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 ?
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 ?
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.)
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.

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.
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.
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.

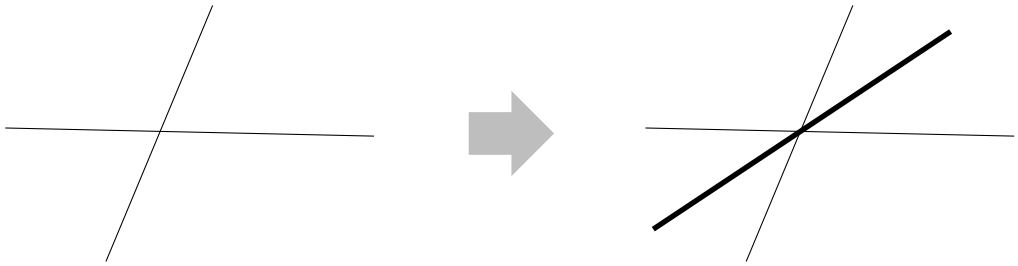
4. Proposez un algorithme de déchiffrement, prenant en entrée le message chiffré et une clé et renvoyant le message décodé. À titre d'exemple, déchiffrez le message « kajex »sachant que la clé de chiffrement vaut 9.

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 ?

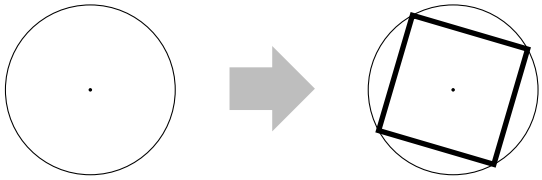
6. Plus généralement, un tel codage est-il utilisable en pratique ? Autrement dit, est-il efficace en termes de sécurité du secret dans le cas général (imaginez que vous recevez un message chiffré et que vous ne savez pas si c'est le codage de César qui a été utilisé par l'émetteur) ?

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 ?



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 ?



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 ?