1$ $\equiv 0$	$2^4 - 1$ $\equiv 15$ $\equiv 0$	$3^4 - 1$ $\equiv 80$ $\equiv 0$	$4^5 - 1$ $\equiv (-1)^4 - 1$ $\equiv 1 - 1$ $\equiv 0$
$2n(n^4 - 1) \equiv$	$0 \times (-1)$ $\equiv 0$	1×0 $\equiv 0$	$(-1) \times 0$ $\equiv 0$	1×0 $\equiv 0$	3×0 $\equiv 0$

Par disjonction de cas la dernière ligne du tableau de congruence montre que :
$\forall n \in \mathbb{Z}, 5|2n(n^4 - 1)$, autrement dit que : $\mathbf{5|abc}$.