Thème : Les nombres premiers

Corrigé de l'activité 1. Autour des nombres premiers (6 exercices)

Exercice 1 *Nombres croisés*

	A	B	C	D	E
1	**9**	**6**	**7**	**2**	**1**
2	**4**	**9**	**4**	9	■
3	**9**	**7**	**3**	■	**3**
4	**4**	**4**	**4**	**2**	**3**
5	**9**	■	**7**	**7**	**8**

Remarque : l'ordre n'est qu'indicatif. Certaines étapes peuvent être permutées.

1)	Emplacement 3b	Le reste de la division euclidienne de 2001 par 9 est égal à **3**.
2)	Emplacement Ea	**1** est le seul entier positif n'admettant qu'un seul diviseur positif (tous les autres entiers positifs ont au minimum deux diviseurs positifs : 1 et eux-mêmes).
3)	Emplacement Eb	Le produit de ses chiffres est $72 = 2^3 \times 3^2$ et l'emplacement comporte trois cellules. Donc les seuls produits possibles sont : $2 \times 6 \times 6$; $2 \times 4 \times 9$; $4 \times 6 \times 3$; $8 \times 3 \times 3$. La condition "seul son dernier chiffre est pair" impose donc que le chiffre des unités soit 8 et donc que le nombre soit égal à **338**.
4)	Emplacement 5b	Le produit de ses chiffres est $392 = 2^3 \times 7^2$ et l'emplacement comporte trois cellules. Donc le seul produit possible est $392 = 8 \times 7 \times 7$. Le 8 ayant déjà été placé, on déduit que le nombre est égal à **778**.
5)	Emplacement Db	Les cubes parfaits à deux chiffres sont $3^3 = 27$ et $4^3 = 64$. Un 7 ayant déjà été placé dans la cellule D5, **27** est la seule possibilité.
6)	Emplacement 4	Le nombre est formé d'une permutation des chiffres 2, 3, 4, 4, 4. 2 et 3 étant déjà placés le nombre est égal à **44423**.
7)	Emplacement C	Le nombre est un palindrome. Le nombre finissant par 4 et 7 déjà placés, **commence donc par 74**.
8)	Emplacement 2	Les deux premiers chiffres sont respectivement les mêmes que les deux derniers chiffres. Un 4 ayant déjà été placé dans la cellule C2, il y a donc aussi un **4 dans la cellule A2.**
9)	Emplacement A	La somme de ses cinq chiffres est 35. Or, les chiffres 4 et 4 ont déjà été placés. La somme des trois chiffres manquants est égale à $35 - 2 \times 4 = 27$. Donc la seule possibilité est que les trois chiffres manquants soient **tous des 9**.
10)	Emplacement 3a	Il s'agit d'un multiple de 139 de trois chiffres. Un 9 ayant déjà été placé dans la cellule A3, la seule possibilité est $139 \times 7 =$ **973**.
11)	Emplacement 1	Le produit des cinq chiffres est $756 = 2^2 \times 3^3 \times 7$. Les chiffres $9, 7, 1$ ayant déjà été placés, il reste à placer deux chiffres dont le produit est $2^2 \times 3$. Ces deux chiffres ne peuvent donc qu'être 4 *et* 3 ou bien 2 *et* 6. Le nombre ne peut donc être que 9**473**1 ou 9**374**1 ou 9**276**1 ou 9**672**1. Or ce doit être un carré parfait. Seul 96721 convient.
12)	Emplacement D	C'est un nombre premier à deux chiffres commençant par un 2. Seuls 23 ou 29 peuvent convenir.
13)	Emplacement 2	Les cellules A2 et C2 contiennent déjà un 4. La cellule D2, d'après l'étape précédente, contient soit un 3, soit un 9. Donc seuls **4343** ou **4949** peuvent convenir.
14)	Emplacement B	D'après l'étape précédente, les deux seuls nombres possibles sont 6374 et 6974. Seul **6974** est divisible par 11. Donc la cellule B2 contient un **9** et le nombre de l'emplacement Da est **29**.

Exercice 2 ***Le crible d'Eratosthène***

1)

		2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~
~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29
~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~
~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59
~~60~~	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~
~~70~~	71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79
~~80~~	~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89
~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~

2) Les nombres entourés sont donc : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97.

3) Chacun de ces nombres possèdent exactement deux diviseurs positifs : 1 et lui-même. Le crible d'Eratosthène permet donc de générer les nombres premiers. La liste précédente est donc la liste des nombres premiers inférieurs à 100.

Exercice 3 ***Tester la primalité (exercice identique à l'exercice 1 de l'activité 2 « Algorithmes sur les nombres premiers »)***

1) 107 n'est pas divisible par 2, 3, 5, …, 103 : c'est donc un **nombre premier**.
- 227 n'est pas divisible par 2, 3, 5, …, 223 : c'est donc **un nombre premier**.
- 375 est divisible par 5, ce n'est donc pas un nombre premier.
- 377 est divisible par 13, ce n'est donc pas un nombre premier.
- 379 n'est pas divisible par 2, 3, 5, …, 373 : c'est donc un **nombre premier**.
- 571 n'est pas divisible par 2, 3, 5, …, 569 : c'est donc un **nombre premier**.

2) Pour 107, il n'est pas utile de tester tous les nombres premiers de 2 jusqu'à 103. En effet, il est certes nécessaire de tester la division par 2, 3, …

Mais par exemple, le test de la division par 73 est inutile : E(107/73) = 1.

Les élèves auront tendance à énoncer le fait qu'il faut "s'arrêter" à 107/2.

Il faudra relancer le débat en demandant si l'on ne peut pas faire mieux…

Et ce jusqu'à obtenir que si n est composé alors son plus petit diviseur noté p est inférieur ou égal à $\sqrt{n}$.

Preuve : On suppose que n a au moins un autre diviseur que 1 et lui-même. On appelle p *le plus petit* de ces diviseurs.

Donc $1 < p < n$ où p est un diviseur de n. Alors :

- il existe un second diviseur q tel que $pq = n$
- Ce second diviseur est tel que $p \leq q$. Donc $1 < p \leq q < n$

$$p < p^2 \leq pq$$

$$p^2 \leq n$$

$$p \leq \sqrt{n}$$

$\sqrt{107} \approx 10{,}3$. Donc il faut et il suffit de tester la division par tous les nombres premiers inférieurs ou égaux à 7.

3) On fait fonctionner l'algorithme sur le papier :

Pour $N = 19$

	N	I
	19	
1^er^ tour de boucle Tant que		2
2^e^ tour de boucle Tant que		3
3^e^ tour de boucle Tant que		4
4^e^ tour de boucle Tant que		5
Sortie de boucle car la condition I ne divise pas N est vraie et la condition $I \leq E(\sqrt{N})$ est fausse		

L'affichage est PREMIER.

Pour $N = 21$,

	N	I
	21	
1er tour de boucle Tant que		2
2e tour de boucle Tant que		3
Sortie de boucle car la condition I ne divise pas N est fausse et la condition $I \leq E(\sqrt{N})$ est vraie		

L'affichage est NON PREMIER.

Pour $N = 53$,

	N	I
	53	
1er tour de boucle Tant que		2
2e tour de boucle Tant que		3
3e tour de boucle Tant que		4
4e tour de boucle Tant que		5
5e tour de boucle Tant que		6
6e tour de boucle Tant que		7
7e tour de boucle Tant que		8
Sortie de boucle car la condition I ne divise pas N est vraie et la condition $I \leq E(\sqrt{N})$ est fausse		

L'affichage est PREMIER.

4) a) Programme TESTA

Programme TESTA sur TI

```
Prompt N
If N ≤ 3
Then
If N=2 ou N=3
Then
Disp "N PREMIER"
Else
Disp "N NON PREMIER"
End
Else
2→I
While (partEnt(N/I)≠N/I) et
(I≤ partEnt(√(N)))
```

Programme TESTA sur Casio

```
"N="?→N
If N≤ 3
Then
If N=2 Or N=3
Then
"N PREMIER"◢
Else
"N NON PREMIER"◢
IfEnd
Else
2→I
While (Intg(N÷I)≠N÷I) And
(I≤ Intg(√(N)))
```

b) En utilisant ce programme, on affiche :

- 19 et 53 sont premiers et 21 n'est pas premier.
- 2011 et 2017 sont premiers et 2013, 2015 et 2019 ne pas premiers.

c)	TI83	TI83 CE Premium	Casio Graph 35+ USB
TESTA : Durée du test de la primalité de 7 237 031	75 s	58 s	31 s

5) a) Modification de l'algorithme pour tester la division par 2 et pour ensuite ne pas tester la division par les autres nombres pairs :

Déclaration des variables : *N* et *I* sont des entiers

Début de l'algorithme

Saisir *N*

Si $N \leq 3$

Alors

Si $N = 2\ ou\ N = 3$

Alors

Afficher "*N* PREMIER"

Sinon

Afficher "*N* NON PREMIER"

Fin Si

Sinon

Si 2 divise N

Alors

Afficher "N NON PREMIER"

Sinon

b) Programmation sur calculatrice :

Programme TESTB sur TI

```
Prompt N
If N ≤ 3
Then
If N=2 ou N=3
Then
Disp "N PREMIER"
Else
Disp "N NON PREMIER"
End
Else
If partEnt(N/2)=N/2
Then
Disp "N NON PREMIER"
Else
```

Programme TESTB sur Casio

```
"N="?→N
If N≤ 3
Then
If N=2 Or N=3
Then
"N PREMIER"◢
Else
"N NON PREMIER"◢
IfEnd
Else
If Intg(N÷2)=N÷2
Then
"N NON PREMIER"◢
Else
```

c) L'amélioration du temps d'exécution du programme est très significative. La durée d'exécution du programme est divisée par 2. C'est une très nette amélioration pour de grandes valeurs de *N*.

	TI83	TI83 CE Premium	Casio Graph 35+ USB
TESTB : Durée du test de la primalité de 7 237 031	38 s	29 s	16 s

Exercice 4 ***L'infinitude des nombres premiers***

1) En utilisant les programmes de test de primalité et de recherche de facteurs premiers de la calculatrice, on constate que $u_1,\ u_2,\ u_3,\ u_4,\ u_5$ sont premiers. Par contre $u_6,\ u_7,\ u_8$ sont composés et on obtient leur plus petit diviseur.

n	1	2	3	4	5	6	7	8
U_n	3	7	31	211	2311	30031	510511	9699691
U_n est-il premier ?	oui	oui	oui	oui	oui	non	non	non
Plus petit diviseur premier de U_n	3	7	31	211	2311	59	19	347

2) Dans chacun des huit premiers termes, le plus petit diviseur premier de U_n n'est pas l'un des nombres premiers p_i utilisés pour construire le terme U_n.

3) Démonstration par l'absurde.

On suppose qu'il existe un plus grand nombre premier. On pose *p* le plus grand des nombres premiers.

On note $u_p = N = 2 \times 3 \times \ldots \times p + 1$.

a) On a $2 \times 3 \times \ldots \times p > p$ donc $2 \times 3 \times \ldots \times p + 1 > p$ donc $N > p$.

b) Par hypothèse, le plus grand des nombres premiers est *p* donc *N* n'est pas premier, donc *N* est composé.

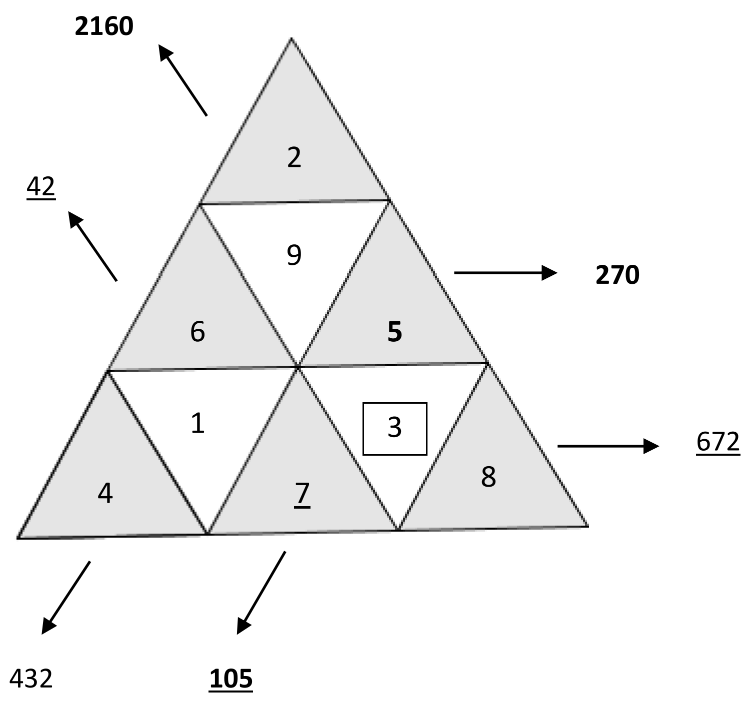
c) Par définition de *N*, on a $N \equiv 1(2),\ N \equiv 1(3),\ N \equiv 1(5),\ N \equiv 1(7),\ \ldots N \equiv 1(p)$. Donc ni 2, ni 3, …, ni *p* ne sont des diviseurs de *N*.

d) On peut en déduire que *N* n'admet aucun diviseur premier. Donc *N* est premier. Or on a démontré précédemment que *N* était composé. Il y a donc contradiction !

e) La conjecture émise est donc fausse. Il n'existe donc pas de " plus grand des nombres premiers".

Conclusion : Il existe une infinité de nombres premiers.

Exercice 5 *Le triangle mystère*



- L'ordre n'est qu'indicatif. Certaines étapes peuvent être permutées.
- On peut commencer le raisonnement en écrivant pour chacun des nombres la décomposition en produits de facteurs premiers.

$2160 = 2^4 \times 3^3 \times \mathbf{5}^1$
$42 = 2^1 \times 3^1 \times \underline{7}^1$
$432 = 2^4 \times 3^3$
$105 = 3^1 \times \mathbf{5}^1 \times \underline{7}^1$
$672 = 2^5 \times 3^1 \times \underline{7}^1$
$270 = 2^1 \times 3^3 \times \mathbf{5}^1$

- 5 et 7 sont des facteurs premiers qui ne peuvent pas être multipliés avec d'autres pour former des nombres dans le triangle car on sait que ces nombres sont les neuf entiers de 1 à 9.

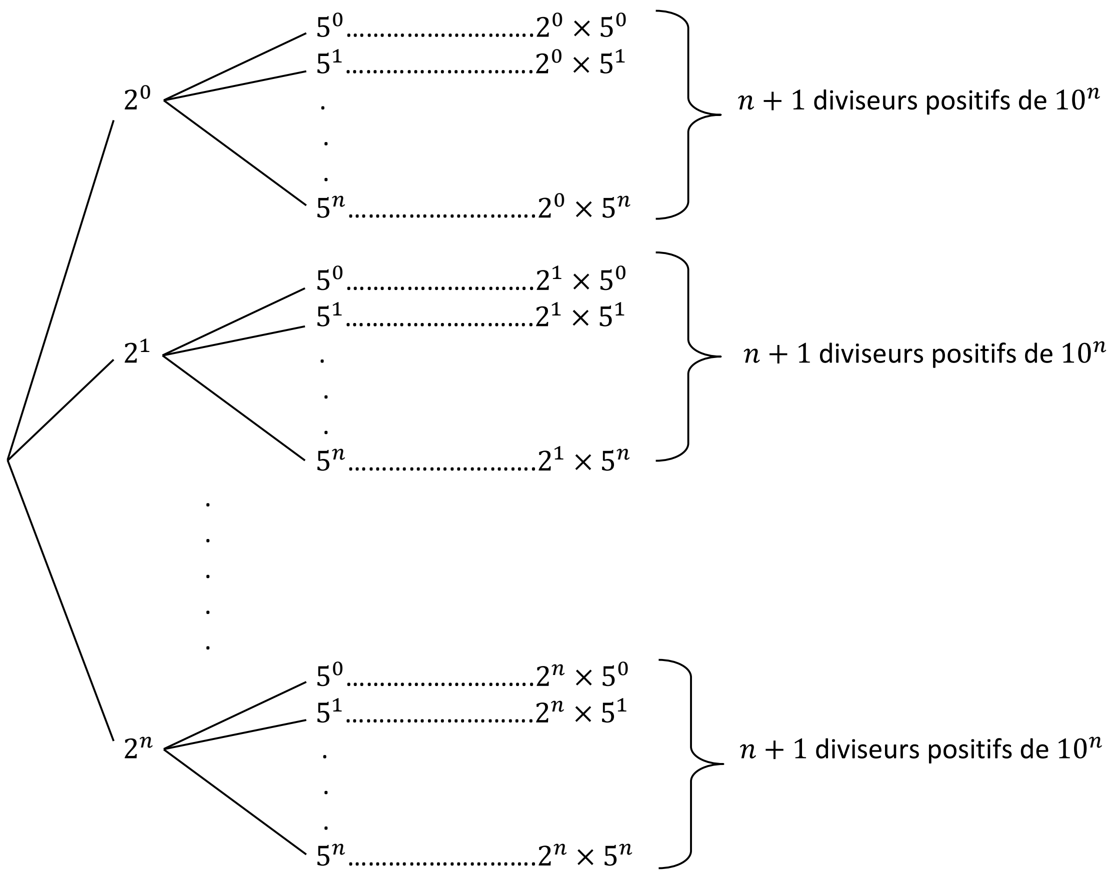
1) 5 : seuls **270**, **105** et **2160** sont divisibles par 5. Donc **5** est à l'intersection des rangées correspondantes.
2) 7 : seuls 42, 105 et 672 sont divisibles par 7. Donc 7 est à l'intersection des rangées correspondantes.
3) 105 est le produit de trois nombres. 5 et 7 ont déjà été placés. Donc la troisième case de sa rangée est occupée par $\boxed{3}$.
4) Le 3 ne peut donc pas être présent dans la rangée du 42. Donc le produit qui donne 42 est nécessairement $1 \times 6 \times 7$.
5) Le 6 est nécessairement dans la ligne qui forme le 270. Cette remarque permet de compléter la ligne du 270 par 9.
6) A ce stade, il reste 2, 4 et 8 à placer. La rangée du 432 qui a encore deux cases de libres nécessite que le produit de ces deux nombres soit égal à 2^3. Il ne peut pas s'agir que de 2×4.
7) Le 8 est donc en bas à droite du triangle. Il est alors facile de placer le 2 et le 4.

Exercice 6 *Vrai - Faux*

1) Faux : Contre-exemple $2 + 3 = 5$. La somme des 2 nombres premiers 2 et 3 est égale à 5 qui est aussi un nombre premier.
2) Faux : Contre-exemple $3^2 + 4 = 13$. 3 et 13 sont tous les deux premiers.
3) Vrai : Démonstration :

   $10^n = (2 \times 5)^n = 2^n \times 5^n$

   Utilisons un arbre afin de dénombrer les diviseurs positifs de 10^n :



Il y a donc bien $(n + 1)^2$ diviseurs positifs de 10^n.

4) Faux : Contre-exemple le nombre 2^{14} admet 15 diviseurs dont seul 2 est premier.

5) Vrai : $u_5 = 5a + 5 = 5(a + 1)$ et donc quelle que soit la valeur de l'entier naturel non nul a, le terme u_5 est composé. Donc toutes les suites u, définie par $u_n = an + 5$ avec a un entier naturel non nul, comportent au moins un nombre composé : u_5.

6) Vrai : L'algorithme proposé fournit $n - 2 + 1 = n - 1$ nombres. Montrons que tous ces nombres sont composés.

- 1er nombre affiché : $n! + 2 = 1 \times 2 \times \ldots \times (n-1) \times n + 2 = 2(3 \times 4 \times \ldots \times (n-1) \times n + 1)$, il est donc divisible par 2, c'est donc un nombre composé.
- 2ème nombre affiché : $n! + 3 = 1 \times 2 \times \ldots \times (n-1) \times n + 3 = 3(2 \times 4 \times \ldots \times (n-1) \times n + 1)$, il est donc divisible par 3, c'est donc un nombre composé.
- Avant dernier nombre affiché :

$n! + n - 1 = 1 \times 2 \times \ldots \times (n-1) \times n + n - 1 = (n-1)(2 \times 3 \times 4 \times \ldots (n-2) \times n + 1)$, il est donc divisible par $n - 1$ c'est donc un nombre composé.

- Dernier nombre affiché : $n! + n = 1 \times 2 \times \ldots \times (n-1) \times n + n = n(2 \times 3 \times 4 \times \ldots (n-1) + 1)$, il est donc divisible par n, c'est donc un nombre composé.