

Nombres premiers

Définition et critère d'arrêt

EXERCICE 1

Sans calculatrice, à l'aide de divisions successives et du critère d'arrêt, déterminer si les entiers suivants sont premiers ou non.

97 ; 109 ; 117 ; 271 ; 317 ; 323 ; 401 ; 419 ; 437 ; 527 ; 719

EXERCICE 2

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 ?

EXERCICE 3

Vrai-Faux

- 1) **Proposition 1 :** Il existe une valeur de $n \in \mathbb{N}$ tel que $2n^2 + n - 10$ est premier.
- 2) **Proposition 2 :** Il existe une valeur de $n \in \mathbb{N}$ tel que $2n^2 + 7n + 6$ est premier.
- 3) **Proposition 3 :** Pour $n \in \mathbb{N}$ et $n > 5$, $n^2 - 3n - 10$ n'est jamais premier.

Aide : On cherchera à factoriser les quantités.

EXERCICE 4

Soit p un nombre premier et deux entiers n_1 et n_2 tels que : $n_1 = p + 1\,000$ 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 ?

Théorème de Gauss et nombres premiers

EXERCICE 5

p est premier et $p \geq 5$.

- 1) Démontrer que $(p^2 - 1)$ est divisible par 3 et par 8.
- 2) En déduire que $(p^2 - 1)$ est divisible par 24

EXERCICE 6

p est premier et $p \geq 5$.

- 1) Démontrer que $(p^4 - 1)$ est divisible par 3 et par 5.
- 2) Démontrer que $(p^4 - 1)$ est divisible par 16.
- 3) En déduire que $(p^2 - 1)$ est divisible par 240

EXERCICE 7

$p > 3$ est un nombre premier

- 1) Quels sont les restes possibles dans la division de p par 12?
- 2) Prouver que $p^2 + 11$ est divisible par 12.

EXERCICE 8

Soit n un entier naturel supérieur ou égal à 1.

Démontrer que $(30n + 7)$ n'est pas la somme de deux nombres premiers.

EXERCICE 9

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 .

EXERCICE 10**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 :

NORMAL FLOTT AUTO RÉEL RAD MP	
$(2^{33}-1)/3$	2863311530
$(2^{33}-1)/4$	2147483648
$(2^{33}-1)/12$	715827882.6

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

- a) En quoi cette affirmation contredit le corollaire du théorème de Gauss.
 - b) Montrer que 4 ne divise pas $2^{33} - 1$.
 - c) En remarquant que $2 \equiv -1 \pmod{3}$, montrer que 3 ne divise pas $2^{33} - 1$.
- 2) a) Calculer la somme : $S = 1 + 2^3 + (2^3)^2 + (2^3)^3 + \dots + (2^3)^{10}$.
 - b) En déduire que 7 divise $2^{33} - 1$.

Décomposition**EXERCICE 11**

- 1) Décomposer en produit de facteurs premiers : 6 468 et 16 380.
- 2) En déduire $\text{pgcd}(6\,468, 16\,380)$.

EXERCICE 12

- 1) Déterminer $\text{pgcd}(8\,316, 5\,670)$ à l'aide :
 - a) d'une décomposition en facteurs premiers.

- b) de l'algorithme d'Euclide.
2) Quelle est la méthode la plus « économe » en opérations ?

EXERCICE 13

À l'aide d'une décomposition en facteurs premiers, déterminer $(a, b) \in \mathbb{N}^2$ tel que :

$$\frac{a}{b} = \frac{5\,292}{5\,5544} \text{ et } a + b = 903$$

EXERCICE 14

- 1) a) Quelle est la condition sur les puissances des facteurs premiers d'un carré parfait ?
b) Trouver un nombre de trois chiffres qui soit un carré parfait divisible par 56.
2) Trouver les diviseurs de 84, puis résoudre dans \mathbb{N} : $x(x+1)(2x+1) = 84$

EXERCICE 15

- 1) Expliquer comment procède cette fonction `decomposition(n)` en Python pour trouver la décomposition en facteurs premiers de n .
2) Expliquer l'avant dernière ligne : `L.append(n)`

```
def decomposition(n):
    d=2
    c=1
    L=[]
    while d<=sqrt(n):
        if n%d==0:
            L.append(d)
            n=int(n/d)
        else:
            d=d+c
            c=2
    L.append(n)
    return L
```

EXERCICE 16

Cet exercice a pour but de déterminer par combien de zéros se termine $1\,000!$.
On rappelle que : $1\,000! = 1 \times 2 \times 3 \times \dots \times 1\,000$.

- 1) Montrer qu'il existe $p, q \in \mathbb{N}^*$ et un entier N premier avec 10 tels que :
$$1\,000! = 2^p \times 5^q \times N$$

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.

Nombre de diviseurs**EXERCICE 17**

- 1) À l'aide d'une décomposition en facteurs premiers, déterminer le nombre de diviseurs de : 2 025 et 1 575.
2) En déduire la liste des diviseurs de 2 025 et 1 575.

EXERCICE 18

- 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.

EXERCICE 19

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

EXERCICE 20

α et β sont deux naturels et $n = 2^\alpha 3^\beta$.

Le nombre de diviseurs de n^2 est le triple du nombre de diviseurs de n .

- 1) Prouver que $(\alpha - 1)(\beta - 1) = 3$
- 2) En déduire n

EXERCICE 21

α et β sont deux naturels et $n = 2^\alpha 3^\beta$.

Le nombre de diviseurs de $18n$ est le double du nombre de diviseurs de n .

- 1) Montrer que : $18n = 2^{\alpha+1} 3^{\beta+2}$
- 2) Prouver que $\alpha(\beta - 1) = 4$
- 3) En déduire les valeurs de n possibles.

EXERCICE 22

L'entier parmi les nombres inférieurs ou égaux à 50 qui possède le plus de diviseurs en possède 10. Trouver cet entier.

EXERCICE 23

Parmi les nombres inférieurs ou égaux à 100, quatre possèdent 12 diviseurs.

- 1) Montrer qu'il existe 4 configurations pour un entier de posséder 12 diviseurs.
- 2) Trouver ces quatre entiers inférieurs à 100 parmi ces configurations.

EXERCICE 24

On cherche le plus petit entier naturel n possédant 8 diviseurs.

- 1) Montrer qu'il existe 3 configurations pour un entier de posséder 8 diviseurs.
- 2) Tester ces 3 configurations et en déduire la solution du problème.

EXERCICE 25

Parmi les nombres inférieurs ou égaux à 200, un seul possède 18 diviseurs.

- 1) Montrer qu'il existe 4 configurations pour un entier de posséder 18 diviseurs.
- 2) Trouver cet entier inférieur à 200 parmi ces configurations.

EXERCICE 26

Le produit de deux entiers naturels a et b ($a < b$) est 11 340. On note d leur pgcd.

- 1) a) Pourquoi d^2 divise-t-il 11 340?
b) Pourquoi $d = 2^\alpha \times 3^\beta$ avec $0 \leq \alpha \leq 1$ et $0 \leq \beta \leq 2$?
- 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 .

EXERCICE 27

Un entier n a 5 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 n

EXERCICE 28

Déterminer deux entiers naturels a et b tels que $a > b$, $\text{pgcd}(a, b) = 18$, et qui ont respectivement 21 et 10 diviseurs.

EXERCICE 29

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.

EXERCICE 30**Théorème d'Euclide**

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 a s'écrit $2^n(2^{n+1} - 1)$ est si $2^{n+1} - 1$ est premier, alors a est parfait ».

- 1) Trouver les quatre premiers nombres parfaits.
- 2) On pose $a = 2^n(2^{n+1} - 1)$ 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 .

Remarque : Le problème de savoir s'il existe des nombres parfaits impairs n'est toujours pas résolu.

Petit théorème de Fermat

EXERCICE 31

- 1) Montrer que pour tout $n \in \mathbb{N}$, $3^{6n} - 1$ est divisible par 7.
- 2) Soit p un nombre premier différent de 3.
Démontrer que pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est divisible par p .

EXERCICE 32

Soit $n \in \mathbb{N}$ et $a = n^5 - n$.

- 1) Montrer que a est divisible par 5.
- 2) Montrer que $a = n(n^2 - 1)(n^2 + 1)$ puis que a est divisible par 2 et 3.
Pourquoi a est-il divisible par 30?

EXERCICE 33

- 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 $4^{28} - 1$.

EXERCICE 34

Soit $n \in \mathbb{N}^*$. On note $a = n^{13} - n$.

- 1) Montrer que a est divisible par 13 et 7.
- 2) En déduire que a est divisible par 182.

EXERCICE 35

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

EXERCICE 36

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

EXERCICE 37

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 $3^p + 1$.

EXERCICE 38

- 1) Vérifier que 761 est un nombre premier.
- 2) L'entier n est un naturel composé de 760 chiffres tous égaux à 9 : $n = \underbrace{999 \dots 99}_{760 \text{ fois}}$.
 - a) Calculer $n + 1$.
 - b) Montrer que n est divisible par 761.

EXERCICE 39

- 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) De $(n^2 - 1)(n^2 + 1) = n^4 - 1$, 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.

Modulo p premier

EXERCICE 40

Soit p un nombre premier et a, b, n des entiers relatifs.

- 1) Montrer que si $na \equiv nb \pmod{p}$ avec $n \not\equiv 0 \pmod{p}$ alors : $a \equiv b \pmod{p}$.
- 2) Montrer que si a est premier avec p et n un multiple de $p - 1$ alors : $a^n \equiv 1 \pmod{p}$.
- 3) Montrer que si a est premier avec p alors il existe b tel que : $ab \equiv 1 \pmod{p}$.
En déduire que tout entier non nul $a < p$ possède un inverse inférieur à p modulo p .

EXERCICE 41

Soit a un entier naturel pair non nul. Soit p un nombre premier divisant $a^2 + 1$.

- 1) Montrer que p est de la forme $4n + 1$ ou $4n + 3$.
- 2) On suppose que p est de la forme $4n + 3$.
 - a) Montrer que p ne divise pas a .
 - b) Montrer que $(a^4)^n \times a^2 \equiv 1 \pmod{p}$.
 - c) En déduire une contradiction.
- 3) Conclure.

EXERCICE 42

Soit N un entier supérieur ou égal à 2 et a un entier naturel pair non nul.
On pose $a = N!$

- 1) Montrer qu'il existe un nombre premier p divisant $(a^2 + 1)$.
- 2) En utilisant le résultat de l'exercice précédent :

- a) Montrer que $p > 1$.
 b) Justifier qu'il existe une infinité de nombres premiers p de la forme $(4n + 1)$.

EXERCICE 43

Soit le système (S) suivant : $(S) : \begin{cases} 3x + 4y \equiv 5 \pmod{13} \\ 2x + 5y \equiv 7 \pmod{13} \end{cases}$ avec $(x, y) \in \mathbb{Z}^2$

- 1) Justifier que (S) est équivalent à : $\begin{cases} 3x + 4y \equiv 5 \pmod{13} \\ 7y \equiv 11 \pmod{13} \end{cases}$
 2) Déterminer $k_1, k_2 \in \llbracket 0, 12 \rrbracket$ tels que : $7k_1 \equiv 1 \pmod{13}$ et $3k_2 \equiv 1 \pmod{13}$.
 3) En déduire les solutions du système (S) .

EXERCICE 44

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

$$M = 5 \times 7 \times 11 \times \cdots \times q$$

On pose : $N = 2^2 \times M + 3$.

- 1) a) Montrer que N est impair.
 b) Montrer que $N \not\equiv 0 \pmod{3}$.
 2) Soit p un nombre premier divisant N .
 a) Montrer que $p > q$.
 b) Montrer que : $p \equiv 1 \pmod{4}$ ou $p \equiv 3 \pmod{4}$.
 3) Soit $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$ la décomposition de N en facteurs premiers.
 a) Montrer par l'absurde qu'il existe un facteur premier p_i avec $i \in \llbracket 1, r \rrbracket$ tel que : $p_i \equiv 3 \pmod{4}$.
 b) Déduire qu'il existe une infinité de nombres premiers de la forme $(4n + 3)$.

EXERCICE 45

Soit $A = \llbracket 1, 46 \rrbracket$.

- 1) On considère l'équation : $(E) : 23x + 47y = 1$ avec $x, y \in \mathbb{Z}$.
 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 x appartenant à A tel que $23x \equiv 1 \pmod{47}$.
 2) Soit a et b deux entiers relatifs.
 a) Montrer que si $ab \equiv 0 \pmod{47}$ alors $a \equiv 0 \pmod{47}$ ou $b \equiv 0 \pmod{47}$.
 b) En déduire que si $a^2 \equiv 1 \pmod{47}$ alors $a \equiv 1 \pmod{47}$ ou $a \equiv -1 \pmod{47}$.
 3) a) Montrer que pour tout p de A , il existe un entier relatif q tel que $pq \equiv 1 \pmod{47}$.
 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 $p \times p^{-1} \equiv 1 \pmod{47}$.
 b) Quels sont les entiers p de A qui vérifient $p = p^{-1}$?
 c) Montrer que $46! \equiv 1 \pmod{47}$.

Triplets pythagoriciens

EXERCICE 46

Soit p un nombre premier. On se propose d'étudier l'existence de couples (x, y) d'entiers naturels non nuls vérifiant l'équation : (E) $x^2 + y^2 = p^2$.

- 1) On pose $p = 2$. Montrer que l'équation (E) est sans solution.
- 2) On suppose que $p \neq 2$ et que $(x; y)$ est solution de l'équation (E).
 - a) Montrer que x et y sont de parités différentes.
 - b) Montrer que x et y ne sont pas divisible par p .
 - c) En déduire que x et y sont premiers entre eux.
- 3) On suppose que p est une somme de deux carrés non nuls, c'est à dire que : $p = u^2 + v^2$ où u et v sont deux entiers naturels strictement positifs.
 - a) Vérifier que le couple $(|u^2 - v^2|, 2uv)$ est solution de (E).
 - b) Donner une solution de (E) lorsque que $p = 5$ puis lorsque $p = 13$.
- 4) On se propose enfin de vérifier sur deux exemples, que l'équation (E) est impossible lorsque p n'est pas la somme de deux carrés.
 - a) $p = 3$ et $p = 7$ sont-ils la somme de deux carrés ?
 - b) Démontrer que $x^2 + y^2 = 9$ et $x^2 + y^2 = 49$ n'admettent pas de solutions.

EXERCICE 47

Un TP, triplet pythagoricien, est un triplet $(x, y, z) \in (\mathbb{N}^*)^3$ tels que $x^2 + y^2 = z^2$. Ainsi $(3, 4, 5)$ est un TP car $3^2 + 4^2 = 5^2$.

Partie A : généralités

- 1) Démontrer que, si (x, y, z) est un TP, et p un entier naturel non nul, alors le triplet (px, py, pz) est lui aussi un TP.
- 2) Démontrer que, si (x, y, z) est un TP, alors les entiers naturels x, y et z ne peuvent pas être tous les trois impairs.
- 3) On admet que tout $n \in \mathbb{N}^*$ peut s'écrire sous la forme d'un produit unique d'une puissance de 2 par un entier impair : $n = 2^\alpha \times k$ où $\alpha, k \in \mathbb{N}$ et k impair. Par exemple : $9 = 2^0 \times 9$, et $120 = 2^3 \times 15$.
 - a) Donner la décomposition de l'entier 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 puissances de 2 les 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 (x, z) tels que $2x^2 = z^2$.
 - d) En déduire qu'un TP est formé de trois naturels x, y, z deux à deux distincts.

Partie B : recherche d'un TP contenant 2015

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

- 1) Décomposer 2 015 en produit de facteurs premiers puis, en utilisant le TP(3,4,5), déterminer un TP de la forme $(x, y, 2\,015)$.
- 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 $(2\,015, y, z)$.
- 3) a) En remarquant que $403^2 = 169 \times 961$, déterminer un couple (x, z) tels que : $z^2 - x^2 = 403^2$, avec $x < 403$.
b) En déduire un TP de la forme $(x, 2\,015, z)$.

Nombres premiers et suites

EXERCICE 48

On considère la suite (u_n) définie sur \mathbb{N}^* par : $u_n = 2^n + 3^n + 6^n - 1$.

- 1) Calculer les six premiers termes de la suite.
- 2) Montrer que, pour tout $n \in \mathbb{N}^*$, u_n est pair.
- 3) Montrer que, pour tout $n \in \mathbb{N}^*$ pair, 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 : $6 \times 2^{p-2} \equiv 3 \pmod{p}$ et $6 \times 3^{p-2} \equiv 2 \pmod{p}$.
 - b) En déduire que $6u_{p-2} \equiv 0 \pmod{p}$.
- 6) Le nombre p appartient-il à l'ensemble (E)?

EXERCICE 49

On considère la suite (u_n) définie sur \mathbb{N} par :
$$\begin{cases} u_0 = 1 \\ u_{n+1} = 10u_n + 21 \end{cases}$$

- 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 $n \in \mathbb{N}$, u_n n'est divisible ni par 2, ni par 3, ni par 5.
- 5) a) Démontrer que, pour tout $n \in \mathbb{N}$: $3u_n \equiv 4 - (-1)^n \pmod{11}$.
b) En déduire que, pour tout $n \in \mathbb{N}$, u_n n'est pas divisible par 11.
- 6) a) Démontrer l'égalité : $10^{16} \equiv 1 \pmod{17}$.
b) En déduire que, pour tout $k \in \mathbb{N}$, u_{16k+8} est divisible par 17.

EXERCICE 50

- 1) Calculer :
 - a) $(1 + \sqrt{6})^2$
 - b) $(1 + \sqrt{6})^4$
 - c) $(1 + \sqrt{6})^6$
 d) Décomposer en produit de facteurs premiers 847 et 342.
Que peut-on en déduire?
- 2) Soit $n \in \mathbb{N}^*$. On note a_n et b_n les entiers tels que : $(1 + \sqrt{6})^n = a_n + b_n\sqrt{6}$.
 - a) Que valent a_1 et b_1 ? D'après 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 $a_{n+1} + b_{n+1}$.
En déduire que, quel que soit $n \in \mathbb{N}^*$, 5 ne divise pas $a_n + b_n$.
 - d) Démontrer que, si a_n est premier avec b_n , alors a_{n+1} est premier avec b_{n+1} .
En déduire que, quel que soit $n \in \mathbb{N}^*$, a_n est premier avec b_n .

Nombres premiers et produit de nombres premiers

EXERCICE 51

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.

EXERCICE 52

On suppose que 250 507 n'est pas premier.

On se propose de chercher des couples $(a, b) \in \mathbb{N}^2$ 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 de n^2 modulo 9.
 - b) Sachant que (E) est vérifiée, déterminer les restes modulo 9 de $a^2 - 250\,507$.
 - c) Montrer que les restes modulo 9 de a sont 1 ou 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 3) une écriture de 250 507 en un produit deux facteurs.
 - b) Cette écriture est-elle unique?

EXERCICE 53

On recherche 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 $6 \times 104 < N < 8 \times 104$.
Donner les valeurs pour p_2 et en déduire les valeurs de N correspondantes.

Aide : 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

Nombres premiers et équations

EXERCICE 54

- 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 ?
- Montrer que 401 est premiers puis résoudre dans \mathbb{N}^2 : $x^2 - y^2 = 401$.

EXERCICE 55

Le but de cet exercice est de trouver $x \in \mathbb{Z}$, solutions de : (E) : $x^2 + x - 2 \equiv 0 \pmod{13}$.

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

EXERCICE 56

Le but de cet exercice est de trouver $x \in \mathbb{Z}$, solutions de (E) : $x^2 - 2x + 2 \equiv 0 \pmod{17}$

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

EXERCICE 57

- Montrer que pour tous réels x et y , on a : $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$.
- Résoudre alors dans \mathbb{N}^2 l'équation : $x^3 - y^3 = 127$.

EXERCICE 58

- Décomposer en produit de facteurs premiers 8 633.
- Résoudre dans \mathbb{N}^2 , l'équation : $x^2 - 4y^2 = 8 633$.

Réciproque du théorème de Fermat

EXERCICE 59

Nombres de Poulet

Soit $n \in \mathbb{N}^*$, un entier impair tel que : $2^{n-1} \not\equiv 1 \pmod{n}$.

- Montrer que n n'est pas premier.
- 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.
- 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 $2^{n-1} \not\equiv 1 \pmod{n}$, « n n'est pas premier »,
 - si $2^{n-1} \equiv 1 \pmod{n}$, « n est premier ».
 - Quelle est la probabilité d'énoncer un résultat faux ?
 - Quelle est la probabilité que le nombre soit premier sachant qu'il a été annoncé comme tel ?

EXERCICE 60**Nombres de Carmichael**

Un nombre de Carmichael est un entier n non premier qui vérifie la propriété : « 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 : $a^{n-1} \equiv 1 \pmod{n}$ et que n est un nombre de Carmichael.
- 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 ?

Nombres de Mersenne et de Fermat**EXERCICE 61****Nombres de Mersenne bis**

Un nombre de Mersenne M_n est de la forme $M_n = 2^n - 1$ avec $n \in \mathbb{N}^*$.

On a montré que si M_n est premier alors n est premier et que la réciproque est fausse.

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 : $2s \equiv 1 \pmod{p}$.

Soit s_0 son plus petit élément.

- 1) On divise s par s_0 : $s = s_0q + r$ avec $0 \leq r < s_0$. Montrer que $r = 0$.
- 2) En déduire que s_0 divise n puis que $s_0 = n$.
- 3) 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 .
- 4) Application : trouver un diviseur premier à M_{23} .

EXERCICE 62**Nombres de Fermat**

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

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

- b) Montrer que si m est impair alors, $2^m + 1$ n'est pas premier.
- c) Montrer que si m est un entier possédant un diviseur strict impair alors, $2^m + 1$ n'est pas premier.
- 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 : $F_n = 2^{2^n} + 1$.
 - 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.
 - c) Vérifier que pour tout $n \in \mathbb{N}$: $F_{n+1} = (F_n - 1)^2 + 1$. En déduire $\text{pgcd}(F_n, F_{n+1})$
- 3) Montrer par récurrence que tout nombre de Fermat pour $n \geq 2$ a une écriture décimale se terminant par 7.

Le système RSA

EXERCICE 63

Le nom du système de cryptage RSA provient des initiales des noms de ses inventeurs américains en 1977 : Ronald Rivest (informaticien), Adi Shamir (informaticien) et Leonard Adleman (mathématicien).

Partie 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 e tel que : $1 < e < m$ avec e premier avec m .

- 1) Montrer qu'il existe un entier d unique tel que : $1 \leq d < m$ 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

Partie 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 e (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 envoyer à Bob le mot : SALUT. Elle transforme les 5 lettres en nombres :

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 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 avec sa fonction « trappe inverse » : $a = f_B^{-1}(b) \equiv b^d (n)$
Expliquer pourquoi cette fonction f_B^{-1} 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.

Partie C Authentification

Le but 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 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.

Problèmes

EXERCICE 64

Une boîte, en forme de pavé droit, a des dimensions qui s'expriment, en cm, par des nombres entiers. Son volume est de $22,661 \text{ dm}^3$.

Quelles sont les dimensions de cette boîte ?

EXERCICE 65

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 ?

EXERCICE 66

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.

	a	b	c	d	e
A					
B		■			
C			■		■
D					
E			■		

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.

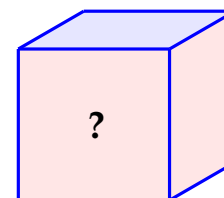
EXERCICE 67

Dimension d'une cuve

Une 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 et l'on justifiera le choix retenu.



EXERCICE 68

Ristournes

Un détaillant de matériel audiovisuel effectue trois remises successives de pourcentages entiers, sur un article qui coûtait 300 € et qu'il vend 222,87 €.

Quels sont les pourcentages des trois remises ?

EXERCICE 69**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 ?

EXERCICE 70**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 ?

EXERCICE 71**Cible**

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

