

8

Nombres premiers

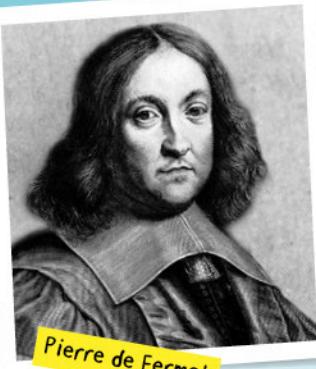
HISTOIRE DES MATHS

Vers 300 ans avant notre ère, **Euclide** dans *Les Éléments* démontre que l'ensemble des nombres premiers est infini ; c'est l'une des premières preuves qui repose sur un raisonnement par l'absurde. Il établit également la décomposition de tout entier naturel $n \geq 2$ en un produit de facteurs premiers.

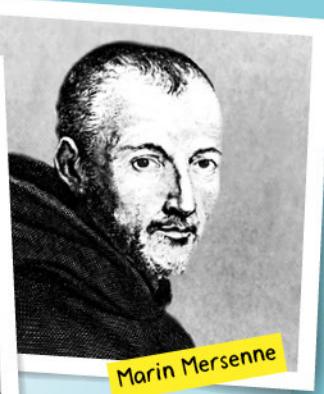
Vers le milieu du 17^e siècle, **Pierre de Fermat**, influencé par la lecture de Diophante s'intéresse à la primalité des nombres de la forme $2^{(2^n)} + 1$ et correspond sur ces sujets avec **Marin Mersenne**.

Il énonce le petit théorème de Fermat démontré plus tard par **Leibniz**, puis par **Euler** dans le langage des congruences.

De nos jours, les nombres premiers sont encore mal connus et restent l'objet de recherches.



Pierre de Fermat



Marin Mersenne

► **Pierre de Fermat** (1607-1665) est un mathématicien français de génie. Il est connu pour ses théorèmes qui influencent la recherche mathématique de son époque. C'est le fondateur de la théorie moderne des nombres.

► **Marin Mersenne** (1588-1648) est un mathématicien et philosophe français. Il entretient des correspondances avec les plus grands savants de son époque. À ce jour, 51 nombres premiers de Mersenne sont connus.

1640
Fermat énonce pour la première fois le petit théorème de Fermat.

1680
Leibniz démontre le petit théorème de Fermat.

1750
Euler prouve que $M_{31} = 2^{31} - 1$ est un nombre de Mersenne premier.

1867
Landry trouve un nombre premier non-Mersenne de 13 chiffres.

1994
Wiles démontre le grand théorème de Fermat.

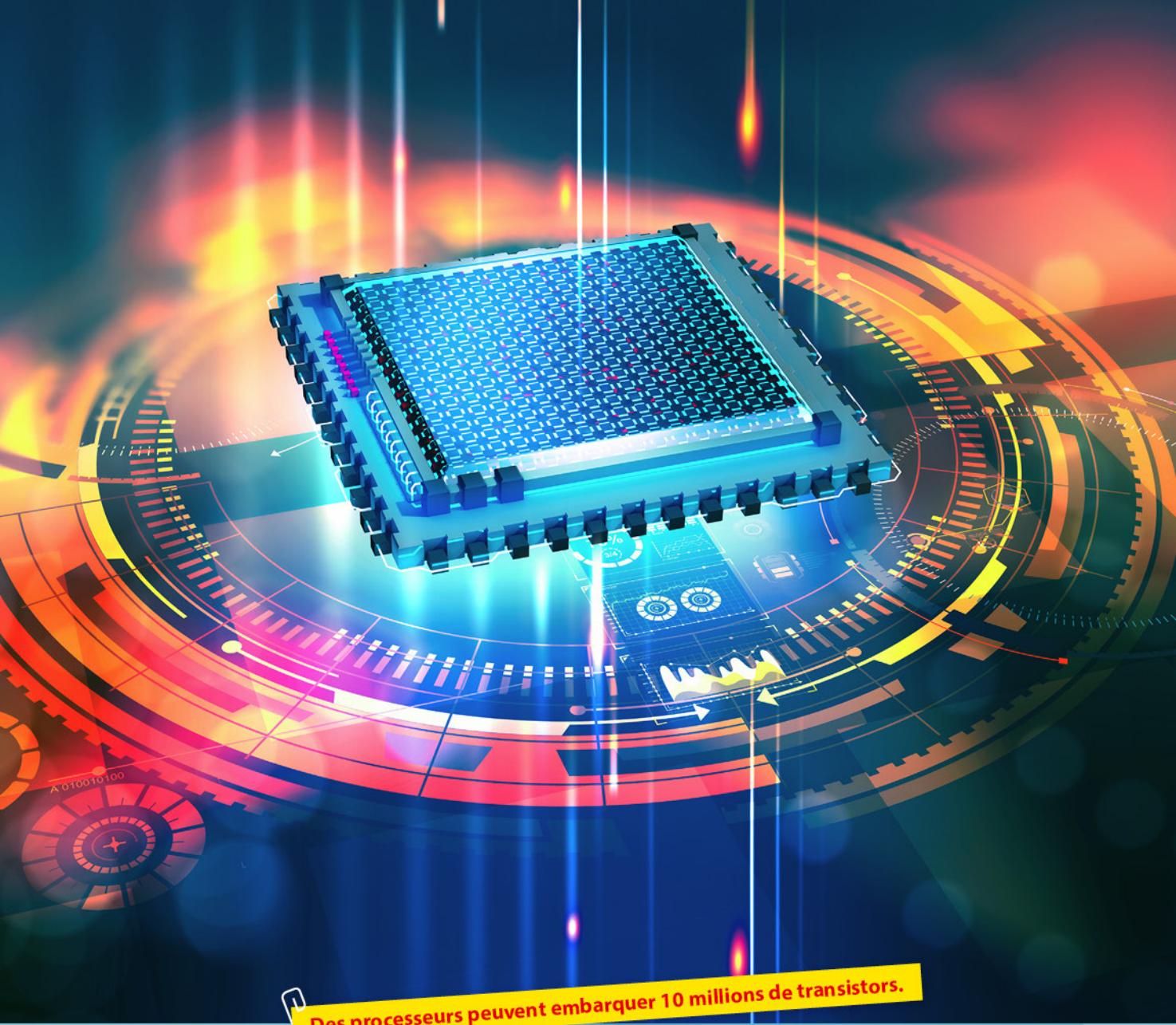
1603
Première société savante fondée à Rome

1664
Première présentation de Tartuffe

1789
Prise de la Bastille

1848
Proclamation de la Deuxième République

1977
Invention de l'algorithme RSA



Des processeurs peuvent embarquer 10 millions de transistors.

De nombreuses applications reposent sur les possibilités limitées de reconnaissance des grands nombres premiers par les algorithmes. On peut citer les systèmes cryptographiques bancaires ou ceux de transmission d'informations (RSA).

L'arrivée des ordinateurs quantiques avec l'algorithme Shor (qui permet de factoriser en un temps record) peut d'ici quelques années rendre vulnérables ces systèmes.

Les contenus et capacités travaillés dans ce chapitre

- Nombres premiers. Étudier la primalité de certains nombres.
- Décomposition d'un entier en produit de facteurs premiers.
- Petit théorème de Fermat.

Savoir-faire	Exercices
1 à 7, 21 à 24	25 à 44, 95
8 à 13	45 à 65
14 à 20	66 à 85



Rappels utiles

• Nombre premier

Un nombre premier est un nombre entier naturel qui a exactement deux diviseurs : 1 et lui-même.

• Décomposition en produit de facteurs premiers

Pour décomposer un nombre entier naturel en produits de facteurs premiers, on peut utiliser l'une des méthodes :

- (1) on cherche ses diviseurs premiers dans l'ordre croissant ;
- (2) on décompose successivement le nombre en produits.

• Une conséquence du théorème de Gauss

a , b et c désignent trois nombres entiers relatifs non nuls.

Si b et c sont premiers entre eux et divisent a , alors bc divise a .

• Raisonnement par l'absurde

Pour démontrer qu'une proposition P est vraie, on peut utiliser un raisonnement par l'absurde :

- on suppose que la proposition P est fausse (c'est-à-dire que « non P » est vraie) ;
- on démontre que l'on aboutit à une contradiction.

À l'oral

Questions-Tests

Pour chaque question, il y a une seule réponse exacte.

- 1** Parmi les entiers naturels suivants, un seul est premier. Lequel ?

(1) $a = 89$ (2) $b = 2020$ (3) $c = 33\,927$

- 2** Un nombre entier naturel premier qui divise 20 est :

(1) 4 (2) 5 (3) 10

- 3** La somme de deux nombres entiers naturels impairs consécutifs est un nombre :

(1) premier
(2) non premier
(3) impair

- 4** n désigne un nombre entier naturel.

On note $N = n^2 + 2n + 1$.

L'affirmation vraie est :

- (1) pour $n = 25$, N est un nombre premier ;
- (2) pour tout nombre n , N est pair ;
- (3) pour tout nombre n , N n'est pas premier.

- 5** La décomposition en produit de facteurs premiers de 132 est :

(1) 12×11 (2) $2^2 \times 3 \times 13$ (3) $2^2 \times 3 \times 11$

- 6** Voici deux décompositions en produits de facteurs premiers :

$$1500 = 2^2 \times 3 \times 5^3 \quad \text{et} \quad 360 = 2^3 \times 3^2 \times 5$$

Alors, la décomposition en produit de facteurs premiers de $1500^2 \times 360^3$ est :

(1) $2^{13} \times 3^8 \times 5^9$ (2) $2^5 \times 3^3 \times 5^4$ (3) $2^{10} \times 3^5 \times 5^8$

- 7** La décomposition en produit de facteurs premiers de $24 \times 36 \times 42$ est :

(1) $2^6 \times 3^4 \times 7$ (2) $2^4 \times 3^2 \times 12 \times 21$ (3) $2^6 \times 3^3 \times 11$

- 8** On donne $A = 2^3 \times 5^4 \times 11^2$.

A est divisible par :

(1) 33 (2) $4 \times 25 \times 11$ (3) $2^2 \times 5^5 \times 11$

- 9** Un nombre entier naturel n est divisible par 2, 4 et 5.

On peut affirmer que n est divisible par :

(1) 8 (2) 20 (3) 40

- 10** On souhaite démontrer par l'absurde la proposition P : « Il existe une infinité de nombres premiers ».

Alors, on suppose que :

- (1) il existe un seul nombre premier ;
- (2) il existe un nombre fini de nombres premiers ;
- (3) aucun nombre entier naturel n'est premier.

1

Algo  python Le crible d'Ératosthène

On considère l'algorithme suivant :

- se donner un nombre entier naturel n supérieur ou égal à 2 ;
 - écrire les nombres entiers naturels compris entre 2 et n ;
 - entourer 2 et barrer les multiples de 2 ;
 - entourer le plus petit des nombres non barrés et barrer tous ses multiples ;
 - recommencer jusqu'à ce que le plus petit nombre non barré soit supérieur à \sqrt{n} .

Cet algorithme est connu sous le nom de crible d'Ératosthène (3^e siècle avant notre ère).

- 1** a) Dresser un tableau avec les nombres entiers naturels de 2 à 100 (10 lignes, 10 colonnes), puis faire fonctionner manuellement l'algorithme précédent avec $n = 100$.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	...						

- b)** Expliquer pourquoi les nombres non barrés sont des nombres premiers inférieurs à 100.

- 2** La fonction **Erato** de paramètre n , écrite en langage Python, traduit l'algorithme précédent et permet d'obtenir tous les nombres premiers inférieurs à n .

Saisir et tester cette fonction pour :

- $n = 200$
 - $n = 500$
 - $n = 800$

```
1 from math import *
2
3 def Erato(n):
4     P=list(range(2,n+1))
5     j=2
6     while j <= sqrt(n):
7         if P[j-2]>=1:
8             for k in range(2,floor(n/j)+1):
9                 P[j*k-2]=0
10    j=j+1
11 L=[]
12 for s in P:
13     if s!=0:
14         L=L+[s]
15 return L
```

2

Algo  python Décomposition en prod

n désigne un nombre entier naturel supérieur ou égal à 2.

- 1** Dans chaque cas, décomposer le nombre n en produit de facteurs premiers.

a) $n = 72$ b) $n = 1\,620$ c) $n = 5\,439$

- 2** Ce programme écrit en langage Python, définit une fonction **Decomp** de paramètre n .

- a) Exécuter pas à pas ce programme pour la valeur $n = 24$ du paramètre en complétant le tableau ci-dessous après l'avoir recopié.

n	24	12	6	
$n\%p$	0	0		
L	[2]	[2,2]		
q	12			

- b)** Quel résultat la fonction **Decomp** renvoie-t-elle ?

3 On complète le programme précédent (la ligne 10 est modifiée).

 - a)** Saisir ce programme.
 - b)** Exécuter la nouvelle fonction **Decomp** avec $n = 5\,439$. Qu'obtient-on ?
 - c)** Quel est le rôle de ce programme ?

```
1 from math import *
2
3 def Decomp(n):
4     L=[ ]
5     p=2
6     while n%p==0:
7         L.append(p)
8         q=int(n/p)
9         n=q
10    return L
```

```
10 d=3
11 while d<=n:
12     while n%d==0:
13         L.append(d)
14         q=int(n/d)
15         n=q
16         d=d+2
17 return L
```

1

Nombres premiers

A Nombres premiers dans \mathbb{N}

Définition

Dire qu'un nombre entier naturel est **premier** signifie qu'il admet **exactement deux diviseurs** dans \mathbb{N} : 1 et lui-même.

Exemples

- 0 n'est pas un nombre premier, car il admet une infinité de diviseurs dans \mathbb{N} .
- 1 n'est pas premier, car il a un seul diviseur dans \mathbb{N} : lui-même.
- 2 est le plus petit nombre premier et le seul qui soit pair.

Un entier $n \geq 2$ non premier est dit composé.

B Reconnaissance d'un nombre premier

Propriété

n désigne un nombre entier naturel supérieur ou égal à 4.

Si n n'est pas premier, alors n admet au moins un diviseur premier p : son plus petit diviseur dans \mathbb{N} autre que 1, tel que $2 \leq p \leq \sqrt{n}$.

Démonstration

$n \geq 4$ est un nombre entier naturel non premier. L'ensemble de ses diviseurs supérieurs ou égaux à 2 contient au moins un élément différent de n . On note p le plus petit de ces diviseurs.

On raisonne par l'absurde et **on suppose que p n'est pas premier**. Alors p admet un diviseur d tel que $2 \leq d < p$. De d divise p et p divise n , on déduit que d divise n , ce qui établit une contradiction, car p est le plus petit diviseur de n strictement supérieur à 1. Ainsi, **p est premier**.

Il reste à démontrer que p vérifie $2 \leq p \leq \sqrt{n}$.

On sait que $n = pq$ avec $2 \leq p \leq q$ donc $p^2 \leq pq$ soit $p^2 \leq n$ et par suite, $p \leq \sqrt{n}$.

Propriété

n désigne un nombre entier naturel supérieur ou égal à 4.

Si n n'est divisible par aucun nombre premier p tel que $2 \leq p \leq \sqrt{n}$, alors n est premier.

Démonstration

- C'est la contraposée de la propriété précédente.

« Si P, alors Q » et sa contraposée « Si non Q, alors non P » sont équivalentes.

C L'ensemble des nombres premiers

Propriété

Il existe une infinité de nombres premiers.

Démonstration

On raisonne par l'absurde. **On suppose qu'il existe un nombre fini** de nombres premiers p_1, p_2, \dots, p_n .

On considère le nombre $a = p_1 p_2 \dots p_n + 1$. Ce nombre entier naturel est supérieur ou égal à 2, donc il admet au moins un diviseur premier p_i parmi les nombres p_1, p_2, \dots, p_n .

Cet entier p_i divise a et divise $p_1 p_2 \dots p_n$, donc il divise la différence, c'est-à-dire 1. D'où la contradiction.

Ainsi, il existe une infinité de nombres premiers.

EXERCICES RÉSOLUS

1 Reconnaître un nombre premier

Dans chaque cas, dire si le nombre est premier.

a) 133

b) 547

Solution

a) $\sqrt{133} \approx 11,5$.

Les nombres premiers inférieurs à $\sqrt{133}$ sont 2, 3, 5, 7 et 11.

133 n'est pas divisible par 2, 3 et 5 mais $133 = 7 \times 19$.

Donc 133 n'est pas un nombre premier.

b) $\sqrt{547} \approx 23,4$.

Les nombres premiers inférieurs à $\sqrt{547}$ sont 2, 3, 5, 7, 11, 13, 17, 19 et 23.

547 n'est divisible par aucun de ces nombres.

Donc 547 est un nombre premier.

Il est utile de connaître les nombres premiers inférieurs à 100 :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

2 Déterminer si un nombre (fonction de n , $n \in \mathbb{N}$) est premier

n désigne un nombre entier naturel supérieur ou égal à 3. On donne $a = n^2 - 2n - 3$.

Existe-t-il des valeurs de n telles que a soit un nombre premier ?

Solution

On remarque que pour tout entier naturel $n \geq 3$, $a = (n+1)(n-3)$.

Donc pour $n \geq 5$, a est le produit de deux nombres entiers $n+1$ et $n-3$ supérieurs ou égaux à 2 et a n'est pas un nombre premier.

Il reste à observer les cas $n = 3$ et $n = 4$.

- Si $n = 3$, alors $a = 0$ et a n'est pas un nombre premier.

- Si $n = 4$, alors $a = 5$ et a est un nombre premier.

Conclusion : a est un nombre premier si, et seulement si, $n = 4$.

Si un nombre entier naturel $a \geq 4$, s'écrit $a = pq$ avec p et q nombres entiers naturels supérieurs ou égaux à 2, alors a n'est pas un nombre premier.

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 1

3 Dans chaque cas, dire si le nombre est premier.

a) 287

b) 467

4 Voici une copie d'écran de calcul formel.

1	EstPremier(684)
	→ false
2	EstPremier(739)
	→ true
3	EstPremier(2021)
	→ false

Justifier les résultats obtenus.

Sur le modèle de l'exercice résolu 2

5 n désigne un nombre entier naturel.

On pose $a = n^2 + 3n + 2$.

Existe-t-il des valeurs de n telles que a soit un nombre premier ?

6 Dans les inédits de Marcel Pagnol (Éditions Pastorelli, 1992), l'écrivain indique que pour tout entier naturel impair n , le nombre $n + (n+2) + n(n+2)$ est premier. Cette affirmation est-elle vraie ? Justifier.

7 n désigne un nombre entier naturel.

Le nombre $n^2 + 6n + 9$ peut-il être premier ?

- 8 à 13 (ci-contre)
- 45 à 65

2

Décomposition en produit de facteurs premiers

A Existence et unicité d'une décomposition

Propriété

Tout entier naturel $n \geq 2$ est premier ou produit de nombres premiers.

Démonstration

Si n est premier, la propriété est établie.

Si n n'est pas premier, alors son plus petit diviseur $p_1 \geq 2$ est premier et il existe un entier naturel n_1 tel que $n = p_1 \times n_1$ avec $n_1 < n$.

Si n_1 est premier, la propriété est établie.

Si n_1 n'est pas premier, alors on recommence comme précédemment.

De proche en proche, on obtient ainsi une suite strictement décroissante de nombres entiers naturels n_i tels que $2 \leq \dots < n_i < \dots < n_2 < n_1$. Cette suite est finie et le dernier d'entre eux est un nombre premier n_k , donc $n = p_1 p_2 \dots p_k n_k$ avec $p_1, p_2, \dots, p_k, n_k$ premiers.

Notation : les nombres premiers ci-dessus ne sont pas nécessairement distincts. En les regroupant, on obtient $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ où p_1, p_2, \dots, p_r sont des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_r$ des nombres entiers naturels non nuls. On dit que **n est décomposé en produit de facteurs premiers**.

Propriété

La décomposition en produit de facteurs premiers de tout nombre entier naturel supérieur ou égal à 2 est unique.

Démonstration

On suppose qu'un certain nombre premier p apparaît avec l'exposant $\alpha \geq 1$ dans une décomposition de n , et l'exposant $\beta \geq 0$ dans une autre (on envisage $\beta = 0$ pour le cas où p ne figurerait pas dans la deuxième décomposition). Alors $n = p^\alpha a = p^\beta b$, où a et b sont des produits de nombres premiers distincts de p .

Si $\alpha > \beta$, $p^{\alpha-\beta} a = b$, ce qui contredit que p et b sont premiers entre eux.

Si $\alpha < \beta$, $a = p^{\beta-\alpha} b$, ce qui contredit que p et a sont premiers entre eux. Donc $\alpha = \beta$.

B Diviseurs d'un nombre entier naturel non premier

Propriété

$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ est la décomposition en produit de facteurs premiers d'un nombre entier naturel $n \geq 2$.

Les diviseurs positifs de n sont de la forme $p_1^{\alpha'_1} p_2^{\alpha'_2} \dots p_r^{\alpha'_r}$ où $0 \leq \alpha'_1 \leq \alpha_1, \dots, 0 \leq \alpha'_r \leq \alpha_r$.

Démonstration

- Les nombres entiers naturels de la forme $p_1^{\alpha'_1} p_2^{\alpha'_2} \dots p_r^{\alpha'_r}$ sont des diviseurs de n . En effet, on peut écrire : $n = (p_1^{\alpha'_1} p_2^{\alpha'_2} \dots p_r^{\alpha'_r}) \times p_1^{\alpha_1 - \alpha'_1} p_2^{\alpha_2 - \alpha'_2} \dots p_r^{\alpha_r - \alpha'_r}$, où les exposants $\alpha_i - \alpha'_i$ sont positifs ou nuls.

- d est un diviseur de n . Si $p^{\alpha'}$ avec p premier, divise d , alors $p^{\alpha'}$ divise n . L'unicité de la décomposition de n en facteurs premiers implique que le nombre $p^{\alpha'}$ doit figurer dans cette décomposition, donc p est l'un des p_i et $0 \leq \alpha' \leq \alpha_i$.

Ainsi d est de la forme $p_1^{\alpha'_1} p_2^{\alpha'_2} \dots p_r^{\alpha'_r}$ où $0 \leq \alpha'_1 \leq \alpha_1, \dots, 0 \leq \alpha'_r \leq \alpha_r$.

Conséquence : a et b désignent deux nombres entiers naturels supérieurs ou égaux à 2.

Le PGCD de a et b est égal au produit des facteurs premiers communs aux décompositions de a et b , chacun d'eux étant affecté du plus petit exposant avec lequel il figure dans a et b .

EXERCICES RÉSOLUS

8 Reconnaître un diviseur

Dans chaque cas, dire sans calcul si b est un diviseur de a .

a) $a = 2^4 \times 3^2 \times 7$ et $b = 2^2 \times 3^2$ b) $a = 2 \times 3^2 \times 11^2$ et $b = 2^2 \times 3 \times 11$ c) $a = 3^4 \times 5^2$ et $b = 2 \times 3^2$

Solution

- a) Les facteurs premiers de b (2 et 3) figurent dans la décomposition de a avec des exposants plus grands que dans celle de b . Donc b divise a .
- b) Les facteurs premiers de b (2, 3, 11) figurent dans la décomposition de a . Mais l'exposant de 2 dans la décomposition de b est plus grand que dans celle de a . Donc b ne divise pas a .
- c) Dans la décomposition de b figure le facteur 2, qui n'est pas dans la décomposition de a .
Donc b ne divise pas a .

9 Déterminer tous les diviseurs d'un nombre entier naturel

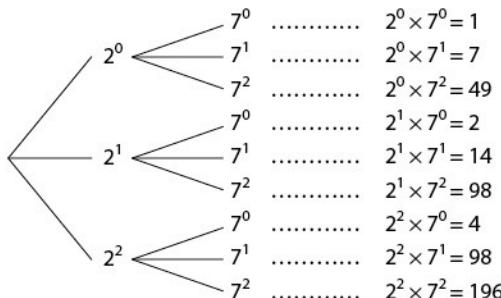
a) Décomposer 196 en produit de facteurs premiers.

b) À l'aide d'un arbre, en déduire tous les diviseurs positifs de 196.

Solution

a) $196 = 4 \times 49 = 2^2 \times 7^2$.

b) Les diviseurs de 196 s'écrivent $2^\alpha \times 7^\beta$ avec $0 \leq \alpha \leq 2$ et $0 \leq \beta \leq 2$.



Les diviseurs positifs de 196 sont donc : 1 ; 2 ; 4 ; 7 ; 14 ; 28 ; 49 ; 98 ; 196.

Il y en a $(2+1) \times (2+1) = 9$.

On peut chercher les diviseurs premiers dans l'ordre croissant :

196	2
98	2
49	7
7	7
1	

On obtient les diviseurs de 196 en multipliant les diviseurs 1, 2, 4 par chacun des diviseurs 1, 7, 49.

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 8

10 Dans chaque cas, dire sans calcul si b est un diviseur de a .

a) $a = 2^3 \times 5^2 \times 11$ et $b = 2 \times 7^2 \times 11$

b) $a = 2^2 \times 3^3 \times 7^2$ et $b = 2 \times 3^2 \times 7$

11 Utiliser l'écran de calcul formel ci-contre pour dire si 550 divise 24 500.

1	Factoriser(24500)
<input type="radio"/>	$\rightarrow 2^2 \cdot 5^3 \cdot 7^2$
2	FacteursPremiers(550)
<input type="radio"/>	$\rightarrow \{2, 5, 5, 11\}$

Sur le modèle de l'exercice résolu 9

12 1. a) Décomposer $a = 220$ en produit de facteurs premiers.

b) À l'aide d'un arbre, en déduire tous les diviseurs positifs de $a = 220$.

2. Reprendre les questions ci-dessus avec $a = 735$.

13 On donne $a = 256$ et $b = 5040$.

a) Décomposer a et b en produit de facteurs premiers, puis déterminer PGCD($a; b$).

b) Retrouver PGCD($a; b$) à l'aide de l'algorithme d'Euclide.

3 Petit théorème de Fermat

A Bref historique

Pierre de Fermat est un mathématicien atypique dont la célébrité provient surtout d'une annotation placée en marge d'un exemplaire des *Arithmétique* de Diophante : « Diviser un cube en deux cubes, une puissance quatrième en deux puissances quatrièmes ou une puissance quelconque en deux puissances de même dénomination est impossible ».

En termes modernes, « Pour tout entier naturel $n > 2$, il est impossible de trouver un triplet $(x ; y ; z)$ d'entiers positifs et non nuls tels que $x^n + y^n = z^n$. » Cette propriété uniquement démontrée par Fermat dans le cas $n = 4$, porte le nom de **Grand théorème de Fermat**.

Plus de 350 ans de recherche ont été nécessaires pour établir une preuve. C'est en 1994 que le Britannique Andrew Wiles est parvenu à le démontrer. Les contributions de Fermat sont cependant importantes, en particulier le **Petit théorème de Fermat** qu'il cite en 1640 dans l'une de ses lettres mais ne le démontre pas. Les premières preuves sont de Leibniz et Euler.

B Petit théorème de Fermat

Petit théorème de Fermat

p désigne un nombre premier et a un nombre entier naturel non divisible par p .

Alors $a^{p-1} - 1$ est divisible par p , c'est-à-dire $a^{p-1} \equiv 1 [p]$.

Démonstration

- p est un nombre premier, donc p est premier avec $1, 2, \dots, p-1$ (sinon p admettrait un diviseur positif autre que 1) et donc p est premier avec $(p-1)!$.

- Si k est un entier tel que $1 \leq k \leq p-1$, alors le reste r_k de la division de ka par p est non nul.

En effet, si p divise ka , alors p divise a car p est premier avec k ; or, ceci est impossible car par hypothèse a n'est pas divisible par p .

- Si k' est un entier distinct de k (par exemple $k < k'$) tel que $1 \leq k' \leq p-1$, alors les restes $r_{k'}$ et r_k des divisions respectives de $k'a$ et ka par p sont distincts. En effet, si $r_{k'} = r_k$ alors p divise $k'a - ka$, c'est-à-dire $(k' - k)a$ avec $1 \leq k' - k \leq p-1$, ce qui est impossible car a n'est pas divisible par p .

- Ainsi, les $p-1$ restes r_1, r_2, \dots, r_{p-1} des divisions respectives de $a, 2a, \dots, (p-1)a$ par p sont donc des nombres entiers naturels non nuls, strictement inférieurs à p et tous distincts.

Donc l'un des restes est égal à 1, l'autre à 2, ..., l'autre à $p-1$. D'où en utilisant le produit des congruences : $a \times 2a \times \dots \times (p-1)a \equiv r_1 r_2 \dots r_{p-1} [p]$, c'est-à-dire $(p-1)! a^{p-1} \equiv (p-1)! [p]$.

Donc p divise $(p-1)! a^{p-1} - (p-1)!$, c'est-à-dire $(p-1)! (a^{p-1} - 1)$.

Or, p est premier avec $(p-1)!$, donc d'après le théorème de Gauss, p divise $a^{p-1} - 1$, c'est-à-dire $a^{p-1} \equiv 1 [p]$.

Conséquence

p désigne un nombre premier et a un entier naturel.

Alors $a^p - a$ est divisible par p , c'est-à-dire $a^p \equiv a [p]$.

Démonstration

$$a^p - a = a(a^{p-1} - 1).$$

- Si a est divisible par p , alors $a(a^{p-1} - 1)$, c'est-à-dire $a^p - a$ est divisible par p .

- Si a n'est pas divisible par p , alors d'après le petit théorème de Fermat, $a^{p-1} - 1$ est divisible par p et donc $a(a^{p-1} - 1)$, c'est-à-dire $a^p - a$ est divisible par p .

EXERCICES RÉSOLUS

14 Résoudre une congruence

On considère l'équation (E) : $5x \equiv 28 [31]$.

- a) Justifier que $5^{30} \equiv 1 [31]$.
- b) En déduire une solution particulière x_0 , $0 \leq x_0 \leq 30$ de (E).
- c) Résoudre alors l'équation (E).

Solution

- a) 31 est premier et 5 n'est pas divisible par 31, d'après le petit théorème de Fermat, $5^{30} \equiv 1 [31]$.
- b) D'après a), $28 \times 5^{30} \equiv 28 [31]$, c'est-à-dire $5 \times 28 \times 5^{29} \equiv 28 [31]$.
Donc 28×5^{29} est une solution de (E). Or, $29 = 9 \times 3 + 2$ et $5^{29} = (5^3)^9 \times 5^2$. De $5^3 \equiv 1 [31]$, on déduit que $28 \times 5^{29} \equiv 28 \times 5^2 [31]$, soit $28 \times 5^{29} \equiv 700 [31]$, c'est-à-dire $28 \times 5^{29} \equiv 18 [31]$.
Ainsi, $x_0 = 18$ est une solution particulière de (E) telle que $0 \leq x_0 \leq 30$.
- c) x est solution de (E) si, et seulement si, $5x \equiv 28 [31]$, c'est-à-dire $5x \equiv 5 \times 18 [31]$ d'après a).
Ainsi x est solution de (E) si, et seulement si $5(x - 18) \equiv 0 [31]$, c'est-à-dire $x - 18 \equiv 0 [31]$ car 5 et 31 sont premiers entre eux.
Les solutions de (E) sont les entiers $x = 18 + 31k$ avec $k \in \mathbb{Z}$.

15 Établir une divisibilité

Démontrer que pour tout entier naturel n , $n^{13} - n$ est divisible par 26.

Solution

- On remarque que $26 = 2 \times 13$ avec 2 et 13 nombres premiers.
- D'après une conséquence du petit théorème de Fermat, 13 divise $n^{13} - n$.
- Si $n \equiv 0 [2]$, alors $n^{13} \equiv 0 [2]$.
- Si $n \equiv 1 [2]$, alors $n^{13} \equiv 1 [2]$ et $n^{13} \equiv n [2]$, soit 2 divise $n^{13} - n$.
- Conclusion :** 2 et 13 divisent $n^{13} - n$, 2 et 13 sont premiers entre eux, donc 26 divise $n^{13} - n$.

On utilise une conséquence du théorème de Gauss : si b et c sont premiers entre eux et divisent a , alors bc divise a .

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 14

16 (E) est l'équation $6x \equiv 32 [37]$.

- a) Justifier que $6^{36} \equiv 1 [37]$.
- b) En déduire une solution particulière x_0 de (E) telle que $0 \leq x_0 \leq 36$. Résoudre alors l'équation (E).

17 x et y désignent des entiers relatifs. (E) est l'équation $8x - 31y = 25$.

- a) Justifier que $8^{30} \equiv 1 [31]$.
- b) En déduire une solution particulière $(x_0 ; y_0)$ de (E) avec $0 \leq x_0 \leq 30$. Résoudre alors l'équation (E).

Sur le modèle de l'exercice résolu 15

18 Démontrer que pour tout entier naturel n , $n^7 - n$ est divisible par 21.

- 19 a) Démontrer que pour tout entier naturel n , $n(n^4 - 1)$ est divisible par 15.
- b) Pour tout entier naturel n , le nombre $n(n^4 - 1)$ est-il divisible par 30 ?

20 Démontrer que pour tout entier naturel n , $n(n^6 - 1)$ est divisible par 42.

EXERCICE RÉSOLU

21 Étudier un test de primalité

Cours 1

n désigne un nombre entier naturel, $n \geq 4$.

On rappelle une propriété du cours :

si n n'est divisible par aucun nombre premier p tel que $2 \leq p \leq \sqrt{n}$, alors n est premier.

Voici une fonction **Primalite** de paramètre n écrite en langage Python.

- a) Exécuter pas à pas ce programme pour $n = 35$ et $n = 47$. Dans chaque cas, réaliser un tableau de suivi des variables.
- b) Expliquer le rôle de cette fonction et donner la signification du nombre qu'elle renvoie.
- c) Saisir le programme et l'exécuter avec différentes valeurs de n .

```

1 from math import *
2
3 def Primalite(n):
4     N=floor(sqrt(n))
5     d=1
6     for k in range(2,N+1):
7         if n % k == 0 :
8             d=0
9     return d

```

Solution

a) La variable d est initialisée à 1.

- Pour $n = 35$, alors $N = 5$.

k	2	3	4	5
$n \% k$	1	2	3	0
d	1	1	1	0

La fonction renvoie la valeur 0.

- Pour $n = 47$, alors $N = 6$.

k	2	3	4	5	6
$n \% k$	1	2	3	2	5
d	1	1	1	1	1

La fonction renvoie la valeur 1.

b) Cette fonction permet de tester la primalité de l'entier naturel $n \geq 4$.

Si n est un nombre premier, alors elle renvoie la valeur 1 et sinon, elle renvoie la valeur 0.

c) Voici quelques exemples.

>>> Primalite(71)
1

>>> Primalite(1111)
0

>>> Primalite(563)
1

>>> Primalite(481)
0

EXERCICES D'APPLICATION DIRECTE

Sur le modèle de l'exercice résolu 21

22 n est un nombre entier naturel, $n \geq 4$.

a) Écrire une fonction **Pair** en langage Python qui permet de tester la parité de l'entier naturel n .

b) Lorsque n est pair, n n'est pas un nombre premier. Proposer une modification du programme de l'exercice 21 qui prend en compte cette remarque.

c) Saisir le programme et l'exécuter avec différentes valeurs de n .

23 n désigne un nombre entier naturel, $n \geq 4$.

a) Lorsque n est pair ou multiple de 5, n n'est pas un nombre premier. Modifier le programme de l'exercice 21 afin de prendre en compte cette remarque.

b) Saisir et tester le programme obtenu.

24 a) Compléter le programme de l'exercice 21 afin de renvoyer également le nombre des entiers naturels k rencontrés dans la boucle tels que $n \% k == 0$.

b) Saisir et tester le programme obtenu.

Nombres premiers

Cours 1

Questions flash

À l'oral

25 Expliquer oralement pourquoi aucun des nombres suivants n'est premier.

- a) 21 b) 325 c) 777 d) 169

26 S est la somme de trois nombres entiers naturels impairs consécutifs. L'affirmation vraie est :

- (1) S est toujours un nombre premier.
 (2) S est parfois un nombre premier.
 (3) S n'est jamais un nombre premier.

27 L'une de ces affirmations est exacte. Laquelle ?

- (1) Tous les nombres premiers sont impairs.
 (2) Un nombre premier peut être la somme de deux nombres premiers.
 (3) Un nombre premier peut être le produit de deux nombres premiers.

28 Wilson affirme : « $\sqrt{113} \approx 10,6$, cela permet de conclure que 113 est un nombre premier ». Que peut-on en penser ?

29 Anaë affirme « $2^{2020} - 1$ est un nombre premier ».

Que peut-on en penser ?

30 Dans chaque cas, déterminer si le nombre est premier ou non.

- | | | |
|--------|----------|----------|
| a) 251 | b) 341 | c) 853 |
| d) 712 | e) 1 021 | f) 1 023 |

31 Voici une copie d'écran de calcul formel. Justifier les résultats obtenus.

	EstPremier(327)
1	→ false
	EstPremier(733)
2	→ true

32 Un nombre entier naturel inférieur à 150 n'est divisible par aucun des cinq premiers nombres premiers. Peut-on affirmer qu'il est premier ?

33 n est un nombre entier naturel supérieur ou égal à 3. Démontrer que le nombre $n^2 + 2n - 3$ n'est jamais premier.

34 n est un nombre entier naturel.

On donne $a = n^2 + 4n + 3$.

Existe-t-il des valeurs de n telles que a soit premier ?

35 Pour tout entier naturel n, on pose :

$$f(n) = 2n^2 + 29.$$

a) Vérifier que $f(28)$ est un nombre premier.

b) Qu'en est-il de $f(29)$?

c) En déduire que $f(n)$ est un nombre composé pour une infinité de valeurs de n.

36 Algo python

Maëva a écrit les fonctions suivantes en langage Python :

```
1 from sympy import *
2
3 def f(x):
4     y=x**2-x+41
5     return y
6
7 def Test(n):
8     c=0
9     for k in range(0,n+1):
10         if isprime(f(k)):
11             c=c+1
12
13 return c
```

a) Expliquer le rôle de la fonction **Test**.

Pour une valeur n (n entier naturel) du paramètre, quel résultat renvoie-t-elle ?

b) Pour les valeurs n = 40 et n = 41 du paramètre, elle obtient les résultats ci-dessous.

```
>>> Test(40)
41
>>> Test(41)
41
```

Les interpréter.

isprime(n) renvoie le booléen True si n est premier et False sinon.

c) En déduire une valeur de l'entier naturel n pour laquelle $n^2 - n + 41$ n'est pas un nombre premier.

37 n désigne un nombre premier strictement supérieur à 3.

a) Démontrer que n est de la forme $3k + 1$ ou $3k + 2$, avec k nombre entier naturel non nul.

b) La réciproque est-elle vraie ?

38 p désigne un nombre premier, $p \geq 5$.

a) Démontrer que $p^2 - 1$ est divisible par 3.

b) Démontrer que $p^2 - 1$ est divisible par 8.

c) En déduire que $p^2 - 1$ est divisible par 24.

39 p désigne un nombre premier.

$P = 2 \times 3 \times 5 \times \dots \times p$ est le produit des nombres entiers naturels premiers inférieurs ou égaux à p.

a) Démontrer que les $(p - 1)$ nombres entiers naturels consécutifs $P + 2, P + 3, \dots, P + p$ ne sont pas premiers.

b) Donner un exemple de dix nombres entiers naturels consécutifs non premiers.

40 k désigne un nombre entier naturel impair, $k > 1$ et n un nombre entier naturel.

a) Vérifier que, pour tout réel x ,

$$x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + \dots - x + 1).$$

b) En prenant $x = 2^{(2^n)}$, en déduire que le nombre $2^{(2^n)k} + 1$ n'est pas un nombre premier.

c) Quelle valeur de k faut-il prendre si l'on veut trouver des nombres premiers dans la famille des nombres $2^{(2^n)k} + 1$?

Un nombre de Fermat est un nombre entier naturel qui peut s'écrire sous la forme $2^{(2^n)} + 1$ avec n nombre entier naturel. On note F_n un tel nombre.

41 n désigne un nombre entier naturel.

On donne $F_n = 2^{(2^n)} + 1$.

a) Vérifier que les cinq premiers nombres de Fermat sont premiers.

b) Justifier que $F_5 \equiv 0 \pmod{641}$.

Conclure.

42 On considère l'équation (E) : $n^2 = 19p + 1$ d'inconnue le couple $(n; p)$ où n est un entier naturel et p un nombre premier

a) Si $(n; p)$ est solution, écrire $19p$ comme le produit de deux facteurs en fonction de n .

b) Résoudre l'équation (E).

43 n et a désignent des nombres entiers naturels supérieurs ou égaux à 2.

1. a) Vérifier que :

$$a^n - 1 = (a-1)(1+a+a^2+\dots+a^{n-1}).$$

b) Les nombres $2^5 - 1$ et $3^{35} - 1$ sont-ils premiers ?

2. Justifier que si $a > 2$, alors $a^n - 1$ n'est pas premier.

Les nombres de la forme $M_n = 2^n - 1$ où n désigne un nombre entier naturel, $n \geq 1$, sont appelés nombres de Mersenne.

44 n, p et q désignent des nombres entiers naturels supérieurs ou égaux à 2.

1. a) Vérifier que :

$$2^{pq} - 1 = (2^p - 1)(1+2^p+2^{2p}+\dots+2^{(q-1)p}).$$

b) En déduire que si n n'est pas premier, alors $M_n = 2^n - 1$ n'est pas premier.

c) Parmi les nombres de Mersenne M_2, \dots, M_{12} , quels sont ceux qui sont premiers ?

2. a) Justifier que si M_n est premier, alors n est premier.

b) La réciproque est-elle vraie ?

Décomposition en produit de facteurs premiers

Cours 2

Questions Flash

À l'oral

45 On sait que $260 = 20 \times 13$.

Donner oralement la décomposition en produit de facteurs premiers de 260.

46 Décomposer mentalement chaque nombre en produit de facteurs premiers.

- a) 30 b) 32 c) 50 d) 81 e) 242

47 Laquelle de ces affirmations est fausse ?

La décomposition en produit de facteurs premiers :

(1) de 360 est $2^2 \times 3^2 \times 5$;

(2) de 126 est $2^2 \times 3 \times 7$;

(3) de 248 est $2^3 \times 31$

48 On donne $a = 2^3 \times 5^2 \times 7$ et $b = 2^2 \times 5 \times 7^2$.

Alexia affirme « $\text{PGCD}(a; b) = 2^3 \times 5^2 \times 7^2$. »

A-t-elle raison ?

49 On donne $a = 3^5 \times 5^3 \times 11^6$ et $b = 3^2 \times 5 \times 11^3$

Félix affirme « a est divisible par b^2 . »

A-t-il raison ?

50 Décomposer chacun des nombres en produit de facteurs premiers.

- a) 1 080 b) 521 c) 69×21
d) $12^2 \times 10^4$ e) $2^{12} - 1$ f) $10^3 - 1$

51 Dans chaque cas, décomposer le nombre donné en produit de facteurs premiers.

- a) 1 309 b) 2 314 c) 3 214

52 On donne $N = 65\ 065\ 000$.

On a obtenu l'écran

ci-contre à l'aide

d'une calculatrice.

Donner le plus grand nombre entier naturel :

- a) dont le carré divise N ;
b) dont le cube divise N .

factor(65065000)

$$2^3 \times 5^4 \times 7 \times 11 \times 13^2 = 6.5065 \times 10^7$$

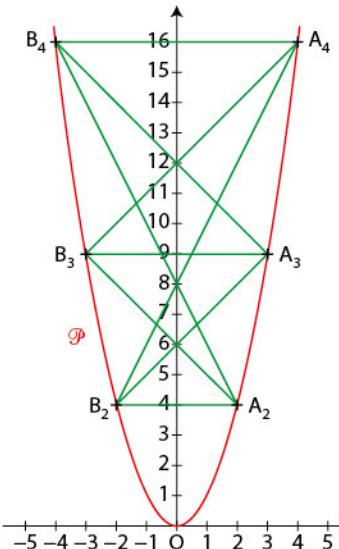
53 a) Décomposer 8 775 en produit de facteurs premiers.

b) Déterminer le plus petit nombre entier naturel k non nul tel que $8775k$ soit :

- le carré d'un nombre entier ;
- le cube d'un nombre entier.

- 54** Dans un repère orthonormé, \mathcal{P} est la parabole d'équation $y = x^2$. Pour i et j entiers naturels, $i \geq 2$ et $j \geq 2$, on note $A_i(i; i^2)$ et $B_j(-j; j^2)$ des points de \mathcal{P} .

On relie tous les points A_i aux points B_j .



- 1. a)** Vérifier qu'une équation de la droite (A_iB_j) est :

$$y = (i - j)x + ij.$$

- b)** Déterminer l'ordonnée du point d'intersection de la droite (A_iB_j) et de l'axe des ordonnées.

- 2. a)** Par certains points de coordonnées $(0; k)$, avec k nombre entier naturel, il ne passe aucune droite (A_iB_j) . Lesquels ?

- b)** Déterminer toutes les droites qui passent par le point de coordonnées $(0; 30)$.

- 55** **a)** Décomposer 756 en produit de facteurs premiers.

- b)** Sans calculatrice, en déduire la décomposition en produit de facteurs premiers de chaque nombre :

$$\bullet 756^3 \quad \bullet 50 \times 756^2 \quad \bullet \frac{756}{9} \quad \bullet (6 \times 756)^5$$

- 56** À l'aide d'un logiciel de calcul formel, on a obtenu l'écran ci-dessous.

1	Factoriser(2020)
<input type="radio"/>	$\rightarrow 2^2 \cdot 5 \cdot 101$
2	Factoriser(28848428)
<input type="radio"/>	$\rightarrow 2^2 \cdot 7 \cdot 101^3$

- a)** Justifier les résultats obtenus.

- b)** Donner la décomposition en produit de facteurs premiers de chacun des nombres suivants :

$$\bullet 2020^3 \quad \bullet 28\ 848\ 428^2 \\ \bullet 2\ 020 \times 28\ 848\ 428 \quad \bullet 2\ 020 + 28\ 848\ 428$$

- 57** **a)** Vérifier que la décomposition en produit de facteurs premiers du nombre entier 4 563 676 729 est $251 \times 257 \times 263 \times 269$.

- b)** Le *prime gap* de deux nombres premiers consécutifs est leur différence positive.

En déduire quatre nombres premiers consécutifs ayant le même *prime gap*.

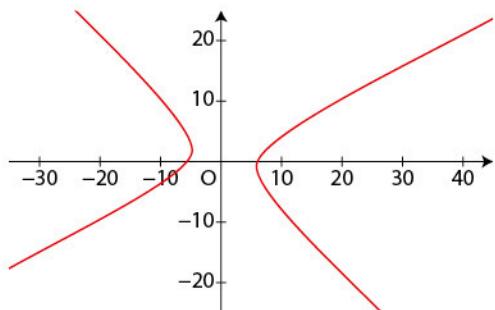
- c)** Justifier qu'il n'existe pas de *prime gap* égal à 5.

- 58** **a)** Décomposer 255 en produit de facteurs premiers.

- b)** Dans chaque cas, déterminer le ou les nombres entiers naturels solutions de l'équation :

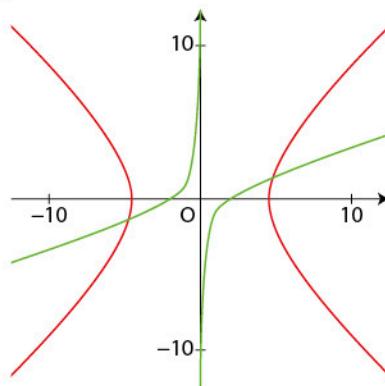
$$\bullet (n+1)(n+3) = 255 \\ \bullet 3n^2 + 6n - 105 = 255$$

- 59** La courbe tracée dans le repère ci-dessous a pour équation $(x+y-1)(2x-4y+1) = 65$.



Déterminer les points à coordonnées entières de cette courbe.

- 60** Dans le repère ci-dessous, la courbe rouge a pour équation $x^2 - y^2 = 21$ et la courbe verte a pour équation $x(2x - 6y) = 8$.



- a)** Déterminer les points à coordonnées entières appartenant à :

• la courbe rouge ; • la courbe verte.

- b)** Les points d'intersection de ces courbes sont-ils à coordonnées entières ?

61 1. a et b désignent deux nombres entiers naturels ($a \geq 2, b \geq 2$) dont les décompositions en produits de facteurs premiers sont :

$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$, où les exposants sont des nombres entiers naturels éventuellement nuls.

a) Déterminer l'écriture de tout diviseur commun à a et b .

b) En déduire que $\text{PGCD}(a; b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}$, où γ_i est le plus petit des deux nombres entiers α_i et β_i .

2. Calculer le PGCD de $2^3 \times 3^7 \times 5^2 \times 11 \times 13^5$ et $4 \times 9 \times 11 \times 13^6$.

62 a) Pour tout entier naturel $n \geq 3$,

$$S_n = 1 + 2 + 3 + \dots + n.$$

Montrer que S_n n'est pas premier.

b) Le nombre 101 est-il premier ?

c) Sachant que $2021 = 43 \times 47$, en déduire, sans calculatrice, la décomposition en produit de facteurs premiers de :

$$1 + 2 + 3 + \dots + 2020.$$

63 1. a) Vérifier que $M_{13} = 2^{13} - 1$ est premier.

b) En déduire que $2^{12}M_{13}$ est parfait.

2. Démontrer la propriété d'Euclide :

Pour tout entier naturel $n \geq 1$, si $M_n = 2^n - 1$ est premier, alors $N = 2^{n-1}M_n$ est parfait.

Dire qu'un nombre entier naturel n est parfait signifie que la somme de ses diviseurs stricts est égale à n .

64 1. a) Décomposer 6 776 en produit de facteurs premiers.

b) En utilisant éventuellement un arbre, déterminer le nombre de diviseurs positifs de 6 776.

2. a) Un nombre entier naturel $N \geq 2$ a pour décomposition en produit de facteurs premiers :

$$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_n^{\alpha_n}.$$

Expliquer pourquoi le nombre de diviseurs positifs de N est :

$$(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_n).$$

b) Déterminer le nombre de diviseurs positifs de 3 600.

c) Trouver un nombre entier naturel de la forme 121×15^n ($n \in \mathbb{N}^*$) ayant 75 diviseurs positifs.

65 α et β sont deux nombres entiers naturels non nuls tels que $n = 2^\alpha 3^\beta$.

Le nombre de diviseurs positifs de n^2 est le triple de celui de n .

a) Prouver que $(\alpha - 1)(\beta - 1) = 3$.

b) Quelles sont les valeurs possibles de n ?

Petit théorème de Fermat

Cours 3

Questions Flash

À l'oral

66 Pierre affirme « $12^{16} \equiv 1 [17]$ ».

A-t-il raison ? Justifier oralement.

67 p désigne un nombre premier, $p \neq 2$.

Camille affirme : « Il existe un nombre entier naturel k tel que $2^k \equiv 1 [p]$. » A-t-elle raison ?

68 Donner mentalement le reste de la division euclidienne de 17^6 par 7.

69 On admet que 2 017 est premier.

Déterminer mentalement le reste de la division de 2020^{2017} par 2 017.

70 Lukas affirme : « Pour tout entier naturel n , $3^{17+n} - 3^{n+1}$ est divisible par 17. » A-t-il raison ?

71 Dans chaque cas, déterminer le reste de la division de a par b .

a) $a = 3^{31}$, $b = 7$

b) $a = 2^{35}$, $b = 7$

c) $a = 128^{129}$, $b = 17$

d) $a = 55^{28}$, $b = 23$

72 Déterminer l'entier naturel k , $0 \leq k \leq 6$ tel que : $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv k [7]$.

73 Justifier que 17 divise $11^{104} + 1$.

74 a) Pour chacun des nombres, calculer le reste de la division par 13.

5^{206}

5^{381}

5^{883}

b) Le nombre $5^{206} + 5^{381} + 5^{883}$ est-il divisible par 13 ?

75 Démontrer que pour tout entier naturel n , 13 divise $11^{12n+6} + 1$.

76 p désigne un nombre premier.

Démontrer que pour tout entier naturel n , $3^{n+p} - 3^{n+1}$ est divisible par p .

77 (a_n) est la suite d'entiers définie par $a_1 = 4$ et pour tout entier naturel $n \geq 1$, $a_{n+1} = 4^{a_n}$.

a) Démontrer que pour tout entier naturel n , $a_{n+1} \equiv 4 [6]$.

b) En déduire que pour tout entier naturel $n \geq 1$, $a_n \equiv 4 [7]$.

78 p désigne un nombre premier et a un nombre entier naturel non nul, non divisible par p .

a) Démontrer qu'il existe un entier naturel b , $1 \leq b \leq p-1$ tel que $ab \equiv 1 [p]$.

b) Quel est le reste de la division euclidienne de a^{p-2} par p ?

c) Appliquer le résultat précédent avec $a = 17$ et $p = 101$.

79 p désigne un nombre premier ($p \neq 2$) et a un nombre entier naturel non nul, non divisible par p .

1. Démontrer que si r et s sont deux entiers naturels tels que $r \equiv s [p-1]$, alors $a^r \equiv a^s [p]$.

2. a) Déterminer, à l'aide du petit théorème de Fermat, l'entier naturel n ($0 \leq n \leq 10$) tel que $2^{402} \equiv n [11]$.

b) Retrouver le résultat précédent à l'aide de 1.

80 Déterminer les nombres entiers naturels x tels que :

$$\bullet x^{103} \equiv 4 [11] \quad \bullet x^{86} \equiv 6 [29]$$

81 a) Décomposer 561 en produit de facteurs premiers.

b) Démontrer que si a est un nombre entier naturel premier avec 561 alors :

$$\bullet a^{560} \equiv 1 [3] \quad \bullet a^{560} \equiv 1 [11] \quad \bullet a^{560} \equiv 1 [17]$$

c) En déduire que pour tout entier naturel a premier avec 561, $a^{560} \equiv 1 [561]$.

Un nombre de Carmichael est un nombre non premier (composé) n ($n > 1$) tel que pour tout entier naturel a premier avec n , $a^{n-1} \equiv 1 [n]$.

561 est un nombre de Carmichael. Ces nombres sont aussi appelés « menteurs de Fermat ».

82 Algo python

Voici une fonction **Carmichael** de paramètre n écrite en langage Python.

```

1 from sympy import *
2
3 def Carmichael(n):
4     c=0
5     d=0
6     for a in range(1,n):
7         if gcd(a,n)==1:
8             c=c+1
9         p=1
10        for k in range(1,n):
11            p=(p*a)%n
12            if p == 1 :
13                d=d+1
14    return c==d

```

a) Interpréter le résultat de la console suivant.

```
>>> Carmichael(1105)
True
```

b) Démontrer le résultat précédent.

83 On donne $n=pq$ avec p et q des nombres premiers tels que $p \neq 2$, $q \neq 2$ et $p \neq q$.

a est un nombre entier naturel qui n'est ni divisible par p ni par q .

a) Justifier que :

$$(a^{p-1})^{\frac{q-1}{2}} \equiv 1 [p] \text{ et } (a^{q-1})^{\frac{p-1}{2}} \equiv 1 [q].$$

b) En déduire que $a^{\frac{(p-1)(q-1)}{2}} \equiv 1 [pq]$.

2. Démontrer que $a^{(p-1)(q-1)} \equiv 1 [pq]$.

84 a est un nombre entier naturel non divisible par 7.

1. Justifier que $a^6 \equiv 1 [7]$.

2. L'ordre de a modulo 7 est le plus petit entier naturel non nul k tel que $a^k \equiv 1 [7]$.

a) Montrer que le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1 [7]$.

b) En déduire que k divise 6, et donner les valeurs possibles de k .

3. Donner l'ordre modulo 7 de tous les entiers a compris entre 2 et 6.

4. On pose $A_n = 2^n + 3^n + 4^n + 5^n + 6^n$ pour $n \in \mathbb{N}$.

Montrer que $A_{2020} \equiv 6 [7]$.

85 a désigne un nombre entier naturel, c et g sont des nombres entiers naturels vérifiant :

$$25g - 108c = 1.$$

1. a) Démontrer que si a n'est pas un multiple de 7, alors

$$a^{108} \equiv 1 [7].$$

En déduire que $(a^{25})^9 \equiv a [7]$.

b) A-t-on le même résultat si a est un multiple de 7 ?

c) On admet que $(a^{25})^9 \equiv a [19]$

Démontrer que $(a^{25})^9 \equiv a [133]$.

2. On note A l'ensemble des nombres entiers naturels a tels que $1 \leq a \leq 26$.

Un message, constitué d'entiers appartenant à A , est codé puis décodé.

La phase de codage consiste à associer à chaque entier de A , l'entier r tel que :

$$a^{25} \equiv r [133] \text{ avec } 0 \leq r < 133.$$

La phase de décodage consiste à associer à r , l'entier r_1 tel que :

$$r^{13} \equiv r_1 [133] \text{ avec } 0 \leq r_1 < 133.$$

a) Justifier que $r_1 \equiv a [133]$.

b) Un message codé conduit à la suite des deux entiers suivants : 128 et 59.

Décoder ce message.

86 QCM Dans chaque cas, donner la réponse exacte sans justifier.

		A	B	C	D
1	Pour savoir si 137 597 est un nombre premier, il suffit de le diviser par les nombres premiers inférieurs à ...	353	370	379	137 597
2	La décomposition en produit de facteurs premiers de 15 750 est ...	$6 \times 5 \times 42$	$2 \times 3 \times 7^2 \times 210$	$2^2 \times 3 \times 5^3 \times 7$	$2 \times 3^2 \times 5^3 \times 7$
3	n désigne un nombre entier naturel et $a = n^2 + 9n + 14$. Alors ...	a n'est jamais premier	a est toujours premier	a est premier pour certaines valeurs de n	a est premier pour une infinité de valeurs de n
4	Le reste de la division euclidienne de 21^{36} par 37 est ...	21	1	16	0
5	Pour tout entier naturel n , le nombre $n^{17} - n$ est divisible par ...	7	11	17	23

87 QCM Dans chaque cas, donner la ou les réponses exactes sans justifier.

		A	B	C	D
1	$a = 2^3 \times 3 \times 5^2 \times 7^4$ et $b = 2^2 \times 3^3 \times 5 \times 11$. Alors PGCD($a ; b$) est égal à ...	$2^3 \times 3^3 \times 5^2$	$2^2 \times 3 \times 5$	5 400	60
2	p est un nombre premier et $S_n = 1^n + 2^n + \dots + (p-1)^n$ ($n \in \mathbb{N}$). Alors p divise ...	S_p	$(p-1)!$	S_{p-1}	$S_{p-1} + 1$
3	n est un nombre entier naturel non divisible par 3 et par 5. Alors $n^{60} - 1$ est divisible par ...	3	15	61	5
4	Modulo 19, le nombre 2020^{19} est congru à ...	2 020	6	1	18

88 Vrai/Faux Dans chaque cas, dire si l'affirmation est vraie ou fausse en justifiant.

- Affirmation :** le nombre 94 799 est premier.
- Affirmation :** la décomposition de 2 045 en produit de facteurs premiers est 5×409 .
- Affirmation :** pour tout entier naturel n , $n^5 - n$ est divisible par 30.
- Affirmation :** il existe un nombre premier p tel que p divise $2^p + 5$.
- Affirmation :** s'il existe un nombre premier p qui divise $a - b$, alors p divise $a^p - b^p$.

Vérifiez vos réponses : p. 293

89 Démontrer l'existence de trois diviseurs premiers

n désigne un nombre entier naturel pair, $n \geq 6$.

On se propose de démontrer la propriété suivante :

Le nombre $2^n - 1$ admet dans sa décomposition en produit de facteurs premiers au moins trois nombres premiers, deux au moins étant distincts.

Rédiger la démonstration en suivant le guide ci-dessous.

(1) Exploiter la parité de n :

n est pair donc il existe un entier naturel $k \geq 3$ tel que $n = \dots$

(2) Factoriser $2^n - 1$: on peut donc écrire $2^n - 1 = (2^{\dots} - 1)(2^{\dots} + \dots)$.

(3) Tirer des conséquences : les deux facteurs ne peuvent pas avoir de diviseurs premiers communs car

Donc, n étant supérieur ou égal à 6, il y a au moins deux diviseurs premiers distincts divisant $2^n - 1$, l'un divisant ... et l'autre divisant

(4) Exploiter des nombres entiers consécutifs : parmi les trois nombres $2^k - 1, 2^k, 2^k + 1$, l'un est divisible par 3, et cela ne peut être que ... ou

(5) Conclure : $k \geq 6$, donc $2^k - 1 \geq \dots$ et $2^k + 1 \geq \dots$

Si 3 divise $2^k - 1$, alors $2^k - 1$ admet au moins ... diviseurs premiers.

De même, si 3 divise $2^k + 1$, alors $2^k + 1$ admet au moins

Ainsi,

90 Résoudre une équation

x désigne un nombre entier relatif.

(E) est l'équation $x^{21} \equiv 6 [7]$.

a) Montrer que l'équation (E) est équivalente à l'équation $x^3 \equiv 6 [7]$.

b) Recopier et compléter le tableau ci-dessous.

x	0	1	2	3	4	5	6
$x^3 \equiv \dots [7]$	0						

c) En déduire les solutions de l'équation (E).

91 Déterminer un diviseur premier

p désigne un nombre premier et a, b désignent deux nombres entiers naturels.

a) Montrer que si p divise $a+b$, alors p divise $a^p + b^p$.

b) En déduire un diviseur premier de $5^{11} + 6^{11}$.

Vérifier ce résultat.

c) Déterminer une valeur de p telle que p divise $5^p + 7^p$.

92 Déterminer un nombre entier n

Un nombre entier naturel n a 5 diviseurs et $n - 16$ est le produit de deux nombres premiers.

a) Prouver qu'il existe un nombre premier p tel que $n = p^4$.

b) Écrire $n - 16$ comme un produit de trois facteurs dépendant de p .

c) En déduire la valeur de n .



JAI
COMPRIS.COM

Toutes les démonstrations
au programme en vidéo

Liste des démonstrations :

- L'ensemble des nombres premiers est infini.

Conseil

Ce sont trois entiers consécutifs donc l'un d'entre eux est divisible par 3.

Conseil

On utilise la conséquence du petit théorème de Fermat ainsi que la compatibilité des congruences avec les opérations.

Conseil

On applique la conséquence du petit théorème de Fermat.

Conseil

Lorsqu'on a la décomposition en produit de facteurs premiers, on connaît le nombre de diviseurs.

UTILISER DES NOMBRES PREMIERS

93 On se propose de déterminer les nombres premiers p tels que $4p^2 + 1$ et $6p^2 + 1$ soient aussi des nombres premiers.

1. a) Vérifier que $p \neq 2$ et $p \neq 3$.

b) Justifier que $p = 5$ est l'un de ces nombres.

2. On suppose maintenant que $p > 5$.

a) Justifier que $4p^2 + 1 \equiv -(p^2 - 1) \pmod{5}$ et que :

$$6p^2 + 1 \equiv (p+2)(p+3) \pmod{5}.$$

b) En déduire que $p(4p^2 + 1)(6p^2 + 1) \equiv 0 \pmod{5}$.

c) Prouver que $4p^2 + 1$ ou $6p^2 + 1$ est composé.

d) Conclure.

94 n désigne nombre entier naturel tel que $10 \leq n \leq 120$.

a) Décomposer 210 en facteurs premiers.

b) Montrer que si n est premier, alors il existe un entier naturel a non nul tel que $an \equiv 1 \pmod{210}$.

c) Montrer que s'il existe un entier naturel non nul a tel que $an \equiv 1 \pmod{210}$, alors n est premier.

d) Déterminer n pour : • $a = 13$ • $a = 319$

95 Algo python

p désigne un entier naturel, $p \geq 2$. On se propose de démontrer que si $(p-1)! \equiv -1 \pmod{p}$, alors p est premier.

1. a) Montrer que $(p-1)! \equiv -1 \pmod{p}$ si, et seulement si, il existe un entier relatif k tel que $kp - (p-1)! = 1$.

b) En déduire, si cette condition est vérifiée, que p est premier avec tous les nombres premiers strictement inférieurs à p .

c) Conclure.

2. Voici une fonction **Wilson** de paramètre n écrite en langage Python.

```
1 def Wilson(p):
2     r=1
3     for k in range(1,p):
4         r=(r*k)%p
5         if r==p-1:
6             d=1
7         else:
8             d=0
9     return d
```

a) Expliquer le rôle de la boucle des lignes 3 et 4.

b) Interpréter le résultat qu'elle renvoie.

Ce résultat, appelé théorème de Wilson, est en réalité une équivalence. Il peut servir de test de primalité.

96 Algo python

L'indicatrice d'Euler est la fonction, notée φ , qui à un nombre entier naturel non nul n , associe le nombre d'entiers naturels inférieurs à n , qui sont premiers avec n . On se propose d'étudier des propriétés de la fonction φ .

1. Le programme ci-dessous, écrit en langage Python, définit une fonction **Phi** de paramètre n .

```
1 from sympy import *
2
3 def Phi(n):
4     e=0
5     for i in range(1,n+1):
6         if gcd(i,n)==1:
7             e=e+1
8     return e
```

a) Quel résultat la fonction **Phi** renvoie-t-elle pour :

- $n = 4$
- $n = 5$
- $n = 7$
- $n = 8$?

b) Saisir ce programme et le tester.

2. On se propose de trouver une formule permettant de déterminer $\varphi(n)$ pour $n \in \mathbb{N}, n \geq 1$.

a) Démontrer que n est un nombre premier si, et seulement si, $\varphi(n) = n - 1$.

b) On admet que : « $\varphi(pq) = (p-1)(q-1)$, avec p et q nombres premiers distincts. »

Vérifier ce résultat avec $p = 5$ et $q = 7$.

c) On admet que : « $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ avec p nombre premier et α entier naturel, $\alpha \geq 1$ ».

Vérifier ce résultat avec $p = 5$ et $\alpha = 2$.

d) Darius affirme « Si u et v désignent des nombres entiers naturels non nuls, alors $\varphi(uv) = \varphi(u) \times \varphi(v)$. »

Tester la conjecture de Darius avec :

- | | |
|----------------------|----------------------|
| • $u = 4$ et $v = 6$ | • $u = 4$ et $v = 9$ |
|----------------------|----------------------|

Quelle hypothèse portant sur u et v faudrait-il ajouter pour que la formule fonctionne ?

On admettra ce résultat.

e) La décomposition en produit de facteurs premiers de $n = 9500$ est $n = 2^2 \times 5^3 \times 19$.

Calculer $\varphi(9500)$. Vérifier le résultat avec la fonction **Phi**.

HISTOIRE DES MATHS

Leonhard Euler a introduit et étudié cette fonction vers 1750.

En 1784, il utilise la lettre π pour la désigner. Puis, en 1801, **Carl Friedrich Gauss** la note Φ dans ses *Disquisitiones Arithmeticae*.

De nos jours, on note φ cette fonction.

n	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	2	2	4	2	6	4	6	4

DÉCOMPOSER EN PRODUIT DE FACTEURS PREMIERS

97 On veut décomposer en produit de facteurs premiers le nombre entier naturel :

$$a = 12\,345\,678\,987\,654\,321.$$

1. a) Calculer 1001001×111 .

b) Décomposer $1\,001\,001$ en produit de facteurs premiers sachant que $333\,667$ est un nombre premier.

2. Calculer 11^2 , 111^2 et 1111^2 .

3. Donner la décomposition en produit de facteurs premiers de a .

98 n désigne un nombre entier naturel non nul et p un nombre premier supérieur ou égal à 3.

On donne $a = 2^n$, $b = ap$ et on note $S(q)$ la somme des diviseurs positifs de l'entier q ($q \geq 1$).

1. a) Déterminer l'ensemble des diviseurs positifs de a et l'ensemble des diviseurs positifs de b .

b) Démontrer l'égalité $S(a) + 2^{n+1} = 1 + 2S(b)$.

En déduire $S(a)$ en fonction de n .

c) Exprimer $S(b)$ en fonction de $S(a)$. Calculer $S(b)$.

2. a) On suppose que $S(b) = 2b$.

Déterminer p en fonction de n .

b) Pour $1 \leq n \leq 9$, déterminer alors les nombres premiers p et les valeurs correspondantes de b .

99 p est un nombre premier supérieur à 2.

1. Donner la liste des diviseurs positifs de p^4 .

2. S désigne la somme de ces diviseurs positifs.

Vérifier que $(2p^2 + p)^2 < 4S < (2p^2 + p + 2)^2$.

3. a) On suppose que S est un carré parfait : $S = n^2$ ($n \in \mathbb{N}$).

Démontrer que $n = p^2 + \frac{p+1}{2}$.

b) Existe-t-il des valeurs de p telles que S soit un carré parfait ?

100 La décomposition en produit de facteurs premiers d'un entier naturel $N \geq 2$ s'écrit $p_1^\alpha p_2^\beta p_3^\gamma$.

Si on multiplie N par p_1^3 , le nombre de ses diviseurs augmente de 18.

Si on multiplie N par p_2 , le nombre de ses diviseurs augmente de 8.

Si on multiplie N par p_3 , le nombre de ses diviseurs augmente de 12.

a) Déterminer α , β et γ .

b) Trouver N sachant que $p_1 + p_2 = p_3$ et $p_1 + p_2 + p_3 = 14$. Donner toutes les solutions.

101 Algo python

n désigne un nombre entier naturel impair.

La méthode de Fermat pour décomposer n , consiste à chercher des nombres entiers naturels a et b tels que $n = a^2 - b^2$, c'est-à-dire $n = (a - b)(a + b)$.

1. Démontrer que $n = xy$ avec x, y entiers naturels tels que $x > y$ si, et seulement si, n s'écrit comme différence de deux carrés.

2. Pour tout entier naturel k non nul, on pose $a_k = q + k$ où $q = E(\sqrt{n})$ désigne la partie entière de \sqrt{n} .

a) Vérifier que $a_{k+1}^2 - n = (a_k + 1)^2 - n$, puis que $a_{k+1}^2 - n = a_k^2 - n + 2a_k + 1$.

b) Montrer que si $a_k^2 - n$ est un carré, alors on peut décomposer n .

c) Recopier et compléter le tableau ci-dessous pour obtenir une décomposition de $n = 407$.

k	a_k	$2a_k + 1$	$a_k^2 - n$
1	21	43	34
2	22
⋮	⋮	⋮	⋮

3. Voici une fonction **Dfermat** de paramètre n qui permet de donner une décomposition de n sous la forme $n = xy$ avec x, y entiers naturels.

```
1 from math import *
2
3 def Dfermat(n):
4     q=floor(sqrt(n))
5     if q*q==n :
6         L=[q,q]
7     else:
8         a=q+1
9         d=2*a+1
10        b2=a**2-n
11        while floor(sqrt(b2))**2 != b2:
12            b2 = d + b2
13            a = a + 1
14            d = d + 2
15        b = sqrt(b2)
16        L= [a+b,a-b]
17    return L
```

a) Expliquer le test effectué ligne 5 ?

b) Expliquer la condition de la ligne 11.

c) Saisir et tester ce programme avec le nombre choisi par Fermat : $n = 2\,027\,651\,281$.

Obtient-on la décomposition en produit de facteurs premiers de n ? Si oui, qu'est-ce qui permet de l'affirmer ?

d) Déterminer la décomposition de chacun des nombres suivants :

$$\bullet 1\,233\,635$$

$$\bullet 2^{30} - 1$$

Remarque : le programme peut être en défaut pour des valeurs très grandes de n .

102 a et b désignent deux nombres entiers naturels supérieurs ou égaux à 2.

On se propose de démontrer qu'il n'existe aucun nombre premier p tel que $a^2 = pb^2$.

On raisonne par l'absurde et on suppose que p est un nombre premier tel que $a^2 = pb^2$.

a) Montrer que l'on peut supposer que a et b sont premiers entre eux.

b) Expliquer pourquoi cela est impossible en envisageant les deux cas :

- p est un facteur de la décomposition de a en produit de facteurs premiers ;
- p n'est pas un facteur de la décomposition de a en produit de facteurs premiers.

c) Conclure.

103 x désigne un nombre rationnel.

On note (1) l'équation d'inconnue un rationnel x :

$$78x^3 + ux^2 + vx - 14 = 0$$

où u et v sont des nombres entiers relatifs.

On se propose de déterminer le nombre de rationnels, non entiers, positifs solutions de cette équation.

1. On suppose dans cette question que $\frac{14}{39}$ est solution de l'équation (1).

a) Démontrer que les nombres entiers relatifs u et v sont liés par la relation $14u + 39v = 1129$.

b) Trouver un couple $(x; y)$ de nombres entiers relatifs vérifiant l'équation $14x + 39y = 1$.

c) En déduire un couple $(u_0; v_0)$ de nombres entiers relatifs, solution particulière de l'équation $14u + 39v = 1129$. Donner la solution générale de cette équation.

d) Déterminer, parmi les couples $(u; v)$ précédents, celui pour lequel le nombre u est le nombre entier naturel le plus petit possible.

2. a) Décomposer 78 et 14 en produit de facteurs premiers. En déduire, dans \mathbb{N} , l'ensemble des diviseurs de 78 et l'ensemble des diviseurs de 14.

b) $x = \frac{p}{q}$ ($p \in \mathbb{N}, q \in \mathbb{N}^*$) est une solution de l'équation (1).

Montrer que si p et q sont des nombres premiers entre eux, alors p divise 14 et q divise 78.

c) En déduire le nombre de rationnels, non entiers, positifs, pouvant être solutions de l'équation (1).

HISTOIRE DES MATHS

Gotthold Eisenstein (1823-1852) est un mathématicien allemand. Il s'est intéressé à la résolution dans \mathbb{N} des polynômes à coefficients entiers.

104 p et q désignent des nombres premiers distincts supérieurs ou égaux à 3.

α et β désignent des nombres entiers naturels non nuls. On note $n = p^\alpha q^\beta$.

a) Déterminer les diviseurs positifs de p^α et q^β .

b) Démontrer que la somme des diviseurs positifs de n est donnée par :

$$S = \frac{p^{\alpha+1}-1}{p-1} \times \frac{q^{\beta+1}-1}{q-1}.$$

2. Dire que n est parfait signifie que la somme de ses diviseurs est égale à $2n$.

a) Vérifier que :

$$2n(p-1)(q-1) - p^{\alpha+1}q^{\beta+1} = p^\alpha q^\beta [(p-2)(q-2) - 2].$$

b) Démontrer que n est parfait si, et seulement si, $p^\alpha q^\beta [(p-2)(q-2) - 2] = 1 - p^{\alpha+1} - q^{\beta+1}$

c) En étudiant le signe de chaque membre, démontrer qu'il ne peut exister de nombres parfaits impairs dont la décomposition en produit de facteurs premiers ne contienne que deux facteurs premiers distincts.

3. Démontrer que s'il existe un nombre parfait impair, alors il est supérieur à 105.

On ne sait pas à l'heure actuelle s'il existe des nombres parfaits impairs.

Actuellement, 40 nombres parfaits sont connus ; le plus grand est $2^{20\,996\,010}(2^{20\,996\,011} - 1)$.

105 n désigne un nombre entier naturel non nul.

a et b désignent deux nombres entiers naturels supérieurs ou égaux à 2 dont les décompositions en produits de facteurs premiers sont :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \text{ et } b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$$

où p_1, p_2, \dots, p_n sont des nombres premiers distincts et $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n$ des nombres entiers naturels (éventuellement nuls).

On se propose d'étudier certaines propriétés déduites de ces décompositions.

1. a) En utilisant l'unicité de la décomposition en produit de facteurs premiers, démontrer que les décompositions de a et a^2 ont les mêmes facteurs premiers.

b) Démontrer que si un nombre premier p divise a^2 , alors p divise a et p^2 divise a^2 .

2. a) Démontrer que si a^2 divise b^2 , alors a divise b .

b) Démontrer que si a^3 divise b^2 , alors a divise b .

c) Si a^2 divise b^3 , peut-on conclure que a divise b ?

3. m désigne un nombre entier naturel non nul.

a) Démontrer que :

$$\text{PGCD}(a^m; b^m) = [\text{PGCD}(a; b)]^m.$$

b) Déterminer $\text{PGCD}(3\,375; 1\,728)$ en utilisant $m = 3$.

UTILISER LE PETIT THÉORÈME DE FERMAT

106 On se propose de coder le nom « FERMAT » de la façon suivante :

- à chaque entier x compris entre 0 et 30, on lui associe une lettre de l'alphabet français ou un symbole ($A : 0$, $B : 1, \dots, Z : 25$, $\alpha : 26$, $\beta : 27$, $\gamma : 28$, $\delta : 29$, $\varepsilon : 30$) ;
- on calcule le reste y de la division euclidienne de x^7 par 31 ;
- on fait correspondre à y l'un des symboles précédents.

Exemple

La première lettre F est associée à 5.

Ainsi $5^7 \equiv 5 [31]$ donc $y = 5$ et F est codée F.

1. Coder le mot FERMAT.

2. Montrer que 7 et 30 sont premiers entre eux et écrire l'égalité de Bézout correspondante.

3. Démontrer que deux lettres distinctes sont codées par deux lettres distinctes.

4. a) Démontrer que $y \equiv x^7 [31]$ équivaut à $x \equiv y^{13} [31]$.

b) Décoder le mot XCQMMQ.

107 p désigne un nombre premier.

Dire que -1 est un résidu quadratique modulo p signifie qu'il existe un nombre entier x tel que $x^2 \equiv -1 [p]$.

1. Montrer que -1 est un résidu quadratique modulo 2.

2. On suppose que $p \equiv 3 [4]$ et qu'il existe un entier x tel que $x^2 \equiv -1 [p]$.

a) En remarquant que $x^{p-1} = (x^2)^{\frac{p-1}{2}}$, montrer que :

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} [p].$$

b) Quelle est la parité de $\frac{p-1}{2}$?

En utilisant le petit théorème de Fermat, montrer que :

$$1 \equiv -1 [p].$$

c) En déduire que $p = 2$ et conclure.

3. On suppose que $p \equiv 1 [4]$ et on admet le théorème de Wilson : si p est premier alors $(p-1)! \equiv -1 [p]$.

a) Vérifier que :

$$\left(p - \frac{p-1}{2}\right) \times \dots \times (p-1) \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! [p]$$

b) En écrivant

$$(p-1)! = 1 \times 2 \times \dots \times \frac{p-1}{2} \times \left(p - \frac{p-1}{2}\right) \times \dots \times (p-1)$$

montrer que $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 [p]$,

puis que $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 [p]$.

c) Que peut-on conclure ?

3. -1 est-il un résidu quadratique modulo 157 ?

108 **1.** On considère l'ensemble $A_7 = \{1; 2; 3; 4; 5; 6\}$.

a) Pour tout élément a de A_7 , écrire dans le tableau ci-dessous l'unique élément y de A_7 tel que $ay \equiv 1 [7]$.

a	1	2	3	4	5	6
y						6

b) Pour tout entier relatif x , démontrer que :

$$3x \equiv 1 [7] \text{ équivaut à } x \equiv 5 [7].$$

c) Si a est un élément de A_7 , montrer que les seuls entiers relatifs x solutions de l'équation $ax \equiv 0 [7]$ sont les multiples de 7.

2. p désigne un nombre premier supérieur ou égal à 3.

On note $A_p = \{1; 2; \dots; p-1\}$.

On considère un élément a de A_p .

a) Justifier que a^{p-2} est une solution de $ax \equiv 1 [p]$.

b) On note r le reste de la division euclidienne de a^{p-2} par p . Démontrer que r est l'unique solution x dans A_p de l'équation $ax \equiv 1 [p]$.

c) x et y désignent deux nombres entiers relatifs.

Démontrer que $xy \equiv 0 [p]$ si, et seulement si, x est un multiple de p ou y est un multiple de p .

d) Application : $p = 31$

Résoudre dans A_{31} chacune des équations :

$$2x \equiv 1 [31] \text{ et } 3x \equiv 1 [31].$$

À l'aide des résultats précédents, résoudre dans \mathbb{Z} , l'équation $6x^2 - 5x + 1 \equiv 0 [31]$.

S'ENTRAÎNER À LA LOGIQUE → p. 290

109 Quantificateurs universel, existentiel

(a_n) est la suite définie sur \mathbb{N} par $a_n = 4^n - 1$.

Les affirmations ci-dessous sont-elles vraies ou fausses ? Justifier à l'aide d'une démonstration ou d'un contre-exemple.

a) Pour tout n de \mathbb{N} , a_n est un multiple de 3.

b) Pour tout n de \mathbb{N} , a_n est un multiple de 4.

c) Il existe n dans \mathbb{N} tel que a_n est divisible par 5.

d) Pour tout nombre premier $p \geq 3$, il existe n de \mathbb{N}^* tel que a_n soit un multiple de p .

110 Condition nécessaire et suffisante

a et b sont deux entiers naturels tels que $a > b$.

P est la proposition :

« Si a et b sont consécutifs et $a+b$ premier, alors $a^2 - b^2$ est premier. »

a) P est-elle vraie ?

b) Énoncer la réciproque de P. Est-elle vraie ?

111 Résoudre une équation du second degré**Raisonner** **Calculer**On considère l'équation d'inconnue n dans \mathbb{N} :

$$(E) : n^2 - Sn + 11994 = 0$$

où S est un nombre entier naturel.On s'intéresse aux valeurs de S telles que (E) admette deux solutions dans \mathbb{N} .**a)** Peut-on déterminer un entier naturel S tel que 3 soit solution de (E) ?

Si oui, préciser la seconde solution.

b) Peut-on déterminer un entier naturel S tel que 5 soit solution de (E) ?**c)** Montrer que tout entier naturel n solution de (E) est un diviseur de 11 994.**d)** En déduire toutes les valeurs possibles de S telles que (E) admette deux solutions dans \mathbb{N} .**112** Réfuter une conjecture**Chercher** **Raisonner** **Calculer**

En 1789, Euler conjecture la propriété :

« Si la somme de n puissances k -ièmes de nombres entiers naturels non nuls est une puissance k -ième d'un entier, alors $n \geq k$ ».En 1966, L.J. Lander et T.R. Parkin ont trouvé un contre-exemple pour $k = 5$.On cherche un nombre entier naturel a tel que :

$$27^5 + 84^5 + 110^5 + 133^5 = a^5.$$

a) Démontrer que $a \equiv 4 [5]$.**b)** Démontrer que a est divisible par 3.**c)** Justifier que $a > 133$.**d)** Déterminer la valeur de a .**113** Trouver des diviseurs d'un nombre**Raisonner** **Calculer** p désigne un nombre premier supérieur ou égal à 7.On pose $n = p^4 - 1$.**a)** Montrer que p est congru à -1 ou 1 modulo 3.En déduire que n est divisible par 3.**b)** En remarquant que p est impair, prouver qu'il existe un entier naturel $k \geq 3$ tel que $p^2 - 1 = 4k(k+1)$.En déduire que n est divisible par 16.**c)** Démontrer que 5 divise n .**d)** Décomposer 240 en produit de facteurs premiers.En déduire que 240 divise n .**e)** Existe-t-il quinze nombres premiers p_1, p_2, \dots, p_{15} supérieurs ou égaux à 7 tels que l'entier :

$$A = p_1^4 + p_2^4 + \dots + p_{15}^4$$

soit un nombre premier ?

114 Prendre des initiatives**Chercher** **Raisonner** **Calculer** n est un entier naturel, $n \geq 2$, de décomposition $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ où p_1, p_2, \dots, p_k sont des nombres premiers distincts et $\alpha_1, \alpha_2, \dots, \alpha_k$ sont des nombres entiers naturels non nuls. f est la fonction définie sur \mathbb{N}^* telle que $f(1) = 1$ et $f(n) = \alpha_1^{p_1} \alpha_2^{p_2} \dots \alpha_k^{p_k}$.**a)** Calculer $f(720)$ et $f(2\ 020)$ **b)** Pour tout $n \in \mathbb{N}$ et tout $i \in \mathbb{N}^*$, on pose $f^i(n) = f(n)$ et $f^{i+1}(n) = f(f^i(n))$.Calculer $f^i(36^{36})$ pour tout $i \in \mathbb{N}^*$.**c)** Résoudre chacune des équations :

$$\bullet f(n) = 1 \quad \bullet f(n) = 2 \quad \bullet f(n) = 4$$

115 Étudier des nombres premiers jumeaux**Raisonner** **Communiquer**

Deux nombres premiers sont dits jumeaux si leur différence est égale à 2. Par exemple, 3 et 5 sont deux nombres premiers jumeaux.

1. On note $(p; q)$ un couple de nombres premiers jumeaux avec $q = p + 2$ et $p \geq 5$.**a)** En remarquant que 2 et 3 sont premiers avec p , démontrer que $p = 6k - 1$ et $q = 6k + 1$, où k est un nombre entier naturel non nul.**b)** En déduire que $p \equiv 2 [3]$.**c)** Démontrer que $p + 4$ n'est pas premier.**2.** $(x; y)$ est un couple de nombres entiers naturels supérieurs à 2 tels que $y = x + 2$.Démontrer que $(x; y)$ est un couple de nombres premiers jumeaux si, et seulement si, $x^2 + 2x$ a exactement 4 diviseurs positifs.**116** Énoncer une condition nécessaire**Raisonner** **Calculer** n désigne un nombre entier naturel non nul.Le rep-unit à n chiffres est le nombre $r_n = \underbrace{1\dots 1}_{n \text{ chiffres}}$.**1.** Les nombres r_2, r_3 et r_4 sont-ils premiers ?

$$2. \text{ Démontrer } r_n = \frac{10^n - 1}{9}.$$

3. On pose $s_n = 9r_n$ et $n = pq$ avec p et q nombres entiers strictement supérieurs à 1.**a)** Montrer que $10^n \equiv 1 [s_p]$, puis en déduire que r_p divise r_n .**b)** Énoncer une condition nécessaire pour que r_n soit un nombre premier.

Cette condition est-elle suffisante ?

117 Définir l'ordre d'un entier modulo p **Raisonner** **Calculer**

a et p sont deux nombres entiers naturels, $a \geq 2$, $p \geq 2$ et p premier. On suppose qu'il existe un entier naturel non nul k tel que $a^k \equiv 1 [p]$. On note k_0 le plus petit entier naturel non nul tel que $a^{k_0} \equiv 1 [p]$.

1. Démontrer que k est un multiple de k_0 .

On dit que k_0 est l'ordre de a modulo p .

2. On suppose qu'il existe un nombre premier q qui divise $M_p = 2^p - 1$.

a) Démontrer que p est l'ordre de 2 modulo q .

b) Démontrer, avec le petit théorème de Fermat, qu'il existe un entier naturel k non nul tel que $q = 1 + 2kp$.

3. a) Vérifier que 179 951 est un nombre premier.

b) M_{59} est-il premier ?

118 Résoudre un problème**Chercher** **Raisonner** **Calculer**

Rédiger les différentes étapes de la recherche, sans omettre les fausses pistes et les changements de méthode.

Problème

Déterminer les nombres entiers naturels compris entre 3 000 et 4 000 dont la décomposition est le produit de trois nombres premiers distincts p_1, p_2, p_3 tels que $p_1 < p_2$ et $p_3 = p_2 + p_1$.

119 Use Fermat's little theorem**Calculer** **Communiquer**

Let m be an integer, $m \geq 2$ and $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be its prime factorisation.

Show that, for all $x \in \mathbb{N}$, $f(x) \equiv 0 [m]$, where :

$$f(x) = (x^{p_1} - x)^{\alpha_1} \dots (x^{p_k} - x)^{\alpha_k}.$$

120 Chercher des points**Chercher** **Calculer**

n désigne un nombre entier naturel non nul.

Dans un repère orthonormé $(O; \vec{i}, \vec{j})$, on note H_n la courbe d'équation $xy = n^4 + 4$.

1. Déterminer les points à coordonnées entières appartenant aux courbes H_1 et H_5 .

2. a) Vérifier que pour tout entier naturel n ,

$$(n^2 - 2n + 2)(n^2 + 2n + 2) = n^4 + 4.$$

b) En déduire que pour tout entier naturel $n \geq 2$, $n^4 + 4$ n'est pas premier.

c) Quel est le nombre minimum de points à coordonnées entières appartenant à H_n dans le cas $n \geq 2$. Justifier.

121 Étudier des fonctions arithmétiques**Raisonner** **Calculer**

1. Déterminer deux nombres entiers naturels u et v , $u \leq 226$ tels que :

$$109u - 226v = 1.$$

2. On note A l'ensemble des 227 nombres entiers naturels a tels que $a \leq 226$.

f et g sont les deux fonctions de A dans A définies de la manière suivante :

- à tout entier a de A, f associe le reste de la division euclidienne de a^{109} par 227 ;

- à tout entier a de A, g associe le reste de la division euclidienne de a^{141} par 227.

a) Vérifier que $g[f(0)] = 0$.

b) Justifier que pour tout a de A,

$$a^{226} \equiv 1 [227].$$

c) Montrer que pour tout a de A,

$$g[f(a)] = a.$$

d) A-t-on, pour tout a de A, $f[g(a)] = a$?

122 Imaginer une stratégie**Chercher** **Raisonner**

k désigne un nombre entier naturel.

On considère l'ensemble des nombres entiers naturels de la forme :

$$n = 2310k + 2100.$$

Ambre étudie cet ensemble. Elle constate que :

- si l'on change un quelconque des chiffres de n autre que celui des unités, on obtient un nombre non premier,

- $n+1$ est divisible par 11,

- $n+3$ et $n+9$ sont divisibles par 3,

- $n+5$ est divisible par 5,

- $n+7$ est divisible par 7.

Elle conjecture donc que si l'on change un quelconque des chiffres de n , on n'obtient jamais un nombre premier.

Vérifier l'exactitude des différents points constatés par Ambre, puis démontrer sa conjecture.

123 Établir une propriété**Chercher** **Raisonner**

n désigne un nombre entier naturel, $n \geq 2$.

On note $P(x) = ax^3 + bx$ où a et b sont des nombres entiers relatifs non nuls.

On dit que le couple $(a; b)$ est n -parfait lorsque pour tous entiers naturels m et k :

si $P(m) \equiv P(k) [n]$, alors $m \equiv k [n]$

a) Montrer que le couple $(1; -5^2)$ est 51-parfait.

b) Montrer que si un couple est 2020-parfait, alors il est 101-parfait.

124 Le chiffrement RSA

1. Établir une propriété fondamentale

$n = pq$ est le produit de deux nombres premiers p et q distincts.

On pose $m = (p-1)(q-1)$ et on note c un nombre premier avec m .

On note x un entier naturel.

a) Démontrer qu'il existe des entiers d et k tels que :

$$cd = km + 1 \text{ (c'est-à-dire } cd \equiv 1 [m]).$$

b) Cas où x est non divisible par p

Démontrer que $x^{p-1} \equiv 1 [p]$.

En déduire que $x^{km} \equiv 1 [p]$, puis que $x^{cd} \equiv x [p]$.

c) Cas où x est divisible par p

Démontrer que $x^{cd} \equiv x [p]$.

c) Démontrer de façon analogue que pour tout entier naturel x , $x^{cd} \equiv x [q]$.

d) En déduire que pour tout entier naturel x , $x^{cd} \equiv x [n]$.

HISTOIRE DES MATHS

Les trois lettres RSA sont les initiales de Rivest, Shamir, Adleman qui ont mis au point ce procédé en 1978.

Le système RSA 1 024 bits correspond à un nombre $n = pq$ de l'ordre de $2^{1024} \approx 10^{308}$ s'écrivant avec 309 chiffres.

Principe

- Pour chiffrer un message (cartes bancaires, internet, ...), on choisit deux nombres premiers p et q distincts très grands et on calcule $n = pq$.

On pose $m = (p-1)(q-1)$.

On cherche deux nombres entiers naturels c et d tels que $cd \equiv 1 [m]$.

- Les messages x seront des entiers naturels appartenant à $\{0; 1; \dots; n-1\}$.

Le codage de ce message consiste à calculer $C(x) \equiv x^c [n]$.

Le décodage consiste à calculer $D(y) \equiv y^d [n]$.

On a bien $D(C(x)) \equiv x^{cd} \equiv x [n]$.

- Pour chiffrer un message on a besoin de connaître c et n .

Le couple $(c; n)$ est appelé la **clé publique** car elle est connue de tous et répertoriée dans un annuaire.

- Pour déchiffrer, il faut connaître d et n .

d est appelée la **clé privée** car elle n'est connue que de la personne qui reçoit le message codé.

2. Application 1

Alex veut choisir une clé publique $(n; c)$ et sa clé privée d .

Il prend $p = 5$, $q = 11$ et donc $n = 55$ (p et q sont choisis petits, contrairement à la réalité, pour la simplicité des calculs).

a) Démontrer qu'il peut choisir $c = 3$ et $d = 27$.

b) Les lettres de l'alphabet sont chiffrées par A : 01, B : 02, ..., Z : 26.

Paula, qui connaît la clé publique d'Alex, crypte le message :

« VIVE LA CRYPTOGRAPHIE » et lui envoie.

Quel message crypté Alex reçoit-il ?

Comment le décode-t-il ?

3. Application 2

Lise a pour clé publique $(n; c)$ avec $n = pq$, $p = 3$, $q = 13$.

a) Démontrer qu'elle peut choisir $c = 29$ et $d = 5$.

b) Elle reçoit le message crypté suivant de Félix : 28 01 12 21 11 12 03 28 05.

Décrypter ce message.

125 Des témoins de Fermat

n désigne un nombre entier naturel, $n \geq 2$.

On appelle **témoin de Fermat** (TDF) de la non primalité de n , tout entier naturel a , $2 \leq a \leq n-1$ tel que $a^{n-1} \not\equiv 1 [n]$. Dans le cas contraire, on dit que n passe le test pour a .

- 1. a)** Sachant que $2^{33} \equiv 1 [161]$, déterminer l'entier k ($1 \leq k \leq 160$) tel que $2^{160} \equiv k [161]$.

En déduire que 161 n'est pas premier et donner un TDF pour 161.

- b)** Voici une fonction **Test_Fermat** écrite en langage Python de paramètres a et n . Quel résultat cette fonction renvoie-t-elle ?

- 2.** La fonction **Liste_NP_Pass** a pour paramètres N et a . Expliquer son rôle. Quelle liste renvoie-t-elle ?

- 3. a)** Saisir ce programme.

- b)** Obtenir la liste des entiers naturels inférieurs à 10 000 qui ne sont pas premiers et qui passent le test de Fermat avec $a = 2$.

- c)** Effectuer le même travail avec $a = 3$.

- d)** Si a n'est pas un TDF de n et qui n'est pas premier, on dit que n est un faux témoin de a .

Donner des faux témoins pour $a = 2$ et $a = 3$.

```

1 from sympy import *
2 from builtins import *
3
4 def Test_Fermat(n,a):
5     r=pow(a,n-1,n)
6     if r!=1:
7         b=True
8     else:
9         b=False
10    return b
11
12 def Liste_NP_Pass(N,a):
13     L=[]
14     for k in range(1,N+1):
15         if isprime(k)==False and Test_Fermat(k,a)==False:
16             L.append(k)
17     return L

```

$\text{pow}(a,n-1,n)$ calcule $a^{n-1} [n]$.

126 Des nombres de Carmichael

Un nombre de Carmichael est un nombre non premier n ($n > 1$) tel que pour tout entier naturel a premier avec n , $a^{n-1} \equiv 1 [n]$.

- 1. a)** Décomposer 561 en produit de facteurs premiers.

- b)** Vérifier que 560 est un multiple de 2, 10 et 16.

- 2. a)** a désigne un nombre entier naturel premier avec 561. On pose $b = a^{560} - 1$.

Vérifier que b est divisible par $a^2 - 1$, par $a^{10} - 1$ et par $a^{16} - 1$.

- b)** En déduire que b est divisible par 3, par 11 et par 17.

- c)** Montrer alors que 561 est un nombre de Carmichael.

- 3.** On admet le théorème suivant dû à Alwin Korselt :

n est un nombre non premier ($n > 1$).

n est un nombre de Carmichael si, et seulement si :

- aucun carré de nombre premier ne divise n ;
- pour tout nombre premier p qui divise n , $p-1$ divise $n-1$.

- a)** Démontrer à l'aide de ce théorème que 1 105, 1 729 et 2 465 sont des nombres de Carmichael.

- b)** Écrire en langage Python une fonction qui permet de tester si un entier naturel n ($n \geq 2$) est un nombre de Carmichael.

- c)** Dans chaque cas, déterminer s'il s'agit d'un nombre de Carmichael.

• 9 746 347 772 161

• 5 122 666 777 121

127 Des nombres de Mersenne premiers

p est un nombre premier, $p \geq 3$ et $M_p = 2^p - 1$ est un nombre de Mersenne.

1. Étudier la primalité des nombres M_p pour $p = 3, 5, 7, 11, 13, 17$ et 19 .

2. (u_n) est la suite définie par $u_0 = 4$ et pour tout entier naturel n , $u_{n+1} = u_n^2 - 2$.

(r_n) est la suite des restes de la division euclidienne de u_n par M_p .

Dans cette question, on prend $p = 3$.

a) Calculer r_1, r_2, r_3, r_4, r_5 .

b) Vérifier que $r_{n+1} \equiv r_n^2 - 2 \pmod{M_p}$ pour $n \in \{0, 1, 2, 3, 4\}$.

3. De façon, plus générale, démontrer que pour tout entier naturel n , $r_{n+1} \equiv r_n^2 - 2 \pmod{M_p}$.

4. Voici un programme écrit en langage Python qui calcule les restes r_1, r_2, \dots, r_n pour les nombres premiers $p \in \{3, 5, 7, 11, 13, 17, 19\}$.

a) Saisir et exécuter ce programme pour $n = 20$.

b) Pour quel nombre premier p , 0 ne figure-t-il pas dans les termes de la suite ?

Émettre alors une conjecture concernant la primalité du nombre de Mersenne M_p .

c) Pour les autres nombres premiers p , conjecturer un lien entre p et le rang k du reste nul.

d) Démontrer que si pour un rang r , u_r est un multiple de M_p , alors les restes r_k sont égaux à 2 à partir du rang $r + 2$.

```

1 from sympy import *
2
3 n=int(input("n= "))
4 L=[3,5,7,11,13,17,19]
5 for r in range(0,7):
6     L1=[L[r],4]
7     M=2**L[r]-1
8     u=4
9     for k in range(0,n):
10        u=(u**2-2)%M
11        L1.append(u)
12 print(L1)

```

128 Les entiers de Gauss

On note $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss, c'est-à-dire des nombres complexes $a + ib$ où $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

La norme de $z = a + ib$ ($a \in \mathbb{Z}$, $b \in \mathbb{Z}$) est l'entier $N(z) = a^2 + b^2$.

Dire que w divise z dans $\mathbb{Z}[i]$ signifie qu'il existe un élément v de $\mathbb{Z}[i]$ tel que $z = vw$.

1. a) Montrer que $4 + 5i$ divise $14 - 3i$ mais ne divise pas $14 + 3i$.

b) Vérifier que $N(4 + 5i)$ divise $N(14 - 3i)$ dans \mathbb{Z} .

2. a) Démontrer que pour tous z et z' de $\mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.

b) En déduire que si z divise z' dans $\mathbb{Z}[i]$, alors $N(z)$ divise $N(z')$ dans \mathbb{Z} .

La réciproque est-elle vraie ?

3. Déterminer les entiers de Gauss de norme égale à 1. On les appelle « unités de $\mathbb{Z}[i]$ ».

4. Dire qu'un élément z de $\mathbb{Z}[i]$ est entier de Gauss premier signifie que z n'est pas une unité et que les seuls diviseurs de z dans $\mathbb{Z}[i]$ sont les unités et les produits de z par une unité.

a) Justifier que 2 n'est pas entier de Gauss premier et que 3 l'est.

b) p est un nombre premier dans \mathbb{Z} . On suppose qu'il n'existe pas a et b dans \mathbb{N} tels que $p = a^2 + b^2$.

Démontrer que p est un entier de Gauss premier.

c) Démontrer que si $N(z)$ est premier dans \mathbb{Z} , alors z est un entier de Gauss premier.

La réciproque est-elle vraie ?

129 Nombres amicaux

Deux nombres sont dit amicaux lorsque la somme des diviseurs positifs stricts de l'un est égale à l'autre.

On pose, pour tout entier naturel n non nul :

$$a = 3 \times 2^{n-1} - 1, b = 3 \times 2^n - 1, c = 9 \times 2^{2n-1} - 1$$

$$A = 2^n \times a \times b \text{ et } B = 2^n \times c.$$

1. a) Vérifier que pour $n = 2$, a , b et c sont premiers, et que A et B sont amicaux.

b) Étudier le cas $n = 4$.

2. On suppose que a , b et c sont des nombres premiers.

a) Donner les décompositions en produit de facteurs premiers de A et B .

b) Établir les listes des diviseurs de A et de B .

c) Démontrer que les sommes S_A et S_B des diviseurs respectifs de A et B sont :

$$S_A = (1 + a + ab)(2^{n+1} - 1)$$

$$\text{et } S_B = (1 + c)(2^{n+1} - 1)$$

d) En utilisant les expressions de a , b et c en fonction de n , montrer que $S_A = S_B$. Conclure.

130 Racines primitives

p désigne un nombre premier.

On note E l'ensemble des restes possibles dans la division euclidienne par p et E^* l'ensemble E privé de 0.

On dit qu'un élément x de E^* est une racine primitive modulo p si l'ensemble des restes de la division de x^k par p est égal à E^* lorsque k décrit l'ensemble des nombres entiers naturels.

a) Quelles sont les racines primitives :

• modulo 5 ? • modulo 7 ?

b) On admet que quel que soit le nombre premier p il existe au moins une racine primitive g modulo p .

Montrer que g^k décrit E^* lorsque k décrit l'ensemble des nombres entiers naturels compris entre 0 et $p - 2$.

Conseil : il existe un entier naturel q tel que $k = q(p - 1) + r$ avec $0 \leq r < p - 1$.

c) A est un élément de E^* .

Démontrer qu'il existe un unique nombre entier k compris entre 0 et $p - 2$ tel que $g^k = A$ [p].

k est appelé logarithme de base g modulo p de A , on le note $\ell(A)$.

d) Une solution élémentaire pour déterminer $\ell(A)$ consiste à calculer les restes successifs de la division de g^k par p pour $k = 0, k = 1, k = 2, \dots$ jusqu'à trouver A .

Proposer un algorithme en langage Python permettant de calculer le logarithme de 40 de base 20 modulo 53, en admettant que 20 est une racine primitive modulo 53.

131 Les diviseurs d'un nombre

1. Dans cette question, a , m , n et p désignent des nombres entiers naturels supérieurs ou égaux à 2.

Démontrer que si $a^m \equiv 1$ [p] et $a^n \equiv 1$ [p], alors $a^{\text{PGCD}(m,n)} \equiv 1$ [p].

2. Dans cette question, n est un nombre entier naturel strictement supérieur à 1 tel que n divise $2^n + 1$.

On note p le plus petit nombre premier figurant dans la décomposition en produit de facteurs premiers de n .

a) Démontrer que $2^{2n} \equiv 1$ [p].

b) Justifier que $2^{p-1} \equiv 1$ [p].

c) Justifier $\text{PGCD}(p - 1; 2n) = \text{PGCD}(p - 1; 2)$.

d) En déduire que $p = 3$, puis que les diviseurs de $2^n + 1$ sont de la forme $n = 3^k m$, avec $k \in \mathbb{N}^*$ et $\text{PGCD}(m; 3) = 1$.

132 Le théorème d'Édouard Lucas

n désigne un nombre entier naturel non nul et $F_n = 2^{2^n} + 1$.

1. Montrer que $F_{n-1}^2 - 2^{2^{n-1}+1} = F_n$.

2. p désigne un nombre premier qui divise F_n .

a) Montrer que $2^{2^n} \equiv -1$ [p].

b) Montrer que $F_{n-1}^2 \equiv 2^{2^{n-1}+1}$ [p], puis $F_{n-1}^4 \equiv -2^2$ [p].

c) On pose $x = F_{n-1}^4$.

Déduire de ce qui précède que $x^{2^{n-1}} \equiv -1$ [p], puis que $x^{2^n} \equiv 1$ [p].

d) En déduire l'ordre de F_{n-1} modulo p , c'est-à-dire l'entier m tel que $(F_{n-1})^m \equiv 1$ [p].

e) Conclure quant à l'existence d'un nombre entier k tel que $p = 2^{n+2} k + 1$.

**133 Déterminer une fonction**

Déterminer la fonction f définie sur \mathbb{N} à valeurs dans \mathbb{N} telle que pour tout entier naturel n et tout nombre premier p ,

$$(f(n))^p \equiv n \text{ [p].}$$

134 Écrire un entier comme somme de trois carrés

Démontrer que si p est un nombre premier supérieur ou égal à 5, alors $4p^2 + 1$ peut se mettre sous la forme d'une somme de trois carrés.