DIAPORAMA
Calculs et automatismes
lienmini.fr/maths-e05-06

Exercices calculs et automatismes

23 Nombres premiers

Les propositions suivantes sont-elles vraies ou fausses ?

	V	F
a) L'ensemble des nombres premiers est fini.	☐	☐
b) Si p est un nombre premier alors p n'est pas pair.	☐	☐
c) Si p est un nombre premier ne divisant pas a alors les nombres a et p sont premiers entre eux	☐	☐
e) Si p est un nombre premier ne divisant pas a alors les nombres p et a sont premiers.	☐	☐

24 Critère d'arrêt

Méthode Comment faire pour déterminer de « tête » les nombres premiers parmi les entiers suivants ?

39 – 47 – 51 – 67 – 77 – 83 – 91

25 Crible et critère d'arrêt

1. Rayer les entiers qui ne sont pas premiers dans ce tableau.

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

2. En déduire la liste des nombres premiers compris entre 30 et 60.

26 Théorème de Gauss (1)

Méthode Soit p un nombre premier. Comment faire pour montrer que si p divise n^2 alors p^2 divise n^2 ?

27 Théorème de Gauss (2)

Les propositions suivantes sont-elles vraies ou fausses ? Justifier.

	V	F
a) Si a est un entier naturel tel que 13 divise a^5 alors 13^4 divise $\frac{a^5}{13}$.	☐	☐
b) Si p est un nombre premier divisant ab alors p divise a et p divise b	☐	☐

28 Décomposition (1)

1. Donner mentalement la décomposition en produits de facteurs premiers des nombres suivants.

a) 30 **b)** 40 **c)** 64 **d)** 70 **e)** 120

2. Méthode En utilisant la décomposition de $10 = 2 \times 5$, comment faire pour donner la décomposition en produit de facteurs premiers des nombres suivant ?

a) 800 **b)** 2 000 **c)** 60 000

29 Décomposition (2)

Déterminer la décomposition en produit de facteurs premiers des nombres suivants en utilisant leur caractéristique.

a) $6! = 2 \times 3 \times 4 \times 5 \times 6$ **b)** $29^2 - 4$ **c)** $85^2 - 16$

30 Décomposition (3)

Choisir la (les) bonne(s) réponse(s).

La décomposition de 2 520 est :

a $2^3 \times 3^2$ **b** $2^3 \times 3^2 \times 5 \times 7$

c $2^2 \times 3^2 \times 5 \times 7$ **d** $2^3 \times 5 \times 7$

31 PGCD

Méthode Comment faire pour décomposer les nombres a et b en produit de facteurs premiers, puis déterminer leur PGCD dans chacun des cas suivants ?

a) $a = 350$ et $b = 980$ **b)** $a = 792$ et $b = 924$

32 Nombre de diviseurs (1)

Les propositions suivantes sont-elles vraies ou fausses ? Justifier.

	V	F
a) La décomposition en produit de facteurs premiers de PGCD(2 142 , 6 664) ne contient que des facteurs à la puissance 1.	☐	☐
b) Si $a \geqslant 2$ est un nombre impair, alors le nombre $2a$ possède deux fois plus de diviseurs que le nombre a	☐	☐

33 Nombre de diviseurs (2)

Méthode Comment faire pour déterminer le nombre de diviseurs de 48 et 60 ?

34 Nombre de diviseurs (3)

Choisir la (les) bonne(s) réponse(s).

Parmi les entiers suivants celui qui admet le plus de diviseurs est :

a 60 **b** 72 **c** 90 **d** 100

35 Nombre de diviseurs (4)

Déterminer l'entier α tel que $a = 25 \times 6^{\alpha}$ pour que a admette 48 diviseurs.

36 Théorème de Fermat (1)

Quel est le reste dans la division par 41 des nombres suivants ?

a) 4^{20} **b)** 25^{20} **c)** 49^{20} **d)** 50^{41}

37 Théorème de Fermat (2)

Les propositions suivantes sont-elles vraies ou fausses ? Justifier.

	V	F
a) Pour tout $n \in \mathbb{N}$, 7 divise $5^{6n} - 1$.	☐	☐
b) Pour tout $n \in \mathbb{N}$, 4 divise $7^{3n} - 1$.	☐	☐

38 Théorème de Fermat (3)

Méthode Comment faire pour montrer que l'entier $a = 2^{37} + 3^{37} - 5$ est divisible par 74 ?

Exercices d'application

Déterminer si un nombre est premier

Méthode 1 p. 137

39 Montrer que 419 est un nombre premier.
On expliquera clairement la méthode utilisée.

40 Déterminer si les entiers suivants sont premiers ou non.

a) 117 **b)** 271 **c)** 323
d) 401 **e)** 527 **f)** 719

41 Soit $n \in \mathbb{N}$. On pose $N = 2n^2 + n - 10$.
1. Factoriser N par $(n - 2)$.
2. Pour quelle valeur de n, le nombre N est-il premier ?

42 Soit $n \in \mathbb{N}$. On pose $N = 2n^2 + 7n + 6$.
La proposition suivante est-elle vraie ou fausse ? Justifier.
« Il existe une valeur de n pour laquelle N est un nombre premier. »

Coup de pouce S'inspirer de l'exercice précédent.

43 Soit p un nombre premier et deux entiers n_1 et n_2 tels que :

$$n_1 = p + 1\,000 \text{ et } n_2 = p + 2\,000.$$

1. En raisonnant modulo 3, montrer que la seule valeur possible de p pour que n_1 et n_2 soient des nombres premiers est 3.
2. Peut-on avoir n_1 et n_2 premiers ?

44 Démo
Soit p un nombre premier et a un entier tel que : $2 \leqslant a \leqslant n - 2$.
Montrer que p ne divise pas $a^2 - 1$.

45 Algo
On donne ci-dessous la fonction `f` en **Python** dont des mots ont été effacés.

```
from math import*
def f(n):
    i=2
    if n%i==0:
        return "non … car … par",i
    i+=1
    while i<=sqrt(n):
        if n%i==0:
            return "non … car … par",i
        i+=2
    return L
```

1. Compléter cet algorithme par des mots adaptés.
2. **a)** Que détermine cette fonction ?
b) Expliquer clairement comment procède cette fonction.

46 Dans les *Inédits* de Marcel Pagnol, l'écrivain indique que, pour tout n entier impair $n > 1$, le nombre $N = n + (n + 2) + n(n + 2)$ est premier. Qu'en pensez-vous ?

Utiliser le théorème de Gauss appliqué aux nombres premiers

Méthode 2 p. 137

47 Démo
Soit p un nombre premier et $a, b \in \mathbb{N}$.
Montrer que si p divise a et $a^2 + b^2$ alors p divise b.

48 Soit un entier relatif n tel que : $n^2 = 17p + 1$ où p est un nombre premier.
1. Écrire $17p$ comme un produit de facteurs fonction de n.
2. Montrer que n est de la forme :

$$n = 17k + 1 \text{ ou } n = 17k - 1 \text{ avec } k \in \mathbb{Z}$$

On citera le théorème utilisé.
3. Montrer qu'une seule valeur de k convient.
En déduire les valeurs de n et p

49 Soit un entier relatif n tel que : $n^2 = 29p + 1$ où p est un nombre premier.
1. Écrire $29p$ comme un produit de facteurs fonction de n.
2. En s'inspirant de l'exercice précédent, déterminer les valeurs de n et p qui conviennent au problème.

50 Démo
Démontrer le théorème de Gauss appliqué aux nombres premiers :
« Si un nombre premiers p divise le produit ab de deux entiers non nuls alors, p divise a ou p divise b ».

Décomposer en produit de facteurs premiers

Méthode 3 p. 139

51 Décomposer en produit de facteurs premiers 960 et 221 222.

52 **1.** Décomposer en produit de facteurs premiers 2 650 et 1 272.
2. En déduire PGCD(2 650 , 1 272).
3. Retrouver ce résultat à l'aide de l'algorithme d'Euclide puis comparer les deux méthodes.

53 **1.** Décomposer en produit de facteurs premiers $a = 428\,904$ et $b = 306\,360$.
2. En déduire PGCD(a , b).
3. Retrouver ce résultat à l'aide de l'algorithme d'Euclide et comparer les deux méthodes.

54 **1.** Quelle est la condition sur les puissances des facteurs premiers d'un carré parfait ?
2. Trouver un nombre de trois chiffres qui soit un carré parfait divisible par 56.

55 Une boîte, en forme de pavé droit, a des dimensions qui s'expriment, en centimètres, par des nombres entiers.
Son volume est de 22,661 dm^3.
Quelles sont les dimensions de cette boîte ?

Exercices d'application

56 **1.** Décomposer 2 016 en produit de facteurs premiers.
2. Déterminer, en expliquant la méthode choisie, la plus petite valeur de l'entier naturel n tel que n^2 est un multiple de 2 016.

57 À l'aide de la décomposition en facteurs premiers de 84, résoudre dans $\mathbb{N}$ l'équation :
$$x(x+1)(2x+1) = 84.$$

58 Cet exercice a pour but de déterminer par combien de zéros se termine le nombre 1 000! On rappelle :
$1\,000! = 1 \times 2 \times 3 \times \ldots \times 1\,000$.
1. Montrer qu'il existe p et q ($p > 1$ et $q > 1$) et un entier N premier avec 10 tels que :
$$1000! = 2^p \times 5^q \times N.$$
2. **a)** Combien y a-t-il de nombres inférieurs ou égaux à 1 000 divisible par 5 ? divisible par 5^2 ? divisible par 5^3 ? divisible par 5^4 ?
b) En déduire alors que $q = 249$.
3. Montrer que $p > q$ et que q est le nombre cherché.

59 Dans un annuaire de moins de 1 000 pages sont inscrits 999 991 noms.
Chaque page contient le même nombre de noms.
1. Montrer que 997 est un nombre premier.
2. Combien de pages contient cet annuaire ?

Trouver le nombre de diviseurs d'un entier

Méthode 4 p. 141

60 **1.** Décomposer 792 en produit de facteurs premiers. Quel est le nombre de diviseurs de 792 ?
2. À l'aide d'un tableau double entrée déterminer tous les diviseurs de 792.

61 **1.** Décomposer 8 316 en produit de facteurs premiers. Quel est le nombre de diviseurs de 8 316 ?
2. Proposer un algorithme pour énumérer tous les diviseurs de 8 316.

62 **1.** Décomposer 300^{300} en produit de facteurs premiers. Quel est le nombre de diviseurs de 300^{300} ?
2. À partir du résultat de la question **1.**, trouver un nombre possédant plus d'un milliard de diviseurs.

63 Démontrer qu'un entier naturel n est un carré parfait si, et seulement si, le nombre de ses diviseurs est impair. Démo

64 Un entier n a cinq diviseurs et $(n - 16)$ est le produit de deux nombres premiers.
1. Prouver que $n = p^4$ avec p premier.
2. Écrire $(n - 16)$ sous forme d'un produit de trois facteurs dépendant de p.
3. En déduire la valeur de p puis de n.

65 Le produit de deux entiers naturels a et b avec $a < b$ est 11 340. On note $d = \text{PGCD}(a, b)$.
1. **a)** Pourquoi d^2 divise-t-il 11 340 ?
b) Pourquoi $d = 2^\alpha \times 3^\beta$ avec $0 \leqslant \alpha \leqslant 1$ et $0 \leqslant \beta \leqslant 2$?
2. On sait de plus que a et b ont six diviseurs communs et a est un multiple de 5.
a) Démontrer que $d = 18$.
b) En déduire a et b.

Appliquer le petit théorème de Fermat

Méthode 5 p. 141

66 **1.** Montrer que $4^{28} - 1$ est divisible par 29.
2. Montrer que pour tout n, $4^n - 1$ est divisible par 3.
3. Montrer que pour tout k, $4^{4k} - 1$ est divisible par 5 et par 17.
4. En déduire quatre diviseurs premiers de $4^{28} - 1$.

67 Soit $n \in \mathbb{N}^*$. On note $a = n^{13} - n$.
1. Montrer que a est divible par 13 et 7.
2. En déduire que a est divisible par 182.

68 **1.** Montrer que, pour tout $a \in \mathbb{N}$:
$$a^{31} - a \equiv 0\ (62).$$
2. Montrer que, pour tout $a, n \in \mathbb{N}$:
$$a^{30+n} - a^n \equiv 0\ (62).$$

69 **1.** Soit p un nombre premier supérieur à 2.
Montrer que p divise $1 + 2 + 2^2 + \ldots + 2^{p-2}$.
2. Est-ce que 97 divise la somme S telle que
$$S = \sum_{n=1}^{98} n^{96} ?$$

70 Soit p un nombre premier.
1. Montrer que si p divise $3^p + 1$ alors p divise 4.
2. Trouver p tel que p divise $3^p + 1$.

71 **1.** Vérifier que 761 est un nombre premier.
2. L'entier n est un naturel composé de 760 chiffres tous égaux à 9 : $n = \underbrace{999\ldots99}_{760\text{ fois}}$.
a) Calculer $n + 1$.
b) Montrer que n est divisible par 761.

72 **1.** Soit $n \in \mathbb{N}$ et $A = n^7 - n$.
a) Montrer que A est divisible par 7.
b) Vérifier que : $A = n(n^3 - 1)(n^3 + 1)$ puis montrer que A est divisible par 2 et par 3.
c) En déduire que A est divisible par 42.
2. Soit $n \in \mathbb{N}$ et $B = n^2(n^2 - 1)(n^2 + 1)$.
a) Montrer que B est divisible par 3.
b) En remarquant que $(n^2 - 1)(n^2 + 1) = n^4 - 1$, montrer que B est divisible par 5.
c) En utilisant un tableau de congruence, montrer que B est divisible par 4.
d) En déduire que B est divisible par 60.

Exercices d'entraînement

Déterminer un entier conditionné par le nombre de ses diviseurs

Méthode 6 p. 142

73 Un entier naturel n possède seulement deux diviseurs premiers.
Sachant que n a 6 diviseurs et que la somme de ses diviseurs est 28, déterminer n.

74 α et β sont deux entiers naturels et $n = 2^\alpha \times 3^\beta$.
Le nombre de diviseurs de $12n$ est le double du nombre de diviseurs de n.
1. Montrer que l'on a : $\beta(\alpha - 1) = 4$
2. En déduire les trois valeurs possibles pour n.

75 α et β sont deux entiers naturels et $n = 2^\alpha \times 3^\beta$.
Le nombre de diviseurs de n^3 est égal à 8 fois le nombre de diviseurs de n.
1. Prouver que $(\alpha - 5)(\beta - 5) = 32$.
2. Déduire les valeurs possibles pour n.

76 Déterminer le plus petit entier naturel possédant :
a) 10 diviseurs.
b) 15 diviseurs.

77 Déterminer deux entiers naturels a et b tels que $a > b$, PGCD$(a, b) = 18$, et qui ont respectivement 21 et 10 diviseurs.

78 Un entier naturel n est tel que :
• 4 divise n,
• n admet 14 diviseurs,
• n est de la forme $n = 37p + 1$ avec p premier.
1. Montrer que n possède au plus deux diviseurs premiers.
2. Montrer que n ne peut avoir qu'un seul diviseur premier.

79 Un nombre parfait est un nombre dont la somme des diviseurs stricts est égal à lui-même. Euclide donne la règle suivante pour trouver des nombres parfaits :
« Si un nombre a s'écrit $2^n(2^{n+1} - 1)$ et si $2^{n+1} - 1$ est premier, alors a est parfait ».

Démo

1. Trouver les quatre premiers nombres parfaits.
2. Soit $a = 2^n(2^{n+1} - 1)$ avec $2^{n+1} - 1$ premier.
a) Quelle est la décomposition de a en facteurs premiers ?
b) En déduire la liste des diviseurs de a.
c) Démontrer alors que la somme des diviseurs stricts est égale à ce nombre a.


Euclide

Travailler modulo p, p premier

Méthode 7 p. 143

80 Soit le système (S) suivant : $(x ; y) \in \mathbb{Z}$

$$(S) : \begin{cases} 3x + 4y \equiv 5 \ (13) \\ 2x + 5y \equiv 7 \ (13) \end{cases}$$

1. Justifier que (S) est équivalent à :

$$\begin{cases} 3x + 4y \equiv 5 \ (13) \\ 7y \equiv 11 \ (13) \end{cases}$$

2. Déterminer $k_1, k_2 \in [\![0 ; 12]\!]$ tels que :
$7k_1 \equiv 1 \ (13)$ et $3k_2 \equiv 1 \ (13)$.
3. En déduire les solutions du système (S).

81 Soit $q > 5$, un nombre premier et M le produit des nombres premiers de 5 à q :

$$M = 5 \times 7 \times 11 \times \ldots \times q.$$

On pose : $N = 2^2 \times M + 3$.
1. a) Montrer que N est impair.
b) Montrer que $N \not\equiv 0 \ (3)$.
2. Soit p un nombre premier divisant N.
a) Montrer que $p > q$.
b) Montrer que : $p \equiv 1 \ (4)$ ou $p \equiv 3 \ (4)$.
3. Soit $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ la décomposition de N en facteurs premiers.
a) Montrer en raisonnant par l'absurde qu'il existe un facteur premier p_i avec $i \in [\![1 ; r]\!]$ tel que : $p_i \equiv 3 \ (4)$.
b) En déduire qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

Nombres premiers et suites

82 Soit $A = [\![1 ; 46]\!]$.
1. On considère l'équation

$$(E) : 23x + 47y = 1$$

où x et y sont des entiers relatifs.
a) Donner une solution particulière $(x_0 ; y_0)$ de (E).
b) Déterminer l'ensemble des couples $(x ; y)$ solutions de (E).
c) En déduire qu'il existe un unique entier x appartenant à A tel que $23x \equiv 1 \ (47)$.
2. Soit a et b deux entiers relatifs.
a) Montrer que si $ab \equiv 0 \ (47)$ alors $a \equiv 0 \ (47)$ ou $b \equiv 0 \ (47)$.
b) En déduire que si $a^2 \equiv 1 \ (47)$ alors $a \equiv 1 \ (47)$ ou $a \equiv -1 \ (47)$.
3. a) Montrer que pour tout entier p de A, il existe un entier relatif q tel que $pq \equiv 1 \ (47)$.
Pour la suite, on admet que pour tout entier p de A, il existe un unique entier, noté p^{-1} appartenant à A tel que $p \times p^{-1} \equiv 1 \ (47)$.
b) Quels sont les entiers p de A qui vérifient $p = p^{-1}$?
c) Montrer que $46! \equiv 1 \ (47)$.

83 On considère la suite (u_n) définie pour tout entier naturel n non nul par :

$$u_n = 2^n + 3^n + 6^n - 1.$$

1. Calculer les six premiers termes de la suite.
2. Montrer que, pour tout entier naturel n non nul, u_n est pair.
3. Montrer que, pour tout entier naturel n pair non nul, u_n est divisible par 4.
On note E l'ensemble des nombres premiers qui divisent au moins un terme de la suite (u_n).
4. Les entiers 2, 3, 5 et 7 appartiennent-ils à l'ensemble E ?
5. Soit p un nombre premier strictement supérieur à 3.
a) Montrer que : $6 \times 2^{p-2} \equiv 3\ (p)$ et $6 \times 3^{p-2} \equiv 2\ (p)$.
b) En déduire que $6u_{p-2} \equiv 0\ (p)$.
6. Le nombre p appartient-il à l'ensemble (E) ?

84 On considère la suite (u_n) d'entiers naturels définie par : $u_0 = 1$ et, pour tout entier naturel n, $u_{n+1} = 10u_n + 21$.
1. Calculer u_1, u_2 et u_3.
2. a) Démontrer par récurrence que, pour tout entier naturel n :

$$3u_n = 10^{n+1} - 7$$

b) En déduire, pour tout entier naturel n, l'écriture décimale de u_n.
3. Montrer que u_2 est un nombre premier.
4. On se propose maintenant d'étudier la divisibilité des termes de la suite (u_n) par certains nombres premiers.
Démontrer que, pour tout entier naturel n, u_n n'est divisible ni par 2, ni par 3, ni par 5.
5. a) Démontrer que, pour tout entier naturel n :

$$3u_n \equiv 4 - (-1)n\ (11).$$

b) En déduire que, pour tout entier naturel n, u_n n'est pas divisible par 11.
6. a) Démontrer l'égalité : $10^{16} \equiv 1\ (17)$.
b) En déduire que, pour tout entier naturel k, $u_{16k} + 8$ est divisible par 17.

85 **1.** Calculer :
a) $(1+\sqrt{6})^2$;
b) $(1+\sqrt{6})^4$;
c) $(1+\sqrt{6})^6$.
d) Décomposer en produit de facteurs premiers le nombre 847 et 342. Que peut-on en déduire ?
2. Soit n un entier naturel non nul. On note a_n et b_n les entiers naturels tels que :

$$(1+\sqrt{6})^n = a_n + b_n\sqrt{6}\ .$$

a) Que valent a_1 et b_1 ? D'après la question **1. a)** donner d'autres valeurs de a_n et b_n.
b) Calculer a_{n+1} et b_{n+1} en fonction de a_n et b_n.
c) Démontrer que, si 5 ne divise pas $a_n + b_n$, alors 5 ne divise pas non plus a_{n+1} et b_{n+1}.
En déduire que, quel que soit $n \in \mathbb{N}^*$, 5 ne divise pas $a_n + b_n$.
d) Démontrer que, si a_n et b_n sont premiers entre eux, alors a_{n+1} et b_{n+1} sont premiers entre eux.
En déduire que, quel que soit $n \in \mathbb{N}^*$, a_n et b_n sont premiers entre eux.

Divisibilité et nombres premiers

86 On désigne par p un nombre entier premier supérieur ou égal à 7. Le but de l'exercice est de démontrer que l'entier naturel $n = p^4 - 1$ est divisible par 240, puis d'appliquer ce résultat.
1. Montrer que p est congru à – 1 ou à 1 modulo 3.
En déduire que n est divisible par 3.
2. En remarquant que p est impair, prouver qu'il existe un entier naturel k tel que $p^2 - 1 = 4k(k+1)$, puis que n est divisible par 16.
3. En considérant tous les restes possibles dans la division euclidienne de p par 5, démontrer que 5 divise n.
4. a) Soit a, b et c trois entiers naturels. Démontrer que si a et b divise c, avec a et b premiers entre eux, alors ab divise c.
b) Déduire de ce qui précède que 240 divise n.
5. Existe-t-il quinze nombres premiers $p_1, p_2, \ldots, p_{15}$ supérieurs ou égaux à 7 tels que l'entier $A = p_1^4 + p_2^4 + \ldots + p_{15}^4$ soit un nombre premier ?

87 Pour tout entier naturel n supérieur ou égal à 2, on pose $A(n) = n^4 + 1$. L'objet de l'exercice est l'étude des diviseurs premiers de $A(n)$.
1. a) Étudier la parité de l'entier $A(n)$.
b) Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.
c) Montrer que tout entier d diviseur de $A(n)$ est premier avec n.
d) Montrer que, pour tout entier d diviseur de $A(n)$:

$$n^8 \equiv 1\ (d).$$

2. Soit d un diviseur de $A(n)$. On note s le plus petit des entiers naturels non nuls k tels que $n^k \equiv 1\ (d)$.
a) Soit k un tel entier. En utilisant la division euclidienne de k par s, montrer que s divise k.
b) En déduire que s est un diviseur de 8.
c) Montrer que si, de plus, d est premier, alors s est un diviseur de $d - 1$.
3. Recherche des diviseurs premiers de $A(n)$ dans le cas où n est un entier pair. Soit p un diviseur premier de $A(n)$.
En examinant successivement les cas $s = 1$, $s = 2$ puis $s = 4$, conclure que p est congru à 1 modulo 8.
4. On donne la liste des nombres premiers congrus à 1 modulo 8 :17, 41, 73, 89, 97, 113, 137 …
Appliquer ce qui précède à la recherche des diviseurs premiers de $A(12)$.

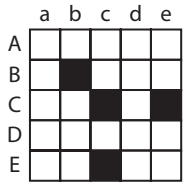
88 Soit n un entier relatif et A le nombre défini par :

$$A = n^4 - 12n^2 + 16.$$

1. En remarquant que $A = n^4 - 8n^2 + 16 - 4n^2$, factoriser A.
2. Montrer que si n est pair alors, A n'est pas premier.
3. On suppose que n est impair. On pose alors $n = 2k + 1$ avec $k \in \mathbb{Z}$.
a) Montrer que : $A = (4k^2 + 8k - 1)(4k^2 - 5)$.
b) En déduire les valeurs de n pour lesquelles A est nombre premier.

Exercices d'entraînement

89 Soit les définitions des « nombres croisés » suivant.
Horizontalement :
A. C'est un carré parfait.
B. Un nombre premier dont le produit de ses chiffres est 63 et sa somme 17.
C. Le produit de ses chiffres est 1.
D. Les chiffres de ce nombre, dans l'ordre, sont consécutifs.
E. Un multiple de 11. La somme de ses chiffres est supérieure de 1 à leur produit.
Verticalement :
a. C'est un cube parfait dont le produit de ses chiffres est 90.
b. Les chiffres, dans l'ordre, sont impairs consécutifs.
c. Un carré parfait, le produit de ses chiffres est 36.
d. Son premier chiffre et son dernier chiffre sont identiques, le produit de ses chiffres est 105.
e. La somme des chiffres est 7 et leur produit 6. Un multiple de 12.



D'après *Jeux et stratégie n°14*.

Produit de nombres premiers

90 On suppose que 250 507 n'est pas premier.
On se propose de chercher des couples d'entiers naturels $(a\,;b)$ vérifiant la relation :

$$(E) : a^2 - 250\,507 = b^2.$$

1. Soit n un entier naturel.
a) À l'aide d'un tableau de congruence donner les restes possibles de n^2 modulo 9.
b) Sachant que (E) est vérifiée, déterminer les restes possibles modulo 9 de $a^2 - 250\,507$.
c) Montrer que les restes possibles modulo 9 de a sont 1 et 8.
2. Vérifier que si le couple $(a\,;b)$ vérifie (E), alors $a > 501$.
3. On suppose que le couple $(a\,;b)$ vérifie (E).
a) Démontrer que a est congru à 503 ou à 505 modulo 9.
b) Déterminer le plus petit entier naturel k tel que $(505 + 9k\,;b)$ soit solution de (E), puis donner le couple solution correspondant.
4. a) Déduire de la question **3.** une écriture de 250 507 en un produit deux facteurs.
b) Cette écriture est-elle unique ?

91 On se propose de rechercher des nombres N dont la décomposition est $N = p_1 \times p_2 \times p_3$ où p_1, p_2, p_3 sont trois nombres premiers tels que $p_1 + p_2 = p_3$.
Par exemple : $286 = 2 \times 11 \times 13$ est un tel nombre.
1. Montrer que nécessairement $p_1 = 2$.
2. On suppose que $680 < N < 1\,920$.
Déterminer p_2 puis déduire N.
3. On suppose que $6 \times 10^4 < N < 8 \times 10^4$.
Donner les valeurs possibles pour p_2 et en déduire les valeurs de N correspondantes.

Coup de pouce Les nombres premiers de 100 à 200 sont :
101 103 107 109 113 127 131 137 139 149
151 157 163 167 173 179 181 191 193 197 199.

Équations et nombres premiers

92 **1.** On suppose que $a, b \in \mathbb{N}$ et que $a^2 - b^2$ est un nombre premier.
Quelle relation existe-t-il entre a et b ?
2. Montrer que 401 est premiers puis résoudre dans $\mathbb{N}^2$ l'équation :

$$x^2 - y^2 = 401.$$

93 Le but de cet exercice est de trouver tous les entiers relatifs x solutions de :

$$(E) : x^2 + x - 2 \equiv 0\ (13).$$

1. Trouver une solution particulière α de (E).
2. On pose $X = x - \alpha$, trouver alors toutes les solutions de (E).

94 Le but de cet exercice est de trouver tous les entiers relatifs x solutions de

$$(E) : x^2 - 2x + 2 \equiv 0\ (17)$$

1. Montrer que $\alpha = 5$ est une solution de (E).
2. On pose $X = x - \alpha$, trouver alors toutes les solutions de (E).

95 **1.** Montrer que pour tous réels x et y, on a :

$$x^3 - y^3 = (x - y)(x^2 + xy + y^2).$$

2. Résoudre alors dans $\mathbb{N}^2$ l'équation :

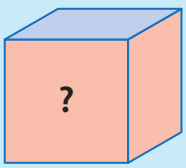
$$x^3 - y^3 = 127.$$

96 **1.** Décomposer en produit de facteurs premiers 8 633.
2. Résoudre dans $\mathbb{N}^2$, l'équation :

$$x^2 - 4y^2 = 8\,633.$$

Travailler l'oral

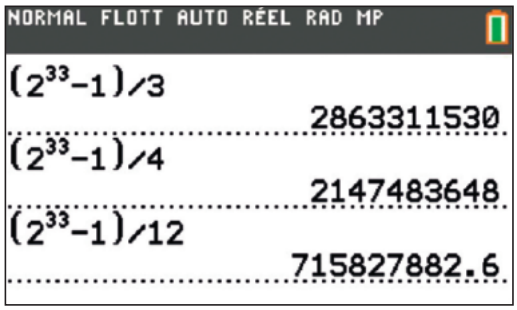
97 Le problème de la cuve
La cuve est à peu près cubique. Sa base est carrée. Les dimensions de la cuve sont des nombres entiers de décimètres et son volume est égal à 1 450 litres à 2 litres près.
Quelles sont les dimensions de la cuve ?
On expliquera la procédure suivie et l'on justifiera le choix retenu.



98 Nombres de Mersenne

Les nombres de la forme $2^n - 1$ où $n \in \mathbb{N}^*$ sont appelés nombres de Mersenne.
On s'intéresse au nombre de Mersenne : $2^{33} - 1$.

1. Un élève utilise sa calculatrice et obtient les résultats suivants :



Il affirme alors que 3 et 4 divise $2^{33} - 1$ mais pas 12.

a) En quoi cette affirmation contredit-elle le corollaire du théorème de Gauss ?

b) Montrer que 4 ne divise pas $2^{33} - 1$.

c) En remarquant que $2 \equiv -1$ (3), montrer que 3 ne divise pas $2^{33} - 1$.

2. a) Calculer la somme : $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + \ldots + (2^3)^{10}$.

b) En déduire que 7 divise $2^{33} - 1$.

99 Nombres de Poulet

Histoire des Maths

Soit $n \in \mathbb{N}^*$, un entier impair tel que :

$$2^{n-1} \not\equiv 1 \ (n).$$

1. Montrer que n n'est pas premier.

2. Quel est le reste de 2^{340} dans la division par 341 ?
Que cela signifie-t-il par rapport au petit théorème de Fermat ?
Un nombre comme 341 est appelé nombre de Poulet.

Paul Poulet est un mathématicien belge né en 1887 et mort en 1946.
Autodidacte, il apporta une contribution importante à la théorie des nombres.
Il est notamment connu pour avoir exhibé des nombres quasi premiers.

3. Parmi les nombres entiers inférieurs à 25 milliards, 1 091 987 405 sont premiers et seulement 21 853 sont des nombres de Poulet (donc non premier).
On prend un nombre n au hasard parmi les entiers inférieurs à 25 milliards et l'on décide de déclarer, après avoir calculé 2^{n-1} modulo n :

- si $2^{n-1} \not\equiv 1 \ (n)$, « n n'est pas premier »,
- si $2^{n-1} \equiv 1 \ (n)$, « n est premier ».

a) Quelle est la probabilité d'énoncer un résultat faux ?

b) Quelle est la probabilité que le nombre soit premier sachant qu'il a été annoncé comme tel ?

100 Triplets pythagoriciens

On appelle triplet pythagoricien, noté TP, un triplet d'entiers naturels non nuls $(x\,;y\,;z)$ tels que : $x^2 + y^2 = z^2$.
Ainsi $(3\,;4\,;5)$ est un TP car $3^2 + 4^2 = 5^2$.

A ▸ Généralités

1. Démontrer que, si $(x\,;y\,;z)$ est un TP et p un entier naturel non nul, alors $(px\,;py\,;pz)$ est lui aussi un TP.

2. Démontrer que, si $(x\,;y\,;z)$ est un TP, alors x, y et z ne peuvent pas être tous les trois impairs.

3. On admet que tout $n \in \mathbb{N}^*$ peut s'écrire d'une façon unique sous la forme du produit d'une puissance de 2 par un entier impair :

$$n = 2^\alpha \times k \text{ où } \alpha, k \in \mathbb{N} \text{ et } k \text{ impair.}$$

Par exemple : $9 = 2^0 \times 9$ et $120 = 2^3 \times 15$.

a) Donner l'écriture en puissance de 2 de 192.

b) Soit x et z deux entiers naturels non nuls, tels que $x = 2^\alpha \times k$ et $z = 2^\beta \times m$.
Écrire en puissance de 2 des entiers $2x^2$ et z^2.

c) En examinant l'exposant de 2 dans la décomposition de $2x^2$ et z^2, montrer qu'il n'existe pas de couple d'entiers naturels non nuls $(x\,;z)$ tels que $2x^2 = z^2$.

d) En déduire que un TP est formé de trois entiers naturels x, y, z deux à deux distincts.

B ▸ Recherche d'un TP contenant 2 015

Tout TP $(x\,;y\,;z)$, est rangé dans l'ordre suivant :

$$x < y < z.$$

1. Décomposer 2 015 en produit de facteurs premier puis, en utilisant le TP(3 ; 4 ; 5), déterminer un TP de la forme $(x\,;y\,;2015)$.

2. On admet que, pour tout entier naturel n :

$$(2n+1)^2 + (2n^2+2n)^2 = (2n^2+2n+1)^2.$$

Déterminer un TP de la forme $(2015\,;y\,;z)$.

3. a) En remarquant que $403^2 = 169 \times 961$, déterminer un couple d'entiers non nuls $(x\,;z)$ tel que :

$$z^2 - x^2 = 403^2, \text{ avec } x < 403.$$

b) En déduire un TP de la forme $(x\,;2015\,;z)$.

101 Écriture décimale

Soit E l'ensemble des entiers naturels écrits, en base 10, sous la forme $\overline{abba}$ où a est un chiffre supérieur ou égal à 2 et b est un chiffre quelconque.
Exemples : 2 002 , 3 773 , 9 119.
On cherche le nombre d'éléments de E ayant 11 comme plus petit facteur premier.

1. a) Décomposer 1 001 en produit de facteurs premiers.

b) Montrer que tout élément de E est divisible par 11.

2. a) Quel est le nombre d'éléments de E ?

b) Quel est le nombre d'éléments de E qui ne sont ni divisibles par 2 ni par 5 ?

3. Soit n un élément de E s'écrivant sous la forme $\overline{abba}$.

a) Montrer que : « n est divisible par 3 » équivaut à « $a + b$ est divisible par 3 ».

b) Montrer que : « n est divisible par 7 » équivaut à « b est divisible par 7 ».

4. Déduire des questions précédentes le nombre d'éléments de E qui admettent 11 comme plus petit facteur premier.

Exercices bilan

102 Fonctions modulo 227

1. Soit l'équation (E) : $109x - 226y = 1$.
où x et y sont des entiers relatifs.
a) Déterminer PGCD(109 , 226).
Que peut-on en conclure pour l'équation (E) ?
b) Montrer que l'ensemble solutions de (E) est l'ensemble des couples de la forme :
$141 + 226k$, $68 + 109k$, où $k \in \mathbb{Z}$.
c) En déduire qu'il existe un unique couple $(d\,;e)$ d'entiers naturels non nuls tel que :
$d \leqslant 226$ *et* $109d = 1 + 226e$.
Donner les valeurs des entiers d et e.
2. Démontrer que 227 est un nombre premier.
3. On note A l'ensemble des 227 entiers naturels a tels que $a \leqslant 226$.
On définit deux fonctions f et g de A dans A telles que, à tout entier $a \in$ A :
• f associe le reste de la division euclidienne de a^{109} par 227,
• g associe le reste de la division euclidienne de a^{141} par 227.
a) Vérifier que $g[f(0)] = 0$.
b) Montrer que, quel que pour tout $a \in$ A non nul : $a^{226} \equiv 1$ (227).
c) En utilisant **1. b)**, déduire que, pour tout $a \in$ A non nul, $g\,[f\,(a)] = a$.
d) Que peut-on dire de $f\,[g(a)]$?
Comment sont f et g l'une par rapport à l'autre ?

103 Conjecture de Goldbach

Soit la fonction F définie sur $\mathbb{N}^*$ qui vérifie les propriétés suivantes.
• $F(a \times b) = F(a) \times F(b)$ si PGCD(a , b) = 1.
• $F(p + q) = F(p) + F(q)$ si p et q premiers.
1. Justifier que $F(6) = F(2) \times F(3)$ et $F(6) = 2F\,(3)$.
En déduire $F(2)$.
2. a) Déterminer $F(4)$.
b) En utilisant plusieurs fois la 2e propriété, montrer que $F(12) = 2F(3) + 6$.
c) Justifier que $F(12) = 4F(3)$.
d) En déduire $F(3)$.
3. Montrer que $F(n) = n$ pour $1 \leqslant n \leqslant 17$.
4. a) Décomposer 2006 en produit de facteurs premiers.
b) Justifier que $F(59) = F(66) - 7$. En déduire que $F(59) = 59$.
c) Déterminer $F(2006)$.

Remarque
Les calculs précédents incitent à penser que pour tout entier naturel non nul, $F(n) = n$. Mais cela reste une conjecture.
Pour démontrer cette conjecture, il faudrait que l'hypothèse de Goldbach soit vraie : « Tous les entiers pairs supérieurs ou égaux à 4 sont la somme de deux nombres premiers. »

104 Décompositions de 40

A ▶ **1.** Donner deux nombres premiers x, et y tels que :
$$40 = x + y.$$
2. Soit l'équation $20x + 19y = 40$, où $x, y \in \mathbb{Z}$.
Résoudre cette équation.
3. On veut savoir si 40, peut s'écrire comme différence de deux carrés, soit savoir si l'équation $x^2 - y^2 = 40$, admet des couples solutions dans $\mathbb{N}^2$.
a) Donner la décomposition de 40 en produit de facteurs premiers.
b) Montrer que, si x et y désignent des entiers naturels, les nombres $(x - y)$ et $(x + y)$ ont la même parité.
c) Déterminer toutes les solutions de l'équation $x^2 - y^2 = 40$ où $x, y \in \mathbb{N}$.

B ▶ Certains nombres entiers peuvent se décomposer en somme ou différence de cubes d'entiers naturels. Par exemple :
$$13 = 4^3 + 7^3 + 7^3 - 9^3 - 2^3$$
$$13 = -1^3 - 1^3 - 1^3 + 2^3 + 2^3$$
$$13 = 1^3 + 7^3 + 10^3 - 11^3$$
Dans tout ce qui suit, on écrira pour simplifier « sommes » à la place de « somme ou différence ».
Les deux premiers exemples montrent que 13 peut se décomposer en « somme » de 5 cubes.
Le troisième exemple montre que 13 peut se décomposer en « somme » de 4 cubes.
1. a) En utilisant $13 = 1^3 + 7^3 + 10^3 - 11^3$, donner une décomposition de 40 en « somme » de 5 cubes.
b) On admet que pour tout entier naturel n on a :
$$6n = (n + 1)^3 + (n - 1)^3 - n^3 - n^3.$$
En déduire une décomposition de 48 en « somme » de 4 cubes, puis une décomposition de 40 en « somme » de 5 cubes, différente de celle donnée en **1. a)**
2. Le nombre 40 est une « somme » de 4 cubes : $40 = 4^3 - 2^3 - 2^3 - 2^3$.
On veut savoir si 40 peut être décomposé en « somme » de 3 cubes.
a) Recopier et compléter sans justifier :

$n \equiv \ldots$ (9)	0	1	2	3	4	5	6	7	8
$n^3 \equiv \ldots$ (9)									

b) En déduire que, pour tout $n \in \mathbb{N}$, n^3 est congru à 0, 1, ou –1 modulo 9.
Prouver alors que 40 ne peut pas être décomposé en « somme » de 3 cubes.

D'après Bac Pondichéry 2019

Nombres premiers

- Un nombre premier p est un entier naturel qui admet **exactement 2 diviseurs :** 1 et lui-même.
- Il est bon de mémoriser les quinze premiers de ces nombres : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.
- Il y existe une **infinité** de nombre premiers.

(On peut le démontrer par l'absurde en supposant un nombre fini de nombres premiers).

Test de primalité ou critère d'arrêt

- Tout entier naturel $n \geqslant 2$ admet un diviseur premier

Si n n'est pas premier alors, il admet un diviseur premier p tel que :

$$2 \leqslant p \leqslant \sqrt{n}.$$

- Pour montrer qu'un nombre est premier, on utilise la contraposée :

Si n n'admet pas de diviseur premier $p \leqslant \sqrt{n}$, alors n est premier.

Théorème de Gauss appliqué aux nombres premiers

- **Si p premier divise ab alors p divise a ou b.**
- Si p divise un produit de facteurs premiers alors p est l'un d'entre d'eux.

Crible d'Ératosthène

Pour obtenir une liste de nombres premiers inférieurs à un entier n donné, on procède par **élimination des multiples stricts**, par ordre croissant des nombres sur la liste des entiers de 2 à n. Les entiers restants sont alors premiers.

	(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~~	~~100~~

Théorème fondamental de l'arithmétique

Tout entier naturel $n \geqslant 2$ peut se décomposer de façon unique en produit de facteurs premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$$

Diviseurs

- Tout diviseur d de $n \geqslant 2$ admet la décomposition :

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_m^{\beta_m} \quad \text{avec } 0 \leqslant \beta_i \leqslant \alpha_i.$$

- Le nombre N de diviseurs de n vaut :

$$N = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_m + 1)$$

Petit théorème de Fermat

- Soit un nombre premier p et un naturel a **non multiple de p** alors : $a^{p-1} \equiv 1\ (p)$.
- Si a est un **entier naturel quelconque**, on a : $a^p \equiv a\ (p)$.

Préparer le BAC — Je me teste

Je dois être capable de…		Parcours d'exercices
Déterminer si un nombre est premier	Méthode 1	1, 2, 39, 40
Utiliser le théorème de Gauss appliqué aux nombres premiers	Méthode 2	3, 4, 47, 48
Décomposer un nombre en produit de facteurs premiers	Méthode 3	5, 6, 51, 52
Trouver tous les diviseurs d'un entier	Méthode 4	10, 11, 60, 61
Appliquer le petit théorème de Fermat	Méthode 5	12, 13, 66, 67
Déterminer un entier conditionné par le nombre de ses diviseurs	Méthode 6	14, 15, 73, 74
Travailler modulo p avec p premier	Méthode 7	21, 22, 80, 81

EXOS
QCM interactifs
lienmini.fr/maths-e05-07

QCM

Pour les exercices suivants, choisir la (les) bonnes réponse(s).

	A	B	C	D
105 Lequel parmi ces nombres n'est pas premier ?	227	379	221	131
106 Pour établir la liste des nombres premiers inférieurs ou égaux à 4 000 à l'aide du crible d'Ératosthène, on raye les multiples des nombres premiers jusqu'à :	61	67	100	4 000
107 Le plus petit entier possédant 8 diviseurs est :	2^7	30	24	18
108 On considère le nombre $N = n + (n + 2) + n(n + 2)$ avec $n \in \mathbb{N}$. Le nombre N est premier :	si n est impair.	pour aucune valeur de n.	pour les 4 premières valeurs impaires de n.	si n est premier.
109 p premier supérieur à 2 différent de 7. L'entier $N = 7^{p-1} - 1$ est :	toujours divisible par p mais pas par $2p$.	toujours divisible par $2p$.	parfois divisible par $2p$.	jamais divisible par p.
110 Les entiers n et $(n + 2)$ sont premiers et $n > 3$. On peut avoir :	$n \equiv 2\ (3)$	$n \equiv 1\ (3)$	$n \equiv 2\ (6)$	$n^2 - 1 \equiv 0\ (6)$
111 Tout nombre premier strictement supérieur à 2 peut s'écrire :	$3k - 1$ ou $3k + 1$ avec $k \in \mathbb{N}^*$.	$4k - 1$ ou $4k + 1$ avec $k \in \mathbb{N}^*$.	$6k - 1$ ou $6k + 1$ avec $k \in \mathbb{N}^*$.	$6k - 3$ ou $6k + 3$ avec $k \in \mathbb{N}^*$.
112 Soit $x, y \in \mathbb{N}$. Le système $\begin{cases} x^2 - y^2 = 5\,440 \\ \text{PGCD}(x, y) = 8 \end{cases}$	possède un couple solution.	possède quatre couples solutions.	n'a pas de couple solution.	possède deux couples solutions.

113 Critère d'arrêt

Déterminer à l'aide du critère d'arrêt si les nombres suivants sont premiers ou non.

a) 157
b) 243
c) 427
d) 509
e) 671.

Méthode 1 p. 137

114 Décomposition

Décomposer en produit de facteurs premiers 5 940 et 27 720.
Combien ont-ils de diviseurs ?

Méthode 4 p. 141

115 Trouver un entier

1. Donner la décomposition en facteurs premiers de 2 016.
2. Déterminer, en expliquant la méthode choisie, la plus petite valeur de l'entier naturel k pour laquelle k^6 est un multiple de 2 016.

Méthode 4 p. 141

116 PGCD

Démo

Montrer qu'un nombre p est un nombre premier si, et seulement si, p est premier avec chacun des entiers 2, 3, 4, … , $p - 1$.

Méthode 2 p. 137

117 Nombre de diviseurs (1)

Un nombre n s'écrit $2^\alpha 3^\beta$.
Le nombre de diviseurs de $36n$ est le triple du nombre de diviseurs de n
Déterminer les valeurs de n possibles.

Méthode 6 p. 142

118 Nombre de diviseurs (2)

1. Décomposer 2 268 en produit de facteurs premiers.
En déduire les nombres de diviseurs de 2 268.
2. Déterminer les entiers naturels a et b avec $a < b$ tels que $ab = 2\,268$ et ayant exactement six diviseurs communs.

Méthode 6 p. 142

119 Logique

Pour chacune des propositions suivantes, en justifiant, préciser si elle est vraie ou fausse puis énoncer sa réciproque en indiquant la véracité de celle-ci.
Proposition 1 Si n divise a^2, alors n divise a.
Proposition 2 Si n est premier, alors n est impair.
Proposition 3 Si p et q sont deux nombres premiers distincts, alors p et q sont premiers entre eux.
Proposition 4 Si p premier divise le produit ab, alors p divise a ou p divise b.
5. Proposition 5 p est un nombre premier Si $a \equiv p\ (p)$, alors a est premier.

Méthode 1 Méthode 2 p. 137

120 Autour de Fermat

1. Soit p un nombre premier impair.
a) Montrer qu'il existe un entier naturel k, non nul, tel que $2^k \equiv 1\ (p)$.
b) Soit k un entier naturel non nul tel que $2^k \equiv 1\ (p)$ et soit n un entier naturel.
Montrer que, si k divise n, alors $2^n \equiv 1\ (p)$.
c) Soit b tel que $2^b \equiv 1\ (p)$, b étant le plus petit entier non nul vérifiant cette propriété.
Montrer, en utilisant la division euclidienne de n par b, que si $2^n \equiv 1\ (p)$, alors b divise n.
2. Soit q un nombre premier impair et le nombre $A = 2^q - 1$.
On prend pour p un facteur premier de A.
a) Justifier que : $2^q \equiv 1\ (p)$.
b) Montrer que p est impair.
c) Soit b tel que $2^b \equiv 1\ (p)$, b étant le plus petit entier non nul vérifiant cette propriété.
Montrer, en utilisant **1.** que b divise q. En déduire que $b = q$.
d) Montrer que q divise $(p - 1)$, puis montrer que $p \equiv 1\ (2q)$.
3. Soit $A_1 = 2^{17} - 1$.
Voici la liste des nombres premiers inférieurs à 400 et qui sont de la forme $34m + 1$, avec m entier non nul : 103, 137, 239, 307.
En déduire que A_1 est premier.

Méthode 5 p. 141

121 Résolution d'équations

1. Résoudre l'équation dans $\mathbb{N}^2$:

$$x^2 - y^2 = 11.$$

2. D'une façon plus générale, soit p un nombre premier.
Résoudre l'équation dans $\mathbb{N}^2$:

$$x^2 - y^2 = p.$$

122 Coordonnées entières des points d'un plan de l'espace

1. a) Soit p un entier naturel.
Montrer qu'un seul des trois nombres p, $(p + 10)$ et $(p + 20)$ est divisible par 3.
b) Les entiers naturels a, b et c sont dans cet ordre les trois premiers termes d'une suite arithmétique de raison 10.
Déterminer ces trois nombres sachant qu'ils sont premiers.
2. Soit E l'ensemble des triplets d'entiers relatifs $(u\,;v\,;w)$ tels que :

$$3u + 13v + 23w = 0.$$

a) Montrer que pour un tel triplet $v \equiv w\ (3)$.
b) On pose $v = 3k + r$ et $w = 3k' + r$ où k, k' et r sont des entiers relatifs et $0 \leqslant r \leqslant 2$.
Montrer que les éléments de E sont de la forme :

$$(-13k - 23k' - 12r\,,\ 3k + r\,,\ 3k' + r).$$

Méthode 1 p. 137

Exercices vers le supérieur

123 Nombres premiers

Démo

Pour $n \in \mathbb{N}^*$, on note p_n le n-ième nombre premier :

$$p_1 = 2, p_2 = 3, \ldots$$

Montrer que pour tout entier $n \geqslant 2$:

$$p_{n+1} < p_1 \times p_2 \times \ldots \times p_n.$$

124 PGCD

Trouver le PGCD de $(3^{37} - 3)$ et de 1 221.

125 Autre démonstration du petit théorème de Fermat

Démo

1. Soit p un entier tel que $p \geqslant 2$.

Montrer que pour tout k avec $1 \leqslant k \leqslant p - 1$:

$$k \times \binom{p}{k} = p \times \binom{p-1}{k-1}$$

Dans la suite p est un nombre premier.

2. Montrer que p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p - 1$.

3. À l'aide de la formule du binôme, déduire que pour a et b entiers :

$$(a + b)^p \equiv a^p + b^p \ (p).$$

4. Démontrer par récurrence que :

$$\text{pour tout } n \in \mathbb{N}^*,\ n^p \equiv n \ (p)$$

et retrouver ainsi le théorème de Fermat.

126 Nombres premiers de Sophie Germain

Sophie Germain

1. Un nombre premier p de Sophie Germain est tel que p et $2p + 1$ sont premiers.

• Le nombre $2p + 1$ est alors appelé nombre premier sûr.

• Une suite $(p\ ,\ 2p + 1\ ,\ 2(2p + 1) + 1\ ,\ \ldots)$ de nombres premiers de Sophie Germain est appelée une chaîne de Cunningham.

a) Déterminer les nombres premiers de Sophie Germain inférieurs à 100.

b) Démontrer que 239 est un nombre premier de Sophie Germain et que 227 est un nombre premier sûr.

c) Déterminer une chaîne de Cunnigham de 5 termes.

2. a) Montrer que, pour tout entier, on a l'égalité dite de « Sophie Germain » :

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

b) n est un entier naturel, pour quelle(s) valeur(s) de n, $n^4 + 4$ est-il premier ?

c) Démontrer que $4^{545} + 545^4$ n'est pas premier.

3. Factoriser $n^4 + n^2 + 1$.

Pour quelle(s) valeur(s) de n, $n^4 + n^2 + 1$ est-il premier ?

127 Déterminer un nombre

Un professeur de mathématiques donne l'énoncé suivant : « Déterminer un entier naturel n ayant 9 diviseurs s'écrivant sous la forme $n = 39p + 1$ où p est un nombre premier. »

En analysant l'ensemble des cas possible donner toutes les valeurs possibles de l'entier n.

128 Problème de lampes

On considère 1 000 lampes numérotées de 1 à 1 000 qui peuvent être allumées ou éteintes. Une lampe change d'état lorsqu'elle passe d'éteinte à allumée et réciproquement. Au départ toutes les lampes sont éteintes et l'on effectue les 1 000 étapes suivantes.

Étape 1 On allume toutes les lampes.

Étape 2 Seules les lampes où le numéro est multiple de 2 changent d'état.

Étape 3 Seules les lampes où le numéro est multiple de 3 changent d'état.

Ainsi de suite jusqu'à :

Étape 1 000 Seules les lampes où le numéro est multiple de 1 000 changent d'état.

Quels sont les numéros des lampes qui sont allumées après ces 1 000 étapes ?

129 L'âge du capitaine

Le capitaine dit à son fils :

« La cabine n° 1 abrite M. Dupont et ses deux filles. Le produit de leurs trois âges est 2 450 et la somme de leurs trois âges est égale à 4 fois le tien. Peux-tu trouver les âges des trois passagers ? »

Après un instant, le fils répond : « Non, il me manque une donnée. »

Le capitaine ajoute alors : « Je suis plus âgé que M. Dupont. »

Le fils du capitaine en déduit alors les trois réponses.

Quel est l'âge du capitaine ? de son fils ? de M. Dupont ? des deux filles ?

130 Le théorème de Wilson

Démo

Soit un nombre premier $p > 3$ et l'ensemble des naturels $A = [2\ ;\ p - 2]$.

1. Montrer que pour tout $x \in A$, p ne divise pas $x^2 - 1$.

2. a) Soit $x \in A$, montrer qu'il existe $u \in \mathbb{Z}$ tel que : $xu \equiv 1 \ (p)$.

b) En déduire l'existence d'un unique entier $r \in A$ distinct de x tel que $xr \equiv 1 \ (p)$.

c) Établir que : $2 \times 3 \times \ldots \times (p - 2) \equiv 1 \ (p)$ puis que $(p - 1)! \equiv -1 \ (p)$.

3. Ce résultat est-il encore vrai pour $p = 2$ et $p = 3$?

4. Réciproquement, soit p un entier $(p \geqslant 2)$ tel que : $(p - 1) \equiv -1 \ (p)$.

En raisonnant par l'absurde, montrer que p est premier.

5. En déduire le théorème de Wilson : « Un entier naturel n est premier si, et seulement si, $(n - 1)! + 1$ est divisible par n ».

6. Application : montrer que 13 est premier à l'aide du théorème de Wilson.

Ce théorème est-il judicieux comme test de primalité ?

131 Ristournes

Un magasin informatique effectue trois remises successives sur un ordinateur qui coûtait 300 € et qu'il vend alors 222,87 €.

Quels sont les pourcentages des trois remises sachant qu'elles s'expriment avec des nombres entiers ?

132 Tableau infini

On considère le tableau composé d'une infinité de lignes : L_1, L_2, …, L_k, … où la ligne L_k est formée des termes de la suite arithmétique de premier terme $k(k+1)$ et de raison $k+(k+1)$.

L_1	2	5	8	11	14	…
L_2	6	11	16	21	26	…
L_3	12	19	26	33	40	…
…	…	…	…	…	…	…

Soit n un entier naturel non nul.

1. Montrer que n est dans le tableau si, et seulement si, il existe $k \in \mathbb{N}^*$ et $N \in \mathbb{N}$ tels que :

$$n = (2k+1)N + k(k+1).$$

2. En déduire que $(4n+1)$ est premier si, et seulement si, n n'est pas dans le tableau.

133 Décomposition d'un nombre de 17 chiffres

Le nombre 333 667 est un nombre premier.

1. Décomposer 1 001 001 en produit de facteurs premiers.

2. a) Calculer 11^2, 111^2, 1111^2.

b) Conjecturer la valeur de $111\,111\,111^2$.

c) Démontrer cette conjecture.

3. Décomposer en produit de facteurs premiers, l'entier :

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

134 Nombre de Mersenne divisible par 343

1. Vérifier que $(2^{21}-1)$ est divisible par 49.

2. Soit $x \in \mathbb{N}$ et $A = (1+x)^7 - (1-7x)$.
Montrer que le nombre A est divisible par x^2.

3. En déduire que $(2^{147}-1)$ est divisible par 343.

135 Décomposition impossible

1. On suppose qu'il existe des entiers naturels non nuls m et n tels que :

$$(4m+3)(4n+3) = 4a^2 + 1.$$

a) Soit p un nombre premier divisant $(4m+3)$.
Montrer que p est impair et que :

$$(2a)^{p-1} \equiv (-1)^{\frac{p-1}{2}} (p).$$

b) À l'aide du théorème de Fermat, montrer que $p \equiv 1\ (4)$.

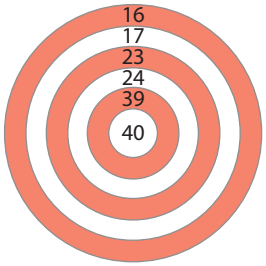
c) En utilisant la décomposition de $(4m+3)$ en produit de facteurs premiers, obtenir une contradiction.

2. Soit $a \geqslant 1$. Montrer que le nombre $4a^2+1$ n'est pas premier si, et seulement si, il existe des entiers naturels m et n non nuls tels que :

$$4a^2 + 1 = (4m+1)(4n+1).$$

136 Le compte est bon

Combien faut-il de flèches pour faire un score de 100 points sur la cible ?



137 Nombres de Carmichaël


Carmichaël

Un nombre de Carmichaël est un entier n non premier qui vérifie la propriété suivante :
« Pour tout entier a premier avec n, l'entier n est un diviseur de $(a^n - a)$. »

1. a) Soit $n = 561$. Décomposer n en produit de facteurs premiers.

b) Vérifier que pour tout facteur premier p de n, $(p-1)$ divise $(n-1)$.

c) En déduire que pour tout entier a premier avec n, on a : $a^{n-1} \equiv 1\ (n)$ et que n est un nombre de Carmichaël.

2. Reprendre les mêmes questions avec $n = 1\,105$.

3. En quoi ces deux exemples montrent que la réciproque du petit théorème de Fermat n'est pas vérifiée ?

Travaux pratiques

TICE 50 min Calculer Chercher Raisonner

1 Nombres générant des nombres premiers

A ▸ Les nombres de Mersenne

On appelle nombre de Mersenne, les nombres M_n de la forme :

$$M_n = 2^n - 1 \text{ avec } n \in \mathbb{N}^*.$$

1. Calculer les six premiers nombres de Mersenne.
Quels sont ceux qui sont premiers ?

2. Soit n un entier naturel non nul et a un entier.

a) Montrer la factorisation standard :

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

b) En déduire que si d est un diviseur de n, M_n est divisible par $2^d - 1$.

3. Montrer que si M_n est premier alors n est premier.
La réciproque est-elle vraie ?
Dans le cas où la réponse est négative, déterminer un contre-exemple.

4. Soit a et n deux entiers tels que : $a \geqslant 2$ et $n \geqslant 2$.
Montrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.

5. Dans le but de déterminer un nombre de Mersenne premier, on veut montrer que si n est un nombre premier impair, alors tout diviseur premier p de M_n est de la forme $p = 2kn + 1$.
Soit E l'ensemble des nombres s tels que $2^s \equiv 1\ (p)$.
Soit s_0 son plus petit élément.

a) On divise un élément s de E par s_0 :

$$s = s_0 q + r \text{ avec } 0 \leqslant r < s_0.$$

Montrer que $r = 0$.

b) En déduire que s_0 divise n puis que $s_0 = n$.

c) À l'aide du petit théorème de Fermat, montrer que n divise $p - 1$ puis que $2n$ divise $p - 1$.
En déduire la forme du diviseur premier p de M_n.

d) Application : trouver un diviseur premier à M_{23}.

Remarque
Le fait que les nombres de Mersenne génèrent des nombres premiers est utile pour en déterminer de plus grands, cependant on doit tester avec n premier si M_n est premier.
Le plus grand nombre premier connu en 2018 était $M_{82\,589\,933}$ qui possède plus de 24 millions de chiffres !

B ▸ Les nombres de Fermat

1. a) Montrer que pour tout $x \in \mathbb{N}$ et $k \in \mathbb{N}^*$:

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

b) Montrer que si m est impair alors, $2^m + 1$ n'est pas premier.

c) Montrer que si m est un entier possèdant un diviseur strict impair alors, $2^m + 1$ est composé.

d) En déduire que les seuls nombres premiers de la forme $2^m + 1$ sont de la forme $2^{2^n} + 1$.

2. On appelle nombre de Fermat, un nombre noté F_n tel que :

$$F_n = 2^{2^n} + 1 \text{ avec } n \in \mathbb{N}.$$

a) Calculer F_0, F_1, F_2, F_3, F_4 et vérifier qu'ils sont tous premiers.

b) Fermat pensait que F_5 était également premier.
Qu'en pensez vous ?
On pourra utiliser un algorithme donnant la primalité d'un nombre.

3. Vérifier que pour tout $n \in \mathbb{N}$:

$$F_{n+1} = (F_n - 1)^2 + 1.$$

En déduire PGCD(F_n , F_{n+1})

4. Montrer par récurrence que tout nombre de Fermat pour $n \geqslant 2$ a une écriture décimale se terminant par 7.

TICE 50 min Communiquer Raisonner Modéliser

2 Le système RSA

Le nom du système de cryptage RSA provient des initiales des noms de ses inventeurs américains en 1977 : Ronald **R**ivest (informaticien), Adi **S**hamir (informaticien) et Leaonard **A**dleman (mathématicien).

A ▸ Arithmétique du système RSA

Soit p et q deux nombres premiers impairs distincts.
On pose $n = pq$ et $m = (p - 1)(q - 1)$ et on désigne par e un entier tel que : $1 < e < m$ avec e et m premier entre eux.

1. Montrer qu'il existe un entier d unique tel que : $1 \leqslant d < m$ et $ed \equiv 1\ (m)$.

2. Prouver que pour tout $a \in \mathbb{N}$, $a^{ed} \equiv a\ (n)$.

3. On choisit $p = 3$, $q = 11$ et $e = 7$. Calculer d

B ▸ Envoi d'un message

Alice veut transmettre un message à Bob.
Pour cela Bob diffuse à tout le monde (donc à Alice) les nombres n et c (clé publique).
Il garde pour lui les nombres p et q (clé privé) qui lui permettent de calculer d et déchiffrer un message.
Bob rend publique : $n = 33$ et $e = 7$.
Alice veut transmettre à Bob le mot : SALUT.
Alice transforme les 5 lettres à l'aide du tableau :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Alice code ensuite ces nombres avec la fonction « trappe » de Bob : $b = f_B(a) \equiv a^e\ (n)$.
Ainsi pour la lettre S : $a_1 = 18 \rightarrow 18^7 \equiv 6\ (33)$, on obtient alors $b_1 = 6$.

1. Rentrer cette fonction en **Python** puis vérifier qu'Alice envoie à Bob les nombres suivants :
06 – 00 – 11 – 26 – 13.

2. Bob décode alors ces nombres avec sa fonction « trappe inverse » : $a = f_B^{-1}(b) \equiv b^d\ (n)$
Expliquer pourquoi cette fonction inverse permet de déchiffrer le message d'Alice.

3. La clé privée de Bob est $p = 3$ et $q = 11$.
Il reçoit un deuxième message d'Alice avec les nombres : 14 – 20 – 08 – 12 – 02 – 09 – 00 – 01 – 11 – 16.

Rentrer la fonction inverse en **Python** puis décoder le message d'Alice.

C ▸ Authentification

Le but de cette partie est de montrer comment Bob peut être sûr de recevoir un message d'Alice.
Alice dispose également d'une clé publique (fonction trappe f_A) et d'une clé privée (fonction trappe inverse f_A^{-1}).
Alice envoie à Bob un message contenant :
- ce qu'elle a à lui dire,
- une double signature : A, f_A^{-1}(A).

Comment Bob peut-il s'assurer que le message vient bien d'Alice ?

Remarque
La clé publique (n , e) permet donc à « tout public » de transmettre un message à Bob. La clé personnelle (p, q) n'est connue que de Bob et lui permet d'être le seul à pouvoir déchiffrer le message en calculant d.
La sécurité du système réside dans la construction de nombre premier p et q très grands (300 chiffres) et la difficulté de décomposer le nombre n en produit de 2 nombres premiers.

PARTIE 3

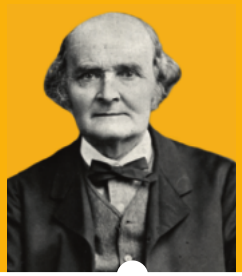
Graphes et matrices

Leonhard Euler (1707-1783)

En 1736, Euler résout le problème des sept ponts de Königsberg. En 1771, Vandermonde étudie le problème du cavalier dans ses *Remarques sur des problèmes de situation*.

↪ Dicomaths p. 238

Arthur Cayley (1821-1895)



Au XIX^{e} siècle, Cayley est le premier à multiplier des matrices et Hamilton découvre les quaternions. Ils sont à l'origine du théorème de Cayley-Hamilton.

↪ Dicomaths p. 237

James Joseph Sylvester (1814-1897)

En 1850, Sylvester introduit le terme « matrice ». Il étudie les formes quadratiques, les invariants et les déterminants.

↪ Dicomaths p. 241

Mon parcours au lycée

Dans les classes précédentes…

• J'ai étudié les probabilités conditionnelles et certains algorithmes.

En Terminale…

• Je vais découvrir les matrices et leurs applications notamment en théorie des graphes.

Ferdinand Frobenius (1849-1917)

En 1878, Frobenius donne la première démonstration complète du théorème de Cayley-Hamilton. À la même époque, le mathématicien Jordan étudie les décompositions d'endomorphismes et leurs équivalents matriciels.

↪ Dicomaths p. 239

Andreï Markov (1856-1922)

En 1902, Markov introduit la notion de chaîne de Markov afin de formaliser des problèmes de cryptage, notion généralisée par Kolmogorov en 1936.

↪ Dicomaths p. 239

Lester S. Hill (1891-1961)

En 1929, le chiffrement de Hill permet de (dé)chiffrer un message par bloc de deux lettres. Par la suite, les chaînes de Markov constituent les prémisses du calcul stochastique. Elles sont également liées en physique au mouvement brownien et modèlisent des processus en dynamique des populations ou en épidémiologie.

↪ Dicomaths p. 239

Domaines professionnels

- Un·e **statisticien·ne** étudie la dynamique des déménagements des personnes d'une région.
- Un·e **concepteur·trice** de GPS utilise des algorithmes de théorie des graphes pour calculer des itinéraires.
- Un·e **organisateur·trice de tourisme** optimise les trajets lors d'un circuit touristique.
- Un·e **ingénieur·e en télécommunication** combine réseaux et intelligence artificielle pour optimiser un système de communication.
- Un·e **chercheur·se dans le domaine de l'environnement** étudie l'équilibre d'un écosystème à travers des systèmes proie-prédateur.
- Un·e **expert-comptable** peut utiliser les matrices pour étudier le bilan d'une société.