Partie I

1) a) Soit H le projeté orthogonal de O_2 sur AD. En utilisant le théorèmede Thalès dans le triangle ADO_3 :

$$\frac{O_2H}{O_3D} = \frac{AO_2}{AO_3}, \text{ donc } O_2H = \frac{3R}{5}$$

Comme $O_2H < R$, la droite (AD) coupe bien le cercle en deux points B et C. De plus, ces points vérifient d'après le théorème de Pythagore :

$$HB = HC = \sqrt{R^2 - O_2H^2} = \frac{4R}{5}.$$

Ainsi : $BC = \dfrac{8R}{5}$.

b) Si (A_1B) et (A_2C) étaient parallèles, on pourrait utiliser le théorème de Thalès dans le triangle AA_2C et on aurait :

$$\frac{AB}{AC} = \frac{AA_1}{AA_2} = \frac{1}{2},$$

ce qui est impossible car $AB > 2R$ et $BC < 2R$. Donc A_1B et A_2C sont sécantes en un point P

Comme $[A_1, A_2]$ est un diamètre, A_1BA_2 est rectangle en B, donc (A_2B) est une hauteur de PA_1A_2. De même, (A_1C) est une hauteur de ce triangle, donc les droites (A_1C) et (A_2B) sont sécantes en Q orthocentre du triangle PA_1A_2. On en déduit que la droite (PQ) est la hauteur issue de P et (PQ) est orthogonale à Δ.

2) a) Comme précédemment, d'après le théorème de Thalès, en notant H le projeté orthogonal de O_k sur AD :

$$\frac{O_kH}{O_nD} = \frac{AO_k}{AO_n} = \frac{2k-1}{2n-1} \text{ donc } O_kH = \frac{2k-1}{2n-1}r.$$

D'après le théorème de Pythagore : $HB_k = HC_k = \sqrt{r^2 - \dfrac{(2k-1)^2}{(2n-1)^2}r^2}$

donc $B_kC_K = 4\dfrac{\sqrt{n^2-n-k^2+k}}{2n-1}r$, et :

$$L(n,k) = \frac{4}{2n-1}\sqrt{n(n-1)-k(k-1)}$$

b) Soit m un nombre entier, alors $\sqrt{m}$ est un entier ou est un nombre irrationnel. En effet :
→ Si la factorisation de m en produit de nombres premiers est de la forme $m = p_1^{2\alpha_1} \dots p_\ell^{2\alpha_\ell}$, le nombre $\sqrt{m}$ est entier.

→ Sinon, la factorisation de m contient au moins un nombre premier à une puissance impaire, disons $m = p_1^{2\alpha_1+1}p_2^{\alpha_2}\dots$
Si on avait $\sqrt{m} = \dfrac{a}{b}$ avec a et b entiers premiers entre eux, on aurait $a^2 = b^2p_1^{2\alpha_1+1}p_2^{\alpha_2}\dots$.
Ainsi le nombre premier p_1 apparaîtrait dans la factorisation de a, et apparaîtrait à une puissance paire dans la factorisation de a^2. Par conséquent b^2 serait divisible par p_1 et b aussi, ce qui est contradictoire avec a et b premiers entre eux.

Donc, $L(n,k)$ est rationnel si et seulement si $n(n-1)-k(k-1)$ est le carré d'un entier, et comme $n(n-1)-k(k-1)$ est pair, ce ne peut être que le carré d'un nombre entier pair. D'où la condition $\mathcal{C}_1$.

Partie II

1) En coupant par $x = \lambda$, on trouve l'équation $z^2 + y(y-1) = \mu$, où $\mu = \lambda(\lambda-1)$.

On remarque que $\mu = \big(\lambda - \dfrac{1}{2}\big)^2 - \dfrac{1}{4} \geq -\dfrac{1}{4}$.

L'équation trouvée est équivalente à $\big(y - \dfrac{1}{2}\big)^2 + z^2 = \mu + \dfrac{1}{4}$.

Comme $\mu+\dfrac{1}{4}\geq 0$, il s'agit du cercle, éventuellement réduit à un point pour $\lambda=\dfrac{1}{2}$ de centre $\big(\lambda,\dfrac{1}{2},0\big)$ de rayon $\sqrt{\mu+\dfrac{1}{4}}=\big|\lambda-\dfrac{1}{2}\big|$ et contenu dans le plan P_λ.

2) Soit M de coordonnées (x,y,z). Son symétrique orthogonal par rapport à (d) est le point M' de coordonnées $(1-x,1-y,-z)$. Vu l'équation donnée pour Σ, M appartient à Σ si et seulement M' y appartient : (d) est axe de symétrie de Σ.
Intersecter le plan P d'équation $y=\dfrac{1}{2}$ et Σ conduit donc à l'équation :

$$z^2=x(x-1)+\frac{1}{4}$$

qui est équivalente à $z^2=\big(x-\dfrac{1}{2}\big)^2$ soit à $\big(z-x+\dfrac{1}{2}\big)\big(z+x-\dfrac{1}{2}\big)=0$. Il s'agit de la réunion de deux droites, passant par I, symétriques par rapport au plan $(O,\vec{i},\vec{j}\,)$ et perpendiculaires.

3) Finalement Σ est un cône de révolution, d'axe la droite d'équation $\begin{cases} y=\frac{1}{2} \\ z=0 \end{cases}$, de sommet I et de demi-angle d'ouverture $\pi/4$.

4) Application directe de la conclusion de **I. 2. b)**.

Partie III

1) a) f est dérivable comme primitive d'une fonction continue, de dérivée $f'(x)=\sqrt{1-x^2}$, et sin est dérivable, donc la composée F est dérivable et $F'(x)=\cos x\times f'(\sin x)=\cos x\sqrt{1-\sin^2 x}=\cos^2 x$, sur $[0,\pi/2]$.

b) $F(0)=0$ donc $F(x)=\displaystyle\int_0^x \cos^2 t\,\mathrm{d}t$.

c) On fait le changement de variable $u=\dfrac{\pi}{2}-t$:

$$\int_0^{\pi/2}\cos^2 t\,\mathrm{d}t=\int_{\pi/2}^0 \sin^2 t(-\mathrm{d}t)=\int_0^{\pi/2}\sin^2 t\,\mathrm{d}t$$

La somme des intégrales est $\displaystyle\int_0^{\pi/2}\mathrm{d}t=\frac{\pi}{2}$ donc $\displaystyle\int_0^{\pi/2}\sin^2 t\,\mathrm{d}t=\int_0^{\pi/2}\cos^2 t\,\mathrm{d}t=\frac{\pi}{4}$.

d) Ainsi $\dfrac{\pi}{4}=F\big(\dfrac{\pi}{2}\big)=f(1)=\displaystyle\int_0^1\sqrt{1-t^2}\,\mathrm{d}t$.
Or, dans le plan rapporté à un repère orthonormé, cette intégrale est l'aire de la surface comprise entre l'axe des abscisses, la courbe représentative de la fonction $t\mapsto\sqrt{1-t^2}$ et les verticales d'abcisses 0 et 1, il s'agit donc de l'aire du quart de disque de centre O et de rayon 1.

2) a) Il suffit de reprendre la formule de **I. 2 .a)** :

$$\lambda_n=\frac{1}{AD}\sum_{k=1}^{n-1}B_kC_k=\frac{1}{\sqrt{(2n-1)^2-1}}\sum_{k=1}^{n-1}\frac{4}{2n-1}\sqrt{n(n-1)-k(k-1)}$$

Soit :

$$\lambda_n=\frac{2}{2n-1}\sum_{k=1}^{n-1}\sqrt{1-\frac{k(k-1)}{n(n-1)}}$$

(on pourrait convenir de sommer jusqu'à n, en posant $A_n=B_n=D$.)

b) D'une part : $\dfrac{k}{n}\times\dfrac{k-1}{n-1}=\dfrac{k-1}{n}\times\dfrac{k}{n-1}\geq\dfrac{k-1}{n}\times\dfrac{k-1}{n}$.

D'autre part : $-n\leq -k$ donc $(k-1)n\leq k(n-1)$ et $\dfrac{k-1}{n-1}\leq\dfrac{k}{n}$ d'où $\dfrac{k}{n}\times\dfrac{k-1}{n-1}\leq\big(\dfrac{k}{n}\big)^2$.
Ainsi, pour $n\geq 2$ et $1\leq k\leq n$:

$$\left(\frac{k-1}{n}\right)^2 \leq \frac{k}{n}\times\frac{k-1}{n-1} \leq \left(\frac{k}{n}\right)^2$$

c) La fonction $t \mapsto 1-t^2$ est positive et décroissante sur $[0,1]$, il en est donc de même de la fonction $t \mapsto \sqrt{1-t^2}$. Ainsi pour $t \in \left[\frac{k-1}{n}, \frac{k}{n}\right]$, avec $1 \leq k \leq n-1$:
$\sqrt{1-\left(\frac{k}{n}\right)^2} \leq \sqrt{1-t^2} \leq \sqrt{1-\left(\frac{k-1}{n}\right)^2}$ et, par conservation des inégalités par intégration :

$$\frac{1}{n}\sqrt{1-\left(\frac{k}{n}\right)^2} \leq I_{n,k} \leq \frac{1}{n}\sqrt{1-\left(\frac{k-1}{n}\right)^2}$$

Vu le **2. b)**, on a donc :

$$nI_{n,k+1} \leq \sqrt{1-\left(\frac{k}{n}\right)^2} \leq \sqrt{1-\frac{k}{n}\times\frac{k-1}{n-1}} \leq \sqrt{1-\left(\frac{k-1}{n}\right)^2} \leq nI_{n,k-1}$$

pour $n \geq 3$ et $2 \leq k \leq n-1$.

3) En sommant les encadrements précédents, il vient, pour $n \geq 3$:

$$\frac{2n}{2n-1}\sum_{k=2}^{n-1} I_{n,k+1} \leq \lambda_n - \frac{2}{2n-1} \leq \frac{2n}{2n-1}\sum_{k=2}^{n-1} I_{n,k-1}$$

Soit :

$$\frac{2n}{2n-1}\int_{2/n}^{1}\sqrt{1-t^2}\,\mathrm{d}t \leq \lambda_n - \frac{2}{2n-1} \leq \frac{2n}{2n-1}\int_{0}^{(n-2)/n}\sqrt{1-t^2}\,\mathrm{d}t$$

Or : $0 \leq \int_0^{2/n}\sqrt{1-t^2}\,\mathrm{d}t \leq \frac{2}{n}$ et $0 \leq \int_{(n-2)/n}^{1}\sqrt{1-t^2}\,\mathrm{d}t \leq \frac{2}{n}$.

Les deux intégrales écrites ci-dessus ont donc pour limite $\int_0^1\sqrt{1-t^2}\,\mathrm{d}t = \frac{\pi}{4}$ lorsque n tend vers l'infini, d'où l'on déduit :

$$\lim_{n\to+\infty}\lambda_n = \frac{\pi}{4}$$

Partie IV

1) $\mathcal{C}_1$ est équivalente à $(2n-1)^2-(2k-1)^2 = 16a^2$ *i.e.* à $p^2-q^2 = 16a^2$.
p et q doivent être impairs par construction et $k \leq n-1$ donne $q < p$.

2) Si u et v sont de parités différentes, u^2 et v^2 également, donc p et q sont impairs.
De plus $p^2-q^2 = 4u^2v^2 = 16a^2$, car on peut mettre 4 en facteur dans le carré pair.
Posons $\alpha = \frac{p+q}{2}$ et $\beta = \frac{p-q}{2}$, qui sont bien des entiers car p et q sont impairs. La condition $\mathcal{C}_2$ donne $\alpha\beta = 4a^2$.
Or comme p et q sont premiers entre eux, il existe des entiers r et s tels que $rp+sq = 1$ soit $1 = r(\alpha+\beta)+s(\alpha-\beta) = (r+s)\alpha+(r-s)\beta$: α et β sont également premiers entre eux.
Comme leur produit est un carré, chacun des deux doit être un carré ; il existe donc u, v tels que $\alpha = u^2$ et $\beta = v^2$, soit $p = u^2+v^2$ et $q = u^2-v^2$. Enfin, u et v doivent être de parités différentes pour que p et q soient impairs.
Par ailleurs : $4a^2 = u^2v^2$, d'où $a = \frac{uv}{2}$.

Partie V

1) a) S'il existe u et v tels que $n = u^2+v^2$, ceux-ci doivent être de parités différentes puisque n est impair. Supposons par exemple $u = 2k$, $v = 2\ell+1$, k et ℓ entiers.
Alors : $n = 4k^2+4\ell^2+4\ell+1 \equiv 1 \pmod 4$.

b) $2 = 1^2+1^2$ et $5 = 1^2+2^2$.

1) a) $(m,1,1)\in S$ donc $S\neq\emptyset$.
Si $(x,y,z)\in S$, on ne peut avoir $x=0$ ou $y=0$ (sinon $z^2=p$ et p ne serait pas premier) on a donc pour tout (x,y,z) de S : $1\leq x\leq p$, $1\leq y\leq p$ et $-p\leq z\leq p$.
Chacune des coordonnées ne peut prendre qu'un nombre fini de valeurs, donc S est fini.

Si (x,y,z) vérifiait $\begin{cases} z^2+4xy=p \\ x=y+z \end{cases}$, alors $p=(x-y)^2+4xy=(x+y)^2$, ce qui contredit que p est premier. Ainsi, l'intersection de S avec le plan d'équation $x=y+z$ est vide.

b) $\star$ Si $x>y+z$, alors $(x',y',z')=(x-y-z,y,2y+z)\in\mathbb{N}\times\mathbb{N}\times\mathbb{Z}$ et :
$4x'y'+z'^2=4xy-4y^2-4yz+4y^2+4yz+z^2=4xy+z^2=p$, donc $(x',y',z')\in S$.

$\star\star$ Si $x<y+z$, alors $(x',y',z')=(y+z-x,x,2x-z)\in\mathbb{N}\times\mathbb{N}\times\mathbb{Z}$ et :
$4x'y'+z'^2=4xy+4xz-4x^2+4x^2-4xz+z^2=4xy+z^2=p$, donc $(x',y',z')\in S$.

3) a) Ici $m=10$ (notons que dans ce cas $p=41$ est premier). On obtient alors la succession de triplets :

$$\begin{aligned}(10,1,1)&\underset{\star}{\longrightarrow}(8,1,3)\underset{\star}{\longrightarrow}(4,1,5)\underset{\star\star}{\longrightarrow}(2,4,3)\underset{\star\star}{\longrightarrow}(5,2,1)\underset{\star}{\longrightarrow}(2,2,5)\underset{\star\star}{\longrightarrow}(5,2,-1)\\ &\underset{\star}{\longrightarrow}(4,2,3)\underset{\star\star}{\longrightarrow}(1,4,5)\underset{\star\star}{\longrightarrow}(8,1,-3)\underset{\star}{\longrightarrow}(10,1,-1)\underset{\star}{\longrightarrow}(10,1,1).\end{aligned}$$

b) Si (a,b,c) est un élément de la suite, il ne peut avoir comme antécédent que $(a-b+c,b,c-2b)$ ou $(b,a-b+c,2b-c)$, et ce à condition que $a-b+c>0$.

Si on pose $\begin{cases} u=a-b+c \\ v=b \\ w=c-2b \end{cases}$, on remarque que ces deux antécédents sont (u,v,w) et $(v,u,-w)$. Ils ne peuvent eux-mêmes avoir un antécédent que si, respectivement $u-v+w=a-4b+2c>0$ ou $v-u-w>0$.
Ces deux conditions ne peuvent être vérifiées en même temps. On en déduit donc que tout point (a,b,c) de la suite d'indice au moins 2 a pour antécédent :

$$\begin{cases} (a-b+c,b,c-2b) & \text{si } a-4b+2c>0 \\ (b,a-b+c,-c+2b) & \text{si } a-4b+2c<0 \end{cases}$$

Par ailleurs, $(x_1,y_1,z_1)=(m-2,1,3)$ a pour antécédent $(x_0,y_0,z_0)=(m,1,1)$, ce qui concide bien avec la relation ci-dessus.

c) S étant fini, la suite ne peut pas prendre une infinité de valeurs distinctes, on obtiendra donc à un moment un triplet déjà obtenu auparavant, d'où l'existence de k et ℓ, avec par exemple $k>\ell$ tels que $(x_k,y_k,z_k)=(x_\ell,y_\ell,z_\ell)$.

Si $\ell=0$, alors $n=k$ convient.

Si $\ell\geq 1$, alors $(x_k,y_k,z_k)=(x_\ell,y_\ell,z_\ell)$, donne par unicité de l'antécédent $(x_{k-1},y_{k-1},z_{k-1})=(x_{\ell-1},y_{\ell-1},z_{\ell-1})\ \ldots,\ (x_{k-\ell},y_{k-\ell},z_{k-\ell})=(x_0,y_0,z_0)=(m,1,1)$ et on peut prendre $n=k-\ell$.

4) a) Comme $m>2$, l'image du triplet $(m,1,1)$ est le triplet $(m-2,1,3)$, donc n est au moins égal à 2.
Alors $(x_{n-1},y_{n-1},z_{n-1})=(m,1,-1)=(x_0,y_0,-z_0)$;
puis $(x_{n-2},y_{n-2},z_{n-2})=(m-2,1,-3)=(x_1,y_1,-z_1)$.

b) Supposons $(x_{j-1},y_{j-1},z_{j-1})=(x_{n-j},y_{n-j},-z_{n-j})$, avec $x_{j-1}>y_{j-1}+z_{j-1}$, alors on a :
$(x_j,y_j,z_j)=(x_{j-1}-y_{j-1}-z_{j-1},y_{j-1},2y_{j-1}+z_{j-1})$.
$\star$ Si $x_j>y_j+z_j$, *i.e.* $x_{j-1}-4y_{j-1}-2z_{j-1}=x_{n-j}-4y_{n-j}+2z_{n-j}>0$, on trouve :

$$(x_{n-j-1},y_{n-j-1},z_{n-j-1})=(x_{n-j}-y_{n-j}+z_{n-j},y_{n-j},z_{n-j}-2y_{n-j})=(x_j,y_j,-z_j).$$

$\star$ Si $x_j<y_j+z_j$, *i.e.* $x_{j-1}-4y_{j-1}-2z_{j-1}=x_{n-j}-4y_{n-j}+2z_{n-j}<0$, on trouve :

$$(x_{n-j-1},y_{n-j-1},z_{n-j-1})=(y_{n-j},x_{n-j}-y_{n-j}+z_{n-j},-z_{n-j}+2y_{n-j})=(y_j,x_j,z_j).$$

On fait de même dans le cas $(x_{j-1},y_{j-1},z_{j-1})=(y_{n-j},x_{n-j},z_{n-j})$ avec $x_{j-1}<y_{j-1}+z_{j-1}$, ce qui termine la récurrence.

c) Enfin, il ne peut exister de triplet (x_k, y_k, z_k) tel que $(x_{k+1}, y_{k+1}, z_{k+1}) = (x_k, y_k, -z_k)$ ou $(x_{k+1}, y_{k+1}, z_{k+1}) = (y_k, x_k, z_k)$, car cela imposerait $y_k = -z_k$ ou $x_k = y_k = z_k$, ce qui est impossible sur S pour p premier.
Ce qui assure qu'il y a un nombre impair d'éléments dans notre bout de suite.

d) Le terme (x_r, y_r, z_r) au milieu doit être image d'un triplet (a, b, c) et antécédent du triplet $(a, b, -c)$ ou (b, a, c) ce qui ne peut se produire que pour $x_r = y_r$ et alors $p = (2x_r)^2 + z_r^2$.
Nous venons donc de montrer que tout nombre premier de la forme $4m + 1$ est somme de deux carrés.

5) a) Clair : il suffit de programmer l'algorithme décrit en **2) b)**, jusqu'à obtenir un triplet de la forme (x, x, z).

b) Le plus petit nombre premier supérieur à 40 et qui est somme de deux carrés est 41. Au cours de la question **3) a)** nous avons obtenu dans la chaîne de triplets le triplet $(2, 2, 5)$, ce qui prouve que $41 = 4{\times}2{\times}2 + 5^2 = 4^2 + 5^2$.

Partie VI

1) $mn = |(a+ib)(c+id)|^2 = |x+iy|^2 = x^2+y^2$ avec $\begin{cases} x = ac - bd \\ y = bc + ad \end{cases}$.

2) a) $\star$ $1^2 + 1 = 2$ et $2^2 + 1 = 5$ sont premiers et somme de deux carrés, donc $\mathcal{P}(1)$ et $\mathcal{P}(2)$ sont vraies.

$\star$ $3^2 + 1 = 10$, de diviseurs premiers 2 et 5 qui sont sommes de deux carrés et $\mathcal{P}(3)$ est vraie.

b) i) On a $n^2 + 1 = n\big(n + \dfrac{1}{n}\big)$ et $n + \dfrac{1}{n}$ n'est pas entier, donc n ne divise pas $n^2 + 1$.

ii) Si $p < n$, on écrit : $(n-p)^2 + 1 = (n^2+1) - 2pn + p^2$ et p divise les trois termes donc divise $(n-p)^2 + 1$. L'hypothèse de récurrence assure alors que p, qui est premier, est somme de deux carrés, donc congru à 1 modulo 4.

iii) On suppose $p > n$ et $p < n^2+1$, donc $n^2+1 = pq$, avec $q < n$ (sinon $pq \geq (n+1)^2 > n^2+1$) et $q > 1$ et les diviseurs premiers de $n^2 + 1$ autres que p sont les diviseurs premiers de q, donc sont compris entre 2 et $n - 1$.

$\rightarrow$ Si n est pair, alors $n^2 + 1$ est congru à 1 modulo 4 et tous les diviseurs premiers de q sont impairs, donc par **ii)** sont somme de deux carrés et sont congrus à 1 modulo 4. Ainsi q est congru à 1 modulo 4 et p aussi.

$\rightarrow$ Si n est impair, alors $n^2 + 1$ est congru à 2 modulo 4 et $n^2 + 1 = p{\times}2q'$, avec q' impair. Ainsi, par **ii)** les diviseurs premiers de q' sont impairs sommes de deux carrés et sont congrus à 1 modulo 4. Donc q' est congru à 1 modulo 4 et il en est de même de p.

iv) Si $n^2 + 1$ est premier, alors $p = n^2 + 1$ est somme de deux carrés. Sinon, les questions précédentes montrent que $p = 2$ (qui est somme de deux carrés) ou que p est congru à 1 modulo 4, donc est somme de deux carrés.

c) En supposant $\mathcal{P}(i)$ vraie jusqu'au rang $n - 1$, nous venons de montrer que $\mathcal{P}(n)$ est vraie. On conclut alors par le principe de récurrence.

3) a) Soit $N = (s!)^2 + 1$; N n'est pas divisible par 2, 3, $\ldots n$, donc son plus petit facteur premier p_s est strictement supérieur à n, et somme de deux carrés d'après **2)**.

b) Ainsi, pour tout entier naturel n, on peut trouver un nombre premier somme de deux carrés supérieur à n. L'ensemble de ces nombres n'est donc pas majoré et il contient une infinité d'éléments.

4) a) On prend p premier impair somme de deux carrés (on peut choisir p d'une infinité de faons) : $p = u^2 + v^2$, avec $u > v$, on prend $q = u^2 - v^2$; $n = \dfrac{p+1}{2}$; $k = \dfrac{q+1}{2}$, alors, d'après les résultats de la partie **IV**, $L(n, k)$ est rationnel : il existe bien une infinité de couples (n, k) tels que $L(n, k)$ soit rationnel.

b) Par exemple : $65 = 8^2 + 1^2 = 7^2 + 4^2$. Avec les notations précédentes on a donc $n = 33$ et $k = 32$ ou $k = 17$.
Ainsi $L(33, 32)$ et $L(33, 17)$ sont rationnels.