Devoir surveillé 4 : solutions

1 Première partie : informatique et mathématiques

1.1 Autour de la suite de Fibonacci modulaire

a) (i)
```
def Fibo1(n):
    if n<=1:
        return n
    else:
        f0,f1=0,1
        for i in range(n-1):
            f0,f1=f1,f0+f1
        return f1
```
(ii)
```
def Fibo2(n):
    L=[0]
    if n>=1:
        L.append(1)
    if n>=2:
        for i in range(2,n+1):
            L.append(L[i-2]+L[i-1])
    return L
```
b) On fixe maintenant un entier naturel $m \in \mathbb{N}_{\geq 2}$ et on considère la suite $(\overline{F_n}) \in (\mathbb{Z}/m\mathbb{Z})^{\mathbb{N}}$ où $\overline{F_n}$ est la classe de F_n dans $\mathbb{Z}/m\mathbb{Z}$.

(i)
```
def Fibo3(n,m):
    if n<=1:
        return n
    else:
        f0,f1=0,1
        for i in range(n-1):
            f0,f1=f1,(f0+f1)%m
        return f1
```

N.B. Il vaut beaucoup mieux calculer `%m` à chaque étape, que de prendre le modulo `m` seulement à la fin.

(ii) C'est immédiat $\overline{F_2} = \overline{1}$, $\overline{F_3} = \overline{1} + \overline{1} = \overline{0}$, $\overline{F_4} = \overline{1}$. Comme $(\overline{F_3}, \overline{F_4}) = (\overline{F_0}, \overline{F_1})$ et que la suite est récurrente d'ordre 2, on sait sûr que la suite est 3-périodique.

(iii) Comme $\mathbb{Z}/m\mathbb{Z}^2$ est fini de cardinal m^2, les couples (F_k, F_{k+1}) ne peuvent prendre que m^2 valeurs. Il existe donc un entier n et un entier p avec $p > 0$ tels que $(F_{n+p}, F_{n+p+1}) = (F_n, F_{n+1})$.
Mais comme pour tout k, $F_k = F_{k+2} - F_{k+1}$, on déduit de l'égalité précédente que $F_{n-1} = F_{n+p-1}$ et ainsi par récurrence descendante immédiate que $F_0 = F_p$ et $F_1 = F_{p+1}$. Autrement dit, aux rangs $(p, p+1)$, on est revenu à la même situation qu'aux rangs $(0, 1)$ donc la suite est p périodique.

(iv)
```
def periode(m):
    i=1
    while Fibo3(i,m)!=0 or Fibo3(i+1,m)!=1:
        i=i+1
    return i
```

c) Avec le théorème Chinois : comme $2 \wedge 5 = 1$, $(F_n, F_{n+1}) \equiv (0,1)\,[10] \Leftrightarrow (F_n, F_{n+1}) \equiv (0,1)\,[2]$ et$(F_n, F_{n+1}) \equiv (0,1)\ [5]$. Par le résultat précédent pour $m = 2$ et $m = 5$ on a alors $(F_n, F_{n+1}) \equiv (0,1)\,[10] \Leftrightarrow 3|n$ et $20|n$.

Comme 3 et 20 sont aussi premiers entre eux, on a la conclusion :

$(F_n, F_{n+1}) \equiv (0,1)\,[10] \Leftrightarrow 60|n$.

1.2 Autour de la courbe du dragon (barème I.P.T. seulement)

1.2.1 Tracés de lignes polygonales à partir des angles successifs

a) La relation de l'énoncé (module et arguments) donne que $\dfrac{z_{k+1} - z_k}{z_k - z_{k-1}} = e^{ia_k}$.

Donc $z_{k+1} - z_k = e^{ia_k}(z_k - z_{k-1})$.

Par récurrence immédiate $z_{k+1} - z_k = e^{ia_k} e^{ia_{k-1}} \cdots e^{ia_0}(z_0 - z_{-1}) = e^{i\theta_k}$ où $\theta_k = a_k + a_{k-1} + \cdots + a_0$.

D'où la formule demandée.

b)
```
def trace(a):
    plt.clf()
    theta=[a[0]]
    # remplissage du tableau des thetas
    for i in range(1,len(a)):
        theta.append(theta[-1]+a[i])
    # remplissage du tableau des z
    z=[complex(1,0)]
    for i in range(1,len(a)):
        #z.append(theta[i])
        z.append(z[-1]+np.exp(np.complex(0,theta[i-1])))
        #print(z)
    X=np.real(z)
    Y=np.imag(z)
    print(X)
    plt.plot(X,Y)
    plt.show()
```

c) Il suffit de tourner d'un angle constant égal à $2\pi/n$. Autrement de passer en argument à la fonction `trace` le tableau `a=[2*np.pi/n]*n`.

Pour n assez grand, on voit un cercle !

1.2.2 Application à la courbe du dragon

```
def dragon(n):
    T=[1]
    for i in range(n):
        T=iter(T)
    return T

def iter(L):
    T=[1]
    for i in range(len(L)):
        T.append(L[i])
        T.append(int((-1)**(i-1)))
    return T
```

Remarque : pour tracer la courbe, on a besoin d'avoir le tableau des $\varepsilon_k \pi/2$. On peut faire comme suit ;

```
def mult(L,a):
    """multiplie chaque entrée de L par a"""
    T=[]
    for valeur in L:
        T.append(valeur*a)
    return T
plt.clf()
plt.axis("off")
trace(mult(dragon(3),np.pi/2))
```

2 Seconde partie : homographies du plan complexe

a) On pose $z = x + iy$ avec $(x, y) \in \mathbb{R}^2$ et $A = a + ib$ avec $(a, b) \in \mathbb{R}^2$. Alors $Az = (x + iy)(a + ib)$ et $\mathrm{Re}(Az) = ax - by$.

Alors $c_1|z|^2 + Az + \overline{A}\overline{z} + c_2 = c_1(x^2 + y^2) + 2(ax - by) + c_2$.

• 1er cas : $c_1 = 0$. Alors $z \in \mathcal{E} \iff 2(ax - by) + c_2 = 0$. Si $A \neq 0$, $\mathcal{E}$ est alors une droite.

Si $A = 0$, $\mathcal{E}$ est défini par $c_2 = 0$ donc est ou bien vide si $c_2 \neq 0$ ou bien $\mathbb{C}$ entier.

• 2ème cas : $c_1 \neq 0$. Alors $z \in \mathcal{E} \Leftrightarrow x^2 + y^2 + \alpha x + \beta y + \gamma = 0$ en posant $\alpha = 2a/c_1$, $\beta = -2b/c_1$, $\gamma = c_2/c_1$.

Avec la forme canonique, on conclut que $\mathcal{E}$ est ou bien un cercle, ou bien un point, ou bien vide.

b) Il suffit de le faire pour les droites et les cercles.

• Pour une droite D : $ax + by + c = 0$, en posant $x = (z + \bar{z})/2$ et $y = \dfrac{z - \bar{z}}{2i}$, on a l'égalité : $ax + by + c = a\dfrac{z + \bar{z}}{2} + b\dfrac{z - \bar{z}}{2i} + c = (\dfrac{a}{2} - i\dfrac{b}{2})z + (\dfrac{a}{2} + i\dfrac{b}{2})\bar{z} + c$.

Autrement dit $ax + by + c = Az + \bar{A}\bar{z} + c$ avec $A = (\dfrac{a}{2} - i\dfrac{b}{2})$.

Donc l'équation $ax + by + c = 0$ est bien équivalente à $c_1|z|^2 + Az + \overline{A}\overline{z} + c_2 = 0$ avec $c_1 = 0$, et $c_2 = c \in \mathbb{R}$.

• Pour un cercle $\mathcal{C}$ d'équation $x^2 + y^2 + ax + by + c = 0$. Le calcul précédent pour $ax + by + c$ donne directement le résultat en rajoutant seulement $|z|^2 = x^2 + y^2$.

c) (i) Soit D une droite ne passant pas par 0 : elle admet une équation de la forme $Az + \bar{A}\bar{z} + c = 0$ avec $c \neq 0$. Soit $z' = 1/z$ ce qui est équivalent à $z = 1/z'$.

Le point M d'affixe z est sur D si, et seulement son image M' d'affixe z' vérifie $\dfrac{A}{z'} + \dfrac{\bar{A}}{\bar{z'}} + c = 0$.

Cette équation équivaut à $z' \neq 0$ et $c|z'|^2 + A\bar{z'} + \bar{A}z' = 0 \qquad (*)$

Comme $c \neq 0$, $(*) \Leftrightarrow |z'|^2 + \dfrac{A}{c}\bar{z'} + \dfrac{\bar{A}}{c}z' = 0$.

Par le a), ceci est l'équation d'un cercle $\mathcal{C}$, passant par 0.

A cause de l'*équivalence* $z \in D \Leftrightarrow \begin{cases} z' \in \mathcal{C} \\ z' \neq 0 \end{cases}$, on conclut qu'on a l'égalité d'ensemble $\mathrm{inv}(D) = \mathcal{C} \setminus \{0\}$.

(ii) Le calcul est identique à celui de la question précédente, sauf que $c = 0$. Donc $z \in D \Leftrightarrow A\bar{z'} + \bar{A}z' = 0 \qquad (*)$.

L'équation $(*)$ est l'équation d'une droite D'. L'équivalence montre l'égalité d'ensemble $\mathrm{inv}(D) = D'$.

Remarque : vérifier que D' est la symétrique de D par la réflexion d'axe (Ox).

d) Soient $(a, b, c, d) \in \mathbb{C}^4$ avec $c \neq 0$ vérifiant $ad - bc \neq 0$ et soit $h : z \mapsto \mathbb{C} \setminus \{-d/c\} \to \mathbb{C}$, $z \mapsto \dfrac{az + b}{cz + d}$.

(i) Comme $c \neq 0$ par division euclidienne :

$$\forall z \in \mathbb{C} \setminus \{-\frac{d}{c}\},\ \frac{az+b}{cz+d} = \frac{a}{c} - \frac{ad-bc}{c(cz+d)} = A + \frac{B}{z+C}(*)$$

Donc en posant $t : z \mapsto z+C$ (translation en cplxe), $s : z \mapsto A+Bz$, l'égalité $(*)$ équivaut à :

$$h = s \circ \mathrm{inv} \circ t,$$

ce qui montre le résultat demandé.

(ii) On sait que les similitudes directes envoie droite sur droite et cercle sur cercle. Le résultat obtenu pour inv à la question c) donne alors le même résultat pour h.

(iii)

3 Problème : quand -1 et 2 sont-ils des carrés dans $\mathbb{Z}/p\mathbb{Z}$?

3.1 Propriétés générales des carrés dans $\mathbb{Z}/p\mathbb{Z}$

a) $\mathbb{Z}/7\mathbb{Z}^* = \{\pm\bar{1}, \pm\bar{2}, \pm\bar{3}\}$ donc $C = \{\bar{1}^2, \bar{2}^2, \bar{3}^2\} = \{\bar{1}, \bar{4}, \bar{2}\}$.

b) En prenant un système de représentants centré en 0, autrement dit en écrivant $\mathbb{Z}/p\mathbb{Z}^* = \{\pm\bar{1}, \pm\bar{2}, \dots, \pm\overline{\frac{p-1}{2}}\}$ on sait que $C = \{\bar{1}^2, \dots, \overline{\frac{p-1}{2}}^2\}$ puisque les éléments opposés ont le même carré. Reste à voir que ces éléments de C sont deux à deux distincts. Or, réciproquement, comme p est premier $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau intègre, donc si deux éléments ont le même carré, ils sont opposés : en effet $x^2 = y^2 \Leftrightarrow (x-y)(x+y) = 0 \Leftrightarrow x - y = 0$ ou $x + y = 0$ par intégrité.
On conclut qu'il y a exactement $(p-1)/2$ éléments dans C.

c) Soit $x \in C$. Par déf., il s'écrit $x = y^2$ avec $y \in \mathbb{Z}/p\mathbb{Z}^*$. Donc $x^{(p-1)/2} = y^{p-1} = \bar{1}$ par petit théorème de Fermat.

d) D'après le résultat cité, l'équation $x^{(p-1)/2} - 1 = 0$ ayant déjà comme solution tous les éléments de C par c), et ceci faisant $(p-1)/2$ éléments par b), on conclut que si $x \notin C$, $x^{(p-1)/2} - 1 \neq 0$. Mais comme par petit théorème de Fermat, pour tout $x \in \mathbb{Z}/p\mathbb{Z}^*$, $(x^{(p-1)/2})^2 = 1$, on sait que $(x^{(p-1)/2})$ est une racine carrée de 1 donc ne peut valoir que 1 ou -1. Donc si $x \notin C$, $(x^{(p-1)/2}) = -1$.

3.2 Introduction du symbole de Legendre :

a) C'est immédiat puisque
• si $n \equiv 0\,[p]$ alors $n^{(p-1)/2} \equiv 0\,[p]$ d'une part
• et d'autre part pour $n \not\equiv 0\,[p]$, par le 3.1. $n^{(p-1)/2} \equiv 1\,[p]$ si $n \in C$ et si $n^{(p-1)/2} \equiv -1\,[p]$ sinon.

b) Par déf. du symbole de Legendre $-\bar{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $L(-1,p) = -1$. Or par la formule d'Euler, $L(-1,p) \equiv (-1)^{(p-1)/2}\,[p]$.
Donc $-\bar{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $(-1)^{(p-1)/2} = 1$ ce qui équivaut à $(p-1)/2 = 2k$ avec $k \in \mathbb{N}$, ce qui équivaut à $p \equiv 1\,[4]$.

c) $-\bar{1} = \bar{4} = \bar{2}^2$ dans $\mathbb{Z}/5\mathbb{Z}$. et $-\bar{1} = \overline{25} = \bar{5}^2$ dans $\mathbb{Z}/13\mathbb{Z}$.

3.3 Introduction de la notion d'entier algébrique

a) On prend $P(x) = x^2 - 2$ polynôme unitaire (coefficient dominant 1) à coefficients entiers. On a bien $P(\sqrt{2}) = 0$. Donc $\sqrt{2}$ est un *entier algébrique*.

b) Soit $\alpha = p/q$ avec $p \wedge q = 1$ un rationnel tel qu'il existe $(a_0, \dots, a_{n-1}) \in \mathbb{Z}^n$ tels que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$.
Alors $p^n/q^n + a_{n-1}p^{n-1}/q^{n-1} + \cdots + a_1 p/q + a_0 = 0$.

En multipliant par q^n, on a $p^n + a_{n-1}p^{n-1}q + \cdots + a_1pq^{n-1} + a_0q^n = 0$.
Donc $p^n = q(-a_{n-1}p^{n-1} + \cdots - a_0q^{n-1})$ Donc $q|p^n$. Or $p \wedge q = 1$ donc $q \wedge p^n = 1$, ce qui entraîne que $q = 1$.

c) On vient de montrer au b) que si $\alpha \in \Omega \in \mathbb{Q}$ alors $\alpha \in \mathbb{Z}$.
La réciproque est immédiate car si $\alpha \in \mathbb{Z}$, $\alpha \in \Omega$ puisque racine de l'équation $x - \alpha = 0$.
Conclusion : $\Omega \cap \mathbb{Q} = \mathbb{Z}$.

d) Comme Ω est un anneau commutatif, par la formule du binôme, pour tout $(\omega_1, \omega_2) \in \Omega^2$:
$(\omega_1 + \omega_2)^p = \displaystyle\sum_{k=0}^{p} \binom{p}{k} \omega_1^k \omega_2^{p-k}$.
Mais d'après le cours $\forall\, k \in [\![1, p-1]\!]$, $\binom{p}{k} \equiv 0\,[p]$ dans $\mathbb{Z}$, donc $\binom{p}{k}\omega_1^k\omega_2^{p-k} \equiv 0\,[p]$ dans Ω.
On conclut que $(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p\,[p]$ (congruence dans Ω).

3.4 Comment savoir si 2 est un carré modulo p :

a) On sait que $\zeta^8 = 1$ donc $P(\zeta) = 0$ où $P(x) = x^8 - 1$, donc $\zeta \in \Omega$.

b) $(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2\zeta.\zeta^{-1}$.
Or $\zeta^2 = e^{i\pi/2} = i$ et donc $\zeta^{-2} = -i$ donc $\zeta^2 + \zeta^{-2} = 0$.
On conclut bien que $(\zeta + \zeta^{-1})^2 = 2$.

c) Comme p est impair, on peut écrire $p - 1 = 2\dfrac{p-1}{2}$ où $\frac{p-1}{2} \in \mathbb{N}$. Donc $\tau^p = (\tau^2)^{\frac{p-1}{2}}$.
Comme $\tau^2 = 2$, on obtient $\tau^{p-1} = 2^{\frac{p-1}{2}}$.
Mais par le lemme d'Euler $2^{\frac{p-1}{2}} \equiv L(2,p)[p]$.
On conclut bien que $\tau^{p-1} \equiv L(2,p)[p]$ dans $\mathbb{Z}$.

d) En multipliant la congruence précédente dans $\mathbb{Z}$ par τ, on a $\tau^p \equiv L(2,p)\tau \;\; [p] \quad (1)$ dans Ω.
(En effet, la congruence précédente disait $\tau^{p-1} = L(2,p) + kp$ avec $k \in \mathbb{Z}$, en en multipliant par τ, on a $\tau^p = L(2,p)\tau + k\tau p$ et $k\tau = \kappa \in \Omega$.)
Or $\tau^p = (\zeta + \zeta^{-1})^p$ et par le 3.3. d), on a donc $\tau^p \equiv \zeta^p + \zeta^{-p}\,[p] \quad (2)$ dans Ω.
Avec (1) et (2), on a la conclusion : $\zeta^p + \zeta^{-p} \equiv L(2,p).\tau\,[p]$ dans Ω.

e) Comme $\zeta^8 = 1$, donc $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ pour $p \equiv \pm 1\,[8]$, ce qui prouve déjà que :
$\tau^p \equiv \tau\,[p]$ dans ce cas et donc avec (†) $L(2,p)\tau \equiv \tau\,[p]$ ce qui prouve que $L(2,p) = 1$ dans ce cas.
De même si $p \equiv \pm 3\,[8]$, on a : comme $\zeta^3 = -\zeta^{-1}$, que $\zeta^p + \zeta^{-p} = -(\zeta + \zeta^{-1})$ et donc que $L(2,p) = -1$. □

f) Conclusion : 2 est un carré modulo $p \in \mathbb{P}$, ssi $p \equiv \pm 1\,[8]$.