Devoir sur table n°5 – maths expertes

Jeudi 8 janvier 2026 – 1h

L'utilisation d'une calculatrice est autorisée.
La qualité de la rédaction et la précision des raisonnements entreront pour une part importante dans l'appréciation de la copie.

Exercice 1 : Étude d'une équation diophantienne quadratique **(5 points)**

On considère l'équation (F) : $11x^2 - 7y^2 = 5$, où x et y sont des entiers relatifs.

1. Démontrer que si le couple $(x; y)$ est solution de (F), alors $x^2 \equiv 2y^2\,[5]$.
2. Soient x et y des entiers relatifs. Compléter (sans justification) les deux tableaux suivants :

Modulo 5, x est congru à	0	1	2	3	4
Modulo 5, x^2 est congru à	.....	.....	.....	.....	.....

Modulo 5, y est congru à	0	1	2	3	4
Modulo 5, $2y^2$ est congru à	.....	.....	.....	.....	.....

Quelles sont les valeurs possibles du reste de la division euclidienne de x^2 et de $2y^2$ par 5 ?

3. En déduire que si le couple $(x; y)$ est solution de (F), alors x et y sont des multiples de 5.
4. Démontrer que si x et y sont des multiples de 5, alors le couple $(x; y)$ n'est pas solution de (F). Que peut-on en déduire pour l'équation (F) ?

Solution:

1. Si $(x\,;\,y)$ est solution de (F), alors $11x^2 - 7y^2 = 5$.

   En travaillant modulo 5 :

$$\begin{aligned} 11x^2 - 7y^2 &\equiv 5\,[5] \\ &\equiv 0\,[5] \end{aligned}$$

   Or $11 \equiv 1\,[5]$ et $7 \equiv 2\,[5]$, donc :

$$x^2 - 2y^2 \equiv 0\,[5]$$

   i.e.

$$x^2 \equiv 2y^2\,[5]$$

2. Complétons les tableaux :

Modulo 5, x est congru à	0	1	2	3	4
Modulo 5, x^2 est congru à	0	1	4	4	1

Modulo 5, y est congru à	0	1	2	3	4
Modulo 5, $2y^2$ est congru à	0	2	3	3	2

Les valeurs possibles du reste de la division euclidienne de x^2 par 5 sont : 0, 1, 4.

Les valeurs possibles du reste de la division euclidienne de $2y^2$ par 5 sont : 0, 2, 3.

3. D'après la question 1, si $(x\,;\,y)$ est solution de (F), alors $x^2 \equiv 2y^2\,[5]$.

D'après les tableaux de la question 2, on constate que x^2 et $2y^2$ n'ont qu'une seule valeur commune modulo 5, qui est 0.

Donc nécessairement : $x^2 \equiv 0\,[5]$ et $2y^2 \equiv 0\,[5]$.

Or $x^2 \equiv 0\,[5]$ implique que 5 divise x^2, et comme 5 est premier, cela implique que 5 divise x, donc x est un multiple de 5.

De même, $2y^2 \equiv 0\,[5]$ implique que 5 divise $2y^2$. Or 5 ne divise pas 2, donc 5 divise y^2, et comme 5 est premier, cela implique $5|y$, donc y est un multiple de 5.

Conclusion : Si $(x\,;\,y)$ est solution de (F), alors x et y sont des multiples de 5.

4. Supposons que x et y sont des multiples de 5. On peut alors écrire $x = 5x'$ et $y = 5y'$ où x' et y' sont des entiers relatifs.

Substituons dans l'équation (F) :

$$\begin{aligned} 11x^2 - 7y^2 &= 11(5x')^2 - 7(5y')^2 \\ &= 11 \times 25x'^2 - 7 \times 25y'^2 \\ &= 275x'^2 - 175y'^2 \\ &= 25(11x'^2 - 7y'^2) \end{aligned}$$

Si $(x\,;\,y)$ était solution de (F), on aurait : $25(11x'^2 - 7y'^2) = 5$

Ce qui donnerait : $11x'^2 - 7y'^2 = \dfrac{5}{25} = \dfrac{1}{5}$

Or $11x'^2 - 7y'^2$ est un entier (car x' et y' sont des entiers), donc il est impossible qu'il soit égal à $\frac{1}{5}$.

Conclusion : Si x et y sont des multiples de 5, alors $(x\,;\,y)$ n'est pas solution de (F).

Synthèse : D'après la question 3, toute solution de (F) est telle que x et y sont multiples de 5. Or d'après la question 4, si x et y sont multiples de 5, alors $(x\,;\,y)$ n'est pas solution de (F).

Par conséquent, l'équation (F) : $11x^2 - 7y^2 = 5$ n'a aucune solution dans $\mathbb{Z}^2$.

Exercice 2 : Date d'anniversaire et tour de magie **(3 points)**

Dans cet exercice, on appelle numéro du jour de naissance j le rang de ce jour dans le mois et numéro du mois de naissance m, le rang du mois dans l'année.

Par exemple, pour une personne née le 14 mai, alors $j = 14$ et $m = 5$.

Lors d'une représentation, un magicien demande aux spectateurs d'effectuer le programme de calcul suivant :

« Prenez le numéro de votre jour de naissance et multipliez-le par 12. Prenez le numéro de votre mois de naissance et multipliez-le par 37. Ajoutez les deux nombres obtenus. Je pourrai alors vous donner la date de votre anniversaire. »

Un spectateur annonce 308 et en quelques secondes, le magicien déclare : « Votre anniversaire tombe le 1er août ! »

1. Vérifier que pour une personne née le 1er août, le programme de calcul donne effectivement le nombre 308.
2. (a) Pour un spectateur donné, on note z le résultat obtenu en appliquant le programme de calcul.

   Exprimer z en fonction de j et de m et démontrer que $z \equiv m\ [12]$.

   (b) M. Dhénin affirme qu'il vous rendra les contrôles à la date correspondant au nombre 193. Retrouver la date à laquelle vous recevrez vos copies.

Solution:

1. Pour une personne née le 1er août, on a $j = 1$ et $m = 8$.

   Appliquons le programme de calcul :

   - Étape 1 : $j \times 12 = 1 \times 12 = 12$
   - Étape 2 : $m \times 37 = 8 \times 37 = 296$
   - Étape 3 : $12 + 296 = 308$

   Le programme de calcul donne bien le nombre 308 pour une personne née le 1er août.

2. (a) D'après le programme de calcul, le résultat z est :

$$z = 12j + 37m$$

   On a :

$$z = 12j + 37m$$

   Calculons z modulo 12 :

$$\begin{aligned} z &\equiv 12j + 37m\ [12] \\ \text{i.e. } z &\equiv 0 + 37m\ [12] \quad (\text{car } 12j \equiv 0\ [12]\ ) \end{aligned}$$

   Or $37 = 3 \times 12 + 1$, donc $37 \equiv 1\ [12]$.

Ainsi :

$$z \equiv 1 \times m \,[12]$$

i.e.

$$z \equiv m \,[12]$$

(b) Pour retrouver la date à laquelle M. Dhénin rendra les contrôles avec $z = 193$:

Étape 1 : Trouver le mois m

D'après la question précédente, $z \equiv m \,[12]$.

Calculons 193 mod 12 : $193 = 16 \times 12 + 1$

Donc $193 \equiv 1 \,[12]$, ce qui signifie $m = 1$ (janvier).

Étape 2 : Trouver le jour j

On sait que $z = 12j + 37m$, donc :

$$\begin{aligned} 193 &= 12j + 37 \times 1 \\ \text{i.e. } 193 &= 12j + 37 \\ \text{i.e. } 12j &= 193 - 37 \\ \text{i.e. } 12j &= 156 \\ \text{i.e. } j &= 13 \end{aligned}$$

Vérification : $12 \times 13 + 37 \times 1 = 156 + 37 = 193$

Conclusion : M. Dhénin rendra les contrôles le 13 janvier.

Exercice 3 : Clef RIB **(3 points)**

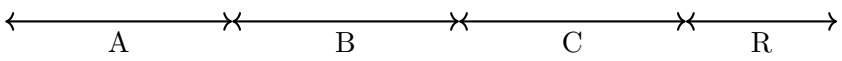
On donne les informations suivantes :

- Le reste de la division euclidienne de 23 104 par 97 est 18.
- Le reste de la division euclidienne de 15 231 par 97 est 2.
- Le reste de la division euclidienne de 64 621 113 par 97 est 70.

$10^1 \equiv 10\,[97]$	$10^2 \equiv 3\,[97]$	$10^3 \equiv 30\,[97]$
$10^4 \equiv 9\,[97]$	$10^5 \equiv 90\,[97]$	$10^6 \equiv 27\,[97]$
$10^7 \equiv 76\,[97]$	$10^8 \equiv 81\,[97]$	$10^9 \equiv 34\,[97]$
$10^{10} \equiv 49\,[97]$	$10^{11} \equiv 5\,[97]$	$10^{12} \equiv 50\,[97]$
$10^{13} \equiv 15\,[97]$	$10^{14} \equiv 53\,[97]$	$10^{15} \equiv 45\,[97]$
$10^{16} \equiv 62\,[97]$	$10^{17} \equiv 38\,[97]$	$10^{18} \equiv 89\,[97]$

Un numéro de compte bancaire **N** est un nombre de 23 chiffres.

Code Banque	**Code Agence**	**n° de compte**	**Clé RIB**
23104	15231	00006462113	



Le nombre **A** constitué des 5 premiers chiffres correspond au code de la banque.

Le nombre **B** constitué des 5 chiffres suivants correspond au code de l'agence de cette banque.

Le nombre **C** constitué des 11 chiffres suivant correspond au numéro de compte du client pour la banque considérée.

Le nombre **R** constitué des deux derniers chiffres est la « **Clé RIB** ».

La « **Clé RIB** » est un nombre de 2 chiffres compris entre 01 et 97 (on écrit le zéro pour obtenir un numéro de compte N de 23 chiffres.

On détermine **R** en imposant au nombre N d'être divisible par 97.

Exemple :

1. Déterminer les entiers naturels n, p et k tels que :

$$N = A \times 10^n + B \times 10^p + C \times 10^k + R$$

2. Déterminer la « Clé RIB » pour l'exemple considéré.

Solution:

1. En utilisant la définition de la numération dans le système décimal, on obtient :

$$N = A \times 10^n + B \times 10^p + C \times 10^k + R$$

donc $n = 18$ et $p = 13$ et $k = 2$

2. Pour l'exemple

$$\begin{array}{ccc} A \equiv 18\,[97] & B \equiv 2\,[97] & C \equiv 70\,[97] \\ 10^{18} \equiv 89\,[97] & 10^{13} \equiv 15\,[97] & 10^{2} \equiv 3\,[97] \end{array}$$

et $R \equiv R\,[97]$.

On suppose que 97 divise N, c'est-à-dire $N \equiv 0\,[97]$ donc

$$\begin{aligned} & 18 \times 89 + 2 \times 15 + 70 \times 3 + R \equiv 0\,[97] \\ \text{i.e. } & 1602 + 30 + 210 + R \equiv 0\,[97] \\ \text{i.e. } & 1842 + R \equiv 0\,[97] \end{aligned}$$

Or, $1842 = 97 \times 18 + 96$. Donc

$$96 + R \equiv 0\,[97]$$

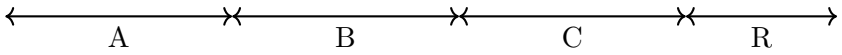
donc $R \equiv -96\,[97]$ ou encore

$$R \equiv 1\,[97]$$

R contient deux chiffres, donc $R = 01$.

On complète le tableau

Code Banque	**Code Agence**	**n° de compte**	**Clé RIB**
23104	15231	00006462113	**01**



Remarques :

- Si R $\equiv 0\,[97]$ alors $R = 97$ et non 00.
- On utilise le nombre 97 car les restes des divisions euclidiennes de 10^k par 97, pour k compris entre0 et 22 sont distincts deux à deux et tous les chiffres de N interviennent pour la congruence modulo 97.

  Si on se trompe pour un chiffre (et un seul) des 23 chiffres de N, le nouveau nombre obtenu N' n'est pas divisible par 97 (l'ordinateur vérifie immédiatement ce résultat).

  S'il y a plusieurs erreurs, alors le nouveau nombre obtenu peut-être lui aussi divisible par 97.

Exercice 4 : Nombres de Mersenne[1] **(9 points)**

Soit $n \in \mathbb{N}$.
Les nombres de la forme $2^n - 1$ sont appelés **nombres de Mersenne**. On les note M_n.

1. Montrer que M_5 est premier et que M_{11} n'est pas premier.
2. Soient p et q sont deux entiers naturels non nuls. On considère :

$$S = 1 + 2^p + 2^{2p} + 2^{3p} + ... + 2^{p(q-1)}$$

   (a) Exprimer S en fonction de 2^{pq}

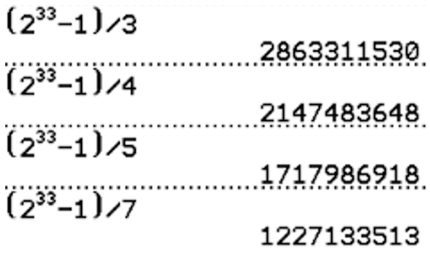
   (b) Démontrer que $2^{pq} \equiv 1\,[2^p - 1]$

   (c) En déduire que M_{pq} n'est pas un nombre premier.

Application : Étude de $M_{33} = 2^{33} - 1$

On considère le nombre de Mersenne $M_{33} = 2^{33} - 1$

Un élève utilise sa calculatrice et obtient les résultats ci-contre :



Il affirme donc que les entiers 3, 4, 5 et 7 divisent M_{33}

3. Justifier qu'en réalité 4 ne divise pas M_{33}
4. En remarquant que $2 \equiv -1\,[3]$, montrer que 3 ne divise pas M_{33}.
5. Montrer que 5 ne divise pas M_{33}.
6. (a) Exprimer la somme $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + ... + (2^3)^{10}$ en fonction de M_{33}.

   (b) En déduire que 7 divise M_{33}.

Bonus

Soit $n \in \mathbb{N}$. Démontrer que si M_n est un nombre premier, alors n est un nombre premier.
La réciproque est-elle vraie?

Solution:

1. $M_5 = 31$ qui est un nombre premier.
   $M_{11} = 2^{11} - 1 = 2048 - 1 = 2047$. On regarde si 2047 est divisible par un nombre premier p tel que $p^2 \leqslant 2047$

   On trouve que 2047 est divisible par 23. En effet, $2047 = 23 \times 89$.

   Donc $2^{11} - 1$ n'est pas un nombre premier.

2. (a) $S = 1 + 2^p + 2^{2p} + 2^{3p} + ... + 2^{p(q-1)}$

   S est la somme des q premiers termes de la suite géométrique de premier terme 1 et de raison 2^p.

[1] Marin Mersenne (1588-1648) est un religieux français, physicien, mathématicien, musicologue et philosophe. On lui doit les premières lois de l'acoustique (lois de Mersenne) et, concomitamment avec Galilée, les premières formules de la loi de la chute des corps.

Donc, comme $p \neq 0$, i.e. $2^p \neq 1$,

$$S = \frac{1-(2^p)^q}{1-2^p} = \frac{1-2^{pq}}{1-2^p}$$

(b) D'après la question précédente : $S = \dfrac{1-(2^p)^q}{1-2^p}$

En multipliant les deux membres par $(1-2^p) = -(2^p-1)$:

$$S(1-2^p) = 1-(2^p)^q$$

$$S(2^p-1) = 2^{pq}-1$$

donc $(2^p-1)S = (2^p)^q - 1$

Par suite,

$$\begin{aligned}(2^p)^q - 1 &\equiv 0\,[2^p-1]\\ 2^{pq} &\equiv 1\,[2^p-1]\end{aligned}$$

(c) D'après la question précédente :

$$(2^p)^q - 1 \equiv 0\,[2^p-1]$$

Donc $(2^p)^q - 1 = 2^{pq}-1$ est divisible par 2^p-1.

3. $2^{33}-1$ est impair (car 2^{33} est pair), donc $2^{33}-1$ n'est pas divisible par 4.
4. On a $2 \equiv -1\,[3]$, donc:

$$\begin{aligned}2^{33} &\equiv (-1)^{33}\,[3]\\ 2^{33} &\equiv -1\,[3]\\ 2^{33}-1 &\equiv -1-1\,[3]\\ 2^{33}-1 &\equiv -2\,[3]\\ 2^{33}-1 &\equiv 1\,[3]\end{aligned}$$

Donc $2^{33}-1$ n'est pas divisible par 3.

5. Calculons les premières puissances de 2 modulo 5 :

$$\begin{aligned}2^1 &\equiv 2\,[5]\\ 2^2 &\equiv 4\,[5]\\ 2^3 &\equiv 8 \equiv 3\,[5]\\ 2^4 &\equiv 2\times 3 \equiv 6 \equiv 1\,[5]\end{aligned}$$

Donc $2^4 \equiv 1\,[5]$

Or $33 = 4 \times 8 + 1$, donc:

$$\begin{aligned} 2^{33} &= 2^{4\times 8+1} = (2^4)^8 \times 2 \\ 2^{33} &\equiv 1^8 \times 2\,[5] \\ 2^{33} &\equiv 2\,[5] \\ 2^{33} - 1 &\equiv 1\,[5] \end{aligned}$$

Donc $2^{33} - 1$ n'est pas divisible par 5.

6. (a) $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + ... + (2^3)^{10}$

S est la somme de 11 termes de la suite géométrique de premier terme 1 et de raison $2^3 = 8$.

$$S = \frac{1 - (2^3)^{11}}{1 - 2^3} = \frac{1 - 2^{33}}{1 - 8} = \frac{1 - 2^{33}}{-7} = \frac{2^{33} - 1}{7}$$

Donc

$$S = \frac{M_{33}}{7}$$

(b) D'après la question précédente, $M_{33} = 7S$ où S est un entier (en tant que somme d'entiers).

Donc $M_{33} = 2^{33} - 1$ est divisible par 7.

Bonus : On suppose que $2^n - 1$ ($n \in \mathbb{N}$) est un nombre premier et que n n'est pas un nombre premier.

Si n n'est pas un nombre premier, alors il existe $p \neq 1$ et $p \neq n$ et $q \neq 1$ et $q \neq n$ tels que $n = pq$

D'après la question 2.c), $2^p - 1$ est un diviseur de $2^{pq} - 1$, c'est-à-dire :

$2^p - 1$ est un diviseur de $2^n - 1$

Or, $2^n - 1$ est un nombre premier.

Donc $2^p - 1 = 1$ ou $2^p - 1 = 2^n - 1$

c'est-à-dire $2^p = 2$ ou $2^p = 2^n$

Donc $p = 1$ ou $p = n$. D'où contradiction.

Conséquence : si $2^n - 1$ ($n \in \mathbb{N}$) est un nombre premier alors n est un nombre premier.

La réciproque est-elle vraie ?

11 est un nombre premier et $2^{11} - 1 = 2047 = 23 \times 89$ n'est pas un nombre premier (d'après la question 1).

Donc la réciproque de la propriété est fausse.