Arithmétique – Nombres premiers – Exercices

	Chercher	Modéliser	Représenter	Raisonner	Calculer	Comm.
Exercices ⋆			13, 24	24	1, 2, 3, 4, 5, 18	
Exercices ⋆⋆	7	12		6, 9, 16	7, 8, 10, 16, 19, 20, 21	9
Exercices ⋆⋆⋆	17, 23, 26, 27	28, 29, 14	14, 15	25, 27	11, 22, 28, 29	15, 26

Exercice 1 ⋆ [Calculer]

Parmi les entiers suivants, déterminer ceux qui sont premiers.

- 97
- 187
- 1 081
- 1 009

Exercice 2 ⋆ [Calculer]

Déterminer le nombre de diviseurs des entiers suivants.

- 51
- 72
- 101
- 1 024

Exercice 3 ⋆ [Calculer]

Déterminer l'ensemble des diviseurs des entiers suivants.

- 67
- 36
- 1 309
- 2 1097

Exercice 4 ⋆ [Calculer]

Déterminer le PPCM de 9 060 et de 2 466.

Exercice 5 ⋆ [Calculer]

1. Montrer que pour tous entiers naturels n et m,

   $$n \times m = \text{PGCD}(n\,;m) \times \text{PPCM}(n\,;m).$$

2. Comment calcule-t-on efficacement le PPCM de deux entiers ?

Exercice 6 ⋆⋆ [Raisonner]

Déterminer en justifiant si les affirmations suivantes sont vraies ou fausses.

1. La somme de deux entiers consécutifs peut être un nombre premier.
2. La somme de trois entiers impairs consécutifs peut être un nombre premier.
3. Pour tout entier $p \geqslant 2$, $p^2 - 1$ n'est pas premier.
4. Il existe $n \in \mathbb{N}$ tel que n et $2n$ soient des carrés parfaits.
5. n est un carré parfait si, et seulement si, il admet un nombre impair de diviseurs.

Exercice 7 ⋆⋆ [Calculer, Chercher]

Déterminer l'ensemble des valeurs de $n \in \mathbb{N}$ pour lesquelles les entiers n, $n+10$ et $n+20$ sont trois nombres premiers.

Exercice 8 ⋆⋆ [Calculer]

Déterminer le plus petit entier naturel admettant exactement 21 diviseurs.

Exercice 9 ⋆⋆ [Raisonner, Communiquer]

Montrer que si k est un entier naturel impair et supérieur à 5, alors la somme de k entiers consécutifs n'est pas un nombre premier.

Exercice 10 ⋆⋆ [Calculer]

1. Montrer que pour tous $x, y \in \mathbb{R}$:
$$x^3 - y^3 = (x-y)(x^2+xy+y^2).$$
2. Déterminer l'ensemble des nombres premiers de la forme $n^3 - 8$, où n est un nombre entier.
3. Montrer que l'entier $n^3 + 1$ n'est pas premier.

Exercice 11 ⋆⋆⋆ [Calculer]

1. Montrer que pour tous $x, y \in \mathbb{R}$:
$$x^4 + 4y^4 = (x-y)(x^2+xy+y^2).$$
2. Déterminer l'ensemble des nombres premiers de la forme $n^4 + 4$, où n est un nombre entier.
3. Montrer que l'entier $285 + 4^{285}$ n'est pas premier. Pourquoi n'est-il pas envisageable de répondre à cette question en utilisant simplement un test classique de primalité tel que celui présenté dans le cours ?

Exercice 12 ⋆⋆ [Chercher]

Déterminer les trois petits entiers naturels n tels que $n^2 - 1$ soit le produit de trois nombres premiers disctincts.

Exercice 13 ⋆ [Représenter]

Écrire une fonction algorithmique en langage Python permettant de tester si un entier n est premier ou non.

Exercice 14 ⋆⋆⋆ [Modéliser, Représenter]

On considère un entier $n \geqslant 2$. La fonction algorithmique ci-dessous **Eratosthene**, écrite en langage Python, renvoie la liste des nombres premiers inférieurs ou égaux à n.

```
def Eratosthene(n):
  Nombres=[1]*n
  Nombres_premiers=[2]
  for i in range(3,n,2):
    if Nombres[i]==1:

     Nombres_premiers.append(i)
       for j in range(2*i,n,i):
         Nombres[j]=0
  return Nombres_premiers
```

1. Expliquer chaque ligne de l'algorithme afin de justifier pourquoi l'algorithme renvoie bien la liste des nombres premiers inférieurs ou égaux à n.
2. Pourquoi l'algorithme ci-dessus est plus efficace que celui consistant à tester la primalité de tous les entiers entre 2 et n indépendemment les uns des autres ?
3. Implémenter le programme puis le tester pour $n = 100\,000$. Combien y'a-t-il de nombres premiers inférieurs ou égaux à 100 000 ?
4. Un théorème, démontré indépendamment par Charles de la Vallée Poussin et Jacques Hadamard en 1896, indique que pour n suffisamment grand, le nombre de nombres premiers inférieurs ou égaux à n est environ $\dfrac{n}{\ln(n)}$. Vérifier cette propriété pour $n = 100\,000$.

Exercice 15 ⋆⋆⋆ [Raisonner, Communiquer]

1. Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$.
2. Montrer qu'il existe une infinité de nombres premiers de la forme $6n + 5$.

Exercice 16 ⋆⋆ [Calculer, Raisonner]

Montrer que pour tout entiers x et y, et pour tout entier premier p,

$$(x + y)^p \equiv x^p + y^p \,[p].$$

Exercice 17 ⋆⋆ [Chercher]

Montrer que pour tout $n \leqslant 10^9$, la décomposition de n en produit de facteurs premiers fait apparaître moins de dix facteurs premiers distincts.

Exercice 18 ⋆ [Calculer]

Dans chaque cas, déterminer le reste de la division euclidienne de n par a.

1. $n = 2^{10}$ et $a = 11$
2. $n = 3^{17}$ et $a = 17$
3. $n = 5^{20}$ et $a = 19$
4. $n = 4^{13}$ et $a = 7$
5. $n = 15^{100}$ et $a = 97$

Exercice 19 ⋆⋆ [Calculer]

Calculer 3^{24} modulo 35.

Calculer 4^{207} modulo 55.

Exercice 20 ⋆⋆ [Calculer]

Déterminer le chiffre des unités de 3^{80} et de 7^{28}.

Exercice 21 ⋆⋆ [Calculer, Chercher]

Montrer que pour tout entier $n \in \mathbb{N}$, $n^7 - n$ est divisible par 14.

Exercice 22 ⋆⋆⋆ [Calculer]

Montrer que pour tout $n \in \mathbb{N}^*$,

$$15^{15^n} \equiv 1 \,[11].$$

Exercice 23 ⋆⋆⋆ [Chercher]

Montrer que pour tout $n \geqslant 2$, il existe n entiers consécutifs qui ne sont pas premiers.

Exercice 24 ⋆ [Représenter, Raisonner]

Dans la fonction algorithmique ci-dessous écrite en langage Python, on considère un entier $n \geqslant 3$.

```
def testFermat(n):
    F=2**(n-1)%n
    return(F)
```

1. Que renvoie l'algorithme si n est un nombre premier ?
2. Que peut-on dire lorsque la valeur renvoyée par l'algorithme est différente de 1 ?
3. Tester l'algorithme pour $n = 561$. Que peut-on en déduire ?
4. En utilisant l'algorithme, que peut-on dire des entiers suivants ?
   - 244 608 079
   - 154 515 677

Exercice 25 ⋆⋆⋆ [Raisonner]

Chercher On considère un entier $n \geqslant 2$ et on définit le n^{e} nombre de Mersenne par $M_n = 2^n - 1$.

1. Montrer que si M_n est premier, alors n est premier.
2. En considérant le cas $n = 11$, montrer que la réciproque de la proposition précédente est fausse.

Exercice 26 ⋆⋆⋆ [Chercher, Communiquer]

On considère un entier $n \geqslant 1$ et on définit le n^{e} nombre de Fermat par $M_n = 2^{2^n} + 1$.

1. En utilisant la calculatrice, montrer que F_1, F_2, F_3 et F_4 sont premiers.
2. Soit $n \geqslant 5$ et soit p un diviseur premier de F_n.
   Montrer que $p \equiv 1 \left[2^{n+1}\right]$.
3. Déterminer un diviseur premier de F_5 inférieur à 1000.

Exercice 27 ⋆⋆⋆ [Chercher, Raisonner]

On définit la fonction indicatrice d'Euler de la manière suivante :

$$\left\{\begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ n & \longmapsto & \phi(n) \end{array}\right.$$

où $\phi(n)$ désigne le nombre d'entiers premiers avec n entre 1 et n.

1. Si p est premier, exprimer $\phi(p)$ en fonction de p.
2. Si p est premier et $k \in \mathbb{N}^*$, montrer que :
$$\phi(p^k) = p^k - p^{k-1}.$$
3. L'objectif de cette question est de montrer que ϕ est une fonction multiplicative, c'est-à-dire que si a et b sont premiers entre eux, on a :
$$\phi(a \times b) = \phi(a) \times \phi(b).$$
Dans toute la suite, a et b désignent donc deux entiers strictement positifs et premiers entre eux.
   (a) Pour tout entier $x \geqslant 1$, on note $E_x = \{0, 1, \ldots, x\}$ sur lequel on définit l'addition et la multiplication modulo x. De plus, on note E_x^* l'ensemble des éléments de E_x qui sont inversibles modulo x.
   Montrer que pour tout $x \geqslant 1$,
$$\phi(x) = \text{Card}(E_x^*).$$
   (b) On définit l'application suivante :
$$\text{F} : \left\{\begin{array}{ccc} E_{ab} & \longrightarrow & E_a \times E_b \\ k & \longmapsto & (k \bmod a \,;\, k \bmod b) \end{array}\right.$$
   Montrer que tout $(x\,;y) \in E_a \times E_b$ admet un unique antécédent par la fonction F.
   (c) Montrer que pour tout $k \in E_{ab}$, $k \in E_{ab}^*$ si, et seulement si, $\text{F}(k) \in E_a^* \times E_b^*$.
   (d) En déduire que :
$$\text{Card}(E_{ab}^*) = \text{Card}(E_a^*) \times \text{Card}(E_b^*)$$
   puis que la fonction ϕ est multiplicative.
4. Calculer le nombre d'entiers premiers avec 3 096 entre 1 et 3096.

Exercice 28 ⋆⋆⋆ [Modéliser, Calculer]

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978.

1. **Chiffrement dans le système RSA**
   Alice veut communiquer de manière sécurisée. Elle choisit deux nombres premiers p et q, puis calcule les produits $N = pq$ et $n = (p-1)(q-1)$. Elle choisit également un entier naturel c premier avec n puis elle publie le couple $(N\ ;\ c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre chiffré.

   Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $N-1$. Pour chiffrer un entier a de cette suite, on procède ainsi : on calcule le reste b dans la division euclidienne par N du nombre a^c, et le nombre chiffré est l'entier b.

   Dans la pratique, cette méthode est sûre si on choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres. On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$. Alice choisit également $c = 23$.

   (a) Calculer les nombres N et n, puis justifier que la valeur de c vérifie la condition voulue.

   (b) Bob souhaite envoyer à Alice le nombre $a = 8$. Déterminer la valeur du nombre chiffré b correspondant.

1. **Déchiffrement dans le système RSA**
   Alice calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leqslant d < n$ et $cd \equiv 1 \mod n$.

   Elle garde secret ce nombre d qui lui permet, et à elle seule, de déchiffrer les nombres qui lui ont été envoyés chiffrés avec sa clé publique.

   Pour déchiffrer un nombre crypté b, Alice calcule le reste a dans la division euclidienne par N du nombre b^d, et le nombre en clair – c'est-à-dire le nombre avant chiffrage – est le nombre a.

   (a) Justifier qu'en faisant cette opération, Alice retombe bien sur le nombre a modulo N.

   (b) Les nombres choisis par Alice sont encore $p = 5$, $q = 11$ et $c = 23$. Quelle est la valeur de d ?

   (c) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.

Exercice 29 ⋆⋆⋆ [Modéliser, Calculer]

À toute lettre de l'alphabet, on associe un nombre entier entre 0 et 25 :

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10

L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Alice veut communiquer de manière sécurisée. Elle choisit deux nombres premiers p et q et un entier naturel B tel que :

$$1 \leqslant B < pq.$$

Elle publie les nombres $n = pq$ et B et garde secret les nombres p et q.
Si Bob veut envoyer un message à Alice, il le code lettre par lettre. Plus précisément, le codage d'une lettre représentée par l'entier x est l'entier $y \in [\![0\,;n[\![$ tel que :

$$y \equiv x(x+B) \,[\![n]\!].$$

Dans tout l'exercice, on prend $p = 3$, $q = 11$ et $B = 13$.

1. Bob veut envoyer la lettre N à Alice. Quel nombre crypté doit-il lui transmettre ?
2. Aice a reçu un message crypté qui commence par le nombre 3. Elle doit donc déterminer l'entier x compris entre 0 et 25 tel que $x(x+13) \equiv 3 \,[\![33]\!]$.
   (a) Montrer que cette équation est équivalente à :
   $$(x+23)^2 \equiv 4 \,[\![33]\!].$$
   (b) Montrer ensuite qu'elle est équivalente au système suivant :
   $$\begin{cases} (x+23)^2 \equiv 1 \quad [\![3]\!] \\ (x+23)^2 \equiv 4 \quad [\![11]\!] \end{cases}$$
   (c) En déduire que l'entier x recherché est congru à 0 ou 2 modulo 3 et qu'il est congru à 8 ou 1 modulo 11.
3. En énumérant les différentes possibilités, Alice peut-elle connaître la première lettre du message envoyé par Bob ? Cette méthode de chiffrement est-elle utilisable pour décoder un message lettre par lettre ?