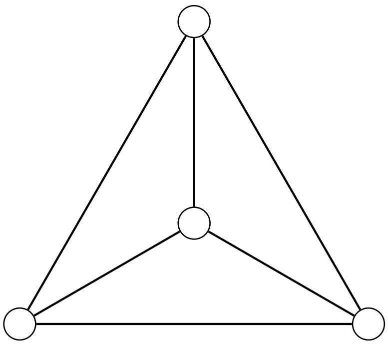
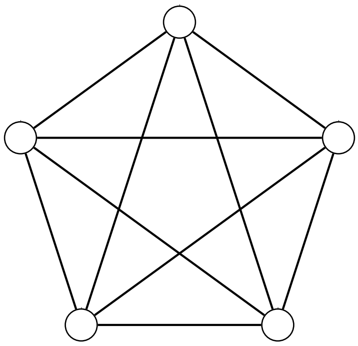
Gymnase de Burier 2019 – 2021

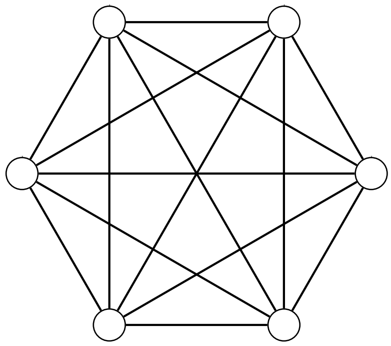
2OS – 3OS Mathématiques



K_4



K_5



K_6

Table des matières

Chapitre 1

Sommes et récurrence

1.1 Sommes

1.1.1 On donne

$$x_1 = 3, \quad x_2 = 5, \quad x_3 = 6, \quad x_4 = 2 \quad \text{et} \quad x_5 = 7.$$

Calculer :

a) $\displaystyle\sum_{i=1}^{5} x_i$

b) $\displaystyle\sum_{i=2}^{4} x_i$

c) $\displaystyle\sum_{k=1}^{5} x_k$

d) $\displaystyle\sum_{j=1}^{5} {x_j}^3$

e) $\displaystyle\sum_{i=1}^{5} (x_i + 8)$

f) $\displaystyle\sum_{k=1}^{5} (8 \cdot x_k)$

1.1.2 On donne

$$x_1 = 3, \quad x_2 = 5, \quad x_3 = 6, \quad x_4 = 2 \quad \text{et} \quad x_5 = 7.$$

On donne également

$$y_1 = 2, \quad y_2 = 8, \quad y_3 = 3, \quad y_4 = 1 \quad \text{et} \quad y_5 = 6.$$

Calculer :

a) $\displaystyle\sum_{i=1}^{5} (x_i + y_i)$

b) $\displaystyle\sum_{i=1}^{5} (x_i - y_i)$

c) $\displaystyle\sum_{k=1}^{5} (x_k \cdot y_k)$

d) $\displaystyle\sum_{j=1}^{5} (2 \cdot x_j)$

e) $\displaystyle\sum_{j=1}^{5} (x_j + y_j)^2$

f) $\displaystyle\sum_{i=1}^{5} 8$

g) $\displaystyle\sum_{i=1}^{5} (2 \cdot x_i) + \sum_{j=1}^{5} (3 \cdot y_j)$

h) $\displaystyle\sum_{j=1}^{5} {x_j}^2 - \left(\sum_{j=1}^{5} y_j \right)^2$

i) $\displaystyle\sum_{i=1}^{4} (x_{i+1} + y_i)$

1.1.3 Développer les sommes suivantes

a) $\sum_{i=0}^{n}(-1)^i$ b) $\sum_{j=0}^{n} 3j$ c) $\sum_{k=1}^{n} n$ d) $\sum_{i=1}^{n} \frac{n}{i}$

1.1.4 Développer chacune des sommes écrites à l'aide du symbole Σ, en faisant disparaître ce symbole :

a) $\displaystyle\sum_{k=3}^{10} \frac{1}{k^2}$ b) $\displaystyle\sum_{k=1}^{10} \frac{1}{2\,k+1}$ c) $\displaystyle\sum_{k=1}^{n} \frac{(k+1)!}{k}$

1.1.5 Développer et calculer les sommes suivantes :

a) $\sum_{i=0}^{n} 1$ d) $\sum_{m=0}^{3} (m^2 - 6m + 9)$ g) $\sum_{k=1}^{5} \frac{k+2}{k}$

b) $\sum_{j=1}^{2011} (-1)^j$ e) $\sum_{l=1}^{5} 4l\ (l^2 - 1)$ h) $\sum_{k=1}^{6} \frac{1}{3^k}$

c) $\sum_{k=-n}^{n} (k+1)$ f) $\sum_{i=0}^{4} \left(2^i + \left(\frac{1}{2}\right)^i\right)$ i) $\sum_{j=-2}^{2} \frac{2^{j+3}}{j^2+1}$

1.1.6 Soit $x_1, \dots, x_n$ une suite de nombres réels. Calculer $\displaystyle\sum_{i=2}^{n}(x_i - x_{i-1})$

1.1.7 Traduire à l'aide du symbole Σ les sommes suivantes :

a) $1^2 + 2^2 + 3^2 + \cdots + 12^2 + 13^2 + 14^2$

b) $11^2 + 12^2 + 13^2 + \cdots + 102^2 + 103^2 + 104^2$

c) $\frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \cdots + \frac{13}{14} + \frac{14}{15} + \frac{15}{16}$

d) $1^2 + 3^2 + 5^2 + \cdots + 11^2 + 13^2 + 15^2$

e) $(1 \cdot 3) + (2 \cdot 4) + (3 \cdot 5) + (4 \cdot 6) + (5 \cdot 7)$

f) $1 + 8 + 27 + 64 + 125$

1.1.8 Ecrire les sommes suivantes à l'aide du symbole Σ.

a) $2 + 4 + 6 + \cdots 248 =$

b) $1000 + 1010 + 1020 + \cdots + 1540 =$

c) $1^2 + 2^2 + 3^2 + \cdots 15^2 =$

d) $1 + 2 + 4 + 8 + 16 + \cdots + 1024 =$

e) $2 + 3 + 5 + 9 + 17 + \cdots + 1025 =$

f) $4 + 12 + 36 + 108 + 324 =$

g) $9 - 12 + 15 - 18 + \cdots + 303 =$

h) $45 - 40 + 35 - 30 + 25 - 20 + 15 =$

i) $1+\dfrac{1}{2}+\dfrac{1}{3}+\dfrac{1}{4}+\cdots+\dfrac{1}{n}=$

j) $\dfrac{1}{2}+\dfrac{2}{3}+\dfrac{3}{4}+\cdots+\dfrac{9}{10}+32=$

k) $\dfrac{1}{2}+\dfrac{4}{5}+\dfrac{9}{10}+\cdots+\dfrac{10000}{10001}=$

l) $\dfrac{5}{3}+\dfrac{10}{7}+\dfrac{15}{11}+\dfrac{20}{15}+\cdots+\dfrac{70}{55}=$

m) $(1\cdot 3)+(2\cdot 4)+(3\cdot 5)+(4\cdot 6)+(5\cdot 7)=$

1.1.9 Traduire à l'aide du symbole Σ la somme suivante :

$$1000-\frac{3}{1\cdot(1+3+5)}+\frac{5}{(1+3)\cdot(1+3+5+7)}-\frac{7}{(1+3+5)\cdot(1+3+5+7+9)}+\ldots$$

1.1.10 Est-ce que $A=B=C=D$ si on définit

$$A=\sum_{i=1}^{n} i\cdot n \qquad B=\sum_{k=1}^{n} k\cdot n \qquad C=n\cdot\sum_{k=1}^{n} k \qquad D=k\cdot\sum_{i=0}^{n} n \qquad ?$$

1.1.11 Ecrire les sommes suivantes en faisant en sorte que la première valeur de l'indice soit 0, puis 49 :

a) $\sum\limits_{i=2}^{45} 1=\sum\limits_{i=0}^{\ldots}\ldots=\sum\limits_{i=49}^{\ldots}\ldots$

b) $\sum\limits_{i=10}^{20} i$

c) $\sum\limits_{k=-4}^{180} \dfrac{k}{k+5}$

1.1.12 Changer l'indice et ses bornes de sorte que le terme général soit plus simple :

a) $\sum\limits_{i=0}^{n} \dfrac{(i+1)^2+3}{1+\sqrt{i+1}}$ b) $\sum\limits_{j=3}^{n+2} \dfrac{x^{j-3}}{(j-3)^x}$ c) $\sum\limits_{k=1}^{n+1} (k-1)\,2^k+3^{k-1}$

1.1.13 On considère une suite de n nombres $x_1, x_2, x_3, \ldots, x_n$. Écrire les expressions suivantes de la manière la plus synthétique possible à l'aide d'un symbole de sommation.

a) La somme des termes de cette suite de nombres.
b) La somme des carrés des termes de cette suite de nombres
c) Le carré de la somme des termes de cette suite de nombres
d) La différence entre la somme des carrés et le carré de la somme des termes de cette suite de nombre

1.1.14 On considère deux suites de n nombres $x_1, x_2, x_3, \ldots, x_n$ et $y_1, y_2, y_3, \ldots, y_n$. Écrire les expressions suivantes de la manière la plus synthétique possible.

a) Produit de la somme des x_i et de la somme des y_i
b) Somme des produits $x_i\, y_i$
c) Somme des y_i moins k fois la somme des x_i

1.1.15 Ecrire un programme qui fait calculer les sommes suivantes :

a) $\sum\limits_{i=1}^{100000} (2+3\,i)$

b) $\sum\limits_{i=-237}^{325} i^2$

c) $\sum\limits_{j=0}^{100} 2^j$

d) $\sum\limits_{k=1}^{10^6} (2\,k-1)$

1.1.16 Ecrire un programme qui fait calculer les sommes suivantes :

a) $\sum\limits_{n=1}^{23} \sum\limits_{k=1}^{37} k^n$

b) $\sum\limits_{i=1}^{100} \sum\limits_{j=1}^{100} 1$

c) $\sum\limits_{n=1}^{20} \sum\limits_{j=1}^{10} (n^j+1)$

d) $\sum\limits_{n=-10}^{10} \sum\limits_{k=-n}^{n} k$

1.1.17 Soit $x_1, x_2, x_3, \ldots, x_n$ des nombres réels et $m = \frac{1}{n}\sum\limits_{i=1}^{n} x_i$. Montrer que :

$$\frac{1}{n}\sum_{i=1}^{n} (x_i - m)^2 = \frac{1}{n}\sum_{i=1}^{n} {x_i}^2 - m^2$$

1.2 Récurrence

La démonstration par récurrence s'applique dans le cas où on doit démontrer une proposition P_n pour tout entier $n \geq 0$ ou $n \geq 1$ ou plus généralement $n \geq n_0$ ($n_0 \in \mathbb{N}$).

Une démonstration par récurrence se fait toujours en deux étapes :

a) Première phase, dite d'initialisation : on démontre que la proposition est vraie pour la plus petite valeur de l'entier n : 0, 1 ou n_0.

b) Deuxième phase : on suppose que la proposition P_n est vraie et on démontre sous cette hypothèse, appelée hypothèse de récurrence, que la proposition P_{n+1} est vraie.

D'un point de vue formel, on peut écrire :

$$\begin{cases} P_0 \text{ est vrai} \\ n \geq 0 \text{ et } P_n \Rightarrow P_{n+1} \end{cases} \Rightarrow \forall n \geq 0 : P_n \text{ est vrai}$$

1.2.1 Démontrer par récurrence que, $\forall n \in \mathbb{N}^*$:

a) $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

b) $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

c) $\displaystyle\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$

d) $\displaystyle\sum_{k=1}^{n} (-1)^{k+1}\, k^2 = (-1)^{n+1}\,\frac{n(n+1)}{2}$

e) $\displaystyle\sum_{k=1}^{n} \frac{1}{(2\,k-1)\,(2\,k+1)} = \frac{n}{2\,n+1}$

f) $\displaystyle\sum_{k=1}^{n} \frac{k^2}{(2\,k-1)\,(2\,k+1)} = \frac{n\;(n+1)}{2\;(2\,n+1)}$

g) $\displaystyle\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$

h) $\displaystyle\sum_{k=1}^{n} k \cdot 5^k = \frac{5+(4\,n-1)\;5^{n+1}}{16}$

i) $\displaystyle\sum_{k=1}^{n} \frac{1}{k\;(k+1)\,(k+2)} = \frac{n\;(n+3)}{4\;(n+1)\,(n+2)}$

1.2.2 Démontrer par récurrence que, $\forall n \in \mathbb{N}$:

a) $8^n - 1$ est divisible par 7

b) $3^{2\,n+2} - 2^{n+1}$ est un multiple de 7

c) $10^{6\,n+2} + 10^{3\,n+1} + 1$ est un multiple de 111

d) $n^3 + 5\,n$ est divisible par 3

e) $\frac{2}{3}\,n^3 + n^2 + \frac{1}{3}\,n$ est un nombre pair

f) $11^{n+2} + 12^{2\,n+1}$ est divisible par 133

1.2.3 Soit $n \in \mathbb{N}$. Prouver par récurrence puis directement que 3 divise $n^3 - n$.

1.2.4 Établir une formule pour la somme

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n\;(n+1)}$$

1.2.5 Établir une formule pour la somme

$$1 + \frac{1}{1+2} + \frac{1}{1+2+3} + \cdots + \frac{1}{1+2+3+\cdots+n}$$

1.2.6 Écrire en fonction de n la somme des carrés des n premiers nombres impairs.

1.2.7 Démontrer que « $\forall n \in \mathbb{N},\; n^2 - n + 41$ *est premier* » est une proposition fausse.

1.2.8 Démontrer que « $\forall n \in \mathbb{N}^*,\;$ (n *est premier* $\Rightarrow 2^n - 1$ *est premier*) » est une proposition fausse.

1.2.9 Trouver l'erreur commise dans la démonstration ci-dessous :
On note P_n l'assertion « $\forall n \in \mathbb{N}^*,\;$ (6 *divise* $7^n + 1$) ».
Prouvons que 6 divise 7^n+1. Supposons que P_n est vraie. Alors il existe k tel que $7^n+1 = 6\,k$. Ainsi, $7^{n+1}+1 = 7\cdot 7^n + 1 = 7\,(6\,k-1) + 1 = 42\,k - 6 = 6\,(7\,k-1)$. Par conséquent 6 divise $7^{n+1}+1$, i.e. P_{n+1} est vraie. Par récurrence, P_n est vraie pour tout n.

1.2.10 Trouver l'erreur commise dans la démonstration ci-dessous :
Prouvons que tout le monde a la même taille. On pose $P_n =$ « n personnes ont toujours la même taille ». Cette fois on n'oublie pas d'initialiser : une personne a la même taille qu'elle-même, donc P_1 est vraie.
L'hérédité ensuite. Soit $n > 1$ et supposons que P_n est vraie. On considère alors $n + 1$ personnes. Les personnes 1 jusqu'à n ont la même taille, par hypothèse de récurrence. De même, les personnes 2 jusqu'à $n + 1$ ont la même taille. Ainsi, ces $n + 1$ personnes ont la même taille.

1.2.11 Démontrer par récurrence :

a) Pour tout nombre réel positif x, la propriété suivante est vérifiée :
$\forall n \in \mathbb{N}, (1+x)^n \geq 1 + n\,x$

b) Pour tout $a \in \mathbb{R}$ et $r \in \mathbb{R} - \{1\}$, on a :
$$\forall n \in \mathbb{N}^*, \quad a + a\,r + a\,r^2 + \cdots + a\,r^{n-1} = \frac{a\,(r^n - 1)}{r - 1}$$

c) Pour tout $\alpha \in \mathbb{R} - \{k\,\pi \,|\, k \in \mathbb{Z}\}$, on a :
$$\forall n \in \mathbb{N}, \quad \cos(\alpha) \cdot \cos(2\,\alpha) \cdot \cos(4\,\alpha) \cdot \ldots \cdot \cos(2^n\,\alpha) = \frac{\sin(2^{n+1}\,\alpha)}{2^{n+1}\,\sin(\alpha)}$$

d) Pour des nombres réels strictement positifs $x_1, x_2, x_3, \ldots$, on a :
$$\forall n \in \mathbb{N}, \quad (x_1 + x_2 + \cdots + x_n) \cdot \left(\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n}\right) \geq n^2$$

1.2.12 Démontrer par récurrence :

a) $\forall n \in \mathbb{N}^*, \quad (n+1)! > 1! + 2! + 3! + \cdots + n!$

b) $\forall n \in \mathbb{N} - \{0\,, 1\,, 2\,, 3\}, \quad n! > 2^n$

1.2.13 Soit (u_n) la suite de *Fibonacci* définie comme suit :

$$\begin{cases} u_1 = 1 \\ u_2 = 1 \\ u_{n+1} = u_n + u_{n-1}, \quad \text{pour} \quad n \geq 2 \end{cases}$$

a) Démontrer que $\forall n \in \mathbb{N}^* \quad , \quad {u_1}^2 + {u_2}^2 + \ldots + {u_n}^2 = u_n \cdot u_{n+1}$

b) Calculer l'expression ${u_n}^2 - u_{n-1} \cdot u_{n+1}$ pour quelques valeurs de n.

c) Démontrer que $\forall n \in \mathbb{N}^* \quad , \quad u_n = \dfrac{\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n}{\sqrt{5} \cdot 2^n}$

1.2.14

1.3 Solutions des exercices

1.1.1

a) $\sum_{i=1}^{5} x_i = 23$

b) $\sum_{i=2}^{4} x_i = 13$

c) $\sum_{k=1}^{5} x_k = 23$

d) $\sum_{j=1}^{5} {x_j}^3 = 719$

e) $\sum_{i=1}^{5} (x_i + 8) = 63$

f) $\sum_{k=1}^{5} (8 \cdot x_k) = 184$

1.1.2

a) $\sum_{i=1}^{5} (x_i + y_i) = 43$

b) $\sum_{i=1}^{5} (x_i - y_i) = 3$

c) $\sum_{k=1}^{5} (x_k \cdot y_k) = 108$

d) $\sum_{j=1}^{5} (2 \cdot x_j) = 46$

e) $\sum_{j=1}^{5} (x_i + y_i)^2 = 453$

f) $\sum_{i=1}^{5} 8 = 40$

g) $\sum_{i=1}^{5} (2 \cdot x_i) + \sum_{j=1}^{5} (3 \cdot y_j) = 106$

h) $\sum_{j=1}^{5} {x_j}^2 - \left(\sum_{j=1}^{5} y_j \right)^2 = -277$

i) $\sum_{i=1}^{4} (x_{i+1} + y_i) = 34$

1.1.3

a) 1 si n est pair ; 0 si n est impair

b) $3 + 6 + 9 + \ldots + 3n$

c) n^2

d) $n + \frac{n}{2} + \frac{n}{3} + \ldots + \frac{n}{n-1} + 1$

1.1.4 –

1.1.5

a) $n + 1$

b) -1

c) $2\,n+1$

d) $\sum\limits_{m=0}^{3}(m-3)^2=14$

e) $4\cdot 0+8\cdot 3+12\cdot 8+16\cdot 15+20\cdot 24=840$

f) $1+1+2+\frac{1}{2}+4+\frac{1}{4}+8+\frac{1}{8}+16+\frac{1}{16}=\frac{527}{16}$

g) $3+2+\frac{5}{3}+\frac{3}{2}+\frac{7}{5}=\frac{287}{30}$

h) $\frac{1}{3}+\frac{1}{9}+\frac{1}{27}+\frac{1}{81}+\frac{1}{243}+\frac{1}{729}=\frac{364}{729}$

i) $\frac{2}{5}+\frac{4}{2}+\frac{8}{1}+\frac{16}{2}+\frac{32}{5}=\frac{124}{5}$

1.1.6 $\displaystyle\sum_{i=2}^{n}(x_i-x_{i-1})=x_n-x_1$

1.1.7

a) $1^2+2^2+3^2+\cdots+12^2+13^2+14^2=\displaystyle\sum_{i=1}^{14} i^2=\sum_{i=0}^{13}(i+1)^2$

b) $11^2+12^2+13^2+\cdots+102^2+103^2+104^2=\displaystyle\sum_{i=11}^{104} i^2$

c) $\frac{1}{2}+\frac{2}{3}+\frac{3}{4}+\cdots+\frac{13}{14}+\frac{14}{15}+\frac{15}{16}=\displaystyle\sum_{i=1}^{15}\frac{i}{i+1}$

d) $1^2+3^2+5^2+\cdots+11^2+13^2+15^2=\displaystyle\sum_{i=1}^{8}(2\,i-1)^2$

e) $(1\cdot 3)+(2\cdot 4)+(3\cdot 5)+(4\cdot 6)+(5\cdot 7)=\displaystyle\sum_{i=1}^{5} i\,(i+2)$

f) $1+8+27+64+125=\displaystyle\sum_{i=1}^{5} i^3$

1.1.8

a) $\sum\limits_{i=1}^{124} 2i$

b) $\sum\limits_{i=100}^{154} 10i$

c) $\sum\limits_{k=1}^{15} k^2$

d) $\sum\limits_{i=0}^{10} 2^i$

e) $\sum_{i=0}^{10}(2^i+1)$

f) $\sum_{i=0}^{4} 4\cdot 3^i$

g) $\sum_{i=3}^{101}(-1)^{i+1}\, 3i$

h) $\sum_{i=0}^{6}(-1)^i(45-5i)$

i) $\sum_{i=1}^{n}\frac{1}{i}$

j) $\sum_{i=1}^{9}\frac{i}{i+1}+32$

k) $\sum_{i=1}^{100}\frac{i^2}{i^2+1}$

l) $\sum_{i=1}^{14}\frac{5i}{4i-1}$

m) $\sum_{j=1}^{5} j(j+2)$

1.1.9 $1000+\sum_{i=1}^{\infty}\frac{(-1)^i(2i+1)}{\sum_{j=1}^{i}(2j-1)\sum_{k=1}^{i+2}(2k-1)}$

1.1.10 $A=B=C=\frac{n^2(n+1)}{2} \neq D = k\,n\,(n+1)$

1.1.11

a) $\sum_{i=2}^{45}1=\sum_{i=0}^{43}1=\sum_{i=49}^{92}1$

b) $\sum_{i=10}^{20}i=\sum_{i=0}^{10}(i+10)=\sum_{i=49}^{59}(i-39)$

c) $\sum_{k=-4}^{180}\frac{k}{k+5}=\sum_{k=0}^{184}\frac{k-4}{k+1}=\sum_{k=49}^{233}\frac{k-53}{k-48}$

1.1.12

a) $\sum_{i=0}^{n}\frac{(i+1)^2+3}{1+\sqrt{i+1}}=\sum_{j=1}^{n+1}\frac{j^2+3}{1+\sqrt{j}}$

b) $\sum_{j=3}^{n+2}\frac{x^{j-3}}{(j-3)^x}=\sum_{k=0}^{n-1}\frac{x^k}{k^x}$

c) $\sum_{k=1}^{n+1}(k-1)\,2^k+3^{k-1}=\sum_{l=0}^{n}l\cdot 2^{l+1}+3^l$

1.1.13

a) $\sum x_i$

b) $\sum (x_i)^2=\sum {x_i}^2$

c) $\left(\sum x_i\right)^2$

d) $\sum {x_i}^2-\left(\sum x_i\right)^2$

1.1.14

a) $\left(\sum_i x_i\right)\left(\sum_i y_i\right)=\sum_i x_i\,\sum_j y_j=\sum_{i,j}x_iy_j$

b) $\sum_i x_i\, y_i$

c) $\sum y_i - k\sum x_i$

1.1.15

```
def somme(f, n, m):
    s = 0
    for i in range(n, m + 1):
        s += f(i)
    return s
def a(i):
    return 2 + 3 * i
def b(i):
    return i**2
def c(j):
    return 2**j
def d(k):
    return 2*k - 1

print("a)", somme(a, 1, 100000))
print("b)", somme(b, -237, 325))
print("c)", somme(c, 0, 100))
print("d)", somme(d, 1, 10**6))
```

1.1.16

```
def somme(f, n_1, m_1, n_2, m_2):
    s = 0
    for i in range(n_1, m_1 + 1):
        for j in range(n_2, m_2 + 1):
            s += f(i, j)
    return s
def a(k, n):
    return k^n
def b(i, j):
    return 1
```

```
def c(n, j):
    return n**j + 1


print("a)", somme(a, 1, 23, 1, 37))
print("b)", somme(b, 1, 100, 1, 100))
print("c)", somme(c, 1, 20, 1, 10))


d = 0


for n in range(-10, 11):
    for k in range(-n, n + 1):
        d += k


print("d)", d)
```

1.1.17

1.2.1 –

1.2.2 –

1.2.3 –

1.2.4 –

1.2.5 –

1.2.6 –

1.2.7 –

1.2.8 –

1.2.9 –

1.2.10 –

1.2.11 –

1.2.12 –

1.2.13 –

1.2.14 –

Chapitre 2

Un peu de cryptologie

2.1 Calculer modulo un nombre entier

2.1.1 On calcule *modulo 5*, c'est à dire avec les entiers compris entre 0 et 4. L'ensemble de ces nombres peut être noté

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}.$$

Établir la table d'addition de $\mathbb{Z}_5$.

2.1.2 On calcule *modulo 3*, c'est à dire avec les entiers compris entre 0 et 2. L'ensemble de ces nombres peut être noté

$$\mathbb{Z}_3 = \{0, 1, 2\}.$$

Établir la table de multiplication de $\mathbb{Z}_3$.

2.1.3 Donner tous les nombres qui sont dans l'ensemble $\mathbb{Z}_{26}$.

2.1.4 Effectuer les calculs ci-dessous et réduire le résultat modulo 26.

a) $12 + 3$
b) $7 + 15$
c) $11 + 11$
d) $15 + 8$
e) $13 + 13$
f) $5 + 20$
g) $21 + 22$
h) $17 + 16$
i) $24 + 3$
j) $21 + 7$
k) $8 + 19$
l) $5 + 25$
m) $12 - 15$
n) $20 - 25$
o) $8 - 19$
p) $5 - 25$

2.1.5 Effectuer les calculs ci-dessous et réduire le résultat modulo 26.

a) $27 + 33$
b) $41 + 28$
c) $35 + 36$
d) $72 + 100$
e) $132 - 150$
f) $53 - 12$
g) $30 - 8$
h) $-5 - 12$

2.1.6 Pour chaque calcul donné à l'exercice 2.1.5, réduire les nombres modulo 26 avant d'effectuer l'opération. On veillera à réduire le résultat modulo 26 également, après avoir fait le calcul. Cela modifie-t-il le résultat final ?

2.1.7 Effectuer les calculs ci-dessous et réduire le résultat modulo 26.

a) $6 \cdot 3$
b) $5 \cdot 4$
c) $2 \cdot 12$
d) $8 \cdot 4$
e) $5 \cdot 6$
f) $10 \cdot 4$
g) $15 \cdot 3$
h) $5 \cdot 7$
i) $12 \cdot 3$
j) $7 \cdot 6$
k) $8 \cdot 9$
l) $20 \cdot 30$
m) $14 \cdot 5$
n) $25 \cdot 2$
o) $4 \cdot 11$
p) $6 \cdot 6$

2.1.8 Effectuer les calculs ci-dessous et réduire le résultat modulo 26.

a) $27 \cdot 33$
b) $41 \cdot 28$
c) $35 \cdot 36$
d) $72 \cdot 100$
e) $132 \cdot 150$
f) $53 \cdot 12$
g) $30 \cdot 8$
h) $(-5) \cdot 12$

2.1.9 Pour chaque calcul donné à l'exercice 2.1.8, réduire les nombres modulo 26 avant d'effectuer l'opération. On veillera à réduire le résultat modulo 26 également, après avoir fait le calcul. Cela modifie-t-il le résultat final ?

2.2 Le chiffre de César

2.2.1 On numérote les lettres majuscules de l'alphabet à partir de 0. Traduire le message

`ILYACEUXQUIONTUNPISTOLETCHARGE`

à l'aide d'une liste de nombres.

2.2.2 On donne la liste de nombres

$$M = (4, 19, 2, 4, 20, 23, 16, 20, 8, 2, 17, 4, 20, 18, 4, 13, 19)$$

Trouver le message correspondant à M.

2.2.3 Chiffrer le message M de l'exercice 2.2.2 à l'aide du code de César. Donner le chiffre sous forme d'une liste de nombres.

2.2.4 Chiffer le message

`ILYACEUXQUIONTUNPISTOLETCHARGE`

en utilisant le code de César.

2.2.5 J'ai chiffré un message avec le code de César et le chiffre résultant est

`HWFHXATXLFUHXVHQW`

Quel était le message secret ?

2.2.6 Chiffrer le message donné ci-dessous à l'aide du décalage 7 :

$$M = (19, 14, 8, 19, 20)$$

Donner le résultat sous forme d'une liste de nombres.

Plutôt que dire que le décalage vaut 7, on dira que la *clef de chiffrement* vaut 7.

2.2.7 Trouver une technique pour déchiffrer le message

$$C = \{9, 24, 11, 1, 25, 11, 25\}$$

sachant qu'il a été codé à l'aide d'un décalage de 7.

2.2.8 Combien y a-t-il de décalages de « type César » possibles ?

2.2.9 Donner une technique générale pour déchiffrer un message codé à l'aide d'un décalage de César quelconque. Si l'on note

$$n \in \mathbb{Z}_{26}$$

le décalage utilisé, donner une formule qui donne le décalage permettant de déchiffrer le message ou *clef de déchiffrement*, notée

$$c \in \mathbb{Z}_{26}$$

.

2.2.10 J'ai chiffré un message avec le décalage 13. Trouver la clef de déchiffrement.

2.2.11 On a pu intercepter le chiffre ci-dessous :

`ARZTLVZCCZTVSIZEUVSILPVIV`

On sait que l'expéditeur a chiffré le message clair à l'aide du code de César, mais on ignore la clef. Comment faire pour trouver le message clair ? Cela revient à *casser le code de César*.

2.2.12 Chiffrer le message m ci-dessous à l'aide du chiffrement de César et la clef 24.

`JAMAISPERSONNENAVAITETEAUSSITROPFORT`

Donner toutes les étapes du chiffrement :

a) écrire M, la liste des nombres qui correspondent aux lettres du message ;
b) chiffrer M, c'est à dire donner la liste C des nombres calculés à l'aide de la formule

$$z' = (z + 24) \mod 26;$$

c) écrire c le chiffre formé de la suite des lettres qui correspondent aux nombres de C.

2.2.13 On donne ci-dessous le chiffre c obtenu à l'aide du chiffrement de César et la clef 4 :

`PEXSTMWWMXYHIIXPEWIHYGXMZMXI`

Donner toutes les étapes du déchiffrement :

a) écrire C, la liste des nombres qui correspondent aux lettres du message ;
b) déchiffrer C, c'est à dire donner la liste M des nombres calculés à l'aide de la formule

$$z = (z' + (26 - 4)) \mod 26;$$

c) écrire m le message formé de la suite des lettres qui correspondent aux nombres de M.

2.2.14 On a pu intercepter le chiffre ci-dessous :

`SNBDRBUJVJDEJRBNQNAKNKAJENBPNWBKAJENBPNWB`

Trouver le texte clair.

2.3 Le chiffrement affine

2.3.1 Soit z un nombre de $\mathbb{Z}_{26}$. On a vu que z peut représenter une lettre de l'alphabet majuscule. On sait que pour le chiffrement de type César on choisit une clef n et que le chiffrement de z est calculé à l'aide de la formule

$$z' = z + n \mod 26$$

On peut définir une autre méthode de chiffrement, nommée *chiffrement affine* en suivant la procédure ci-dessous :

i) On choisit a et b deux nombres de Z_{26} ;

ii) On chiffre chaque « lettre » de la façon suivante :

$$z' = (a \cdot z + b) \mod 26$$

Cette façon de procéder soulève deux questions :

a) Peut-on choisir a « sans réfléchir » ?

b) Qu'en est-il pour le choix de b ?

2.3.2 Chiffrer le message ci-dessous à l'aide du chiffrement affine avec $a = 5$ et $b = 3$.

`m = JAMAISPERSONNENAVAITETEAUSSITROPFORT`

2.3.3 On a chiffré un message à l'aide du chiffrement affine avec $a = 15$ et $b = 7$. Le chiffre est donné ci-dessous :

`QHGJYXRRXGVAPPGQHRPAVLGXKXGP`

Déchiffrer ce message.

2.3.4 On a chiffré $z \in \mathbb{Z}_{26}$ à l'aide de la formule

$$z' = a \cdot z + b$$

pour a et b choisis dans Z_{26} tel que a est inversible modulo 26.

Trouver une formule permettant de retrouver z à partir de z', a, et b.

2.4 Chiffrement polyalphabétique

2.4.1 (Chiffre de Vigenère)

a) Chiffrer à l'aide du chiffrement de Vigenère le texte suivant : `textesecretadecoder` en utilisant comme clé le mot `crypto`.

b) Pour le même texte clair on obtient le texte chiffré suivant `BRQKSMZCSPXIQXTCXZR`. Quelle est la clé ?

c) Déchiffrer le message `VHOSDAVH` avec la clé `cake`.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY
```

2.4.2 Qu'apporte le chiffrement de Vigenère en matière de sécurité par rapport à une simple substitution monoalphabétique ?

2.4.3

a) Chiffrer à l'aide de l'algorithme de Vigenère le texte suivant : textesecretadecoder en utilisant comme clé le mot CRYPTO.

b) Pour le même texte clair on obtient le texte chiffré suivant

$$BRQKSMZCSPXIQXTCXZR$$

Quelle est la clé ?

2.4.4 (Chiffre de Polybe) On considère l'alphabet privé du `W`, soit 25 lettres. `Polybe` a proposé le mécanisme de chiffrement suivant : on range les lettres dans un tableau `5 X 5`, en commençant par le mot clé (et en supprimant les doublons), puis on continue avec les lettres restantes de l'alphabet, dans l'ordre.
Par exemple, avec le mot-clé `MYSTERE`, on construit le tableau suivant :

	1	2	3	4	5
1	M	Y	S	T	E
2	R	A	B	C	D
3	F	G	H	I	J
4	K	L	N	O	P
5	Q	U	V	X	Z

Le chiffrement s'effectue alors en remplaçant chaque lettre par les deux chiffres : ligne colonne qui indiquent sa position dans la grille.
Par exemple, F est chiffré 31.

Ce chiffrement est-il polyalphabétique ?

Déchiffrer le message suivant

```
421513 132243 324244 141342 444332 132515 135334 444244
431325 154222 521444 114315 234215 131315 431411 444324
441552 212552 431542 224332 521552 211144 434414 444315
```

2.4.5 Écrire une fonction `CodageVigenere(texte,cle)` qui a deux paramètres : le texte à chiffrer et la clé.

2.4.6 Écrire une fonction `DecodageVigenere(texteChiffre,cle)` qui a deux paramètres : le texte à déchiffrer et la clé.

2.5 Plus grand diviseur commun et plus petit multiple commun

2.5.1 Soit a et b deux entiers positifs. On note $\gcd(a, b)$, de l'anglais *greatest common divisior*, le plus grand diviseur commun de a et b.

Montrer que $\gcd(a, b)$ existe.

On dira de plus que a et b sont *premiers entre eux* si $\gcd(a, b) = 1$

2.5.2 Trouver tous les diviseurs communs positifs de

a) 16 et 48,

b) 30 et 45,

c) 18 et 65.

2.5.3 Trouver le plus grand diviseur commun de

a) 35 et 65,

b) 135 et 156,

c) 49 et 99.

2.5.4 Trouver le plus grand diviseur commun de 17017 et 19210.

2.5.5 Trouver le plus grand diviseur commun de de 21331 et de 43947. (L'utilisation d'une calculette peut être judicieuse.)

2.5.6 Trouver le plus grand diviseur commun de de 210632 et de 423137. (L'utilisation d'un ordinateur peut être judicieuse.)

2.5.7 Montrer que pour tout $n \in \mathbb{N}$, n et $n + 1$ sont premiers entre eux.

2.5.8 Montrer que si $a \mid b$, alors $\gcd(a, b) = a$.

2.5.9 Soit a et b deux nombres entiers. Supposons qu'il existe r et s deux nombres, également entiers, tels que $a \cdot r + b \cdot s = 1$. Montrer que a et b sont premiers entre eux.

2.6 Factoriser un nombre entier

2.6.1 Un nombre supérieur à 1 est dit *premier* s'il a exactement deux diviseurs : 1 et lui-même. Les nombres qui ne sont pas premiers sont dits *composés*.

Soit $n \in \mathbb{N}$ un nombre composé. Montrer que n admet un facteur inférieur ou égal à $\sqrt{n}$.

2.6.2 A l'aide du crible d'Eratosthène, déterminer « à la main » les nombres premiers inférieurs à 500.

2	3	5	7	9	11	13	15	17	19
21	23	25	27	29	31	33	35	37	39
41	43	45	47	49	51	53	55	57	59
61	63	65	67	69	71	73	75	77	79
81	83	85	87	89	91	93	95	97	99
101	103	105	107	109	111	113	115	117	119
121	123	125	127	129	131	133	135	137	139
141	143	145	147	149	151	153	155	157	159
161	163	165	167	169	171	173	175	177	179
181	183	185	187	189	191	193	195	197	199
201	203	205	207	209	211	213	215	217	219
221	223	225	227	229	231	233	235	237	239
241	243	245	247	249	251	253	255	257	259
261	263	265	267	269	271	273	275	277	279
281	283	285	287	289	291	293	295	297	299
301	303	305	307	309	311	313	315	317	319
321	323	325	327	329	331	333	335	337	339
341	343	345	347	349	351	353	355	357	359
361	363	365	367	369	371	373	375	377	379
381	383	385	387	389	391	393	395	397	399
401	403	405	407	409	411	413	415	417	419
421	423	425	427	429	431	433	435	437	439
441	443	445	447	449	451	453	455	457	459
461	463	465	467	469	471	473	475	477	479
481	483	485	487	489	491	493	495	497	499

2.6.3 Ecrire un programme en python qui renvoie la liste de tous les nombres premiers inférieurs à 10^6. Utiliser le crible d'Eratosthène.

2.6.4 Trouver un facteur de 4841.

2.6.5 Montrer que 521 est un nombre premier.

2.6.6 Factoriser les nombres ci-dessous.

a) 200	e) 35	i) 713	m) 4897
b) 150	f) 77	j) 1147	n) 6319
c) 128	g) 143	k) 473	o) 1591
d) 164	h) 323	l) 493	p) 901

2.7 Puissances modulo un nombre entier

2.7.1 Effectuer les calculs ci-dessous et réduire le résultat modulo 7.

a) 5^6 b) 2^6 c) 4^6 d) 6^6

2.7.2 Effectuer les calculs ci-dessous et réduire le résultat modulo 17.

a) 8^{16} b) 2^{16} c) 11^{16} d) 5^{16}

2.7.3 Effectuer les calculs ci-dessous :

a) $3^5 \mod 5$
b) $2^5 \mod 5$
c) $3^7 \mod 7$
d) $5^7 \mod 7$
e) $6^7 \mod 7$
f) $5^{13} \mod 13$
g) $11^{13} \mod 13$
h) $10^{19} \mod 19$
i) $2^{19} \mod 19$
j) $8^{19} \mod 19$
k) $12^{17} \mod 17$
l) $10^{17} \mod 17$

Que peut-on en déduire ?

2.7.4 Établir la table de multiplication de $\mathbb{Z}_{15}$.

2.7.5 Trouver l'inverse de 13 dans $\mathbb{Z}_{15}$.

2.7.6 Donner la liste de tous les nombres inversibles de $\mathbb{Z}_{15}$.

2.7.7 Expliquer pourquoi si a est inversible dans $\mathbb{Z}_{15}$, alors

$$a^8 \equiv 1 \mod 15$$

2.7.8 Établir la table de multiplication de $\mathbb{Z}_{21}$.

2.7.9 Trouver l'inverse de 13 dans $\mathbb{Z}_{21}$.

2.7.10 Donner la liste de tous les nombres inversibles de $\mathbb{Z}_{21}$.

2.7.11 Expliquer pourquoi si a est inversible dans $\mathbb{Z}_{21}$, alors

$$a^{12} \equiv 1 \mod 21$$

2.7.12 Effectuer les calculs ci-dessous :

a) $25^5 \mod 133$
b) $100^{65} \mod 133$
c) $107^5 \mod 133$
d) $46^{65} \mod 133$
e) $234^{65} \mod 667$
f) $447^{65} \mod 667$
g) $99^{417} \mod 667$
h) $664^{65} \mod 667$

2.7.13 Soit $p = 23$ et $q = 31$. On donne encore $e = 17$.

a) Calculer d, l'inverse de e modulo $(p-1)\cdot(q-1) = 22\cdot 30 = 660$.

b) Ecrire la clef privée correspondante.

c) Ecrire la clef publique correspondante.

d) Chiffrer le « message » $m = 333$ en utilisant la formule

$$c = m^e \mod n$$

si $n = p \cdot q$.

e) Retrouver le message à partir du chiffre c en utilisant la formule

$$m = c^d \mod n$$

f) Chiffrer $m = 555$.

g) Déchiffrer $c = 100$.

2.7.14 Soit $p = 13$ et $q = 19$. On donne encore $e = 11$.

a) Calculer d, l'inverse de e modulo $(p-1)\cdot(q-1)$.

b) Ecrire la clef privée correspondante.

c) Ecrire la clef publique correspondante.

d) Chiffrer le « message » $m = 123$ en utilisant la formule

$$c = m^e \mod n$$

si $n = p \cdot q$.

e) Retrouver le message à partir du chiffre c en utilisant la formule

$$m = c^d \mod n$$

f) Chiffrer $m = 222$.

g) Déchiffrer $c = 55$.

2.7.15 Soit $p = 7$ et $q = 23$. On donne encore $e = 5$.

a) Calculer d, l'inverse de e modulo $(p-1)\cdot(q-1)$.

b) Ecrire la clef privée correspondante.

c) Ecrire la clef publique correspondante.

d) Chiffrer le « message » $m = 111$ en utilisant la formule

$$c = m^e \mod n$$

si $n = p \cdot q$.

e) Retrouver le message à partir du chiffre c en utilisant la formule

$$m = c^d \mod n$$

f) Chiffrer $m = 22$. Commenter le résultat.

g) Déchiffrer $c = 100$.

2.8 Théorie des nombres

2.8.1 Démontrer les propriétés de la relation de divisibilité suivantes :

a) si $m \mid n$ et $m \mid r$, alors $m \mid (n+r)$ et $m \mid (n-r)$;

b) si $m \mid n$ et $r \in \mathbb{Z}$, alors $m \mid r\,n$;

c) si r, m et $n \in \mathbb{Z}$, et $r \neq 0$, alors $m \mid n$ si et seulement si $r\,m \mid r\,n$;

d) si $m \mid n$ et si $n \mid r$, alors $m \mid r$.

2.8.2 Quels sont les diviseurs de 0 ?

2.8.3 Écrire en un programme qui cherche les nombres premiers inférieurs à n à l'aide du crible d'Ératosthène.

2.8.4 Déterminer la décomposition en facteurs premiers du nombre 4027 à l'aide de la machine à calculer seulement.
Idem avec 4087.

2.8.5 Idem avec 716539 et 1488391.

2.8.6 Démontrer les propriétés de la relation de congruence suivantes :

a) $a \equiv a \pmod{n}$;

b) si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$;

c) si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$;

d) tout nombre a est congru modulo n au reste de la division de a par n ;

e) on a $a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste après division par n ;

f) si $a \equiv c \pmod{n}$ et si $b \equiv d \pmod{n}$, alors $a+b \equiv c+d \pmod{n}$ et $a\,b \equiv c\,d \pmod{n}$

2.8.7 Trouver une dizaine de nombres entiers congrus à 22 modulo 7.

2.8.8 On donne un nombre naturel a. Chercher son reste après division par n.

a) $a = 111$; $n = 2, 3, 4, \ldots, 12$;

b) $a = 123456789 \cdot 987654321$; $n = 2$, $n = 9$, $n = 11$;

c) $a = 22^{22}$, $n = 3$, $n = 9$, $n = 10$, $n = 11$;

d) $a = 1234^5$, $n = 9$, $n = 11$, $n = 99$;

e) $a = 2^{64} - 1, = 2, n = 3, n = 9$.

2.8.9 Si n est un nombre naturel, la n-ième puissance d'un nombre a est, par définition, le produit de n facteurs égaux à a. Ainsi, d'après cette définition, le calcul de a^n nécessite $n - 1$ multiplications. On peut cependant obtenir le même résultat en effectuant moins d'opérations.
Voici à titre d'exemple l'évaluation de a^{35}.

— On écrit l'exposant n comme une somme de puissance de 2. Ici, $35 = 32 + 2 + 1$;
— on calcule ensuite les puissances paires de a : $a^2 = a \cdot a$, $a^4 = a^2 \cdot a^2$, $a^8 = a^4 \cdot a^4$, $a^{16} = a^8 \cdot a^8$, $a^{32} = a^{16} \cdot a^{16}$.
— on multiplie pour terminer les « bons » carrés : $a^{35} = a^{32} \cdot a^2 \cdot a^1$;
Le nombre de multiplications nécessaires est dans ce cas de 7, au lieu de 34.

a) Combien de multiplications nécessite cet algorithme pour calculer chacune des puissances suivantes : a^{10}, a^{61}, a^{1000} ?

b) Calculer $835^{25} \pmod{1073}$, en 6 multiplications.

2.8.10 Calculer $\text{pgcd}(987, 610)$ à l'aide de l'énumération des diviseurs, puis à l'aide de l'algorithme d'Euclide.

2.8.11 Calculer à l'aide de l'algorithme d'Euclide le pgcd des nombres a et b suivants :

a) $a = 1233$, $b = 9999$;

b) $a = 12345$, $b = 54321$;

2.8.12 Calculer les nombres s et t tels que $s \cdot a + t \cdot b = \text{pgcd}(a, b)$, avec les nombres a et b suivants :

a) $a = 72$, $b = 39$;

b) $a = 1008$, $b = 25$;

c) $a = 1993$, $b = 210$;

d) $a = 1995$, $b = 323$.

2.8.13 Montrer que $\text{pgcd}(n, 0) = n$, quel que soit l'entier naturel n.

2.8.14 Écrire un programme qui calcule le pgcd de deux nombres entiers a et b à l'aide de l'algorithme d'Euclide.

2.8.15 Modifier le programme de l'exercice précédent de façon à calculer à l'aide de l'algorithme d'Euclide étendu les nombres s et t tels que $a \cdot s + b \cdot t = \text{pgcd}(a, b)$.

2.8.16 Calculer $\varphi(n)$ dans les cas suivants :

a) $n = 4$, $n = 8$, $n = 16$, $n = 32$;

b) $n = 3$, n =9, $n = 27$, $n = 81$;

c) $n = 7^5$;

d) $n = 4027$;

e) $n = 4087$;

2.8.17 Montrer que, pour tout nombre naturel n, les nombres n et $n^2 + 1$ sont premiers entre eux.

2.9 Systèmes cryptographiques modernes : la clé publique

2.9.1 Chiffrer et déchiffrer le message $m = 8$ à l'aide du système RSA, avec $p = 7$, $q = 11$ et $e = 17$.

2.9.2 Connaissant la clef publique (n, e) d'un individu, déterminer la clé privée d dans les cas suivants :

a) $n = 1073$, $e = 117$;

b) $n = 1073$, $e = 115$;

c) $n = 111$, $e = 31$;

d) $n = 117$, $e = 17$;

e) $n = 105$, $e = 13$;

f) $n = 10001$, $e = 187$.

2.9.3 Un ennemi intercepte le message chiffré $c = 10$, dont le destinataire possède la clef publique $e = 5$, $n = 35$. Quel est le texte clair m ?

2.9.4 Un professeur envoie ses notes au secrétariat de l'école par mail. La clef publique du professeur est (3; 55) et celle du secrétariat est (3; 33).

a) Vérifier que la clef du professeur (supposée connue de lui seul) est 27 et que celle du secrétariat est 7.

b) Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef RSA du secrétariat. Quel est le message chiffré qui correspond à la note 12 ?

c) Pour assurer l'authenticité des messages contenant les notes, le professeur signe ses messages pour le secrétariat après les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?

2.9.5 Définir les termes cryptographie, cryptanalyse et cryptologie.

2.9.6 Bob utilise le protocole RSA et publie sa clef publique $N = 187$ et $e = 3$.

a) Encoder le message $m = 15$ avec la clef publique de Bob.

b) En utilisant le fait que $\varphi(N) = 160$, retrouver la factorisation de N, puis la clef privee de Bob.

2.9.7 Bob$_1$ et Bob$_2$ ont pour clef publique RSA respectivement (N, e_1) et (N, e_2) avec e_1 et e_2 premiers entre eux.
Alice envoie le même message m crypté avec les clefs publiques RSA de Bob$_1$ et Bob$_2$ en c_1 et c_2.
Expliquer comment Eve, qui intercepte les deux messages cryptés et qui connait les clefs publiques de Bob$_1$ et Bob$_2$, peut retrouver le message clair m.

2.9.8 Supposons que l'entier n soit le produit de deux nombres premiers p et q proches (on peut toujours supposer que $p > q$).
On pose $t = \dfrac{p+q}{2}$ et $s = \dfrac{p-q}{2}$.
Montrer que :

a) l'entier s est petit ;

b) $n = t^2 - s^2$;

c) t est légèrement supérieur à la racine carrée de n ;

d) à l'aide de ces informations, écrire un programme pour factoriser n ;

e) appliquer cet algorithme pour factoriser 899, 110417 et 364957402 ;

f) Trouver la clef secrète d correspondante à ($n = 51983$, $e = 17$).

2.9.9 Le fichier `nombres_p_q_1.txt` contient deux nombres premiers `p` et `q`.
On choisit `e = 65537` qui satisfait la condition $\gcd(e, \varphi(n)) = 1$, où $n = p \cdot q$. On dispose ainsi d'une clé publique `(n, e)`.

a) Dans un fichier `clef.py`, construire la clé privée `(n, d)`. Afficher à la console la valeur de `d`.

b) Coder le message suivant (présent dans `message_1.txt`) à l'aide de la clé publique `(n, e)` et l'afficher à la console :

   1212121212121212121212121212121212121212121212121212121212

c) Décoder le message chiffré suivant (présent dans `chiffre_1.txt`) à l'aide de la clé privée `(n, d)` et l'afficher à la console.

```
25567439145662233958692485794698610817081042607044
76375740884794753357993630922231929342522549252625
83666181770268506210137463778407056604376942495443
54344442167885488175571510178529674397470719290002
50564288716583429743123017673776013168016434939838
37662442086433370446824338338022627966782937829223
36951763006508399321713627145581271533380725975341
78087248990732332457837418659413481406361983817252
46437822132392448183737304695659768807011137853820
```

```
23696953041028388595531536455164593424945746561789
34884366199670482448616653509555427947511254862696
41398200342295055677990818953963680224811410674869
657356236000829
```

2.10 Solutions des exercices

2.1.1

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

2.1.2

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2.1.3 $\mathbb{Z}_{26} = \{0, 1, 2, 3, 4, 5, \ldots, 20, 21, 22, 23, 24, 25\}$

2.1.4

a) 15
b) 22
c) 22
d) 23
e) 0
f) 25
g) 17
h) 7
i) 1
j) 2
k) 1
l) 4
m) 23
n) 21
o) 15
p) 6

2.1.5

a) 8
b) 17
c) 19
d) 16
e) 8
f) 15
g) 22
h) 9

2.1.6

a) $1 + 7 = 8$
b) $15 + 2 = 17$
c) $9 + 10 = 19$
d) $20 + 22 = 42 \equiv 16 \mod 26$
e) $2 - 20 = -18 \equiv 8 \mod 26$
f) $1 - 12 = -11 \equiv 15 \mod 26$

g) $4 + 18 = 22$

h) $21 + 14 = 35 \equiv 9 \mod 26$

Le résultat final n'est pas modifié.

2.1.7

a) 18

b) 20

c) 24

d) 6

e) 4

f) 24

g) 19

h) 9

i) 10

j) 16

k) 20

l) 2

m) 18

n) 24

o) 18

p) 10

2.1.8

a) $27 \cdot 33 = 891 \equiv 7 \mod 26$, vu que $891 = 34 \cdot 26 + 7$

b) $41 \cdot 28 = 1148 \equiv 4 \mod 26$, vu que $1148 = 44 \cdot 26 + 4$

c) $72 \cdot 100 = 7200 \equiv 24 \mod 26$, vu que $7200 = 276 \cdot 26 + 24$

d) $132 \cdot 150 = 19800 \equiv 14 \mod 26$, vu que $19800 = 761 \cdot 26 + 14$

e) $53 \cdot 12 = 636 \equiv 12 \mod 26$, vu que $636 = 24 \cdot 26 + 12$

f) $30 \cdot 8 = 240 \equiv 6 \mod 26$, vu que $240 = 10 \cdot 26 - 20$

g) $(-5) \cdot 12 = -60 \equiv 18 \mod 26$, vu que $-60 = (-2) \cdot 26 - 8$

2.1.9

a) $1 \cdot 7 = 7$

b) $15 \cdot 20 = 30 \equiv 4 \mod 26$

c) $9 \cdot 10 = 90 \equiv 12 \mod 26$

d) $20 \cdot 22 = 440 = 16 \cdot 26 + 24 \equiv 24 \mod 26$

e) $2 \cdot 20 = 40 \equiv 14 \mod 26$

f) $1 \cdot 12 = 12$

g) $4 \cdot 8 = 32 \equiv 6 \mod 26$

h) $21 \cdot 12 = 252 = 9 \cdot 26 + 18 \equiv 18 \mod 26$

Le résultat final n'est pas modifié.

2.2.1

```
M = (8, 11, 24, 0, 2, 4, 20, 23, 16, 20, 8, 14, 13, 19, 20,
     13, 15, 8, 18, 19, 14, 11, 4, 19, 2, 7, 0, 17, 6, 4)
```

2.2.2

```
ETCEUXQUICREUSENT
```

2.2.3

```
C = (7, 22, 5, 7, 23, 0, 19, 23, 11, 5, 20, 7, 23, 21, 7, 16, 22)
```

2.2.4

```
LOBDFHXATXLRQWXQSLVWROHWFKDUJH
```

2.2.5

```
ETCEUXQUICREUSENT
```

2.2.6

```
m = TOITU
C = (0, 21, 15, 0, 1)
```

2.2.7 Le décalage permettant de déchiffrer vaut $26 - 7 = 19$.

```
M = (2, 17, 4, 20, 18, 4, 18)
m = CREUSES
```

2.2.8 Il y a 25 décalages si l'on excepte le « décalage 0 » qui n'est pas intéressant.

2.2.9 $c = 26 - n$

2.2.10 $c = 26 - 13 = 13$; c'est le seul décalage qui permet de chiffrer et déchiffrer avec la même clef.

2.2.11 On procède *par force brute* : On teste les 25 décalages différents de 0 et on trouve la ligne qui a une signification.

```
ARZTLVZCCZTVSIZEUVSILPVIV
BSAUMWADDAUWTJAFVWTJMQWJW
CTBVNXBEEBVXUKBGWXUKNRXKX
DUCWOYCFFCWYVLCHXYVLOSYLY
EVDXPZDGGDXZWMDIYZWMPTZMZ
FWEYQAEHHEYAXNEJZAXNQUANA
GXFZRBFIIFZBYOFKABYORVBOB
HYGASCGJJGACZPGLBCZPSWCPC
IZHBTDHKKHBDAQHMCDAQTXDQD
*************************
JAICUEILLICEBRINDEBRUYERE
*************************
KBJDVFJMMJDFCSJOEFCSVZFSF
LCKEWGKNNKEGDTKPFGDTWAGTG
MDLFXHLOOLFHEULQGHEUXBHUH
NEMGYIMPPMGIFVMRHIFVYCIVI
OFNHZJNQQNHJGWNSIJGWZDJWJ
PGOIAKORROIKHXOTJKHXAEKXK
QHPJBLPSSPJLIYPUKLIYBFLYL
RIQKCMQTTQKMJZQVLMJZCGMZM
SJRLDNRUURLNKARWMNKADHNAN
TKSMEOSVVSMOLBSXNOLBEIOBO
ULTNFPTWWTNPMCTYOPMCFJPCP
```

```
VMUOGQUXXUOQNDUZPQNDGKQDQ
WNVPHRVYYVPROEVAQROEHLRER
XOWQISWZZWQSPFWBRSPFIMSFS
YPXRJTXAAXRTQGXCSTQGJNTGT
ZQYSKUYBBYSURHYDTURHKOUHU
```

S'il n'y a pas d'ordinateur à disposition, on peut se mettre à plusieurs et chacun essaye un ou deux décalages.

2.2.12

```
M = (9, 0, 12, 0, 8, 18, 15, 4, 17, 18, 14, 13, 13, 4, 13, 0, 21, 0, 8,
     19, 4, 19, 4, 0, 20, 18, 18, 8, 19, 17, 14, 15, 5, 14, 17, 19)
C = (7, 24, 10, 24, 6, 16, 13, 2, 15, 16, 12, 11, 11, 2, 11, 24, 19, 24,
     6, 17, 2, 17, 2, 24, 18, 16, 16, 6, 17, 15, 12, 13, 3, 12, 15, 17)
c = HYKYGQNCPQMLLCLYTYGRCRCYSQQGRPMNDMPR
```

2.2.13

```
C = (15, 4, 23, 18, 19, 12, 22, 22, 12, 23, 24, 7, 8, 8, 23, 15, 4, 22,
     8, 7, 24, 6, 23, 12, 25, 12, 23, 8)
M = (11, 0, 19, 14, 15, 8, 18, 18, 8, 19, 20, 3, 4, 4, 19, 11, 0, 18, 4,
     3, 20, 2, 19, 8, 21, 8, 19, 4)
m = LATOPISSITUDEETLASEDUCTIVITE
```

2.2.14

```
m = JESUISLAMAUVAISEHERBEBRAVESGENSBRAVESGENS
```

2.3.1

a) Non ; en effet, il faut que a soit inversible modulo 26. En clair, il doit exister un nombre dans $\mathbb{Z}_{26}$, noté a', tel que $a \cdot a' \equiv 1 \mod 26$.

b) Le nombre b peut être choisi au hasard dans $\mathbb{Z}_{26}$.

2.3.2

`c = WDLDRPAXKPVQQXQDEDRUXUXDZPPRUKVACVKU`

2.3.3

`m = LATOPISSITUDEETLASEDUCTIVITE`

2.3.4 Soit a' tel que $a' \cdot a \equiv 1 \mod 26$. On peut écrire

$$z = a' \cdot (z' - b) = a' \cdot z' - a' \cdot b$$

2.4.1 a) VVVIXGGTPTMOFVADWST
b) INTROUVABLE
c) THEOBALD

2.4.2 Vigenère apporte un plus car une même lettre peut être chiffrée différemment dans le texte ce qui complique l'analyse statistique. Vigenère est donc plus solide.

2.4.3

a) vvvixggtptmofvadwst

b) -

2.4.4 Les sanglots longs des violons de l'automne blessent mon cœur d'une langueur monotone

2.4.5 –

2.4.6 –

2.5.1 L'ensemble D des diviseurs communs de a et b n'est pas vide, car $1 \mid a$ et $1 \mid b$. Vu que l'ensemble des diviseurs de a est fini, D est également fini. Vu que D est fini, cet ensemble admet un maximum, noté d. Le nombre d n'est autre que $\gcd(a, b)$.

2.5.2

a) $\{1, 2, 4, 8, 16\}$,

b) $\{1, 3, 5, 15\}$,

c) $\{1\}$.

2.5.3

a) 5

b) 3

c) 1

2.5.4 17

2.5.5 $21331 = 83 \cdot 257$ et $43947 = 3 \cdot 3 \cdot 19 \cdot 257$.
On peut donc écrire $\gcd(21331, 43947) = 257$.

2.5.6 $210632 = 2 \cdot 2 \cdot 2 \cdot 113 \cdot 233$ et $423137 = 11 \cdot 11 \cdot 13 \cdot 269$.
On peut donc écrire $\gcd(21331, 43947) = 1$.

2.5.7 Soit $m \in \mathbb{N}$ tel que $m \mid n$ et $m \mid (n+1)$. Le nombre m doit alors diviser la différence $(n + 1) - n$. Ce qui fait que $m \mid 1$. Cela implique finalement que $m = 1$. On a donc $\gcd(n, n + 1) = 1$.

2.5.8 Supposons que $a \mid b$. Dans ce cas, a est un diviseur commun de a et b. C'est forcément le plus grand, car si $d \mid a$, alors $d \leq a$.

2.5.9 Notons $d = \gcd(a, b)$. On sait que $d \mid a$ et $d \mid b$, ce qui fait que $d \mid a \cdot r$ et $d \mid b \cdot r$. Par conséquent, $d \mid (a \cdot r + b \cdot s)$. Finalement, $d \mid 1$ et donc $d = 1$.

2.6.1 Soit n un nombre entier composé. Cela signifie que $n = a \cdot b$ avec a et b des entiers différents de 1. Supposons que $a > \sqrt{n}$ et que $b > \sqrt{n}$. On peut, dans ce cas, écrire que $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, ce qui est contradictoire. L'un des deux facteurs est donc plus petit ou égal à $\sqrt{n}$.

2.6.2

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229

233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499					

2.6.3

```
def listePremiers(borne):
    liste_premiers = list(range(3, borne, 2))
    liste_premiers = [2] + liste_premiers
    r = int(borne**(1/2))

    n = 3
    j = 1
    t = len(liste_premiers)

    while n <= r:
        for i in range(j + n, t, n):
            if liste_premiers[i]:
                liste_premiers[i] = 0
        j += 1
        while not liste_premiers[j]:
            j += 1
        n = liste_premiers[j]

    premiers = []
    for p in liste_premiers:
        if p:
            premiers.append(p)
    return premiers
```

2.6.4 $4841 = 103 \cdot 47$

2.6.5 Vu que $\sqrt{521} \simeq 22.83$, si 521 n'admet pas de facteur premier inférieur à 22, c'est un nombre premier. Aucun des nombres de la liste

$$(2, 3, 5, 7, 11, 13, 17, 19)$$

n'étant un diviseur de 521, c'est un nombre premier.

2.6.6 On donne ci-dessous la liste des facteurs premiers de chaque nombre :

a) $(2, 2, 2, 5, 5)$ e) $(5, 7)$ i) $(23, 31)$ m) $(59, 83)$

b) $(2, 3, 5, 5)$ f) $(7, 11)$ j) $(31, 37)$ n) $(71, 89)$

c) $(2, 2, 2, 2, 2, 2, 2)$ g) $(11, 13)$ k) $(11, 43)$ o) $(37, 43)$

d) $(2, 2, 41)$ h) $(17, 19)$ l) $(17, 29)$ p) $(17, 53)$

2.7.1 Pour tout $1 \leq a \leq 6$, on a $a^6 \equiv 1 \mod 7$.

2.7.2 Pour tout $1 \leq a \leq 16$, on a $a^{16} \equiv 1 \mod 17$.

2.7.3 On peut émettre l'hypothèse que si p est premier, alors $a^p \equiv a \mod p$. C'est un théorème, appelé le « petit théorème de Fermat ».

2.7.4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	0	9	3	12	6	0	9	3	12	6	0	9	3	12	6

10	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

2.7.5 Comme on peut le voir dans la table de multiplication établie à l'exercice 2.7.4, le nombre 1 se trouve à l'intersection de la ligne numéro 13 et de la colonne numéro 7. Cela signifie que $7 \cdot 13 \equiv 1 \mod 15$ et que donc, modulo 15, l'inverse de 13 est 7.

2.7.6 La liste de tous les nombres inversibles modulo 15 est la suivante :

$$(1, 2, 4, 7, 8, 11, 13, 14)$$

2.7.7 Soit $(1, 2, 4, 7, 8, 11, 13, 14)$ la liste des nombres inversibles de $\mathbb{Z}_{15}$ et a un nombre de cette liste. Il a 8 nombres inversibles. On construit une nouvelle liste comme suit :

$$\ell = (a \cdot 1, a \cdot 2, a \cdot 4, a \cdot 7, a \cdot 8, a \cdot 11, a \cdot 13, a \cdot 14)$$

Voyons pourquoi cette liste ne compte que des éléments distincts : Soit $a \cdot z_1$ et $a \cdot z_2$ deux éléments de ℓ et supposons que

$$a \cdot z_1 \mod 15 = a \cdot z_2 \mod 15$$

Notons encore a' l'inverse de a modulo 15. On a alors

$$a' \cdot a \cdot z_1 \mod 15 = a' \cdot a \cdot z_2 \mod 15$$

ce qui veut dire que

$$z_1 \mod 15 = z_2 \mod 15$$

vu que $a' \cdot a \mod 15 = 1$. Cela signifie que si $z_1 \neq z_2$, alors $a \cdot z_1 \neq a \cdot z_2$, modulo 15 bien entendu.

La liste ℓ compte donc 8 éléments, tous inversibles, vu que l'inverse de $a \cdot z$ est donné par $z' \cdot a'$ si z' désigne l'inverse de z modulo 15. On peut donc dire que ℓ est la liste des inversibles de $\mathbb{Z}_{15}$, éventuellement placés dans un ordre différent.

Cela signifie que

$$1\cdot 2\cdot 4\cdot 7\cdot 8\cdot 11\cdot 13\cdot 14\equiv a\cdot 1\cdot a\cdot 2\cdot a\cdot 4\cdot a\cdot 7\cdot a\cdot 8\cdot a\cdot 11\cdot a\cdot 13\cdot a\cdot 14 \mod 15$$

et donc que

$$1\cdot 2\cdot 4\cdot 7\cdot 8\cdot 11\cdot 13\cdot 14\equiv 1\cdot 2\cdot 4\cdot 7\cdot 8\cdot 11\cdot 13\cdot 14\cdot a\cdot a\cdot a\cdot a\cdot a\cdot a\cdot a\cdot a \mod 15$$

Après simplification, on obtient $1\equiv a^8 \mod 15$. La simplification est possible vu que tous les nombres impliqués dans l'écriture ci-dessus sont des inversibles.

2.7.8

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	0	2	4	6	8	10	12	14	16	18	20	1	3	5	7	9	11	13	15	17	19
3	0	3	6	9	12	15	18	0	3	6	9	12	15	18	0	3	6	9	12	15	18
4	0	4	8	12	16	20	3	7	11	15	19	2	6	10	14	18	1	5	9	13	17
5	0	5	10	15	20	4	9	14	19	3	8	13	18	2	7	12	17	1	6	11	16
6	0	6	12	18	3	9	15	0	6	12	18	3	9	15	0	6	12	18	3	9	15
7	0	7	14	0	7	14	0	7	14	0	7	14	0	7	14	0	7	14	0	7	14
8	0	8	16	3	11	19	6	14	1	9	17	4	12	20	7	15	2	10	18	5	13
9	0	9	18	6	15	3	12	0	9	18	6	15	3	12	0	9	18	6	15	3	12
10	0	10	20	9	19	8	18	7	17	6	16	5	15	4	14	3	13	2	12	1	11
11	0	11	1	12	2	13	3	14	4	15	5	16	6	17	7	18	8	19	9	20	10
12	0	12	3	15	6	18	9	0	12	3	15	6	18	9	0	12	3	15	6	18	9
13	0	13	5	18	10	2	15	7	20	12	4	17	9	1	14	6	19	11	3	16	8
14	0	14	7	0	14	7	0	14	7	0	14	7	0	14	7	0	14	7	0	14	7
15	0	15	9	3	18	12	6	0	15	9	3	18	12	6	0	15	9	3	18	12	6
16	0	16	11	6	1	17	12	7	2	18	13	8	3	19	14	9	4	20	15	10	5
17	0	17	13	9	5	1	18	14	10	6	2	19	15	11	7	3	20	16	12	8	4
18	0	18	15	12	9	6	3	0	18	15	12	9	6	3	0	18	15	12	9	6	3
19	0	19	17	15	13	11	9	7	5	3	1	20	18	16	14	12	10	8	6	4	2
20	0	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

2.7.9 On voit dans la table que $13 \cdot 13 \equiv 1 \mod 21$. Le nombre 13 est son propre inverse dans $\mathbb{Z}_{21}$.

2.7.10 $(1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20)$

2.7.11 Il y a 12 inversibles dans $\mathbb{Z}_{21}$. Un argument analogue à celui donné à l'exercice 2.7.7 donne la congruence $a^{12} \equiv 1 \mod 21$ si a est inversible.

2.7.12

a) $25^5 \mod 133$

```
25^1 mod 133 = 25
25^2 mod 133 = 93
25^4 mod 133 = 4
25 * 4 mod 133 = 100
```

b) $100^{65} \mod 133$

```
100^1 mod 133 = 100
100^2 mod 133 = 25
100^4 mod 133 = 93
100^8 mod 133 = 4
100^16 mod 133 = 16
100^32 mod 133 = 123
100^64 mod 133 = 100
100 * 100 mod 133 = 25
```

c) $107^5 \mod 133$

```
107^1 mod 133 = 107
107^2 mod 133 = 11
107^4 mod 133 = 121
107 * 121 mod 133 = 46
```

d) $46^{65} \mod 133$

```
46^1 mod 133 = 46
46^2 mod 133 = 121
46^4 mod 133 = 11
46^8 mod 133 = 121
46^16 mod 133 = 11
46^32 mod 133 = 121
46^64 mod 133 = 11
46 * 11 mod 133 = 107
```

e) $234^{65} \mod 667$

```
234^1 mod 667 = 234
234^2 mod 667 = 62
234^4 mod 667 = 509
234^8 mod 667 = 285
234^16 mod 667 = 518
234^32 mod 667 = 190
234^64 mod 667 = 82
234 * 82 mod 667 = 512
```

f) $447^{65} \mod 667$

```
447^1 mod 667 = 447
447^2 mod 667 = 376
447^4 mod 667 = 639
447^8 mod 667 = 117
447^16 mod 667 = 349
447^32 mod 667 = 407
447^64 mod 667 = 233
447 * 233 mod 667 = 99
```

g) $99^{417} \mod 667$

```
99^1 mod 667 = 99
```

```
99^2 mod 667 = 463

99^4 mod 667 = 262

99^8 mod 667 = 610

99^16 mod 667 = 581

99^32 mod 667 = 59

99^64 mod 667 = 146

99^128 mod 667 = 639

99^256 mod 667 = 117

99 * 59 * 639 * 117 mod 667 = 447
```

h) $664^{65} \mod 667$

```
664^1 mod 667 = 664

664^2 mod 667 = 9

664^4 mod 667 = 81

664^8 mod 667 = 558

664^16 mod 667 = 542

664^32 mod 667 = 284

664^64 mod 667 = 616

664 * 616 mod 667 = 153
```

2.7.13 Soit $p = 23$ et $q = 31$. On donne encore $e = 17$.

a) Calculer d, l'inverse de e modulo $(p-1)\cdot(q-1) = 22\cdot 30 = 660$.

```
660 = 1 * 660 + (0) * 17

17 = 0 * 660 + (1) * 17

14 = 1 * 660 + (-38) * 17

3 = -1 * 660 + (39) * 17

2 = 5 * 660 + (-194) * 17

1 = -6 * 660 + (233) * 17
```

b) Ecrire la clef privée correspondante :

$$(23; 31; 233)$$

c) Ecrire la clef publique correspondante :

$$(713; 17)$$

d) Chiffrer le « message » $m = 333$ en utilisant la formule

$$c = m^e \mod n$$

si $n = p \cdot q$.

```
333^1 = 333
333^2 = 374
333^4 = 128
333^8 = 698
333^16 = 225
333 * 225 = 60
```

e) Retrouver le message à partir du chiffre c en utilisant la formule

$$m = c^d \mod n$$

```
60^1 = 60
60^2 = 35
60^4 = 512
60^8 = 473
60^16 = 560
60^32 = 593
60^64 = 140
60^128 = 349
60 * 473 * 593 * 140 * 349 = 333
```

f) Chiffrer $m = 555$.

```
555^1 = 555
555^2 = 9
555^4 = 81
```

```
555^8 = 144
555^16 = 59
555 * 59 = 660
```

g) Déchiffrer $c = 100$.

```
100^1 = 100
100^2 = 18
100^4 = 324
100^8 = 165
100^16 = 131
100^32 = 49
100^64 = 262
100^128 = 196
100 * 165 * 49 * 262 * 196 = 41
```

2.7.14 Soit $p = 13$ et $q = 19$. On donne encore $e = 11$.

a) Calculer d, l'inverse de e modulo $(p-1) \cdot (q-1) = 12 \cdot 18 = 216$.

```
216 = 1 * 216 + (0) * 11
11 = 0 * 216 + (1) * 11
7 = 1 * 216 + (-19) * 11
4 = -1 * 216 + (20) * 11
3 = 2 * 216 + (-39) * 11
1 = -3 * 216 + (59) * 11
```

b) Ecrire la clef privée correspondante :

$$(13; 19; 59)$$

c) Ecrire la clef publique correspondante :

$$(247; 11)$$

d) Chiffrer le « message » $m = 123$ en utilisant la formule

$$c = m^e \mod n$$

si $n = p \cdot q$.

```
123^1 = 123
123^2 = 62
123^4 = 139
123^8 = 55
123 * 62 * 55 = 24
```

e) Retrouver le message à partir du chiffre c en utilisant la formule

$$m = c^d \mod n$$

```
24^1 = 24
24^2 = 82
24^4 = 55
24^8 = 61
24^16 = 16
24^32 = 9
24 * 82 * 61 * 16 * 9 = 123
```

f) Chiffrer $m = 222$.

```
222^1 = 222
222^2 = 131
222^4 = 118
222^8 = 92
222 * 131 * 92 = 40
```

g) Déchiffrer $c = 55$.

```
55^1 = 55
55^2 = 61
55^4 = 16
55^8 = 9
55^16 = 81
55^32 = 139
55 * 61 * 9 * 81 * 139 = 139
```

2.7.15 Soit $p = 7$ et $q = 23$. On donne encore $e = 5$.

a) Calculer d, l'inverse de e modulo $(p-1)\cdot(q-1) = 6 \cdot 22 = 132$.

```
132 = 1 * 132 + (0) * 5

5 = 0 * 132 + (1) * 5

2 = 1 * 132 + (-26) * 5

1 = -2 * 132 + (53) * 5
```

b) Ecrire la clef privée correspondante :

$$(7; 23; 53)$$

c) Ecrire la clef publique correspondante :

$$(161; 5)$$

d) Chiffrer le « message » $m = 111$ en utilisant la formule

$$c = m^e \mod n$$

si $n = p \cdot q$.

```
111^1 = 111

111^2 = 85

111^4 = 141

111 * 141 = 34
```

e) Retrouver le message à partir du chiffre c en utilisant la formule

$$m = c^d \mod n$$

```
34^1 = 34

34^2 = 29

34^4 = 36

34^8 = 8

34^16 = 64

34^32 = 71

34 * 36 * 64 * 71 = 111
```

f) Chiffrer $m = 22$.

```
22^1 = 22
22^2 = 1
22^4 = 1
22 * 1 = 22
```

Le chiffre est identique au message. C'est une situation critique, à éviter.

g) Déchiffrer $c = 100$.

```
100^1 = 100
100^2 = 18
100^4 = 2
100^8 = 4
100^16 = 16
100^32 = 95
100 * 2 * 16 * 95 = 32
```

2.8.1 —

2.8.2 —

2.8.3 —

2.8.4 4027 est un nombre premier

2.8.5 $4087 = 67 \cdot 67\,;\ 716539 = 83 \cdot 189 \cdot 197\,;\ 1488391 = 1217 \cdot 1223$

2.8.6 —

2.8.7 —

2.8.8 —

2.8.9 —

2.8.10 —

2.8.11 —

2.8.12 —

2.8.13 —

2.8.14 —

2.8.15 —

2.8.16 —

2.8.17 —

2.9.1 —

2.9.2 —

2.9.3 $m = 5$

2.9.4

a) Pour le professeur $\varphi(55) = 40$ et $27 \cdot 3 = 81 = 1 \pmod{40}$.

Pour le secrétariat $\varphi(33) = 20$ et $7 \cdot 3 = 21 = 1 \pmod{20}$.

b) Le professeur envoie $m = 12 \pmod{33}$. Or $12^2 = 12 \pmod{33}$; donc $m = 12 \pmod{33}$.

c) La note $\left(23^3 \pmod{55}\right)^7 \pmod{33} \equiv 12^7 \pmod{33} \equiv 12$.

2.9.5 La cryptographie est l'art de rendre inintelligible, de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance. Le chiffre, le code est le procédé, l'algorithme, la fonction, qui permet de crypter un message.

La cryptanalyse est l'art pour une personne non habilitée, de décrypter, de décoder, de déchiffrer, un message. C'est donc l'ensemble des procédés d'attaque d'un système cryptographique.

La cryptologie est l'ensemble formé de la cryptographie et de la cryptanalyse.

2.9.6

a) Le message codé est $c \equiv 15^3 \pmod{187} \equiv 9$.

b) Ecrivons $N = p\,q$. On a donc $\varphi(N) = (p-1)(q-1) = pq-p-q+1 = N-(p+q)+1$, et ainsi $p+q = N - \varphi(N) + 1 = 187 - 160 + 1 = 28$.

Les nombres p et q sont racines du polynôme

$$X^2 - (p+q)X + pq = X - 28\,X + 187$$

Le discriminant est $282 - 4 \cdot 187 = 36$ et ainsi $p = (28-6)/2 = 11$ et $q = (28+6)/2 = 17$.

2.9.7 Puisque e_1 et e_2 sont premiers entre eux, il existe deux entiers u et v tels que $u \cdot e_1 + v \cdot e_2 = 1$. Eve peut calculer u et v, et finalement retrouve le message en faisant

$$c_1{}^u \cdot c_2{}^v \equiv m^{u\,e_1} \cdot m^{v\,e_2} \equiv m^{u\,e_1 + v\,e_2} \equiv m \pmod{N}$$

2.9.8

```
# exemple
p=1093
q=1091
n=p*q

# algorithme
from math import sqrt

t=int(sqrt(n))
z=2
while int(sqrt(z)) != z:
    t += 1
    z = t**2-n

print('p=',t+sqrt(z))
```

Chapitre 3

Graphes

3.1 Généralités

3.1.1 Voici le plan des bus de notre région.

a) Ce plan est-il un graphe ?

b) Que représentent les sommets ?

c) Que représentent les arêtes ?

d) Ce graphe est-il connexe ?

e) Ce graphe est-il simple ou orienté ?

f) Quel est le degré du sommet `Gilamont` ? du sommet `Vevey Gare` ?

3.1.2 Dessiner un graphe représentant les amitiés suivantes parmi quatre personnes :

— John est ami avec Joan and Jill, mais pas avec Jack ;

— Jack est ami avec Jill, mais pas avec Joan ;

— Joan est amie avec Jill.

3.1.3 Dessiner le graphe suivant : les sommets sont les faces d'un cube, deux sommets sont reliés si les faces correspondantes ont une arête du cube en commun.

3.1.4 On a six wagons à trier. Dans la gare de triage, les wagons entrent dans l'ordre 2, 5, 3, 6, 1, 4 et doivent sortir dans l'ordre croissant.

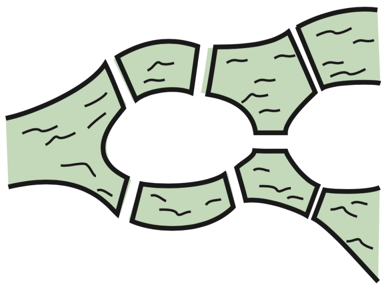
Deux wagons `i` et `j` peuvent être mis sur la même voie si et seulement s'ils entrent dans l'ordre dans lequel ils doivent sortir.

Dessiner un graphe illustrant la situation, en indiquant ce que représentent les sommets et les arêtes de votre graphe.

Quel sera le nombre minimal de voies nécessaires au tri ?

3.1.5 (Les sept ponts de Königsberg)

Au XVIIIe siècle les habitants de Königsberg aimaient se promener le dimanche et traverser les différents ponts de leur ville. Ils se demandaient s'il leur était possible de parcourir la ville en empruntant chacun des 7 ponts une fois et une seule.



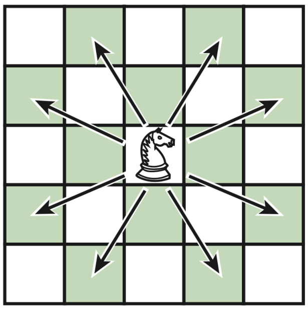
Un promeneur veut traverser, une fois et une seule, chacun des sept ponts de la ville.

a) Peut-il trouver un itinéraire tel que la région d'arrivée soit la même que celle de départ ?

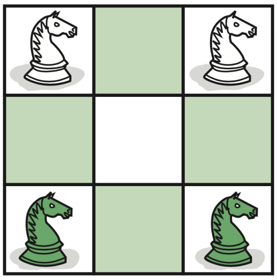
b) Peut-il trouver un itinéraire tel que les régions d'arrivée et de départ soient distinctes ?

3.1.6 (Cavaliers sur un échiquier 3 x 3)

Dans le jeu d'échecs la pièce dont le déplacement est le plus compliqué est le cavalier. Les possibilités de déplacement d'un cavalier sur un échiquier sont indiquées sur la figure ci-dessous.



On considère maintenant le mini échiquier 3 x 3 de la figure ci-dessous où sont placés deux cavaliers blancs et deux cavaliers en couleur.



Est-il possible de permuter les deux cavaliers blancs et les deux cavaliers en couleur ?

3.1.7 Démontrer le **théorème des poignées de main** : La somme des degrés des sommets d'un graphe est égale à deux fois le nombre d'arêtes.

3.1.8 Est-il possible de relier 15 ordinateurs de sorte que chaque appareil soit relié avec exactement trois autres ?

3.1.9 Montrer que dans un groupe formé de six personnes, il y en a nécessairement trois qui se connaissent mutuellement ou trois qui ne se connaissent pas (on suppose que si A connaît B, B connaît également A).

Montrer que cela n'est plus nécessairement vrai dans un groupe de cinq personnes.

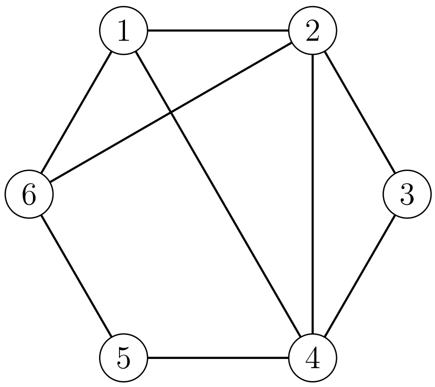
3.1.10

a) Quel est l'ordre du graphe ci-dessous ?

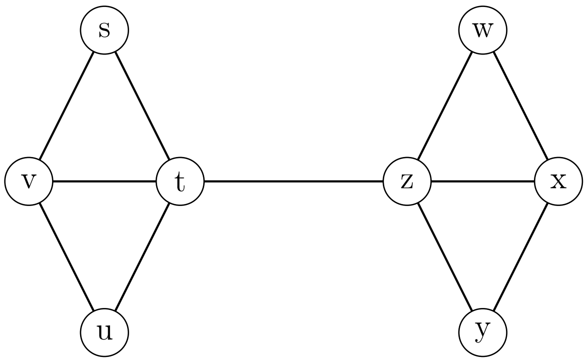
b) Quel est le degré du sommet 1 ? du sommet 4 ?

c) Quels sont les sommets adjacents au sommet 2 ? au sommet 6 ?

d) Il y a deux sommets adjacents chacun à quatre autres sommets. Lesquels ?



3.1.11 Écrire tous les chemins reliant s à y sur le graphe donné ci-dessous. Donner la longueur des chemins trouvés.



Rappel : un chemin est une chaîne telle que chaque arête de celle-ci soit parcourue une et une seule fois.

3.1.12 Dessiner :

a) un graphe connexe avec 8 sommets ;

b) un graphe non connexe avec 8 sommets et deux composantes ;

c) un graphe non connexe avec 8 sommets et trois composantes.

3.1.13

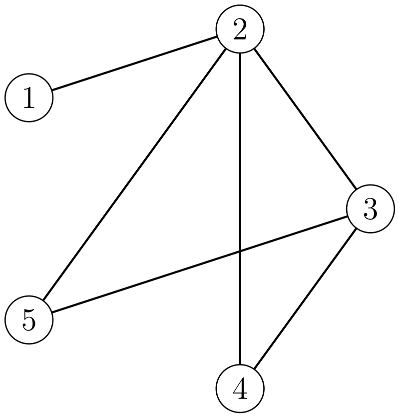
a) Le graphe G ci-dessous est-il complet ?

b) Est-il connexe ?

c) Trouver tous les sous-graphes complets de G (donner la liste de leurs sommets) ?

d) Trouver un chemin de longueur 4 pour aller du sommet 1 au sommet 5 sans passer deux fois par le même sommet.

e) Peut-on trouver un cycle comprenant le sommet 1 ?

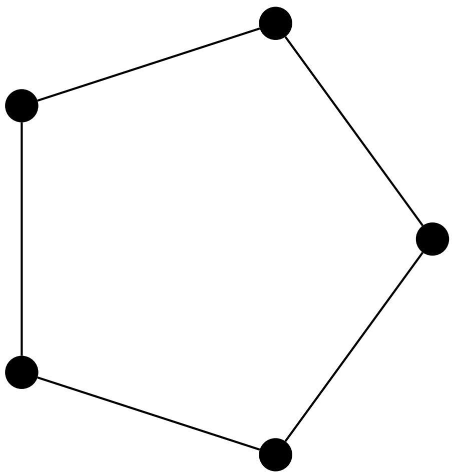


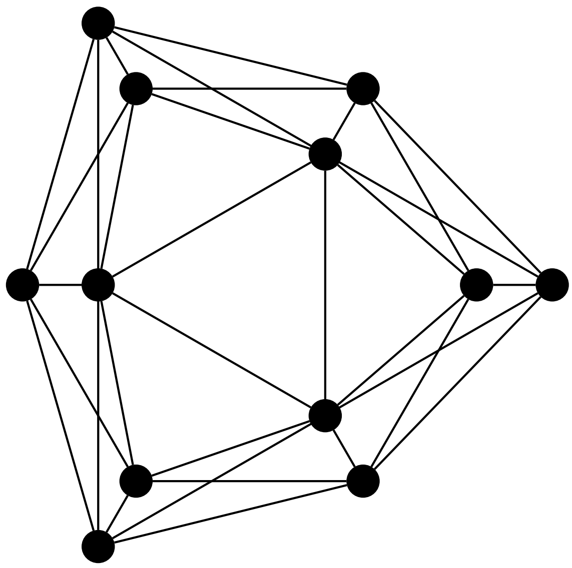
3.1.14 Construire un graphe dont la suite des degrés est (1, 1, 1, 2, 2, 3, 4, 5, 5).

3.1.15 Construire un graphe **connexe** dont la suite des degrés est (1, 1, 2, 3, 3, 4, 4, 6).

3.1.16 Construire un graphe **connexe** dont la suite des degrés est (1, 1, 1, 2, 2, 2, 4, 5, 5).

3.1.17 Soit G un graphe. On dit que G est r-régulier si chaque sommet de G est de degré r. On a le résultat suivant : Si G est r-régulier et qu'il a n sommets, alors G a $n \cdot r/2$ arêtes.
Vérifier ce résultat sur les graphes réguliers suivants :





3.1.18

a) Prouver qu'il n'y a pas de graphe 3-régulier à sept sommets.

b) Prouver que, si n et r sont les deux impairs, il n'y a pas de graphe r-régulier avec n sommets.

3.1.19 Dessiner les 11 graphes simples non étiquetés d'ordre 4.

3.1.20 Dessiner tous les graphes simples non étiquetés d'ordre 5. Il y en a 34.

3.1.21 Notons C_5 le graphe cyclique d'ordre 5 et $\overline{C}_5$ son complémentaire. Montrer que

$$C_5 \simeq \overline{C}_5$$

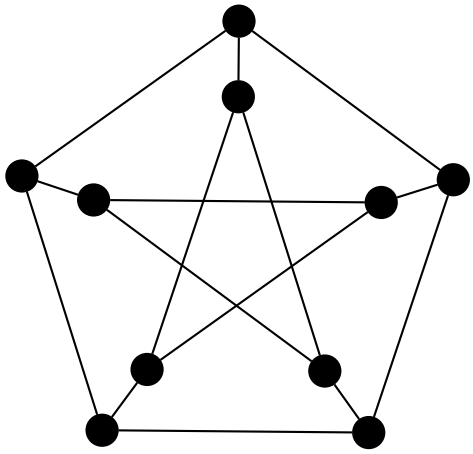
ou, autrement dit, que ces deux graphes sont isomorphes. Montrer ensuite qu'il n'y a pas d'autre graphe cyclique isomorphe à son complémentaire.

3.1.22 Soit G un graphe à ν sommets. Montrer que si $G \simeq \overline{G}$ alors ν ou $\nu - 1$ est un multiple de 4.

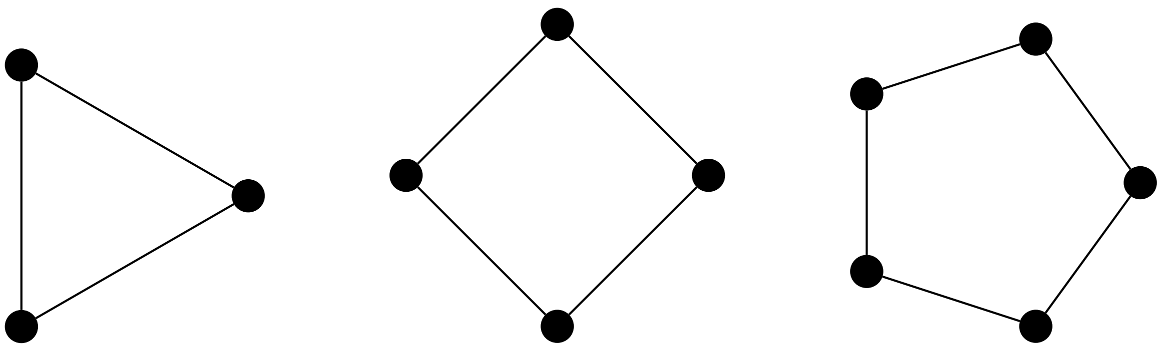
3.1.23 Vu qu'il y a un nombre impair de graphes à quatre sommets, l'un d'entre eux doit être « auto-complémentaire », c'est à dire isomorphe à son complémentaire. Duquel s'agit-il ?

3.2 Graphes eulériens

3.2.1 Soit le graphe de Petersen représenté ci-dessous.

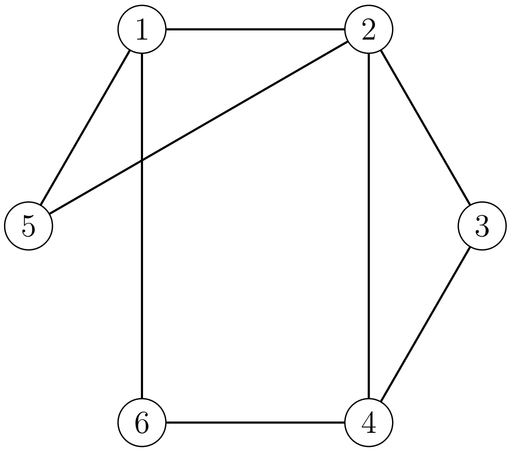


Parmi les graphes représentés ci-dessous, quels sont ceux qui sont un sous-graphe du graphe de Petersen ?



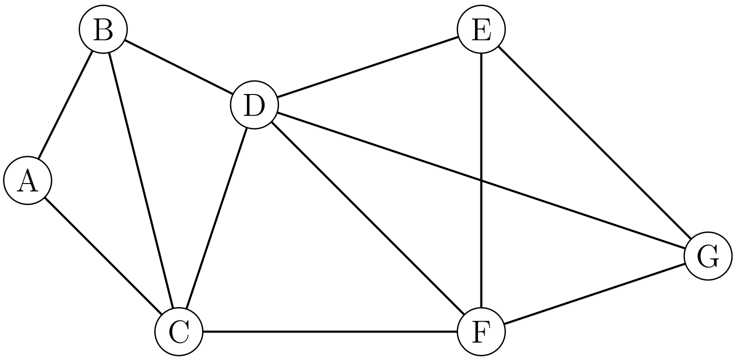
Le graphe de Petersen (1839-1910, mathématicien danois) est, en théorie des graphes, un graphe particulier possédant 10 sommets et 15 arêtes. Il s'agit d'un petit graphe qui sert d'exemple et de contre-exemple pour plusieurs problèmes de la théorie des graphes (Wikipédia).

3.2.2 Soit le graphe ci-dessous.



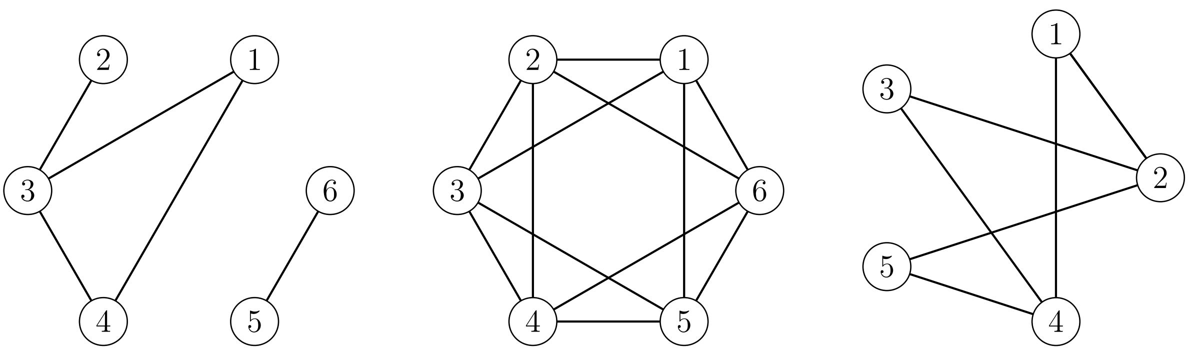
a) Pourquoi le graphe ci-dessus n'admet-il pas de cycle eulérien ?
b) Pourquoi le cycle $1 - 2 - 4 - 3 - 2 - 5 - 1 - 6$ n'est-il pas une chaîne eulérienne pour ce graphe ?
c) Trouver une chaîne eulérienne d'origine 4.
d) On ajoute une arête de 1 à 4. Montrer qu'il est alors possible de trouver un cycle eulérien.

3.2.3 Soit le graphe ci-dessous.

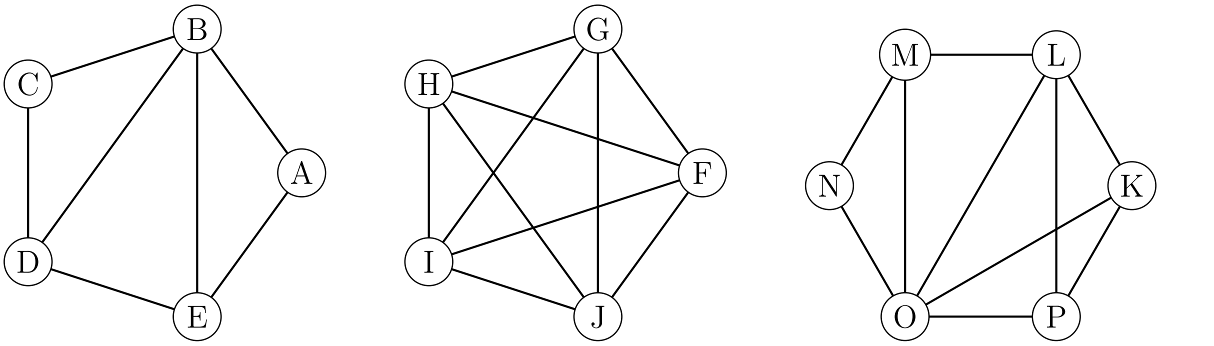


a) Ce graphe admet-il une chaîne eulérienne ? Justifier la réponse. Si oui donner une telle chaîne.
b) Ce graphe admet-il un cycle eulérien ? Justifier la réponse. Si oui donner un tel cycle.

3.2.4 Les graphes ci-dessous sont-ils eulériens (ou semi-eulériens) ?

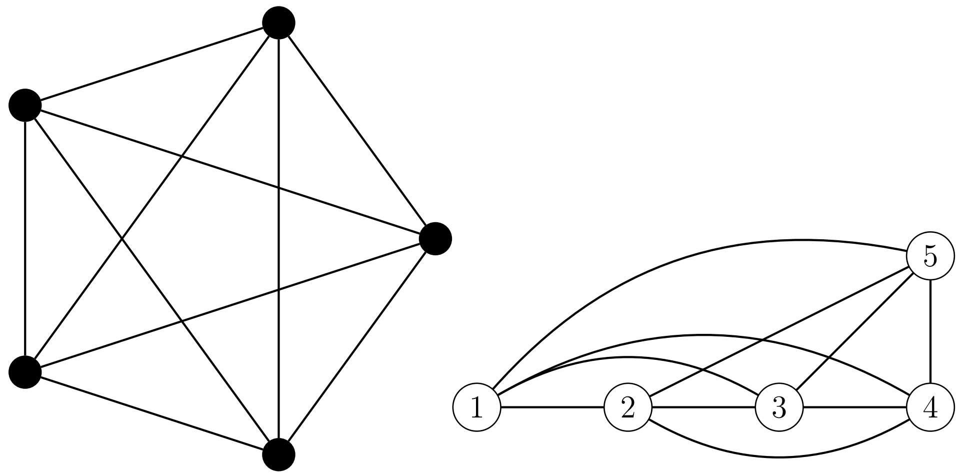


3.2.5 Les graphes ci-dessous admettent-ils un cycle eulérien ou une chaîne eulérienne ?

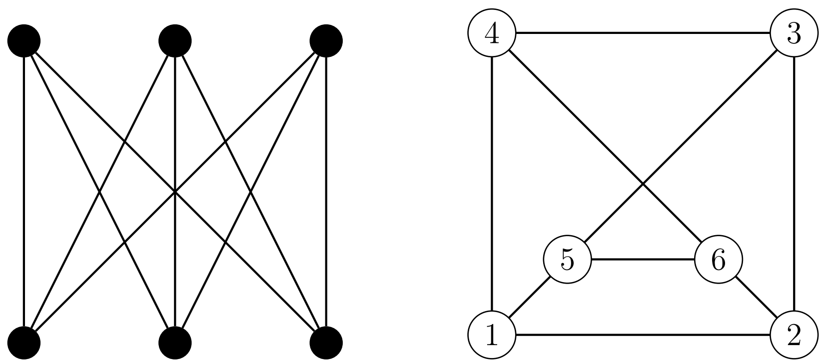


3.2.6 Une chèvre, un chou et un loup se trouvent sur la rive d'un fleuve ; un passeur souhaite les transporter sur l'autre rive mais, sa barque étant trop petite, il ne peut transporter qu'un seul d'entre eux à la fois. Comment doit-il procéder afin de ne jamais laisser ensemble et sans surveillance le loup et la chèvre, ainsi que la chèvre et le chou ?

3.2.7 Montrer que les deux graphes représentés ci-dessous sont isomorphes.



3.2.8 Montrer que les deux graphes représentés ci-dessous sont isomorphes.



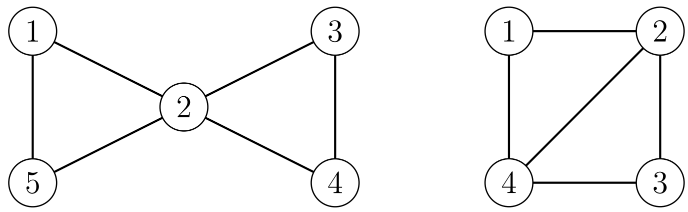
3.3 Arbres

3.3.1 Dessiner tous arbres non étiquetés à 6 sommets ou moins.

3.3.2 En ajoutant à chaque arbre à 6 sommets une arête à la fois, et ceci de toutes les façons possibles, dessiner les 11 arbres à 7 sommets.

3.3.3 En ajoutant à chaque arbre à 7 sommets une arête à la fois, et ceci de toutes les façons possibles, dessiner les 23 arbres à 8 sommets.

3.3.4 On considère les deux graphes ci-dessous :



Pour chaque graphe

a) dessiner tous les arbres couvrants étiquetés ;

b) indiquer ceux qui sont isomorphes.

3.3.5 Trouver tous les arbres couvrants non isomorphes de $K_{3,3}$.

3.3.6 Une *forêt* est un graphe non forcément connexe dont chacune des composantes connexes est un arbre.

a) Soit G une forêt à n sommets et k composantes connexes. Donner le nombre d'arêtes de G.

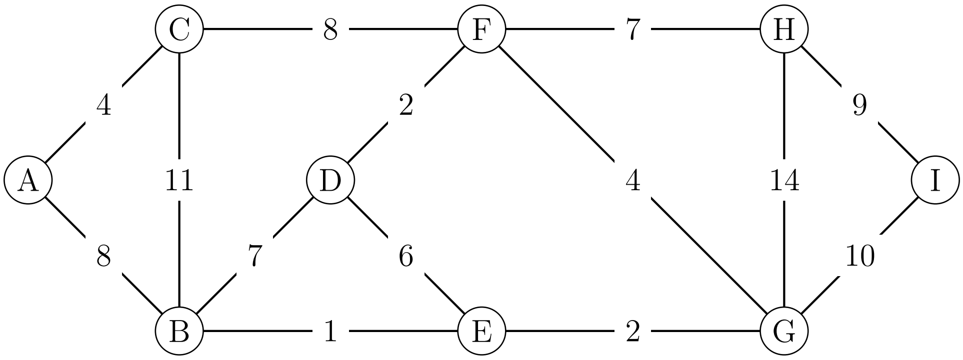
b) Construire une forêt à 12 sommets et 9 arêtes.

c) Est-il vrai que toute forêt à k composantes connexes a au moins $2k$ sommets de degré 1 ?

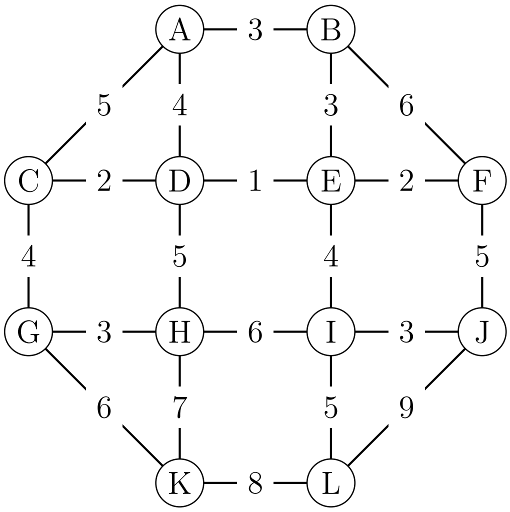
3.3.7 Par l'absurde, démontrer que la suppression d'une arête d'un arbre ne peut le déconnecter en plus de deux composantes connexes.

3.3.8 Par l'absurde, démontrer que l'ajout d'une arête à un arbre ne peut créer plus d'un cycle.

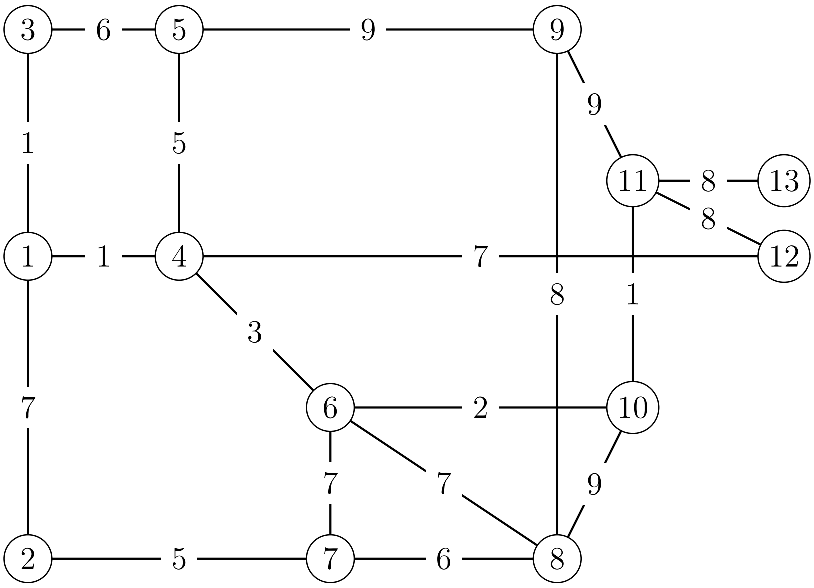
3.3.9 Pour le graphe pondéré ci-dessous, trouver un arbre couvrant de poids minimum.



3.3.10 Pour le graphe pondéré ci-dessous, trouver un arbre couvrant de poids minimum.



3.3.11 Considérons le graphe G ci-dessous.

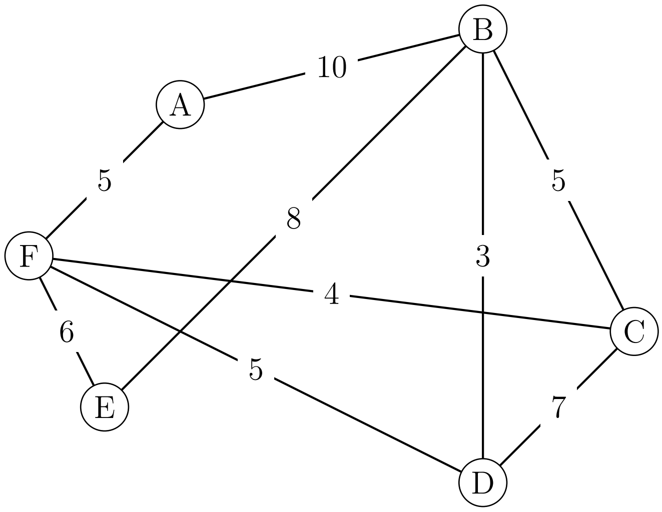


a) Déterminer un arbre de poids minimal de G à l'aide de l'algorithme de Kruskal.

b) Déterminer un arbre de poids minimal de G à l'aide de l'algorithme de Prim, en partant du sommet initial ①.

3.4 Graphes valués : le chemin le plus court

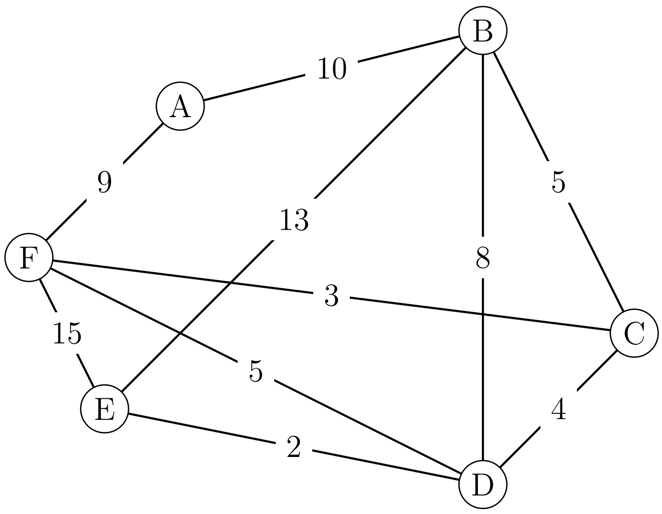
3.4.1 Soit le graphe ci-dessous.



a) Quelle est la longueur du chemin $A - B - C - F - E$?

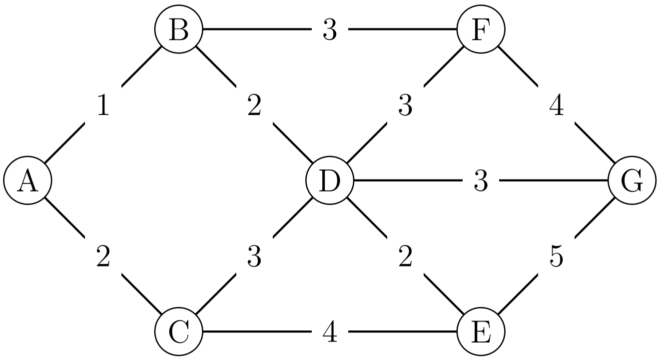
b) Déterminer le chemin de poids minimal reliant F à B.

3.4.2 Soit le graphe ci-dessous.



Déterminer le chemin de poids minimal reliant A à E.

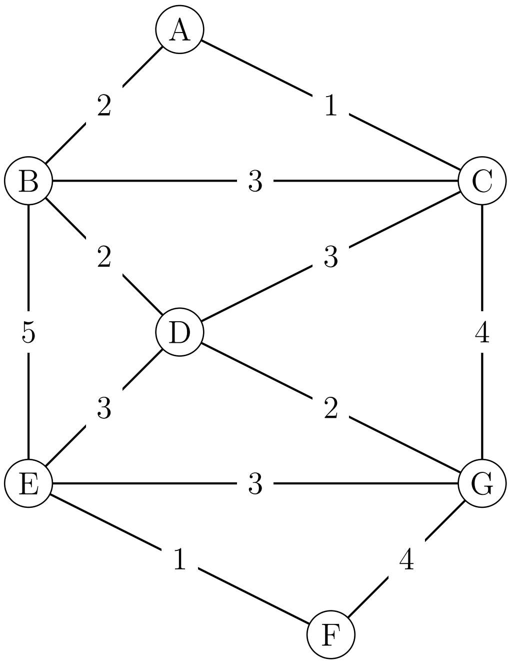
3.4.3 Soit le graphe ci-dessous.



Utiliser l'algorithme de Dijkstra pour déterminer le plus court chemin entre A et G.

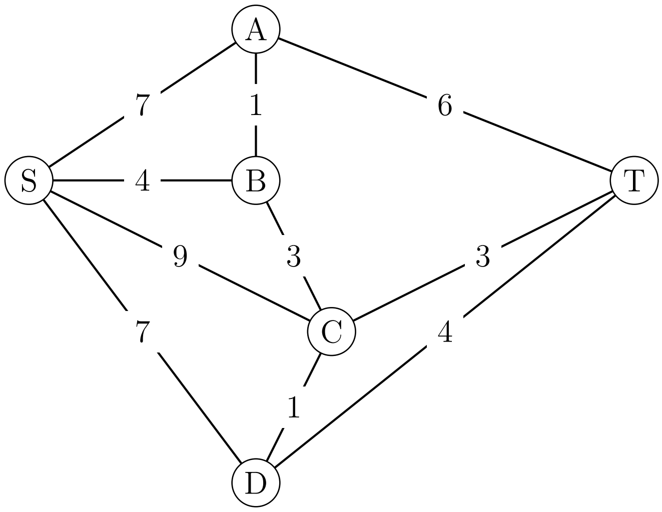
3.4.4 Le graphe présente un réseau routier entre différents points d'une ville.

Chaque tronçon est pondéré par le temps nécessaire, en minute, pour le parcourir.



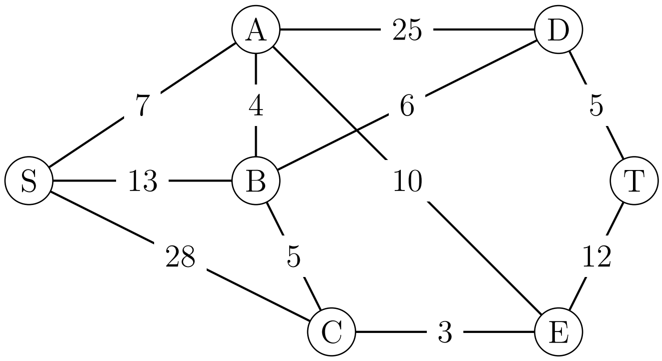
Utiliser l'algorithme de Dijkstra pour déterminer le(s) chemin(s) qui minimise(nt) le temps pour aller de A à F.

3.4.5 Soit le graphe ci-dessous :



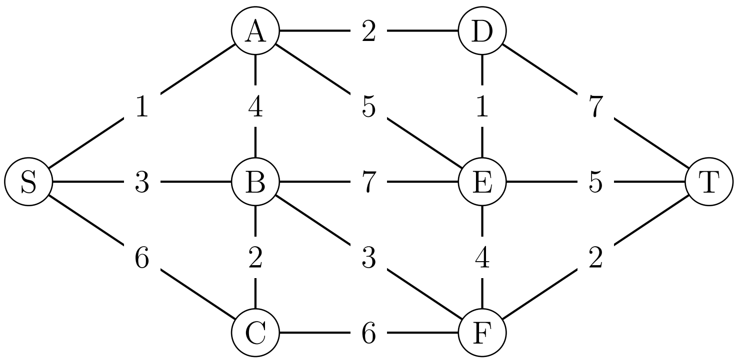
À l'aide de l'algorithme de Dijkstra, trouver le chemin le plus court qui mène de S à T.

3.4.6 Soit le graphe ci-dessous :



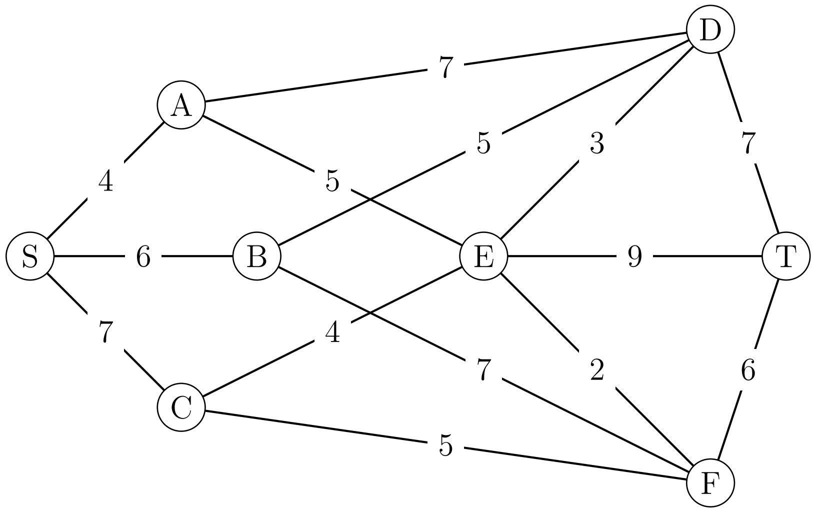
À l'aide de l'algorithme de Dijkstra, trouver le chemin le plus court qui mène de S à T.

3.4.7 Soit le graphe ci-dessous :



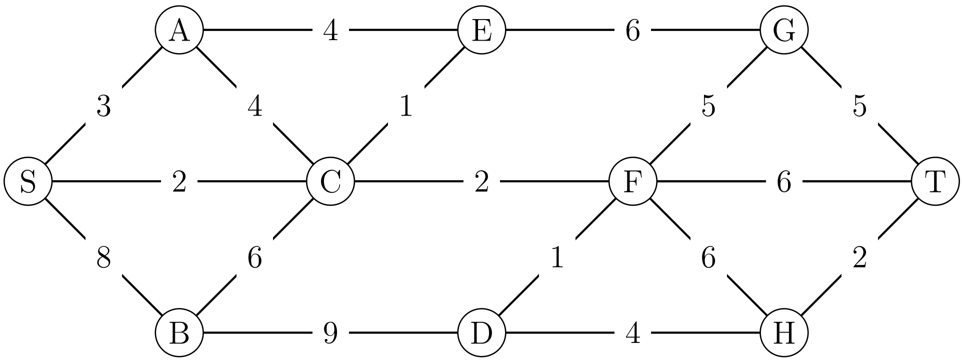
À l'aide de l'algorithme de Dijkstra, trouver le chemin le plus court qui mène de S à T.

3.4.8 Soit le graphe ci-dessous :



À l'aide de l'algorithme de Dijkstra, trouver le chemin le plus court qui mène de S à T.

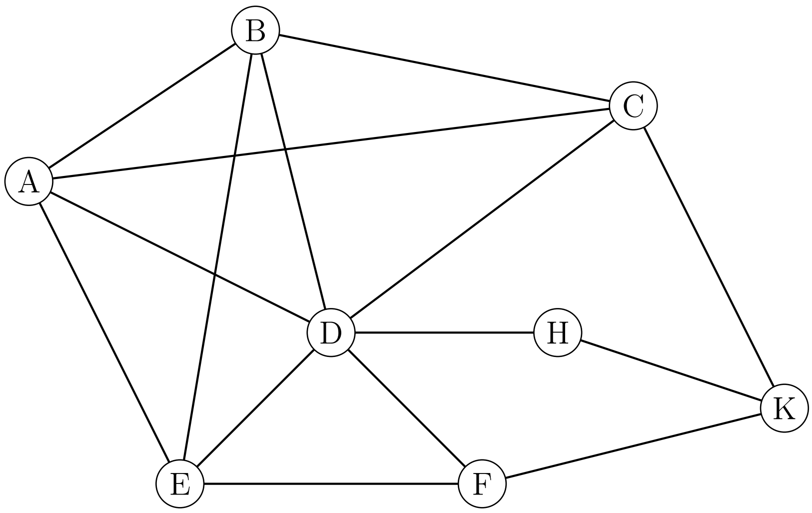
3.4.9 Soit le graphe ci-dessous :



À l'aide de l'algorithme de Dijkstra, trouver le chemin le plus court qui mène de S à T.

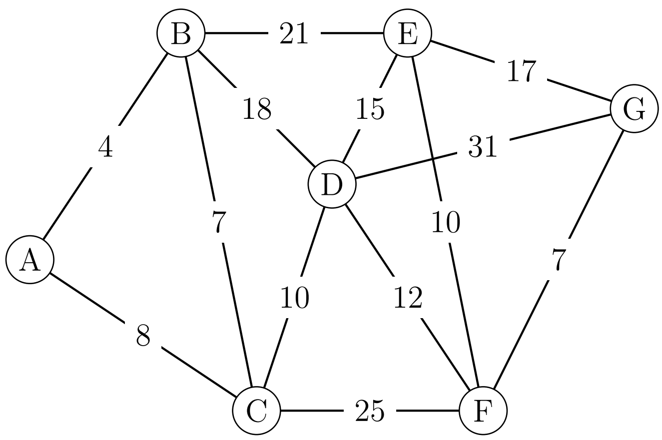
3.4.10 Le graphe ci-dessous représente le plan d'un zoo. Le sommet A désigne son accès, les autres sommets désignent les différents secteurs animaliers de ce zoo.
Une arête représente l'allée reliant deux secteurs et est pondérée par la distance de parcours, exprimée en mètres, entre ces deux secteurs. Les distances sont données dans un tableau.

AB	AC	AD	AE	BC	BD	BE	CD	CK	DE	DF	DH	EF	FK	HK
90	290	175	150	185	155	180	120	260	110	105	220	135	230	145



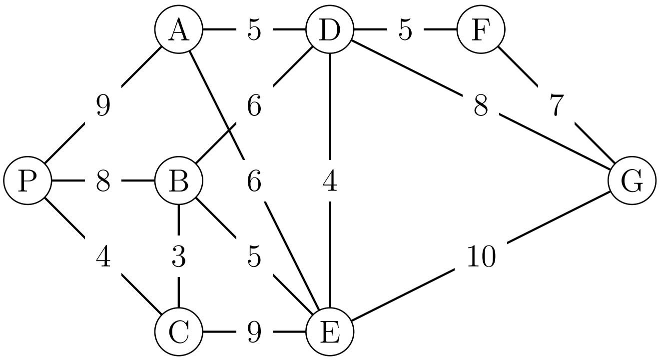
Les services de sécurité basés au sommet A doivent intervenir dans le secteur K. Déterminer, à l'aide de l'algorithme de Dijkstra, l'itinéraire le plus court. Donner sa longueur en mètres.

3.4.11 Une région est munie d'un réseau de train représenté par le graphe ci-dessous. Les stations sont symbolisées par les sommets A, B, C, D, E, F et G. Chaque arête représente une ligne reliant deux gares. Le temps de parcours en minutes entre chaque sommet ont été rajoutés sur le graphe.



Déterminer, en minutes, le plus court chemin reliant la gare B à la gare G.

3.4.12 Un réseau de navettes gratuites est mis en place entre des parkings situés aux abords de la ville et les principaux sites de la ville.
Le graphe ci-contre indique les voies et les temps des liaisons, en minutes, entre ces différents sites.

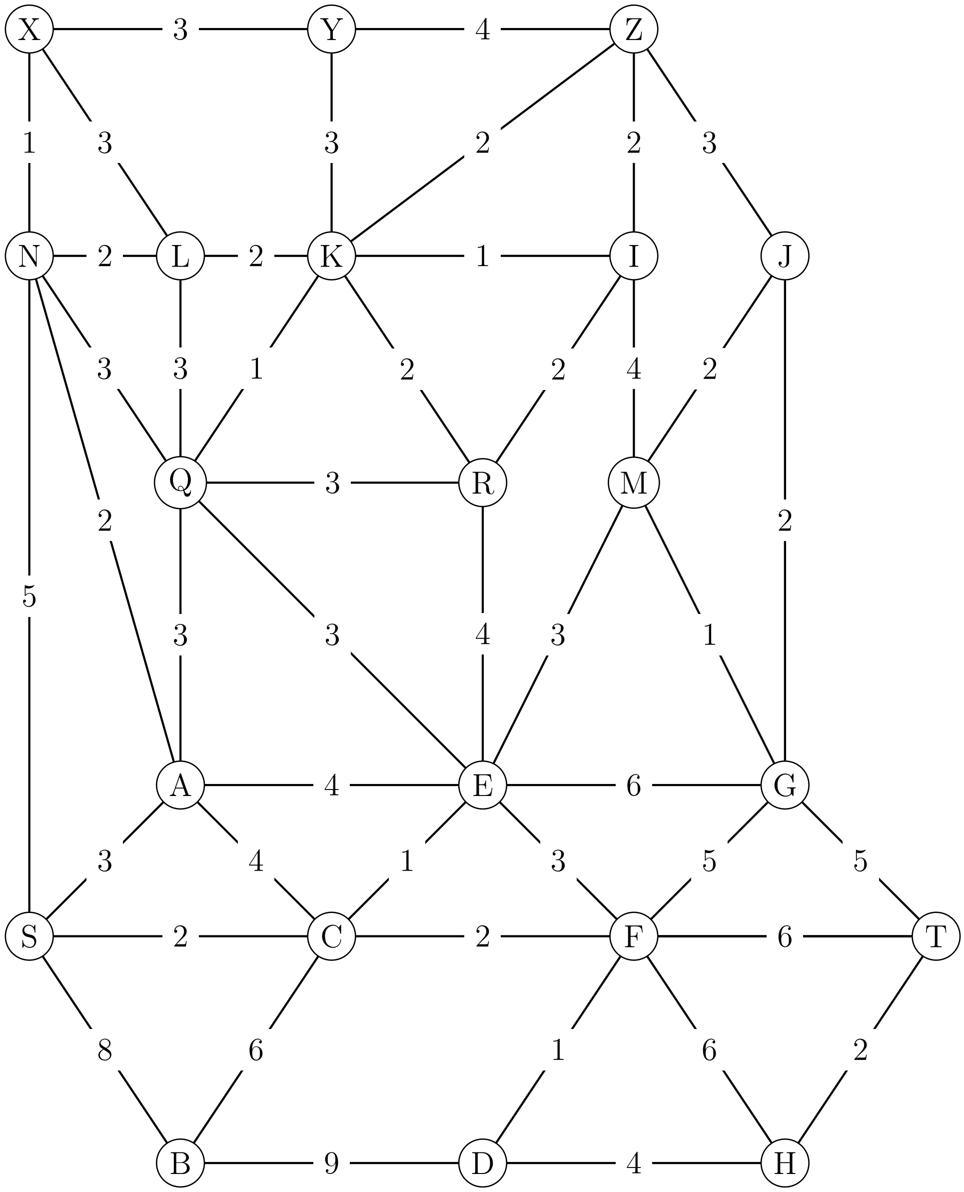


a) Peut-on envisager un itinéraire qui relierait le parking P à la gare G en desservant une et une seule fois tous les sites ?

b) Peut-on envisager un itinéraire qui emprunterait une et une seule fois toutes les voies ?

c) Déterminer un trajet de durée minimale pour se rendre du parking P à la gare G.

3.4.13 Soit le graphe ci-dessous :



À l'aide de l'algorithme de Dijkstra, trouver le chemin le plus court qui mène de X à H.

3.5 Solutions des exercices

3.1.1 a) oui.

b) Un sommet représente une station (ou arrêt) de bus.

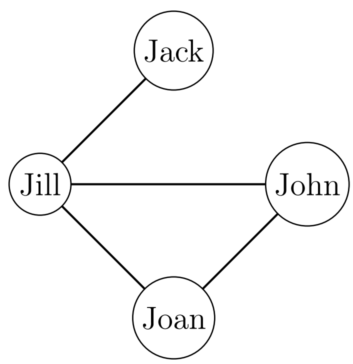
c) Une arêtes représente la route reliant deux stations consécutives.

d) Oui, on peut aller de toute station A (un sommet) à toute station B (un autre sommet).

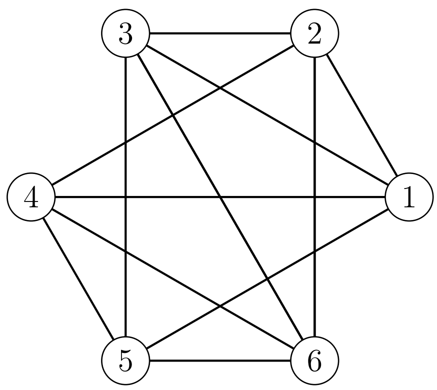
e) Orienté (cf ligne 202 par exemple).

f) 2 et 7.

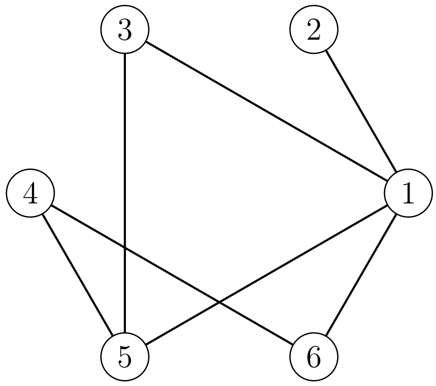
3.1.2



3.1.3



3.1.4 On représente les wagons par les sommets. Une arête relie deux sommets `i` et `j` si les wagons `i` et `j` ne peuvent pas être sur la même voie. On obtient le graphe ci-dessous.



On voit que 1, 3 et 5 ne peuvent pas être sur la même voie. Il faut donc trois voies au minimum.

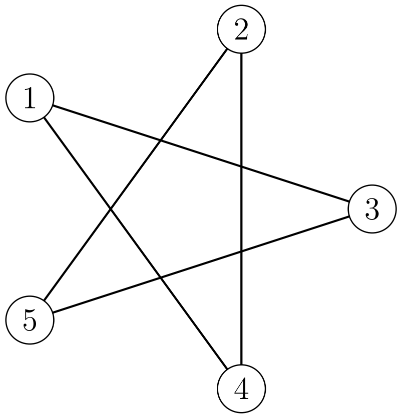
3.1.5 -

3.1.6 -

3.1.7 Considérons un graphe formé au départ d'un certain nombres de sommets et de 0 arêtes. La somme des degrés est alors 0. Chaque fois que l'on ajoute une arête à ce graphe, la somme des degrés augmente de 2, vu que l'arête relie 2 sommets entre eux. Après l'ajout de n arêtes, la somme des degrés du graphe vaut donc $2\,n$. Vu que tout graphe est obtenu par ce procédé, on obtient bien que la somme des degrés est le double du nombre des arêtes.

3.1.8 Considérons le graphe simple dont les sommets sont les 15 ordinateurs, les arêtes étant les liaisons entre ces ordinateurs. Si chaque appareil est relié à exactement 3 ordinateurs du réseau, les sommets du graphe sont tous de degré impair. D'après un résultat établi, un tel graphe doit posséder un nombre pair de sommets, le réseau ne peut donc pas être réalisé.
Autrement dit, il n'est pas possible de relier 15 ordinateurs de sorte que chaque appareil soit relié avec exactement trois autres, car dans ce cas, la somme des degrés serait égale à $15 \times 3 = 45$ qui n'est pas pair.

3.1.9 On suppose que 6 invités sont là, et que Jack en fait partie. Parmi les 5 autres invités, soit il y en a 3 qui le connaissent, soit 3 ne le connaissent pas (par le principe des tiroirs). Sans perte de généralité, on peut supposer que ces trois invités connaissent Jack, et qu'ils s'appellent respectivement Karen, Natalie et Billy. Deux possibilités alors : soit ces trois invités ne se connaissent pas (et on a notre trio gagnant), soit il y en a au moins deux qui se connaissent, et ils forment avec David le trio gagnant.



3.1.10

a) Le graphe est d'ordre 6 (6 sommets).

b) Le degré du sommet 1 : 3 ; du sommet 4 : 4.

c) Les sommets adjacents au sommet 2 : 1, 3, 4 et 6 ; au sommet 6 : 1, 2 et 5.

d) Les sommets adjacents à quatre sommets : 2 et 4.

3.1.11

longueur 3 : $stzy$;

longueur 4 : $stzxy$ et $svtzy$:

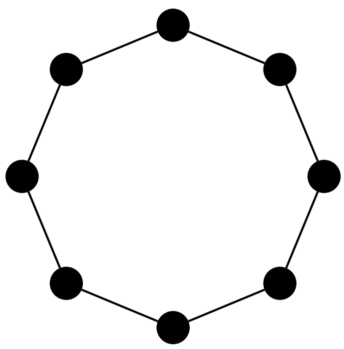
longueur 5 : $stzwxy$, $svtzxy$ et $svutzy$;

longueur 6 : $svutzxy$ et $svtzwxy$;

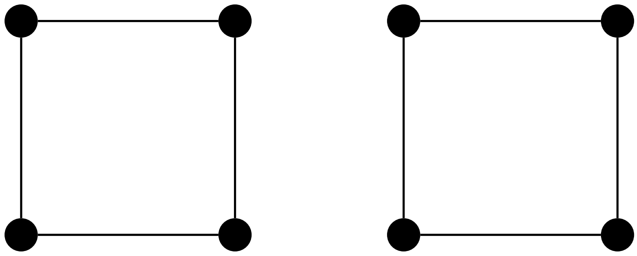
longueur 7 : $svutzwxy$.

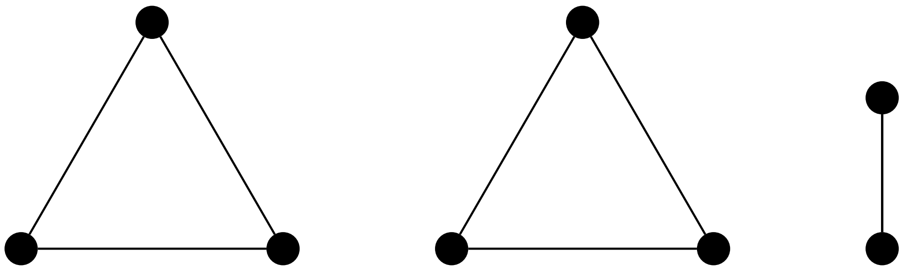
3.1.12

Il y a plusieurs possibilités, par exemple :



a)

b) 

c) 

3.1.13

a) Il n'est pas complet, car le sommet 1 n'est pas relié au sommet 5, par exemple.

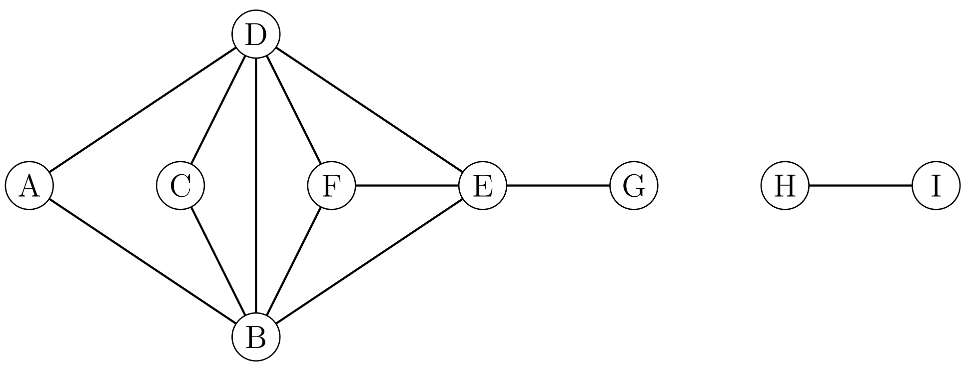
b) Il est connexe, car il est fait « d'un seul morceau ».

c) $G_1 = (2, 5, 3)$ et $G_2 = (2, 4, 3)$. Toute arête du graphe est un graphe complet d'ordre 2.

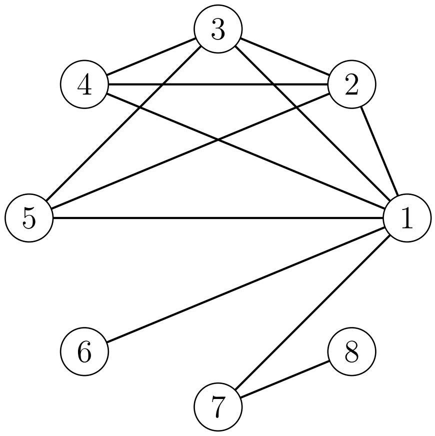
d) Le chemin est donné par la suite de sommets $(1, 2, 4, 3, 5)$; sa longueur est bien 4.

e) Il n'y a pas de cycle comprenant le sommet 1 vu que celui-ci est de degré 1.

3.1.14 Par exemple :



3.1.15 Par exemple :



3.1.16 C'est impossible, car tout graphe a un nombre pair de sommets de degré impair.

3.1.17 —

3.1.18 —

3.1.19 —

3.1.20 —

3.1.21 —

3.1.22 —

3.1.23 —

3.2.1 Les deux premiers ne sont pas des sous-graphes du graphe de Petersen, alors que le troisième est un sous-graphe.

3.2.2

a) Les sommets 1 et 4 sont de degré impair.

b) Il manque l'arête $6 - 4$.

c) $4 - 2 - 1 - 5 - 2 - 3 - 4 - 6 - 1$.

d) $4 - 2 - 1 - 5 - 2 - 3 - 4 - 6 - 1 - 4$.

3.2.3

a) On remarque que le graphe est connexe et que tous ses sommets sont de degré pair sauf les sommets D et G.

   Donc il existe une chaîne eulérienne entre les sommets D et G.

b) Comme on l'a vu dans la question précédente tous les sommets du graphe ne sont pas pairs donc il n'y a pas de cycle eulérien.

3.2.4 Le graphe de gauche n'est évidemment pas eulérien puisque non connexe. Celui du milieu est eulérien car tous les sommets sont de degré pair. Celui de droite est semi-eulérien, car seuls deux sommets sont de degré impair.

3.2.5 Le premier graphe admet une chaîne eulérienne, par exemple $D-B-C-D-E-A-B-E$. Le deuxième graphe admet un cycle eulérien: $F-G-H-I-J-F-H-J-G-I-F$. Le troisième graphe n'admet ni chaîne, ni cycle eulérien.

3.2.6 —

3.2.7 –

3.2.8 –

3.3.1 —

3.3.2 —

3.3.3 —

3.3.4 —

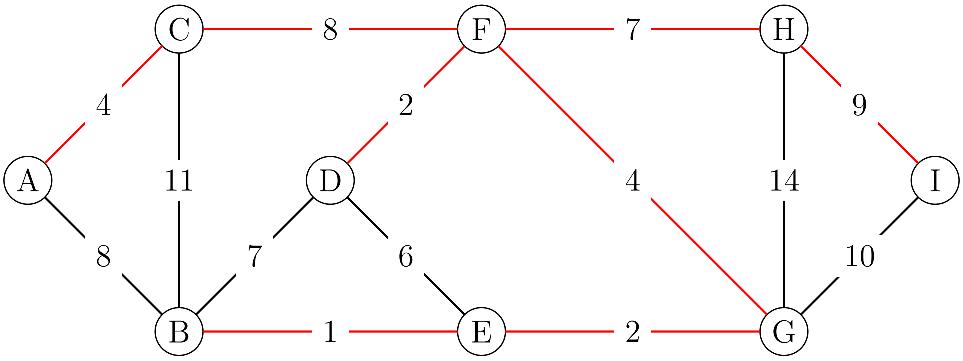
3.3.5 —

3.3.6 —

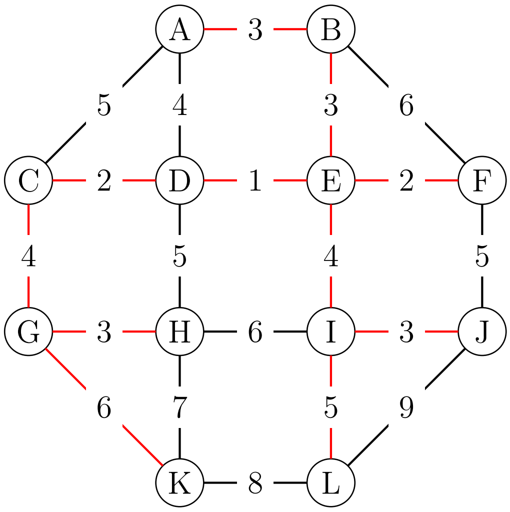
3.3.7 —

3.3.8 —

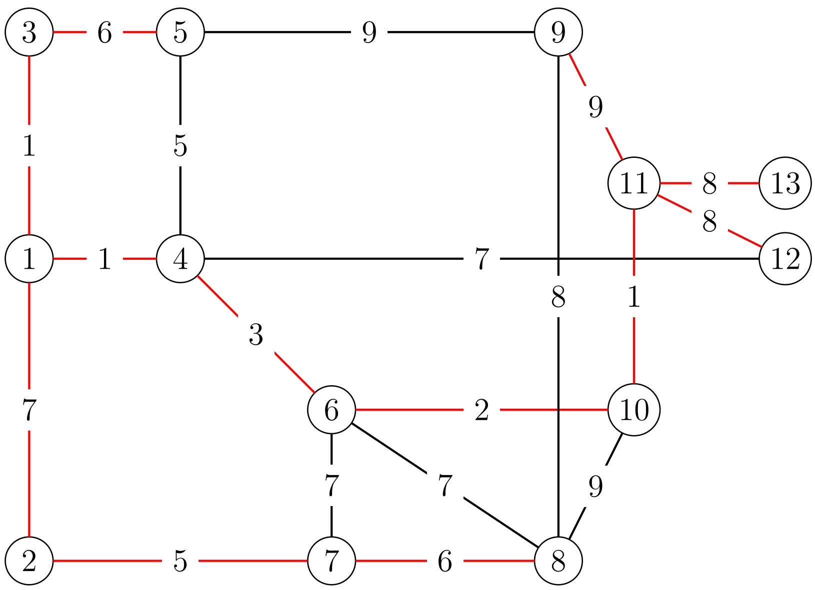
3.3.9



3.3.10



3.3.11 Par exemple, pour l'algorithme de Prim.



3.4.1

a) 4

b) $F - D - B$ de poids 8

3.4.2

Le chemin de poids minimal reliant A à E est $A - F - D - E$ de poids égal à 16.

3.4.3 $A - B - D - G$ de longueur 6

3.4.4 On obtient 3 chemins de 8 minutes :

a) $A - B - E - F$

b) $A - B - D - E - F$

c) $A - C - D - E - F$

3.4.5 Le chemin le plus court est $S - B - C - T$, de longueur 10.

3.4.6

S	T	B	A	C	D	E
0	∞	∞	∞	∞	∞	∞
—	∞	13_{S}	$\mathbf{7_S}$	28_{S}	∞	∞
—	∞	$\mathbf{11_A}$	—	28_{S}	32_{A}	17_{A}
—	∞	—	—	$\mathbf{16_B}$	17_{B}	17_{A}
—	∞	—	—	—	$\mathbf{17_B}$	17_{A}
—	22_{D}	—	—	—	—	$\mathbf{17_A}$
—	$\mathbf{22_D}$	—	—	—	—	—

Le chemin le plus court est S-A-B-D-T, de longueur 22.

3.4.7

S	A	B	C	D	E	F	T
0	∞	∞	∞	∞	∞	∞	∞
—	$\mathbf{1_S}$	3_{S}	6_{S}	∞	∞	∞	∞
—	—	$\mathbf{3_S}$	6_{S}	3_{A}	6_{A}	∞	∞
—	—	—	5_{B}	$\mathbf{3_A}$	6_{A}	6_{B}	∞
—	—	—	5_{B}	—	$\mathbf{4_D}$	6_{B}	10_{D}
—	—	—	$\mathbf{5_B}$	—	—	6_{B}	9_{E}
—	—	—	—	—	—	$\mathbf{6_B}$	9_{E}
—	—	—	—	—	—	—	$\mathbf{8_F}$

Le chemin le plus court est S-B-F-T, de longueur 8.

3.4.8

S	A	B	C	D	E	F	T
0	∞	∞	∞	∞	∞	∞	∞
—	$\mathbf{4_S}$	6_S	7_S	∞	∞	∞	∞
—	—	$\mathbf{6_S}$	7_S	11_A	9_A	∞	∞
—	—	—	$\mathbf{7_S}$	11_A	9_A	13_B	∞
—	—	—	—	11_A	$\mathbf{9_A}$	12_C	∞
—	—	—	—	$\mathbf{11_A}$	—	11_E	18_E
—	—	—	—	—	—	$\mathbf{11_E}$	18_E
—	—	—	—	—	—	—	$\mathbf{17_F}$

Le chemin le plus court est S-A-E-F-T, de longueur 17.

3.4.9

S	A	B	C	D	E	F	G	H	T
$\mathbf{0}$	∞	∞	∞	∞	∞	∞	∞	∞	∞
—	3_{S}	8_{S}	$\mathbf{2_S}$	∞	∞	∞	∞	∞	∞
—	$\mathbf{3_S}$	8_{S}	—	∞	3_{C}	4_{C}	∞	∞	∞
—	—	8_{S}	—	∞	$\mathbf{3_C}$	4_{C}	∞	∞	∞
—	—	8_{S}	—	∞	—	$\mathbf{4_C}$	9_{E}	∞	∞
—	—	8_{S}	—	$\mathbf{5_F}$	—	—	9_{E}	10_{F}	10_{F}
—	—	$\mathbf{8_S}$	—	—	—	—	9_{E}	9_{D}	10_{F}
—	—	—	—	—	—	—	$\mathbf{9_E}$	9_{D}	10_{F}
—	—	—	—	—	—	—	—	$\mathbf{9_D}$	10_{F}
—	—	—	—	—	—	—	—	—	$\mathbf{10_F}$

Le chemin le plus court est S-C-F-T, de longueur 10.

3.4.10

A	B	C	D	E	F	H	K
$\mathbf{0}$	∞	∞	∞	∞	∞	∞	∞
—	$\mathbf{90_A}$	290_{A}	175_{A}	150_{A}	∞	∞	∞
—	—	275_{B}	175_{A}	$\mathbf{150_A}$	∞	∞	∞
—	—	275_{B}	$\mathbf{175_A}$	—	285_{E}	∞	∞
—	—	$\mathbf{275_B}$	—	—	280_{D}	395_{D}	∞
—	—	—	—	—	$\mathbf{280_D}$	395_{D}	535_{C}
—	—	—	—	—	—	$\mathbf{395_D}$	510_{F}
—	—	—	—	—	—	—	$\mathbf{510_F}$

Le chemin le plus court est A-D-F-K, de longueur 510.

3.4.11 Le plus court chemin est B-C-D-F-G. La longueur de ce chemin est de 36 minutes.

3.4.12 a) P–B–C–E–A–D–F–G

b) D'après le théorème d'Euler, il existe une chaîne eulérienne dans un graphe connexe si et seulement si exactement zéro ou deux de ses sommets sont de degrés impairs. Tous les sommets de ce graphe sont de degrés impairs sauf F, donc il n'existe aucun itinéraire qui emprunte une et une seule fois toutes les voies.

c) Le chemin le plus rapide de P vers G est d'une durée de 21 minutes : P-C-B-D-G.

3.4.13

Le chemin le plus court est X-N-A-C-F-D-H, de longueur 14.

Chapitre 4

Programmation en Python

4.1 Manipuler des fichiers en Python

4.1.1 Copier l'intégralité du fichier `oiseaux.txt` dans un fichier `oiseauxBis.txt`.

4.1.2 Compter le nombre d'oiseaux qui figurent dans le fichier `oiseaux.txt`.

4.1.3 Afficher à la console le premier oiseau du fichier `oiseaux.txt` qui contient la lettre `x`.

4.1.4 Afficher à la console un oiseau choisi au hasard dans le fichier `oiseaux.txt`.

4.1.5 Créer deux fichiers `oiseaux1.txt` et `oiseaux2.txt`. Le premier contient la première moitié de la liste du fichier `oiseaux.txt` et le deuxième la deuxième moitié.

4.1.6 Compter le nombre de fois qu'apparaît la lettre e dans le fichier `oiseaux.txt`.
Puis calculer sa fréquence d'apparition dans le fichier.
Ensuite faire de même avec toutes les voyelles.
Consigner les résultats dans un fichier `statistiques.txt`

4.1.7 A partir du fichier `oiseaux.txt`, créer un fichier `secret.txt` qui transforme toutes les occurrences de `a` en `x`, de `e` en `y` et de `i` en `z`.
Est-il possible, à partir du fichier `secret.txt`, de créer un fichier `oiseaux3.txt` qui permette de retrouver le nom des oiseaux (opération inverse) ?

4.1.8 Écrire un script qui génère automatiquement un fichier texte contenant les tables de multiplication de 2 à 30 (chacune d'entre elles incluant 20 termes seulement).

4.1.9 Écrire un script qui recopie un fichier texte en triplant tous les espaces entre les mots.

4.1.10 Écrire un script qui permet de créer et de relire aisément un fichier texte. Le programme demandera d'abord à l'utilisateur d'entrer le nom du fichier. Ensuite il lui proposera le choix, soit d'enregistrer de nouvelles lignes de texte, soit d'afficher le contenu du fichier.

L'utilisateur devra pouvoir entrer ses lignes de texte successives en utilisant simplement la touche `Enter` pour les séparer les unes des autres. Pour terminer les entrées, il lui suffira d'entrer une ligne vide (c'est-à-dire utiliser la touche `Enter` seule).
L'affichage du contenu devra montrer les lignes du fichier séparées les unes des autres de la manière la plus naturelle (les codes de fin de ligne ne doivent pas apparaître).

4.1.11 Écrire un script qui permet de transformer un texte écrit en français en un texte ne contenant que les 26 lettres majuscules de l'alphabet.

4.1.12 Écrire un script qui permet de calculer la fréquence des lettres majuscules dans un texte écrit en français, uniquement avec les 26 majuscules de l'alphabet.

4.1.13 En utilisant tous les textes figurant dans le dossier `textes_bruts`, donner la fréquences d'apparition des majuscules dans un texte écrit avec des majuscules uniquement, sans accents et sans espaces.

4.2 Solutions des exercices

4.1.1 –

4.1.2 –

4.1.3 –

4.1.4 –

4.1.5 –

4.1.6 –

4.1.7 –

4.1.8 –

4.1.9 –

4.1.10 –

4.1.11 –

4.1.12 –

4.1.13 –

Chapitre 5

Méthodes numériques

5.1 La bibliothèque matplotlib de Python : les fonctions de base

5.1.1 Copier ces lignes dans une fenêtre de Python et observer le résultat.

```
import matplotlib.pyplot as plt
import numpy as np

plt.plot([1,3,4],[2,1,6])

plt.show()
```

5.1.2 Copier ces lignes dans une fenêtre de Python et observer le résultat.

```
import matplotlib.pyplot as plt
import numpy as np

x = np.linspace(-2, 2, 100)
y = 2*x**2+3*x-4

plt.plot(x,y)
plt.show()
```

5.1.3 Copier ces lignes dans une fenêtre de Python et observer le résultat.

```
import matplotlib.pyplot as plt
import numpy as np
from math import *

abscisses = np.linspace(-4,4,100)
ordonnées = [cos(x)+3*sin(2*x) for x in abscisses]

plt.plot(abscisses,ordonnées)
plt.show()
```

5.1.4 Copier ces lignes dans une fenêtre de Python et observer le résultat.

```
import matplotlib.pyplot as plt
import numpy as np

x = np.linspace(-4,4,100)
y = np.cos(x)+3*np.sin(2*x)

plt.plot(x,y)
plt.show()
```

5.1.5 Copier ces lignes dans une fenêtre de Python et observer le résultat.

```
import matplotlib.pyplot as plt
import numpy as np

x = np.linspace(-1,3,100)
y = -2*x+3
plt.plot(x,y)
y = x**2 - 4*x + 4

plt.plot(x,y)
plt.show()
```

5.1.6 Copier ces lignes dans une fenêtre de Python et observer le résultat.

```
import matplotlib.pyplot as plt
import numpy as np

x = np.linspace(-np.pi,np.pi,100)
for n in range(1,5):
    y = np.cos(n*x)
    plt.plot(x,y, label="n="+str(n))

plt.legend(loc="lower right")
plt.show()
```

5.1.7 Afficher la représentation graphique de la fonction $f(x) = x^3 + 3x^2 - 9x + 1$ pour x entre -2 et 4.

5.1.8 Afficher la représentation graphique de la fonction $f(x) = 3\,\cos(2\,x) - 2\,\sin(3\,x)$ pour x entre $-\pi$ et π.

5.1.9 Afficher les représentations graphiques de la famille de fonctions $f(x) = \dfrac{1 - n\,x}{x - 1}$ pour n allant de -3 à 3. On se placera dans un repère allant de -2 à 4 pour les abscisses et de -8 à 8 pour les ordonnées. On fera apparaitre aussi une légende en haut à gauche.

5.1.10

a) Tracer en vert la fonction qui à x associe $log(x)$ pour x variant de 0.1 à 10 avec un pas de 0.1. Utiliser la fonction `np.log()`.
Ajouter les légendes et le titre appropriés.

b) Tracer en rouge la fonction qui à x associe $\sqrt{x}$ pour x variant de 0.1 à 10 avec un pas de 0.1. Utiliser la fonction `np.sqrt()`.
Ajouter les légendes et le titre appropriés.

c) Selon vous quelle est la fonction qui croit le plus vite en $+\infty$? qui décroit le plus vite en 0 ?
Vérifier en superposant les 2 courbes.

d) Tracer `plt.plot(x,np.exp(np.log(x)))`. Quelle est la forme de la courbe obtenue ? Pourquoi obtient-on cette forme ?

5.1.11 Tracer la spirale d'Archimède donné par le système d'équations paramétriques.

$$\begin{cases} x(t) = t\cos(t) \\ y(t) = t\sin(t) \end{cases}$$

5.1.12 Tracer la courbe de la fonction f dans l'intervalle I ainsi que sa tangente au point d'abscisse a.

a) $f(x) = x^2$, $I = [-1\,;3]$, $a = 1$.

b) $f(x) = e^x - 3\,x^2$, $I = [-1\,;5]$, $a = 4$.

c) $f(x) = \sin(x) - \dfrac{x}{4}$, $I = [-1\,;\pi]$, $a = 2$.

5.2 Zéros de fonctions : méthode de la bissection

5.2.1 Soit la fonction $f(x) = (x+2)(x+1)(x-1)$.

a) Représenter la fonction dans l'intervalle $I = [0.1\,;2.4]$.

b) Écrire les six premiers intervalles successifs obtenus par la méthode de la bissection pour chercher les zéros de la fonction $f(x)$ dans l'intervalle I.

5.2.2 Pour chacune des fonctions suivantes, faire trois itérations de la méthode de la bissection à partir de l'intervalle indiqué pour trouver sa racine dans cet intervalle. Puis déterminer le nombre d'itérations nécessaires pour obtenir une solution dont le chiffre des millièmes est significatif.

a) $f(x) = 0.3\,x^2 - 0.6\,x - 0.8$ dans l'intervalle $[2.8\,;3]$.

b) $f(x) = x^5 + x^3 - 1$ dans l'intervalle $[0\,;1]$.

c) $f(x) = (x\,\cos(x))^2 - 2.3$ dans l'intervalle $[1.3\,;5.3]$.

5.2.3 On considère l'équation :

$$e^x - (x+5) = 0$$

a) Déterminer le nombre et la position approximative des solutions positives de cette équation.

b) Utiliser l'algorithme de la bissection pour déterminer chacune de ces racines avec une erreur absolue inférieure à 10^{-7}.

5.2.4 Montrer que chacune des fonctions f suivantes possède un zéro unique. Calculer ce zéro par l'algorithme de la bissection.

a) $f(x) = x^3 + 10$
b) $f(x) = x^5 - 2\,x^4 + 100\,x^3 - 2$
c) $f(x) = x - 1 + \frac{1}{2}\sin(x)$
d) $f(x) = 3\,x - \cos(x)$
e) $f(x) = \ln(x) - \cos(x)$
f) $f(x) = x + e^x$

5.2.5 Montrer que la fonction $f = x^3+2\,x-1$ possède un zéro dans l'intervalle $I = [0\,;1]$. Calculer ce zéro par l'algorithme de la bissection.

5.2.6 Déterminer une valeur approchée à 10^{-6} près des éventuels zéros de la fonction

$$f(x) = x^7 + 23\,x^5 + 2\,x^4 - 2$$

Calculer ce zéro par l'algorithme de la bissection.

5.2.7 Soit la fonction

$$f(x) = \cos(x^x) - \sin(e^x)$$

a) Représenter cette fonction sur l'intervalle $I = [0.5\,;\,2.5]$.
b) Déterminer graphiquement le nombre de zéros de f dans I.
c) Déterminer un zéro de f.
d) Représenter cette fonction sur l'intervalle $I = [0.1\,;\,10]$.

5.2.8 Utiliser la méthode de la bissection pour obtenir une valeur approchée du nombre $\sqrt[3]{2}$ à 10^{-4} près.

5.2.9 Utiliser la méthode de la bissection pour obtenir une valeur approchée du nombre π.

5.3 Zéros de fonctions : méthode de Newton

5.3.1 Soit la fonction

$$f(x) = -5\,x^3 + 7\,x^2 + 3\,x - 3$$

a) Calculer les coordonnées des points à tangente horizontale et du point d'inflexion. Tracer le graphe de f dans l'intervalle $[-1\,;2]$.
b) Calculer la valeur des premiers termes de la suite de Newton si l'on choisit l'estimation initial $x_0 = 1$.
c) Calculer la valeur des premiers termes de la suite de Newton si l'on choisit l'estimation initial $x_0 = 2$.
d) Déterminer l'unique zéro de f compris entre 1 et 2.

5.3.2 L'équation

$$e^x - 3\,x^2 = 0$$

possède les solutions $s_1 = -0.4589623$ et $s_2 = 0.91$ ainsi qu'une troisième solution s_3 située près de 4.
Utiliser la méthode de Newton pour déterminer s_3 avec six décimales.

5.3.3 Trouver une estimation d'un zéro strictement positif des fonctions suivantes en appliquant la méthode de Newton.

a) $f(x) = x^3 - 2$

b) $f(x) = \sin(x) - \dfrac{x}{4}$

5.3.4 Soit la fonction

$$f(x) = x^3 - 2\,x - 5$$

a) Montrer que l'équation $f(x) = 0$ admet une unique solution α sur $\mathbb{R}$. Montrer que $2 < \alpha < 3$.

b) A partir de $x_0 = 1$, déterminer le zéro de la fonction.

5.3.5 Donner une approximation de $\sqrt{2}$ avec la méthode de Newton en partant du point $x_0 = 2$.

5.3.6 Une des difficultés de la méthode de Newton est de bien choisir x_0 de sorte que l'on ne tombe pas sur un point où la dérivée s'annule.
Utiliser l'algorithme de Newton avec la fonction $f(x) = \cos(x)$ en partant des points d'abscisse 1, 0.5, 0.1 puis 0.01.
Commenter et expliquer la situation à l'aide d'un graphique.

5.4 Zéros de fonctions : méthode de la sécante

5.4.1 A l'aide de la méthode de la sécante, calculer la racine douzième de 1.1 avec une précision de 8 décimales.

5.4.2 Rechercher, en utilisant la méthode de la sécante, les solutions de l'équation

$$x^3 + 1 = 3\,x$$

5.4.3 Calculer dans l'intervalle $I = [0\,;\pi]$ une approximation de la solution de l'équation

$$\cos(x) = 2\,\sin(x)$$

5.4.4 Rechercher, en utilisant la méthode de la sécante, les solutions de l'équation

$$e^{-x} = -\ln(x)$$

5.5 Un peu d'intégration numérique

5.5.1 Sans utiliser de bibliothèque autre que la bibliothèque mathématique standard de python, écrire une fonction qui prend deux nombres réels $a < b$ et un nombre entier n en paramètres. Cette fonction doit renvoyer une liste de $n + 1$ valeurs réelles, notées $x_0, x_1, \ldots, x_n$ telles que $x_0 = a$, $x_n = b$, tous les autres nombres étant uniformément répartis dans l'intervalle $[a, b]$.
L'instruction

```
print(listePoints(0, 2, 10))
```

fait afficher la liste

```
[0, 0.2, 0.4, 0.6, 0.8, 1.0, 1.2, 1.4, 1.6, 1.8, 2]
```

à quelques erreurs d'arrondi près.

5.5.2 Compléter le code de la fonction de l'exercice précédent en lui ajoutant un paramètre optionnel `aleatoire=False`. Par défaut, le comportement de la fonction est le même que celle de l'exercice précédent. Si le paramètre `aleatoire` prend la valeur `True`, la fonction doit renvoyer une liste de $n + 1$ valeurs réelles, notées $x_0, x_1, \ldots, x_n$ telles que $x_0 = a$, $x_n = b$, tous les autres nombres étant aléatoirement choisis dans l'intervalle $[a, b]$.

L'instruction

```
print(listePoints(0, 2, 10)) # Valeur par défaut de aleatoire
```

fait afficher la liste

```
[0, 0.2, 0.4,
 0.6000000000000001, 0.8, 1.0, 1.2, 1.4,
 1.5999999999999999, 1.7999999999999998,
 1.9999999999999998]
```

L'instruction

```
print(listePoints(0, 2, 10, True))
```

fait afficher la liste

```
[0,
 0.06479694651588885, 0.28981342176727964, 0.3179007067671271,
 0.4070274425545328,  1.015739468424949,   1.1182123677493638,
 1.2618287932253878,  1.473438685747842,   1.519412756197574,
 2]
```

Il faut noter que le résultat change à chaque fois que le programme tourne.

5.5.3 Créer une classe `Fonction` qui stocke dans un champ une fonction mathématique f. Dans cette classe, créer une méthode dont le nom est `listeValeurs` qui prend une liste de nombres en paramètre et qui renvoie la liste des valeurs prises par la fonction f en chacun des points.

Importer le module `math` de python et vérifier que l'exécution des lignes

```
lp = listePoints(0, math.pi / 2, 10)
    f = Fonction(math.sin)
    for val in f.listeValeurs(lp):
        print(val)
```

donne l'affichage suivant :

```
0.0
0.15643446504023087
0.3090169943749474
0.45399049973954675
0.5877852522924731
0.7071067811865475
0.8090169943749473
0.8910065241883678
0.9510565162951535
0.9876883405951378
1.0
```

5.5.4 Compléter la classe `Fonction` avec une méthode dont l'en-tête est

```
def sommeRect(self, a, b, n, aleatoire=False)
```

qui renvoie

- la liste des n points choisis dans l'intervalle $[a, b]$;
- une liste de valeurs définies par l'expression

$$\min(f(x_i); f(x_{i+1}))$$

  pour i compris entre 0 et $n - 1$.
- Une approximation de

$$\int_a^b f(x)\, dx$$

  par une somme d'aires de rectangles, en sélectionnant à chaque itération le rectangle « sous la courbe ».
- une liste de valeurs définies par l'expression

$$\max(f(x_i); f(x_{i+1}))$$

  pour i compris entre 0 et $n - 1$.
- Une approximation de

$$\int_a^b f(x)\, dx$$

  par une somme d'aires de rectangles, en sélectionnant à chaque itération le rectangle « en dessus de la courbe ».

La valeur par défaut du paramètre `aleatoire` donne un découpage régulier de l'intervalle $[a, b]$. Si la valeur `True` est passée en paramètre, le découpage est aléatoire.

Faire calculer

$$\int_0^2 (2\,x^2 - x^3)\,dx$$

en découpant l'intervalle en 10 morceaux, uniformément ou aléatoirement.
Écrire les instructions qui donnent l'affichage suivant lorsque le programme tourne :

```
Intervalle découpé en 10 morceaux identiques :

1.0848000000000002
1.5552

Intervalle découpé aléatoirement en 10 morceaux (5 essais)

0.8943893487419508
1.7009476901969376
*
0.8878935584553052
1.770292543499321
*
0.8352384010982953
1.5033073760799847
*
0.9881561937421527
1.5762026218159841
*
0.8617505588265767
1.7164006543400632
```

5.5.5 À l'aide de la méthode `sommeRect()` de la classe `Fonction`, calculer une approximation de

$$\int_{-0.5}^{1} e^{-x^2}\,dx$$

dont les 6 premières décimales sont correctes, en découpant l'intervalle $[-0.5, 1]$ en n morceaux. Quelle est la plus petite valeur de n qui garantit ce résultat ?

5.5.6 Pour $n \in \{10, 100, 1000, 10000, 100000\}$, faire calculer une approximation de

$$\int_1^2 \frac{1}{x}\,dx$$

uniforme et aléatoire.

a) Comparer les valeurs obtenues par les deux méthodes.

b) Comparer avec la valeur exacte obtenue par le calcul de la primitive.

Quelle conclusion en tirer ?

5.5.7 Compléter la classe `Fonction` avec une méthode dont l'en-tête est

```
def sommeTrap(self, a, b, n, aleatoire=False)
```

qui renvoie une approximation de

$$\int_a^b f(x)\,dx$$

à l'aide d'une somme d'aires de trapèzes. La somme peut être calculée de la façon suivante: Pour tout i compris entre 0 et $n-1$, l'expression

$$(x_{i+1}-x_i)\cdot\frac{(f(x_i)+f(x_{i+1}))}{2}$$

contribue à la somme totale.

5.5.8 À l'aide de la méthode `sommeTrap()` de la classe `Fonction`, calculer une approximation de

$$\int_{-0.5}^{1} e^{-x^2}\,dx$$

dont les 6 premières décimales sont correctes, en découpant l'intervalle $[-0.5, 1]$ en n morceaux. Quelle est la plus petite valeur de n qui garantit ce résultat ?

5.5.9 Compléter la classe `Fonction` avec une méthode dont l'en-tête est

```
def sommeSim(self, a, b, n, aleatoire=False)
```

qui renvoie une approximation de

$$\int_a^b f(x)\,dx$$

à l'aide d'une somme d'aires, calculées de la façon suivante :

- L'intervalle $[a, b]$ est découpé en n sous-intervalles, régulièrement ou non.
- On détermine pour chaque sous-intervalle $I_i = [x_i, x_{i+1}]$ l'expression mathématique de la parabole qui passe par les trois points $(x_i, f(x_i))$, $(m, f(m))$ et $(x_{i+1}, f(x_{i+1}))$ où m désigne le milieu de l'intervalle I_i.
- On calcule ensuite la valeur exacte de l'intégrale de cette parabole sur l'intervalle I_i, qui contribue à la somme totale.
- Ce calcul ayant été fait pour tout i, on renvoie la somme qui donne l'approximation de l'intégrale.

5.5.10 Compléter la classe `Fonction` avec une méthode dont l'en-tête est

```
def sommeNewt(self, a, b, n, aleatoire=False)
```

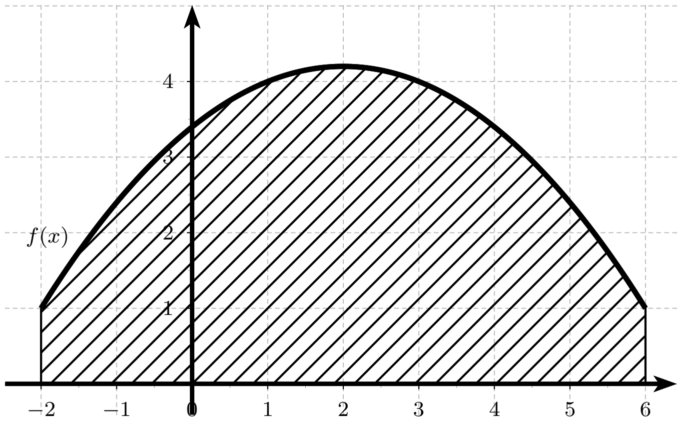
qui renvoie une approximation de

$$\int_a^b f(x)\,dx$$

à l'aide d'une somme d'aires.

5.6 Calcul d'aire sous une courbe par la méthode des rectangles

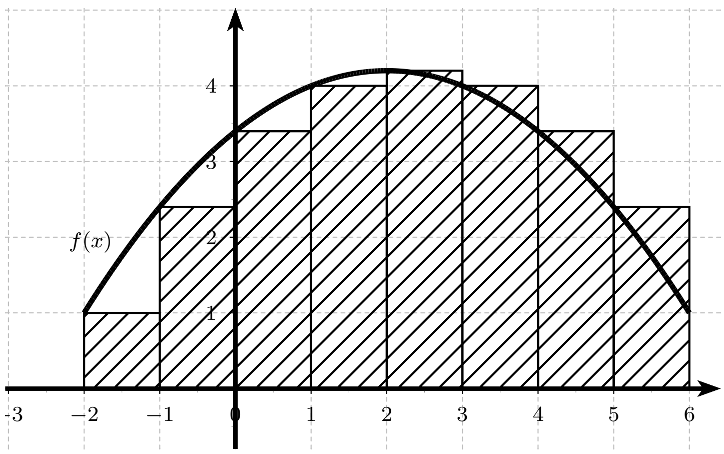
5.6.1 On supposera ici que nos fonctions sont toutes positives sur l'intervalle sur lequel on les considère.
Définissons d'abord ce qu'est l'aire sous la courbe représentative d'une fonction sur un intervalle $[a; b]$: c'est tout simplement l'aire comprise entre la courbe représentative, l'axe des abscisses et les droites $x = a$ et $x = b$. On note cette aire $\int_a^b f(x)\,dx$.



Dans cette méthode, on calcule l'intégrale numérique en réalisant une somme de surfaces de rectangles. Le domaine d'intégration est découpé en intervalles et on fait comme si la fonction restait constante sur chaque intervalle.
Sur chaque intervalle, on réalise ainsi l'approximation suivante :

$$\int_a^b f(x)\,dx = (b-a)\cdot f(\alpha)$$

où α est une abscisse appartenant à l'intervalle limité par a et b.
Nous nous limiterons ici aux cas où $\alpha = a$ ou $\alpha = b$, ce qui signifie que pour chaque intervalle nous considérons comme constante la valeur prise par la fonction à l'extrémité gauche ou droite de l'intervalle.
Comme exemple, nous allons réaliser un programme d'intégration pour $\alpha = a$ et nous visualiserons les rectangles. Cette approximation de l'aire est appelée somme à gauche, notée `SommeGauche`.



a) Représenter la fonction $f(x) = \frac{-1}{5}(x+2)(x-6)+1$ définie dans l'intervalle $[-2;\, 6]$.

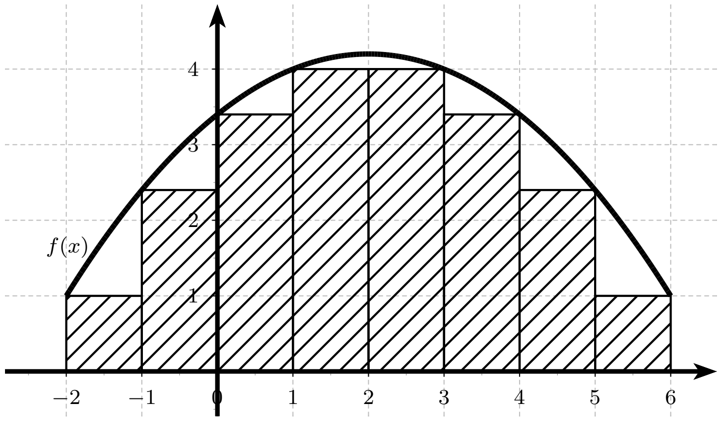
b) Représenter ensuite les 8 rectangles comme sur la figure ci-dessus.

c) Finalement, estimer l'aire sous la courbe comme la somme de ces huit rectangles.

5.6.2 Soit la fonction $f(x) = \frac{-1}{5}(x+2)(x-6)+1$ définie dans l'intervalle $[-2;\, 6]$ représentée dans l'exercice précédent.

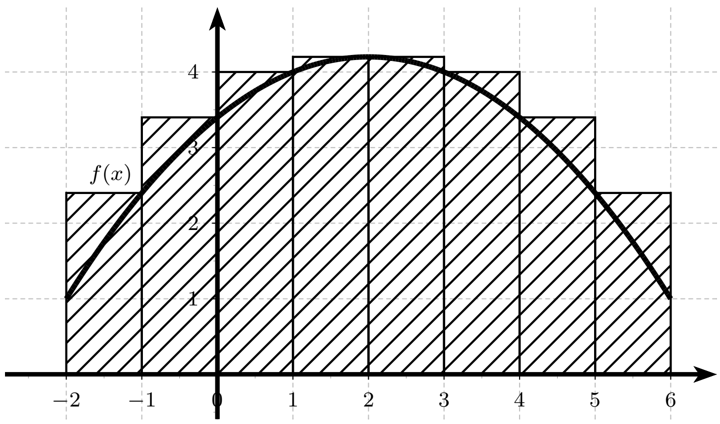
a) Calculer la somme à droite (`SommeDroite`) de cette fonction.

b) Pour chaque rectangle, choisir $\alpha = Min\,(f(x_i), x_i \in [a_i, a_i+1])$ où $a_i = -2, -1, \ldots, 5$. La somme de ces huit rectangles donne la somme inférieure (`SommeInferieure`).



Calculer cette somme inférieure.

c) Calculer également la somme supérieure (`SommeSuperieure`) de cette fonction sur le même intervalle.



5.6.3 Pour une fonction f continue et positive sur un intervalle $[a;\, b]$ et $n \in \mathbb{N}$, posons $h = \frac{b-a}{n}$ et $x_i = a + i\,h$ pour tout $i = 0, \ldots, n$.

Pour les quatre méthodes, écrire un programme qui dessine les rectangles et approche l'aire sous la courbe.

a) Avec la méthode de la somme à gauche (`SommeGauche`).

b) Avec la méthode de la somme à droite (`SommeDroite`).

c) Avec la méthode de la somme à inférieure (`SommeInferieure`).

d) Avec la méthode de la somme à supérieure (`SommeSuperieure`).

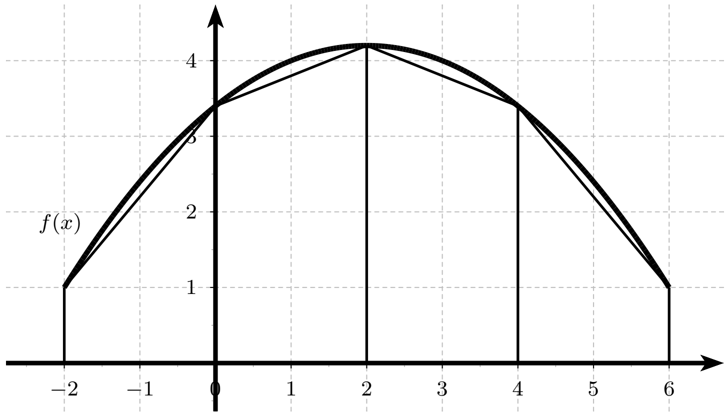
5.6.4 Estimer les deux intégrales à l'aide des 4 méthodes de l'exercice 5.6.3.

a) $\int_0^{\frac{1}{2}} \cos(\pi\, x)\, \sqrt{x^2+1}\, dx$

b) $\int_0^1 (x\, \ln(x+1)+1)\, dx$

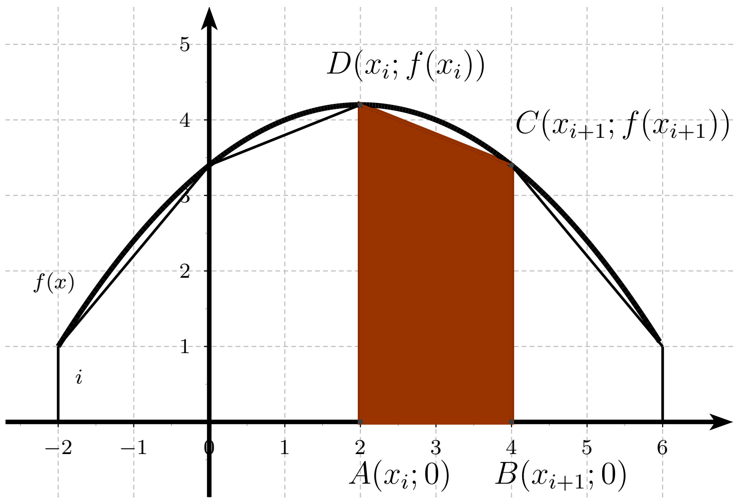
5.7 Calcul d'aire sous une courbe par la méthode des trapèzes

5.7.1 Le principe général est exactement le même que celui de la méthode des rectangles, mais on approche cette fois-ci la courbe sur le segment $[a_i, a_{i+1}]$ par le segment de droite reliant les deux points de la courbe d'abscisses a_i et a_{i+1}, ce qui revient à calculer une somme d'aires de trapèzes pour approcher l'intégrale.



Pour la fonction $f(x) = \frac{-1}{5}\,(x+2)(x-6)+1$ définie dans l'intervalle $[-2;\, 6]$, représenter les 4 trapèzes, puis estimer l'aire comme somme de ces quatre trapèzes (`SommeTrapeze`).

5.7.2 Pour une fonction f continue et positive sur un intervalle $[a;\, b]$ et $n \in \mathbb{N}$, posons $h = \frac{b-a}{n}$ et $x_i = a + i\, h$ pour tout $i = 0, \ldots, n$.
Écrire un programme `SommeTrapeze` qui dessine les trapèzes de sommets $A(x_i;\, 0)$, $B(x_{i+1};\, 0)$, $C\,(x_{i+1};\, f(x_{i+1}))$ et $D\,(x_i;\, f(x_i))$, puis approche l'aire sous la courbe comme la somme de tous les trapèzes.



5.7.3 Soit l'intégrale

$$I = \int_1^2 \frac{1}{x}\, dx$$

a) Évaluer cette intégrale par la méthode des trapèzes pour le pas $h = \frac{1}{3}$.

b) Calculer la valeur exacte de I.

c) Expliquer pourquoi la valeur numérique obtenue est supérieure à $\ln(2)$.

d) Est-ce vrai pour tout pas h ?

5.7.4 Calculer à l'aide de la méthode des trapèzes

$$I = \int_0^1 \frac{4}{1+x^2}\, dx$$

Combien de sous-intervalles sont nécessaires pour que $|\pi - I| < 10^{-6}$?

5.7.5 (5.5.8) À l'aide des programmes des exercices 5.6.3 et 5.7.2, calculer une approximation de

$$\int_{-0.5}^1 e^{-x^2}\, dx$$

dont les 6 premières décimales sont correctes, en découpant l'intervalle $[-0.5, 1]$ en n morceaux. Quelle est la plus petite valeur de n qui garantit ce résultat ?

5.8 Calcul d'aire sous une courbe par la méthode de Simpson

5.8.1 Soit une fonction f continue et positive sur un intervalle $[a;\, b]$.
Soit x_0 le milieu de l'intervalle.

a) Démontrer qu'il existe $h > 0$ tel que $a = x_0 - h$ et $b = x_0 + h$.

b) Pour calculer l'aire sous la courbe, on remplace le graphe de f par la parabole (ou la droite) $y = a\,x^2 + b\,x + c$ passant par les trois points $P(x_0 - h;\, f(x_0 - h))$, $Q(x_0;\, f(x_0))$ et $R(x_0 + h;\, f(x_0 + h)$. Démontrer que

$$I = \int_{x_0-h}^{x_0+h} \left(a\,x^2 + b\,x + c\right)\, dx = \int_{-h}^{h} \left(A\,x^2 + B\,x + C\right)\, dx$$

où $g : x \to A\,x^2 + B\,x + C$ est le polynôme qui passe par les points $P'(-h;\, f(x_0 - h))$, $Q'(0;\, f(x_0))$ et $R'(h;\, f(x_0 + h)$.

c) Démontrer que $I = \frac{2}{3}\,Ah^3 + 2Ch$.

d) Finalement, démontrer que $I = \dfrac{h}{3}\left(f(x_0 - h) + 4f(x_0) + f(x_0 + h)\right)$.

5.8.2 Utiliser la méthode de Simpson pour calculer

$$I = \int_1^9 \sqrt{x}\, dx$$

5.8.3 On souhaite calculer $I = \displaystyle\int_{-1}^{1} 8\,x^4 - 8\,x^2 + 2\,dx$.

a) Donner la valeur de l'approximation de l'intégrale obtenue par la méthode de Simpson.

b) Calculer l'erreur exacte en se servant du calcul explicite de I.

c) Dans ce cas, la méthode de Simpson donne-t-elle un bon résultat ? Expliquer votre réponse.

5.9 Applications de l'intégration numérique

5.9.1 Soit f une fonction qui ne possède pas de primitive s'exprimant à l'aide de fonctions simples.

On peut toutefois définir une primitive F en estimant l'intégrale $\displaystyle\int_a^x f(t)\,dt$.

Tracer les graphes de f et F sur l'intervalle $[a;\, b]$ dans les situations suivantes :

a) $f(x) = \dfrac{\sin(x)}{x}$, $a = \frac{\pi}{3}$ et $b = \pi$.

b) $f(x) = \dfrac{1}{\sqrt{1+x^4}}$, $a = 0$ et $b = 3$.

c) $f(x) = \dfrac{1}{\sqrt{1-\cos(x)}}$, $a = 1$ et $b = 5$.

5.9.2 Estimer les intégrales suivantes et démontrer que leur valeur converge vers la valeur donnée.

a) $I_1 = \displaystyle\int_0^{10} x^3\,e^{-x}\,dx = 6 - 1366\,e^{-10}$.

b) $I_2 = \displaystyle\int_0^{10} \frac{1}{e^x + e^{-x}}\,dx = \arctan\left(e^{10}\right) - \frac{\pi}{4}$.

c) $I_3 = \displaystyle\int_0^{10} \frac{1}{(1+x^2)^2}\,dx = \frac{1}{2}\,\arctan(10) + \frac{5}{101}$.

5.9.3 Calculer le plus précisément possible les intégrales suivantes.

a) $I_1 = \displaystyle\int_0^{\infty} \frac{1}{\sqrt{1+x^4}}\,dx$.

b) $I_2 = \displaystyle\int_0^{\pi} \frac{\sin(x)}{x}\,dx$.

c) $I_3 = \displaystyle\int_0^{\infty} \frac{\sin(x)}{x}\,dx$.

5.10 Solutions des exercices

5.1.1 —

5.1.2 La fonction `np.linspace(debut, fin, nombre)` permet de créer une liste de `N` nombres qui commencent à la valeur `debut` et s'arrête à la valeur `fin` et uniformément répartis.

5.1.3 Tracé de $y = \cos(x) + 3\,\sin(2\,x)$

5.1.4 Tracé de $y = \cos(x) + 3\,\sin(2\,x)$

5.1.5 —

5.1.6 —

5.1.7

```
import matplotlib.pyplot as plt
import numpy as np
def f(x):
    return x**3+3*(x**2)-9*x+1
x = np.linspace(-2,4,100)
plt.plot(x,f(x))
plt.grid(True)
plt.title("Exercice 5.1.7")
plt.xlabel('x')
plt.ylabel('f(x)')
plt.show()
```

5.1.8

```
import matplotlib.pyplot as plt
import numpy as np
import math
pi = math.pi
```

```
def f(x):
    return 3*np.cos(2*x)-2*np.sin(3*x)
x = np.linspace(-pi,pi,100)
plt.plot(x,f(x))
plt.grid(True)
plt.title("Exercice 5.1.8")
plt.xlabel('x')
plt.ylabel('f(x)')
plt.show()
```

5.1.9

Il faut faire attention à ne pas représenter la droite $x = 1$.

```
import matplotlib.pyplot as plt
import numpy as np
def f(x, n):
    return (1-n*x)/(x-1)
x = np.linspace(-2,4,201)
for n in range(-3, 4):
    l = 'n = ' + str(n)
    plt.plot(x,f(x, n), label=l)
plt.grid(True)
plt.title("Exercice 5.1.9")
plt.xlabel('x')
plt.ylabel('f(x)')
plt.xlim(-2, 4)
plt.ylim(-8, 8)
plt.legend()
plt.show()
```

5.1.10

```
import matplotlib.pyplot as plt
```

```
import numpy as np
x = np.linspace(0.1,10,100)
plt.plot(x,np.log(x),color="green",label="log(x)")
plt.plot(x,np.sqrt(x),color="red",label="sqrt(x)")
plt.plot(x,np.exp(np.log(x)),color="blue")
plt.grid(True)
plt.title("Exercice 5.1.10")
plt.xlabel('x')
plt.ylabel('f(x)')
plt.legend()
plt.show()
```

On a $e^{\ln(x)} = x$.

5.1.11

```
import matplotlib.pyplot as plt
import numpy as np
t = np.linspace(0, 10 * np.pi, 300) # Spirale d'Archimede
x = t * np.cos(t)
y = t * np.sin(t)
plt.plot(x, y)
plt.show()
```

5.1.12

Par exemple :

```
import matplotlib.pyplot as plt
import numpy as np
def f(x):
    return x*x
def df(x):
    return 2*x
x = np.linspace(-1,3,100)
```

```
y = df(1)*(x-1)+f(1)
plt.plot(x,f(x),color="green",label="x^2")
plt.plot(x,y,color="red",label="tangente")
plt.grid(True)
plt.title("Exercice 5.1.12")
plt.xlabel('x')
plt.ylabel('f(x)')
plt.legend()
plt.show()
```

5.2.1

$I_0 = [0.1\,;2.4]\,;\, I_1 = [0.1\,;1.25]\,;\, I_2 = [0.675\,;1.25]\,;\, I_3 = [0.9625\,;1.25]\,;\, I_4 = [0.9625\,;1.10625]\,;$ $I_5 = [0.9625\,;1.034375]$

5.2.2

a) 2.9 ; 2.95 ; 2.925. Il faut au moins neuf itérations.

b) 0.5 ; 0.75 ; 0.875. Il faut au moins onze itérations.

c) 3.3 ; 2.3 ; 1.8. Il faut au moins treize itérations.

5.2.3

a) Si $f(x) = e^x - (x+5)$, alors $f'(x) = e^x - 1$ est positive pour $x > 0$ et donc f est strictement croissante sur $\mathbb{R}^+$. Par conséquent, f ne croise l'axe des x qu'une seule fois. Puisque $f(0) = -4$ et $f(2) = 0.38$, il y a une seule racine entre $x = 0$ et $x = 2$.

b) On obtient $x = 1.9368473291$ en 23 itérations à partir de l'intervalle $[0\,;2]$.

5.2.4

a) -2.1544347

b) 0.2718682

c) 0.6840367

d) 0.3167508

e) 1.302964

f) -0.5671433

5.2.5

$x = 0.4533976515$

5.2.6

$x = 0.595471$

5.2.7 —

5.2.8 —

5.2.9 —

5.3.1

a) minimum : $(-0.18\,;-3.28)$, maximum : $(1.11\,;2.12)$, point d'inflexion : $(0.47\,;-0.58)$

b) 0, 1, 0, 1, 0, 1, 0, ...

c) 1.6896552, 1.5618930, 1.5372456, 1.5363390, 1.5363378

d) 1.5363378

5.3.2

$s_3 = 3.733079$

5.3.3

a) 1.259921050

b) 2.474576794

5.3.4

a) A partir du tableau des variations de f

b) 2.0945514815

5.3.5 —

5.3.6 —

5.4.1

$r = 1,00796779$

5.4.2

$x_1 = -1.8793852416$, $x_2 = 0.3472963553$ et $x_3 = 1.5320888862$

5.4.3

$x = 0.4636476092$

5.4.4

$x = 0.5671432873$

5.5.1

```
def listePoints(a, b, n):
    if a > b:
        a, b = b, a
    lp = [a]
    delta = (b - a) / n
    for i in range(n):
        a = a + delta
        lp.append(a)
    return lp
```

5.5.2

```
import random


def listePoints(a, b, n, aleatoire=False):
    if a > b:
        a, b = b, a
    lp = [a]
    if not aleatoire:
        delta = (b - a) / n
        for i in range(n):
            a = a + delta
            lp.append(a)
    else:
        for i in range(n - 1):
            x = a + (b - a) * random.random()
```

```
            lp.append(x)
        lp.append(b)
        lp.sort()
    return lp
```

5.5.3

```
import math
import random



def listePoints(a, b, n, aleatoire=False):
    if a > b:
        a, b = b, a
    lp = [a]
    if not aleatoire:
        delta = (b - a) / n
        for i in range(n):
            a = a + delta
            lp.append(a)
    else:
        for i in range(n - 1):
            x = a + (b - a) * random.random()
            lp.append(x)
        lp.append(b)
        lp.sort()
    return lp



class Fonction(object):
    def __init__(self, f):
        self.f = f
```

```
    def listeValeurs(self, lp):
        lv = []
        for x in lp:
            lv.append(self.f(x))
        return lv


if __name__ == "__main__":
    lp = listePoints(0, math.pi / 2, 10)
    f = Fonction(math.sin)
    for val in f.listeValeurs(lp):
        print(val)
```

5.5.4

```
import math
import random

def listePoints(a, b, n, aleatoire=False):
    if a > b:
        a, b = b, a
    lp = [a]
    if not aleatoire:
        delta = (b - a) / n
        for i in range(n):
            a = a + delta
            lp.append(a)
    else:
        for i in range(n - 1):
            x = a + (b - a) * random.random()
            lp.append(x)
```

```
        lp.append(b)
        lp.sort()
    return lp



class Fonction(object):
    def __init__(self, f):
        self.f = f

    def listeValeurs(self, lp):
        lv = []
        for x in lp:
            lv.append(self.f(x))
        return lv

    def sommeRect(self, a, b, n, aleatoire=False):
        lp = listePoints(a, b, n, aleatoire)
        sSup, sInf = 0.0, 0.0
        lvSup = []
        lvInf = []
        for i in range(n):
            delta = lp[i + 1] - lp[i]
            valeurs = self.f(lp[i]), self.f(lp[i + 1])

            v_inf = min(valeurs)
            lvInf.append(v_inf)
            sInf += v_inf * delta

            v_sup = max(valeurs)
            lvSup.append(v_sup)
            sSup += v_sup * delta
```

```
        return lp, lvSup, sSup, lvInf, sInf

if __name__ == "__main__":
    g = Fonction(lambda x : 2 * x**2 - x**3)
    lp, lvSup, sSup, lvInf, sInf = g.sommeRect(0.0, 2.0, 10)
    print("Intervalle découpé en 10 morceaux identiques : ")
    print()
    print(sInf)
    print(sSup)
    print()
    print("Intervalle découpé aléatoirement en 10 morceaux (5 essais)")
    print()
    for i in range(5):
        lp, lvSup, sSup, lvInf, sInf = g.sommeRect(0.0, 2.0, 10, True)
        # print(lv)
        print(sInf)
        print(sSup)
        print("*")
```

5.5.5

```
if __name__ == "__main__":
    h = Fonction(lambda x : math.e**(-x**2))
    n = 100
    lp, lvSup, sSup, lvInf, sInf = h.sommeRect(-0.5, 1.0, n)
    print("Intervalle découpé en {} morceaux identiques : ".format(n))
    print()
    print(sInf)
    print(sSup)
    print()
    while sSup - sInf > 0.000001:
```

```
        n *= 10
        lp, lvSup, sSup, lvInf, sInf = h.sommeRect(-0.5, 1.0, n)
    print(sSup)
    print(sInf)
    print(n)
    print("Valeur donnée par le site Wolfram Alpha")
    print("1.208105139225219474155170372872306108438258775776897 4")

if __name__ == "__main__":
    aire = 0.693147180559836
    g = Fonction(lambda x : 1 / x)
    nombres = [10, 100, 1000, 10000, 100000]
    for n in nombres:
        lp, lvSup, sSup, lvInf, sInf = g.sommeRect(1.0, 2.0, n)
        lpa, lvSupa, sSupa, lvInfa, sInfa = g.sommeRect(1.0, 2.0, n, True)
        print(sInf, sInfa, sSup, sSupa)
        print(5 * "*")
        lpa, lvSupa, sSupa, lvInfa, sInfa = g.sommeRect(1.0, 2.0, n, True)
    print(5 * "*")
    print(aire)

def sommeTrap(self, a, b, n, aleatoire=False):
    lp = listePoints(a, b, n, aleatoire)
    s = 0.0
    lv = []
    for i in range(n):
        delta = lp[i + 1] - lp[i]
        valeur = (self.f(lp[i]) + self.f(lp[i + 1])) * 0.5

        lv.append(valeur)
        s += delta * valeur
```

```
    return lp, lv, s
```

5.5.6 5.5.7 5.5.8

```
if __name__ == "__main__":
    h = Fonction(lambda x : math.e**(-x**2))
    n = 100
    lp_1, lv_1, s_1 = h.sommeTrap(-0.5, 1.0, n)
    n *= 10
    lp_2, lv_2, s_2 = h.sommeTrap(-0.5, 1.0, n)
    while abs(s_2 - s_1) > 0.000001:
     lp_1, lv_1, s_1 = h.sommeTrap(-0.5, 1.0, n)
        n *= 10
        lp_2, lv_2, s_2 = h.sommeTrap(-0.5, 1.0, n)
    print(s_2)
    print(n)
    print("Valeur donnée par le site Wolfram Alpha")
    print("1.20810513922521947415517037287230610843825877577689 74")

# Deux fonctions auxiliaires
def coeffParaboleParTroisPoints(x_1, y_1, x_2, y_2, x_3, y_3):
    a = ((y_3 - y_1)/(x_3 - x_1) - (y_2 - y_1)/(x_2 - x_1)) / (x_3 - x_2)
    b = -a * (x_2 + x_1) + (y_2 - y_1)/(x_2 - x_1)
    c = y_1 - a * x_1**2 - b * x_1
    return a, b, c


def primPara(a, b, c):
    return lambda x: 1/3 * a * x**3 + 1/2 * b * x**2 + c * x


# Méthode de la classe Fonction
def sommeSim(self, a, b, n, aleatoire=False):
    lp = listePoints(a, b, n, aleatoire)
    s = 0.0
```

```
    for i in range(n):
        x_3 = lp[i + 1]
        y_3 = self.f(x_3)
        x_2 = (lp[i + 1] + lp[i]) / 2
        y_2 = self.f(x_2)
        x_1 = lp[i]
        y_1 = self.f(x_1)
        a, b, c = coeffParaboleParTroisPoints(x_1, y_1, x_2, y_2, x_3, y_3)
        F = primPara(a, b, c)
        s += F(x_3) - F(x_1)

    return lp, s

def sommeNewt(self, a, b, n, aleatoire=False)
    pass
```

5.5.9 5.5.10 5.6.1

5.6.2

5.6.3

5.6.4

5.7.1

5.7.2

5.7.3

5.7.4

5.7.5

5.8.1

5.8.2

5.8.3

5.9.1

5.9.2

5.9.3

Chapitre 6

Géométrie sphérique

6.1 Approche graphique

6.1.1 Dans le logiciel `Geogebra`, ouvrir une vue `Graphique` standard et une vue `Graphique 3D` d'un même document. Nommer ce document `Exercice_6.1.1`. Ensuite,

a) définir un `Nombre R=5` ;
b) placer les points `O=(0, 0, 0)`, `X=(R, 0)` et `Y=(0, R)` ;
c) tracer le cercle de centre `O` et de rayon `R` dans le plan `XOY`. Nommer ce cercle `Equateur` ;
d) placer les points `Nord=(0, 0, R)` et `Sud=(0, 0, -R)` ;
e) tracer la sphère de de centre `O` et de rayon `R`. La couleur de cette sphère est bleue avec une opacité de 25% ;
f) tracer le cercle passant par les point `X`, `Nord` et `Sud`. Nommer ce cercle `Greenwitch`.

6.1.2 Dupliquer le document `Exercice_6.1.1` sous `Exercice_6.1.2`. Puis,

a) tracer à partir du méridien de `Greenwitch`, cinq autres méridiens équidistants sur l'`Equateur` ;
b) tracer quatre parallèles aux latitudes $0° + k \cdot 30°$, avec $k = -2, -1, 1, 2$.

6.1.3 Dupliquer le document `Exercice_6.1.2` sous `Exercice_6.1.3`. Puis,

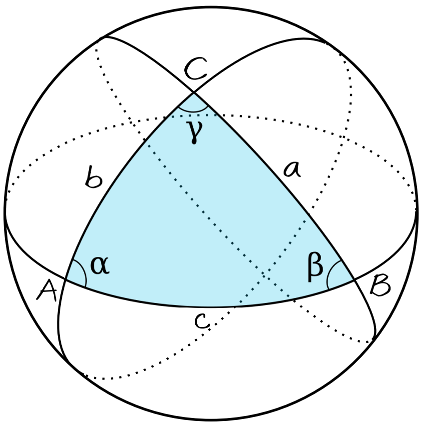
a) placer le point `Dep=(60° N, 30° E)` ;
b) placer le point `Arr=(30° S, 60° W)` ;
c) représenter le plus court chemin reliant le point `Dep` au point `Arr` ;
d) quelle est la distance entre ces deux points sur la terre sachant que `R=6371 km`.

6.1.4 Dupliquer le document `Exercice_6.1.1` sous `Exercice_6.1.4`. Puis,

a) dans la vue `Graphique` standard créer un `curseur Long` de type `angle` de type `intervalle` variant entre $-90°$ et $90°$ avec un `incrément` de $0.1°$;
b) dans la vue `Graphique` standard créer un `curseur Lati` de type `angle` de type `intervalle` variant entre $-180°$ et $180°$ avec un `incrément` de $0.1°$;
c) placer ensuite un point sur la sphère dans la `Graphique 3D` situé aux coordonnées `(Long, Lati)`.

6.2 Formules des cosinus et des sinus

6.2.1 Soit Σ une sphère de centre O et de rayon R.



a) Un grand cercle de Σ est un cercle de Σ centré en O.

b) ABC est un triangle sphérique si AB, AC et BC sont des arcs de grands cercles de Σ.

c) Si t_{AB} et t_{AC} sont respectivement les tangentes aux arcs AB et AC dans les plans OAB et OAC, $\alpha = \measuredangle(t_{AB}\ , t_{AC})$ est l'angle sphérique ABC.

d) a, b et c sont respectivement les mesures des arcs BC, AC et AB dans les plans OBC, OAC et OAB.

Démontrer les formules du théorème fondamental.

a) $\cos(a) = \cos(b) \cdot \cos(c) + \sin(b) \cdot \sin(c) \cdot \cos(\alpha)$

b) $\cos(b) = \cos(c) \cdot \cos(a) + \sin(c) \cdot \sin(a) \cdot \cos(\beta)$

c) $\cos(c) = \cos(a) \cdot \cos(b) + \sin(a) \cdot \sin(b) \cdot \cos(\gamma)$

d) $\cos(\alpha) = -\cos(\beta) \cdot \cos(\gamma) + \sin(\beta) \cdot \sin(\gamma) \cdot \cos(a)$

e) $\cos(\beta) = -\cos(\gamma) \cdot \cos(\alpha) + \sin(\gamma) \cdot \sin(\alpha) \cdot \cos(b)$

f) $\cos(\gamma) = -\cos(\alpha) \cdot \cos(\beta) + \sin(\alpha) \cdot \sin(\beta) \cdot \cos(c)$

g) $\dfrac{\sin(a)}{\sin(\alpha)} = \dfrac{\sin(b)}{\sin(\beta)} = \dfrac{\sin(c)}{\sin(\gamma)}$

6.3 Calculs sur la sphère

6.3.1 Déterminer a, b, c, α, β et γ dans le cas où A représente le pôle nord, B la ville de San Francisco (37°48' N ; 122°24' W) et C la ville de St-Petersbourg (59°54' N ; 30°18' E).

6.3.2 Résoudre les triangles sphériques ABC suivants :

a) $a = 121°\ 15{,}4'$, $b = 104°\ 54{,}7'$, $c = 65°\ 42{,}5'$

b) $\alpha = 117°\ 22{,}8'$, $\beta = 72°\ 38{,}6°$, $\gamma = 58°\ 21{,}2'$

c) $a = 136°\ 2{,}9'$, $c = 21°\ 46{,}3'$, $\beta = 75°\ 31{,}4'$

d) $a = 107°\ 8{,}4'$, $\beta = 66°\ 42{,}7°$, $\gamma = 84°\ 57{,}5'$

6.3.3 On note Γ l'arc de grand cercle passant par Burier (46,45° N ; 6,87° E) et Sydney (31,24° S ; 149,07° E).

a) Calculer la longueur de l'arc Γ.

b) Calculer β et γ les angles formés par Γ et les méridiens passant respectivement par Burier et par Sydney.

c) Donner précisément la position du point de l'équateur qui se trouve sur l'arc Γ.

6.3.4 Calculer la distance, l'angle de route initial, et l'angle de route à l'arrivée lors du parcours de Honolulu (21° 18,3' N ; 157° 52,3' W) à San Francisco (37° 47,5' N ; 122° 25,7' W).

6.3.5 Un navire se rend de Dutch Harbor (53° 53' N ; 166° 35' W) à Melbourne (37° 50' S ; 144° 59' E).

a) Calculer la distance, l'angle de route initial et l'angle de route à l'arrivée.

b) Trouver le point d'intersection du parcours avec l'équateur. Calculer l'angle de route en ce point et sa distance de Dutch Harbor.

c) Trouver le point de la route de longitude 180°. Calculer l'angle de route en ce point et sa distance de Dutch Harbor.

6.3.6 Un navire quitte New York (40° 48,6' N ; 73° 57,5' W) en suivant un angle de route initial égal à 36°.

a) Trouver la position du bateau après qu'il ait parcouru 500 milles.

b) Trouver le point le plus au nord de la route.

6.3.7

a) Calculer la distance, l'angle de route initial, et l'angle de route à l'arrivée lors du parcours de Calcutta (22° 35' N ; 880 27' E) à Melbourne (37° 48' S ; 144° 58' E).

b) Trouver la position du navire lorsqu'il franchit l'équateur, et calculer alors sa distance à Calcutta.

6.3.8 Un avion quitte Honolulu (21° 18,3' N ; 157° 52,3' W) et suit un angle de route de 40° 43'.

a) Trouver le point de la route le plus près du pôle Nord.

b) Calculer sa position quand la longitude est de 74° W.

6.3.9 Bordeaux et Belgrade sont situés pratiquement sur le même parallèle ($44°55'0''$). La longitude de Bordeaux est $0°31'0''$ Ouest, celle de Belgrade est $20°30'0''$ Est.
Calculer la distance entre ces deux villes :

a) en creusant un tunnel permettant d'aller en ligne droite de l'une à l'autre ;

b) en se déplaçant le long d'un arc de grand cercle (route orthodromique) ;

c) en se déplaçant le long du parallèle commun à ces deux villes (route loxodromique).

On prendra $R = 6378$ km pour le rayon terrestre.

6.4 Solutions des exercices

6.1.1 –

6.1.2 –

6.1.3 –

6.1.4 –

6.2.1 –

6.3.1

$a = 79.74°$, $b = 30.1°$, $c = 52.2°$, $\alpha = 152.7°$, $\beta = 13.52°$ et $\gamma = 21.61°$

6.3.2

a) $\alpha = 117.9614°$, $\beta = 93.2142°$, $\gamma = 70.3304°$

b) $a = 111.9051°$, $b = 85.6581°$, $c = 62.7937°$

c) $b = 127°10'24''$, $\alpha = 122°30'6''$, $\gamma = 26°47'18''$

d) $b = 67°8'24''$, $c = 92°7'36''$, $\alpha = 107°43'24''$

6.3.3

a) Γ = 16'377.164 km

b) β = 75.83°, γ = 51.38°

c) (0° N ; 116.08° E)

6.3.4

a) Distance : 3'855 km

b) Angle initial : 53° 40' 10,7548"

c) Angle à l'arrivée : 71° 45' 53.942"

6.3.5

a) Distance : 11'203.2 km ; angle de départ : 216.96° ; angle d'arrivée : 206.67°

b) (0° N ; 162.11° E)

c) (39.11° N ; 180° E) ; angle de route : 207.15° ; distance : 1940.16 km

6.3.6

a) (47.34° N ; 67.74° W)

b) (9.36° N ; 63.58° W)

6.3.7

a) distance : 8937.8 km ; angle de route initial : 138.05° ; angle de route à l'arrivée : 128.64°

b) sur l'équateur : (0° N ; 127.49° E)

6.3.8

a) (52.57° N ; 85.23° W)

b) longitude : 52.04°

6.3.9

a) 1647 km ; b) 1652 km ; c) 1657 km

Chapitre 7

Mathématiques financières

7.1 Intérêts simples

7.1.1 A partir de la formule $S_n = S + n \cdot i \cdot S$, calculer les valeurs de S, i et n.

7.1.2 Quel montant faut-il placer aujourd'hui au taux annuel simple de 3% pour obtenir un capital de 5'000 francs dans 120 jours ?

7.1.3 On place 5'000 francs pendant 90 jours et l'on obtient 5'050 francs. Quel est le taux d'intérêt ?

7.1.4 On place 5'000 francs au taux annuel simple de 3.35% et l'on obtient 5'110 francs. Quelle est la durée du placement en jours ?

7.1.5 On place 5'000 francs au taux annuel simple de 3% pendant 45 jours. Quel est le montant des intérêts obtenus ?

7.1.6 Sur un livret de caisse d'épargne, lorsque, au cours d'un mois, ont été effectués des versements, leur date de valeur (date à laquelle est enregistrée l'opération) est le 1$^{\text{er}}$ ou le 16 qui suit la date de l'opération (on travaille par quinzaine). Pour les retraits, la date de valeur est le 1$^{\text{er}}$ ou le 16 qui précède l'opération. Une personne effectue les opérations suivantes :

a) le 26 décembre 2004, ouverture du livret avec un versement de 10'000 francs.

b) le 20 janvier 2005, versement de 15'000 francs

c) le 10 mars 2005, retrait de 5'000 francs

d) le 30 juin 2005, versement de 7'000 francs

e) le 10 octobre 2005, retrait de 6'000 francs

f) le 14 décembre 2005, versement de 4'000 francs

Le taux d'intérêts est de 6 % jusqu'au 1er août 2005 et de 4 % ensuite. Les intérêts sont calculés par quinzaine. Déterminer le solde du compte, intérêts capitalisés, au 1er janvier 2006.

7.1.7 Un individu place le 1^{er} de chaque mois, du 1^{er} janvier au 1er décembre inclus, une somme de 1'000 francs sur un compte au taux d'intérêts simples de 4.5 % annuel. De quel capital disposera-t-il au 1^{er} janvier de l'année suivante ?

7.2 Intérêts composés

7.2.1 A partir de la formule $C_n = C_0\,(1 + i\,n)$, calculer les valeurs de C_0, i et n.

7.2.2 On place un capital de 10'000 francs à un taux annuel de 5.25%. Quelle somme aura-t-on accumulé (selon la pratique bancaire) après 5 ans ? 10 ans ? 6 mois ? 11 ans et 8 mois ?

7.2.3 Un de vos ancêtres a placé une somme à la banque en l'an 810. Comme un intérêt bancaire de 2% a été capitalisé annuellement jusqu'à aujourd'hui, vous allez recevoir en 2010 une somme de 209'028'794 francs. Quel était le placement de votre ancêtre ?

7.2.4 On place un capital de 100'000 francs à un taux de 12%. Quelle somme aura-t-on selon la pratique bancaire après 6 ans et 3 mois si la capitalisation est annuelle ? semestrielle ? trimestrielle ?

7.2.5 A quel taux nominal capitalisé semestriellement a-t-on placé un capital de 100'000 francs si l'on obtient un capital de 166'817.25 francs après 8 ans ?

7.2.6 Combien de temps faut-il placer un capital initial de 12'000 francs à un taux nominal de 8% capitalisé semestriellement pour obtenir 527'272.09 francs selon la pratique bancaire ?

7.2.7 Un capital C_0 est placé à 6% l'an. Après combien d'années entières a-t-il triplé ? a-t-il été multiplié par dix ?
Démontrer que le temps nécessaire pour centupler le capital est le double du temps nécessaire à le décupler.

7.2.8 Quel est le taux d'intérêt annuel d'un capital qui double en dix ans si la capitalisation est annuelle ? Et si la capitalisation est semestrielle ?

7.3 Annuités

7.3.1 Trouver la valeur future et la valeur actuelle d'un placement constitué de huit versements annuels de 1'500 francs chacun, sachant que le taux d'intérêt est de 8% capitalisé annuellement. Expliquer ce que représentent la valeur future et la valeur actuelle, comparativement au montant total placé par versements.

7.3.2 Quelle est la valeur du capital constitué par des versements mensuels de 100 francs pendant quinze ans à un taux de 7.5% capitalisé mensuellement ? Quel est le gain en intérêts ?

7.3.3 Quels versements trimestriels devrez-vous effectuer pour constituer un capital de 10'000 francs en dix ans, le taux étant de 8% capitalisé trimestriellement ? Quel est le gain en intérêts ?

7.3.4 Vous devez préparer le contrat de deux clients empruntant chacun 2'000 francs. L'un désire rembourser en deux ans et l'autre en quatre ans. Le taux pour les prêts personnels est de 12% capitalisé mensuellement. Quels sont les versements mensuels que chacun doit effectuer et quel est le coût en intérêts de ces prêts ?

7.3.5 M. Dubois veut s'offrir un objet d'art d'une valeur de 10'000.- francs dans 15 ans. Pour préparer cet achat, il place dès aujourd'hui 500.- francs à 3% au début de chacune de ces 15 années. Quel versement complémentaire devra-t-il effectuer dans 15 ans pour atteindre la somme désirée ? Et si les 16 versements devaient être égaux, que vaudrait chacun d'eux ?

7.3.6 Vous versez 100 francs par mois pour rembourser une dette. Le taux est de 14.4% capitalisé mensuellement. Déterminer la valeur actuelle de la dette s'il vous reste quatre ans pour la rembourser.

7.3.7 Vous achetez une automobile de 13'500 francs en versant 3'500 francs comptant. Vous empruntez le reste à 12% capitalisé mensuellement, que vous devez rembourser en cinq ans. Quels sont les versements mensuels et le coût de cet emprunt ?

7.3.8 Vous remboursez actuellement un emprunt par des versements mensuels de 80 francs. Il vous reste dix ans pour rembourser le tout et vous désirez augmenter le montant des annuités afin de vous acquitter de la dette en cinq ans. Quels seront les nouveaux versements sachant que le taux est de 12% capitalisé mensuellement ?

7.3.9 Vous placez 30 francs par semaine à un taux de 7.8% capitalisé annuellement. Dans combien de temps aurez-vous accumulé le montant de 10'000 francs ?

7.3.10 Vous avez emprunté 50'000.- au taux de 5% que vous devez remboursez en en 15 annuités. A la fin de la 10ème année, vous convertissez votre emprunt au taux de 4%. L'annuité est alors recalculée. Calculer l'économie annuelle des 5 dernières années.

7.3.11 Vous avez effectué 10 versements annuels de 2'000.- francs, le premier il y a 17 ans ; le taux a été de 4% les 6 premières années et de 5% par la suite. De quelle somme disposerez-vous dans une année ?

7.3.12 M. Dupont décide de se constituer un 3ème pilier en versant 15 annuités de 1'000.- francs au taux de 5%. Il effectue son premier versement le 31 décembre 2000. Pour des raisons financières, M. Dupont est dans l'incapacité de verser les 6ème et 7ème annuités.
De quelle somme disposera-t-il une année après son dernier versement, sachant que le taux a augmenté de 1% le 1er janvier 2011.

7.3.13 M. Durand emprunte 40'000.- francs aujourd'hui au taux de 6.5%. Son contrat prévoit qu'il remboursera sa dette par annuité fixe en 13 ans, mais en effectuant le 1er versement dans 3 ans seulement.

a) Déterminer le solde de la dette au début de la 12^{e} année, comptée à partir d'aujourd'hui.
b) Déterminer le montant du 7ème amortissement.
c) Déterminer la valeur de l'intérêt de la dette lors du versement de la 10ème annuité

7.3.14 M. Dupré emprunte une certaine somme au taux de 6% qu'il doit rembourser par des annuités de 10'000.- pendant 15 ans. Au début de la 11ème année, il convertit son emprunt.

a) A quel taux doit-il le faire pour réaliser une économie annuelle de conversion de 270.50 francs ?
b) Quelle est la somme empruntée ?

7.3.15 On considère une capitalisation en 8 annuités de 200.- chacune. Calculer le taux sachant que la valeur actuelle de cette capitalisation est 1'412.- francs.

7.3.16 Madame Béa a actuellement une dette de 10'000.- francs que son banquier lui propose de rembourser en versant aujourd'hui 5'000.- francs, puis 1'000.- à la fin de chacune des 6 prochaines années. Quel est le taux d'intérêt ?

7.3.17 Aujourd'hui, Pierre prête 10'000.- francs à Jean en demandant d'être remboursé par 10 annuités de 1'323.77. Au fur et à mesure des versements, Pierre place les annuités reçues de Jean sur un livret d'épargne à 3.5%. À quel taux Pierre aurait-il dû placer les 10'000.- francs pour obtenir après 10 ans le même montant que celui se trouvant sur le livret d'épargne ?

7.3.18 On place 1'000.- au début de chaque semestre. Les intérêts étant calculés semestriellement au taux annuel de 5%, calculer la valeur cumulée 6 mois après le 21^{e} versement.

7.3.19 M. Young s'est engagé à payer 1'000.- au début de chaque année, en tout 20 fois. II décède après avoir payé 6 annuités. Ses héritiers proposent de se libérer des autres versements par le paiement d'un solde, à déterminer à l'échéance de la 7^{e} annuité. Le créancier est d'accord. (Taux 3%)

7.3.20 Calculer la valeur cumulée d'une rente (de capitalisation) de 30 annuités de 1'000.-, 6 ans après l'échéance de la dernière annuité. Le taux, d'abord de 4.5%, a passé à 4% au début de la 9^{e} période, puis à 3.5% au début de la 21^{e} période.

7.3.21 On veut créer un fond de 10'000.- par une rente (de capitalisation) dont chaque annuité se monte à 1'000.-. Calculer le montant dont il faudra majorer la dernière annuité pour arriver à la création du fonds projeté. (Taux 3%)

7.3.22 Quelle somme peut-on emprunter aujourd'hui sous garantie de versements (de fin de période) de 15 annuités de 1'000.-. (Taux 3.5%)
Et si la première annuité est payable seulement dans 4 ans (il y a toujours 15 annuités) ?

7.3.23 Un particulier doit payer 10'000.- dans 12 ans. Quelles sont les annuités de fin de période qui régleraient sa dette en 12 ans. (Taux 4%)

7.3.24 M. Xeros doit payer 10'000.- dans 15 ans. Pour préparer ce versement, il place dès aujourd'hui 500.- au début de chacune de ces 15 années, à 3%. Quel versement complémentaire devra-t-il faire dans 15 ans ? Et si les 16 versements sont égaux, que vaut chacun d'eux ?

7.3.25 On affiche un taux nominal de 6% capitalisé mensuellement. Calculer le taux périodique équivalent pour des versements mensuels.

7.3.26 On affiche un taux nominal de 9% capitalisé semestriellement. Calculer le taux périodique équivalent pour des versements bimensuels.

7.3.27 On affiche un taux nominal de 9% capitalisé mensuellement. Calculer le taux périodique équivalent pour des versements trimestriels.

7.3.28 On affiche un taux nominal de 9% capitalisé six fois par années. Calculer le taux périodique équivalent pour des versements trimestriels.

7.3.29 Vous empruntez 6'000 francs au taux de 12% capitalisé trimestriellement. Quelles sont les mensualités à verser pour s'acquitter de cette dette en trois ans ? Quel sera le coût en intérêts ?

7.3.30 Quelle est la valeur cumulée et la valeur actuelle d'une suite de remboursement de 75 francs par mois au taux nominal de 9% capitalisé semestriellement, sachant que la durée du contrat est de trois ans ?

7.3.31 Vous placez 100 francs par mois à un taux de 7.5% capitalisé trimestriellement pour constituer un capital pour votre retraite dans 25 ans. Quel sera alors le montant accumulé ? Quel sera le gain en intérêts ?

7.3.32 Vous effectuez un emprunt de 40'000 francs pour vingt ans afin d'acheter une nouvelle machine pour votre usine. Le taux est de 9% capitalisé trimestriellement.

a) Quelles seront les mensualités ?

b) Quelle sera la valeur actuelle après un an ?

c) Quel aura alors été le montant de l'amortissement ?

d) Lors du renouvellement de votre emprunt après un an, le taux est de 15%. Quels seront les versements mensuels que vous devrez effectuer au cours de la deuxième année ?

7.3.33 Quel capital peut-on constituer en dix ans en effectuant des versements mensuels de 200 francs à un taux de 9% capitalisé trimestriellement ? Quel est le gain en intérêts ?

7.3.34 Votre entreprise rembourse actuellement un emprunt en versant 3'500 francs tous les deux mois. On vous demande d'établir le montant qu'il faudrait verser pour liquider cette dette. Le taux d'intérêt est de 13% capitalisé trimestriellement et il reste vingt-deux versements à effectuer.

7.3.35 A l'achat de votre maison vous prenez une hypothèque de 50'000 francs à un taux de 9% capitalisé semestriellement.

a) Votre hypothèque étant de vingt ans, calculer les mensualités à verser ?
b) Quel est le montant de l'amortissement après un an et quel sera le montant versé en intérêts durant cette année ?
c) Si le taux demeure constant, quel est le montant total que vous verserez pour rembourser cette hypothèque ?
d) Si le taux grimpe à 16% après la première année, quels seront les versements que vous devrez effectuer au cours de la deuxième année ?
e) Quel sera le montant de l'amortissement durant la deuxième année et quel sera le montant versé en intérêts durant cette deuxième année ?
f) Si le taux demeure à 16% durant les dix-neuf dernières années, quel sera le montant total que vous aurez versé pour vous acquitter de votre hypothèque ?

7.3.36 Vous désirez accumuler 20'000 francs pour acheter un piano. Pour ce faire, vous placez 150 francs par mois au taux mensuel de 1%. Combien de versements seront nécessaires pour atteindre votre objectif ?

7.3.37 Un fumeur décide d'arrêter de fumer et de placer l'argent économisé pour accumuler un fond de retraite. S'il arrête de fumer à 40 ans alors qu'il fumait un paquet par jour au prix de 4 francs et que le prix du paquet reste le même, déterminer le montant qu'il aura accumulé à 65 ans en plaçant les 120 francs d'économies mensuelles à un taux mensuel de 0.9%.

7.4 Solutions des exercices

7.1.1 –

7.1.2

4950.50 francs

7.1.3

4%

7.1.4

237 jours

7.1.5

18.75 francs

7.1.6

26'106.67 francs

7.1.7

12'292.50 francs

7.2.1

$$C_0 = \frac{C_n}{1 + i \cdot n} \quad ; \quad i = \frac{C_n - C_0}{n \cdot C_0} = \frac{I}{n \cdot C_0} \quad ; \quad n = \frac{C_n - C_0}{i \cdot C_0} = \frac{I}{i \cdot C_0}$$

7.2.2

12'915.48 francs, 16'680.96 francs, 10'262.50 francs, 18'171.20 francs

7.2.3

1 centime

7.2.4

203'303.74 francs, 207'256.24 francs, 209'377.79 francs

7.2.5

(6.5% , 2)

7.2.6

48 ans, 2 mois et 20 jours

7.2.7

19 ans   40 ans

7.2.8

7.18%,   7.05%

7.3.1

$VC_d = 17'231.34$ francs et $VA_d = 9'309.56$ francs

7.3.2

$VC_d = 33'318.17$ francs, gain de $15'318.17$ francs

7.3.3

$A = 162.31$ francs, gain de $3'507.60$ francs

7.3.4

En deux ans $A = 94.15$ francs, coût de 259.60 francs, en quatre ans $A = 52.67$ francs, coût de 528.16 francs

7.3.5

$A = 421.55$ francs et 496.10 francs

7.3.6

$VA_f = 3'632.72$ francs

7.3.7

$A = 222.44$ francs, coût de $3'346.40$ francs.

7.3.8

$VA_f = 5'576.04.44$ francs, $A = 124.04$ francs

7.3.9

272 semaines, soit 5 ans et 12 semaines

7.3.10

$A_1 = 4'817.10$ et $A_2 = 4'684.71$. Économie annuelle $= 132.39$ francs

7.3.11

$38'149.53$ francs

7.3.12

$20'314.41$ francs

7.3.13

a) $10'742.55$ francs b) $4'306.64$ francs c) 698.27 francs

7.3.14

a) 5% b) $97'122.50$ francs

7.3.15

3.75%

7.3.16

5.5%

7.3.17

4.5%

7.3.18

27’862.85

7.3.19

11’634.95

7.3.20

66’893.37

7.3.21

816.40

7.3.22

11'517.40 10'388.05

7.3.23

665.50

7.3.24

421.55 et 496.10

7.3.25

0.5%

7.3.26

0.3675%

7.3.27

2.267%

7.3.28

2.258%

7.3.29

$A = 198.95$ francs, coût de 1'162.20 francs

7.3.30

$VC_f = 3'078.78$ francs, $VA_f = 2'364.19$ francs

7.3.31

$VC_d = 87'611.10$ francs, gains de 57'611.10 francs

7.3.32

a) $A = 358.16$ francs b) 39'244.36 francs (il restera 228 versements à effectuer)

c) 755.64 francs d) $A = 516.10$

7.3.33

$VC_d = 38'843.18$ francs, gains de 14'843.18 francs

7.3.34

$VA_f = 60'809.43$ francs

7.3.35

a) $A = 444.59$ francs b) amortissement de 955.36 francs, intérêts de 4'379.72 francs
c) 106'701.60 francs d) $A = 669.09$
e) amortissement de 462.66 francs, intérêts de 7'566.42 francs f) 157'887.60 francs

7.3.36

85 versements

7.3.37

184'325.48 francs