Résoudre les équations diophantiennes : (1) $x^2+y^2=31z^2$ et (2) $x^2+y^2=29z^2$

I. $\boxed{x^2+y^2=31z^2} \Rightarrow x^2+y^2 \equiv 0\ [31] \Leftrightarrow y^2 \equiv -x^2\ [31]$

On en déduit que -1 doit être un carré modulo 31, ce qui faux d'après le théorème des résidus quadratiques puisque 31 n'est pas congru à 1 modulo 4. **L'équation** (1) **n'a pas de solution**.

II. $\boxed{x^2+y^2=29z^2}$: les triplets $k(m,n,1)$ où $k \in \mathbb{Z}$, $(m,n) \in \{-5,-2,2,5\}^2$ avec $|mn|=10$, sont solutions. **L'équation** (2) **a-t-elle d'autres solutions ?**

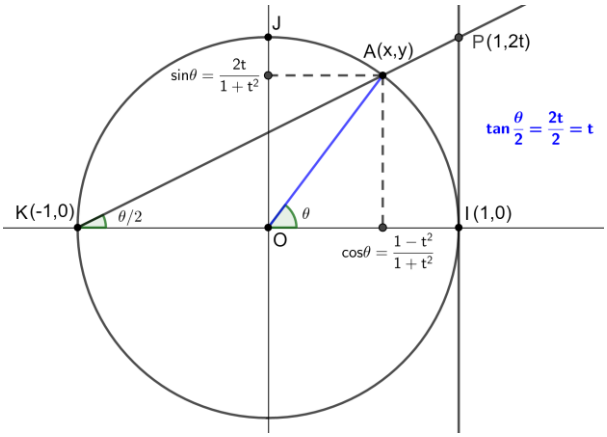
1. Représentation paramétrique du cercle trigonométrique à partir de sa projection sur la droite d'équation $x=1$

Projetons chaque point $A(x,y)$ du cercle sur la droite d'équation $x=1$ à partir du point K. Notons $(1,2t)$ les coordonnées du point projeté P. Soit θ une mesure de l'angle au centre $(\overrightarrow{OI},\overrightarrow{OA})$. Alors, l'angle inscrit $(\overrightarrow{KI},\overrightarrow{KA})$ a pour mesure $\theta/2$. Or, on a :

$$\tan\frac{\theta}{2}=\frac{2t}{2}=t.$$

On en déduit que

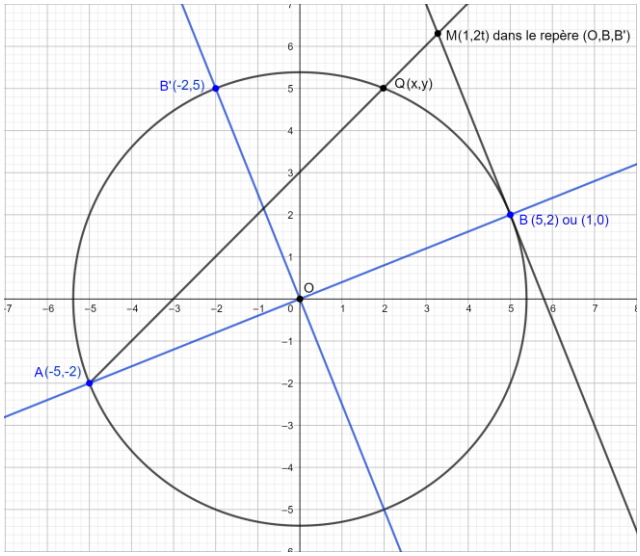
$$x=\cos\theta=\frac{1-t^2}{1+t^2} \text{ et } y=\sin\theta=\frac{2t}{1+t^2}.$$



D'après les formules ci-dessus et la formule $=\frac{y}{x+1}$, il y a bijection entre le cercle privé de K et la tangente au cercle passant par I. Pour obtenir les points du cercle à coordonnées rationnelles, il suffit donc de choisir t rationnel puisque les formules de passage conservent la rationalité.

2. Représentation paramétrique du cercle d'équation $x^2+y^2=29$

Effectuons un changement de repère pour nous ramener sur le cercle trigonométrique.



Plaçons nous dans le repère (O,B,B'), avec $B(5,2)$ et $B'(-2,5)$, qui se déduit du repère (O,I,J) par la similitude directe de matrice

$$S=\begin{pmatrix}5 & -2\\ 2 & 5\end{pmatrix}.$$

Dans ce nouveau repère le cercle a pour équation $X^2+Y^2=1$. D'après 1. il peut être paramétré par la représentation

$$\begin{cases}X=\dfrac{1-t^2}{1+t^2}\\ Y=\dfrac{2t}{1+t^2}\end{cases}$$

où t est le réel tel que le point M a pour coordonnées $(1,2t)$ dans le nouveau repère.

La matrice S étant à coordonnées entières, le changement de repère conserve la rationalité.

Il y a donc une bijection entre les points à coordonnées rationnelles du cercle privé de A et les points à coordonnées rationnelles de la tangente au cercle passant par B.

Or,

$$\begin{pmatrix} x \\ y \end{pmatrix} = S\begin{pmatrix} X \\ Y \end{pmatrix} = \frac{1}{1+t^2}\begin{pmatrix} 5 & -2 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 1-t^2 \\ 2t \end{pmatrix} = \frac{1}{1+t^2}\begin{pmatrix} -5t^2-4t+5 \\ -2t^2+10t+2 \end{pmatrix}$$

En posant $t = a/b$, avec a/b irréductible, on a :

$$\frac{1}{1+t^2}\begin{pmatrix} -5t^2-4t+5 \\ -2t^2+10t+2 \end{pmatrix} = \frac{1}{a^2+b^2}\begin{pmatrix} -5a^2-4ab+5b^2 \\ -2a^2+10ab+2b^2 \end{pmatrix}$$

Ainsi, le **triplet élémentaire** $f(a,b) := (-5a^2-4ab+5b^2, -2a^2+10ab+2b^2, a^2+b^2)$ est solution de l'équation (2).

Remarque 1 Si (x,y,z) est irréductible, x et y sont de parités différentes et z est impair.

En effet, x et y ne peuvent pas être tous les deux pairs car, sinon, z l'est aussi et le triplet (x,y,z) n'est pas irréductible.
Si x et y sont impairs, alors $x^2+y^2 \equiv 1+1 \equiv 2\ [4]$. Or, $29z^2 \equiv z^2 \equiv 0$ ou $1\ [4]$. D'où impossibilité.
Seuls x et y de parités différentes peuvent donc satisfaire l'équation et z ne peut alors qu'être impair.

Lemme. Soit $f(a,b)$ un triplet élémentaire avec a/b est irréductible. Alors :

a) $f(a,b)$ n'est simplifiable que par 2 ou 29.
b) $f(a,b)$ est simplifiable par 2 si et seulement si a et b sont impairs.
c) $f(a,b)$ est simplifiable par 29 si et seulement si $a+12b \equiv 0\ [29]$.
d) $f(a,b)$ n'est simplifiable ni par 4 ni par 29^2.

Démonstration.

a) Soit un entier d tel que $d \mid -5a^2-4ab+5b^2$ (3), $d \mid -2a^2+10ab+2b^2$ (4) et $d \mid a^2+b^2$ (5).
En effectuant la combinaison linéaire $5\times(3)+2\times(4)$, on élimine les termes rectangles (en pq) entre (3) et (4) et on obtient : $d \mid -29a^2+29b^2 = 29(b^2-a^2)$ (6)
D'après le théorème de Gauss, il vient : $d = 1$ ou $d = 29$ ou d divise b^2-a^2 (7).
Si $d \neq 1$ divise b^2-a^2, alors d'après (5), d divise $2b^2$ (par addition de (5) et (7)) et d divise $2a^2$ (par soustraction de (5) et (7)). Or, a et b étant premiers entre eux, d est premier avec a ou avec b, et donc avec a^2 ou avec b^2. D'après le théorème de Gauss, on a en déduit que $d = 2$.
Conclusion : les seuls diviseurs possibles de $f(a,b)$ sont 1, 2 et 29.

b) $-2a^2+10ab+2b^2 \equiv 0[2]$ et $-5a^2-4ab+5b^2 \equiv a^2+b^2\ [2]$, ce qui permet de conclure.

c) Modulo 29, on a :

- $-5a^2-4ab+5b^2 \equiv 0 \Leftrightarrow 5a^2+4ab-5b^2 \equiv 0 \Leftrightarrow a^2+24ab-b^2 \equiv 0$ (en multipliant par 6)
  $\Leftrightarrow b^2((ab')^2+24ab'-1) \equiv 0$ où b' est l'inverse de b modulo 29
  $\Leftrightarrow b^2(ab'+12)^2 \equiv 0$
  $\Leftrightarrow b \equiv 0$ ou $ab' \equiv -12 \equiv 17$.

- Un calcul analogue montre que : $-2a^2 + 10ab + 2b^2 \equiv 0 \Leftrightarrow b^2(ab' + 12)^2 \equiv 0$
  Autrement dit, là encore : $-2a^2 + 10ab + 2b^2 \equiv 0 \Leftrightarrow b \equiv 0$ ou $ab' \equiv -12 \equiv 17$.
- Le cas $b \equiv 0$ impose $a \equiv 0$ ce qui conduit à une fraction a/b non irréductible.
  Si $ab' \equiv -12$, alors $a^2 + b^2 \equiv b^2((ab')^2 + 1) \equiv b^2(144 + 1) \equiv b^2 \times 0 \equiv 0$.

Conclusion : $f(a, b)$ est simplifiable par 29 si et seulement si $a + 12b \equiv 0\ [29]$.

d) Raisonnons par l'absurde.

Si 4 est un diviseur commun à $-5a^2 - 4ab + 5b^2, -2a^2 + 10ab + 2b^2$ et $a^2 + b^2$, on a d'après (6) :
4 divise $29(b^2 - a^2)$. Donc, d'après la démonstration précédente, 4 divise $2a^2$ et $2b^2$.
Donc 2 divise a^2 et b^2, puis a et b d'après le lemme d'Euclide, ce qui est impossible par hypothèse.

Pour 29^2, on suit le même raisonnement : 29^2 divise $29(b^2 - a^2)$, donc 29 divise $b^2 - a^2$.
Comme 29 divise aussi $a^2 + b^2$, il vient 29 divise $2a^2$ et $2b^2$.
Donc 29 divise a^2 et b^2, puis a et b d'après le lemme d'Euclide, ce qui est impossible par hypothèse.

Conclusion. On note :

- $\mathcal{S}$ l'ensemble des solutions de l'équation $x^2 + y^2 = 29z^2$,
- $f(a, b) \coloneqq (-5a^2 - 4ab + 5b^2, -2a^2 + 10ab + 2b^2, a^2 + b^2)$, avec $a, b \in \mathbb{Z}^*$ et a/b irréductible, dit ***triplet élémentaire***,
- G l'ensemble des triplets élémentaires irréductibles.

1) On obtient G en divisant éventuellement une fois les triplets élémentaires $f(a, b)$ par 2 et/ou 29.
2) G est l'ensemble des **triplets générateurs** de S : $\boxed{\mathcal{S} = \mathbb{Z} \cdot G}$

Exemples pour les quatre cas possibles si a/b est irréductible

a) $f(0, 1) = (5, 2, 1)$ est irréductible
   $f(2, 3) = (1, 70, 13)$ est irréductible.
b) $f(1, 3) = (28, 46, 10)$ est égal à $2(14, 23, 5)$.
c) $f(1, 12) = (-667, 406, 145)$ est égal à $29(-23, 14, 5)$.
d) $f(17, 1) = (-1\,508, -406, 290)$ est égal à $29 \times 2(-26, -7, 5)$.