démontrer que π divise les trois facteurs, mais qu'un seul est divisible par π^2.

c) Démontrer que π est un PGCD des trois facteurs.

d) En déduire qu'il existe des éléments λ, μ, ν de $\mathbf{Z}[j]$, premiers entre eux deux à deux, non divisibles par π, et des éléments inversibles ϵ_1, ϵ_2, ϵ_3 tels que l'on ait

$$\alpha + \beta' = \epsilon_1 \pi \lambda^3, \qquad \alpha + j\,\beta' = \epsilon_2 \pi \mu^3, \qquad \alpha + j^2\,\beta' = \epsilon_3 \pi^{3n-2} \nu^3,$$

où β' désigne l'une des racines cubiques de β^3, c'est-à-dire β, $j\beta$ ou $j^2\beta$.

e) En déduire qu'il existe des éléments inversibles η_1 et η_2 de $\mathbf{Z}[j]$ tels que l'on ait

$$\lambda^3 + \eta_1 \mu^3 + \eta_2 \pi^{3n-3} \nu^3 = 0.$$

f) Démontrer l'égalité $\eta_1 = \pm 1$.

5) En utilisant la question précédente, rédiger une démonstration du fait que l'équation $x^3 + y^3 = z^3$, où x, y, z sont tous $\neq 0$, n'a pas de solution dans $\mathbf{Z}$.

4.1.2 Solution de la première épreuve écrite

Ce problème traite de résultats classiques en arithmétique. D'abord les triangles rectangles à côtés entiers, question connue depuis l'Antiquité. Ensuite l'équation de Fermat pour l'exposant 4, abordée ici aussi en arithmétique réelle. La dernière partie traite l'exposant 3, en se plaçant dans l'anneau $\mathbf{Z}[j]$. Cette question a été résolue par Euler. Rappelons cependant qu'une « erreur d'Euler » avait été d'appliquer la factorisation unique dans l'anneau $\mathbf{Z}[i\sqrt{3}]$. Nous suivons ici la présentation de Landau exposée dans HARDY and WRIGHT, *An Introduction to the Theory of Numbers*. Par le même type de méthodes, la quatrième partie étudie les points entiers d'une cubique plane.

I . La relation $a^2 + b^2 = c^2$

1) a) On a

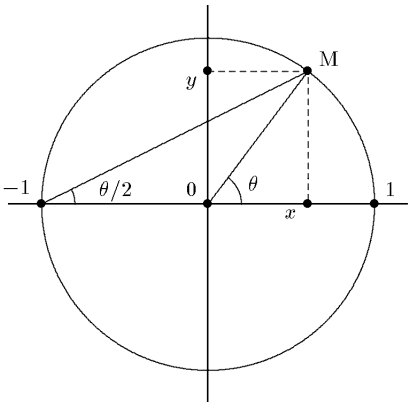
$$x = \cos\theta = \frac{1 - t^2}{1 + t^2}, \qquad y = \sin\theta = \frac{2t}{1 + t^2}\cdot$$

Si t est un nombre rationnel, les nombres x et y sont aussi rationnels.

b) On a $t = \dfrac{y}{1 + x}\cdot$ On peut le voir à partir des deux relations

$$t^2(x + 1) + x - 1 = 0, \qquad t^2\,y - 2t + y = 0.$$

On peut aussi remarquer que t est la pente de la droite joignant le point $(-1, 0)$ au point M.



Par suite, si x et y sont rationnels, t l'est aussi.

2) a) Comme $0 < t < 1$, on a $0 < v < u$, et

$$\frac{a}{c} = \frac{1-t^2}{1+t^2} = \frac{u^2-v^2}{u^2+v^2}, \qquad \frac{b}{c} = \frac{2t}{1+t^2} = \frac{2uv}{u^2+v^2}.$$

b) Les diviseurs communs aux nombres u^2+v^2 et u^2-v^2 divisent leur somme $2u^2$ et leur différence $2v^2$. Comme les nombres u et v sont premiers entre eux, un diviseur premier commun à $2u^2$ et $2v^2$ ne peut être que ± 2. Mais on a supposé les parités de u et v différentes, de sorte que le nombre u^2+v^2 est impair. Par suite les nombres u^2+v^2 et u^2-v^2 n'ont pas de diviseur premier en commun ; ils sont premiers entre eux.

Un diviseur premier commun à $2uv$ et u^2+v^2 divise aussi u^2+v^2+2uv et u^2+v^2-2uv, c'est-à-dire $(u+v)^2$ et $(u-v)^2$. Comme il est premier, il divise aussi $u+v$ et $u-v$, et on raisonne comme ci-dessus.

c) Si les parités des nombres u et v sont différentes, les fractions $(u^2-v^2)/(u^2+v^2)$ et $2uv/(u^2+v^2)$ sont irréductibles d'après ce qui précède. Elles sont égales respectivement aux fractions a/c et b/c. Il existe donc un entier $w \neq 0$ tel que $a = (u^2-v^2)\,w$, $b = 2\,u\,v\,w$, $c = (u^2+v^2)\,w$.

d) Si les nombres u et v sont tous deux impairs, les nombres u^2+v^2, u^2-v^2 et $2uv$ sont pairs. Comme dans la question b) ci-dessus, un diviseur commun à $(u^2+v^2)/2$ et à $(u^2-v^2)/2$ divise les nombres u^2 et v^2 qui sont premiers entre eux. Il en résulte que les nombres $(u^2+v^2)/2$ et $(u^2-v^2)/2$ sont premiers entre eux.

De même, un diviseur premier commun à $(u^2+v^2)/2$ et à uv divise aussi $(u-v)^2/2$; comme le nombre uv est impair, ce diviseur premier ne peut être égal à ± 2. Comme ci-dessus, il divise $2u$ et $2v$, donc aussi u et v, ce qui est impossible. Par suite les nombres $(u^2+v^2)/2$ et uv sont premiers entre eux.

Il existe donc un entier $w \neq 0$ tel que

$$a = \frac{u^2-v^2}{2}\,w, \qquad b = u\,v\,w, \qquad c = \frac{u^2+v^2}{2}\,w.$$

e) Sous l'hypothèse que les nombres u et v sont impairs, les nombres $u+v$ et $u-v$ sont pairs. Posons

$$u' = \frac{u+v}{2}, \qquad v' = \frac{u-v}{2}.$$

On a alors $(u^2-v^2)/2 = 2\,u'\,v'$, $uv = u'^2 - v'^2$ et $(u^2+v^2)/2 = u'^2+v'^2$. Les nombres u' et v' sont premiers entre eux car un diviseur commun diviserait aussi leur somme u et leur différence v. Leurs parités sont distinctes car u et v sont impairs.

3) a) Un diviseur premier commun à a et c divise $b^2 = c^2 - a^2$; il divise donc b. Par suite, si a, b et c sont premiers entre eux dans leur ensemble, les nombres a et c sont premiers entre eux. On démontrerait de façon analogue que les nombres a et b (resp. b et c) sont premiers entre eux.

Ainsi, si deux des entiers a, b et c sont premiers entre eux, ils sont tous premiers entre eux deux à deux.

b) Soit $n = 2k + 1$ un entier impair. On a $n^2 = 4k^2 + 4k + 1$, d'où $n^2 \equiv 1 \pmod 4$. Comme a et b sont premiers entre eux, ils ne peuvent être tous deux pairs. Si a et b sont tous deux impairs, alors $a^2 + b^2 \equiv 2 \pmod 4$. Selon la parité de c, on a $c^2 \equiv 0$ ou $1 \pmod 4$, ce qui est contradictoire. Donc a et b n'ont pas la même parité.

c) Compte tenu des questions (I.2.c) et (I.2.e), il existe des entiers u, v et w tels que l'on ait les relations (I.2.c). Comme les entiers a, b et c sont premiers entre eux deux à deux, on a nécessairement $w = 1$, et les entiers u et v sont premiers entre eux. De plus u et v ont des parités différentes, sinon les entiers a, b et c seraient tous pairs.

4) a) Le nombre a est impair. On a $a^2 + v^2 = u^2$, ce qui est impossible si a et v sont impairs comme on l'a vu dans la question (I.3.b). Donc le nombre v est pair.

b) D'après la question précédente, on a $v = 2v'$, d'où $b^2 = 4uv'$. Dans l'écriture de b^2 comme produit de diviseurs premiers, chaque diviseur premier figure avec un exposant pair en raison de l'unicité de la factorisation. Pour la même raison d'unicité, la factorisation de b^2 est le produit des factorisations de 4, de u^2 et v'^2. Comme u et v' sont premiers entre eux, les diviseurs premiers de b^2 figurent avec un exposant pair dans chacun des facteurs 4, u^2 et v'^2. Ceci prouve que u et v' sont les carrés de nombres x et y premiers entre eux : $u = x^2$, $v' = y^2$, d'où $v = 2y^2$. Le nombre x est impair puisque le nombre u est impair.

c) On a $x^4 = u^2 = a^2 + v^2 = a^2 + (2y^2)^2$. Comme u et v sont premiers entre eux, a et v sont premiers entre eux. En remarquant que v est pair, et en appliquant à nouveau la question (I.3), on voit qu'il existe deux nombres entiers s et t strictement positifs, premiers entre eux, tels que $y^2 = st$, $x^2 = s^2 + t^2$.

d) Comme s et t sont premiers entre eux et que leur produit st est le carré y^2, par le même raisonnement que dans la question (I.4.b), on démontre que s et t sont des carrés.

e) On a bien $m^4 + n^4 = s^2 + t^2 = x^2$. Par ailleurs on a $0 < x \leqslant x^4 < x^4 + (2y^2)^2 = u^2 + v^2 = c$.

f) C'est pour cette démonstration que Fermat invoque le principe de *descente infinie*. Supposons donnés trois nombres entiers a, b, c, strictement positifs, tels que $a^4 + b^4 = c^2$. En raison de cette égalité, les diviseurs premiers communs de chaque couple (a, b), (b, c) et (c, a) sont les mêmes. En divisant a, b et c par leur PGCD, on est ramené à des nombres premiers entre eux deux à deux (question (I.3.a)). En échangeant les noms de a et b, on peut supposer que b est pair (question (I.3.b)). Les questions (I.4.a) à (I.4.e) montrent que l'on peut trouver un nouveau triplet (a, b, c) solution de $a^4 + b^4 = c^2$, où c est strictement plus petit que le c initial. Et Fermat conclut par l'impossibilité d'une descente infinie dans l'ensemble des entiers > 0.

En termes plus modernes, on peut présenter la démonstration par récurrence ou par l'absurde.

Par l'absurde, on suppose qu'il existe des triplets (a, b, c) de nombres > 0 tels que $a^4 + b^4 = c^2$. On en choisit un pour lequel c est minimal. Alors a, b et c sont premiers entre eux deux à deux. Les questions (I.4.a) à (I.4.e) montrent que c n'est pas minimal, d'où la contradiction.

Par récurrence, on suppose l'impossibilité démontrée pour toute valeur de $c < \mathrm{C}$, et on démontre l'impossibilité pour $c = \mathrm{C}$. On raisonne comme ci-dessus pour trouver un $c < \mathrm{C}$ avec un raisonnement par l'absurde. Le raisonnement est initialisé pour $c = 1$ qui est évident.

La démonstration par l'absurde semble plus économique à rédiger que la démonstration par récurrence.

II . L'anneau $\mathbf{Z}[i\sqrt{2}]$

1) L'ensemble $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ est stable par l'addition et la multiplication des nombres complexes :

$$(a + ib\sqrt{2}) + (c + id\sqrt{2}) = (a + c) + i(b + d)\sqrt{2},$$
$$(a + ib\sqrt{2})(c + id\sqrt{2}) = ac - 2bd + i(ad + bc)\sqrt{2}.$$

L'opposé $-a - ib\sqrt{2}$ d'un élément $a + ib\sqrt{2}$ de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ appartient à $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

Enfin l'élément 1 de $\mathbf{C}$ appartient à $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

Par suite $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ est un sous-anneau de $\mathbf{C}$. À ce titre, c'est un anneau commutatif intègre.

2) a) Si $a + ib\sqrt{2}$ est un élément de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, $\mathrm{N}(a + ib\sqrt{2}) = a^2 + 2b^2$ est entier $\geqslant 0$.

b) Si un élément $\alpha = a + ib\sqrt{2}$ de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ est inversible dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, alors $\mathrm{N}(\alpha)$ et $\mathrm{N}(\alpha^{-1})$ sont des entiers $\geqslant 0$ dont le produit est 1. Donc $\mathrm{N}(\alpha) = 1$.

Inversement, si $\mathrm{N}(\alpha) = 1$, alors α est $\neq 0$ et son inverse dans $\mathbf{C}$ est $\alpha^{-1} = \overline{\alpha}/\mathrm{N}(\alpha) = a - ib\sqrt{2}$ qui appartient à $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

c) Les éléments inversibles de l'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ sont ceux dont le module vaut 1, c'est-à-dire les seuls éléments 1 et -1.

3) Posons $\alpha/\beta = a + ib$, où a et $b \in \mathbf{R}$. Le couple (a, b) se trouve dans un rectangle $\mathrm{A} \leqslant x \leqslant \mathrm{A} + 1$, $\mathrm{B}\sqrt{2} \leqslant y \leqslant (\mathrm{B} + 1)\sqrt{2}$ du plan $\mathbf{R}^2$, où A et B sont les parties entières inférieures de a et $b/\sqrt{2}$. Les disques fermés, de rayon la demi-diagonale $\sqrt{3}/2$, centrés aux quatre sommets du rectangle, recouvrent le rectangle. Il y a donc un sommet du rectangle qui est à une distance < 1 du point (a, b). Les affixes des sommets du rectangle sont des éléments de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. Il y a donc un élément γ de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ tel que $|\gamma - \frac{\alpha}{\beta}| < 1$. D'où le résultat.

4) La démonstration est analogue à celle que l'on donne pour $\mathbf{Z}$ en utilisant la division euclidienne.

Il s'agit de démontrer que tout idéal de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ est monogène. Soit I un idéal de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ non réduit à 0. Comme toute partie bornée de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ est finie, l'idéal I contient un élément $\beta \neq 0$ de plus petit module. Soit α un (autre) élément de I et soient γ et $\delta \in \mathbf{Z}[\mathrm{i}\sqrt{2}]$ tels que $\alpha = \beta\gamma + \delta$ et $|\delta| < |\beta|$. L'élément $\delta = \alpha - \beta\gamma$ appartient à I. Comme $|\delta| < |\beta|$ et puisque $|\beta|$ est minimal dans $\mathrm{I} - \{0\}$, c'est que $\delta = 0$, donc $\alpha = \beta\gamma$. On a ainsi prouvé que tout élément de I est un multiple de β dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. Inversement, tout multiple de β dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ appartient à I. Donc l'idéal I est l'ensemble des multiples de β dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

5) Remarquons d'abord que 2 n'est pas irréductible dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ car $2 = -(i\sqrt{2})^2$.

Soit $\alpha \in \mathbf{Z}[\mathrm{i}\sqrt{2}]$ un diviseur de 2 dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. On a donc $2 = \alpha\beta$, où $\beta \in \mathbf{Z}[\mathrm{i}\sqrt{2}]$, d'où $\mathrm{N}(\alpha)\mathrm{N}(\beta) = 4$.

Comme $\mathrm{N}(\alpha)$ est entier et divise 4 dans $\mathbf{Z}$, les seules valeurs possibles pour $\mathrm{N}(\alpha)$ sont 1, 2 et 4.

Si $\mathrm{N}(\alpha) = 1$, on a vu (II.2.b) que α est inversible, ce qui est exclus.

Si $\mathrm{N}(\alpha) = 4$, alors $\beta = \pm 1$ est inversible, et $\alpha = \pm 2$ n'est pas irréductible.

Si $\mathrm{N}(\alpha) = 2$, alors α n'est pas inversible. De plus, si $\alpha = \gamma\delta$ dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, on a $\mathrm{N}(\gamma)\mathrm{N}(\delta) = 2$, donc $\mathrm{N}(\gamma)$ ou $\mathrm{N}(\delta)$ est égal à 1, et l'un des facteurs est inversible. Par suite α est irréductible dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. Les éléments α de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ tels que $\mathrm{N}(\alpha) = 2$ sont $i\sqrt{2}$ et $-i\sqrt{2}$.

III . Somme et différence de deux carrés

1) a) Compte tenu de la première relation (B), on sait d'après (I.3) que les entiers m et n ont des parités distinctes. Il résulte alors des deux relations (B) que les nombres p et q sont impairs.

b) Comme m et n sont premiers entre eux, la relation $m^2 - n^2 = q^2$ entraîne que q et n sont premiers entre eux.

c) Comme dans a), la deuxième relation (B) entraîne que les entiers n et q ont des parités distinctes. D'après a), l'entier n est donc pair. Comme n est pair et p impair, les relations (B) montrent que l'entier m est impair.

On peut aussi dire que les carrés p^2 et q^2 sont $\equiv 1 \pmod 4$, donc $m^2 \equiv 1 \pmod 2$ et $n^2 \equiv 0 \pmod 2$ d'après les relations (C). Par suite m est impair et n est pair.

2) a) Si π divise $(q + in\sqrt{2})$ et $(q - in\sqrt{2})$ dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, il divise leur somme $2q$ et leur différence $2in\sqrt{2}$.

b) Rappelons d'abord que $\mathrm{N}(\pi) = \pi\overline{\pi}$ est un nombre entier. Si π divisait q et n dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, l'entier $\mathrm{N}(\pi)$ diviserait q^2 et n^2 dans $\mathbf{Z}$, ce qui est contradictoire avec (III.1.b).

c) D'après (II.5), les seuls diviseurs irréductibles de 2 dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ sont $\pm i\sqrt{2}$. Si $\pi = \pm i\sqrt{2}$ divise $(q + in\sqrt{2})$ dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, alors π divise q dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, et $\mathrm{N}(\pi) = 2$ divise q^2 dans $\mathbf{Z}$, ce qui est contradictoire avec (III.1.a).

d) D'après les trois questions précédentes, $(q + in\sqrt{2})$ et $(q - in\sqrt{2})$ sont premiers entre eux dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

3) a) Dans l'anneau principal $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, on a $p^2 = (q + in\sqrt{2})(q - in\sqrt{2})$ et les deux facteurs sont premiers entre eux. Ce sont donc des carrés au signe près (i.e. multiplication par un élément inversible de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$).

b) On a $q' + in\sqrt{2} = (f + ig\sqrt{2})^2 = f^2 - 2g^2 + 2fgi\sqrt{2}$. Si les entiers f et g avaient un diviseur commun dans $\mathbf{Z}$, ce serait un diviseur commun à q et n. D'après la question (III.1.b), q et n sont premiers entre eux, donc f et g sont premiers entre eux.

Comme $q' = f^2 - 2g^2$ est impair, f est impair.

c) On a $m^2 = q^2 + n^2 = (f^2 - 2g^2)^2 + 4f^2g^2 = f^4 + 4\,g^4$. Les nombres f^2 et $2g^2$ sont premiers entre eux. D'après la question (I.3), il existe des nombres entiers u et v, premiers entre eux, de parités distinctes, tels que

$$f^2 = u^2 - v^2, \qquad 2g^2 = 2uv.$$

d) Puisque u et v sont premiers entre eux, positifs et que leur produit est un carré dans $\mathbf{Z}$, ce sont tous deux des carrés dans $\mathbf{Z}$.

e) On a $f^2 = u^2 - v^2 = (u - v)(u + v)$. D'après (III.4.b), le nombre f est impair, donc les nombres $u + v$ et $u - v$ sont impairs. Si $u + v$ et $u - v$ ont un diviseur commun p dans $\mathbf{Z}$, alors p est impair

et divise leur somme $2u$ et leur différence $2v$. Comme u et v sont premiers entre eux, c'est impossible ; par suite les nombres $u+v$ et $u-v$ sont premiers entre eux dans $\mathbf{Z}$.

f) On a $f^2 = u^2 - v^2 = (u-v)(u+v)$; comme $u-v$ et $u+v$ sont premiers entre eux et positifs, ce sont des carrés dans $\mathbf{Z}$. Ainsi a^2+b^2 et a^2-b^2 sont des carrés dans $\mathbf{Z}$.

g) $a^2+b^2 \leqslant a^4+b^4 = u^2+v^2 < (u^2+v^2)^2 = m^2 < m^2+n^2$.

h) Pour deux entiers m et n strictement positifs, soit $\mathrm{P}(m,n)$ la propriété que m^2+n^2 et m^2-n^2 soient des carrés dans $\mathbf{Z}$. Procédons par l'absurde. Supposons qu'il existe des couples (m,n) ayant la propriété $\mathrm{P}(m,n)$; il en existe alors un pour lequel m^2+n^2 est minimal.

Soit (m,n) un tel couple. Soit d le PGCD de m et n. En remplaçant m et n par m/d et n/d, on obtient des entiers premiers entre eux m' et n', et le couple (m',n') a la propriété $\mathrm{P}(m',n')$. En raison de la minimalité de m^2+n^2, m et n sont premiers entre eux.

Les questions (III.2) à (III.4) conduisent à un couple (a,b) d'entiers >0 ayant la propriété $\mathrm{P}(a,b)$ et tels que $a^2+b^2 < m^2+n^2$. C'est contradictoire avec la minimalité de m^2+n^2.

5) Soient a, b, c les longueurs des côtés BC, CA, AB du triangle. On a l'égalité $a^2 = b^2+c^2$ (théorème de Pythagore). L'aire du triangle est égale à $bc/2$. Raisonnons par l'absurde, et supposons que l'aire du triangle soit égale au carré d^2 d'un entier d. On a alors $bc = 2d^2$. Il en résulte

$$(b+c)^2 = b^2+2bc+c^2 = a^2+(2d)^2,$$
$$(b-c)^2 = b^2-2bc+c^2 = a^2-(2d)^2.$$

On obtient ainsi deux carrés dont la somme et la différence sont aussi des carrés, ce qui est impossible d'après la question (III.4).

6) Soient x, y et z des entiers >0 satisfaisant à l'égalité $x^4-y^4 = z^2$.

Le produit $x^2y^2z^2 = x^2y^2(x^4-y^4)$ est l'aire du triangle rectangle dont les côtés de l'angle droit sont x^4-y^4 et $2x^2y^2$, et le grand côté x^4+y^4. Ce n'est pas possible d'après la question (III.5).

IV . La relation $x^3-y^2=2$

1) a) Le vecteur gradient $(3x_0^2, -2y_0)$ est normal à la courbe C au point de coordonnées (x_0,y_0). La tangente en M_0 à la courbe C a pour équation paramétriques

$$x = x_0+2y_0t, \qquad y = y_0+3x_0^2t.$$

b) L'équation aux t des points communs à la courbe C et à la droite T_0 est

$$8y_0t^3 + t^2(12x_0y_0^2 - 9x_0^4) = 0.$$

L'équation en t possède la racine double $t=0$ correspondant au point de contact M_0.

Pour $y_0 = 0$, $x_0 = \sqrt[3]{2}$, la tangente est verticale et ne recoupe pas la courbe C.

Pour $y_0 \neq 0$, L'équation en t possède une troisième racine t_1 correspondant à un point $\mathrm{M}_1 = (x_1,y_1)$. On obtient

$$t_1 = \frac{9x_0^4 - 12x_0y_0^2}{8y_0^3}, \qquad x_1 = \frac{x_0^4+16x_0}{4y_0^2}, \qquad y_1 = \frac{-x_0^6+40x_0^3+32}{8y_0^3}.$$

ou encore

$$x_1 = \frac{x_0^4+16\,x_0}{4\,(x_0^3-2)}, \qquad y_1 = \frac{-y_0^4+36\,y_0^2+108}{8y_0^3}.$$

c) Le point M_1 est distinct de M_0 lorsque $t_1 \neq 0$. La condition $t_1 = 0$ s'écrit $12x_0y_0^2 - 9x_0^4 = 0$; ce qui donne $3x_0^3 = 4y_0^2$, d'où $3x_0^3 = 4x_0^3 - 8$, et finalement

$$x_0 = 2, \qquad y_0 = \pm\sqrt{6}.$$

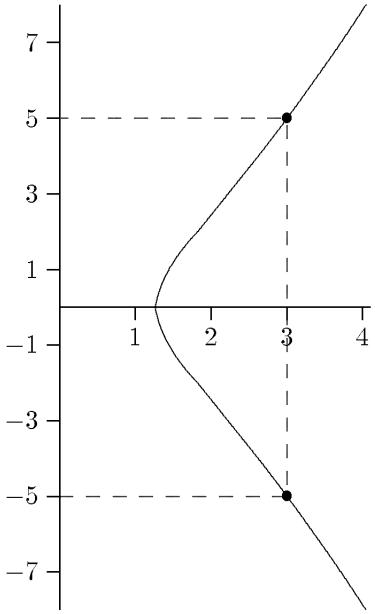
Lorsque $x_0 \neq 2$, la tangente en M_0 rencontre la courbe C en un point M_1 distinct de M_0 ; la courbe n'est pas convexe. Les point d'inflexion, points de changement de convexité, sont les points M_0 pour les quels le point M_1 est confondu avec M_0, c'est-à-dire $x_0 = 2$, $y_0 = \pm\sqrt{6}$.

d) La courbe C admet l'axe des abscisses comme axe de symétrie.

Elle le rencontre au point d'abscisse $x = \sqrt[3]{2}$.

Lorsque y tend vers $\pm\infty$, x tend vers $+\infty$ et $x \sim y^{2/3}$. C'est une branche parabolique dans la direction verticale.

e)



2) $x = 3$, $y = \pm 5$.

3) a) Soit π un élément irréductible de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ qui divise $(y - i\sqrt{2})$ et $(y + i\sqrt{2})$. Alors π divise $2i\sqrt{2} = -(i\sqrt{2})^3$. Par suite π divise $i\sqrt{2}$ donc, d'après (II.5), on a $\pi = \pm i\sqrt{2}$. Par suite π divise y, et $\pi\overline{\pi} = 2$ divise y^2 dans $\mathbf{Z}$. Comme y^2 est un carré, il est divisible par 4, et $y^2 + 2$ n'est pas divisible par 4. Donc x n'est pas divisible par 2, d'où une contradiction avec l'égalité $x^3 = (y - i\sqrt{2})(y + i\sqrt{2})$ et le fait que $i\sqrt{2}$ divise chaque facteur.

b) On en déduit que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont des cubes dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ multipliés par un élément inversible. Mais les éléments inversibles de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ sont 1 et -1 qui sont des cubes. Donc $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont des cubes.

c) Écrivons $y + i\sqrt{2} = (a + ib\sqrt{2})^3$, où a, $b \in \mathbf{Z}$. En développant, on obtient

$$y + i\sqrt{2} = (a^3 - 6ab^2) + i(3a^2b - 2b^3)\sqrt{2}.$$

De $b\,(3a^2-2b^2)=1$, on déduit $b=3a^2-2b^2=\pm1$, donc $b^2=1$, $3a^2-2=1$, $b=1$, $a=\pm1$.

Donc $y=a^3-6ab^2=\pm5$ et $x^3=y^2+2=27$, $x=3$.

Les seuls points à coordonnées entières de la courbe C sont les points $(3,5)$ et $(3,-5)$.

4) a) Prenons pour P_0 le point $(3,\,5)$ de la courbe C. Les coordonnées du point P_1 sont

$$x_1=\frac{x_0^4+16\,x_0}{4\,(x_0^3-2)}=\frac{129}{100},\qquad y_1=\frac{-y_0^4+36\,y_0^2+108}{8y_0^3}=\frac{383}{1000}.$$

Les coordonnées de P_{n+1} sont données, à partir de celles de P_n, par les relations

$$x_{n+1}=\frac{x_n^4+16\,x_n}{4\,(x_n^3-2)},\qquad y_{n+1}=\frac{-y_n^4+36\,y_n^2+108}{8y_n^3}.$$

On en déduit que les coordonnées des points P_n sont rationnelles.

b) Étant donné un nombre rationnel $x\neq0$, notons $v_2(x)$ l'exposant de 2 dans la factorisation de x comme produit de puissances de nombres premiers, avec des exposants positifs ou négatifs.

Les relations ci-dessus permettent de voir que $v_2(x_n)$ est $\leqslant0$ et que $v_2(x_{n+1})=4v_2(x_n)-2$. Il en résulte que la suite des points P_n est injective et que la courbe C a une infinité de points dont les coordonnées sont rationnelles.

V . L'équation $x^3+y^3=z^3$

1) a) Résulte du fait que $j^2=-1-j$.

b) Comme pour l'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, si $\alpha=a+jb$ est un élément de $\mathbf{Z}[j]$, le nombre

$$\mathrm{N}(\alpha)=(a+jb)(a+j^2b)=a^2-ab+b^2$$

est entier.

c) Les éléments inversibles de $\mathbf{Z}[j]$ sont les éléments dont le module est 1. Ce sont ±1, $\pm j$ et $\pm j^2$.

d) L'anneau $\mathbf{Z}[j]$ est un anneau principal. La démonstration est analogue à celle donnée pour $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. Les éléments de $\mathbf{Z}[j]$ sont les sommets d'un pavage du plan par des triangles équilatéraux dont le côté a pour longueur 1. Tout point d'un tel triangle est à une distance $\leqslant\sqrt{3}/3$ de l'un des sommets. On a donc un théorème de division sans unicité dans $\mathbf{Z}[j]$

On procède alors comme pour $\mathbf{Z}$ et $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ en utilisant cette division.

e) Comme $\mathrm{N}(\pi)=3$ est un nombre premier, π est irréductible dans $\mathbf{Z}[j]$.

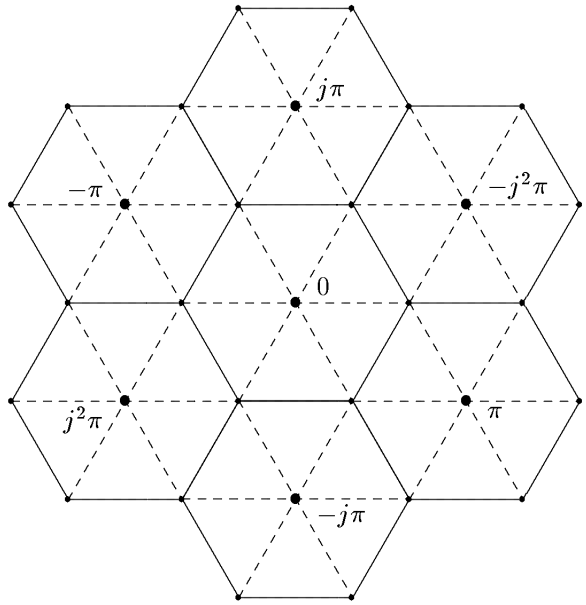
2) Soit α un élément de $\mathbf{Z}[j]$. Ecrivons la division euclidienne de α par π :

$$\alpha=\pi\,\gamma+\delta,\qquad\text{avec}\qquad|\delta|<\sqrt{3}.$$

On a donc $\delta=0$ ou $|\delta|=1$. Si $\delta=0$, alors π divise α. Sinon, δ est un élément inversible et $\delta^3=\pm1$.

$$\begin{aligned}\alpha^3-\delta^3&=(\alpha-\delta)(\alpha-j\delta)(\alpha-j^2\delta),\\&=\pi^3\gamma(\gamma+\delta)(\gamma-j^2\delta).\end{aligned}$$

Les trois derniers facteurs sont les affixes des sommets d'un triangle équilatéral dont le côté mesure 1. L'un d'entre eux est donc divisible par π (voir figure). Il résulte de cela que $\alpha^3\pm1$ est divisible par π^4 dans $\mathbf{Z}[j]$.



3) Supposons, par l'absurde, que π ne divise aucun des éléments α, β ou γ ; alors chacun d'entre eux est congru à $\pm 1 \pmod{\pi^4}$ d'après la question (V.2). Par suite $\alpha^3+\beta^3+\gamma^3$ est congru à ± 1 ou $\pm 3 \pmod{\pi^4}$. Or $|\pi^4| = 9$ et π^4 ne peut diviser ± 1 ni ± 3. D'où la contradiction.

4) a) Comme α, β et γ sont premiers entre eux dans $\mathbf{Z}[j]$, π ne divise ni α ni β. D'après la question (V.2), α et β sont $\equiv \pm 1 \pmod{\pi^4}$; donc $-\epsilon\gamma^3$ est congru à 0 ou $\pm 2 \pmod{\pi^4}$. Par hypothèse, π divise γ, mais π ne divise pas 2 car $|\pi| = \sqrt{3}$; donc γ^3 est divisible par π^4, et nécessairement π^2 divise γ.

b) Considérons les trois facteurs du second membre de l'égalité

$$-\epsilon\,\gamma^3 = (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta).$$

On a

$$(\alpha+\beta)-(\alpha+j\beta) = \pi\beta, \qquad (\alpha+\beta)-(\alpha+j^2\beta) = j\pi\beta. \tag{D}$$

L'élément irréductible π divise γ, il divise donc un des facteurs. D'après les relations (D), l'élément π divise les trois facteurs. Mais π^2 divise un seul facteur car π ne divise pas β.

c) Un autre diviseur irréductible commun aux trois facteurs doit diviser $\pi\beta$, donc β. Il doit aussi diviser $(\alpha+j\beta)-j(\alpha+j^2\beta) = \pi\alpha$ donc α. C'est impossible puisque α et β sont premiers entre eux.

Ainsi π est le seul diviseur commun aux trois facteurs.

d) Chacun des facteurs est donc égal à π multiplié par un élément inversible et par un cube. Autrement dit, il existe des éléments λ, μ, ν de $\mathbf{Z}[j]$, premiers entre eux deux à deux, non divisibles par π, et des éléments inversibles ϵ_1, ϵ_2, ϵ_3 tels que l'on ait

$$\alpha+\beta = \epsilon_1\,\pi\,\lambda^3, \qquad \alpha+j\,\beta = \epsilon_2\,\pi\,\mu^3, \qquad \alpha+j^2\,\beta = \epsilon_3\,\pi^{3n-2}\,\nu^3.$$

e) On a

$$(\alpha+\beta)+j(\alpha+j\beta)+j^2(\alpha+j^2\beta) = (1+j+j^2)(\alpha+\beta) = 0.$$

On en déduit, en posant $\eta_1 = \epsilon_1^{-1}\epsilon_2$, $\eta_2 = \epsilon_1^{-1}\epsilon_3$, et en divisant par π^3 :

$$\lambda^3 + \eta_1\,\mu^3 + \eta_2\,\pi^{3n-3}\,\nu^3 = 0. \qquad \text{(E)}$$

f) Rappelons que n est $\geqslant 2$ (question a)) et que λ^3 et μ^3 sont congrus à ± 1 (mod π^4) (question (V.2)). En conséquence de l'égalité (E) , l'élément π^2 divise un élément ξ de la forme $\pm 1 \pm \eta_1$. Le module de $\pm 1 \pm \eta_1$ est au plus 2 et le module de π^2 est 3 . Nécessairement $\xi = 0$, donc $\eta_1 = \pm 1$.

5) On procède par l'absurde. Supposons qu'il existe des éléments x , y , z de $\mathbf{Z}$, tous $\neq 0$, et tels que $x^3 + y^3 = z^3$. En divisant x , y et z par leur PGCD, on obtient de nouveaux éléments x , y , z de $\mathbf{Z}$, tous $\neq 0$, premiers entre eux deux à deux et tels que $x^3 + y^3 = z^3$.

Remarquons que les entiers x , y , z sont aussi premiers entre eux dans $\mathbf{Z}[j]$. En effet, si $\delta \in \mathbf{Z}[j]$ divise x et y dans $\mathbf{Z}[j]$, l'entier $\mathrm{N}(\delta)$ divise x^2 et y^2 ; par suite $\mathrm{N}(\delta) = 1$ et δ est un élément inversible de $\mathbf{Z}[j]$.

Enfin, d'après la question (V.3), l'un des éléments x , y ou z est divisible par π .

Considérons maintenant tous les triplets (α, β, γ) d'éléments de $\mathbf{Z}[j]$, premiers entre eux dans $\mathbf{Z}[j]$, tels que γ soit divisible par π et pour lesquels il existe un élément inversible ϵ de $\mathbf{Z}[j]$ tel que l'on ait la relation

$$\alpha^3 + \beta^3 + \epsilon\,\gamma^3 = 0.$$

Il y a bien de tels triplets puisque le triplet (x, y, z) , à permutation près, convient.

Pour un tel triplet (α, β, γ) , soit n le plus grand exposant tel que π^n divise γ . Choisissons un triplet (α, β, γ) pour lequel l'exposant n est minimal. D'après la question (4.a), n est $\geqslant 2$. D'après la question 4), on peut trouver un nouveau triplet pour lequel l'exposant est $n - 1$. Ceci est contradictoire avec la minimalité de l'entier n . D'où le résultat par l'absurde.

On notera que la démonstration d'un énoncé sur les entiers a nécessité la démonstration d'un énoncé plus général (introduction de l'élément inversible ϵ) et dans un cadre plus général ($\mathbf{Z}[j]$ au lieu de $\mathbf{Z}$), afin que la descente puisse fonctionner.

4.1.3 Commentaires sur la première épreuve écrite

Cette épreuve appelle peu de commentaires. Les candidats ont suivi la progressivité du problème et les meilleures copies ont réussi à aborder significativement les dernières parties.

Un certain nombre de copies montrent que leurs auteurs ne sont pas à l'aise avec les notions de nombres premiers et de nombres premiers entre eux, ainsi qu'avec les théorèmes de divisibilité correspondant. Ces copies sont heureusement peu nombreuses, mais les correcteurs d'un concours interne s'étonnent que des candidats, professeurs en exercice, puissent laisser apparaître de telles lacunes dans leurs copies.