INF1132 Session Automne 2022
Devoir 1

Professeurs : Srečko Brlek, kelrB okčerS

Nom: SOLUTIONNAIRE

Code permanent: en cours

1	2	3	4	5	**Total**
/ 50	/ 30	/ 40	/ 40	/ 40	/ 200

Directives

1. Le devoir doit être rédigé **individuellement** et remis **avant le 20 octobre 2022 avant midi**.
2. **Aucun retard** n'est permis, car la solution sera mise en ligne après l'heure limite de remise.
3. Votre document doit être **rédigé en LaTeX** , à partir du modèle fourni incluant la page de couverture.
4. Vous devez remplir cette page comme page couverture pour vous identifier lors de la remise de votre devoir sinon votre travail **ne sera pas corrigé**.
5. Vous devez remettre sur Moodle **un fichier compressé (.zip) contenant le pdf de votre devoir ET le code LaTeX ayant servi à le générer.**
6. Pour que votre devoir soit corrigé, l'archive doit obligatoirement être nommée : **VOTRECODEPERMANENT_INF1132_DEVOIR1.zip**.
7. À moins d'avis contraire, vous devez **justifier** chacune de vos réponses.
8. La démarche ainsi que l'utilisation correcte de la notation mathématique seront évaluées.

Question 1 sur la logique propositionnelle (**50** points)

Les parties A et B sont indépendantes.

Partie A — 25 points

Soit l'opérateur logique $\diamondsuit$ tel que $p \diamondsuit q$ est faux dans tous les cas sauf quand la proposition p est fausse et la proposition q est vraie.

(**10** pts) **a)** Donner la table de vérité de l'opérateur logique $\diamondsuit$ ci-dessous.

p	q	p $\diamondsuit$ q
V	V	F
V	F	F
F	V	V
F	F	F

(**5** pts) **b)** Est-ce que l'opérateur $\diamondsuit$ est un opérateur logique commutatif ? Expliquer.

Rappel : un opérateur λ est commutatif si et seulement si

$$\forall p, q, \quad p \; \lambda \; q = q \; \lambda \; p.$$

Supposons p faux et q vrai. Selon la table de vérité, on a que

$$p \diamondsuit q \text{ est Vrai, alors que } q \diamondsuit p \text{ est Faux.}$$

Ainsi, l'opérateur logique $\diamondsuit$ n'est pas commutatif.

(**10** pts) **c)** En utilisant la table de vérité, prouver que $p \diamondsuit q \iff \neg p \wedge q$.

p	q	p $\diamondsuit$ q	$\neg p$	$\neg p \wedge q$
V	V	F	F	F
V	F	F	F	F
F	V	V	V	V
F	F	F	V	F

Les colonnes de la table correspondant à $p \diamondsuit q$ et $\neg p \wedge q$ sont identiques, d'où le résultat.

Partie B — 25 points

On suppose que les 4 propositions suivantes sont **toutes vraies** :

1. $A \to B$
2. $C \to D$
3. $A \vee C$
4. $\neg D$

Quelle(s) valeur(s) de vérité peuvent prendre les propositions A, B, C et D ? Justifier.

En se basant sur les tables de vérité des opérateurs logiques, on a :

$$\neg D \text{ est Vraie} \iff \text{la proposition } D \text{ est fausse.}$$

Comme l'implication $C \to D$ est vraie et que la proposition D est fausse, on déduit que

$$C \text{ est aussi fausse.}$$

Comme la conjonction $A \vee C$ est Vraie et que C est Fausse, il est nécessaire que

$$A \text{ soit vraie.}$$

Comme l'implication $A \to B$ est vraie et que A l'est aussi, on conclut que

$$B \text{ est Vraie.}$$

Ainsi, on trouve les valeurs de vérité suivantes :

A	B	C	D
V	V	F	F

On aurait pu aussi bien faire une table de vérité qui requiert 2^4 lignes .... et la remplir en arrêtant quand une conditions n'est pas satisfaite

A	B	C	D	$\neg D$	$A \vee C$	$C \to D$	$A \to B$
V	V	V	V	*F*			
V	V	V	F	V	V	*F*	
V	V	F	V	*F*			
V	V	F	F	**V**	**V**	**V**	**V**
V	F	V	V	*F*			
V	F	V	F	V	V	*F*	
V	F	F	V	*F*			
V	F	F	F	V	V	V	*F*
...	...	...	...	...	...	...	...

On remarque dans la table que la quatrième ligne satisfait le problème, mais en principe, il faut continuer pour voir s'il y a d'autres solutions...

Question 2 sur la logique des prédicats (**30** points)

Les parties A et B sont indépendantes.

Partie A — 20 points
On considère les énoncés suivants :

- $P(x)$: "L'étudiant x sait programmer en langage Python",
- $Q(x, y)$: "L'étudiant x est dans le groupe-cours y",

où l'univers du discours de x est l'ensemble des étudiants en informatique à l'UQAM et l'univers du discours de y est l'ensemble des groupes-cours du département d'informatique de l'UQAM.

(**12** pts) 1. Écrivez chacune des phrases suivantes sous forme d'énoncés quantifiés.

(**2** pts) (a) Certains étudiants savent programmer en Python.

$$\exists x, P(x)$$

(**2** pts) (b) Les étudiants ne savent pas tous programmer en Python.

$$\exists x, \neg P(x)$$

(**2** pts) (c) Chaque groupe-cours contient au moins un étudiant.

$$\forall y, \exists x, Q(x, y)$$

(**2** pts) (d) Dans chaque groupe-cours, il y a un étudiant qui sait programmer en Python.

$$\forall y, \exists x, P(x) \wedge Q(x, y)$$

(**2** pts) (e) Il y a un étudiant qui n'est dans aucun groupe-cours.

$$\exists x, \forall y, \neg Q(x, y)$$

(**2** pts) (f) Il y a au moins un groupe-cours dans lequel aucun étudiant ne sait programmer en Python.

$\exists y, \forall x, Q(x,y) \to \neg P(x)$

(**8** pts) 2. Exprimez chacun des énoncés quantifiés suivants en langage courant.

(**2** pts) (i) $\forall x, \forall y, Q(x,y)$

Tous les étudiants sont dans tous les groupes-cours.

(**2** pts) (ii) $\forall x, \exists y, P(x) \to Q(x,y)$

Tout étudiant qui sait programmer en Python est dans au moins un groupe-cours.

(**2** pts) (iii) $\exists x, \forall y, P(x) \wedge \neg Q(x,y)$

Il y a un étudiant qui sait programmer en Python et qui n'est dans aucun groupe-cours.

(**2** pts) (iv) $\exists y, \forall x, Q(x,y) \to P(x)$

Il y a un groupe-cours dans lequel tous les étudiants savent programmer en Python.

Partie B — 10 points

Dites si chacune des propositions suivantes est vraie ou fausse lorsqu'on suppose que l'univers du discours est (i) $\mathbb{R}$, (ii) $\mathbb{N}$ ou (iii) $\{0, 1, 2, 4\}$.

(**2** pts) **a)** $\forall x \, \exists y \, (y^2 = x)$

(i) Faux pour $x < 0$: le carré d'un nombre réel est toujours positif.
(ii) Faux pour $x = 2$ car $\sqrt{2}$ est irrationnel et donc n'est pas dans $\mathbb{N}$.
(iii) Faux pour $x = 2$, par le même argument que ci-dessus.

(**2** pts) **b)** $\neg\forall x \, \exists y \, (y > x)$

Les ensembles dans les trois cas sont ordonnés, le troisième est fini. En conséquence,

(i) Faux en prenant $y = x + 1$.
(ii) Faux en prenant $y = x + 1$.
(iii) Vrai pour $x = 4$.

(**2** pts) **c)** $\forall x \, \neg\exists y \, (y > x)$

Faux car pour $x = 0$, il existe un y plus grand dans chacun des cas: par exemple $y = 1$.

(**2** pts) **d)** $\exists x \, \exists y \, \exists z \, ((y \neq z) \wedge (y^2 = x) \wedge (z^2 = x))$

(i) Vrai. En effet, pour $y = 1$ et $z = -1$, nous avons $x = 1$.
(ii) Faux car la fonction carré est injective sur $\mathbb{R}^+$, donc sur $\mathbb{N}^+$.
(iii) Faux car la fonction carré est injective sur N, et donc sur 0,1,2,4.

(**2** pts) **e)** $\forall x \, (x \neq 1 \longrightarrow \exists y \, (2y = x))$

(i) Vrai. Pour tout x on prend $y = x/2$.
(ii) Faux. Pour $x = 3$, il n'y a pas d'entier y tel que $2y = 3$
(iii) Vrai : $2 \cdot 0 = 0$, $2 \cdot 1 = 2$ et $2 \cdot 2 = 4$.

Question 3 sur les ensembles (**40** points)

Les parties A et B sont indépendantes.

Partie A — 20 points

Soient A, B, C, D des ensembles. Pour chacune des propositions suivantes, dites si elle est vraie ou fausse en justifiant votre réponse.

(**4** pts) 1. $((B \cap A) \setminus C) \cup \left(\overline{B \oplus C} \setminus A\right) = ((A \cap B) \oplus (B \cap C)) \cup \left(\overline{A} \setminus (B \cup C)\right)$
(Conseil: utilisez une table d'appartenance)

A	B	C	$(B \cap A)$	$(B \cap A) \setminus C$	$\overline{B \oplus C}$	$\overline{B \oplus C} \setminus A$	$((B \cap A) \setminus C) \cup \left(\overline{B \oplus C} \setminus A\right)$
0	0	0	0	0	1	1	1
0	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0
0	1	1	0	0	1	1	1
1	0	0	0	0	1	0	0
1	0	1	0	0	0	0	0
1	1	0	1	1	0	0	1
1	1	1	1	0	1	0	0

et

			i	j			k		
A	B	C	$(A \cap B)$	$(B \cap C)$	$(i) \oplus (j)$	$\overline{A}$	$(B \cup C)$	$\overline{A} \setminus (k)$	$((i) \oplus (j)) \cup \left(\overline{A} \setminus (k)\right)$
0	0	0	0	0	0	1	0	1	1
0	0	1	0	0	0	1	1	0	0
0	1	0	0	0	0	1	1	0	0
0	1	1	0	1	1	1	1	0	1
1	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	1	0	0
1	1	0	1	0	1	0	1	0	1
1	1	1	1	1	0	0	1	0	0

Les colonnes de droite sont identiques donc l'égalité entre les deux ensembles est vraie.

(**2** pts) 2. Si $A \subseteq B$ et $A \cap C \neq \emptyset$, alors $B \cap C = \emptyset$.

Faux : pour $A = B = C = \{1\}$ on a $A \cap C \neq \emptyset$ et $B \cap C \neq \emptyset$

(**2** pts) 3. Si $A \subseteq B$ et $B \cap C = \emptyset$, alors $A \cap C = \emptyset$.

> Vrai : si $x \notin A$ alors $x \notin A \cap C$; si $x \in A$ alors $x \in B$, or $B \cap C = \emptyset$ donc $x \notin C$, d'où $x \notin A \cap C$.

(**2** pts) 4. Si $A \subseteq B$ et $C \cap \overline{B} \neq \emptyset$, alors $C \cap \overline{A} \neq \emptyset$.

> Vrai : si $A \subseteq B$ alors $\overline{B} \subseteq \overline{A}$. Soit $x \in C \cap \overline{B}$ (non vide), alors $x \in C$ et $x \in \overline{B} \subseteq \overline{A}$ donc $x \in C \cap \overline{A}$, qui est donc non vide.

(**2** pts) 5. Si $B \subseteq A$, $C \subseteq D$, et $A \cap D = \emptyset$, alors $B \cap C = \emptyset$.

> Vrai : Supposons $B \cap C \neq \emptyset$, alors soit $x \in B \cap C$. Comme $B \subseteq A$ et $C \subseteq D$, on a $x \in A$ et $x \in D$, c'est-à-dire $x \in A \cap D$, qui serait donc non vide. ceci contredit l'hypothèse $A \cap D = \emptyset$. Donc $B \cap C = \emptyset$.

(**2** pts) 6. Si $A \subseteq B$, $D \subseteq C$, et $A \cap D = \emptyset$, alors $B \cap C = \emptyset$.

> Faux : pour $A = D = \emptyset$ et $B = C = \{1\}$.

(**3** pts) 7. $A \cup B = A \Longleftrightarrow A \cap B = B$.

> Vrai :
> Supposons $A \cup B = A$, alors si $x \in B$, comme $B \subseteq A \cup B = A$, on a $x \in A$, d'où $x \in A \cap B$. Donc $B \subseteq A \cap B \subseteq B$, d'où l'égalité.
> Réciproquement, supposons $A \cap B = B$. Si $x \in A \cup B$, alors $x \in A$ ou $x \in B = A \cap B$, donc $x \in A$ ou ($x \in A$ et $x \in B$). Dans tous les cas on a $x \in A$, donc $A \cup B \subseteq A$ et comme l'inclusion inverse est toujours vraie on a l'égalité.

(**3** pts) 8. $A \oplus B = \emptyset \Longleftrightarrow A = B$.

> Vrai :
> $$\begin{aligned} A \oplus B = \emptyset &\Longleftrightarrow (A \setminus B) \cup (B \setminus A) = \emptyset \\ &\Longleftrightarrow A \setminus B = \emptyset \text{ et } B \setminus A = \emptyset \\ &\Longleftrightarrow A \subseteq B \text{ et } B \subseteq A \\ &\Longleftrightarrow A = B \end{aligned}$$

Partie B — 20 points: 3 pts par cardinalité juste et 8 pts pour les justifications

Soient A, B et C trois sous-ensembles de l'ensemble universel U qui satisfont les 8 conditions suivantes :

(a) $|\mathscr{P}(A \cap B \cap C)| = 128$

(b) $|B \cap C| = 17$

(c) $|A \cap C| = 12$

(d) $|A \cap B| = 14$

(e) $|A| = |B| - 1$

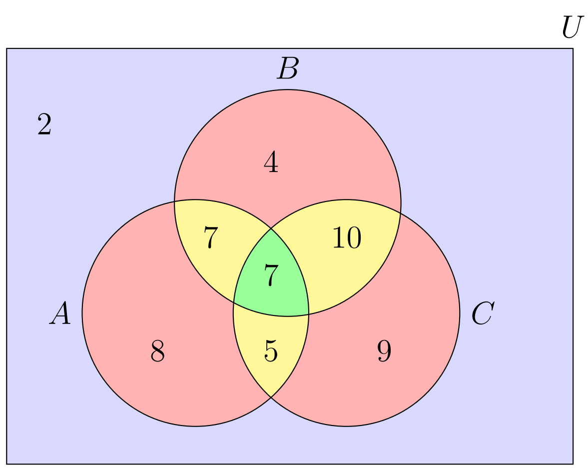
(f) $|B \oplus C| = 25$

(g) $|A \times B| = 756$

(h) $|\overline{A} \cap \overline{B} \cap \overline{C}| = |\mathscr{P}(\{\varnothing\})|$

Déterminez les cardinalités des ensembles A, B, C et U en justifiant soigneusement votre raisonnement.

On peut s'aider du diagramme de Venn ci-dessous, qu'on remplit dans l'ordre suivant :
(a) nous donne le 7 au milieu (vert) car $|\mathscr{P}(A \cap B \cap C)| = 128 = 2^7 \iff |A \cap B \cap C| = 7$.
(b), (c) et (d) nous donnent les nombres des zones jaunes, en retirant le 7 du milieu.
(e) et (g) nous donnent $|A| = 27$ et $|B| = 28$, d'où les nombres 8 et 4 dans les zones rouges.
(f) nous dit que $|B \cup C| - |B \cap C| = 25$, d'où $|B \cup C| = 25 + 17 = 42$ et on a déjà 33 éléments dans cet ensemble donc il y a 9 dans la dernnière zone en rouge.
(h) nous donne le 2 de la zone bleue, car $|\mathscr{P}(\{\varnothing\})| = 2$.



Finalement, on a donc $|A| = 27$, $|B| = 28$, $|C| = 31$ et $|U| = 52$.

Question 4 sur le dénombrement (**40** points)

A l'UQAM les chiffres en date de l'automne 2021 indiquent qu'il y avait :

- 36 960 étudiants dont 28 060 au 1er cycle, 6769 au 2e cycle et 2131 au 3e cycle; parmi ceux-là 4387 étaient des étudiants internationaux provenant de 95 pays;
- 2124 chargé(e)s de cours;
- 1143 professeur(e)s.
- 335 programmes d'études dont: 180 de premier cycle, 125 de deuxième cycle et 30 de troisième cycle

Déterminez pour chacun des énoncés suivants s'il est vrai ou faux. Justifiez votre réponse.

(**7** pts) **a)** Il y a au moins deux étudiants qui sont dans le même programmme et qui sont nés le même jour.

(**7** pts) **b)** Il y a deux étudiants internationaux qui sont dans le même programme d'études

(**4** pts) **c)** Chaque professeur a au moins 2 étudiants internationaux dans un cours

(**7** pts) **d)** Il y a deux professeurs qui ont la même date d'anniversaire

(**7** pts) **e)** Deux chargés de cours sont nés le même jour

(**4** pts) **f)** Il y a au moins deux étudiants de troisième cycle ayant la même date de naissance

(**4** pts) **g)** il y a au plus deux étudiants de maitrise ayant la même date de naissance

L'interprétation pouvant être ambigüe, nous allons utiliser celle-ci:

jour: lundi, mardi, mercredi, jeudi, vendredi, samedi, dimanche.

date d'anniversaire : numéro de jour dans le mois + mois (exemple: 13 avril)

date de naissance : numéro de jour + mois + année (exemple: 13 avril 2001)

Si vous avez choisi une autre interprétation, ce qui est important est que vous justifiez le raisonnement qui vous amenant à répondre vrai ou faux.
Il s'agit donc de déterminer la cardinalité des ensembles et l'inégalité qui s'en suit

a) Vrai: $36960 > 335 \times 7 = 2345$.

b) Vrai: $4387 > 335$.

c) On ne sait pas.

d) Vrai: $1143 > 366$.

e) Vrai: $2124 > 7$.

f) On ne sait pas.

g) On ne sait pas.

Question 5 sur les fonctions(**40** points)

Les parties A et B sont indépendantes.

Partie A — 20 points

Considérez les fonctions suivantes :

$$f : \mathbb{N} \to \mathbb{N},\ f(n) = \begin{cases} 2n+1 & \text{si } n \text{ est pair;} \\ 2n-2 & \text{si } n \text{ est impair.} \end{cases}$$

$$g : \mathbb{N}^* \to \mathbb{N} \times \mathbb{N},\ g(n) = (n+1, n-1)$$

$$h : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{Z},\ h(n,m) = \left\lceil \frac{n-m}{n+m} \right\rceil$$

$$u : \mathbb{R} \to \mathbb{Z},\ u(x) = 2\lfloor x \rfloor + 1$$

$$v : \mathbb{N} \to \mathbb{Z},\ v(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ est pair;} \\ -\frac{n+1}{2} & \text{si } n \text{ est impair.} \end{cases}$$

$$w : \mathbb{R} \to \mathbb{R},\ w(x) = x^3 + 2x - 1$$

(**10** pts) **a)** Complétez le tableau suivant (mettre un **x** si la fonction possède la propriété considérée ou aucune).

	injective	surjective	bijective	aucune
f	**x**			
g	**x**			
h				**x**
u				**x**
v	**x**	**x**	**x**	
w	**x**	**x**	**x**	

-f injective : il y a 2 cas, si (n,m) sont pairs alors $n \neq m \implies 2n+1 \neq 2m+1$. Si (n,m) sont impairs alors $n \neq m \implies 2n-1 \neq 2m-2$.
f non surjective : 3 n'a pas d'antécédents pair.
-g injective: $n \neq m \implies n+1 \neq m+1 \implies (n+1, n-1) \neq (m+1, m-1)$
g non surjective : $(0,0)$ n'a pas d'antécédents, $(m,m)\forall m$ non plus car $n+1 = m = n-1$ n'a pas de solution.
-h non injective car $\lceil x \rceil$ ne l'est pas.
h non surjective car 2 n'a pas d'antécédents puisque n et m sont strictement positifs.
-u n'est pas injective car $\lfloor x \rfloor$ ne l'est pas.

Non surjective car aucun nombre pair n'a d'antécédents: $2\lfloor x \rfloor + 1$ est un nombre impair.
-v injective: si $f(n) = f(m)$ est positif, alors $f(n) = f(m) \implies n/2 = m/2 \implies n = m$. L'autre cas est similaire. Surjectivité: Si $m \geq 0$ alors $v(2m) = m$. Si $m < 0$ alors $v(-2m-1) = m$.
-w est croissante donc injective: Si $x < y$ alors $2x < 2y$ et $x^3 < y^3$ (vérifiez cette dernière). On a donc $w(x) < w(y)$. Surjective : $w(\mathbb{R}) = \mathbb{R}$ car w est $\mathscr{O}(x^3)$.

(**5** pts) **b)** Déterminez toutes les compositions **possibles** de deux fonctions choisies parmi f, g, h, u, v et w. À chaque fois que c'est possible, donnez les fonctions composées.

Les cases avec un **x** sont celles correspondant aux compositions non définies

$\downarrow \circ \rightarrow$	f	g	h	u	v	w
f		**x**		**x**	**x**	**x**
g	**x**	**x**	**x**	**x**	**x**	**x**
h	**x**	**x**	**x**	**x**	**x**	**x**
u		**x**				
v		**x**	**x**	**x**	**x**	**x**
w		**x**				

On a donc

- $(f \circ f)(n) = \begin{cases} 4n & \text{si } n \text{ pair;} \\ 4n-3 & \text{si } n \text{ impair.} \end{cases}$, $\quad (f \circ h)(n) = \begin{cases} 1 & \text{si } m \geq n; \\ 0 & \text{si } m < n. \end{cases}$
- $(u \circ f)(n) = \begin{cases} 4n+3 & \text{si } n \text{ pair;} \\ 4n-3 & \text{si } n \text{ impair.} \end{cases}$
- $(u \circ h)(n) = 2\left\lceil \dfrac{n-m}{n+m} \right\rceil + 1$
- $(u \circ u)(x) = 4\lfloor x \rfloor + 2$
- $(u \circ v)(n) = \begin{cases} n+1 & \text{si } n \text{ est pair;} \\ -n & \text{si } n \text{ est impair.} \end{cases}$
- $(u \circ w)(x) = 2\lfloor (x^3 + 2x - 1) \rfloor + 1$
- $(v \circ f)(n) = \begin{cases} -n-1 & \text{si } n \text{ est pair;} \\ n-1 & \text{si } n \text{ est impair.} \end{cases}$
- $(w \circ f)(n) = \begin{cases} (2n+1)^3 + 4n + 1 & \text{si } n \text{ est pair;} \\ (2n-2)^3 + 4n - 3 & \text{si } n \text{ est impair.} \end{cases}$
- $(w \circ h)(n,m) = \left\lceil \dfrac{n-m}{n+m} \right\rceil^3 + 2\left\lceil \dfrac{n-m}{n+m} \right\rceil + 1$
- $(w \circ u)(x) = (2\lfloor x \rfloor + 1)^3 + 4\lfloor x \rfloor + 1$
- $(w \circ v)(n) = \begin{cases} \left(\dfrac{n}{2}\right)^3 + n + 1 & \text{si } n \text{ pair;} \\ -\left(\dfrac{n+1}{2}\right)^3 - n - 1 & \text{si } n \text{ impair.} \end{cases}$
- $(w \circ w)(x) = x^9 + 6x^7 - 3x^6 + 12x^5 - 12x^4 + 13x^3 - 12x^2 + 10x - 4$

(**5** pts) **c)** La fonction v est-elle inversible ? Si oui, déterminez v^{-1}.
Que pouvez-vous en conclure sur $\mathbb{N}$ et $\mathbb{Z}$?

La fonction v est bijective donc inversible. On a

$$v^{-1}(z) = \begin{cases} 2z & \text{si } z \geq 0 \ ; \\ 1 - 2z & \text{si } z < 0 \ . \end{cases}$$

Il y a une bijection entre $\mathbb{N}$ et $\mathbb{Z}$ c'est à dire ils ont la même cardinalité.

Partie B — 20 points
Le but de cet exercice est de construire des fonctions permettant d'encoder des messages. Les messages sont écrits à l'aide des "caractères" A, B, ..., Z (c'est-à-dire les lettres majuscules), du point et de l'espace (indispensable pour séparer les mots). Pour coder un message, on peut affecter la valeur i (pour $1 \leq i \leq 26$) à la $i^{\text{ième}}$ lettre de l'alphabet, la valeur 27 au point et la valeur 28 à l'espace. Comme il serait trop facile à l'ennemi de décoder un message codé de cette manière, il a été décidé de le transformer. Dans ce qui suit n dénote la "valeur" du caractère telle que définie ci-dessus. Soit $f(n)$ et $g(n)$ les deux fonctions suivantes:

$$f(n) = \begin{cases} n+1 & \text{pour } 1 \leq n \leq 27 \\ 1 & \text{pour } n = 28 \end{cases}$$

$$g(n) = (5n) \bmod 29 \quad \text{pour } 1 \leq n \leq 28.$$

Notez que le domaine et le codomaine de f et de g sont l'ensemble des entiers naturels compris entre 1 et 28. L'opérateur "mod" représente le reste de la division. Par exemple, $g(15) = 75 \bmod 29 = 17$.

(**4** pts)**(a)** Prouvez que f et g sont des fonctions injectives.

Pour vérifier l'injectivité, il suffit maintenant de vérifier que

$$(n_1 - n_2 \neq 0) \Longrightarrow (f(n_1) - f(n_2) \neq 0)$$

Il en est de même pour la fonction g.

- f est injective. Deux cas à considérer à cause de la définition de f
  Cas 1. $n_1 \neq 28$ et $n_2 \neq 28$. Alors on a que

  $$f(n_1) - f(n_2) = (n_1 + 1) - (n_2 + 1) = n_1 - n_2 \neq 0$$

  Cas 2. Si l'un des nombres, disons n_1, est égal à 28, alors

  $$f(n_1) - f(n_2) = 1 - (n_2 + 1) = -n_2 \neq 0.$$

- g est injective. On a $g(n_1) - g(n_2) = 5(n_1 - n_2) \mod 29$. Puisque $5(n_1 - n_2)$ n'est pas un multiple de 29 on a bien le résultat cherché.

(**4** pts)**(b)** Déduire de (a) que f et g sont bijectives.

Il suffit de vérifier la surjectivité. Soit $m \in \{1..28\}$

- f est bijective car $|f([1..28])| = 28$
- Pour la fonction g, on a la relation $5n = m + 29k$. D'où $n = (m + 29)k/5$.

(**3** pts) **(c)** Prouvez que si f et g sont des fonctions bijectives, alors $f \circ g$ est une fonction bijective.

La composition de fonctions injectives est injective, et il en est de même des fonctions surjectives. Dans notre cas nous avons:

$$n_1 \neq n_2 \Longrightarrow g(n_1) \neq g(n_2) \Longrightarrow f(g(n_1)) \neq f(g(n_2))$$

La transitivité de l'implication permet de conclure.

La composition de fonctions surjectives est surjective. En effet, soit $m \in \{1..28\}$. Alors

$$\exists n \in \{1..28\}, f(n) = m, \quad \text{car } f \text{ est surjective.}$$

Mais on a aussi que

$$\exists k \in \{1..28\}, g(k) = n, \quad \text{car } g \text{ est surjective.}$$

On a donc bien que

$$f \circ g(k) = f(g(k)) = f(n) = m.$$

(**3** pts) **(d)** Écrivez la suite de nombres qui représente la phrase

“`LE CIEL EST BLEU.`”

lorsqu'on utilise

(i) la fonction de codage $g \circ f$

`(7, 1, 5, 20, 21, 1, 7, 5, 1, 13, 18, 5, 15, 7, 1, 23, 24)`

(ii) la fonction de codage $g \circ g$.

`(10, 9, 4, 17, 22, 9, 10, 4, 9, 11, 7, 4, 21, 10, 9, 3, 8)`

(**3** pts) **(e)** Pouvez-vous décrire $g \circ g$ de façon concise sans utiliser g?

$(g \circ g)(n) = 25n \bmod 29$

(**3** pts) **(f)** Quelle est la phrase codée par “`UOY .HHH`” avec la fonction $g \circ g$

`BRAVO...`