

Partie A. — Droites rationnelles

1. Nous allons montrer que (1) implique (2) implique (3) implique (1).

Supposons que M est un point rationnel. Alors, par définition, $x_M \in \mathbb{Q}$.

Supposons que $x_M \in \mathbb{Q}$. Alors, comme $M \in \mathcal{D}$, $y_M = mx_M + p$. Or, m , x_M et p sont rationnels donc y_M est rationnel.

Supposons que $y_M \in \mathbb{Q}$. Alors, de même, $y_M = mx_M + p$ et donc, comme $m \neq 0$, $x_M = \frac{1}{m}(y_M - p)$. Comme m est rationnel, $\frac{1}{m}$ aussi et, puisque y_M et p sont rationnels, on conclut que $x_M \in \mathbb{Q}$.

Ainsi, on a bien montré l'équivalence entre (1), (2) et (3).

2. Un exemple

- a. Soit $(u; v) \in \mathbb{Z}^2$. Alors, $10u - 15v = 5(2u - 3v)$ et $2u - 3v \in \mathbb{Z}$ donc 5 divise $10u - 15v$.

- b. Supposons que $M(x_M; y_M)$ soit un point entier de Δ . Alors, $y_M = \frac{2}{3}x_M - \frac{4}{5}$ donc, en multipliant par 15, $15y_M = 10x_M - 12$ donc $12 = 10x_M - 15y_M$. On déduit alors de la question précédente que 5 divise 12 ce qui est absurde. Ainsi, Δ ne contient aucun point entier.

3. Cas général

- a. Par définition, on a $y_M = mx_M + p = \frac{a}{b}x_M + \frac{c}{d}$ donc, en multipliant par bd , il vient $bdy_M = adx_M + cb$ et donc $d(by_M - ax_M) = bc$. Comme $by_M - ax_M \in \mathbb{Z}$, on conclut que d divise bc .

De plus, par hypothèse, d est premier avec c donc, par le théorème de Gauss, d divise b .

- b. Comme a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que $au + bv = 1$. De plus, d divise b donc il existe un entier k tel que $b = kd$ et donc $au + kdv = 1$. On en déduit que $auc + kdv c = c$ donc $\frac{auc}{d} + kvc = \frac{c}{d}$ et ainsi $\frac{auck}{kd} + kvc = \frac{c}{d}$ i.e. puisque $kd = b$, $kvc = \frac{a}{b}(-uck) + \frac{c}{d} = m(-uck) + p$. On en déduit donc que le point $M(-uck; kvc)$ est un point entier appartenant à $\mathcal{D}$. Ainsi, $\mathcal{D}$ passe par un point entier.

- c. Les deux questions précédentes permettent de conclure que $\mathcal{D}$ passe par un point entier si et seulement si d divise b .

Partie B. — Cercles rationnels

1. Un résultat préliminaire

- a. Comme u et v sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers x et y tels que $ux + vy = 1$. En élevant au cube, on obtient $(ux + vy)^3 = 1^3$ i.e. $(ux)^3 + 3(ux)^2vy + 3ux(vy)^2 + (vy)^3 = 1$ donc $(ux^3 + 3x^2vy)u^2 + (3uxv^2 + vy^3)v^2 = 1$ et donc, comme $ux^3 + 3x^2vy$ et $3uxv^2 + vy^3$ sont des entiers, on déduit du théorème de Bézout que u^2 et v^2 sont premiers entre eux.

Autre méthode. — Comme u et v sont premiers entre eux, par un résultat du cours, $\text{PGCD}(u \times u, v) = \text{PGCD}(u, v) = 1$ donc $\text{PGCD}(u^2, v) = 1$. De même, on en déduit que $\text{PGCD}(v \times v, u^2) = \text{PGCD}(v, u^2) = 1$ donc $\text{PGCD}(u^2, v^2) = 1$. Ainsi, u^2 et v^2 sont premiers entre eux.

- b. Notons $d = \text{PGCD}(a, b)$ et posons $u = \frac{a}{d}$ et $v = \frac{b}{d}$. Alors, u et v sont deux entiers premiers entre eux. Comme a^2 divise b^2 , il existe un entier k tel que $k = \frac{b^2}{a^2}$. Alors, $\frac{k}{1} = k = \frac{b^2}{a^2} = \frac{u^2}{v^2}$. Or, $\frac{k}{1}$ est une fraction irréductible et $\frac{u^2}{v^2}$ aussi d'après la question précédente. Ainsi, par unicité de la forme irréductible, $u^2 = k$ et $v^2 = 1$. Ainsi, v vaut 1 ou -1 donc a vaut d ou $-d$ et, dans tous les cas, a divise b .

Autre méthode. — En gardant les mêmes notations, on a $a^2 = d^2 u^2$ et $b^2 = d^2 v^2$ donc, par une propriété du cours, $\text{PGCD}(a^2, b^2) = d^2 \text{PGCD}(u^2, v^2)$. Ainsi, par la question précédent, $\text{PGCD}(a^2, b^2) = d^2$. Or, comme a^2 divise b^2 et $a^2 > 0$, $\text{PGCD}(a^2, b^2) = a^2$ et donc $a^2 = d^2$ i.e. $d = |a|$ et on conclut de même.

2. Points entiers non triviaux sur un cercle de rayon entier centré en O

- a. Comme $x_M^2 = |x_M|^2$ et $y_M^2 = |y_M|^2$, le point de coordonnées $(|x_M|; |y_M|)$ est un point entier de $\mathcal{C}\vec{n}$. De plus, comme $x_M \neq 0$ et $y_M \neq 0$, $|x_M| > 0$ et $|y_M| > 0$. Ainsi, on peut toujours se ramener au cas où $x_M > 0$ et $y_M > 0$.
- b. Par définition, d divise a et b donc d^2 divise a^2 et b^2 . Ainsi, d^2 divise $a^2 + b^2$ i.e. d^2 divise n^2 . On déduit alors de la question 1. que d divise n .

On pose $a = \frac{x_M}{d}$, $b = \frac{y_M}{d}$ et $c = \frac{n}{d}$. Ainsi, a , b et c sont des entiers strictement positifs tels que $a^2 + b^2 = c^2$.

- c. Par théorème, a et b sont premiers entre eux donc ils sont pas tous les deux divisibles par 2. Ainsi, au moins un des deux nombres a ou b est impair.

Soit m un entier quelconque. On a le tableau suivant :

Reste de m modulo 8	0	1	2	3	4	5	6	7
Reste de m^2 modulo 8	0	1	4	1	0	1	4	1

donc les restes possibles pour un carré modulo 8 sont 0, 1 et 4. Pour déterminer les restes possibles de $a^2 + b^2$ modulo 8, faisons un tableau à double entrée.

$b^2 \backslash a^2$	0	1	4
0	0	1	4
1	1	2	5
4	4	5	0

Comme $a^2 + b^2 = c^2$, le reste de $a^2 + b^2$ modulo 8 est 0, 1 ou 4. Or, si $a^2 + b^2$ est congru à 0 ou 4 modulo 8 alors a^2 et b^2 sont congrus à 0 ou 4 modulo 8 donc a et b sont pairs, ce qui est exclu. Ainsi, $a^2 + b^2 \equiv 1 \pmod{8}$ donc $a^2 \equiv 0 \pmod{8}$ et $b^2 \equiv 1 \pmod{8}$ ou $a^2 \equiv 1 \pmod{8}$ et $b^2 \equiv 0 \pmod{8}$. Ainsi, a^2 et b^2 sont de parités différentes et donc, finalement, a et b n'ont pas la même parité.

- d. Comme b est pair, u est entier. Comme b est pair, a est impair et donc c est aussi impair. Ainsi, $c + a$ et $c - a$ sont pairs et donc s et t sont des entiers. De plus, comme a , b et c sont strictement positifs, u et s sont strictement positifs et, comme $c^2 = a^2 + b^2 > a^2$, $c > a$ donc $t > 0$.
- e. Remarquons que $s - t = a$ et $s + t = c$. Notons $\delta = \text{PGCD}(s, t)$. Alors, δ divise s et t donc δ divise $s - t$ et $s + t$ donc δ divise a et c . Ainsi, δ divise a^2 et c^2 donc δ divise $c^2 - a^2 = b^2$. Dès lors, δ divise $\text{PGCD}(a^2, b^2)$. Or, comme a et b sont premiers entre eux, a^2 et b^2 aussi (d'après la question 1.). On conclut que $\delta = 1$ c'est-à-dire que s et t sont premiers entre eux.

- f. Par définition, $st = \frac{c+a}{2} \times \frac{c-a}{2} = \frac{c^2-a^2}{4} = \frac{b^2}{4} = u^2$ donc $\frac{p^2}{q^2} = \frac{u^2}{t^2} = \frac{st}{t^2} = \frac{s}{t}$. Or, les deux fractions $\frac{p^2}{q^2}$ et $\frac{s}{t}$ sont irréductibles (d'après les questions **2.e.** et **1.**) donc, par unicité de l'écriture sous forme irréductible, $p^2 = s$ et $q^2 = t$. On en déduit que $p^2 + q^2 = s + t = c$ donc, comme $n = dc$, $\boxed{n = d(p^2 + q^2)}$.

- g. On remarque que

$$\begin{aligned} [d(p^2 - q^2)]^2 + (2dpq)^2 &= d^2(p^4 - 2p^2q^2 + q^4) + 4d^2p^2q^2 \\ &= d^2(p^4 + 2p^2q^2 + q^4) \\ &= d^2(p^2 + q^2)^2 = n^2 \end{aligned}$$

donc le point M appartient bien à $\mathcal{C}_n$. De plus, comme d, p et q sont des entiers, M est entier et, enfin, comme $p > q > 0$, $\boxed{M \text{ est un point entier non trivial de } \mathcal{C}_n}$.

- h. Les questions précédentes montrent qu'un cercle $\mathcal{C}_n$ passe par des points entiers non triviaux si et seulement si n est de la forme $n = d(p^2 + q^2)$ où d est un entier strictement positif et p et q sont des entiers strictement positifs premiers entre eux.

Or, 7 n'a pas de diviseurs stricts autre que 1 et les seules façons d'écrire 7 comme une somme d'entiers strictement positifs sont $7 = 1 + 6 = 2 + 5 = 3 + 4$. Comme aucune de ces sommes n'est la somme de deux carrés d'entiers, on conclut que $\mathcal{C}_7$ ne passe pas par des points entiers non triviaux.

En revanche, 10 peut s'écrire $10 = 2 \times 5 = 2 \times (1 + 4) = 2 \times (2^2 + 1^2)$ donc le cercle $\mathcal{C}_{10}$ passe par des points entiers non triviaux : par exemple, le point $M(6; 8)$.

3. Points rationnels sur un cercle centré en O et dont le rayon est la racine carrée d'un entier (facultatif)

- a. Comme $\mathcal{C}$ ne contient pas de point entier, $M \neq N$ donc $d > 0$ et ainsi $d^2 > 0$.

Par ailleurs, comme u est l'entier le plus proche de x et v l'entier le plus proche de y , $|u - x| \leq \frac{1}{2}$ et $|v - y| \leq \frac{1}{2}$. Dès lors, $d^2 = (u - x)^2 + (v - y)^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$. Ainsi,

$$\boxed{0 < d^2 \leq \frac{1}{2}}.$$

- b. Comme $x^2 + y^2 = n$, on a

$$\begin{aligned} d^2 &= (u - x)^2 + (v - y)^2 = u^2 - 2ux + x^2 + v^2 - 2vy + y^2 \\ &= u^2 - 2u\frac{a}{m} + v^2 - 2v\frac{b}{m} + n \\ &= \frac{u^2m - 2ua + mv^2 - 2vb + nm}{m} \end{aligned}$$

donc, en posant $m' = u^2m - 2ua + mv^2 - 2vb + nm$, on a $d^2 = \frac{m'}{m}$. De plus, m' est un entier et $m' > 0$ car $d^2 > 0$ et $m > 0$. Comme $d^2 \leq \frac{1}{2}$, $d^2 < 1$ i.e. $\frac{m'}{m} < 1$ et, comme $m > 0$, $\boxed{m' < m}$.

- c. La droite (MN) est dirigée par le vecteur $\overrightarrow{NM}(x - u; y - v)$ et passe par le point N donc un point A appartient à (MN) si et seulement si $\overrightarrow{NA}$ et $\overrightarrow{NM}$ sont colinéaires i.e. si et seulement s'il existe un réel t tel que $\overrightarrow{NA} = t\overrightarrow{NM}$. En coordonnées, cette égalité se traduit par

$$\begin{cases} x_A - u = t(x - u) \\ y_A - v = t(y - v) \end{cases}$$

i.e.

$$\begin{cases} x_A = u + t(x - u) \\ y_A = v + t(y - v) \end{cases}$$

Ainsi, l'ensemble des points de (MN) est l'ensemble des points de coordonnées $(u + t(x - u); v + t(y - v))$ où $t \in \mathbb{R}$.

Un point de (MN) appartient à $\mathcal{C}_n$ si et seulement s'il existe un réel t tel que $(u + t(x - u))^2 + (v + t(y - v))^2 = n$. En développant, on obtient

$$d^2 t^2 + 2(u(x - u) + v(y - v))t + u^2 + v^2 - n = 0$$

Comme M appartient à $\mathcal{C}_n$ et que M correspond à $t = 1$, on peut affirmer que 1 est solution de l'équation du second degré précédente. Celle-ci a donc une autre solution qui est $t' = \frac{u^2 + v^2 - n}{d^2}$ (car le produit des racines d'un trinôme de la forme $ax^2 + bx + c$ est $\frac{c}{a}$). Notons que t' est différent de 1 car $u^2 + v^2 - n$ est un entier et $0 < d^2 \leq \frac{1}{2}$ donc $u^2 + v^2 - n \neq d^2$. Ainsi, $M \neq P$.

d. Comme P correspond à t' , les coordonnées de P sont

$$\begin{cases} x_P = u + \frac{u^2 + v^2 - n}{d^2}(x - u) \\ y_P = v + \frac{u^2 + v^2 - n}{d^2}(y - v) \end{cases}$$

Ainsi,

$$\begin{aligned} x_P &= u + \frac{u^2 + v^2 - n}{\frac{m'}{m}}(x - u) = \frac{m'u + (u^2 + v^2 - n)(mx - mu)}{m'} \\ &= \frac{m'u + (u^2 + v^2 - n)(a - mu)}{m'} \end{aligned}$$

donc, en posant $c = m'u + (u^2 + v^2 - n)(a - mu) \in \mathbb{Z}$, $x_P = \frac{c}{m'}$.

De même,

$$\begin{aligned} y_P &= v + \frac{u^2 + v^2 - n}{\frac{m'}{m}}(y - v) = \frac{m'v + (u^2 + v^2 - n)(my - mv)}{m'} \\ &= \frac{m'v + (u^2 + v^2 - n)(b - mv)}{m'} \end{aligned}$$

donc, en posant $c' = m'v + (u^2 + v^2 - n)(b - mv) \in \mathbb{Z}$, $y_P = \frac{c'}{m'}$.

e. Comme $m' < m$, on aboutit à une contradiction par minimalité de m . Ainsi, $\mathcal{C}_n$ passe par un point entier.