Exercice n° 1

1. MUBC
2. FOURIER
3. (a) JAIME+COVID=LODUH,
   MONMA+COVID=OCIUD,
   SQUEL+COVID=UEPMO,
   AVABL+COVID=CJVJO,
   E+C=G

   (b) *On note* `T[i]` *l'entier donné par le tableau de correspondance pour la lettre d'indice i du texte à chiffrer,* `C[i]` *l'entier donné par le tableau de la lettre d'indice i de la clé et* `CH[i]` *l'entier donné par le tableau de la lettre d'indice i du texte chiffré. On utilise des indices commençant à 0. Comment obtient-on la liste des* `CH[i]` *à partir de la liste des* `T[i]` *et de la liste* `[C[0],C[1],···,C[4]]` *?*
   `CH[i]=(T[i]+C[i%5])%26`

   (c) *Combien de chiffrements différents peut-on obtenir avec des clés de 5 lettres ?*
   26 choix possibles pour chaque lettre donc $26^5 = 11881376$ choix.

   (d) *Quelle(s) méthode(s) peut-on utiliser pour casser un tel chiffrement si on ne connait pas la clé ?*
   Si on sait que la clef est de longueur 5 et le message assez long, on peut faire une analyse statistique des lettres d'indice 0 modulo 5, puis 1 modulo 5, etc. pour retrouver chaque lettre de la clef. On peut aussi faire une attaque par force brute en testant toutes les clefs possibles (un peu plus de 11 millions de possibilités). Si on ne connait pas la longueur de la clef, on peut essayer une attaque statistique ou par force brute en testant pour une clef de 1 lettre, puis de 2 lettres, puis de 3 lettres, etc. L'attaque par force brute ne peut s'envisager que pour une clef d'au plus une douzaine de lettres.

   (e) *Écrire un algorithme en langage naturel qui à un texte (composé uniquement des lettres A à Z) et une clé associe le texte chiffré par la méthode précédente. On supposera que*
   — *le caractère d'indice i d'une chaine de caractère* `s` *est* `s[i]`*, avec des indices commençant à 0,*
   — *la fonction* `len(s)` *renvoie la longueur de la chaine* `s`
   — *la fonction* `ord(c)` *convertit un caractère* `c` *en entier*
   — *la fonction* `chr(n)` *convertit un entier* `n` *en caractère*

```
fonction codage d'arguments msg,cle
l <- len(cle)
n <- len(msg)
msgcode <- msg
pour j de 0 jusque n-1 faire
  msgcode[j]=chr((ord(msg[j])+ord(cle[j%l]))%26)
renvoyer msgcode
```

   Code Python/Xcas correspondant (un peu plus compliqué car les caractères ne commencent pas à 0) :

```
def code(msg,cle):
    l=len(cle)
    n=len(msg)
    msgcode=""
    for j in range(n):
        msgcode += chr((ord(msg[j])-ord("A")+ord(cle[j%l])-ord("A"))%26 +ord("A"))
    return msgcode
```

   On teste : `code("JAIMEMONMASQUELAVABLE","COVID")` renvoie LODUHOCIUDUEPMOCJVJOG.

Exercice n° 2

On rappelle qu'en base 16 les chiffres sont donnés par `0,1,···9,A,B,C,D,E,F`.

1. `0,0b1,0b10,0b11, 0b100, 0b101, 0b110, 0b111`, etc.
2. *Chiffrer de cette manière le mot* **COVID**.
   `10 1110 10101 1000 11` soit en groupant par quatre `1 0111 0101 0110 0011=0x17563`
   Proposer un autre mot ayant le même chiffrement.
   Par exemple `101 110 10101 1000 11` soit **FGVID**

3. *Pour corriger le défaut de la méthode précédente on écrit tous les nombres de 0 à 25 en base 2 avec 5 bits (en ajoutant des 0 au début si nécessaire). On le convertit ensuite en base 16.*

   Chiffrer de cette manière le mot **COVID**.

   `00010 01110 10101 01000 00011` soit `0x275503`

4. *Notons n le chiffrement du mot COVID obtenu à la question précédente. Donner le quotient et le reste, en base 16, de la division euclidienne de n par 6. On utilisera l'algorithme de la potence. Pour s'aider, on pourra écrire la table de multiplication par 6 en base 16.*

	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
*6	6	c	12	18	1e	24	2a	30	36	3c	42	48	4e	54	5a

```
 275503 | 6
-24     |--------
---     | 68e2b
  35    |
 -30    |
 ---    |
   55   |
  -54   |
  ---   |
    10  |
    -c  |
    --  |
     43 |
    -42 |
    --- |
      1 |
```

   On obtient quotient `0x68e2b`, reste 1.

Exercice n° 3

1. *Montrer que 2020 et 33 sont premiers entre eux et donner l'identité de Bézout. On détaillera les calculs en utilisant l'algorithme d'Euclide étendu.*

```
L0           2020   1    0
L1             33   0    1
L2=L0-61L1      7   1  -61
L3=L1-4L2       5  -4  245
L4=L2-L3        2   5 -306
L5=L3-2L4       1 -14  857
```

   Donc `-14*2020+857*33=1`

2. *Déterminer tous les couples d'entiers* (x, y) *tels que* $2020x - 33y = 3$.

   on multiplie par -3 l'identité de Bézout pour avoir une solution particulière $x = -42, y = -2571$ et on utilise que 2020 et 33 sont premiers entre eux pour avoir la solution générale $x = -42 + 33k, y = -2571 + 2020k$

3. *Existe t-il des entiers x positifs et plus petit que 20000 tels que le reste de la dision euclidienne de x par 33 soit 1 et le reste de la dision euclidienne de x par 2020 soit 4 ? Si oui, donner toutes les solutions.*

   Comme 33 et 2020 sont premiers entre eux, x existe parmi les entiers, mais pas forcément entre 0 et 20000. Comme la longueur de l'intervalle des x possibles est 20001 qui est plus petit que 2020×33, il y aura 0 ou 1 solution, on ne peut pas le savoir sans faire le calcul précis.

   On a $x = 1 + 33v = 4 + 2020u$ donc $-2020u + 33v = 4 - 1 = 3$ dont on a calculé des solutions (au signe près) juste avant, par exemple $v = 2571$ On a donc une solution particulière $x = 1 + 33 \times 2571 = 84844$ et la solution générale $x = 84844 + 2020 \times 33k$. Reste à déterminer k, on a :

$$0 \leq x = 84844 + 66660k \leq 20000 \quad \Leftrightarrow \quad \frac{-84844}{66660} \leq k \leq \frac{20000 - 84844}{66660}$$

   donc $k = -1$ et $x = 18184$. On vérifie que x convient.

Exercice n° 4

1. *Déterminer le reste de la division euclidienne de* 2020^{873} *par 14. La méthode doit être explicitée.*
   On divise 2020 par 14, il reste 4, donc on calcule 4^{873} mod 14. On calcule les carrés successifs de 4 mod 14, on obtient mod 14
   $$4^1 = 4, 4^2 = 2, 4^{2^2} = 2^2 = 4, 4^{2^3} = 4^2 = 2...$$
   Comme `873=0b1101101001`, les bits à 1 d'indice pair (indices commençant à 0) contribuent à un facteur 4 et les bits à 1 d'indice impair à un facteur 2, on a modulo 14 :
   $$4^{873} = 4 \times 2 \times 2 \times 4 \times 4 \times 2 = 8$$
   Résultat : 8
   Autre méthode : Pour calculer 4^{873}, on peut observer que $4^4 = 16^2 = 2^2 = 4$ modulo 14. Attention, on ne peut pas simplifier par 4 qui est un diviseur de 0 modulo 14, $4^3 \neq 1$ modulo 14. Donc $4^{1+3k} = 4$ modulo 14, donc
   $$4^{873} = 4^2 \times 4^{1+3\times 290} = 4^2 \times 4 = 8 \pmod 14$$
2. *Donner la liste des inversibles de* $\mathbb{Z}/14\mathbb{Z}$*.*
   Comme $14 = 2 \times 7$, ce sont les classes des entiers premiers avec 2 et 7 : $\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}$
3. *Résoudre l'équation dans* $\mathbb{Z}/14\mathbb{Z}$*,* $\overline{11}x = \overline{3}$*.*
   L'équation a une solution unique puisque 11 est inversible modulo 14.
   Si on voit que $\overline{3} = \overline{-11}$, on trouve immédiatement $x = \overline{-1}$. Sinon, on peut aussi obtenir x rapidement, comme on veut inverser 11 modulo 14, on cherche l'identité de Bézout sur 11 et 14, or la première division euclidienne de l'algorithme d'Euclide donne la relation 14-11=3 donc modulo 14 on a $\overline{11} \times \overline{-1} = \overline{3}$ et $x = \overline{-1} = \overline{13}$.
   Si on ne le voit aucune de ces astuces, on utilise la méthode standard
   ```
   L0          14  1  0
   L1          11  0  1
   L2=L0-L1     3  1 -1
   L3=L1-3L2   2 -3  4
   L4=L2-L3    1  4 -5
   ```
   Donc l'inverse de $\overline{11}$ est $\overline{-5}$, on multiplie par $\overline{3}$, on obtient $\overline{-15} = \overline{13}$.

Exercice n° 5 On considère l'équation suivante :

$$(*) \qquad x^2 - 13y^2 = 7$$

On suppose dans les questions 1 et 3 que (x, y) est un couple d'entiers vérifiant $(*)$.

1. *Montrer que* $x^2 + y^2 \equiv 0$ $[7]$
   En effet, -13=1 et 7=0 modulo 7
2. *Calculer les carrés de tous les éléments de* $\mathbb{Z}/7\mathbb{Z}$*.*
   Modulo 7, on a $0^2 = 0, 1^2 = 6^2 = 1, 2^2 = 5^2 = 4, 3^2 = 4^2 = 2,$
3. *En déduire que x et y sont multiples de 7.*
   Si on somme deux à deux les carrés non nuls $1 + 1 = 2, 1 + 4 = 5, 1 + 2 = 3, 4 + 4 = 1, 4 + 2 = 6, 2 + 2 = 4$ on n'obtient jamais 0, donc la seule possibilité d'obtenir 0 est de sommer $0 + 0 = 0$ donc x et y sont multiples de 7.
   Autre méthode : on vérifie que -1 n'est pas un carré modulo 7 (soit en regardant la table des carrés, soit en calculant $(-1)^{(7-1)/2} \neq 1$ mod 7)
4. $(*)$ *a-t-elle des solutions ? Indication : si c'est le cas, il existe des entiers a et b tels que :*
   $$x = 7a, y = 7b$$
   On a donc $7^2a^2 - 13 \times 7^2b^2 = 7$ on simplifie par 7, $7(a^2 - 13b^2) = 1$ ce est impossible car 7 ne divise pas 1. Donc il n'y a pas de solutions.