Aix-Marseille Université
Préparation à l'agrégation: Option C
`http://iml.univ-mrs.fr/~kohel/tch/Agreg/`

Nombres triangulaires carrés

On étudie les coïncidences des nombres triangulaires et les nombres carrés. Ce problème nous amene à étudier les solutions en entiers d'une équation polynomiale, une équation diophantienne.

Nombres triangulaires

Les nombres triangulaires sont les nombres de la forme

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Le nom "triangulaire" vient de la répresentation de la somme $1+2+\cdots+n$ par un nombre de points empilés en forme d'un triangle équilateral,

$n = 1$: $n = 2$: $n = 3$:

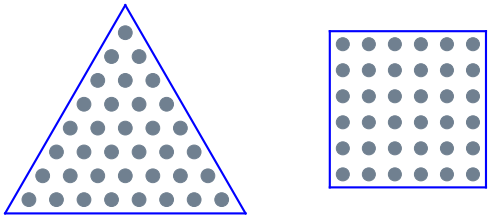
Nombres triangulaires carrés

Pour certaines valeurs de n on peut écrire le nombre triangulaire $n(n+1)/2$ aussi en forme d'un carré ($= m^2$). D'abord pour $n = m = 1$:

$n = 1$: $m = 1$:

en ensuite pour $n = 8$ on trouve $m = 6$.

$n = 8$: $m = 6$:



La prochaine valeur est $n = 49$, pour laquelle $m = 5 \cdot 7 = 35$. On pose la question si ces examples sont finis ou infinis en nombre et s'il existe une construction pour les énumérer.

Équations diophantiennes

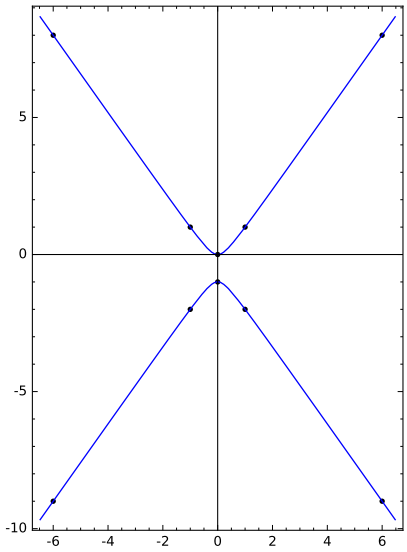
Un nombre triangulaire carré est en bijection avec les tuples (m, n) d'entiers tel que

$$m^2 = \frac{n(n+1)}{2}.$$

On est amené à étudier les points entiers sur la conique affine

$$C : 2x^2 = y^2 + y$$

dans $\mathbb{A}^2/\mathbb{Q}$. On a déjà identifié les points $(1, 1)$ et $(6, 8)$, et par les symétries de la courbe, ces deux points donnent lieu à 8 points (en plus des points triviaux $(0, 0)$ et $(0, -1)$) :



On va d'abord étudier les points rationnels $C(\mathbb{Q})$ de cette courbe. Ensuite on va identifier le sous-ensemble de points entiers

$$C(\mathbb{Z}) = \{(m, n) \in \mathbb{A}^2(\mathbb{Z}) \ : \ 2m^2 = n^2 + n\}.$$

Une équation dont on étudie les solutions en entiers s'appelle une *équation diophantienne*.

Paramétrisation de la conique

Pour décrire une paramétrisation de la conique on construit d'abord sa clôture projective, en plongeant $\mathbb{A}^2$ dans le plan projectif $\mathbb{P}^2$. En mettant $(x, y) = (X/Z, Y/Z)$, on obtient la courbe :

$$\tilde{C} : 2X^2 = Y^2 + YZ.$$

dans laquelle la courbe affine C s'identifie avec les points $(x : y : 1)$ de la courbe.

Remarque. On constate que $\tilde{C} \cap V(Z)$ est l'ensemble $\{(1 : \pm\sqrt{2} : 0)\}$ de deux points à l'infini, qui ne sont pas dans $\tilde{C}(\mathbb{Q})$. Par consequent, on peut identifier $\tilde{C}(\mathbb{Q}) = C(\mathbb{Q})$.

En fixant le point $(x, y) = (0, 0) \in C(\mathbb{Q})$, qui correspond à $(0 : 0 : 1)$ de $\tilde{C}(\mathbb{Q})$, on peut projecter de $(0, 0)$ à la droite $V(Z) \cong \mathbb{P}^1$ à l'infini (par rapport à $\mathbb{A}^2$). On rappel que l'isomorphisme $V(Z) \cong \mathbb{P}^1$est défini par l'identification de $\mathbb{P}^1$ avec les droites de $\mathbb{A}^2$ passant par $(0, 0)$, et de l'autre, par le point d'intersection ce cette droite avec $V(Z)$.

Précisement, pour chaque point (x, y) de C cette projection est donnée simplement par l'image $(x : y : 0) \in V(Z)$. On obtient donc $\pi : C \to \mathbb{P}^1$ donnée par $\pi((x, y)) = (x : y)$. En coordonnées projectives, on peut la décrire de la forme

$$(X : Y : Z) \longmapsto (X : Y)$$

sur la clôture projective $\tilde{C}$.

Remarque. L'extension de la projection π à $\tilde{C}$ est bien-définie sauf au point $(0 : 0 : 1)$, mais elle s'accorde avec l'application $(X : Y : Z) \longmapsto (Y + Z : 2X)$, qui permet de définir l'image de $(0 : 0 : 1)$. On peut vérifier que l'image s'accorde avec la droite tangente de C en $(0, 0)$.

Notation. Pour différencier les fonctions coordonnés (X, Y, Z) sur $\tilde{C} \subset \mathbb{P}^2$ et celles sur $\mathbb{P}^1$, on note ces dernières fonctions (U, V).

Proposition. *Soit $\mathbb{P}^1$ la droite projective, équippée des fonctions coordonnées U, V. Le morphisme $\varphi : \mathbb{P}^1 \to \tilde{C}$, donnée par*

$$(U : V) \longmapsto (UV : V^2 : 2U^2 - V^2),$$

est un isomorphisme, inverse à la projection du point $(0 : 0 : 1)$.

Définition. On appelle un isomorphisme $\varphi : \mathbb{P}^1 \to \tilde{C}$ une paramétrization de la courbe $\tilde{C}$.

Démonstration. Il suffit de noter que l'image dans $\mathbb{P}^2$ de l'application est bien $\tilde{C}$ et que l'inverse est la projection $(X : Y : Z) \mapsto (X : Y)$. □

Remarque. On peut dériver l'expression pour φ en utilisant l'équation $2x^2 = y^2 + y$ pour C et la relation :

$$(x : y) = (U : V).$$

En effet, cette deuxième rélation est équivalent à $yU = xV$. Soit on fait la substitution $x/y = U/V$ dans :

$$2\left(\frac{x}{y}\right)^2 = 1 + \frac{1}{y},$$

pour déterminer y comme fonction de U et V, soit on calcule le résultant des deux polynômes

$$2x^2 - y^2 - y,\ yU - xV,$$

pour éliminer le variable y (ou x), afin de déterminer une expression pour x (ou y) en termes de U et V.

On obtient un isomorphisme sur le complément de la variété $S = V(2U^2 - V^2)$:

$$\begin{aligned} \mathbb{P}^1 \backslash S &\longrightarrow C. \\ (U : V) &\longmapsto \left(\frac{UV}{2U^2 - V^2}, \frac{V^2}{2U^2 - V^2} \right) \end{aligned}$$

Mais comme $S(\mathbb{Q}) = \emptyset$, on obtient une bijection de points $\mathbb{P}^1(\mathbb{Q})$ avec $C(\mathbb{Q})$.

L'équation diophantienne

On peut maintenant étudier l'équation diophantienne

$$2m^2 = n^2 + n.$$

On a démontree que les solutions à $x^2 = y^2 + y$ en valeurs rationnelles, les points de $C(\mathbb{Q})$, sont de la forme

$$x = \frac{UV}{2U^2 - V^2}, \text{ et } \quad y = \frac{V^2}{2U^2 - V^2}. \tag{1}$$

Pour tout point $(U : V) \in \mathbb{P}^1(\mathbb{Q})$ on peut supposer que U et V sont des entiers premiers entre eux. Par conséquent, on peut conclure que

$$\text{pgcd}(2U^2 - V^2, V^2) = \text{pgcd}(2U^2, V^2) = \text{pgcd}(2, V) \in \{1, 2\}.$$

Si on a $V \equiv 0 \bmod 2$, on peut écrire $V = 2W$, et on a

$$x = \frac{UW}{U^2 - 2W^2}, \text{ et } y = \frac{2W^2}{U^2 - 2W^2}, \tag{2}$$

avec $\text{pgcd}(2W^2, U^2 - 2W^2) = 1$. La forme d'une solution paramétrisée est donc (1) ou (2), avec y en forme réduite (numérateur et dénominateur premier entre eux). Pour avoir $(x, y) = (m, n) \in \mathbb{Z}^2$, on réduit à la condition

$$2U^2 - V^2 = \pm 1 \text{ ou } U^2 - 2W^2 = \pm 1,$$

dans le cas (1) ou (2), respectivement.

Une équation de norme

L'équation diophantienne de la forme

$$a^2 - 2b^2 = 1 \text{ ou } a^2 - 2b^2 = -1,$$

s'appelle une équation de Pell. Elle est un exemple d'une *équation de norme* pour l'anneau d'entiers $\mathbb{Z}[\sqrt{2}\,]$. On rappelle que la norme sur $\mathbb{Z}[\sqrt{2}\,]$ est l'application

$$\begin{aligned} N : \mathbb{Z}[\sqrt{2}\,] &\longrightarrow \mathbb{Z}. \\ a + b\sqrt{2} &\longmapsto a^2 - 2b^2 \end{aligned}$$

On remarque que N est la fonction produit des conjugés :

$$N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}),$$

et que N est une fonction multiplicative : $N(\alpha\beta) = N(\alpha)N(\beta)$. De plus, un élément $\alpha \in \mathbb{Z}[\sqrt{2}\,]$ est inversible si et seulement si $N(\alpha) \in \{\pm 1\}$. On énonce un résultat permmettant de déterminer toutes les solutions à notre équation de Pell.

Proposition. *Soit N la fonction norme de $\mathbb{Z}[\sqrt{2}\,]$. On a*

$$N((1+\sqrt{2})^k) = (-1)^k,$$

et toute solution de $N(a+b\sqrt{2}) = \pm 1$ est donnée par un élément

$$a+b\sqrt{2} \in \{\pm(1+\sqrt{2})^k \ : \ k \in \mathbb{Z}\}.$$

Cette proposition peut être exprimée autrement par l'égalité

$$\mathbb{Z}[\sqrt{2}\,]^* = \{\pm 1\} \times \langle 1+\sqrt{2}\rangle,$$

en vue de l'équivalence entre $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}\,]^*$ et $N(a+b\sqrt{2}) \in \mathbb{Z}^* = \{\pm 1\}$.

Exemple. On peut énumérer les premiers puissances : $(1+\sqrt{2})^0 = 1+0\sqrt{2}$ et

$$\begin{array}{ll} (1+\sqrt{2})^1 = 1+\sqrt{2} & (1+\sqrt{2})^{-1} = -1+\sqrt{2} \\ (1+\sqrt{2})^2 = 3+2\sqrt{2} & (1+\sqrt{2})^{-2} = \ \ 3-2\sqrt{2} \\ (1+\sqrt{2})^3 = 7+5\sqrt{2} & (1+\sqrt{2})^{-3} = -7+5\sqrt{2} \\ (1+\sqrt{2})^4 = 17+12\sqrt{2} & (1+\sqrt{2})^{-4} = \ 17-12\sqrt{2} \end{array}$$

Cela donne des tuples de solutions

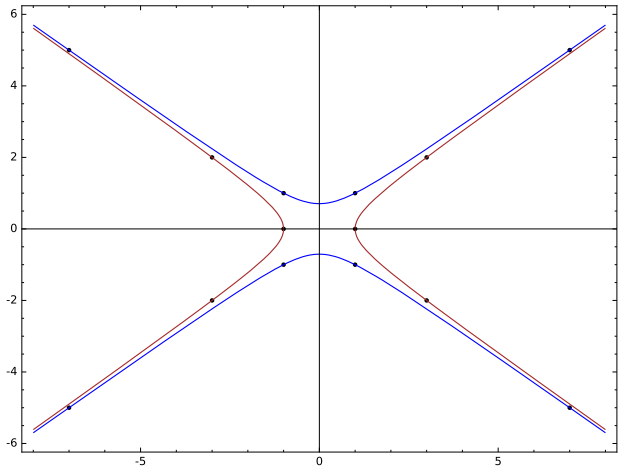
$$\{\ldots, (-1,1), (1,0), (1,1), (3,2), (7,5), (17,12), \ldots\}$$

En particulier on en déduit des points projectifs $(U:V) = (b:a)$ ou $(U:W) = (a:b)$ donnant lieu à des points entiers $(x,y) = (m,n)$ par les equations (1) ou (2).

(a,b)	$(U:V)$	(m,n)	$(U:W)$	(m,n)
$(-1,1)$	$(1:-1)$	$(-1,1)$	$(1:-1)$	$(1,-2)$
$(1,0)$	$(0:1)$	$(0,-1)$	$(1:0)$	$(0,0)$
$(1,1)$	$(1:1)$	$(1,1)$	$(1:1)$	$(-1,-2)$
$(3,2)$	$(2:3)$	$(6,-9)$	$(3:2)$	$(6,8)$
$(7,5)$	$(5:7)$	$(35,49)$	$(7:5)$	$(-35,-50)$

Remarque. On a remplacé l'étude de points entiers sur la courbe affine $C : 2x^2 = y^2 + y$ avec l'étude des points entiers sur les deux courbes affines

$$C_0 : a^2 - 2b^2 = 1 \text{ et } C_1 : a^2 - 2b^2 = -1.$$



L'application envoyant (a, b) à $(U : V) = (b : a)$ donne lieu à des morphismes

$$\begin{array}{ccc} C_0 & \xrightarrow{\tau_0} & C \\ (a,b) & \longmapsto & (-ab, -a^2) \end{array} \quad \text{et} \quad \begin{array}{ccc} C_1 & \xrightarrow{\tau_1} & C, \\ (a,b) & \longmapsto & (ab, a^2) \end{array}$$

et l'application envoyant (a, b) à $(U : W) = (a : b)$ donne lieu à des morphismes

$$\begin{array}{ccc} C_0 & \xrightarrow{\sigma_0} & C \\ (a,b) & \longmapsto & (ab, a^2 - 1) \end{array} \quad \text{et} \quad \begin{array}{ccc} C_1 & \xrightarrow{\sigma_1} & C. \\ (a,b) & \longmapsto & (-ab, -a^2 - 1) \end{array}$$

Les deux couples d'applications sont échangés par l'involution ι de C

$$(x, y) \longmapsto (-x, -y - 1),$$

dans le sens que $(\sigma_0, \sigma_1) = (\iota\tau_0, \iota\tau_1)$ et $(\tau_0, \tau_1) = (\iota\sigma_0, \iota\sigma_1)$. On note en particuler que

$$C(\mathbb{R}) = \tau_0(C_0(\mathbb{R})) \cup \tau_1(C_1(\mathbb{R}))$$

donne les deux composantes connexes de $C(\mathbb{R})$, qui sont échangées par ι et que

$$\begin{aligned} \tau_0(C_0(\mathbb{R})) &= \sigma_1(C_1(\mathbb{R})), \text{ et} \\ \tau_1(C_1(\mathbb{R})) &= \sigma_0(C_0(\mathbb{R})). \end{aligned}$$

Les morphismes τ_i et σ_i sont de degrés deux – le préimage de chaque point est un ensemble $\{(a, b), (-a, -b)\}$ de deux points de C_i.

Recurrences et transformations géométriques

On observe que les solutions (a_k, b_k) à l'équation $a_k^2 - 2b_k^2 = (-1)^k$, données par

$$a_k + b_k\sqrt{2} = \left(1 + \sqrt{2}\right)^k,$$

pour tout $k \in \mathbb{Z}$, satisfaient la recurrence

$$(a_{k+1}, b_{k+1}) = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{bmatrix} a_k \\ b_k \end{bmatrix} = (a_k + 2b_k, a_k + b_k),$$

qui correspond à la multiplication par $1 + \sqrt{2}$, et en multipliant par l'inverse $-1 + \sqrt{2}$, on obtient

$$(a_{k-1}, b_{k-1}) = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix} \begin{bmatrix} a_i \\ b_i \end{bmatrix} = (a_k - 2b_k, -a_k + b_k).$$

Remarque. En observant que la matrice A définissant la recurrence satisfait $A^2 = 2A+I$, on trouve les recurrences

$$\begin{aligned} a_{k+1} &= 2a_k + a_{k-1}, \\ b_{k+1} &= 2b_k + b_{k-1}. \end{aligned}$$

En notant que le sign de la norme $a_k^2 - 2b_k^2$ change avec la parité de l'indice k, on a des sous-suites

$$S_0 = \{\ldots, (a_{-2}, b_{-2}), (a_0, b_0), (a_2, b_2), \ldots\} \subseteq C_0(\mathbb{Q}),$$

et

$$S_1 = \{\ldots, (a_{-1}, b_{-1}), (a_1, b_1), (a_3, b_3), \ldots\} \subseteq C_1(\mathbb{Q}).$$

Plus loin, on peut dire que la transformation du plan $\mu : \mathbb{A}^2 \to \mathbb{A}^2$, donné par

$$(a, b) \longmapsto (a + 2b, a + b),$$

induit des isomorphismes $C_0 \to C_1$ et $C_1 \to C_0$, et non seulement des bijections

$$S_0 \longrightarrow S_1 \text{ et } S_1 \longrightarrow S_0.$$

Le transformation μ de l'espace $\mathbb{A}^2$ induit une transformation de la courbe C.

Proposition. *Soit $\tau_i : C_i \to C$ les morphismes ci-dessus, et μ la transformation de $\mathbb{A}^2$ induisant $C_0 \to C_1$ et $C_1 \to C_0$. Il existe un automorphisme $\xi : C \to C$ donné par*

$$(x, y) \longmapsto (-3x - 2y - 1, -4x - 3y - 2),$$

tel que

$$\begin{aligned} \xi\tau_0 = \tau_1\mu : C_0 \to C, \quad \xi\sigma_0 = \sigma_1\mu : C_0 \to C, \\ \xi\tau_1 = \tau_0\mu : C_1 \to C, \quad \xi\sigma_1 = \sigma_0\mu : C_1 \to C. \end{aligned}$$

Remarque. Par itération de l'automorphisme ξ et son inverse, on obtient un nombre infini de nombres triangulaires carrés à partir d'un seul, par exemple $(m, n) = (0, 0)$.

Suggestions et pistes de réflexion

Les pistes de réflexion suivaantes ne sont qu'indicatives et il n'est pas obligatoire de les suivre. Vous pouvez choisir d'étudier ou non, certains des points proposés, de façon plus ou moins approfondie, mais si possible, des représentations graphiques de vos résultats. À défaut si vos illustrations informatiques n'ont pas abouti, il est conseillé d'expliquer ce que vous auriez souhaité mettre en oeuvre.

— On pourra illustrer à l'aide de l'ordinateur les diverses constructions de nombres triangulaires carrées.
— On pourra compléter les preuves des énoncés et affirmations, ou développer les remarques du texte.
— On pourra modéliser les transformations et récurrences en sage, en montrant des algorithmes pour énumérer des couples (m, n) dont

$$m^2 = n(n+1)/2$$

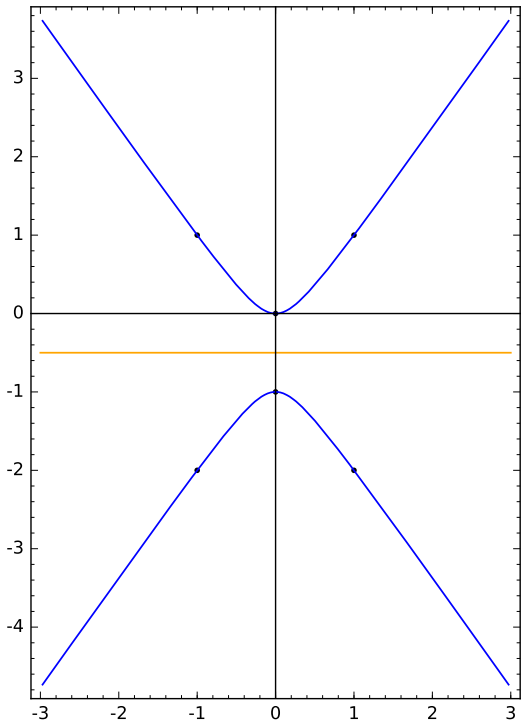
est un nombre triangulaire carré.
— On peut illustrer la géométrie des courbes C_0, C_1 et C, et les transformations, ainsi que leurs systèmes de points entiers (a, b) et (m, n).

Graphiques en Sage

On peux modéliser la courbe affine C en Sage, ainsi que le système de points passage par $(0,0)$ qui donne la projection à la droite à l'infini (ensemble de points $(x:y:0)$).

```
x,y = var("x,y")
f = 2*x^2 - y^2 - y
xmin, xmax = (-3,3)
ymin, ymax = (xmin*s-1/2, xmax*s-1/2)
pnts = [ [0,0], [0,-1], [-1,1], [1,1], [-1,-2], [1,-2] ]
C = implicit_plot(f,(x,xmin,xmax),(y,ymin,ymax),axes=True)
C += sum([ point2d(p,color=dot_color) for p in pnts ])
L = line([(xmin,-1/2),(xmax,-1/2)],color="orange")
```

On voit graphiquement les symétries de la courbe $C : y^2 + y = 2x^2$, autour de l'axe y et la droite $y = -1/2$.



On peut également tracer des droites passant par l'origine $(0,0)$, donnant les projections à la droite à l'infini. Ici on définit les droites $L : y = x$ et $M : y = -2x$ passant aussi par $(1,1)$ et $(1,-2)$.

```
L = plot(x,(x,xmin,xmax),color="red")
L_text = text("$L$",(2.25,2.0),color=dot_color,fontsize=12)
M = plot(-2*x,(x,-ymax/2,-ymin/2),color="red")
M_text = text("$M$",(1.75,-4.0),color=dot_color,fontsize=12)
```

Ensuite les droites D et E définis par $y = \pm\sqrt{2}x$ approchent asymptotiquement les deux branches, parallèle aux droites asymptotes

$$y = \pm\sqrt{2}x - 1/2.$$

```
s = RR(2).sqrt()
# La droite par (0,0) et le point (1:sqrt(2):0) à l'infini
D = plot(+s*x,(x,xmin,xmax-1/s/2),color="brown")
D_text = text("$D$",(2.0,3.2),color=dot_color,fontsize=12)
# La droite asymptote à C, parallèle à D :
Y = plot(+s*x-1/2,(x,xmin,xmax),color="aquamarine")
# La droite par (0,0) et le point (1:-sqrt(2):0) à l'infini
E = plot(-s*x,(x,xmin+1/s/2,xmax),color="brown")
E_text = text("$E$",(-2.0,3.2),color=dot_color,fontsize=12)
# La droite asymptote à C, parallèle à E :
Z = plot(-s*x-1/2,(x,xmin,xmax),color="aquamarine")
```

À gauche on voit les droites L et M. À droit on voit les droites asymptotes Y et Z, parallèle à D et E, qui a une seule intersection double avec C à l'infini.