Cours d'arithmétique

Baccalauréat ++

Mohamed ATOUANI

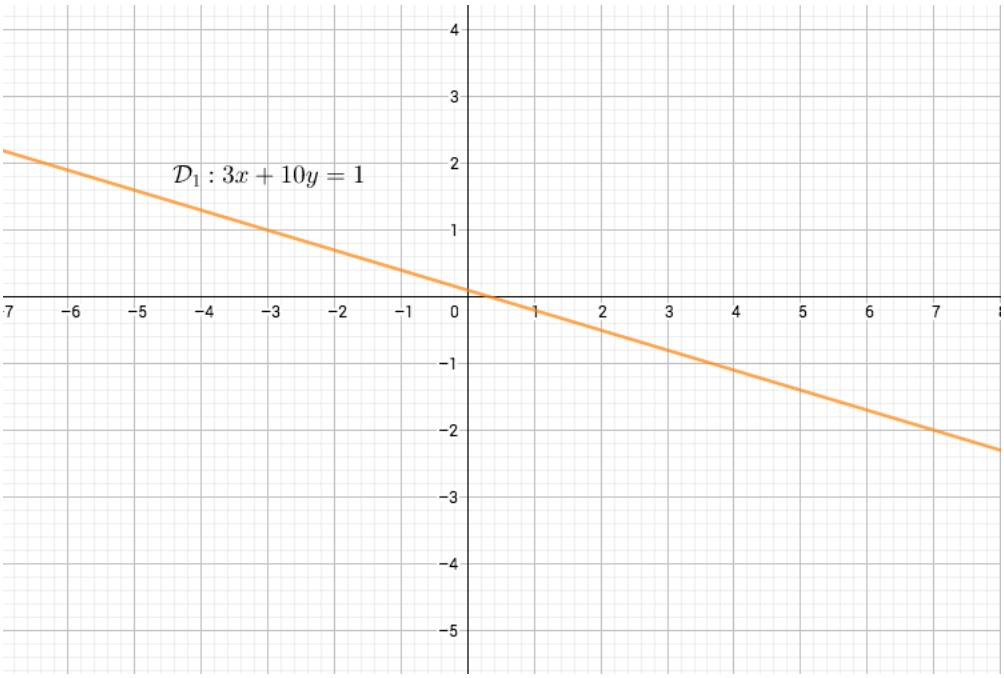
Professeur de Mathématiques
Clandestines

Table des matières

1 Arithmétique sur les droites affines

Nous nous intéressons dans cette première section aux équations diophantiennes de degré 1, à savoir celles de la forme $ax + by = c$, où a, b et c sont des éléments de $\mathbb{Z}$. Les inconnues dans cette histoire sont évidemment x et y et notre objectif est donc de trouver tous les couples d'entiers (x, y) vérifiant l'équation diophantienne. Cette question a un lien direct avec la géométrie, puisque dans le plan, l'équation $ax + by = c$ est celle d'une droite affine. La recherche de couples d'entiers solutions de $ax + by = c$ revient donc à localiser les points à coordonnées entières situés sur la droite de cette même équation. Un exemple vaut bien mieux qu'un long discours.

Exemple 1 : Soit $\mathscr{D}_1$ la droite d'équation $3x + 10y = 1$. On souhaite trouver les points à coordonnées entières situés sur $\mathscr{D}_1$.



Une petite recherche à l'œil nu montre que par exemple le point $(-3, 1)$ est un point à coordonnées entières sur notre droite. Autrement dit, le couple $(-3, 1)$ est solution de l'équation diophantienne $3x + 10y = 1$. Pour s'en convaincre, un petit calcul algébrique montre bien que

$$3 \times (-3) + 10 \times 1 = 1.$$

Super ! Notez toutefois que $(-3, 1)$ n'est pas le seul point à coordonnées entières habitant sur la droite $\mathscr{D}_1$, puisqu'elle passe aussi par le point $(7, -2)$. La question toute naturelle que l'on peut donc se poser ici est : y-a-t-il d'autres points intégrals (un autre mot pour dire à coordonnées entières) situés sur $\mathscr{D}_1$? La réponse est oui et il en existe d'ailleurs une infinité. En effet, en tâtonnant on peut voir que les points intégrals visibles sur la droite sont par exemple lié par la formule

$$x = 10k - 3 \quad \text{et} \quad y = -3k + 1,$$

où k désigne un entier. En prenant $k = 0$, on voit que cette formule donne le point $(-3, 1)$. Pour $k = 1$, on obtient bien le point $(7, -2)$ et pour $k = -1$, on obtient le couple $(-13, 4)$ et

l'on peut vérifier aisément qu'il appartient bien à notre droite car, tout simplement

$$3 \times (-13) + 10 \times 4 = -39 + 40 = 1.$$

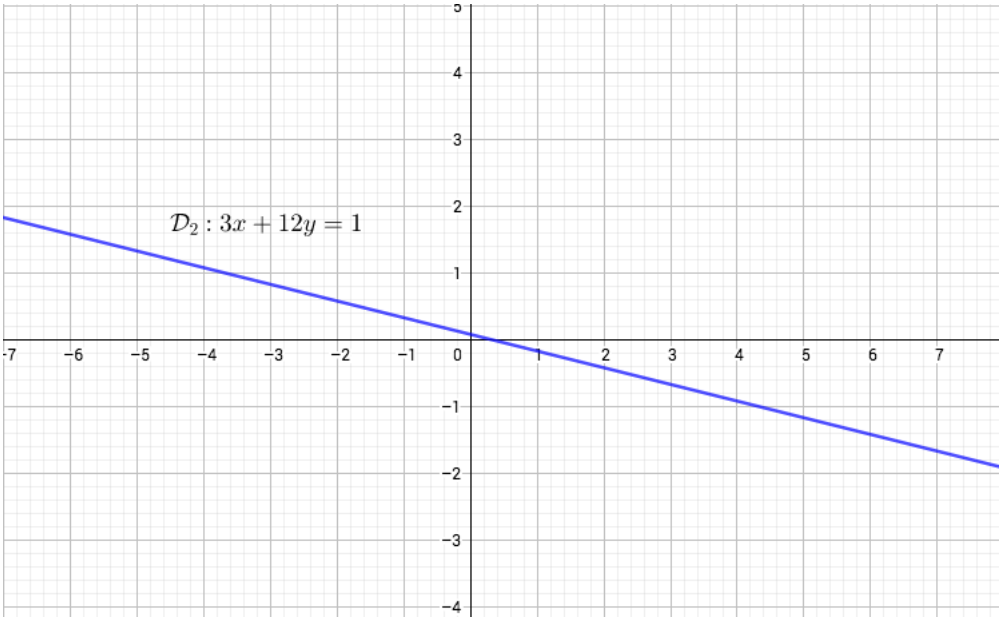
On peut bien sûr vérifier notre formule pour tout entier k, ainsi tout couple de la forme $(10k-3, -3k+1)$ est solution de l'équation diophantienne $3x + 10y = 1$ car

$$3 \times (10k-3) + 10 \times (-3k+1) = 30k - 9 - 30k + 10 = 1.$$

À partir de ce résultat, on peut affirmer qu'il existe une infinité de points à coordonnées entières appartenant à la droite $\mathscr{D}_1$, s'écrivant sous la forme $(10k-3, -3k+1)$. La question toute naturelle serait donc : obtient-on absolument tous les points intégrals habitant sur notre droite en utilisant cette formule ? Autrement dit, existe-il des points à coordonnées entières qui ne s'écrivent pas sous cette forme et qui sont quand même situés sur cette droite ? La réponse est non et l'on pourra affirmer ceci bientôt car cela nécessite quelques connaissances de plus en arithmétique.

Puisqu'on se pose beaucoup de questions ici, une petite dernière avant de terminer cette première section est la suivante : Les droites affines à coefficients entiers croisent-elles toujours des points à coordonnées entières dans le plan ? La réponse est non comme le montre l'exemple ci-dessous.

Exemple 2 : Soit $\mathscr{D}_2$ la droite d'équation $3x + 12y = 1$.



Vous pouvez passer quelques heures à chercher des points à coordonnées entières sur cette droite, vous n'en trouverez pas. L'impossibilité d'un tel fait découle d'une propriété arithmétique des coefficients de la droite $\mathscr{D}_2$. En effet, s'il exite un couple d'entiers (x, y) vérifiant $3x + 12y = 1$ alors $3(x + 4y) = 1$, ce qui signifie que 3 divise 1 (car $x + 4y \in \mathbb{Z}$). Ceci conduit bien évidemment à une contradiction, d'où le résultat.

2 Arithmétique sur le cercle unité

Nous avons aborder dans la première section l'arithmétique sur une droite affine. La droite étant la figure géométrique la plus *simple*, rien ne nous empêche d'étudier l'arith-

métique sur des figures géométriques plus élaborées. Dans cette section, nous allons nous intéresser au cercle unité d'équation $x^2+y^2=1$. Faire de l'arithmétique sur ce cercle signifie qu'on va chercher les points à coordonnées entières sur celui-ci mais pas seulement, nous allons localiser tous les points à coordonnées rationnelles vivant dessus. Un point rationnel est comme son nom l'indique un point dont les coordonnées sont des fractions. Cette recherche conduira à des résultats bien spectaculaires permettant de résoudre le problème le plus ancien des mathématiques, à savoir celui des *triplets pythagoriciens*.

Ainsi, nous souhaitons trouver tous les triplets d'entiers (x,y,z) tels que

$$x^2+y^2=z^2.$$

Cette fameuse équation est bien évidemment en lien avec le fameux théorème de *Pythagore*, auquel cas, sa résolution sur $\mathbb{N}$ signifie qu'on a trouvé un triangle rectangle dont les trois côtés sont des entiers. Notez tout d'abord qu'on peut prendre x et y des entiers arbitraires pour former un triangle rectangle, mais que rien ne garantit que l'hypoténuse z sera entier. Par exemple si $x=3$ et $y=5$, l'équation de Pythagore donne

$$z^2=x^2+y^2=3^2+5^2=34.$$

L'entier 34 n'est pas un carré parfait donc z ne peut pas être un entier. On voit ainsi que la résolution de cette équation avec x,y et z des entiers n'est pas tâche triviale. Le triplet pythagoricien le plus connu du grand public est $(3,4,5)$ car on a $3^2+4^2=5^2$ (vérifier l'égalité seul). Existe-t-il alors d'autres triangles rectangles dont les côtés sont des entiers ? La réponse est oui et là encore il en existe une infinité. En effet, on peut en déduire une infinité à partir du triplet $(3,4,5)$ en agrandissant chacun des côtés par le même facteur k. Pour $k=2$ on obtient le triplet $(6,8,10)$ et on a bien $6^2+8^2=10^2$ car en factorisant par 2^2 cette égalité devient

$$2^2\times 3^2+2^2\times 4^2=2^2\times 5^2,$$

qui est équivalente donc à l'égalité $3^2+4^2=5^2$. Plus généralement, le triplet $(3k,4k,5k)$ est un triplet pythagoricien et ceci est une simple vérification car

$$(3k)^2+(4k)^2=k^2\times(3^2+4^2)=k^2\times 5^2=(5k)^2.$$

On peut alors se demander si tous les triplets pythagoriciens s'obtiennent de cette manière, la réponse est non. En effet, par exemple le triplet $(11,60,61)$ vérifie l'équation de Pythagore et on peut s'en rendre compte sans trop de calculs avec les équivalences suivantes

$$\begin{aligned}
11^2+60^2=61^2 &\iff 11^2=61^2-60^2\\
&\iff 11^2=(61-60)(61+60)\\
&\iff 11^2=1\times 121\\
&\iff 11^2=121.
\end{aligned}$$

La dernière égalité étant une trivialité, le résultat en découle. On voit aisément alors que $(11,60,61)$ n'est pas dérivé du triplet $(3,4,5)$ car par exemple 61 n'est pas multiple de 5. Les triplets que l'on ne peut pas obtenir à partir d'autres triplets s'appellent *triplets primitifs*, combien a-t-on donc de triplets primitifs dans la nature et comment peut-on tous les localiser ? Euclide a répondu à cette question en développant au passage la théorie de la divisibilité qu'on verra ensemble dans ce cours. Toutefois, nous allons présenter ici une méthode géométrique, d'une grande ingéniosité, due à son excellence Diophante d'Alexandrie.

Ainsi, pour résoudre l'équation $x^2+y^2=z^2$, notre ancêtre distingue deux cas :

1er cas : Si $z=0$ alors $x^2+y^2=0$ ce qui implique que $0\leq x^2\leq x^2+y^2=0$ donc que $x^2=0$ ou encore que $x=0$. Par conséquent $y=0$ et dans ce cas ($z=0$) on obtient le triplet trivial $(0,0,0)$.

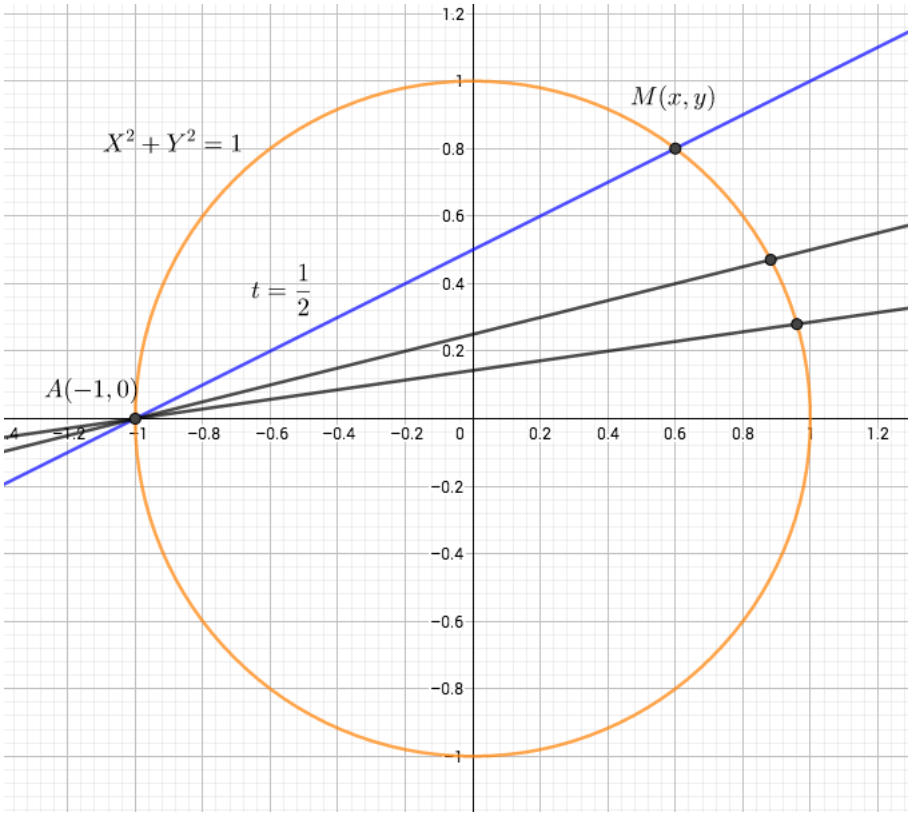
2ème cas : Si $z\neq 0$ alors

$$\begin{aligned} x^2+y^2=z^2 &\iff z^2\left(\frac{x^2}{z^2}+\frac{y^2}{z^2}\right)=z^2 \\ &\iff \left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1. \end{aligned}$$

On voit donc que (x,y,z) est un triplet pythagoricien si et seulement si le point $M(x/z,y/z)$ est un point à coordonnées rationnelles appartenant au cercle unité d'équation $X^2+Y^2=1$. Réciproquement et c'est facile à vérifier, tout point à coordonnées rationnelles situé sur le cercle unité représente un triplet pythagoricien. Diophante dit alors que la recherche de triplets pythagoriciens revient à la recherche de points à coordonnées rationnelles habitant le cercle unité. Notre problème arithmétique se transforme ainsi en un problème géométrique. Néanmoins, on a l'impression qu'on n'a fait que déplacer le problème, car il n'est pas évident de trouver les points rationnels sur notre emblématique figure géométrique. En effet, on peut prendre X un nombre rationnel mais rien ne garantit que Y le sera. Par exemple si $X=1/2$ alors l'équation $X^2+Y^2=1$ implique que

$$Y^2=1-X^2=1-\left(\frac{1}{2}\right)^2=\frac{3}{4},$$

d'où $Y=\pm\sqrt{3}/2$ qui n'est pas rationnel.



Diophante remarque l'existence de points rationnels triviaux sur le cercle unité dont le point $A(-1,0)$, comme le montre la figure ci-dessus. Il dit alors que la droite passant par A et de cœfficient directeur un nombre rationnel t doit croiser le cercle en un deuxième point de coordonnées rationnelles. Il suffit alors de résoudre un couple d'équations afin de localiser ce fameux deuxième point. Diophante prétend qu'on peut obtenir tous les points rationnels de cette manière en faisant varier le rationnel t. Essayons ce procédé avec un exemple concret.

Exemple : Soit $t = 1/2$. La droite $D_{1/2}$ passant par $A(-1,0)$ et de pente égale à t est d'équation $y = t(x+1) = 1/2(x+1)$ (pourquoi ?). Le point $M(x,y)$, le deuxième point d'intersection de $D_{1/2}$ et du cercle unité, vérifie donc le système d'équation

$$\begin{cases} y = \frac{1}{2}(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

En substituant la première équation dans la deuxième on obtient l'équation du second degré en x

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

Pas besoin d'appliquer un *delta* ici, il suffit de remarquer que l'équation se factorise trivialement de la façon suivante

$$\begin{aligned} x^2 + \left(\frac{1}{2}(x+1)\right)^2 = 1 &\iff x^2 - 1 + \frac{1}{4}(x+1)^2 = 0 \\ &\iff (x-1)(x+1) + \frac{1}{4}(x+1)^2 = 0 \\ &\iff (x+1)\left(x - 1 + \frac{1}{4}(x+1)\right) = 0 \\ &\iff (x+1)\left(\frac{5}{4}x - \frac{3}{4}\right) = 0 \\ &\iff x = -1 \quad \text{ou} \quad x = \frac{3}{5}. \end{aligned}$$

La solution $x = -1$ est tout à fait normale car je vous rappelle qu'on est à la recherche des points d'intersection de la droite $D_{1/2}$ et du cercle unité. Le premier point est A qui est d'abscisse $x = -1$, le deuxième point est donc d'abscisse égale à $x = 3/5$. Son ordonnée est donnée par la formule

$$y = \frac{1}{2}(x+1) = \frac{1}{2}\left(\frac{3}{5} + 1\right) = \frac{4}{5}.$$

Le point M est donc de coordonnées $(3/5, 4/5)$, qui est un point à coordonnées rationnelles appartenant au cercle unité. Cela implique en particulier que ses coordonnées vérifient l'équation du cercle, à savoir

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1,$$

en multipliant de part et d'autre par 5^2 on obtient $3^2 + 4^2 = 5^2$. Bingo ! ! ! On a pu localiser un premier triplet pythagoricien. La méthode suggère que si on fait varier la pente t, on obtiendra davantage de triplets pythagoriciens. Ainsi, nous allons faire le même procédé

mais cette fois avec un t quelconque.

Soit donc $t \in \mathbb{Q}$. La droite D_t de pente t et passant par $A(-1,0)$ a pour équation $y = t(x+1)$. Les coordonnées du deuxième point d'intersection de D_t et du cercle unité vérifient le système d'équations

$$\begin{cases} y = t(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

La substitution de la première équation dans la deuxième donne

$$\begin{aligned} x^2 + \big(t(x+1)\big)^2 = 1 &\iff x^2 - 1 + t^2(x+1)^2 = 0 \\ &\iff (x-1)(x+1) + t^2(x+1)^2 = 0 \\ &\iff (x+1)\big(x - 1 + t^2(x+1)\big) = 0 \\ &\iff x = -1 \quad \text{ou} \quad x = \frac{1-t^2}{1+t^2}. \end{aligned}$$

De même, l'ordonnée du deuxième point d'intersection est donnée par la formule

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

Le point M est donc de coordonnées $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, son appartenance au cercle unité implique que

$$\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1.$$

Or t est un nombre rationnel, donc s'écrit sous la forme $t = u/v$ où u et v sont deux entiers. En substituant on obtient

$$\left(\frac{1-(u/v)^2}{1+(u/v)^2}\right)^2 + \left(\frac{2(u/v)}{1+(u/v)^2}\right)^2 = 1$$

Pas peur d'effectuer des simplifications, on multiplie chacune des fractions en haut et en bas par v^2 pour obtenir la relation

$$\left(\frac{v^2-u^2}{v^2+u^2}\right)^2 + \left(\frac{2uv}{v^2+u^2}\right)^2 = 1.$$

En multipliant maintenant de part et d'autre par $(v^2+u^2)^2$ on obtient la fameuse formule donnant tous les triplets pythagoriciens, à savoir

$$\boxed{(v^2-u^2)^2 + (2uv)^2 = (u^2+v^2)^2.}$$

Convaincu ? Non ! ! Prenons $u = 5$ et $v = 6$. La formule donne l'égalité $(6^2-5^2)^2 + (2\times 5\times 6)^2 = (6^2+5^2)^2$, ou encore

$$11^2 + 60^2 = 61^2 !!!$$

On retombe ici sur le triplet $(11, 60, 61)$. Incroyable !

Remarques :

1. On peut démontrer facilement l'exactitude de la formule générant tous les triplets pythagoriciens et ce en développant tout simplement les deux expressions à droite et à gauche de l'égalité. Toutefois, ce qui est difficile, c'est d'imaginer une telle formule. L'idée géniale de Diophante a permis de l'établir, sans trop d'efforts.

2. Pourquoi cette formule donne-t-elle tous les triplets pythagoriciens ? La justification est relativement simple : toute droite D_t de pente rationnelle donne un point rationnel sur le cercle représentant un triplet pythagoricien. Réciproquement, si $M(x,y)$ est un point rationnel sur le cercle unité (différent de A bien sûr) alors la droite passant par M et par notre fameux point A est forcément de pente rationnelle (pourquoi ?).

3. Après calcul, on voit que le deuxième point d'intersection de D_t et du cercle unité est un point à coordonnées rationnelles. Cette observation est la clef de notre petite théorie, sans quoi tout tombe à l'eau. Y-a-t-il une raison plus théorique à ce fait ? En effet, le système d'équations à résoudre conduit à une équation du second degré en x sous la forme $x^2+px+q=0$, où $p,q\in\mathbb{Q}$. Notant alors que si x_1,x_2 sont deux solutions à celle-ci alors

$$x^2+px+q=(x-x_1)(x-x_2)=x^2-(x_1+x_2)x+x_1x_2.$$

   Par identification, on obtient par exemple que $-p=x_1+x_2$. Cela implique en particulier que si $x_1\in\mathbb{Q}$ alors $x_2=-p-x_1\in\mathbb{Q}$. Le résultat tombe donc comme la pomme de Newton.

3 Arithmétique sur l'hyperbole et approximations rationnelles

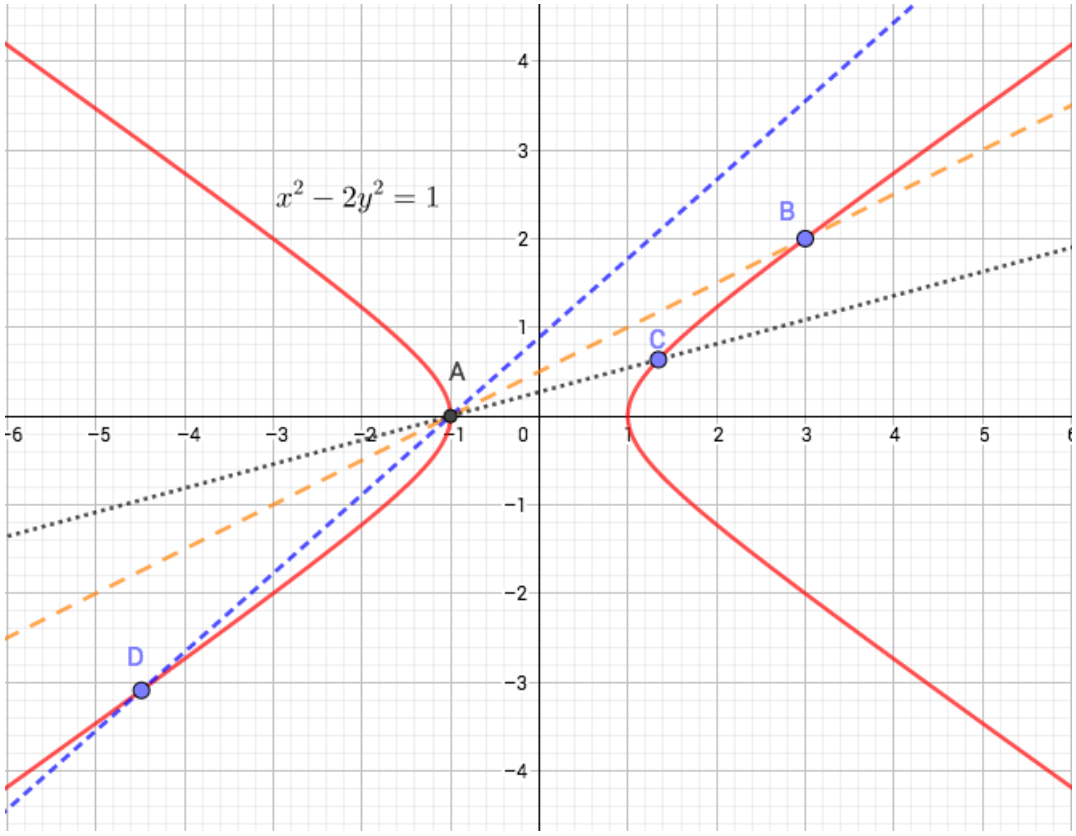
Nous avons abordé dans les deux premières sections l'arithmétique sur les droites affines et l'arithmétique sur le cercle unité, nous aborderons dans cette partie l'arithmétique sur l'hyperbole d'équation $x^2-2y^2=1$. Nous verrons que l'étude des points à coordonnées entières sur cet objet géométrique permet de mieux approcher le fameux irrationnel $\sqrt{2}$.

L'équation diophantienne $x^2-2y^2=1$ est un cas particulier des équations dites de Pell $x^2-ny^2=1$, où n n'est pas un carré parfait. Le cas des carrés parfaits est relativement trivial. En effet, si $n=m^2$, l'équation de notre regretté Pell (en réalité Pell n'est pas le mathématicien à l'origine de l'étude de ce type d'équation, mais ceci est une autre histoire) devient

$$\begin{aligned} x^2-ny^2=1 &\iff x^2-m^2y^2=1\\ &\iff (x-my)(x+my)=1. \end{aligned}$$

Cela signifie en particulier que $x-my=1$ et $x+my=1$ ou $x-my=-1$ et $x+my=-1$, car il s'agit de diviseurs de 1. Dans le premier cas seul le couple $(1,0)$ est solution et dans le deuxième cas il s'agit de $(-1,0)$ (pourquoi ?). D'où notre affirmation. La question devient nettement plus difficile quand n n'est pas un carré parfait.

Nous commençons par inspecter les points rationnels situés sur l'hyperbole, en utilisant la méthode de la corde de Diophante. En effet, sur la figure ci-dessous, on voit que le point A de coordonnées $(-1,0)$ est un point trivial à coordonnées rationnelles vérifiant l'équation $x^2-2y^2=1$.



Soit $t \in \mathbb{Q}$. La droite D_t de pente t et passant par A a pour équation $y = t(x+1)$. Les coordonnées du deuxième point d'intersection de D_t avec l'hyperbole vérifient le système d'équations

$$\begin{cases} y = t(x+1) \\ x^2-2y^2=1 \end{cases}$$

En subsituant la première équation dans la deuxième on obtient l'équation du second degré en x

$$x^2-2\big(t(x+1)\big)^2=1.$$

Là encore, nous n'avons pas besoin d'appliquer la fameuse formule du *delta* [1] car

$$\begin{aligned} x^2-2\big(t(x+1)\big)^2=1 &\iff x^2-1-2\big(t(x+1)\big)^2=0 \\ &\iff (x-1)(x+1)-2t^2(x+1)^2=0 \\ &\iff (x+1)\big(x-1-2t^2(x+1)\big) \\ &\iff x=-1 \quad \text{ou} \quad x=\frac{1+2t^2}{1-2t^2}. \end{aligned}$$

1. Passer par le delta cache souvent la mécanique sous-jacente à la résolution d'équations, à utiliser seulement en cas de nécessité.

La division par $1-2t^2$ n'est pas illicite ici car aucun rationnel au carré ne donne $1/2$ ($t^2 \neq 1/2$). L'ordonnée du point recherché est donc donnée par la formule

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

Puisque ce point appartient à l'hyperbole, ses coordonnées vérifient son équation, à savoir

$$\left(\frac{1+2t^2}{1-2t^2}\right)^2 - 2\left(\frac{2t}{1-2t^2}\right)^2 = 1.$$

Notez alors que cette formule est facile à démontrer, mais difficile à imaginer sans la méthode de Diophante. Si $t=0$ (droite horizontale), ma formule devrait me donner le point $(1,0)$, est-ce correct ? Dans ce cas,

$$x = \frac{1+2\times 0^2}{1+2\times 0^2} = 1 \quad \text{et} \quad y = \frac{2\times 0}{1-2\times 0^2} = 0.$$

Super, notre formule donne le bon point pour $t=0$. Pour $t=1/4$ on obtient

$$x = \frac{1+2\times(1/4)^2}{1-2\times(1/4)^2} = \frac{9}{7} \quad \text{et} \quad y = \frac{2\times 1/4}{1-2\times(1/4)^2} = \frac{4}{7}.$$

Le point $(9/7, 4/7)$ vérifie-t-il l'équation $x^2-2y^2=1$? Pour s'en convaincre un petit calcul s'impose

$$\begin{aligned}\left(\frac{9}{7}\right)^2 - 2\times\left(\frac{4}{7}\right)^2 &= \frac{81}{49} - 2\times\frac{16}{49}\\ &= \frac{81-32}{49}\\ &= \frac{49}{49} = 1.\end{aligned}$$

Bingo ! Cela donne bien un point rationnel sur la courbe et on obtient ainsi tous les points rationnels sur celle-ci.

Les points rationnels, c'est bien, mais peut-on en déduire les points à coordonnées entières comme avec le cercle unité ? Les choses sont plus subtiles dans ce cas. En effet, soit $t = u/v$, où $u, v \in \mathbb{Z}$ et $v \neq 0$.

$$\left(\frac{1+2t^2}{1-2t^2}\right)^2 - 2\left(\frac{2t}{1-2t^2}\right)^2 = 1 \iff \left(\frac{1+2(u/v)^2}{1-2(u/v)^2}\right)^2 - 2\left(\frac{2u/v}{1-2(u/v)^2}\right)^2 = 1.$$

En multipliant en haut et en bas chacune des fractions par v^2 on obtient

$$\left(\frac{v^2+2u^2}{v^2-2u^2}\right)^2 - 2\left(\frac{2uv}{v^2-2u^2}\right)^2 = 1.$$

Cette dernière égalité est équivalente à l'égalité

$$\boxed{(v^2+2u^2)^2 - 2(2uv)^2 = (v^2-2u^2)^2}.$$

La méthode de Diophante donne encore une jolie identité, générant tous les points à coordonnées entières sur l'objet géométrique d'équation $x^2-2y^2=z^2$. Je vous rappelle que dans notre cas, on s'intéresse à l'équation $x^2-2y^2=1$, il suffit alors de prendre $z=1$ dans l'identité ci-dessus afin de résoudre l'équation de Pell dans $\mathbb{Z}^2$. Toutefois, la condition $z=1$ est équivalente à $v^2-2u^2=1$!!! Impasse, retour à la case départ car $v^2-2u^2=1$ est la même que $x^2-2y^2=1$. Heureusement que dans notre cas, il existe des solutions entières faciles [2] à trouver par inspection comme le couple $(3,2)$ car

$$3^2-2\times 2^2=1.$$

Il est alors évident que $(\pm 3,\pm 2)$ sont tous solutions de notre équation. Pour des raisons que nous découvrirons sous-peu, nous allons encoder la solution $(3,2)$ dans le nombre réel $3+2\sqrt{2}$. De même, si (a,b) est solution de l'équation $x^2-2y^2=1$, nous considérerons le nombre $a+b\sqrt{2}$. On dit alors que a est la partie rationnelle de la solution et b sa partie irrationnelle [3]. L'irrationalité de $\sqrt{2}$ se traduit par l'unicité de cette représentation. En effet, si a_1,b_1,a_2 et $b_2\in\mathbb{Z}$ tels que

$$a_1+b_1\sqrt{2}=a_2+b_2\sqrt{2},$$

alors $a_1=a_2$ et $b_1=b_2$. Supposons au contraire que $b_1\neq b_2$, on obtient dans ce cas

$$a_1-a_2=(b_2-b_1)\sqrt{2},$$

ce qui implique une contradiction [4], à savoir

$$\sqrt{2}=\frac{a_1-a_2}{b_2-b_1}.$$

On en déduit que $b_1=b_2$ et que par conséquent $a_1=a_2$. Représenter les solutions d'une équation de type $x^2-ny^2=1$ n'est pas possible quand n est un carré parfait. En effet, si $n=4$ alors les couples $(3,1)$ et $(1,2)$ sont représentés par un même nombre puisque

$$3+\sqrt{4}=1+2\sqrt{4}.$$

Venons-en maintenant à l'intérêt de cette écriture. Afin d'obtenir toutes les solutions de l'équation de Pell $x^2-2y^2=1$, il suffit de calculer les puissances successives de $3+2\sqrt{2}$. Nous avons en effet

$$\begin{aligned}(3+2\sqrt{2})^2&=3^2+2\times 3\times 2\sqrt{2}+(2\sqrt{2})^2\\&=17+12\sqrt{2},\end{aligned}$$

le couple $(17,12)$ est bien solution de l'équation car

$$17^2-2\times 12^2=289-288=1!!$$

Maintenant, un petit calcul montre que $(3+2\sqrt{2})^3=99+70\sqrt{2}$ et on a bien $99^2-2\times 70^2=1$ (vérifier les calculs seul). C'est incroyable, il parait que les puissances successives de $3+2\sqrt{2}$

2. Ce n'est pas toujours le cas. Par exemple la première solution positive de l'équation $x^2-61y^2=1$ est (1766319049, 226153980). Bon courage pour trouver ce couple à la main.

3. Il y a une similarité ici avec partie réelle et partie imaginaire des nombres complexes.

4. Je vous rappelle que $\sqrt{2}$ est un nombre irrationnel, donc ne peut pas s'écrire sous la forme d'une fraction. Nous verrons une preuve de cette affirmation plus loin.

encodent bien les solutions entières de notre chère équation. Mais pourquoi ?

Les équations de Pell contiennent une structure bien particulière et nous allons montrer plus généralement que si $a_1 + b_1\sqrt{2}$ et $a_2 + b_2\sqrt{2}$ sont deux solutions alors

$$a_3 + b_3\sqrt{2} = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$$

l'est aussi. En développant l'expression à droite de l'égalité on obtient

$$\begin{aligned} a_3 + b_3\sqrt{2} &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}. \end{aligned}$$

Pour montrer que (a_3, b_3) est une nouvelle solution, il suffit de montrer que

$$(a_1a_2 + 2b_1b_2)^2 - 2(a_1b_2 + a_2b_1)^2 = 1.$$

Pour se faire, nous procéderons astucieusement. Nous savons en effet que (a_1, b_1) et (a_2, b_2) sont solutions donc

$$a_1^2 - 2b_1^2 = 1 \quad \text{et} \quad a_2^2 - 2b_2^2 = 1,$$

on en déduit en utilisant l'identité remarquable $a^2 - b^2 = (a - b)(a + b)$ que

$$\begin{aligned} 1 &= (a_1^2 - 2b_1^2)(a_2^2 - 2b_2^2) \\ &= (a_1 - b_1\sqrt{2})(a_1 + b_1\sqrt{2})(a_2 - b_2\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2})(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= \big((a_1a_2 + 2b_1b_2) - (a_1b_2 + a_2b_1)\sqrt{2}\big)\big((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\big) \\ &= (a_1a_2 + 2b_1b_2)^2 - 2(a_1b_2 + a_2b_1)^2. \end{aligned}$$

La dernière égalité découle elle aussi de la troisième identité remarquable car

$$(a - b\sqrt{2})(a + b\sqrt{2}) = a^2 - 2b^2.$$

Ce raisonnement justifie que les puissances successives de $3 + 2\sqrt{2}$ sont solutions de l'équation de Pell car on a tout simplement multiplié $3 + 2\sqrt{2}$ par lui-même.

Ce qui est encore plus surprenant dans cette histoire, c'est que les points à coordonnées entières situés sur l'hyperbole d'équation $x^2 - 2y^2 = 1$ donnent des renseignements sur les décimales de $\sqrt{2}$. Tout d'abord, notez qu'il est facile de calculer les décimales d'une fraction, en utilisant l'algorithme de division décimale d'Euclide (celui qu'on a appris à l'école primaire). Cet algorithme fort simple et fort sympathique ne s'applique plus à $\sqrt{2}$ car ce dernier est irrationnel. Ce qui est magique avec notre petite étude de l'hyperbole, ses points à coordonnées entières vont fournir des fractions de plus en plus proche de $\sqrt{2}$. Cela permettra donc de trouver ses décimales en utilisant nos connaissances de base sur la division. En effet, la première solution $(3, 2)$ donne la fraction

$$\frac{3}{2} = 1.5,$$

le couple $(17, 12)$ donne la fraction

$$\frac{17}{12} = 1.416666\cdots$$

et le couple $(99,70)$ donne $\frac{99}{70} = 1.4142\cdots$. À vos calculatrices pour voir que cette fraction partage 4 décimales avec $\sqrt{2}$. Je vous invite à calculer d'autres solutions afin de voir que les fractions se rapprochent de plus en plus de notre fameux irrationel. Mais pourquoi ? La raison à cela est là encore relativement triviale car si (x,y) est un point à coordonnées entières sur l'hyperbole et $y \neq 0$ alors l'égalité $x^2 - 2y^2 = 1$ implique en divisant par y^2 que

$$\left(\frac{x}{y}\right)^2 - 2 = \frac{1}{y^2}.$$

Donc si y est suffisamment grand, $1/y^2$ sera proche de 0. Par conséquent

$$\left(\frac{x}{y}\right)^2 - 2 \simeq 0,$$

ou encore $x/y \simeq \sqrt{2}$. Great ! Avant de finir cette section, une question me vient à l'esprit : toute hyperbole croise-t-elle des points à coordonnées entières dans le plan. La réponse est non et cela dépend là encore des propriétés arithmétiques des coefficients de l'équation de celle-ci.

En effet, soit $\mathscr{H}$ l'hyperbole d'équation $x^2 - 5y^2 = 2$. Cette dernière ne contient aucun point à coordonnées entières pour la raison suivante. Si (x,y) est un couple solution de l'équation $x^2 - 5y^2 = 2$ alors on a $x^2 = 2 + 5y^2$. Cela peut se lire "le reste de la division euclidienne de x^2 par 5 vaut 2". Nous allons démontrer que ceci est impossible. Modulo 5, x ne peut être congru qu'à 0, 1, 2, 3 ou 4. Ainsi,

- Si $x \equiv 0 \pmod 5$ alors $x^2 \equiv 0^2 \pmod 5 \equiv 0 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 1 \pmod 5$ alors $x^2 \equiv 1^2 \pmod 5 \equiv 1 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 2 \pmod 5$ alors $x^2 \equiv 2^2 \pmod 5 \equiv 4 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 3 \pmod 5$ alors $x^2 \equiv 3^2 \pmod 5 \equiv 4 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 4 \pmod 5$ alors $x^2 \equiv 4^2 \pmod 5 \equiv 1 \pmod 5 \not\equiv 2 \pmod 5$.

Dans tous les cas, $x^2 \not\equiv 2 \pmod 5$. Le résultat en découle [5].

4 Le principe de récurrence

Nous allons explorer dans cette section le principe de la récurrence via quelques phénomènes sur les entiers naturels.

Exemple 1 : Dans cet exemple, nous nous intéressons à la somme des entiers naturels impairs, à savoir

$$S_n = \sum_{k=1}^{n} (2k-1).$$

5. Cette preuve est élémentaire pour ceux qui connaissent les congruences, sinon nous aborderons cet outil plus loin en détail.

Rien ne vaut une petite expérimentation pour voir que

$$
\begin{aligned}
S_1 &= 1 = 1^2 \\
S_2 &= \underbrace{1}_{S_1} + 3 = 4 = 2^2 \\
S_3 &= \underbrace{1+3}_{S_2} + 5 = 4 + 5 = 9 = 3^2 \\
S_4 &= \underbrace{1+3+5}_{S_3} + 7 = 9 + 7 = 16 = 4^2 \\
S_5 &= \underbrace{1+3+5+7}_{S_4} + 9 = 16 + 9 = 25 = 5^2 \\
&\vdots
\end{aligned}
$$

On se rend compte donc que pour les premières valeurs de n, la somme des n premiers entiers naturels impairs vaut n^2, autrement dit $\boxed{S_n = n^2}$. Ce résultat reste-t-il vrai pour tout entier naturel $n \geq 1$? C'est à dire je m'amuse à prendre $n = 1000$, vais-je obtenir

$$S_{1000} = 1 + 3 + \cdots + 1999 = 1000^2 ?$$

Notre expérimentation avec les cinq premières valeurs de n nous donne une idée sur ce qui devrait se passer à n'importe quel rang n. Toutefois, sans démonstration mathématique, rien ne garantit la validité de notre conjecture. Afin de prouver ce résultat pour tout entier naturel $n \geq 1$, nous allons procéder par récurrence. Remarquons tout d'abord que la somme S_{n+1}, au rang $n+1$, se déduit à partir de la somme S_n, au rang n, par la formule

$$S_{n+1} = S_n + (2n+1).$$

C'est assez trivial puisque

$$
\begin{aligned}
S_n &= 1 + 3 + \cdots + (2n-1) \\
S_{n+1} &= 1 + 3 + \cdots + (2n-1) + (2n+1),
\end{aligned}
$$

car $(2n+1)$ est l'entier impair suivant $(2n-1)$. Cela suggère que les propriétés de S_{n+1} sont liées aux propriétés de S_n. La récurrence consiste essentiellement à partir de S_n pour prouver S_{n+1}. Pour se faire, notons $\mathscr{P}(n)$ la propriété

$$\mathscr{P}(n) : \quad S_n = n^2.$$

On doit alors vérifier que $\mathscr{P}(1)$ est vraie, étape qu'on appellera **l'initialisation**. Ensuite on doit montrer que si pour un entier naturel n, $\mathscr{P}(n)$ est vraie alors $\mathscr{P}(n+1)$ est vraie aussi. Cette dernière étape s'appelle **l'hérédité**. Puisqu'on a vérifié la véracité de $\mathscr{P}(1)$ et puisqu'on a montré pour un n quelconque que $\mathscr{P}(n) \implies \mathscr{P}(n+1)$, cela donne le schéma

$$\mathscr{P}(1) \underset{HR}{\implies} \mathscr{P}(2) \underset{HR}{\implies} \mathscr{P}(3) \cdots \underset{HR}{\implies} \mathscr{P}(n) \underset{HR}{\implies} \cdots$$

où HR désigne l'hérédité. On comprend alors $\mathscr{P}(1)$ est vraie donc $\mathscr{P}(2)$ est vraie aussi, ce qui implique la véracité de $\mathscr{P}(3)$ etc et tout ceci grâce à l'hérédité. On peut imager la récurrence comme la chute d'une file infinie de dominos comme le montre la figure ci-dessous. Si je suis certain que le premier domino va tomber et si de plus je sais que la chute du n-ème domino entraine la chute du $n+1$-ème domino pour n'importe quel rang n, alors je sais que les dominos vont tomber l'un après l'autre et ce jusqu'à l'infini. L'histoire est la même avec la récurrence !

Revenons à nos moutons et démontrons par récurrence que $S_n = n^2$ pour tout entier naturel $n \geq 1$.

- **Initialisation :** La propriété $\mathscr{P}(1)$ est vraie car

$$S_1 = 1 = 1^2.$$

  Ainsi la formule $S_n = n^2$ s'applique bien pour $n = 1$.

- **Hérédité :** Soit $n \geq 1$ un entier naturel. Supposons que $\mathscr{P}(n)$ est vraie et montrons dans ce cas que $\mathscr{P}(n+1)$ l'est aussi. On sait donc que pour ce n choisi au hasard $S_n = n^2$ et on souhaite prouver que $S_{n+1} = (n+1)^2$. Or on a vu que S_{n+1} et S_n sont liées par la formule $S_{n+1} = S_n + (2n+1)$, cela implique donc que

$$S_{n+1} = n^2 + (2n+1) = (n+1)^2.$$

  D'où le résultat.

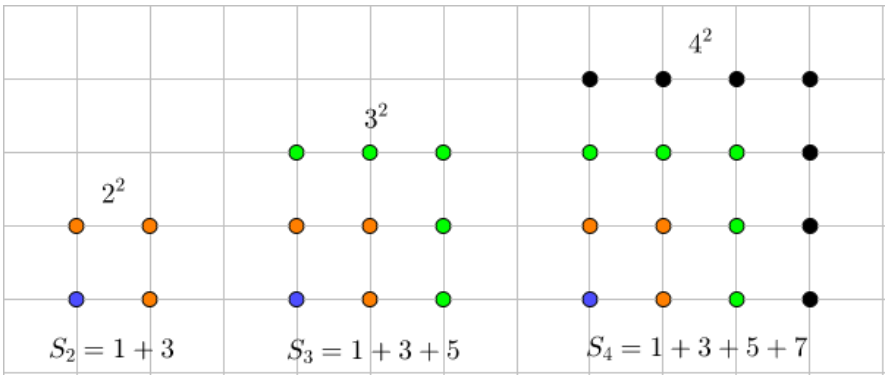
Il existe plusieurs preuves à notre résultat et à vrai dire, la récurrence n'est pas le meilleur moyen pour y arriver. Une deuxième preuve utilise une manipulation algébrique consistant à rajouter tous les entiers pairs et à les soustraire à la fois pour obtenir

$$\begin{aligned}
S_n &= 1+3+\cdots+(2n-1) \\
&= 1+2+3+4+\cdots+(2n-2)+(2n-1)-(2+4+\cdots+(2n-2)) \\
&= 1+2+3+4+\cdots+(2n-2)+(2n-1)-2(1+2+\cdots+(n-1)) \\
&= \frac{(2n-1)(2n-1+1)}{2} - 2\frac{(n-1)(n-1+1)}{2} \\
&= \frac{(2n-1)\times 2n}{2} - n(n-1) \\
&= n(2n-1) - n(n-1) \\
&= n(2n-1-n+1) \\
&= n^2.
\end{aligned}$$

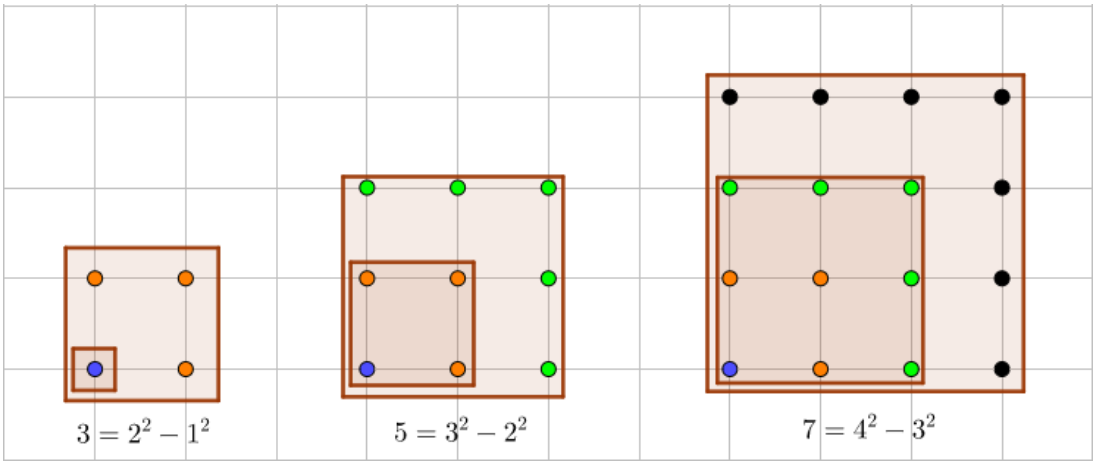
Voilà tout simplement et j'espère que vous avez remarqué qu'on a utilisé le résultat affirmant que la somme des n premiers entiers naturels vaut $n(n+1)/2$. Autrement dit

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

Avouons que cette astuce sort de l'espace. De surcroît, on ne comprend toujours pas bien pourquoi notre somme donne toujours un carré parfait. Une meilleure approche est de visualiser cette somme géométriquement, comme le montre la figure ci-dessous



Une belle preuve sans mots. Je vous invite à dessiner S_5 et S_6 pour vous en convaincre et voir que la figure finale sera toujours un carré. Notez toutefois que suivant les normes de la rigueur moderne, une visualisation ne vaut jamais une preuve mathématique. Néanmoins, cette figure suggère une preuve algébrique rigoureuse,



à savoir tout entier naturel impair est la différence de deux carrés consécutifs. Sachant que tout entier impair peut s'écrire sous la forme $2k-1$, ce résultat se démontre facilement car

$$k^2-(k-1)^2=k^2-(k^2-2k+1)=2k-1.$$

Notre dulcinée somme S_n devient donc

$$\begin{aligned}S_n &= 1+3+5+\cdots+(2n-3)+(2n-1)\\ &= (1^2-0^2)+(2^2-1^2)+(3^2-2^2)+\cdots+((n-1)^2-(n-2)^2)+(n^2-(n-1)^2)\\ &= (\cancel{1}^2-0^2)+(\cancel{2}^2-\cancel{1}^2)+(3^2-\cancel{2}^2)+\cdots+((n\not-1)^2-(n-2)^2)+(n^2-(n\not-1)^2)\end{aligned}$$

et on voit que tous les termes s'annulent sauf $n^2-0^2=n^2$. Le résultat en découle. Cette preuve, bien plus parlante que les autres, cache en réalité une récurrence dans les trois

points de suspension. En toute rigueur et pour éviter toute confusion, on pourra démontrer par récurrence le résultat plus général sur les sommes télescopiques : si (u_n) est une suite de nombres alors

$$\sum_{k=0}^{n}(u_{k+1}-u_k)=u_{n+1}-u_0.$$

En effet, par récurrence on a

- **Initialisation :** Si $n=0$ alors

  $$\sum_{k=0}^{0}(u_{k+1}-u_k)=u_1-u_0,$$

  ce qui prouve que notre propriété est vraie au rang $n=0$.

- **Hérédité :** Soit $n\in\mathbb{N}$. Supposons que la propriété est vraie pour ce n, c'est à dire que

  $$\sum_{k=0}^{n}(u_{k+1}-u_k)=u_{n+1}-u_0.$$

  Dans ce cas, au rang $n+1$ on a

  $$\begin{aligned}S_{n+1}&=\sum_{k=0}^{n+1}(u_{k+1}-u_k)\\&=\sum_{k=0}^{n}(u_{k+1}-u_k)+(u_{n+2}-u_{n+1})\\&\underset{HR}{=}(u_{n+1}-u_0)+(u_{n+2}-u_{n+1})\\&=u_{n+2}-u_0.\end{aligned}$$

  Ce qui achève notre récurrence.

Le résultat sur la somme des nombres entiers impairs en découle en considérant la suite (u_n) définie par $u_n=n^2$.

Exemple 2 Nous nous intéressons dans ce deuxième exemple à une somme similaire définie par

$$\begin{aligned}S_1&=1=1^2\\S_2&=1+2+1=4=2^2\\S_3&=1+2+3+2+1=9=3^2\\S_4&=1+2+3+4+3+2+1=16=4^2\\&\vdots\\S_n&=1+2+3+\cdots+(n-1)+n+(n-1)+(n-2)+\cdots+1\underset{?}{=}n^2.\end{aligned}$$

Notre conjecture semble vraie et c'est une application directe du principe de la récurrence.

En effet

- **Initialisation :** Comme nous venons de voir, la propriété est vraie pour $n = 1$.
- **Hérédité :** Soit $n \geq 1$. Supposons que la propriété est vraie pour ce n, à savoir que

$$S_n = 1+2+3+\cdots(n-1)+n+(n-1)+(n-2)+\cdots+1 = n^2.$$

La somme S_{n+1} s'obtient à partir de S_n en additionnant les entiers $n+1$ et n. Ainsi on a

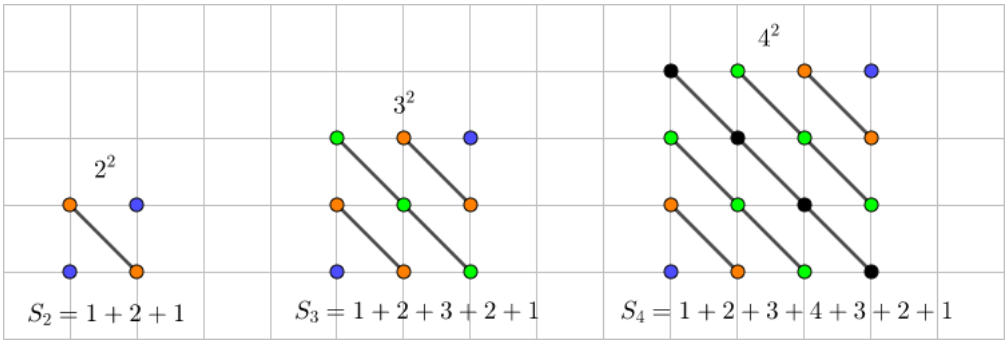
$$\begin{aligned} S_{n+1} &= S_n + (n+1) + n \\ &= n^2 + 2n + 1 \\ &= (n+1)^2. \end{aligned}$$

Ceci achève notre récurrence.

Remarquez qu'on aurait pu se passer de ce raisonnement en procédant directement de la façon suivante

$$\begin{aligned} S_n &= \underbrace{1+2+3+\cdots+(n-1)+n}_{\frac{n(n+1)}{2}} + \underbrace{(n-1)+(n-2)+\cdots+1}_{\frac{n(n-1)}{2}} \\ &= \frac{n(n+1)}{2} + \frac{n(n-1)}{2} \\ &= \frac{n(n+1+n-1)}{2} \\ &= n^2 \end{aligned}$$

Ici encore, une visualisation géométrique vaut bien mieux qu'une preuve formelle. Voilà ce qui se passe avec un petit dessin



Il est temps maintenant de se poser une question fondamentale : peut-on se passer de l'initialisation dans un raisonnement par récurrence ? La réponse est non comme le montre le contre-exemple ci-dessous.

Soit $\mathscr{P}(n)$ la propriété " 3 divise 4^n ". Nous allons démontrer la validité de l'hérédité, c'est à dire que si $\mathscr{P}(n)$ est vraie alors $\mathscr{P}(n+1)$ l'est aussi. Pourtant la propriété $\mathscr{P}(n)$ ne sera vraie pour aucun entier naturel n. Il n'y aura aucun rang pour lequel on pourra initialiser notre propriété et notre file infinie de dominos ne tombera pas.

- **Hérédité** Soit $n \in \mathbb{N}$ et supposons que pour ce n fixé 3 divise 4^n. Il existe alors un entier k pour lequel $4^n = 3k$. Cela implique que

$$4^{n+1} = 4 \times 4^n = 4 \times 3k = 3 \times 4k,$$

ce qui implique que 3 divise 4^{n+1}. Toutefois, à aucun endroit 3 divise 4^n, puisque 3 est un nombre premier et le seul nombre premier divisant 4^n est 2. Par unicité de la décomposition d'un entier naturel en facteurs premiers, 3 ne peut donc pas figurer dans celle-ci. Par ailleurs, pour ceux qui connaissent les congruences, le reste de la division euclidienne de 4 par 3 vaut 1. Cela s'écrit $4 \equiv 1 \pmod 3$, on peut alors voir le signe $\equiv$ comme une égalité dans un autre monde de nombres, une égalité qui se comporte bien par rapport au passage à une puissance n. Ainsi $4 \equiv 1 \pmod 3$ implique que $4^n \equiv 1^n \pmod 3 \equiv 1 \pmod 3$. Du coup, le reste de la division euclidienne de 4^n par 3 vaut toujours $1 \neq 0$. Pour s'en convaincre, les premières puissances de 4 donnent

$$\begin{aligned} 4^2 &= 16 = 3 \times 5 + 1 \\ 4^3 &= 64 = 3 \times 21 + 1 \\ 4^4 &= 256 = 3 \times 85 + 1 \\ &\vdots \end{aligned}$$

Moralité, il faut toujours initialiser la récurrence sinon cela risque de ne pas fonctionner.

Nous terminons cette section avec un paradoxe dû au logicien Alfred Tarski.

Alfred Tarski

Soit $\mathscr{P}(n)$ la propriété

Dans toute collection de n nombres $a_1, a_2, \ldots, a_n$, ces nombres sont tous égaux.

Autrement dit $a_1 = a_2 = \cdots = a_n$. Le moins qu'on puisse dire sur cet énoncé c'est qu'il est très FAUX. Pour $n = 3$, si $a_1 = 2, a_2 = 5$ et $a_3 = 7$, rien ne peut affirmer que $a_1 = a_2 = a_3$ et puis c'est erroné. Toutefois, nous allons bien démontrer l'énoncé de Tarski par récurrence. En effet

- **Initialisation :** Si $n = 1$, il n'y a qu'un nombre, à savoir a_1 et on a bien $a_1 = a_1$. L'énoncé est donc vrai.

- **Hérédité :** Soit $n \geq 1$. Supposons que la propriété est vraie pour ce n et montrons que cela implique $\mathscr{P}(n+1)$. Soit donc $a_1, a_2, \ldots a_{n+1}$ une collection contenant $n+1$ nombres. La collection $a_1, a_2, \ldots, a_n$ est une collection contenant n nombres donc l'hypothèse de la récurrence implique que $a_1 = a_2 = \cdots = a_n$. De même, la collection $a_2, a_3, \ldots, a_{n+1}$ est une collection de n nombres donc sont tous égaux, à savoir $a_2 = a_3 = \cdots = a_{n+1}$. Cela implique donc que

  $$a_1 = a_2 = a_3 = \cdots = a_n = a_{n+1}.$$

  Ceci achève donc notre récurrence ! ! ! Ce résultat intuitivement faux serait-il réellement démontrable par récurrence ? Cela remet-il en cause notre fameux principe ? Où se trouve l'erreur dans ce raisonnement. Je vous invite à méditer avant de lire la suite.

Le passage de $n = 2$ à $n = 3$ ne pose aucun problème. De même le passage de $n = 3$ à $n = 4$ et tous les autres passages de n à $n+1$ se passent sans histoires. Toutefois, le passage de $n = 1$, c'est à dire notre initialisation, à $n = 2$ est impossible. Toute la récurrence tombe donc à l'eau.

5 Le principe de la descente infinie de Fermat

Nous inspectons dans ce paragraphe le fameux principe de la descente infinie de Fermat. Bien qu'il ne soit pas enseigné dans le parcours scolaire ordinaire, nous verrons ensemble qu'il est d'une importance capitale en arithmétique. Ce principe, comme son nom l'indique, a été inventé par notre éminent ancêtre *Pierre de Fermat* afin de répondre à des questions de la théorie des nombres.

Pierre de Fermat

Ce principe affirme tout simplement qu'on ne peut pas construire une suite strictement décroissante d'entiers naturels. J'espère que cela semble évident pour vous car en effet si (u_n) est une suite d'entiers naturels alors pour tout $n \in \mathbb{N}, u_n \geq 0$. De plus si par exemple $u_0 = 12$ alors u_1 doit être un entier naturel strictement plus petit que u_0, prenons $u_1 = 9$. De même, $u_2 < u_1$ et $u_3 < u_2$ etc. On voit donc que cette suite ne peut pas descendre infiniment car elle doit rester positive. Plus formellement, l'ensemble

$$U = \{u_n, n \in \mathbb{N}\} \subset \mathbb{N}$$

est un sous-ensemble non vide de $\mathbb{N}$, il admet ainsi un plus petit élément u_{n_0} [6]. Or la suite (u_n) est strictement décroissante, par conséquent $u_{n_0+1} < u_{n_0}$. Cela signifie que u_{n_0+1} est un élément de U plus petit que son plus petit élément u_{n_0}. Cela conduit évidemment à une *contradiction*. Ainsi pour démontrer l'impossibilité d'un énoncé arithmétique, il suffit de construire à partir de celui-ci une suite strictement décroissante d'entiers naturels. Un exemple vaut mieux qu'un long discours.

Exemple1 : Dans cet exemple, nous allons démontrer que $\sqrt{2}$ est un nombre irrationnel. Autrement dit $\sqrt{2}$ ne peut pas s'écrire sous la forme d'une fraction p/q. Pour se faire, supposons qu'il existe un couple (p,q) d'entiers naturels tel que

$$\sqrt{2} = \frac{p}{q} \quad \text{où } p > q.$$

Cela implique en élévant au carré que $2 = p^2/q^2$ ou encore que $p^2 = 2q^2$. Par conséquent p^2 est un nombre pair et donc p l'est aussi [7]. Notre entier p s'écrit donc sous la forme $p = 2k$, où k désigne un entier naturel. La relation $p^2 = 2q^2$ implique alors la relation $(2k)^2 = 2q^2$ ou encore

$$2k^2 = q^2.$$

Cette relation s'écrit $\sqrt{2} = q/k$ où $q > k$, auquel cas on obtient une deuxième représentation de $\sqrt{2}$ sous forme d'une fraction. Notez alors qu'on a construit les trois premiers termes d'une suite d'entiers naturels tels que $p > q > k$. Nous pouvons construire de même un nouvel entier naturel x tel que $\sqrt{2} = k/x$ et $p > q > k > x$. En réitérant ce même procédé, nous pouvons construire une suite strictement décroissante d'entiers naturels. Cela conduit donc à une contradiction d'après le principe de la descente infinie de Fermat. D'où l'irrationalité de $\sqrt{2}$. Dans le monde mathématique, il existe plusieurs preuves de l'irrationalité de $\sqrt{2}$. L'une d'elle est une preuve géométrique (celle que je préfère à titre personnel), bien plus parlante que la preuve utilisant des arguments arithmétiques. Nous n'aborderons pas cette preuve ici mais notez qu'elle fournit une autre suite strictement décroissante d'entiers naturels prouvant là encore l'irrationalité de $\sqrt{2}$. En effet, l'identité qui découle de l'argument géométrique est

$$\sqrt{2}(\sqrt{2}-1) = 2-\sqrt{2}.$$

Cette identité s'écrit aussi sous la forme

$$\sqrt{2} = \frac{2-\sqrt{2}}{\sqrt{2}-1}.$$

Ainsi si $\sqrt{2} = p/q$ alors on obtient

$$\sqrt{2} = \frac{p}{q} = \frac{2-\frac{p}{q}}{\frac{p}{q}-1} = \frac{2q-p}{p-q}.$$

Aha, pas mal tout ça ! Je viens de trouver une nouvelle fraction égale à $\sqrt{2}$. Il nous reste à démontrer que $q > p-q$. Autrement dit, le dénominateur de la première fraction est strictement plus grand que le dénominateur de la deuxième. Cette inégalité est relativement

6. Par l'axiome du bon ordre qui dit que tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.

7. Nous pouvons démontrer aisément que si p^2 est un entier pair alors p est pair aussi. En effet, si p est impair alors il s'écrit sous la forme $p = 2k+1$, son carré s'écrit alors $p^2 = 2(2k^2+2k)+1$, qui est un nombre impair. Autrement dit si p^2 est pair, p ne peut pas être impair car son carré serait impair !

triviale puisqu'elle est équivalente à l'inégalité $2 > p/q = \sqrt{2}$. Par ailleurs le dénominateur $p-q$ de notre nouvelle fraction est bien un entier positif car rappelez-vous $p > q$. L'irrationalité de $\sqrt{2}$ découle alors de l'impossibilité de la construction d'une telle suite. Merci Fermat !

Exemple2 : Nous nous intéressons dans ce deuxième exemple à un énoncé qui a fait couler beaucoup d'encre. Nous avons vu ensemble que l'équation $x^2 + y^2 = z^2$ admet une infinité de solutions, à savoir les triplets pythagoriciens. Notre regretté Fermat s'est alors posé la question naturelle, à savoir l'équation $x^3 + y^3 = z^3$ admet-elle des solutions entières telles que $xyz \neq 0$ [8] ? Plus généralement, si $n \geq 3$ et $xyz \neq 0$, peut-on résoudre l'équation $x^n + y^n = z^n$ chez les entiers ? Cette dernière question s'appelle le Grand Théorème de Fermat, Fermat lui-même prétend avoir trouvé une preuve à l'impossibilité de la résolution d'une telle équation. Toutefois, il ne publie rien et dit que la marge est trop petite pour qu'il puisse y mettre sa démonstration. Cette conjecture n'a été démontré que par son éminence, le mathématicien britannique Andrew Wiles en 1995, c'est à dire environ 350 années après Fermat, en utilisant au passage un arsenal technique extrêmement sophistiqué, dépassant de bien loin le cadre de notre cours !

Andrew Wiles

Fermat a su toutefois démontrer sa conjecture pour $n = 4$, à savoir si $xyz \neq 0$, l'équation $x^4 + y^4 = z^4$ n'admet pas de solutions. Dans notre cas, nous esquisserons [9] sa preuve. L'une des manières pour démontrer qu'un énoncé est impossible est de lui trouver une conséquence impossible. Mais quelle conséquence donc pour notre petit énoncé ? ! Fermat établit en effet un lien avec les triangles pythagoriciens, à savoir les triangles rectangles dont les côtés sont des entiers. Il démontre que

si $x^4 + y^4 = z^4$ était résoluble dans nos conditions alors il pourrait construire un triangle pythagoricien ayant une aire un carré parfait !

Notre ancêtre démontre alors avec son principe de la descente infinie que ce dernier résultat est impossible : il n'existe pas de triangle pythagoricien dont l'aire est un carré parfait. Pour se faire, il démontre que si un tel triangle existe, alors on pourra construire un triangle strictement plus petit ayant la même propriété. Ici, nous expliciterons seulement le lien en

8. Le cas $xyz = 0$ est trivial et est laissé au lecteur.
9. Nous manquerons d'outils pour l'instant pour finaliser cette démonstration mais nous y reviendrons plus loin.

rouge. En effet, nous avons vu que les triplets pythagoriciens sont tous de la forme $(u^2 - v^2, 2uv, u^2 + v^2)$. Ainsi, si x, y et z vérifie l'équation $x^4 + y^4 = z^4$ alors $x^4 = z^4 - y^4$, ce qui implique que le triplet

$$(z^4 - y^4, 2z^2y^2, z^4 + y^4)$$

est un triplet pythagoricien. L'aire de ce triangle vaut alors

$$\frac{1}{2}(z^4 - y^4) \times 2z^2y^2 = x^4z^2y^2 = (x^2zy)^2.$$

On obtient ainsi un triangle pythagoricien dont l'aire est un carré parfait. Contradiction. Très ingénieux, cela demande de la technique et Fermat n'en manquait pas ! Nous terminerons cette preuve quand on disposera de suffisamment d'artillerie arithmétique.