Aix*Marseille université

Domaine Sciences et Technologies
Portail 1 René Descartes

Introduction à l'informatique : TD 1

Code UE : S14IN1I1

Année 2022–2023

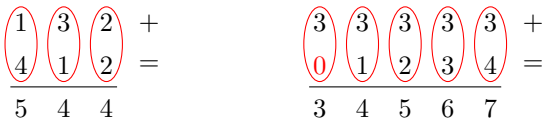
Algorithmes non formalisés

Exercice 1 (Arithmétique de l'école primaire) Dans cet exercice on analysera l'algorithme pour la somme d'entiers naturels qu'on connaît de l'école primaire.

L'algorithme pour la somme est défini, en premier lieu, sur la base d'un opération élémentaire qui est la somme d'entiers à un chiffre ($1+5$, $7+9$, etc.), pour laquelle on apprend par cœur tous les possibles résultats (qui peuvent être d'un ou deux chiffres). Quand l'un des deux nombres a moins de chiffres que l'autre, on le prolongera (à gauche) avec des zéros pour que les deux aient la même longueur.

1. Appliquez cet algorithme pour calculer les sommes $132 + 412$ et $33333 + 1234$. Combien d'opérations élémentaires on effectue dans les deux cas ?

   Solution : Dans le premier cas on exécute 3 opérations élémentaires, et dans le deuxième 5 (y compris une somme avec un zéro implicite). Chaque somme élémentaire correspond à un ovale dans le diagramme suivant :

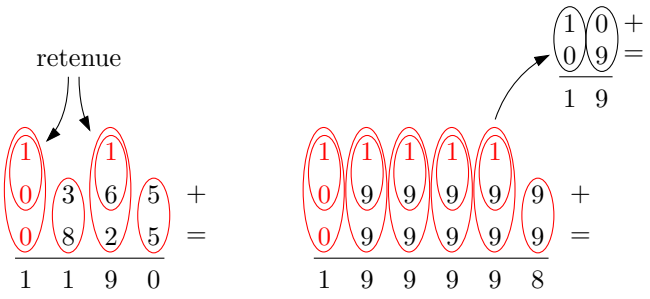
   

2. Combien d'opérations élémentaires on effectue pour calculer la somme de deux entiers naturels dont le plus grand a n chiffres, sous l'hypothèse qu'il n'y ait jamais de retenue ?

   Solution : Il faut exécuter n sommes élémentaires, en incluant celles avec des zéros implicites.

3. Appliquez maintenant l'algorithme pour calculer les sommes $365 + 825$ et $99999 + 99999$. Combien d'opérations élémentaires on exécute dans les deux cas ? (Pour rappel : la seule opération élémentaire admise est la somme de deux entiers d'un chiffre.)

   Solution : Pour la première somme, il s'agit de 6 sommes élémentaires. Dans le deuxième cas, on aura 2 sommes élémentaires pour la première colonne ($1 + 0$, puis $1 + 0$), 1 somme élémentaire ($9 + 9$) pour la dernière et 3 sommes élémentaires pour chacune des 4 colonnes du milieu (1 somme élémentaire pour calculer $1 + 9 = 10$ et 2 sommes élémentaires pour calculer $10 + 9$). En total, cela donne $2 + 3 \times 4 + 1 = 15$ sommes élémentaires.

4. Combien d'opérations élémentaires doit-on effectuer pour calculer la somme de deux entiers naturels quelconques de n chiffres chacun ? Donnez la réponse à cette question dans le meilleur et dans le pire cas, en précisant en quoi consiste ces cas.

Solution : Le meilleur cas est quand on somme deux entiers dont au moins l'un des deux est de n chiffres où aucune opération d'addition ne lève de retenue. Dans ce cas, la somme nécessite n sommes élémentaires.

Le pire des cas est quand on somme deux entiers de n chiffres où chaque chiffre est 9. Dans ce cas, on obtient le plus de retenues possibles ce qui demande, en généralisant la réponse précédente, d'exécuter $2 + 3(n-1) + 1 = 3n$ sommes élémentaires.

Exercice 2 (Chiffrement de César) La cryptologie (étym. science du secret) est un domaine à la frontière des mathématiques et de l'informatique. Elle se sépare en deux pans de même importance. Le premier consiste à transformer une information afin de la rendre secrète, autrement dit à la "crypter" ou "chiffrer". Il s'agit de la *cryptographie* (étym. écriture secrète). Le second consiste à analyser les informations cryptées et trouver des méthodes et techniques afin d'en dévoiler le sens caché. Il s'agit de la *cryptanalyse*.

Historiquement, un procédé de cryptographie bien connu est le *codage de César* que Jules César utilisait dans ses correspondances. Le principe de chiffrement est simple. Étant donné un alphabet (ici, nous utiliserons l'alphabet latin) et un message, le message chiffré s'obtient en remplaçant chacune des lettres du message d'origine par une lettre à distance fixe toujours dans la même direction. Pour les dernières lettres, dans le cas d'une distance à droite, on reprend au début de l'alphabet. Il s'agit d'un chiffrement par décalage. À titre d'exemple, avec un décalage de 5, 'a' devient 'f', 'b' devient 'g', ..., 'y' devient 'd' et 'z' devient 'e'.

1. Soit le message "La vie est un long fleuve tranquille". Donnez ses représentations chiffrées selon le codage de César avec les clés 3 et -7.

   Solution :
   — Pour la clé 3, 'a' se tranforme en 'd', on peut écrire la table de transformation suivante :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

   Le message chiffré est donc : "Od ylh hvw xq orqj iohxyh wudqtxlooh.".
   — Pour la clé -7, 'a' se transforme en 't', on peut écrire la table de transformation suivante :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

   Le message chiffré est donc : "Et obx xlm ng ehgz yexnox mktgjnbeex."

2. En utilisant des phrases en langage naturel (en français, dans notre cas), donnez une description la plus précise possible de l'algorithme de chiffrement utilisé pour le codage de César.

   Solution : Quel que soit le message à chiffrer, une donnée indispensable est la clé d. Considérons maintenant un message m. Pour chacun des caractères c (numérotés de 0 à 25 tel que $a \equiv 0$, $b \equiv 1$, ..., $z \equiv 25$) composant m, c peut être soit une lettre de l'alphabet latin, soit un autre caractère (espacement, ponctuation). Si c est une lettre, on le transforme dans le message chiffré en la lettre $c + d \mod 26$, en respectant sa casse. Si c n'est pas une lettre, on le laisse tel quel.

3. Quelle est la complexité de l'algorithme de chiffrement de César ? On demande de compter le nombre d'opérations de décalage effectuées par l'algorithme en fonction du nombre n de caractères d'un message donné.

   Solution : Chaque caractère du message est décale une fois, ce qui donne un nombre total de n opérations.

4. Proposez un algorithme de déchiffrement, prenant en entrée le message chiffré et une clé et renvoyant le message décodé. À titre d'exemple, déchiffrez le message « kajex »sachant que la clé de chiffrement vaut 9.

Solution : On peut utiliser le même algorithme que précédemment en ne changeant que le calcul $c + d \mod 26$ en $c - d \mod 26$. En effet, décoder avec la clé d, c'est pareil que coder avec la clé $-d$. Le message à déchiffrer est « bravo ».

5. Admettons que quelqu'un vous envoie un message chiffré en vous spécifiant qu'il s'agit d'un codage de César mais sans vous donner la clé. Est-il possible de le déchiffrer ? Si oui, comment et est-ce efficace, en termes de temps ?

Solution : Sachant que l'alphabet latin contient 26 lettres, il existe théoriquement 26 décalages à droite (resp. à gauche) possibles, parmi lesquels 25 seulement sont effectifs. En effet, la clé $0 \equiv 26 \mod 26$ (resp. $0 \equiv -26 \mod 26$) renvoie le message d'origine. Donc, en tout, il existe 50 clés dont 25 seulement sont effectives puisque toute clé négative $-d$ est équivalente à la clé positive $26 - d$.
Considérons maintenant un mot chiffré (effectivement). Pour le déchiffrer, il suffit d'itérer l'algorithme de déchiffrement précédent sur les 25 clés effectives. En termes de complexité, cet algorithme demande $25n$ opérations de décalage, où n est la longueur du message.

6. Plus généralement, un tel codage est-il utilisable en pratique ? Autrement dit, est-il efficace en termes de sécurité du secret dans le cas général (imaginez que vous recevez un message chiffré et que vous ne savez pas si c'est le codage de César qui a été utilisé par l'émetteur) ?

Solution : Admettons que l'on reçoit un message chiffré sans connaître le type de codage utilisé. L'objectif est double :

(a) savoir si l'on est capable de reconnaître si le chiffrement est un code César ;

(b) et si tel est le cas et qu'on a reconnu que le chiffrement utilisé était bien un code César, déchiffrer le mot.

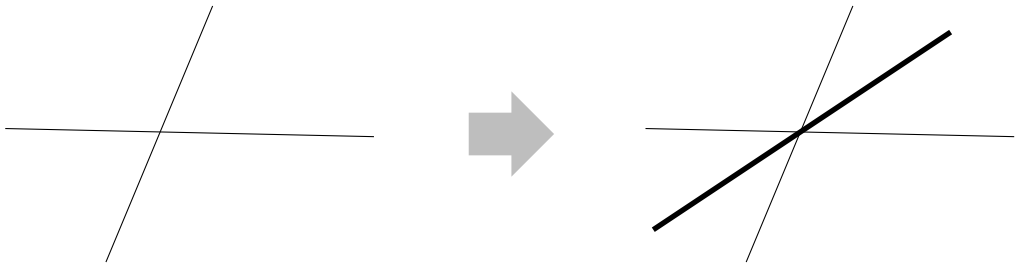
Notons déjà que l'item (b) a été traité à la question précédente.
Pour ce qui est de l'item (a), une bonne technique est d'utiliser l'analyse fréquentielle, sous réserve que l'émetteur a quand même précisé la langue dans laquelle est écrite le message d'origine. En effet, dans une langue (Français, Anglais...), certaines lettres apparaissent plus fréquemment que d'autres. Par exemple, la fréquence d'apparition des lettres dans le corpus 2008 de Wikipedia en Français suit la distribution suivante (en pourcentage par ordre décroissant) :

e	a	i	s	n	r	t	o	l	u	d	c	m
12,10	7,11	6,59	6,51	6,39	6,07	5,92	5,02	4,96	4,49	3,67	3,18	2,62
p	g	b	v	h	f	q	y	x	j	k	w	z
2,49	1,23	1,14	1,11	1,11	1,11	0,65	0,46	0,38	0,34	0,29	0,17	0,15

Or, tout codage de César ne fait que décaler ce type de distribution, ce qui rend aisé son "cassage".

Exercice 3 (Constructions à la règle et au compas) Un autre type d'algorithme, qu'on connaît normalement du collège, sont les constructions à la règle et au compas. On peut tracer des cercles en plantant le compas sur un point connu, soit avec n'importe quelle ouverture, soit en pointant la mine sur un autre point connu. On utilise la règle pour tracer un segment de droite qui passe par deux points connus ou, en alternative, un segment qui passe par un point connu. Nos opérations élémentaires ici sont tracer un cercle et tracer un segment.

1. Étant donné deux (segments de) droites s'intersectant en un point, et une paire d'angles opposés issue de cette intersection, comment construit-on à la règle et au compas la droite bissectrice de cette paire d'angles (comme dans le dessin qui suit) ? Combien d'opérations cela demande-t-il ?



Solution :

— On plante le compas dans l'intersection A des deux droites, avec n'importe quelle ouverture (non-nulle, mais qu'on pourra conserver tout au long du processus de tracé) et on trace le cercle correspondant. Cela identifie deux points B et C d'intersection sur les deux droites.

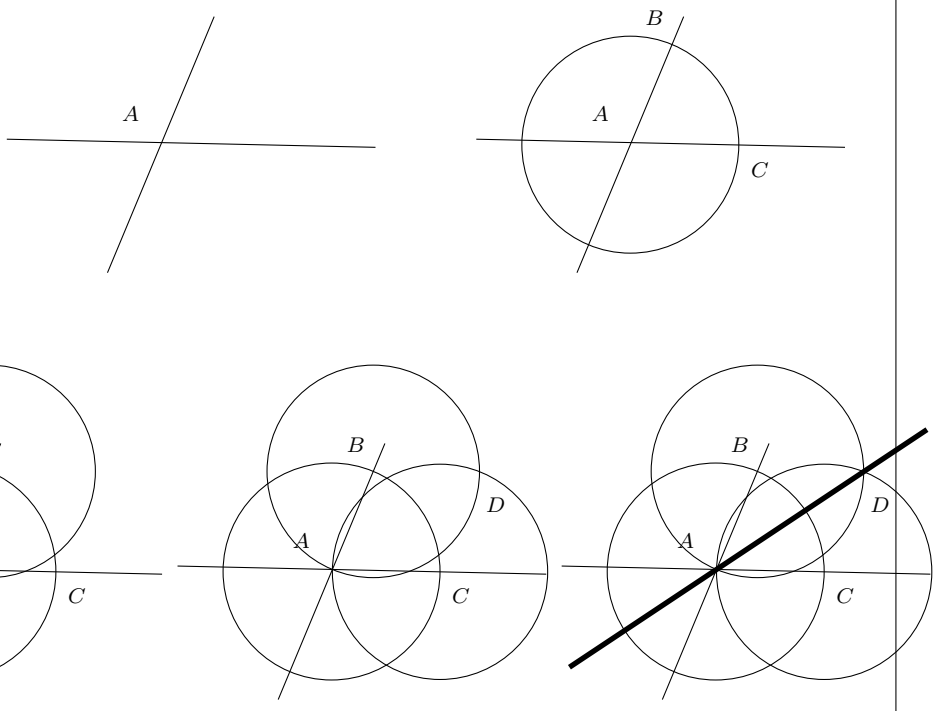
— On plante le compas dans B avec ouverture $AB = AC$ et on trace le cercle correspondant.

— On plante le compas dans C avec ouverture $AB = AC$ et on trace le cercle correspondant.

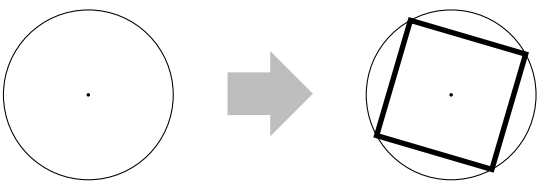
— Ces deux nouveaux cercles centrés sur B et C s'intersectent en un point, nommé D.

— Avec la règle on trace la droite passant par A et D. Il s'agit de la bissectrice demandée.

En total, cela demande donc 4 opérations élémentaires.



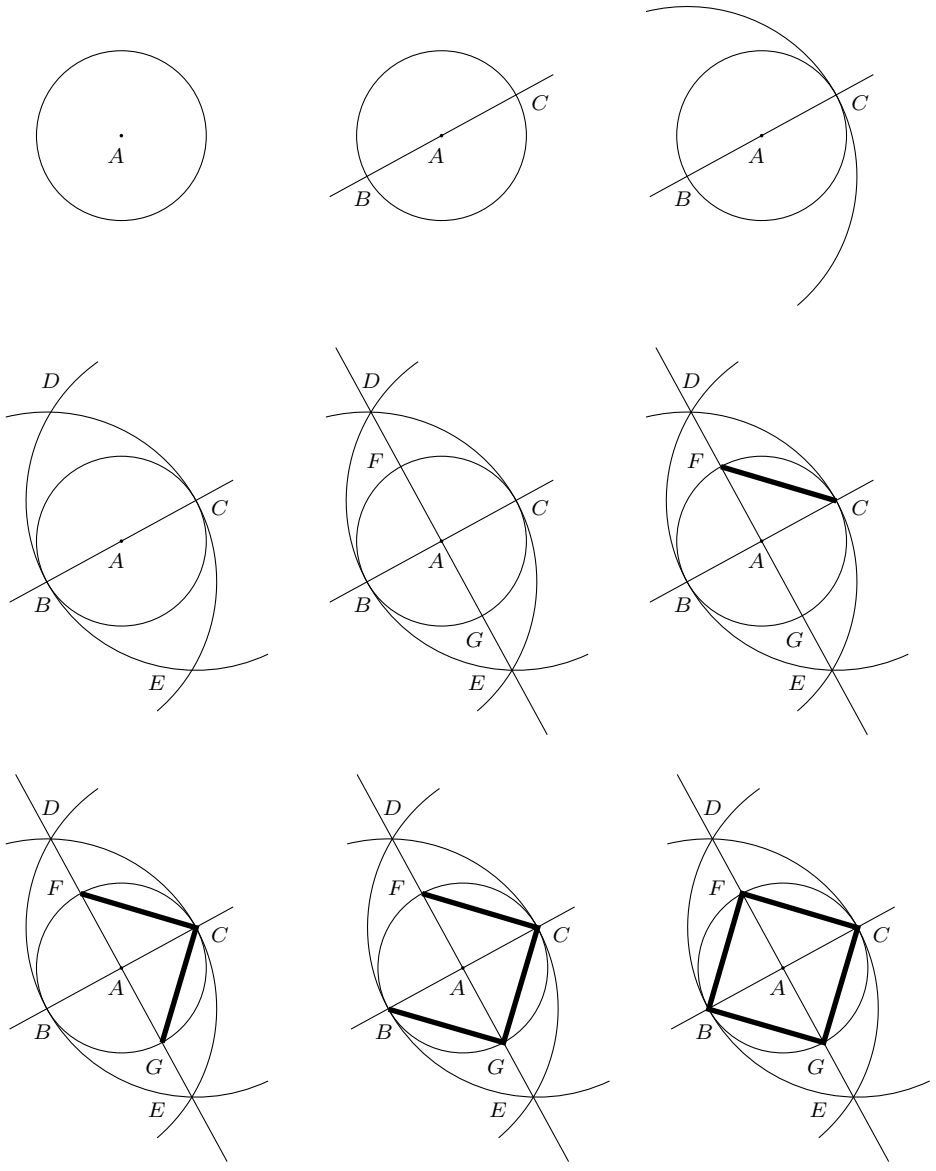
2. À partir d'un cercle donné (y compris son centre), dessinez un carré régulier ayant les quatre sommets sur le cercle. Combien d'opérations exécute-t-on pour réaliser cette construction ?



Solution :

— On dessine n'importe quel segment passant par le centre A du cercle ; cela identifie deux points B et C sur le cercle.
— On plante le compas en B avec ouverture BC et on dessine le cercle correspondant.
— On plante le compas en C avec ouverture CB et on dessine le cercle correspondant, ce qui identifie les points D et E.
— On trace le segment passant par D et E, ce qui identifie les points F et G sur le cercle.
— On trace les quatre segments FC, CG, GB, BF qui constituent les quatre côtés du carré demandé.

En total, cela demande 8 opérations élémentaires.



3. À partir des deux constructions des questions précédentes, comment peut-on construire, à partir d'un cercle donné (y compris son centre), le polygone régulier ayant 2^n sommets sur le cercle (un 2^n-gone) ? Combien d'opérations on exécute en fonction de n ?

Solution :

— Avec 4 opérations on peut trouver, comme dans la question précédente, les segments perpendiculaires BC et FG qui passent par le centre du cercle (et identifient les 4 sommets d'un carré régulier).

— À partir de cela, on construit de façon répétée les bissectrices de tous les angles au centre du cercle, ce qui double à chaque itération le nombre de sommets du polygone. Comme chaque bissectrice permet d'identifier 2 nouveaux sommets, pour passer de 4 à 2^n sommets il faut répéter la construction de la bissectrice $(2^n - 4)/2 = 2^{n-1} - 2$ fois, ce qui demande $3 \times (2^{n-1} - 2)$ opérations.

— Il faut enfin tracer les 2^n côtés, ce qui demande 2^n opérations avec la règle.

En total, on exécute donc $4 + 3 \times (2^{n-1} - 2) + 2^n$ opérations.