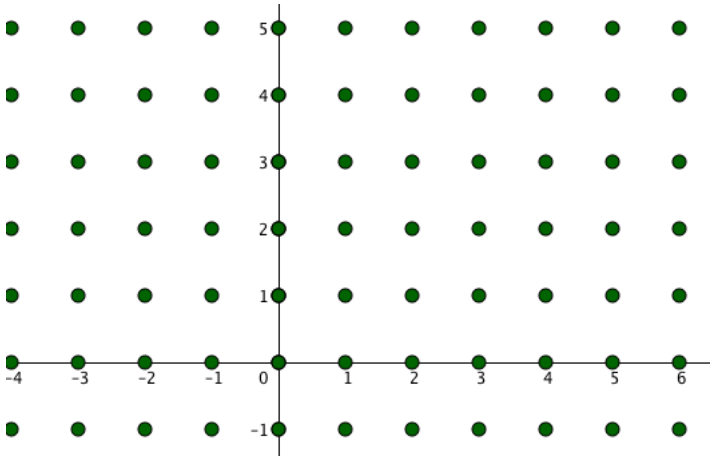
DM 8 (*) L'équation du Pythagore par la voie directissime : $\mathbb{Z}[i]$

1) a) Trois propriétés à vérifier pour montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$:
(SA1) $\mathbb{Z}[i]$ est un sous-groupe de $(\mathbb{C}, +)$,
(SA2) $]\mathbb{Z}[i]$ contient 1,
(SA3) $\mathbb{Z}[i]$ est stable par $\times$.
• Pour SA2 : $1 = 1 + 0i \in \mathbb{Z}[i]$.
• Pour SA3 : si a, b, c, d sont dans $\mathbb{Z}$, alors $(a + ib)(c + id) = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$.
• Pour SA1 : on a encore trois propriétés à vérifier :
On montre que :
(SG1) $\mathbb{Z}[i]$ contient 0
(SG2) $\mathbb{Z}[i]$ est stable par +
(SG3) $\mathbb{Z}[i]$ contient les opposés de ses éléments.
Pour SG1, $0 = 0 + 0i \in \mathbb{Z}[i]$.
Pour SG2 : si $(a, b, c, d) \in \mathbb{Z}^4$, $(a + ib) + (c + id) = (a + c) + i(d + c) \in \mathbb{Z}[i]$.
Pour SG3 : si $(a, b) \in \mathbb{Z}^2$, $-(a + ib) = (-a) + i(-b)$ avec $(-a)$ et $(-b)$ dans $\mathbb{Z}$, donc $-(a + ib) \in \mathbb{Z}[i]$. □

b) Pour ce qui est du dessin demandé, il suffit de dessiner les points à coordonnées entières dans $\mathbb{R}^2$ i.e. $\mathbb{Z}^2$ dans $\mathbb{R}^2$.



Pour la propriété demandée : *Il s'agit juste de dire que tout point à l'intérieur d'un carré de côté 1 est à distance strictement inférieure à 1 d'un des 4 sommets du carré.*
Pour le voir, on peut diviser le carré en quatre petits carrés de côtés 1/2.

Si donc $z = a + ib \in \mathbb{C}$, soit $\alpha \in \mathbb{Z}$ tel que $|a - \alpha| \leq \frac{1}{2}$ et $\beta \in \mathbb{Z}$ tel que $|b - \beta| \leq \frac{1}{2}$ (on dit que α (resp. β) est l'entier le plus proche de a (resp. b)) alors en posant $z_0 = \alpha + i\beta \in \mathbb{Z}[i]$, on a bien : $|z - z_0| \leq \sqrt{1/4 + 1/4} = 1/\sqrt{2} < 1$.

c) Soit $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$.
Soit $z = \frac{a}{b} \in \mathbb{C}$ et soit $z_0 \in \mathbb{Z}[i]$ tel que $|z - z_0| < 1$ comme donné par le b).
Alors $|\frac{a}{b} - z_0| < 1$ donc $|a - bz_0| < |b|$.
Soit $q = z_0 \in \mathbb{Z}[i]$ et $r = a - bq \in \mathbb{Z}[i]$, on a bien $|r| = |a - bz_0| < |b|$. Donc $a = bq + r$ avec $(q, r) \in \mathbb{Z}[i]^2$ et $|r| < |b|$.

d) Clairement si $z\bar{z} = 1$ alors z est inversible d'inverse $\bar{z} \in \mathbb{Z}[i]$.
Réciproquement si z est inversible, on a un $\zeta \in \mathbb{Z}[i]$ tel que $z\zeta = 1$.
Mais alors $\bar{z}\bar{\zeta} = 1$ et en multipliant ces deux égalités, on obtient (avec la notation introduite à la question suivante qui consiste à noter $N(z)$ pour $|z|^2$) : $N(z)N(\zeta) = 1$.
Mais $N(z)$ et $N(\zeta)$ sont dans $\mathbb{N}$ donc la seule possibilité est que $N(z) = N(\zeta) = 1$.
Ainsi on vient de montrer que $z \in \mathbb{Z}[i]$ est inversible dans $\mathbb{Z}[i]$ si, et seulement si, $N(z) = 1$.
Ensuite, il suffit de remarquer que $z \in \mathbb{Z}[i]$ est de module 1 si, et seulement si $z \in \{1, -1, i, -i\}$ car l'équation $a^2 + b^2 = 1$ avec a, b entiers équivaut à $[|a| = 1$ et $|b| = 0]$ ou $[|a| = 0$ et $|b| = 1]$.

2) Propriétés des irréductibles dans $\mathbb{Z}[i]$

a) Dans $\mathbb{Z}[i]$, $2 = (1+i)(1-i)$ décomposition de 2 en produit de deux éléments non inversibles de $\mathbb{Z}[i]$ (puisque qu'on a vu que les seuls inversibles sont ± 1 et $\pm i$).

Donc 2 est *réductible* dans $\mathbb{Z}[i]$.

b) (i) Par contraposée, soit z réductible et $z = z_1 z_2$ une décomposition non triviale de z : ainsi z_1 et z_2 sont des éléments de $\mathbb{Z}[i]$, non inversibles.

Alors $N(z) = N(z_1)N(z_2)$ avec $N(z_1)$ et $N(z_2)$ dans $\mathbb{N}$ différents de 1 (car les z_i non inversibles).

Alors $N(z)$ n'est pas premier dans $\mathbb{N}$.

(ii) Ici $N(1+i) = 2 \in \mathbb{P}$ donc par (i), $(1+i)$ est irréductible dans $\mathbb{Z}[i]$.

c) Contre-exemple pour le lemme d'Euclide dans $\mathbb{Z}[i\sqrt{5}]$.

• Vérifions d'abord l'affirmation sur les inversibles de $A = \mathbb{Z}[i\sqrt{5}]$.

La *même preuve* qu'au 1) d) montre qu'un élément $z = a + ib\sqrt{5}$ est inversible dans $A = \mathbb{Z}[i\sqrt{5}]$ si, et seulement si, $N(z) = |z|^2 = 1$. Or pour $z = a + ib\sqrt{5}$, $N(z) = a^2 + 5b^2$.

Et $a^2 + 5b^2 = 1$ avec $(a,b) \in \mathbb{Z}^2$ force $|a| = 1$ et $|b| = 0$. D'où la conclusion : les seuls inversibles de l'anneau $\mathbb{Z}[i\sqrt{5}]$ sont 1 et -1.

• *Montrons que* 2 *est* irréductible *dans* A :

Par le point précédent, on sait que 2 n'est pas inversible dans A.

Par l'absurde si 2 admettait une décomposition non triviale $2 = ab$ avec $(a,b) \in A^2$ non inversibles alors $N(2) = 4 = N(a)N(b)$ avec $N(a)$ et $N(b)$ différents de 1, ce qui force $N(a) = N(b) = 2$ (car $N(a)$ et $N(b)$ sont des entiers).

Or en notant $a = \alpha + i\sqrt{5}\beta$, on a $N(a) = \alpha^2 + 5\beta^2$.

Et $N(a) = 2 \Leftrightarrow \alpha^2 + 5\beta^2 = 2 \Rightarrow \beta = 0$ et $\alpha^2 = 2$ ce qui est impossible avec $\alpha \in \mathbb{Z}$.

Donc 2 est bien irréductible.

• *Montrons que* 2 *ne divise ni* $(1+i\sqrt{5})$ *ni* $(1-i\sqrt{5})$ *dans* A.

En effet, si on avait $1 + i\sqrt{5} = 2a$ avec $a \in A$, on aurait $N(1+i\sqrt{5}) = N(2)N(a)$ donc $N(2) = 4$ diviserait $N(1+i\sqrt{5}) = 6$ ce qui est une *contradiction*. De même avec $1 - i\sqrt{5}$. □

d) Sens $\Rightarrow$: si on suppose a et b premier entre eux, on applique *l'algorithme d'Euclide* à a et b avec la division euclidienne de $\mathbb{Z}[i]$, et en remontant, on fabrique u et v coefficients de Bézout.

La réciproque est évidente : si on a une relation de la forme $au + bv = 1$ et si d divise a et b il divise $au + bv$ donc 1 donc d est inversible. □

e) La même preuve que dans $\mathbb{Z}$. En effet si a et p ne sont pas premier entre eux, il existe $d \in A$ non inversible diviseur commun à p et a. Or $p = kd$ avec d non inversible force k inversible (décomp. triviale) et donc $d = k^{-1}p$ avec $k^{-1} \in A$ et donc p divise a. □

f) On suppose que p divise ab dans A.

Par l'absurde si p ne divise ni a ni b alors p est premier avec a et avec b par le lemme 2.

Par le lemme 1, on a donc deux identités de Bézout : $pu_1 + av_1 = 1$ et $pu_2 + bv_2 = 1$ avec $(u_1, u_2, v_1, v_2) \in A^4$.

En les multipliant (idem cours), on obtient $pU + abV = 1$ où $V = v_1 v_2$ et $U = ...$

Donc par la récip. du lemme 1, on conclut que ab et p sont premiers entre eux, *contradiction*. □

Remarque – On peut aussi prouver dans $\mathbb{Z}[i]$, à partir du lemme d'Euclide, un théorème d'existence et d'unicité de la décomposition en éléments irréductibles. Pour l'unicité, il faut faire attention aux inversibles. Comment énoncer alors l'unicité de la décomposition en irréductibles ?

Notons $A = \mathbb{Z}[i]$ et $\mathcal{I}$ l'ensemble des irréductibles de A.

Existence de la décomposition en irréductibles : pour tout $z \in A \setminus \{0\}$ il existe $p_1, \dots, p_r$ dans $\mathcal{I}$ distincts et u inversible tels que : $z = up_1^{\alpha_1} \dots p_r^{\alpha_r}$.

(M1) pour énoncer l'unicité : *à permutation près et à inversibles près* si on a deux écritures $z = up_1^{\alpha_1} \dots p_r^{\alpha_r} = vq_1^{\beta_1} \dots q_s^{\beta_s}$ avec u, v inversibles, $p_1, \dots p_r$, distincts et $q_1, \dots, q_s$ distincts et tous dans $\mathcal{I}$, alors $r = s$ et il existe une permutation σ i.e. une bijection $\sigma : [\![1,r]\!] \to [\![1,r]\!]$ telle que pour tout $i \in [\![1,r]\!]$ $p_i = u_i q_{\sigma(i)}$ avec u_i inversible et alors aussi $\alpha_i = \beta_{\sigma(i)}$.

(M2) pour énoncer l'unicité *avec un système de représentants*

Il est commode d'introduire une terminologie : deux éléments z et z' de A sont *associés* ssi il existe un u inversible tel que $z' = u.z$. Cette relation est une relation d'équivalence.

Notons $\mathcal{P}$ un système complet de représentants des irréductibles pour cette relation d'équivalence i.e. un sous-ensemble $\mathcal{P}$ de l'ensemble $\mathcal{I}$ des irréductibles tel que pour tout $q \in \mathcal{I}$ il existe un unique $p \in \mathcal{P}$ tel que q soit associé à p.

Avec ce choix d'un système complet de représentants des irréductibles le théorème de décomposition en irréductibles s'écrit :

$$\forall\, z \in A^*,\ z = u \prod_{p \in \mathcal{P}} p^{v_p(z)},\ \text{avec } u \text{ inversible.}$$

3) Application de l'arithmétique dans $\mathbb{Z}[i]$ à l'équation de Pythagore $x^2 + y^2 = z^2$

Remarque : l'énoncé ne disait pas qu'il était impossible que x et y soient simultanément impairs, ce qui est facile à montrer en réduisant l'équation modulo 4 (cf. l'autre DM).

Chacune des trois étapes du a), b), c) vient d'idées très naturelles dans $\mathbb{Z}$, mais ici, il faut être un peu plus soigneux pour suivre ces idées dans $\mathbb{Z}[i]$.
Au a) parce que 2 n'est pas irréd. Au b) parce qu'il y a plus d'inversibles...

a) Soit $(x, y) \in \mathbb{Z}^2$ premiers entre eux dans $\mathbb{Z}$.

Remarquons que l'identité de Bézout $ax + by = 1$ avec $(a, b) \in \mathbb{Z}^2$ dit que x et y sont premiers entre eux aussi dans $\mathbb{Z}[i]$.

Soit $d \in \mathbb{Z}[i]$ tel que $d|(x + iy)$ et $d|(x - iy)$.

Alors $d|(x + iy) + (x - iy)$ donc $d|2x$.

De même $d|(x + iy) - (x - iy)$ donc $d|2iy$. Comme i est inversible dans $\mathbb{Z}[i]$ ceci équivaut à $d|2y$.

Donc $d|(2x) \wedge (2y)$ autrement dit $d|2$ puisque $x \wedge y = 1$ dans $\mathbb{Z}[i]$.

Attention, on a vu plus haut que 2 n'est pas irréductible dans $\mathbb{Z}[i]$ puisque $2 = (1 + i)(1 - i)$.

Mais $(1 + i)$ et $(1 - i)$ sont, eux, irréductibles car $N(1 + i) = N(1 - i) = 2 \in \mathbb{P}$ (cf. question 2) b)).

Par l'absurde si $(x + iy)$ et $(x - iy)$ ne sont pas premiers entre eux dans $\mathbb{Z}[i]$ alors ils ont un diviseur commun irréductible d et $d|(1 + i)(1 - i)$ (produit) entraine $d|(1 + i)$ ou $d|(1 - i)$.

En fait ici comme $-i(1 + i) = (1 - i)$ et que $-i$ est inversible, les deux prop. $d|(1 + i)$ et $d|(1 - i)$ sont équivalentes.

Comme $(1 + i)$ est aussi irréductible, on conclut que $d = u(1 + i)$ avec u inversible.

Mais alors $|d|^2$ divise $|1 + i|^2 = 2$ dans $\mathbb{Z}$ ce qui force $|d| < 2$ et donc $|d| = 1$ donc d est inversible, *contradiction.*

Donc $x + iy$ et $x - iy$ sont premiers entre eux dans $\mathbb{Z}[i]$.

b) Notons $\mathcal{I}$ l'ensemble des irréductibles dans $\mathbb{Z}[i]$ (ou mieux $\mathcal{P}$ un système complet d'irréd. comme à la fin du 2).

On utilise la même caractérisation des carrés que dans $\mathbb{Z}$ la D.F.P. (ici décomposition en irréd) à une subtilité près, qui est la multiplication par les inversibles $u \in \{1, -1, i, -i\}$

Un élément $z \in \mathbb{Z}[i]$ s'écrit $u.w^2$ avec u inversible et $w \in \mathbb{Z}[i]$ ssi pour tout irréductible $\pi \in \mathcal{I}$, $v_\pi(z)$ est paire.

Avec l'équation $(x+iy).(x-iy) = z^2$, on sait donc que pour tout $\pi \in \mathcal{I}$, $v_\pi(x+iy)+v_\pi(x-iy) \in 2\mathbb{Z}$.

Or $(x - iy)$ et $(x + iy)$ sont premiers entre eux, autrement dit, pour tout $\pi \in \mathcal{I}$, $v_\pi(x + iy) = 0$ ou $v_\pi(x - iy) = 0$, on en déduit que :

$$\forall\, \pi \in \mathcal{I},\ v_\pi(x + iy) \text{ et } v_\pi(x - iy) \text{ sont pairs.}$$

Attention, cela veut dire que $x + iy = uw^2$ où u est inversible ce qui laisse quatre possibilités pour u. Mais comme $-1 = i^2$ et que $-i = (i^2)i$, on peut en déduire (quitte à poser $z_1 = iw$) qu'on a seulement deux possibilité :

$$x + iy = z_1^2 \ \text{ ou } \ x + iy = iz_1^2, \text{ avec } z_1 \in \mathbb{Z}[i].$$

c) Si on avait $x + iy = iz_1^2 = i(a + ib)^2 = i(a^2 - b^2 + 2iab) = -2ab + i(a^2 - b^2)$, on aurait $x = -2ab$ donc x serait pair, ce qui est contraire à notre hypothèse de départ. D'où la conclusion $x + iy = z_1^2$.

d) Conclusion : on vient de montrer que si (x, y) sont premiers entre eux, avec x impair, et y pair, tels qu'il existe un $z \in \mathbb{Z}$ tel que $x^2+y^2 = z^2$ alors il existe $(a, b) \in \mathbb{Z}^2$ tels que $(x+iy) = (a+ib)^2$. donc en identifiant parties réelles et imaginaires : $\begin{cases} x = a^2 - b^2, \\ y = 2ab. \end{cases}$. Alors, si $z \geq 0$, $z = a^2 + b^2$.

Réciproquement tous les triplets $(a^2-b^2, 2ab, a^2+b^2)$ pour $(a,b) \in \mathbb{Z}^2$, sont bien sol. de l'équation de Pythagore. L'ensemble de toutes les solutions s'obtient en multipliant ces triplets par un $k \in \mathbb{Z}$ quelconque (cf. l'autre DM).