MEDIAN

Tous documents (sauf livres) et calculatrices autorisés. Les résultats intermédiaires non démontrés pourront être utilisés tout au long du devoir. Le barème prendra en compte la longueur du sujet.

Exercice 1 Multiplication d'entiers...

L'algorithme 1 qui suit est appelé algorithme de multiplication *à la russe* et est une variante d'une technique connue depuis l'Egypte antique [1]. Les données d'entrée x et y sont des entiers naturels.

Algorithme 1

Function $mult(x, y)$
$r := 0$
while $x \neq 0$ **do**
  if x est impair **then**
    $r := r + y$
    $x := x - 1$
  end if
  $x := x/2$
  $y := y \times 2$
end while
Return r

1. Appliquer l'algorithme et effectuer $mult(132, 45)$. Vous ferez apparaître vos résultats dans une table à trois colonnes, selon l'exemple suivant, où chaque ligne représente les valeurs x, y et r après chaque passage en boucle. La première ligne étant formée des valeurs initiales.

	x	y	r
Avant entrée en boucle	132	45	0
1er passage en boucle	...	...	...
⋮	⋮	⋮	⋮

2. Justifier que l'algorithme est convergent.
3. Que calcule cet algorithme ?
4. On note $x_0 = x$, $y_0 = y$ et $r_0 = 0$, puis x_n, y_n et r_n les valeurs de x, y et r après le n-ème passage en boucle.
   a. Montrer que la propriété $\mathscr{P}(n) : x_n y_n + r_n = xy$ est un invariant de boucle.
   b. Prouver que l'algorithme réalise bien ce pour quoi il a été conçu.
5. Quelles sont les deux opérations arithmétiques élémentaires utilisées par l'algorithme ? Quel peut-être l'intérêt si on utilise cet algorithme avec une machine calculant en binaire (par exemple un ordinateur) ?

1. On peut trouver explicitement cette technique de calcul sur le papyrus de Rhind datant du XVI$^{\text{ème}}$ siècle avant notre ère. Ce payrus regroupe 87 problèmes résolus d'arithmétique, d'algèbre de géométrie et d'arpentage vieux de 4000 ans. Cette méthode de calcul est un algorithme ce qui permet de replacer l'informatique dans un contexte historique non limité au XX$^{\text{ème}}$ et XXI$^{\text{ème}}$ siècles.

6. Pour tout $x \in \mathbb{R}_+$ on rappelle que $\log_2(x) = \dfrac{\ln(x)}{\ln(2)}$. Soit $n \in \mathbb{N}$ tel que $2^n \leqslant x < 2^{n+1}$, en déduire que $n \leqslant \log_2(x) < n+1$. Comment peut-on évaluer le nombre de passages en boucle nécessaires pour effectuer $mul(x,y)$?

7. Effectuer $mult(45,132)$ et comparer avec la question **1**. Est-ce cohérant avec la question **6** ?

8. Complément : donner une version récursive de l'agorithme 1.

Exercice 2 Le système formel MIU

Dans cet exercice on considère l'alphabet $A = \{M, I, U\}$. On note A^* l'ensemble de tous les mots possibles sur l'alphabet A^*. Le sous-ensemble MIU (on dit aussi le langage MIU [2]) de A^* est défini par induction de la manière suivante :

MIU $= \langle \mathscr{B}, \mathscr{R} \rangle$ avec
- $\mathscr{B}$: $MI \in \mathscr{B}$.
- $\mathscr{R}$:
  - R_1 : $xI \in$ MIU $\Rightarrow xIU \in$ MIU (x désigne une chaîne de caractères)
  - R_2 : $Mx \in$ MIU $\Rightarrow Mxx \in$ MIU (x désigne une chaîne de caractères)
  - R_3 : Dans $m \in$ MIU la chaîne de caractère III peut être remplacée par U.
  - R_4 : Dans un mot $m \in$ MIU la chaîne de caractère UU peut être supprimée.

1. Déterminer un arbre de dérivation du mot MUIIU.

2. Montrer que le schéma inductif est ambigü.

3. Démontrer par induction que si $m \in$ MIU, le nombre de I dans l'écriture de m ne peut pas être un multiple de 3.

4. En déduire que $MU \notin$ MIU.

5. On considère la variante de MIU, notée $\overline{\text{MIU}}$ où seules les règles R_1 et R_2 s'appliquent. Montrer qu'il existe un algorithme simple permettant de prouver qu'un mot composé de k lettres appartient ou n'appartient pas à $\overline{\text{MIU}}$ (indication : on raisonnera sur la longueur du mot à chercher). Un tel langage est dit *décidable*. D'après vous le langage MIU est-il décidable ?

Exercice 3 Fonctions inductives

On considère le sous-ensemble $\mathscr{M} \subset \mathbb{N}$ défini par induction par le schéma suivant :

$\mathscr{M} = \langle \mathscr{B}, \mathscr{R} \rangle$
- $\mathscr{B} : 1 \in \mathscr{B}$
- $\mathscr{R}$:
  - $R_1 : m \in \mathscr{M} \Rightarrow 2m \in \mathscr{M}$
  - $R_2 : m \in \mathscr{M} \Rightarrow 3m \in \mathscr{M}$

Soit $A = \{x \in \mathbb{N}^*, x = 2^p 3^q, p, q \in \mathbb{N}\}$

1. Montrer que $A = \mathscr{M}$.

2. On définit f par induction sur $\mathscr{M}$ (et donc sur A) de la manière suivante :
- $f : \mathscr{M} \to \mathbb{N}$
- $\mathscr{B} : f(1) = 0$
- $\mathscr{R}$:

2. D'après *Gödel, Escher and Bach : an Eternal Golden Braid* de Hofstader, R. Douglas. Ce système a été inventé par Hofstader pour donner un exemple simple de langage formel non décidable, c'est-à-dire un language qui ne peut pas toujours répondre par lui-même à la question suivante : «est-ce que m est un mot du langage ?».

- $R_1 : f(2m) = f(m) + 1$
- $R_2 : f(3m) = f(m) + 1$

a. Calculer $f(12)$ et $f(9)$.

b. A priori est-on sûr que f est bien une fonction ?

c. Démontrer par induction que $\forall m = 2^k 3^l \in \mathscr{M}$ avec $(k,l) \in \mathbb{N}^2$, on a $f(m) = k + l$. En déduire que f est bien une fonction.

d. Montrer que f est surjective. Est-elle injective ?

e. f est une surjection d'un sous-ensemble (strict) de $\mathbb{N}$ dans $\mathbb{N}$, est-ce étonnant ?

3. On considère sur $\mathscr{M}$ la relation $m_1 \mathscr{R} m_2 \Leftrightarrow |f(m_1) - f(m_2)| \leqslant 1$.

a. Montrer que $\mathscr{R}$ est réflexive et symétrique.

b. Montrer que $\mathscr{R}$ n'est pas une relation d'équivalence.

c. On considère la relation $\mathscr{R}'$, restriction de $\mathscr{R}$, au sous-ensemble $\mathscr{M}' = \{1,2,3,6\} \subset \mathscr{M}$. Écrire la matrice $M_{\mathscr{R}'}$ de la relation $\mathscr{R}'$.

d. Calculer $M^2_{\mathscr{R}'}$.

e. Complément : On considère $\phi : \mathscr{M} \to \mathbb{N}^2$ la bijection définie par $\phi(2^k 3^l) = (k,l)$ (on ne demande pas de vérifier qu'il s'agit bien d'une bijection). Déterminer une relation sur $\mathbb{N}^2$ qui traduise la relation $\mathscr{R}$ sur $\mathscr{M}$, c'est-à-dire, trouver la relation $\mathscr{S}$ telle que

$$m_1 \mathscr{R} m_2 \Leftrightarrow \phi(m_1) \mathscr{S} \phi(m_2) \tag{1}$$

En déduire une interpétation en terme de distance discrète sur $\mathbb{N}^2$ de la relation $\mathscr{S}$ (et donc de $\mathscr{R}$). Expliquer alors pourquoi le résultat **4.d** était prévisible sans calcul ?

Corrections

Exercice 1

1. Calcul de $mult(132,45)$.

	x	y	r
Avant entrée en boucle	132	45	0
1er passage en boucle	66	90	0
2ème passage en boucle	33	180	0
3ème passage en boucle	16	360	180
4ème passage en boucle	8	720	180
5ème passage en boucle	4	1440	180
6ème passage en boucle	2	2880	180
7ème passage en boucle	1	5760	180
8ème passage en boucle	0	11520	5940

2. La boucle *tant que* est considtionnée à la valeur de x_n (valeur de x après le n-ème passage en boucle). Or (x_n) est une suite d'entiers strictement décroissante, donc il existe un n tel que $x_n = 0$ entraînant la sortie de boucle et la fin de l'algorithme.

3. A priori cet algorithme calcule le produit xy.

4. **a.** La proritéé $\mathscr{P}(n)$ est bien un invariant de boucle. On le montre par récurrence :
- $\mathscr{P}(0)$ est vraie. En effet $x_0y_0 + r_0 = xy + 0 = xy$.
- On suppose $\mathscr{P}(n)$ vraie alors vérifions la propriété sur le passage en boucle suivant. Pour cela on calcule $x_{n+1}y_{n+1} + r_{n+1}$.
  - Si x_n est pair alors d'après l'algorithme on a

$$x_{n+1}y_{n+1} + r_{n+1} = \frac{x_n}{2} y_n \times 2 + r_n = x_n y_n + r_n \underbrace{=}_{HR} xy \tag{2}$$

Dans ce cas $\mathscr{P}(n+1)$ est vérifiée.
  - Si x_n est impair, alors d'après l'algorithme on a

$$x_{n+1}y_{n+1} + r_{n+1} = (x_n - 1)y_n + (r_n + y_n) = x_n y_n + r_n \underbrace{=}_{HR} xy \tag{3}$$

Dans ce cas également $\mathscr{P}(n+1)$ est vérifiée.

On a donc $\mathscr{P}(0)$ est vraie et $\mathscr{P}(n) \Rightarrow \mathscr{P}(n+1)$ donc la proriété $\mathscr{P}(n)$ est vraie après le n-ème passage en boucle.

b. On a vu que l'algorithme est convergent ce qui revient à dire qu'il existe N, valeur du dernier passage en boucle, tel que $x_N = 0$. Au cours dernier passage la propriété $\mathscr{P}(N)$ est encore vraie, c'est-à-dire $x_N y_N + r_N = xy$. Or $x_N = 0$ ce qui implique $r_N = xy$. Mais r_N est bien la valeur retournée par l'algorithme ce qui fournit le résultat voulu.

5. En plus de l'addition et la soustraction de la condition *If*, l'algorithme répète à chaque passage en boucle une division et une multiplication par 2. C'est deux opérations, lorsqu'on calcule sur des entiers codés en binaire sont très faciles à réaliser. Il s'agit pour la première d'un décallage vers la droite (suppression du dernier bit qui doit être nul par parité) ou d'un décallage vers la gauche (ajout d'un zéro).

6. De $2^n \leqslant x \leqslant 2^{n+1}$ on obtient par passage à ln (fonction croissante) $n \leqslant \log_2(x) < n+1$. Si on code x en binaire, la taille (nombre de bits utilisés) est de $n = [\log_2(x)]$. Or à chaque passage en boucle la taille de x diminue de 1 (division par 2). Il faut donc effectuer n passages en boucle pour que la valeur de x soit égale à $2^0 = 1$. Il faudra un passage supplémentaire pour obtenir $x = 0$. On peut donc conclure que le nombre de passage en boucle est :

$$\#\text{passages en boucles} = n+1 = [\log_2(x)]+1 \tag{4}$$

7. Pour la question **1**, on avait bien $8 = [\log_2(132)]+1$. Lorsqu'on refait les calculs en appelant $mult(45,132)$ on obtient également $6 = [\log_2(45)]+1$, ce qui confirme le nombre de passages en boucle. On a donc intérêt à appeler l'algorithme $mult(x,y)$ avec $x \leqslant y$.

8. Version récursive de l'algorithme de multiplication à la russe.

Algorithme 2

```
Function multR(x, y)
if x = 0 then
    return 0
end if
if x impair then
    multR(x − 1, y) + y
else
    multR(x/2, 2y)
end if
```

Exercice 2

1. $MI \to^{R_2} MII \to^{R_2} MIIII \to^{R_2} MIIIIIII \to^{R_3} MUIIII \to^{R_3} MUIIU$

2. Le schéma est ambigü.
- $MI \to^{R_1} MIU$
- $MI \to^{R_2} MII \to^{R_2} MIIII \to^{R_3} MIU$

3. Montrons par induction que $\forall m \in$ MIU le nombre de I n'est pas un multiple de 3. Notons $v_I(m)$ le nombre de I dans m.
- C'est vrai sur la base. $MI \in \mathscr{B}$ et $v_I(MI) = 1 \neq 3k$.
- Supposons $m \in$ MIU construit tel que $v_I(m) \neq 3k$. Cette dernière inégalité peut se traduire en $v_I(m) = 1+3k$ ou $v_I(m) = 2+3k'$. Considérons les éléments construits à partir de m en appliquant les règles $\mathscr{R}$. Pour cela on notera $R_i m$ le mot généré en appliquant R_i à m.
  - R_1 ne modifie pas le nombre de I donc $v_I(R_1 m) = v_I(m) \neq 3k$.
  - R_2 double la chaîne de caractère qui suit le M donc double le nombre de I. On en déduit que $v_I(R_2 m) = \begin{cases} v_I(R_2 m) = 2(1+3k) = 2+3k = 2[3] \\ v_I(R_2 m) = 2(2+3k') = 4+3k' = 1[3] \end{cases}$. Dans les deux cas on a bien $v_I(R_2 m) \neq 3k$.
  - R_3 supprime une chaîne de trois I consécutifs. Donc $v_I(R_3 m) = v_I(m) - 3 = \begin{cases} 1+3k-3 = 1[3] \\ 2+3k'-3 = 2[3] \end{cases}$. Ce qui donne bien $v_I(R_3 m) \neq 3k$.
  - R_4 ne change pas le nombre de I de m donc $v_I(R_4 m) = v_I(m) \neq 3k$.

La propriéé $v_I(m) \neq 0[3]$ est vraie sur la base et est stable par les règles donc elle est vraie pour tout $m \in$ MIU.

4. On a $v_I(MU) = 0[3]$ donc le nombre de I de MU est bien un multiple de 3. Or $v_I(m) \neq 0[3]$ pour tout $m \in$ MIU. On en déduit donc que $MU \notin$ MIU.

5. Si on considère $\overline{\text{MIU}}$ alors à chaque application des règles on augmente le nombre de caractères du mot. De plus la règle R_1 ne peut être appliquée qu'une seule fois. Ainsi un mot de $\overline{\text{MIU}}$ sera toujours composé soit de $1+2^n$ caractères (on applique n fois R_2) ou bien de $1+2^n+1 = 2^{n+1}$ caractères (on applique n fois R_2 et 1 fois R_1). Pour savoir si un mot m de longueur k appartient à $\overline{\text{MIU}}$ il suffit de calculer tous les mots de $\overline{\text{MIU}}$ de longueur k (avec $k = 1+2^n$ ou $k = 2^n$ sinon on peut dire que $m \notin \overline{\text{MIU}}$). Pour cela si $k = 1+2^n$ il n'y a qu'un mot possible $M\underbrace{I\ldots I}_{2^n \text{ fois}}$ et si $k = 2^{n+1}$ il y a $n+1$ mots possibles (ça dépend du moment où on applique R_2). Dans les deux cas il y a un nombre fini de mots et on peut donc facilement décrire une procédure pour répondre à la question.

Algorithme 3

Function $\overline{\text{MIU}}(m)$
Require: m un mot
Ensure: Répond à la question $m \in \overline{\text{MIU}}$?
  if $longueur(m) \neq 1+2^n$ ou $longueur(m) \neq 2^{n+1}$ **then** return NON
  end if
  if $longueur(m) = 1+2^n$ **then**
    if $m = M\underbrace{I\ldots I}_{2^n}$ **then** return OUI
    else return NON
    end if
  else
    for $i \leftarrow n+1$ **do**
      $m_i \leftarrow T_1(T_2(\ldots T_{n+1}MI)$ (avec $T_i = R_2$ et pour $j \neq i$, $T_j = R_1$).
      if $m = m_i$ **then** return OUI
      end if
    end for
    return NON
  end if

Le language $\overline{\text{MIU}}$ est donc décidable.

Par contre le language MIU ne l'est pas. Du fait des règles R_3 et R_4 il n'est pas possible de décrire un algorithme qui puisse énumérer de manière finie tous les mots d'une longueur donnée. Par exemple pour répondre à la question $MU \in \overline{\text{MIU}}$ il existe un nombre infini d'arbres de dérivation à tester si on veut répondre à la question en construisant tous les mots de longueur 2. C'est donc une question concernant le système MIU auquel le système ne peut répondre. Pour y répondre on a du faire un raisonnement en dehors du système en utilisant des propriétés arithmétiques.

Exercice 3

1. Montrons que $A = \{2^k 3^l, (k,l) \in \mathbb{N}^2\} = \mathscr{M}$.
- $\mathscr{M} \subset A$. Par induction :
  - C'est vrai pour la base $1 \in \mathscr{M}$ et $1 = 2^0 3^0 \in A$.
  - Supposons que $m \in \mathscr{M}$ tel que $m \in A$ et montrons que la propriété est stable par les règles. Puisque $m \in A$ on a $m = 2^k 3^l$. En appliquant R_1 il vient $R_1 m = 2m = 2^{k+1} 3^l \in A$ et en appliquant R_2 on a $R_2 m = 3m = 2^k 3^{l+1} \in A$.

  La base est contenue dans A et A stable par R_1 et R_2 donc $\mathscr{M} \subset A$.
- Réciproquement $A \subset \mathscr{M}$ se montre par raisonnement direct. Soit $a = 2^k 3^l \in A$, alors a s'obtient à partir de la base 1 en appliquant k fois R_1 et l fois R_2 comme le montre l'arbre de dérivation suivant : $1 \underbrace{\rightarrow^{R_1} 2 \rightarrow^{R_1} 4 \rightarrow \cdots \rightarrow^{R_1}}_{k \text{ fois}} 2^k \underbrace{\rightarrow^{R_2} 2^k 3 \rightarrow \cdots \rightarrow^{R_2}}_{l \text{ fois}} 2^k 3^l$

2. **a.** $f(12) = f(6)+1 = f(3)+1+1 = f(1)+1+1+1 = 0+3 = 3$ et $f(9) = f(3)+1 = f(1)+1+1 = 0+2 = 2$

b. A priori f n'est pas bien définie car le schéma est ambigü. Il faut donc vérifier que la valeur de f ne dépend pas de l'arbre de dérivation.

c. Montrons par induction que $\forall m = 2^k 3^l \in \mathscr{M} = A$ on a $f(m) = k + l$.
- C'est vrai pour la base puisque $f(1) = 0$ (par définition de f) et que $1 = 2^0 3^0$ donc $f(2^0 3^0) = 0 + 0$.
- Supposons que c'est vrai pour $m = 2^k 3^l$, c'est-à-dire supposons que $f(m) = k + l$ et montrons que la propriété est encore vraie pour $R_1 m$ et $R_2 m$. Par définition on a $f(R_1 m) = f(2m) \underbrace{=}_{\text{def de } f} f(m)+1 \underbrace{=}_{\text{hypothèse d'induction}} = k+l+1 = (k+1)+l$ Or $2m = 2^{k+1} 3^l$ la propriété est vérifiée. De même on a $f(R_2 m) = f(3m) \underbrace{=}_{\text{def de } f} f(m)+1 \underbrace{=}_{\text{hypothèse d'induction}} =$ $k + l + 1 = k + (l + 1)$ Or $3m = 2^k 3^{l+1}$ la propriété est également vérifiée.

  On a donc $f(2^k 3^l) = k + l$ est vraie pour la base et est stable par R_1 et R_2. On en déduit que la propriété est vraie pour tout $m \in \mathscr{M}$.

d. f est surjective. En effet soit $n \in$ Â $\mathbb{N}$ alors $m = 2^n 3^0$ vérifie bien $f(m) = n$. Par contre f n'est pas injective puisque $f(2) = f(3) = 1$.

e. Non ce n'est pas étonnant, la théorie des cardinaux montrent qu'on peut avoir un sous-ensemble de $\mathbb{N}$ strict en bijection avec $\mathbb{N}$.

3. **a.** La relation est réflexive $m_1 \mathscr{R} m_1 \Leftrightarrow |f(m_1) - f(m_1)| \leqslant 1$. Or $|f(m_1) - f(m_1)| = 0$ donc c'est vérifié. La relation est symétrique $m_1 \mathscr{R} m_2 \Leftrightarrow |f(m_1) - f(m_2)| \leqslant 1 \Leftrightarrow |f(m_2) - f(m_1)| \leqslant 1 \Leftrightarrow m_2 \mathscr{R} m_1$.

b. La relation n'est pas transitive. Exemple $m_1 = 2$, $m_2 = 6$ et $m_3 = 12$ on a $m_1 \mathscr{R} m_2$, $m_2 \mathscr{R} m_3$ mais m_1 n'est pas en relation avec m_3.

c. $M_{\mathscr{R}'} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$.

d. $M^2_{\mathscr{R}'} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$.

e. En terme de distance la relation $\phi(m_1) \mathscr{S} \phi(m_2)$ signifie que $\phi(m_1) = (k_1, l_1)$ et $\phi(m_2) = (k_2, l_2)$ sont à une distance $\leqslant 1$ sachant que la distance entre $\phi(m_1)$ et $\phi(m_2)$ est définie dans ce cas par $|k_1 - k_2| + |l_1 - l_2|$. La matrice $M^2_{\mathscr{R}'}$ représente la matrice de la relation

$S \circ S$ restreinte aux couples 1 = (0,0), 2 = (1,0), 3 = (0,1) et 6 = (1,1). La relation $S \circ S$ met en relation des couples qui sont à une distance au plus deux (par composition de $\mathscr{S}$). Or sur cet ensemble de couples, la distance est toujours inférieure à 2 ce qui est cohérant avec le calcul de $M^2_{\mathscr{R}'}$ qui indique que tous les couples sont en relation.