Université Paris Descartes
UFR de Mathématiques et Informatique
45, rue des Saints-Pères 75270 Paris cedex 06

L2 Info 2017/2018

Numération et Logique

Global

01/01/2019 - 15 minutes

☐ **0**	☐ **0**	☐ **0**	☐ **0**	☐ **0**	☐ **0**	☐ **0**	☐ **0**
☐ **1**	☐ **1**	☐ **1**	☐ **1**	☐ **1**	☐ **1**	☐ **1**	☐ **1**
☐ **2**	☐ **2**	☐ **2**	☐ **2**	☐ **2**	☐ **2**	☐ **2**	☐ **2**
☐ **3**	☐ **3**	☐ **3**	☐ **3**	☐ **3**	☐ **3**	☐ **3**	☐ **3**
☐ **4**	☐ **4**	☐ **4**	☐ **4**	☐ **4**	☐ **4**	☐ **4**	☐ **4**
☐ **5**	☐ **5**	☐ **5**	☐ **5**	☐ **5**	☐ **5**	☐ **5**	☐ **5**
☐ **6**	☐ **6**	☐ **6**	☐ **6**	☐ **6**	☐ **6**	☐ **6**	☐ **6**
☐ **7**	☐ **7**	☐ **7**	☐ **7**	☐ **7**	☐ **7**	☐ **7**	☐ **7**
☐ **8**	☐ **8**	☐ **8**	☐ **8**	☐ **8**	☐ **8**	☐ **8**	☐ **8**
☐ **9**	☐ **9**	☐ **9**	☐ **9**	☐ **9**	☐ **9**	☐ **9**	☐ **9**

$\longleftarrow$ codez votre numéro d'étudiant ci-contre, et inscrivez votre nom et prénom ci-dessous.

Nom et prénom :

....

....

Question 1 Un octet contient une suite de 8 "0" ou "1", comme par exemple "00110110"

- [x] oui
- [ ] non

Question 2 Combien a-t-on de bits dans un kibiOctet ?

- [ ] 2^{10}
- [x] autre
- [ ] 10^3

Question 3 Combien de KiloOctets dans un gibiOctet ?

- [ ] 1 million
- [x] $2^{30}/10^3$
- [ ] 2^{20}

Question 4 Combien de kibiOctets dans un gibiOctet ?

- [ ] 1 million
- [ ] 10^3
- [x] 2^{20}

Question 5 Sur un octet, on peut représenter combien d'informations différentes ?

- [ ] deux ("0" ou "1")
- [ ] 255
- [x] 256

Question 6 Un bit contient une suite de 8 "0" ou "1", comme par exemple "00110110"

- [ ] oui
- [x] non

Question 7 Combien vaut $(421)_5$?

- [x] 111
- [ ] $4 * 5^3 + 2 * 5^2 + 1$
- [ ] $4 * 5^2 + 2 * 5 + 5$

Question 8 Quelles assertions sont vraies ?

- [ ] $(36)_{10} * (143)_6 = (11143)_6$
- [x] $(36)_{10} * (143)_6 = (14300)_6$
- [ ] $(7^4)_{10} * (433)_7 = (22543)_7$

Question 9 On a $(537)_8 = 5 * 8^3 + *3 * 8^2 + 7 * 8^1$?

- [ ] oui
- [x] non

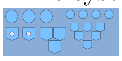
Question 10 Combien vaut $(337)_4$?

- [ ] 67
- [x] autre
- [ ] 13
- [ ] $3 * 4^2 + 3 * 4^1 + 7$

Question 11 Parmi les systèmes suivants, lesquels sont de "position" ?

- [x] Chiffres romains (exemple : MMCMXIII)
- [ ] Systèmes de bâtonnets barrés (exemple : 7=\sout{IIII} II)
- [x] Système décimal actuel (exemple : 12, 1339, ...)
- [x] Binaire (exemple : 6=110)

Question 12 Le système mésopotamien est décrit par **??** 

Combien vaut  ?

- [x] 12226
- [ ] 13412
- [ ] 9885
- [ ] 1157

Question 13 Dans quelles bases 4AB56C a-t-il un sens ?

- [x] 14
- [x] 13
- [ ] 12
- [ ] 11
- [ ] 10

Question 14 Combien vaut le nombre décimal 101 en base 2 ?

- [ ] $1 * 2^2 + 0 * 2^0 + 1 * 2^0$
- [ ] $(101)_2$
- [ ] 5
- [x] un nombre plus grand que $(1000000)_2$
- [ ] $(10011010)_2$
- [x] $(1100101)_2$

Question 15 Quels symboles faut-il pour écrire en base 13 ?

- [x] il faut 13 symboles
- [ ] il faut 12 symboles
- [ ] 0,1,2,...,9, et 4 symboles de plus, comme par exemple A,B,C,D

Question 16 est-ce qu'en base 7, 034=34 ?

- [x] oui
- [ ] non

Question 17 Combien vaut $(244)_6$ en base 10 ?

- ■ $2 * 36 + 4 * 6 + 4$
- □ 127

Question 18 Combien y'a-t-il d'octets dans 1KiloByte dans le système traditionnel?

- ■ 10^3
- □ 2^{10}
- □ 2^3

Question 19 On donne $6^3 = 216, 6^4 = 1296, 6^5 = 7776, 6^6 = 46656$.

- ■ En base 6, 2245 s'écrit avec 5 chiffres
- ■ En base 6, 50000 s'écrit avec 7 chiffres
- □ En base 6, 7 s'écrit avec 1 chiffre
- □ En base 6, 4421113352221 s'écrit avec 12 chiffres

Question 20 Quelles inégalités sont vraies ?

- ■ $(51234)_8 > (51234)_7$
- □ $(B)_{16} > (B)_{17}$
- ■ $(B)_{16} \leq (B)_{18}$
- □ $(3)_8 > (4)_7$

Question 21 cochez

- □ Tous les nombres rationnels ont un développement fini en n'importe quelle base
- ■ En base 10, tous les nombres ayant un développement fini sont rationnels
- □ Tous les nombres rationnels ont un développement fini en base 10
- ■ En n'importe quelle base, tous les nombres ayant un développement fini sont rationnels

Question 22 Quelles inégalités sont vraies ?

- □ $(0,51234)_8 > (0,51234)_7$
- ■ $(3,B)_{16} > (3,B)_{17}$
- □ $(A,B)_{16} \leq (A,B)_{18}$
- ■ $(4,3)_8 > (3,4)_7$
- ■ $(5,3324565)_8 > (5,3324565)_9$

Question 23 Cochez les assertions vraies

- ■ $12/7 = (1,5)_7$
- ■ $(333)_4/(4^2)_{10} = (3,33)_4$
- ■ $(AAA)_{12}/(100)_{12} = (A,AA)_{12}$
- □ $(ABCDEF)_{16}/(16^3)_{10} = (ABC)_{16}$

Question 24 Cochez

- [ ] Un nombre qui a un développement fini dans une base a un développement fini dans toutes les bases
- [ ] Tout nombre s'écrit sous forme d'une fraction (dans n'importe quelle base)
- [ ] $(x/y)_b = (x)_b/(y)_b$?
- [x] autre

Question 25 Parmis ces nombres, lesquels ont un développement fini ?

- [x] $(1/5)_{10}$
- [ ] $(1/3)_{10}$
- [x] 1/49 en base 7
- [x] $(12/21)_7$
- [ ] $(10/21)_7$
- [ ] $(\pi)_3$

Question 26 Si je compte en base 5 avec mes deux mains (une main pour les unités et une main pour les "cinquaines", combien de nombres puis-je représenter (n'oubliez pas le 0 !)?

- [x] $(111)_5$
- [ ] 5*5
- [x] 31
- [ ] 1225
- [ ] autre

Question 27 Comment faire les regroupements ?

- [ ] $(\underbrace{0110}\underbrace{1,110})_2$ vers la base 16
- [ ] $(\underbrace{004}\underbrace{371},\underbrace{330}\underbrace{010})_8$ vers la base 2
- [x] $(\underbrace{\ 11\ }\underbrace{010110},\underbrace{11111})_2$ vers la base 64
- [ ] autre

Question 28 conversion

- [ ] $(111)_{25} = (111)_5$
- [ ] $(731)_9 = (1211)_3$
- [x] $(20)_{64} = (10000000)_2$
- [x] $(34)_{16} = (64)_8$

Question 29 Combien vaut -92 en $CA2_8$?

- [x] Comme le codage binaire de $2^8 - 92$
- [ ] Comme le codage binaire de $2^7 - 92$
- [ ] Ce qu'on obtient si l'on code 92 en binaire sur 8 bits, inverse tous les bits, et remplace le bit de gauche par 1
- [ ] [10100011]
- [x] Le code de -92 en $CA1_8$ auquel on ajoute 1 en binaire

Question 30 On fait les additions suivantes en $CA2$. Cochez les cases où il y a overflow

- [x] $(10)_2 + (111)_2$ sur 4 bits
- [ ] $(10)_2 + (111)_2$ sur 5 bits
- [ ] $11100110101100110011001011001001 + 01110010011001100010000010111001$ sur 32 bits
- [x] 110+32 sur 8 bits
- [x] 10000+25000 sur 16 bits

Question 31 Que faire de la retenue lors de l'addition en CA2 ?

- [x] Elle permet de détecter l'overflow, maisà part pour ça il faut la négliger
- [ ] Il ne faut jamais tenir compte de la retenue
- [ ] Pour l'addition de signes opposés elle permet de détecter l'overflow, mais elle ne sert à rien pour l'addition de même signes
- [ ] Il faut changer le bit de gauche pour qu'il corresponde à la retenue
- [x] Le résultat de l'addition est valide si et seulement si la retenue finale correspond à la retenue du bit de poids fort, autrementil y a overflow

Question 32 On donne $0,4 \cdot 2 = 0,8,\ 0,8 \cdot 2 = 1,6,\ 0,6 \cdot 2 = 1,2$ Cochez les assertions vraies

- [ ] $3,4 = (11,011)_2$
- [ ] Tout nombre de la forme $(x,4)_{10}$ a un développement fini en base 2, où x est un entier
- [x] Tout nombre de la forme $(x,4)_{10}$ a un développement périodique en base 2, où x est un entier
- [x] On peut connaître le développement de 3,4 sans faire une infinité de calculs
- [x] $(3,4)_{10} = (3,6666...)_{16}$

Question 33 On considère un système de stockage de réels avec une mantisse de 4 chiffres décimaux, un exposant de 2 chiffres décimaux, et 2 bits de signe, sans autre contrainte

- [ ] Le plus grand nombre codable est $9999 \cdot 10^{99}$
- [ ] Le plus petit nombre codable est $-9999 \cdot 10^{-99}$
- [ ] Tous les réels entre le plus petit et le plus grand nombre codable ont une représentation dans ce système
- [ ] On peut représenter $4 \cdot 9999 \cdot 99$ nombres différents
- [x] On peut représenter $2 \cdot 199 \cdot 9 \cdot 10^3 + 1$ nombres différents

Question 34 Cochez

- [x] $(10)_2^{(33)_{10}} \leq 2^{(100001)_2}$
- [ ] Sachant qu'un gigaOctet est plus petit qu'un GibiOctet, $9 \cdot (10^9)_{10} \geq 9 * (10)_2^{(30)_{10}}$
- [x] $(100)_2^{(100)_{10}} > 4^4$
- [ ] Sachant qu'un TeraOctet est plus petit qu'un TebiOctet $10^{-12} \leq (10)_2^{-40}$

Question 35 Cochez les bonnes réponses

- [ ] $(110010)_2 = (B2)_{16}$
- [ ] $(1100010)_2 = (82)_{16}$
- [x] autre

Question 36 Quel est le plus grand nombre entier que l'on peut représenter en CA2 sur 16 bits ?

- ■ $(\underbrace{11...111}_{16})_2$
- ☐ $(10000...000)_2$
- ■ $2^{16} - 1$
- ☐ 255

Question 37 Quel est le code de -15 en $CA2_8$ sachant que $15 = (1111)_2$

- ☐ [10001]
- ☐ [10000]
- ■ autre

Question 38 Cochez les assertions vraies

- ■ En $CA2_8$ on peut coder 2^8 nombres différents
- ■ En $CA1_{16}$ on peut coder $2^{16} - 1$ nombres différents

Question 39 De quel nombre [01100101] est-il le code en $CA2_8$?

- ☐ -(1+4+32+64)
- ☐ -(1+2+8+16)
- ■ autre

Question 40 De quel nombre [10011010] est-il le code en $CA2_8$?

- ☐ Aucun nombre
- ■ Un nombre négatif
- ■ Le nombre qu'on obtient si on inverse tous les bits, puis on ajoute 1 en binaire, puis on décode en binaire, puis on met le signe "-"
- ☐ Le nombre qu'on obtient si on inverse tous les bits, puis on décode en binaire, puis on met le signe "-"
- ■ Le nombre qu'on obtient si on retranche 1 en binaire, puis on inverse tous les bits, puis on décode en binaire, puis on met le signe "-"

Question 41 On fait l'addition de $(100001010100000010101010101010)_2$ et $(111001010100000010101010101010)_2$ (ces deux nombres ont 30 chiffres) en $CA2_{31}$. Y'a-t-il overflow ?

- ■ oui
- ☐ non

Question 42 Quel est le codage $CA2_8$ du plus grand nombre entier que l'on peut représenter en $CA2_8$?

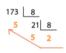
- ☐ 11111111
- ■ 01111111
- ☐ 00000001

Question 43 Combien de nombres à 3 chiffres (ou moins) y'a-t-il en base 8 ?

- [ ] 8^2
- [ ] 24
- [ ] 3*7
- [x] 8^3

Question 44 Comment s'écrit $(172)_{10}$en base 2 ?

- [x] $(10101100)_2$
- [ ] $(10011010)_2$
- [ ] autre

Question 45 En utilisant 

, que peut-on dire?

- [ ] $(552)_{10} = (173)_8$
- [ ] $(173)_{10} = (552)_8$
- [x] $(173)_{10} = (255)_8$
- [ ] $(255)_{10} = (173)_8$

Question 46 Combien vaut 137 en base 3 ?

- [ ] 20021
- [ ] 22002
- [ ] 20022
- [x] autre

Question 47 Est-ce que $(37,8543)_9$ est une approximation de $(37,85439878)_9$ à 10^{-4} près

- [ ] oui
- [x] non

Question 48 Cochez les assertions vraies

- [x] $(132,43)_5 = (132,4329)_5$ à 10^{-1} près
- [ ] $(132,43)_5 = (132,4329)_5$ à 5^{-3} près
- [ ] $(132,43)_5 = (132,4329)_5$ à 10^{-2} près
- [x] $(132,43)_5 = (132,4329)_5$ à 5^{-2} près

Question 49 On stocke les réels dans un système (signe-exposant-manitsse) avec exposant biaisé. On donne les nombres suivant par leur codage dans ce système :
x :(1-110-11001011)
y :(1-101-11001011)
z :(1-101-11000011)
Classez ces nombres du plus petit au plus grand

- [x] x<y<z
- [ ] z<y<x
- [ ] z<x<y
- [ ] y<x<z

Question 50 Cochez au moins une réponse

- ■ $1234567890 > 10^9$
- ■ $(1011101011)_2 < 2^{10}$

Question 51 Quelles inégalités sont vraies

- □ $9,99 * 10^{98} > 99,9 * 10^{97}$
- ■ $84 * 10^{127} < 12 * 10^{128}$

Question 52 On considère un alphabet de 44 symboles pour lequel on veut construire un code binaire

- ■ Si on choisit un code de longueur fixe il faudra 6 bits
- □ Un code de Huffman sera forcément strictement mieux qu'un code de longueur fixe
- □ Si on donne un code de longueur 5 a 20 des symboles, il faudra des codes de longueur 7 pour les symboles restants
- □ Il se peut que le code de longueur fixe soit strictement mieux que le code de Huffman adapté aux probabilités d'apparition de chaque symbole, en terme de longueur moyenne

Question 53 On considère un code de Gray sur 8 bits qui code les entiers de 0 à 255.

- □ Il est possible que 124 soit codé par 11100111 et 126 par 11011111
- ■ Le successeur de 10011001 peut être 00011001
- □ 255 est codé par 11111111 et 0 par 00000000

Question 54 On considère un code binaire de longueur fixe égale à 4 dont le dernier bit (à droite) est un bit de parité

- □ On peut dire qu'il y a une erreur de transmission dans le message 0101001111110110
- ■ Ce code peut coder un alphabet de 8 mots maximum
- □ Si je détecte une erreur dans un message transmis via ce code, je saurai comment la corriger

Question 55 Parmi les codes suivants, indiquez ceux qui sont sans perte

- ■ Le code où une (longue) séquence de 0 et de 1 est remplacé par un code qui contient le nombre de 0 à la suite (en binaire sur 8 bits), puis le nombre de 1 à la suite (en binaire sur 8 bits), puis le nombre de 0 à la suite, etc...
- □ Le codage musical MP3
- ■ Le code de Huffman

Question 56 Cochez les assertions vraies

- □ Lorsque l'on utilise un code préfixe, il faut mettre un séparateur entre chaque mot (par exemple un espace), pour que la personne qui reçoit le message codé sache exactement où commence et où s'arrête chaque mot
- □ Le code Morse (où par exemple E est codé par le signal "court" et T est codé par le signal "long") est un code préfixe
- □ On considère un alphabet à 10 lettres codées par les codes $1, 0001, 0010, 0011, 0111, 010, 001111, 01, 0010101010, 00000000$ Est-ce un code préfixe ?
- ■ On peut utiliser un code binaire préfixe où tous les codes ont une longueur ≤ 3 pour coder l'alphabet $\{A, E, I, O, U\}$

Question 57 cochez les assertions exactes

- [ ] Le code de Huffman donne un résultat satisfaisant, mais au cas par cas on peut peut-être trouver un code qui a une longueur moyene strictement plus courte
- [ ] L'un des principes du code de Huffman est d'affecter un code plus court aux symboles les moins probables
- [ ] Si un alphabet a 4 symboles, le code de Huffman correspondant peut être 01,001,101,100
- [x] Le code de huffman est un code préfixe

Question 58 Le biaisage d'exposant en $CA2_k$ consiste à

- [x] ajouter 2^{k-1} en binaire aux codes de nombres positifs et soustraire 2^{k-1} en binaire aux codes de nombres négatifs
- [x] Inverser le bit de signe
- [ ] Décaler tous les bits d'un cran et mettre le bit de droite tout à gauche

Question 59 On utilise le procédé du bit caché dans un système binaire de stockage des réels où 12 bits sont alloués à la mantisse. Cochez les affirmations vraies.

- [ ] On peut coder 2^{13} mantisses différentes
- [ ] Un code de la forme [0|???|100011011101] code pour un nombre de la forme $(0,100011011101)_2 \cdot 2^?$
- [x] Le plus grand nombre qu'on peut coder a $(0,1111111111111)_2$ comme mantisse

Question 60 Soit x un nombre codé dans un système binaire avec 8 bits d'exposant biaisé. On suppose que le code de son exposant commence par 0. On appelle e le nombre décimal qui représente l'exposant

- [x] l'exposant est négatif
- [x] x<1
- [ ] e est compris entre -127 et +128
- [x] Pour obtenir la valeur absolue de e il faut changer le bit de signe, puis inverser tous les bits, puis ajouter 1, puis décoder le nombre binaire obtenu

Question 61 Soit un système binaire de stockage des réels avec 8 bits d'exposant et 31 bits de mantisse. Soit m la mantisse d'un nombre codé dans ce système ($x = m \cdot 2^{exposant}$)

- [x] Le meilleur encadrement à priori est $0,5 \leq m < 1$ (sans bit implicite)
- [ ] Le meilleur encadrement à priori est $0 \leq m < 1$ (avec bit implicite)
- [x] On peut avoir $m = 0$

Question 62 On rappelle que dans un système de stockage des nombres réels la précsion au niveau d'un nombre x est la différence entre x et son successeur

- [ ] Dans un certain système binaire, la précision au niveau de 1 est la même qu'au niveau de 2
- [x] Dans un certain système binaire, la précision au niveau de $(0,1)_2 * 2^{127}$ est la même qu'au niveau de $(0,111111101)_2 * 2^{127}$
- [ ] Si il y a 23 bits de mantisse, la précision au niveau de $(0,111) * 2^{10}$ est de $2^{10-4} = 2^6$
- [x] Il peut y avoir des nombres pour lesquels la précision est de 1000

Question 63 Soit x un nombre ayant un développement binaire infini. On appelle x' sa valeur stockée en machine dans un système avec 8 bits de mantisse et 6 bits d'exposant, sans bit implicite. On suppose que' $x = m \cdot 2^{-4}$ où m est la mantisse.

- [x] L'incertitude sur x est 2^{-12}
- [x] Soit $y = -2^{-3} \pm 2^{-13}$. Alors il y a une incertitude de $3 \cdot 2^{-16}$ sur xy

Question 64 On considère le nombre x codé par [1|11101|110010100101] dans un système binaire de stockage des réels, avec exposant biaisé

- [x] Le successeur de x est codé par [1|11101|110010100100]
- [x] La précision autour de x, c'est-à-dire l'écart entre x et son successeur, est de 2 (on suppose qu'il n'y a pas de bit caché)
- [x] On suppose qu'il y a un bit implicite. La précision autour de x, c'est-à-dire l'écart entre x et son successeur, est de 1.

Question 65 On travaille dans un système de stockage binaire avec mantisse sur 12 bits et exposant biaisé sur 8 bits. Cochez les cases si le test donne "vrai"

- [x] $x = 42,1$ et $y = 42,1$. Test : $if(x == y)$
- [x] $x = 7/3$. Test : $ifabs(3 \cdot x - 7) < 0,01$ (note : "abs" représente la valeur absolue)
- [x] $x = 111/32$. $if(32 \cdot x == 111)$
- [ ] $x = 11/7$. if$(7 * x == 11)$

Question 66 Soit un système binaire de stockage des réels. Soit x le nombre dont le code est [0|1100|11111111]. Soit y le successeur de x

- [ ] Le code de l'exposant de y dépend du fait qu'on utilise la technique du bit implicite
- [x] Le code de y dépend du fait qu'on utilise un exposant biaisé ou pas
- [ ] $y - x$ est de l'ordre de 2^{-12} (avec exposant biaisé)
- [ ] $y - x$ est de l'odre de 2^{-8} (avec exposant biaisé)

Question 67 Aujourd'hui c'est mon 20ème anniversaire, et nous sommes lundi. On donne $365 \equiv 1[7]$.

- [x] Je suis né un jeudi
- [x] Dans exactement 28 ans, on sera encore un lundi
- [ ] Il faut savoir si je suis né une année bissextile ou pas pour répondre à l'une ou l'autre des deux autres questions

Question 68 Cochez

- [ ] L'inverse de 9^{18} dans F_{37} est 3
- [ ] Sans faire de calculs, on peut affirmer que $1245^{32450} \equiv 1$ dans F_{32451}
- [ ] Pour tout p premier, et $x > p$ un nombre entier,$p^x \equiv 1[x]$
- [x] Le théorème de Fermat sert dans l'algorithme RSA

Question 69 Inverses :

- [ ] A part 0, tous les éléments de F_9 ont un inverse
- [ ] Dans F_6, un élément peut avoir plusieurs inverses
- [x] Soit x, x' deux éléments non-nuls de F_p, ou p est un entier, et y, y' leurs inverses. Alors xx' est l'inverse de yy' dans F_p
- [x] L'inverse de 2^{26} est 16 dans F_{31}

Question 70 Soit p un entier, et a, b, a', b' d'autres entiers. On suppose que $a \equiv a'$ et $b \equiv b'$ modulo p

- [x] On a $a - b \equiv a' - b'$ modulo p
- [ ] Si $ab \equiv ab'$ alors $b \equiv b'$
- [ ] Pour tout entier positif k, $k^a \equiv k^{a'}$
- [x] Pour tout entier positif k, $a^k \equiv (a')^k$

Question 71 On considère un code RSA. On donne $17 \cdot 11 = 187$

- [ ] Il est possible que $(77, 12)$ soit la clé publique
- [ ] Il est possible que $(63, 11)$ soit la clé publique
- [x] Il est possible que $(187, 9)$ soit la clé publique

Question 72 cryptographie

- [ ] Des algorithmes de cryptage modernes se basent sur le fait qu'il est difficile de savoir si un grand nombre est premier ou pas
- [x] Des algorithmes de cryptage modernes se basent sur le fait qu'étant donné deux très grand nombres premier p et q, et n=pq , il est difficile de trouver p et q a partir de n
- [ ] Etant donné une méthode de cryptage basée sur des nombres premiers, il est complètement impossible de le décrypter si on n'a pas les codes, meme avec un ordinateur infiniment puissant

Question 73 On considère un code RSA basé sur deux grands nombres premiers p et q, avec n=pq et $\phi = (p-1)(q-1)$

- [ ] Pour coder un message, on a besoin de la clé privée
- [x] La code est dur à casser car il est dur de trouver p et q à partir de $n = pq$
- [ ] d est l'inverse de e modulo n

Question 74 On considère un code RSA. On donne $31 \cdot 60 \equiv 1[143]$.

- [ ] La clé publique est $(143, 31)$. Alors la clé privée est 60
- [x] On admet que si la clé publique est $(12268044787, 43350051)$, alors la clé privée est 927662347. Si la clé publique était $(12268044787, 927662347)$, la clé publique serait 43350051 ?
- [ ] Pour trouver la clé privée connaissant la clé publique, il faut juste calculer l'inverse d'un nombre modulo un autre nombre connu
- [ ] Si je ne connais que la clé privée d mais pas la clé publique, je peux trouver e

Question 75 Système complet

- [x] Toute formule écrite à l'aide des opérateurs $\vee\wedge, \neg, \rightarrow\leftrightarrow$ est équivalente à une formule qui ne fait intervenir que $\vee, \wedge, \neg$
- [ ] Toute formule écrite à l'aide des opérateurs $\vee, \wedge, \neg, \rightarrow$ est équivalente à une formule qui ne fait intervenir que $\vee, \wedge, \neg$ mais on ne peut pas retirer d'autre opérateur
- [ ] Toute formule écrite à l'aide des opérateurs $\vee, \wedge, \neg$ est équivalente à une formule qui ne fait intervenir que $\vee, \wedge$
- [x] Toute formule écrite à l'aide des opérateurs $\vee, \wedge, \neg$ est équivalente à une formule qui ne fait intervenir que $\rightarrow, \neg$

Question 76 Soit a, b, c des variables propositionelles

- ■ $a \vee b$ est sous FNC
- ■ $a \vee b$ est sous FND
- ■ $(a \vee b) \wedge c$ est sous FNC
- □ $(\neg a \wedge b) \vee (c \wedge \neg b) \vee \neg(c \wedge b)$ est sous FND

Question 77 On considère la formule $F = (a \vee b) \to \neg[(p \to q) \to (a \to q)]$. On dresse son tableau de Karnaugh pour la simplifier.

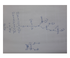
- □ On peut utiliser les colonnes 00,01,11,10 et les lignes 00,01,10,11
- □ On peut utiliser les colonnes 00,01,11,10 et les lignes 1,0
- □ le tableau de Karnaugh nous donnera la formule équivalente la plus compacte possible
- ■ Pour trouver la FNC il faut entourer les "0"

Question 78 Soit $a, b, c, p, q, r, x, y, z$ des variables propositionelles

- ■ $a \vee \neg a$ est une tautologie
- ■ $\neg(p \to (q \to p))$ est une antilogie
- ■ On peut savoir si une formule est une tautologie en faisant sa table de vérité
- □ Toute formule est forcément une tautologie ou une antilogie

Question 79 Cochez

- □ Toute formule est équivalente à une tautologie
- □ La formule $\neg(p \vee q)$ est équivalente à $(\neg p) \wedge (\neg q)$, ce qui se note $\neg(p \vee q) \leftrightarrow (\neg p) \wedge (\neg q)$
- ■ $(a \wedge b) \to a$ est une tautologie
- □ $(a \wedge b) \leftrightarrow a$ est une tautologie

Question 80  On considère l'arbre de Beth de la formule $F = [A \vee \neg D] \wedge [A \vee B \to C] \wedge [\neg[C \leftrightarrow \neg(A \leftrightarrow B)]] \wedge [\neg(A \to (C \to \neg B))] \wedge [D]$

- ■ On a $F \ \underline{eq}\ (A \wedge B \wedge C)$
- ■ Il y a une manière plus simple de développer cet arbre
- □ Le développement est terminé
- □ Cet arbre permet de savoir si D est une déduction de $\{A \vee \neg D, A \vee B \to C, \neg[C \leftrightarrow \neg(A \leftrightarrow B)], \neg(A \to (C \to \neg B))\}$

Question 81 On considère un circuit qui prend un nombre en $CA2_8$ et renvoie en binaire la valeur absolue du nombre qu'il code

- ■ Il y a autant de sorties que d'entrées.
- □ On appelle s la sortie correspondant au bit de poids fort, et on trace le tableau de Karnaugh. On regroupe les 1 de manière optimale, ce qui fait en tout 4 regroupements.
- □ On appelle s la sortie correspondant au bit de poids faible, et $e_1, e_2, ..., e_8$ les entrées (e_1: bit de signe). On a $s \ \underline{eq}\ \neg(e_1 \leftrightarrow e_8)$.

Question 82 On considère un circuit qui fonctionne de la manière suivante : Etant donné deux nombres binaires de 8 bits, il renvoie (en binaire) le nombre de bits à changer pour passer du 1er au 2ème nombre (exemple : pour passer de 10011101 à 10111001 il faut changer 2 bits). On trace les tableaus de Karnaugh de toutes les sorties. On appelle n le nombre de cases de chaque tableau

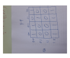
- [ ] Si on trace les tableaux de Karnaugh de toutes les sorties, on aura dessiné en tout $8n$ cases
- [ ] n=64
- [x] Si les entrées sont 11111111 et 10101010 alors le bit de poids faible de la sortie sera 0
- [x] On veut dessiner le circuit logique de la sortie correspondant au bit de poids fort. On suppose qu'on n'a pas de portes "OU", qu'on dispose d'un nombre illimité de portes logique binaires "=", qui donnent en sortie 1 si les entrés sont égales, et 0 autrement, et un certain nombre de portes binaires "ET" (ces portes ne peuvent prendre que 2 entrées à la fois). Le nombre de portes binaires "ET" nécessaire pour terminer le circuit est de 15, mais pas moins.

Question 83 On veut coder le circuit logique de la fonction qui prend en argument deux nombres en base 7 et renvoie le résultat de leur produit modulo 7. Tous les nombres sont codés en binaire. On ne dispose que de portes ET et de portes OU qui peuvent prendre deux entrées à la fois (et pas 3 ou plus)

- [ ] Il y a $2 \cdot 2^3$ entrées et 2^3 sorties
- [x] Si l'on trace le tableau de Karnaugh de chaque sortie en fonction des entrées, il faut faire 3 tableaux de 64 cases chacun
- [ ] On obtient pour la 3ème sortie une FND avec 5 termes. On peut donc construire le circuit à partir de 5 portes OU et un nombre suffisant de portes ET.
- [x] En appelant s_1, s_2, s_3 les sorties, et $e_1, e_2, e_3, ...$ les entrées, on a $\bar{s}_1\bar{s}_2\bar{s}_3 = \bar{e}_1\bar{e}_2\bar{e}_3 + \bar{e}_4\bar{e}_5\bar{e}_6$

Question 84 On considère un circuit qui prend en entrée une lettre codée par un nombre binaire à 5 bits entre 0 et 25 (A=0,B=1,C=2, etc...) et donne en sortie le bit 1 si c'est une voyelle et 0 sinon. (On note que les voyelles sont les 1re, 5ème, 9ème, 15ème, 21, et 25ème lettres de l'alphabet). Faites le tableau de Karnaugh correspondant.

- [ ] Le tableau de Karnaugh peut avoir 3 lignes et 2 colonnes (ou l'inverse)
- [x] On remarque que 0,4,8,20, et 24 sont des multiples de 4. Cela implique que les 1 du tableau de Karnaugh correspondants à A,E,I,Y,U sont tous sur la même ligne (ou la même colonne)
- [ ] On ne peut pas faire mieux que 6 regroupements de 1
- [x] On appelle a,b,c,d,e les 5 entrées conrrespondant aux 5 bits. Alors la sortie est équivalente à $[((\bar{a} + c)\bar{b} + b\bar{c})\bar{d} + \bar{a}bcd]\bar{e}$

Question 85  On considère le tableau de Karnaugh

- [x] En faisant les regroupements optimaux de 1, on obtient 4 groupes
- [ ] La FND obtenue (sans simplifier ou factoriser) via les regroupements optimaux est $\bar{p}\bar{s} + pq\bar{r}s + pq\bar{r}s + r\bar{s}$
- [x] La FNC obtenue (sans simplifier ou factoriser) via les regroupements optimaux est $(p + \bar{s}) \cdot (q + \bar{s}) \cdot (\bar{r} + \bar{s}) \cdot (\bar{p} + \bar{q} + r + s)$
- [ ] En faisant les regroupements optimaux de 0, on obtient 3 groupes

Question 86 Un crime a été commis et les coupables se cachent parmi les 4 suspects : A,B,C,D. On note a="A est coupable", b="B est coupable", etc..

- [ ] "Peut-être que A ou B est coupable mais pas les 2 en même temps" se traduit par $(a \vee b) \wedge \neg(a \wedge b)$
- [x] "Il y a au plus deux coupables" se traduit par $\neg[(a \wedge b \wedge c) \vee (a \wedge c \wedge d) \vee (a \wedge b \wedge d) \vee (b \wedge c \wedge d)]$
- [x] On sait que A n'agit jamais sans B, B jamais sans C, C jamais sans D, et D jamais sans A. Donc $a \wedge b \wedge c \wedge d$ est vrai
- [ ] "A agit toujours seul, B toujours avec un seul complice, et C toujours avec 2 complices" se traduit par $a \vee (b \wedge d) \vee (c \wedge d \wedge b)$

Question 87 Notation polonaise

- [x] La formuleKCxANyzNCKyzAKxyNz en notation polonaise signifie $([x \rightarrow (\neg y \vee z)] \wedge \neg[((y \wedge z) \rightarrow ((x \wedge y) \vee \neg z))]$
- [ ] La formule KCNxyCKzyxwAKtwz est correcte car si on compte +1 pour chaque connecteur binaire, -1 pour chaque variable, et 0 pour chaque "N", on trouve -1
- [x] La formule NAxy est équivalente à KNxNy
- [x] La formule KACNxyNcKNNxy a une signification

Question 88 Arbres de Beth

- [x] Un arbre de Beth complètement développé permet de donner une expressions plus simple
- [ ] Il n'y a qu'une manière de développer un arbre de Beth
- [x] Il n'y a pas forcément besoin de développer tout l'arbre pour dire qu'une formule n'est pas une antilogie
- [ ] Pour montrer qu'une formule est une tautologie, il faut montrer que toutes les brancehs de son arbre de Beth sont fermées