Cours d'arithmétique

Baccalauréat ++

Mohamed ATOUANI

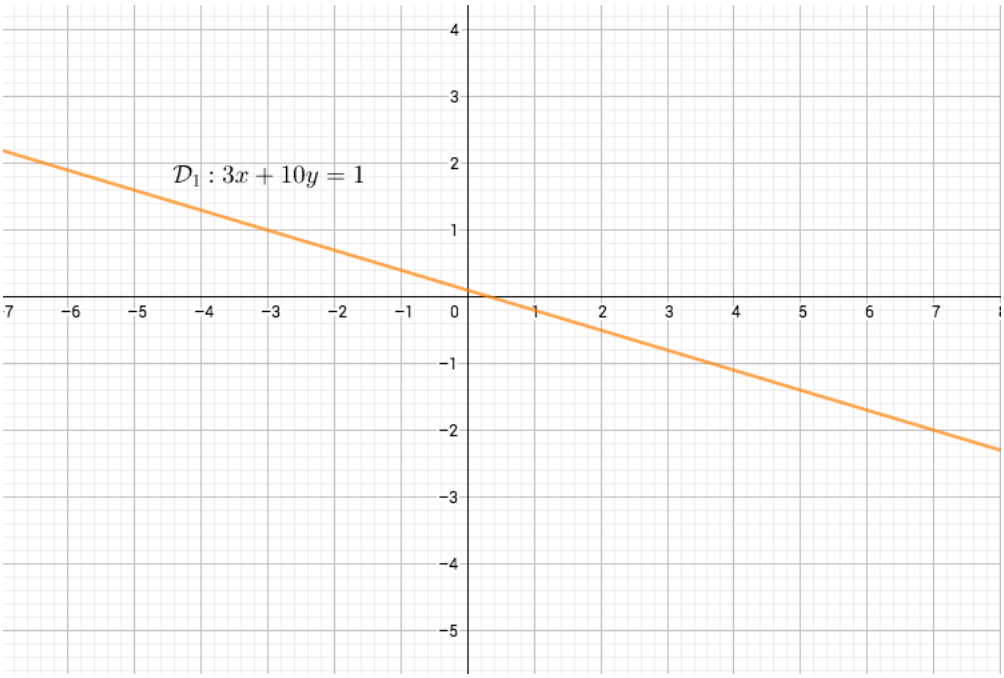
Professeur de Mathématiques
Clandestines

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

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

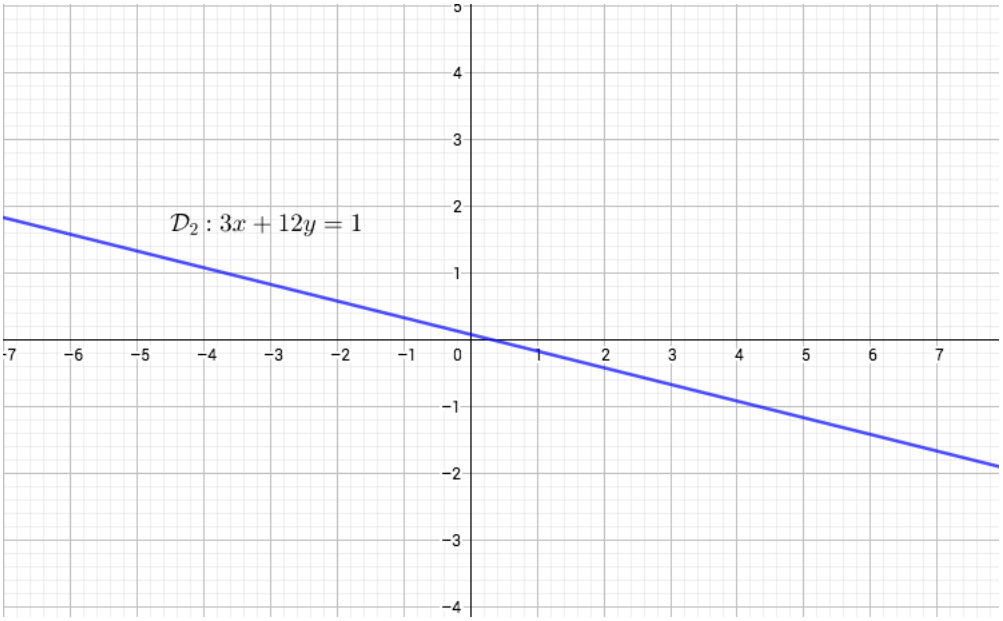
On peut bien sûr vérifier notre formule pour tout entier k, ainsi tout couple de la forme $(10k-3,-3k+1)$ est solution de l'équation diophantienne $3x+10y=1$ car

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

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 $(0,0,0)$.

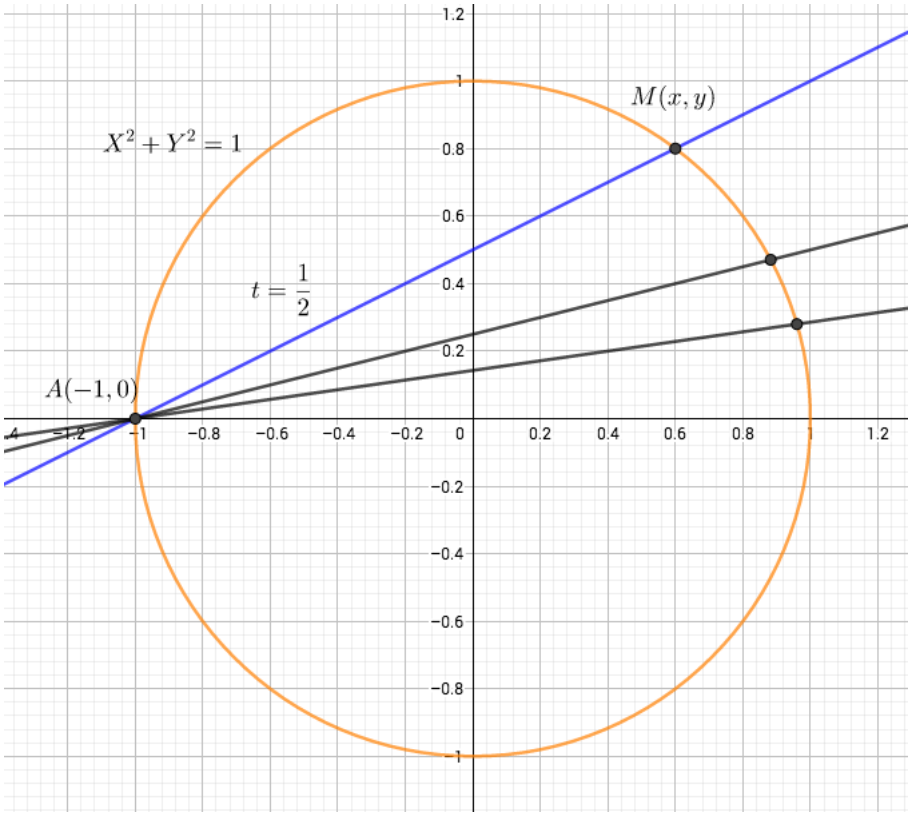
2ème cas : Si $z\neq 0$ alors

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

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 $p,q\in\mathbb{Q}$. Notons 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

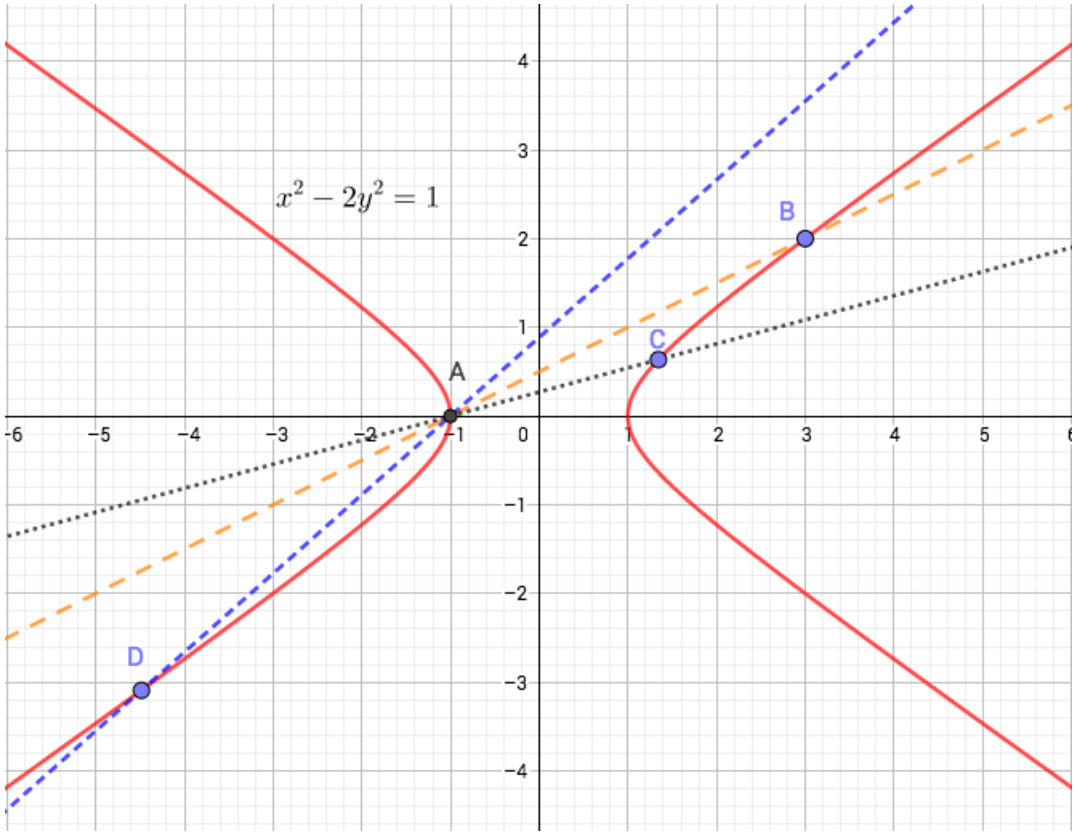
Nous avons abordé dans les deux premières sections l'arithmétique sur les droites affines et l'arithmétique sur le cercle unité, nous aborderons dans cette partie l'arithmétique sur l'hyperbole d'équation $x^2-2y^2=1$. Nous verrons que l'étude des points à coordonnées entières sur cet objet géométrique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

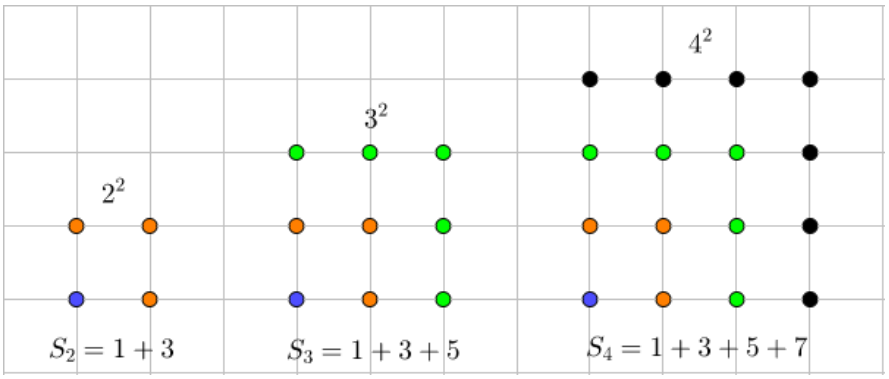
Il existe plusieurs preuves à notre résultat et à vrai dire, la récurrence n'est pas le meilleur moyen pour y arriver. Une deuxième preuve utilise une manipulation algébrique consistant à rajouter tous les entiers pairs et à les soustraire à la fois pour obtenir

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

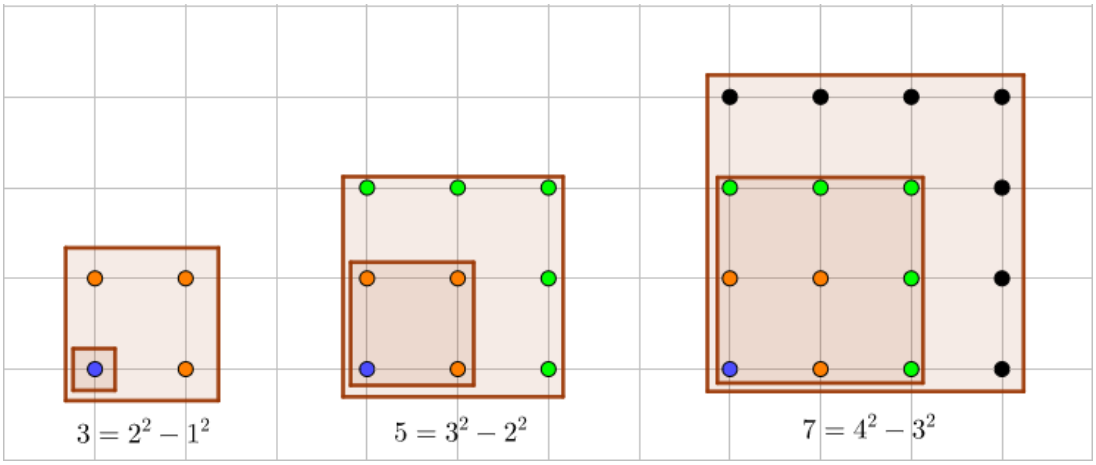
Voilà tout simplement et j'espère que vous avez remarqué qu'on a utilisé le résultat affirmant que la somme des n premiers entiers naturels vaut $n(n+1)/2$. Autrement dit

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

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

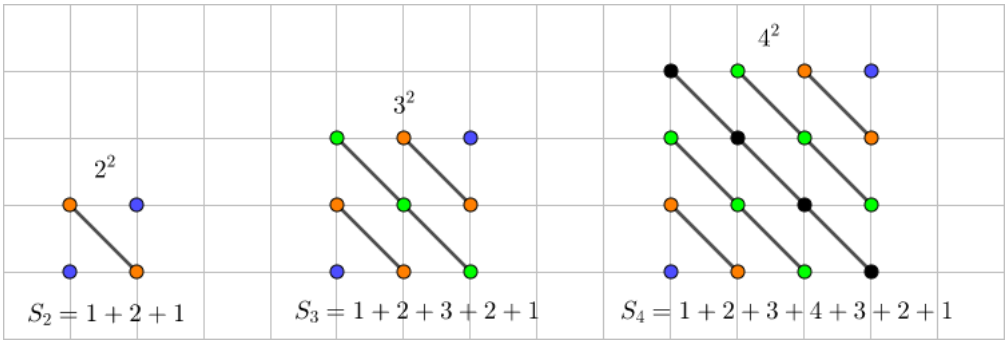
$$\begin{aligned} S_{n+1} &= S_n + (n+1) + n \\ &= n^2 + 2n + 1 \\ &= (n+1)^2. \end{aligned}$$

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.

6 L'axiome du bon ordre et le principe de la récurrence

Ce paragraphe est une petite digression légèrement futuriste. En effet, nous avons parlé rapidement de l'axiome du bon ordre, à savoir tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément. Ce résultat nous parait intuitivement évident. Bien sûr, si on prend un ensemble constitué d'entiers naturels alors il existe un plus petit entier parmi ceux-là. Mais rien n'est bien évident trop longtemps en mathématiques. On pourrait très bien se dire comment sont contruits les entiers naturels à la base ? Et puis qu'est ce qui garantit leur consistence ? Peut-on autrement dit tomber un jour sur un paradoxe chez les entiers ? Cela serait peut être une catastrophe mathématique, tout tombera à l'eau !

Dans notre cas en tout cas, si on accepte le principe de la récurrence, on pourra démontrer relativement sans beaucoup de travail l'axiome du bon ordre. En effet, on pourra démontrer de façon équivalente que si A est une partie de $\mathbb{N}$ sans petit élément alors A est vide. Pour se faire, on montre par récurrence la propriété $\mathscr{P}(n)$

$$\text{pour tout } i \leq n,\ i \notin \text{A}.$$

- **Initialisation :** $\mathscr{P}(0)$ est vraie car sinon 0 serait le plus petit élément de A.
- **Hérédité :** Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}(n)$ est vraie. On sait alors que pour tout $i \leq n$, $i \notin$ A. Par ailleurs, puisque A n'admet pas de plus petit élément, elle ne peut pas contenir $n+1$ (car sinon $n+1$ serait le plus petit élément de A). Ainsi on a démontré que

  $$\text{pour tout } i \leq n+1\ ,\ i \notin \text{A}.$$

  D'où $\mathscr{P}(n+1)$. Élégant n'est ce pas ? !

En vrai (et c'est incroyable), l'axiome du bon ordre implique le principe de la récurrence ! ! ! En plus clair, si on accepte l'axiome du bon ordre comme intuitivement évident alors on pourra démontrer le principe de la récurrence. En effet, soit $\mathscr{P}$ une propriété vérifiant les conditions de la récurrence, c'est à dire que

1. $\mathscr{P}(0)$ est vraie.
2. Pour tout $n \in \mathbb{N}$, si $\mathscr{P}(n)$ est vraie alors $\mathscr{P}(n+1)$ l'est aussi.

Supposons par l'absurde que $\mathscr{P}$ est fausse pour quelques entiers naturels. Soit A la partie

$$\{n \in \mathbb{N} / \mathscr{P}(n) \text{ est fausse}\}.$$

Par hypothèse, A est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément d'après l'axiome du bon ordre. On notera cet élément n_0. D'après l'hypothèse de la récurrence $n_0 \neq 0$ car $\mathscr{P}(0)$ est vraie. On pourra donc considérer l'entier naturel $n_0 - 1$ pour lequel la propriété $\mathscr{P}$ est vraie (car n_0 est le plus petit pour lequel la propriété $\mathscr{P}$ est fausse). Encore d'après l'hypothèse de la récurrence

$$\mathscr{P}(n_0 - 1) \implies \mathscr{P}(n_0).$$

Cela implique du coup que $\mathscr{P}(n_0)$ est vraie. Contradiction, la partie A est ainsi vide et $\mathscr{P}(n)$ est vraie pour tout n. Trop philosophique pour vous ? Vous apprécierez ce paragraphe plus tard dans nos aventures mathématiques.

7 Une première rencontre avec les nombres premiers

Vous n'êtes pas sans savoir (je l'espère) que les nombres premiers sont les éléments de base permettant la construction de tous les entiers naturels > 1 par multiplication. Ainsi, tout entier $n \geq 2$ est le produit de nombres premiers (pas nécéssairement distincts) mais un nombre premier ne s'obtient qu'en le multipliant par 1. On obtient donc la définition suivante

Définition : Un nombre premier est un entier naturel admettant exactement deux diviseurs, 1 et lui-même.

Cette définition implique que 1 n'est pas un nombre premier car certes celui-ci est divisible par 1 et par lui-même mais il ne s'agit que d'un seul diviseur ($1 =$ lui-même) alors que dans notre définition on demande exactement deux diviseurs. Une définition équivalente consiste à dire qu'un nombre premier est un entier naturel $p \neq 1$ divisible uniquement par 1 et par lui-même. Remarquez qu'ici on exclut 1 dès le départ car 1 vérifie la deuxième condition "être divisible uniquement par 1 et par lui-même". Beaucoup se posent la question du pourquoi exclure l'entier 1 de l'ensemble des nombres premiers ! Eh bien, en théorie des nombres, on considère qu'une bonne arithmétique est celle dans laquelle il y a unicité de la factorisation en éléments premiers ! L'entier 1 fait défaut à cette histoire et d'autres aussi, d'où son exclusion. Vous comprendrez cette remarque plus en profondeur si vous vous décidez de vous plonger davantage dans la théorie des nombres.

On voit alors que $p_1 = 2$ est le premier nombre premier (et le seul pair, pourquoi ?) car divisible uniquement par 1 et par lui-même. Le nombre $p_2 = 3$ est le deuxième nombre premier de la liste des nombres premiers, 4 n'est pas premier car il est divisible par 2 qui n'est ni 1 ni lui-même etc. Notez alors que la définition des nombres premiers semble d'une grande facilité, toutefois ces nombres nous donnent beaucoup de mal car sont de nature très profonde et très difficile à décortiquer. La théorie des nombres se caractérise par la facilité de l'énoncé de beaucoup de ses problèmes, qui demeurent toutefois très difficiles à résoudre ou même qui dépassent de bien loin les connaissances (très sophistiquées) actuelles en mathématiques. Citons à titre d'exemple la fameuse conjecture de **Goldbach** : tout entier naturel pair plus grand ou égal à 4 peut s'écrire comme la somme de deux nombres premiers. En essayant les premières valeurs on obtient le tableau suivant

n	Décomposition
4	$2+2$
6	$3+3$
8	$5+3$
10	$7+3$
12	$7+5$
$\vdots$	$\vdots$

Je vous invite à inspecter davantage d'entiers naturels pairs pour se rendre compte de la plausibilité de cette conjecture.

Les nombres premiers sont bien rares parmi les nombres entiers dès qu'on s'intéresse à des nombres bien grands. Cela s'explique grosso modo par le fait qu'un grand nombre a potentiellement plus de diviseurs qu'un petit nombre. Toutefois, malgré leur rareté, Euclide a réussi à démontrer dans son *Livre 9* des *Éléments* qu'il en existe une infinité.

Euclide : Il existe une infinité de nombres premiers.

Avant de vous présenter la preuve (très élégante) d'Euclide, nous démontrons que tout nombre entier $n \geq 2$ est le produit de nombres premiers (pas forcément distincts). Cela impliquera en particulier que tout nombre entier $n \geq 2$ admet au moins un diviseur premier. Cette dernière affirmation nous sera utile dans la démonstration d'Euclide. Pour se faire, nous procéderons de deux manières, la première utilisant l'axiome du bon ordre et la deuxième le principe de la récurrence.

1. **Le bon ordre :** Supposons par l'absurde qu'il existe des entiers naturels > 1 qui ne soient pas produits de nombres premiers. D'après l'axiome du bon ordre l'ensemble de ces nombres admet un plus petit élément z. Cet entier n'est pas premier car sinon on pourrait écrire $z = z$ (il s'agit du produit d'un seul élément premier). Donc z est un nombre composé et s'écrit sous la forme $z = xy$, où $1 < x < z$ et $1 < y < z$. Par minimalité de z, les entiers x et y sont produits d'éléments premiers et s'écrivent donc sous la forme
$$x = p_1 p_2 \cdots p_r \quad \text{et} \quad y = q_1 q_2 \cdots q_t$$
où $p_1, p_2, \ldots p_r$ et $q_1, q_2, \ldots q_t$ sont des nombres premiers. Par conséquent
$$z = xy = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_t$$
est produit de nombres premiers. Contradiction ! Le résultat en découle.

2. **La récurrence :** Soit $\mathscr{P}(n)$ la propriété

   tout entier > 1 et $\leq n$ est produit de nombres premiers.

   - **Initialisation :** La propriété est triviale pour $n = 2$ car comme 2 est premier, il est le produit d'un seul nombre premier, à savoir lui-même.
   - **Hérédité :** Soit $n \geq 2$ et supposons que $\mathscr{P}(n)$ est vraie. Si $n+1$ est premier alors cela coule de source. Sinon, $n+1$ est un nombre composé et s'écrit donc sous la forme $n+1 = xy$ où $1 < x \leq n$ et $1 < y \leq n$. Ainsi d'après l'hypothèse de la récurrence x et y sont produits de nombres premiers et donc leur produit $n+1$ l'est aussi. Ceci achève donc notre brave petite récurrence.

Passons maintenant à la belle démonstration d'Euclide. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers qu'on note $p_1, p_2, \ldots, p_n$. Soit N le nombre

$$N = p_1 p_2 \cdots p_n + 1.$$

D'après ce qui précède, $N > 1$ admet au moins un diviseur premier p. Je prétends alors que p est distinct de $p_1, p_2, \ldots, p_n$, ce qui conduira à une contradiction car on a supposé que $p_1, p_2, \ldots, p_n$ sont les seuls nombres premiers. En effet, si p était l'un des p_i il diviserait leur produit $p_1 p_2 \cdots p_n$. Par ailleurs, p divise N donc doit diviser la différence $N - p_1 p_2 \cdots p_n = 1$. Le nombre premier p divise donc 1, ce qui n'est pas. Cette contradiction implique donc qu'il existe une infinité de nombres premiers.

Tâchons maintenant de voir ce qui se passe expérimentalement avec la preuve euclidienne. On aimerait en effet évaluer le nombre N avec les premiers nombres premiers, d'où le tableau suivant.

N
$p_1 + 1 = 2 + 1 = 3$
$p_1 \cdot p_2 + 1 = 2 \times 3 + 1 = 7$
$p_1 \cdot p_2 \cdot p_3 + 1 = 2 \times 3 \times 5 + 1 = 31$
$p_1 \cdot p_2 \cdot p_3 \cdot p_4 + 1 = 2 \times 3 \times 5 \times 7 + 1 = 211$
$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 + 1 = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$
$\vdots$

On voit alors que les premiers nombres N générés par la formule d'Euclide sont premiers. Toutefois, la preuve d'Euclide dit tout simplement que N admet un diviseur premier. Euclide avait raison de ne pas considérer N comme premier car par exemple le nombre

$$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 + 1 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 59 \times 509$$

n'est pas premier. De même, si on va un peu plus loin, le nombre

$$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 \cdot p_7 + 1 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 + 1 = 19 \times 97 \times 277$$

n'est pas premier non plus. Trop beau pour être vrai. Bien que l'on sache qu'il en existe une infinité, il est très difficile de trouver des nombres premiers très grands. La quête des nombres premiers se poursuit toujours, non seulement parce qu'il s'agit d'un moyen de mesurer la puissance de nos ordinateurs mais aussi parce qu'ils sont très utiles en cryptographie. Avant de conclure ce paragraphe, notez le tour de force technique et psychologique dans la preuve d'Euclide. En effet, ce dernier prouve l'existence d'un nombre infini d'objets sans pouvoir tous les exhiber, ce qui était révolutionnaire pour son époque. D'où son élégance.

La formule d'Euclide ne produit pas que des nombres premiers et la question toute naturelle est : existe-t-il une formule générale relativement simple permettant de générer les nombres premiers ? L'expérimentation montre que l'existence d'une telle formule magique est très peu probable car on ne peut pas prédire la position des nombres premiers parmi les entiers naturels. S'il existe une formule simple générant le n—ième nombre premier p_n alors il existerait une formule simple permettant de trouver la différence entre deux nombres premiers consécutifs $p_{n+1} - p_n$. L'expérimentation là encore montre que cette différence est

extrêmement irrégulière et l'on peut la rendre aussi grande que l'on veut. En effet, pour tout entier $n \geq 2$, les $n-1$ nombres consécutifs

$$n!+2, \quad n!+3, \quad n!+4\ldots, \quad n!+n \quad \text{où } n! = 1\times 2\times 3\cdots\times n$$

sont tous composés (le premier est divisible par 2, le deuxième par 3 etc). Si on prend par exemple $n = 10000$ alors cette suite de nombres fournit 9999 nombres entiers consécutifs dont aucun n'est premier.

Malgré l'extrême difficulté de cette quête, nous n'allons tout de même pas l'abandonner à mi-chemin. Nous pouvons explorer de nouvelles idées et voir si cela permet d'aboutir à davantage de compréhension de nos supers nombres. Soit $\mathbb{P} = \{p_1, p_2, \ldots, p_n, \ldots\}$ la liste des nombres premiers et soit p [10]le nombre défini par

$$p = \sum_{k=1}^{+\infty} \frac{1}{10^{p_k}} = \frac{1}{10^{p_1}} + \frac{1}{10^{p_2}} + \cdots \frac{1}{10^{p_n}} + \cdots$$

Je vois que vous commencez à avoir peur. C'est tout à fait naturel mais il n'y a rien de bien compliqué dans cette somme. En effet, on a

$$\begin{aligned} p &= \sum_{k=1}^{+\infty} \frac{1}{10^{p_k}} \\ &= \frac{1}{10^{p_1}} + \frac{1}{10^{p_2}} + \cdots \frac{1}{10^{p_n}} + \cdots \\ &= \frac{1}{10^2} + \frac{1}{10^3} + \frac{1}{10^5} + \frac{1}{10^7} + \frac{1}{10^{11}} + \cdots \\ &= 0.01 + 0.001 + 0.00001 + 0.0000001 + 0.00000000001 + \cdots \\ &= 0.0110101000101000101\cdots \end{aligned}$$

On remarque alors que le développement décimal du nombre p indique la position des nombres premiers. En effet, sa première décimale vaut 0 ce qui signifie que 1 n'est pas premier, sa deuxième décimale vaut 1 indiquant que 2 est premier, sa troisième décimale vaut 1 aussi indiquant que 3 est premier, sa 4ème décimale vaut 0 ce qui signifie que 4 est un nombre composé etc. Notez alors que pour calculer notre nombre p, nous avons d'abord besoin de connaître les nombres premiers. Si on trouve un jour un autre moyen permettant de le calculer sans les nombres premiers, on gagnera au loto ! Mais pour l'instant, rien n'est gagné !

En 1640, Fermat a écrit à Mersenne autour d'une fameuse formule qui ne produit que des nombres premiers, à savoir la suite (F_n) définie pour tout $n \in \mathbb{N}$ par

$$F_n = 2^{2^n} + 1.$$

10. Pour les fous de l'analyse, ce nombre existe bien car la série de terme général $\frac{1}{10^{p_n}}$ est convergente. En effet, tous les termes de cette série sont positifs donc

$$\sum_{k=1}^{+\infty} \frac{1}{10^{p_k}} \leq \sum_{k=1}^{+\infty} \frac{1}{10^k} = \frac{1}{9}$$

Marin Mersenne

Malgré son génie, Fermat a pensé et à tort que les F_n sont tous premiers. Après une petite expérimentation, on obtient le tableau suivant

n	F_n
0	$2^{2^0}+1=3$
1	$2^{2^1}+1=5$
2	$2^{2^2}+1=17$
3	$2^{2^3}+1=257$
4	$2^{2^4}+1=65537$
$\vdots$	$\vdots$

Vous pouvez alors vérifier que les 5 premiers nombres F_n sont tous premiers, toutefois, Euler a prouvé avec une méthode ingénieuse que le nombre

$$F_5 = 2^{2^5}+1 = 2^{32}+1$$

est un multiple de 641. Pour reproduire cette preuve, nous utiliserons les congruences et il suffit de savoir pour la comprendre que le signe " $\equiv$ " se comporte grosso modo comme le signe " $=$ " (*) et que pour montrer que F_5 est divisible par 641 il suffit de montrer que

$$F_5 \equiv 0 \pmod{641}.$$

Ce résultat est équivalent à montrer que $2^{32}+1 \equiv 0 \pmod{641}$, ou encore à $2^{32} \equiv -1 \pmod{641}$ (par la remarque *). Pour se faire, d'abord on sait que $641 \equiv 0 \pmod{641}$ (car 641 divise 641). Puisque $641 = 640+1 = 5\times 2^7+1$, cela implique en particulier que

$$5\times 2^7+1 \equiv 0 \pmod{641},$$

ou encore que $5\times 2^7 \equiv -1 \pmod{641}$. De même par la remarque * on pourra élever cette "égalité" à la puissance 4 pour obtenir

$$5^4\times 2^{28} \equiv (-1)^4 \pmod{641} \equiv 1 \pmod{641}. \tag{1}$$

Par ailleurs l'égalité $641 = 625 + 16 = 5^4 + 2^4$ implique aussi que $5^4 + 2^4 \equiv 0 \pmod{641}$ ou encore que $5^4 \equiv -2^4 \pmod{641}$. Ainsi en remplaçant 5^4 par -2^4 dans la congruence (1) on obtient

$$-2^4 \times 2^{28} \equiv 1 \pmod{641},$$

ou encore $2^{32} \equiv -1 \pmod{641}$. Le résultat en découle et la question toute naturelle est d'où sort 641 à la base ? Est-ce le génie d'Euler ou alors une recette secrète utilisée par notre ancêtre ? Nous répondrons à cette question au bon moment ! Cette preuve semble un peu technique pour l'instant mais ce n'en est rien. Nous verrons que tout deviendra trivial quand on étudiera en détail les *congruences*. Depuis le temps d'Euler, les mathématiciens ont su démontrer que d'autres nombres de Fermat sont composés et l'on pourra vérifier que $F_6 = 2^{64} + 1$ est divisible par 274177. Notez alors que personne n'a trouvé encore un nombre de Fermat premier pour $n \geq 5$.

Dans la suite de cette section, nous donnons une deuxième preuve de l'infinité des nombres premiers utilisant les nombres de Fermat. Cette idée géniale est due au grand mathématicien hongrois George Pólya.

George Pólya

Pour se faire nous allons démontrer que les nombres de Fermats sont deux à deux premiers entre eux, ce qui signifie qu'ils n'ont aucun diviseur en commun plus grand que 1. Nous pouvons observer en effet l'identité suivante

$$F_0 F_1 F_2 \cdots F_n = F_{n+1} - 2.$$

Pas très évident tout ça allez-vous me dire ! En multipliant le membre de gauche de cette égalité par $2^{2^0} - 1 = 1$ on obtient

$$\begin{aligned}
\left(2^{2^0} - 1\right) F_0 F_1 F_2 \cdots F_n &= \left(2^{2^0} - 1\right)\left(2^{2^0} + 1\right) F_1 F_2 \cdots F_n \\
&= \left(\left(2^{2^0}\right)^2 - 1^2\right) F_1 F_2 \cdots F_n \\
&= \left(2^{2^1} - 1\right)\left(2^{2^1} + 1\right) F_2 \cdots F_n \\
&= \left(\left(2^{2^1}\right)^2 - 1^2\right) F_2 \cdots F_n \\
&\vdots \\
&= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\
&= 2^{2^{n+1}} - 1 \\
&= 2^{2^{n+1}} + 1 - 2 \\
&= F_{n+1} - 2.
\end{aligned}$$

J'avoue que c'est bien astucieux mais cette astuce est fort connue depuis le temps d'Euler, pour qui il s'agit d'une trivialité comparée à ses capacités algébriques. Je vous rappelle alors qu'on a établi cette identité afin de prouver que les nombres de Fermat sont deux à deux premiers entre eux. Soient en effet F_n et F_m deux nombres de Fermat tels que $m < n$ et soit d un diviseur positif en commun à F_n et F_m. On souhaite démontrer que $d = 1$. L'entier d doit diviser alors

$$F_n - (F_0 \cdots F_m \cdots F_{n-1}) = 2.$$

Ceci implique en particulier que $d \in \{1, 2\}$, d ne peut pas être égal à 2 car les F_n sont des nombres impairs. Le résultat en découle. Maintenant pour montrer qu'il existe une infinité de nombres premiers, il suffit de remarquer que chacun des F_n doit admettre au moins un diviseur premier et ce diviseur ne divise aucun des autres nombres de Fermat. Puisque les nombres de Fermat sont en nombre infini, les nombres premiers le sont aussi. Ingénieux, n'est ce pas ?

8 Le théorème de la division euclidienne

Avant d'aller plus loin, nous devons tout de même toucher un mot sur le théorème de la division euclidienne sur lequel repose toute l'arithmétique. Ce théorème (lui aussi intuitivement évident) est fort connu du grand public, puisqu'on l'a tous étudier à l'école primaire : il s'agit en effet de la division avec un quotient et un reste. Prenons donc quelques exemples afin de le bien cerner.

Exemple 1 : Le nombre 42 n'est pas divisible par 11. En effet,

$$11 \cdot 0 = 0, \quad 11 \cdot 1 = 11, \quad 11 \cdot 2 = 22, \quad 11 \cdot 3 = 33, \quad 11 \cdot 4 = 44.$$

On voit ainsi qu'il n'existe pas d'entier n tel que $11n = 42$. Le plus grand multiple de 11 en dessous de 42 est 33 et il reste donc 9 pour arriver à 42. Autrement dit $42 - 11 \cdot 3 = 9$ ou encore

$$42 = 11 \cdot 3 + 9.$$

Remarquez alors que 9 est plus petit entier positif parmi les entiers de la forme $42 - 11n$ et que $0 \leq 9 < 11$. Notez aussi que $q = 3$ est le seul entier tel que $42 - 11q = 9$ et qu'il n'existe pas d'autre entier $n \in \mathbb{Z}$ avec $r = 42 - 11n$ et $0 \leq r < 9$, puisque 9 est le plus petit entier vérifiant ces dernières inégalités.

Exemple 2 : Le nombre 57 n'est pas multiple de 13. Quel est donc le reste de la division euclidienne de 57 par 13 ? Pour répondre à cette question, on calcule mentalement le plus grand multiple de 13 en dessous de 57, qui est dans notre cas $13 \cdot 4 = 52$. Ainsi, le reste de la division euclidienne de 57 par 13 vaut $57 - 13 \cdot 4 = 5$. On écrit donc

$$57 = 13 \cdot 4 + 5.$$

Notez alors que pour trouver ce reste, on a parcouru mentalement tous les nombres r de la forme $r = 57 - 13 \cdot n$ jusqu'à ce qu'on tombe sur un r vérifiant les inégalités $0 \leq r < 13$, puisqu'ici on divise par 13.

Nous sommes maintenant prêt à énoncer le brave théorème de la division euclidienne et à le démontrer en généralisant les deux exemples précédents.

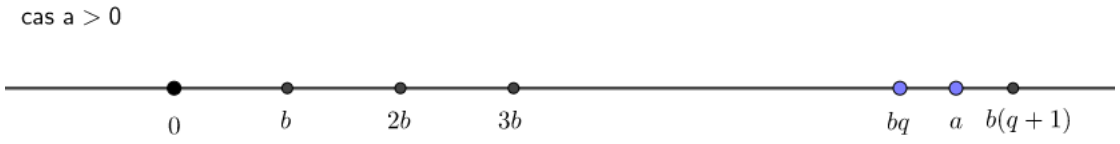
Théorème : Soient a et b deux entiers tels que $b > 0$. Il existe un unique couple (q, r) dans $\mathbb{Z}^2$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

- Montrons d'abord l'existence de q et r. Considérons l'ensemble

$$A = \{a - bm \geq 0 \mid m \in \mathbb{Z}\}$$

A est un sous-ensemble non vide de $\mathbb{N}$. En effet, si $a \geq 0$, il contient $a - b \times 0$. Sinon, il contient $a - ba$. Ainsi, d'après l'axiome du bon ordre il contient un plus petit élément. Appelons cet élément r. L'entier r vérifie alors l'égalité $r = a - bq$ pour un certain $q \in \mathbb{Z}$, par définition de A. De même, $r \geq 0$ par définition. Par ailleurs, $r < b$ car si $r \geq b$, alors $a - b(q+1) \in A$, ce qui est en contradiction avec le fait que r soit le plus petit élément de A.



- Montrons maintenant que (q, r) est unique. Soit (q', r') un deuxième couple de la division euclidienne de a par b. Alors $|r' - r| < b$ [11] et l'égalité $bq + r = bq' + r'$ implique que $b(q - q') = r' - r$. Au final, on obtient que que $|q - q'| < 1$, q et q' étant entiers, on en déduit que $q = q'$. Par conséquent $r = a - bq = a - bq' = r'$. D'où l'unicité.

Exemple 3 : Prenons un dernier exemple avec $a = -33 < 0$. Cet entier n'est pas multiple de 9 et l'on peut voir en cherchant le plus petit entier naturel r de la forme $r = -33 - 9 \cdot q$ qu'il s'agit de

$$3 = -33 - 9 \cdot (-4).$$

On en déduit donc que le quotient de la division euclidienne de -33 par 9 vaut $q = -4$ et son reste vaut $r = 4$.

9 L'algorithme d'Euclide pour calculer le pgcd

Nous avons vu dans ce qui précède que les nombres premiers constituent les éléments de base de l'arithmétique car tout entier plus grand que 2 est le produit de nombres premiers. Toutefois, nous verrons qu'il est difficile de décider si un nombre est premier ou composé et qu'il est encore plus difficile de trouver les diviseurs premiers d'un entier $n \geq 2$. Au lieu donc de s'intéresser aux diviseurs positifs d'un entier, il est plus fructueux de s'intéresser aux diviseurs en commun à deux entiers a et b. Dans *Le livre 7* des *Éléments*, Euclide a décrit une manière très efficace permettant de calculer le **pgcd** de deux entiers a et b. Je vous rappelle que le mot pgcd(a, b) signifie *le plus grand commun diviseur entre a et b*. Avant

11. Si $0 \leq r < b$ et $0 \leq r' < b$ alors l'écart entre r et r', à savoir $|r' - r|$ est strictement plus petit que b (faites un dessin pour vous en convaincre).

de vous décrire l'algorithme ingénieux d'Euclide, prenons un exemple rapide permettant de comprendre le pgcd.

Exemple : Le pgcd de 70 et 42 vaut 14. En effet, les décompositions en facteurs premiers de 70 et de 42 sont

$$70 = 2 \cdot 5 \cdot 7 \quad \text{et} \quad 42 = 2 \cdot 3 \cdot 7.$$

On voit ainsi que les diviseurs premiers en commun entre 70 et 42 sont 2 et 7. Par conséquent

$$\text{pgcd}(70, 42) = 2 \cdot 7 = 14.$$

Cette méthode fonctionne bien quand il s'agit de calculer le pgcd de nombres petits en taille. Toutefois, trouver la factorisation d'un nombre très grand est un problème réputé difficile et très coûteux en temps. L'algorithme d'Euclide contourne cette difficulté et permet de calculer le pgcd de façon très efficace [12].

9.1 Le pgcd avec soustraction

Nous décrivons dans ce paragraphe l'algorithme d'Euclide avec soustraction. On généralisera par la suite cette idée avec la division euclidienne qui permettra d'avoir un procédé bien plus rapide. Pour calculer le pgcd de deux entiers a et b non tous les deux nuls tels que $a \geq b$, il suffit de remarquer que

$$\text{pgcd}(a, b) = \text{pgcd}(b, a - b).$$

Cette égalité découle du fait que les diviseurs en commun de a et b et ceux de b et $a - b$ sont les mêmes. Pour s'en convaincre, soit d un diviseur en commun entre a et b. Dans ce cas, on écrit $a = a'd$ et $b = b'd$ et par conséquent

$$a - b = a'd - b'd = d(a' - b').$$

Ainsi d divise $a - b$. Réciproquement si d divise b et $a - b$ alors d doit diviser leur somme $b + a - b = a$ (appliquer le même raisonnement si vous n'êtes pas convaincus). Maintenant pour calculer le pgcd, il suffit de réitérer la soustraction afin de tomber sur ce qu'il faut. Un exemple vaut toujours mieux qu'un long discours.

Exemple 1 : Pour les raisons évidentes, on notera (a, b) pour désigner le pgcd de a et b. On souhaite ici calculer $(70, 42)$, mais cette fois-ci avec la remarque euclidienne. Nous avons en effet

$$\begin{aligned}
(70, 42) &= (42, 70 - 42) \\
&= (42, 28) \\
&= (28, 42 - 28) \\
&= (28, 14) \\
&= (14, 28 - 14) \\
&= (14, 14) \\
&= (14, 14 - 14) \\
&= (14, 0) = 14.
\end{aligned}$$

12. On comprendra cette histoire d'efficacité quand on parlera de complexité algorithmique.

Bingo ! On réitérant le procédé de la soustraction on tombe sur le pgcd de 14 et 0. Or de façon générale si $a > 0$ alors

$$(a, 0) = a.$$

Voyez-vous pourquoi ? Cela permet en tout cas d'affirmer que $(14, 0) = 14$.

Exemple 2 : Prenons un deuxième exemple pour se fixer les idées. On souhaite calculer ici le pgcd de 42 et 30. En réitérant les soustractions euclidiennes on obtient

$$\begin{aligned}(42, 30) &= (30, 42-30)\\ &= (30, 12)\\ &= (12, 30-12)\\ &= (12, 18)\\ &= (18, 18-12)\\ &= (18, 6)\\ &= (6, 12)\\ &= (6, 6)\\ &= (6, 0) = 6\end{aligned}$$

Ainsi le pgcd de 42 et 30 vaut 6. On voit alors que ce procédé donne toujours à la fin $(a, 0)$. Cela résulte du fait que l'algorithme d'Euclide produit une suite de nombres entiers naturels décroissante, d'après le principe de la descente infinie de Fermat, cette suite doit bien s'arrêter à un moment donné (à méditer).

9.2 Le pgcd avec division

On peut améliorer l'algorithme d'Euclide avec soustraction en utilisant la division euclidienne. La propriété fondamentale qui permet de faire cela est : si r est le reste de la division euclidienne de a par b alors

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

La preuve de cette égalité est une adaptation de celle avec soustraction (à faire seul du coup). Reprenons ensemble l'exemple 2 mais cette fois avec la division euclidienne. En effet,

$$\begin{aligned}42 = 30 \cdot 1 + 12 &\implies (42, 30) = (30, 12)\\ 30 = 12 \cdot 2 + 6 &\implies (30, 12) = (12, 6)\\ 12 = 6 \cdot 2 + 0 &\implies (12, 6) = (6, 0) = 6.\end{aligned}$$

Pas besoin donc de vous convaincre de la rapidité du procédé avec la division euclidienne. Prenons un deuxième exemple (toujours pour se fixer les idées, je vous invite toutefois à en prendre davantage pour bien comprendre l'algorithme).

Exemple : On souhaite calculer le pgcd de 858 et 770. On commence donc par effectuer la division euclidienne de 858 et 770 et on réitère ensuite la même opération. On obtient ainsi

$$\begin{aligned}858 = 770 \cdot 1 + 88 &\implies (858, 770) = (770, 88)\\ 770 = 88 \cdot 8 + 66 &\implies (770, 88) = (88, 66)\\ 88 = 66 \cdot 1 + 22 &\implies (88, 66) = (66, 22)\\ 66 = 22 \cdot 3 + 0 &\implies (66, 22) = (22, 0).\end{aligned}$$

On voit ainsi que $(858, 770) = 22$ et que le procédé se termine en seulement 4 étapes. Bon courage pour le faire avec la soustraction. Je suis souvent assez curieux, je vous ai donc écrit les deux algorithmes avec Python afin de pouvoir faire la comparaison [13].

```
def pgcd_div(a,b):
    i = 0
    while b != 0:
        a, b = b, a%b
        i += 1
    return a, i

def pgcd_sous(a,b):
    i = 0
    while b != 0:
        if a > b :
            a, b = b, (a - b)
            i += 1
        else:
            a, b = b, a
            a, b = b, (a - b)
            i += 1
    return a, i
```

Le compteur i dans chacun des algorithmes permettra de compter le nombre d'itérations effectuées par le programme afin de calculer le pgcd. En exécutant les deux programmes avec $a = 858$ et $b = 770$ on obtient le résultat suivant.

```
>>> pgcd_div(858, 770)
(22, 4)
>>> pgcd_sous(858, 770)
(22, 13)
```

Ainsi on obtient bien ce qu'on a obtenu à la main, à savoir que le pgcd de 858 et 770 vaut 22, l'algorithme de la division euclidienne s'en sort en 4 étapes tandis que celui avec la soustraction en effectue 13, beaucoup trop ! Je vous invite à aller sur Python afin de faire la comparaison par vous même.

10 L'identité de Bézout et quelques conséquences

Nous passons maintenant à une conséquence importante de l'algorithme d'Euclide. On peut en effet exprimer le pgcd de a et b comme combinaison linéaire de ces deux entiers. En d'autres mots, l'algorithme d'Euclide nous permettra de trouver deux entiers u et v tels que

$$(a, b) = a \cdot u + b \cdot v.$$

Cette identité importante s'appelle l'identité de Bézout, due comme son nom l'indique au mathématicien français Étienne Bézout (ne pas confondre avec Bisous hein !). Un exemple parle toujours bien mieux qu'un long discours.

Exemple 1 : Afin de calculer le pgcd de 42 et 30 nous avons effectué les divisions euclidiennes successives suivantes

$$\begin{aligned} 42 &= 30 \cdot 1 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

13. Eh oui les copains, il est grand temps d'apprendre à programmer.

Ainsi le pgcd de 42 et 30 est le dernier reste non nul de cette suite d'opérations. On peut alors remonter ce procédé afin d'exprimer 6 en fonction de 42 et 30. En effet,

$$\begin{aligned} 6 &= 30 - 12 \cdot 2 \\ &= 30 - (42 - 30 \cdot 1) \cdot 2 \quad \text{car } 12 = 42 - 30 \cdot 1 \\ &= 30 - 42 \cdot 2 + 30 \cdot 2 \\ &= 30 \cdot 3 - 42 \cdot 2 \\ &= 30 \cdot 3 + 42 \cdot (-2). \end{aligned}$$

On a donc réussi à exprimer 6 sous la forme $6 = 42 \cdot u + 30 \cdot v$, où ici $u = -2$ et $v = 3$.

Étienne Bézout

Exemple 2 : Reprenons l'exemple avec $a = 858$ et $b = 770$. La suite des divisions euclidiennes est

$$\begin{aligned} 858 &= 770 \cdot 1 + 88 \\ 770 &= 88 \cdot 8 + 66 \\ 88 &= 66 \cdot 1 + 22 \\ 66 &= 22 \cdot 3 + 0. \end{aligned}$$

Là encore le pgcd de 858 et 770 est le dernier reste non nul de cette suite d'opérations. De même, pour trouver u et v tels que $22 = 858u + 770v$, il suffit de remonter ce procédé. En effet,

$$\begin{aligned} 22 &= 88 - 66 \cdot 1 \\ &= 88 - (770 - 88 \cdot 8) \cdot 1 \\ &= 88 \cdot 9 - 770 \cdot 1 \\ &= (858 - 770 \cdot 1) \cdot 9 - 770 \cdot 1 \\ &= 858 \cdot 9 - 770 \cdot 10 \end{aligned}$$

Ainsi $u = 9$ et $v = -10$. Je sens que vous n'êtes pas convaincus. Rien ne vous empêche de vérifier ce calcul pour voir que

$$858 \cdot 9 - 770 \cdot 10 = 7722 - 7700 = 22.$$

Bingo ! Remonter les opérations de l'algorithme d'Euclide s'appelle l'algorithme d'Euclide *étendu*. Notre objectif maintenant est de pouvoir programmer cet algorithme avec Python

et pour se faire, on doit écrire les choses de façon plus formelle.

On aimerait en effet décrire la suite des restes (r_n) obtenus en exécutant l'algorithme d'Euclide. Pour des raisons pratiques, nous prenons $r_0 = a$ et $r_1 = b$. L'algorithme d'Euclide consiste alors à effectuer d'abord la division euclidienne de r_0 par r_1 pour obtenir la relation

$$r_0 = r_1 \cdot q_1 + r_2.$$

La deuxième étape consiste à diviser r_1 par r_2 pour obtenir le reste r_3 vérifiant la relation

$$r_1 = r_2 \cdot q_2 + r_3.$$

La troisième étape de notre fameux algorithme consiste à faire la même chose avec r_2 et r_3, ce qui permettra d'obtenir un nouveau reste r_4 vérifiant la relation

$$r_2 = r_3 \cdot q_3 + r_4.$$

On répète alors ce même procédé jusqu'à ce qu'on obtienne les relations

$$\begin{aligned} r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n \\ r_{n-1} &= r_n \cdot q_n + 0, \end{aligned}$$

où $r_n \neq 0$ désigne le dernier reste non nul. Cela signifie en particulier que r_n est le pgcd tant recherché. Je vous rappelle donc qu'on aimerait écrire r_n en fonction de r_0 et r_1, sous la forme $r_n = r_0 \cdot u + r_1 \cdot v$. Tout d'abord la relation $r_0 = r_1 q_1 + r_2$ implique que $r_2 = r_0 - r_1 q_1$(*). On voit ainsi que r_2 s'écrit comme combinaison de r_0 et r_1. Maintenant la relation $r_1 = r_2 q_2 + r_3$ combinée avec la relation (*) donne

$$\begin{aligned} r_3 &= r_1 - r_2 q_2 \\ &= r_1 - (r_0 - r_1 q_1) q_2 \\ &= r_1(1 + q_1 q_2) - r_0 q_2. \end{aligned}$$

Là encore on voit qu'on peut exprimer r_3 comme combinaison de r_0 et r_1. On effectue la même opération avec r_4 pour obtenir deux entiers u_4 et v_4 tels que $r_4 = r_0 u_4 + r_1 v_4$. On voit alors que plus généralement, le reste r_k s'écrit sous la forme

$$r_k = r_0 u_k + r_1 v_k.$$

Comment cela va-t-il nous aider à programmer notre algorithme ? Pas très évident pour l'instant mais remarquez que l'opération permettant de passer de r_2 à r_3 et ensuite de r_3 à r_4 est essentiellement la même. Cela suggère qu'il existe une relation de récurrence entre u_k et u_{k+1} et entre v_k et v_{k+1}. Regardons ensemble ce que cela donne : on aura besoin des relations suivantes

$$\begin{aligned} r_{k-1} &= r_0 u_{k-1} + r_1 v_{k-1} \\ r_k &= r_0 u_k + r_1 v_k. \end{aligned}$$

On aimerait donc à partir de ces deux relations déduire $r_{k+1} = r_0 u_{k+1} + r_1 v_{k+1}$. En effet, on sait que r_{k-1}, r_k et r_{k+1} sont liés par la relation $r_{k-1} = r_k q_k + r_{k+1}$, ce qui donne que

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k \\ &= r_0 u_{k-1} + r_1 v_{k-1} - (r_0 u_k + r_1 v_k) q_k \\ &= r_0(u_{k-1} - u_k q_k) + r_1(v_{k-1} - v_k q_k). \end{aligned}$$

On obtient ainsi deux suites (u_k) et (v_k) définies par les relations

$$u_{k+1} = u_{k-1} - u_k q_k \quad \text{et} \quad v_{k+1} = v_{k-1} - v_k q_k.$$

On voit alors qu'elles sont définies par la même relation de récurrence. Toutefois, elles ne donneront pas les mêmes nombres pour une raison d'initialisation. En effet, on sait que $r_0 = r_0 u_0 + r_1 v_0$ ce qui suggère de prendre $u_0 = 1$ et $v_0 = 0$. Par ailleurs $r_1 = r_0 u_1 + r_1 v_1$ ce qui donne donc $u_1 = 0$ et $v_1 = 1$. Prenons un exemple pour comprendre ce qui se passe.

Exemple 3 : On souhaite exprimer ici $6 = (42, 30)$ en fonction de 42 et 30. La suite (u_k) est définie par $u_0 = 1$, $u_1 = 0$ et $u_{k+1} = u_{k-1} - u_k q_k$. De même, la suite (v_k) est définie par $v_0 = 0$, $v_1 = 1$ et $v_{k+1} = v_{k-1} - v_k q_k$. En appliquant d'abord l'algorithme d'Euclide on obtient les divisions successives suivantes

$$\begin{aligned} 42 &= 30 \cdot 1 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 + 0. \end{aligned}$$

On en déduit que $q_1 = 1$ et $q_2 = 2$. Ainsi en utilisant les formules générant (u_k) et (v_k) on obtient

k	q_k	u_k	v_k
0	-	1	0
1	1	0	1
2	2	1	-1
3	-	-2	3

Dans notre cas le dernier reste non nul est r_3 et d'après notre tableau on a $u_3 = -2$ et $v_3 = 3$. Cela implique en particulier que

$$6 = r_3 = r_0 u_3 + r_1 v_3 = 42 \cdot (-2) + 30 \cdot 3.$$

Incroyable, c'est bien la relation obtenue à la main. Je vous invite à appliquer cette méthode avec davantage d'exemples afin de comprendre son fonctionnement. Nous sommes enfin prêts à programmer cette méthode avec Python. Il suffit de savoir programmer une suite récurrente d'ordre 2 (avec deux valeurs initiales). On obtient donc

```
def bezout(a,b):
    u = 1 ; uu = 0
    v = 0 ; vv = 1
    while b != 0:
        q = a // b
        a, b = b, (a % b)
        uu, u = u - q*uu , uu
        vv, v = v - q*vv , vv
    return (a, u, v)
```

En exécutant cet algorithme avec $a = 42$ et $b = 30$ on obtient bien

```
>>> bezout(42, 30)
(6, -2, 3)
>>>
```

Pour récapituler donc, le théorème de Bézout affirme que le pgcd de deux nombres entiers a et b non tous les deux nuls, peut s'écrire comme combinaison de a et de b. En d'autres termes, il existe deux entiers u et v tels que

$$(a,b) = a \cdot u + b \cdot v.$$

Ce théorème sera d'une grande importance pour la suite de notre aventure.

Deux conséquences de l'identité de Bézout :

On décrit dans ce paragraphe quelques conséquences importantes de notre si chère identité de Bézout.

Conséquence 1 : Par définition du pgcd, il s'agit du plus grand diviseur en commun entre deux entiers a et b. En d'autres mots, si r est un diviseur de a et de b alors $r \leq (a,b)$. En réalité, il existe une relation plus forte entre un tel r et le pgcd et l'on peut affirmer que non seulement r est plus petit que le pgcd mais aussi qu'il le divise. Notez alors que le pgcd est plus grand diviseur au sens de la divisibilité, c'est à dire si r divise a et b alors r divise le pgcd. Nous allons utiliser l'identité de Bézout afin de démontrer proprement et convenablement ce résultat, relativement évident intuitivement. Le pgcd de a et b s'écrit sous la forme $(a,b) = a \cdot u + b \cdot v$. Si r est un diviseur en commun à a et b alors on peut écrire $a = r \cdot a'$ et $b = r \cdot b'$. Cela implique donc que

$$\begin{aligned}(a,b) &= a \cdot u + b \cdot v \\ &= r \cdot a' \cdot u + r \cdot b' \cdot v \\ &= r(a'u + b'v).\end{aligned}$$

Le résultat en découle. Remarquez alors qu'on a utilisé à plusieurs reprises dans notre exposé que si a divise b et c alors a divise toute combinaison de b et c de la forme $\alpha b + \beta c$. Modulo ce petit résultat, on aurait pu tout simplement dire que puisque (a,b) est combinaison de a et b alors tout diviseur de a et de b doit diviser son pgcd. Dorénavant, nous utiliserons cette histoire de combinaison sans passer par sa démonstration.

Conséquence 2 : Venons-en maintenant au fameux **Lemme de Gauss**, dû au grand génie [14] *Carl Friedrich Gauss*.

Carl Friedrich Gauss

14. Ce résultat n'est qu'une trivialité comparé aux grands travaux réalisés par son excellence Gauss.

Tout d'abord, je vous rappelle qu'on dit que a et b sont **premiers entre eux** s'ils n'ont aucun diviseur positif en commun sauf 1. Cela revient à dire que le pgcd de a et b vaut $(a,b)=1$ (pourquoi ?). Le lemme de Gauss affirme alors que si a divise $b\cdot c$ et si de plus $(a,b)=1$ alors a doit diviser c. Cela semble aussi intuitivement évident puisque si a et b ne partage aucun diviseur en commun sauf 1 et que a divise le produit bc alors a n'a pas le choix que de diviser c. Toutefois, afin d'éviter les dérapages [15], tout nécessite une démonstration correcte en mathématiques. En effet, $(a,b)=1$ implique d'après l'identité de Bézout l'existence de deux entiers u et v tels que

$$1=a\cdot u+b\cdot v.$$

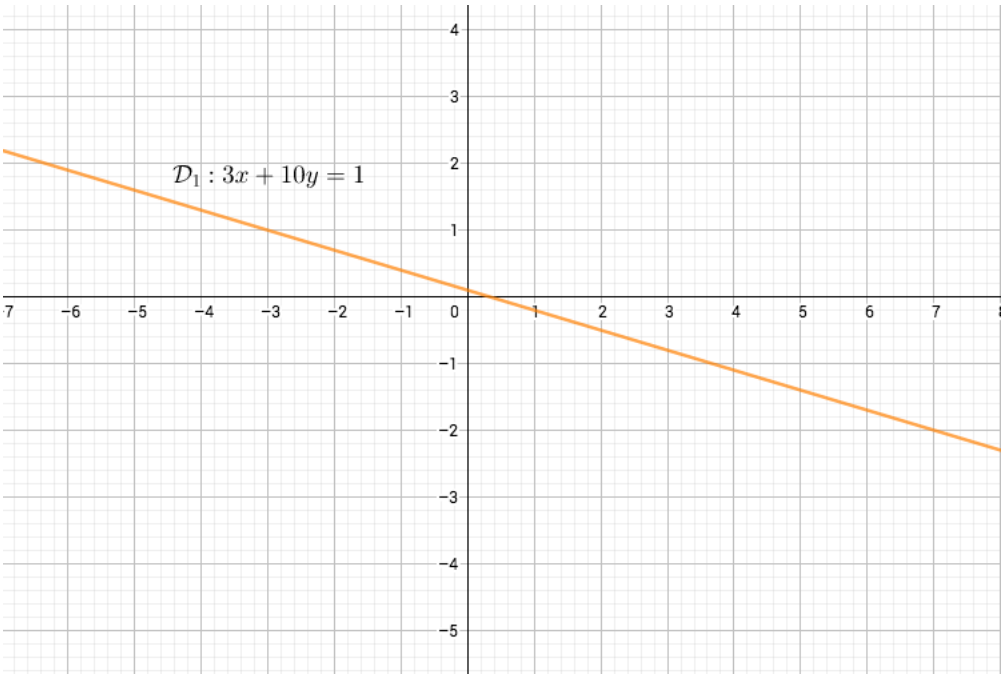
En multipliant cette égalité par c, on obtient $c=c\cdot a\cdot u+(c\cdot b)\cdot v$. Or a divise bc donc a divise c car il divise aussi $c\cdot a\cdot u$.

11 Applications

Nous donnons dans cette section deux applications fondamentales de nos résultats précédents.

11.1 Retour sur les points à coordonnées entières sur une droite

Nous avons vu au début de notre cours que la droite d'équation $3x+10y=1$ contient des points à coordonnées entières comme par exemple le point de coordonnées $(-3,1)$, ou encore le point $(7,-2)$.



En réalité, il existe une infinité de points à coordonnées entières habitant sur cette droite et ils sont de la forme

$$(10k-3,-3k+1).$$

15. Personne n'est à l'abri de déraper mathématiquement, même de très grands mathématiciens.

Nous nous sommes alors demandés si tous les points entiers étaient de cette forme et nous pouvons maintenant répondre à cette question. En effet, $(-3,1)$ est un point sur notre droite et si (x,y) est un point à coordonnées entières situé sur cette même droite alors

$$\begin{cases} 3x+10y & =1 \\ 3\cdot(-3)+10\cdot 1 & =1 \end{cases}$$

On soustrait alors la deuxième équation à la première pour obtenir $3(x+3)+10(y-1)=0$ ou encore

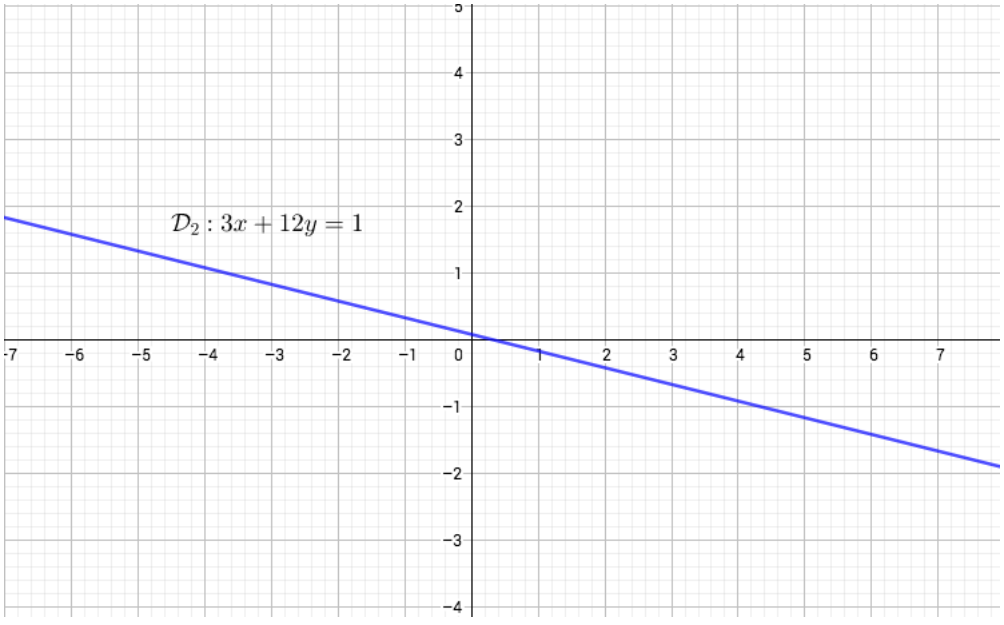
$$3(x+3)=10(1-y).$$

Puisque tout se passe dans $\mathbb{Z}$, cette égalité implique que 3 divise $10(1-y)$. Or 3 et 10 sont premiers entre eux, donc d'après le lemme de notre bon vieux Gauss 3 doit diviser $1-y$. Autrement dit, il existe un entier k tel que $1-y=3k$, ce qui signifie que $y=-3k+1$! Oh, incroyable ! Maintenant l'égalité $3(x+3)=10(1-y)$ devient

$$3(x+3)=10\cdot 3k,$$

en simplifiant par 3 de part et d'autre on obtient $x=10k-3$, qui est la forme voulue pour x. Pour conclure, nous sommes partis d'un couple $(x,y)\in\mathbb{Z}^2$ solution de $3x+10y=1$ et nous avons montré qu'il est forcément de la forme $(10k-3,-3k+1)$. D'où la réponse à notre question, toutefois une deuxième question me saute aux yeux personnellement (j'espère que c'est le cas pour vous aussi). Nous avons en effet utiliser la solution particulière $(-3,1)$ pour résoudre totalement notre équation mais comment trouver une solution particulière à n'importe quelle équation du type $ax+by=c$ et est-ce toujours possible ?

Nous avons vu ensemble que la droite d'équation $3x+12y=1$ n'abrite aucun point à coordonnées entières car dans ce cas on obtient l'égalité $3(x+4y)=1$ ce qui signifie que 3 divise 1, contradiction.



Plus généralement, une équation de la forme $ax+by=c$ admet une solution entière si et seulement si le pgcd de a et b divise c. En effet, le sens direct est relativement évident car si (x_0,y_0) est une solution entière de notre équation alors $ax_0+by_0=c$. Puisque le

pgcd de a et b divise a et b, il divise toute combinaison linéaire de ces deux entiers, en particulier l'entier c. Réciproquement, si (a,b) divise c alors l'équation $ax+by=c$ admet une solution entière. En effet, d'après Bézout on peut toujours trouver deux entiers u et v tels que $(a,b)=a\cdot u+b\cdot v$. Ainsi puisque (a,b) divise c, on peut écrire $c=c'\cdot(a,b)$, donc en multipliant par c' on obtient

$$\begin{aligned} c=c'(a,b) &= c'au+c'bv \\ &= a(c'u)+b(c'v). \end{aligned}$$

On en déduit donc que le couple $(c'u,c'v)$ est solution entière de l'équation $ax+by=c$. Le tout repose donc sur l'algorithme d'Euclide étendu qui permet de trouver les nombres u et v. Sans perte de généralité, nous pouvons supposer $(a,b)=1$ [16]. Dans ce cas, quand on obtient un point particulier (x_0,y_0) sur la droite d'équation $ax+by=c$, on obtient les autres points de la façon suivante. Si (x,y) est un point à coordonnées entières habitant la droite, alors

$$\begin{cases} ax+by &= c \\ ax_0+by_0 &= c \end{cases}$$

On soustrait la deuxième équation de la première pour obtenir $a(x-x_0)+b(y-y_0)=0$, autrement

$$a(x-x_0)=b(y_0-y).$$

Là encore puisque cette égalité se passe dans $\mathbb{Z}$, a divise $b(y_0-y)$. Or a et b sont premiers entre eux car $(a,b)=1$, le lemme de Gauss implique du coup que a divise y_0-y, d'où l'existence d'un entier k tel que $y_0-y=a\cdot k$ ou encore que $y=-a\cdot k+y_0$. L'égalité $a(x-x_0)=b(y_0-y)$ implique alors que

$$a(x-x_0)=b\cdot ak,$$

donc en simplifiant par a, $x=bk+x_0$. Ainsi les solutions de l'équation $ax+by=c$ doivent être de la forme

$$(x_0+bk,y_0-ak), \quad \text{où } k\in\mathbb{Z}.$$

Réciproquement, on voit bien que

$$\begin{aligned} a(x_0+bk)+b(y_0-ak) &= ax_0+by_0+abk-abk \\ &= c. \end{aligned}$$

Voilà donc pour la théorie, prenons maintenant un exemple concret.

Exemple : On souhaite résoudre dans $\mathbb{Z}^2$ l'équation $25x+13y=3$. Les entiers 25 et 13 n'ont aucun diviseur positif en commun sauf 1 donc $(25,13)=1$, or 1 divise 3 donc d'après ce qui précède notre équation admet une solution particulière et par conséquent une infinité de solution. Commençons d'abord par exprimer $(25,13)$ en fonction de 25 et 13. La suite des opérations de l'algorithme d'Euclide est

$$\begin{aligned} 25 &= 13\cdot 1+12 \\ 13 &= 12\cdot 1+1 \\ 12 &= 1\cdot 12+0 \end{aligned}$$

16. Dans le cas contraire, on divise l'équation par (a,b).

Ainsi en remontant ces opérations on obtient

$$\begin{aligned} 1 &= 13 - 12 \cdot 1 \\ &= 13 - (25 - 13 \cdot 1) \cdot 1 \\ &= 13 \cdot 2 + 25 \cdot (-1). \end{aligned}$$

En multipliant par 3 on obtient $25 \cdot (-3) + 13 \cdot 6 = 3$, ce qui nous donne $(-3, 6)$ comme solution particulière de notre équation $25x + 13y = 3$. D'après notre petite théorie, les autres solutions sont de la forme

$$(-3 + 13k, 6 - 25k), \quad \text{où } k \in \mathbb{Z}.$$

11.2 Racines rationnelles d'un polynôme

11.2.1 Ensembles de nombres et racines de polynômes

Le premier ensemble de nombres que l'on rencontre dans la nature et en arithmétique est l'ensemble des entiers naturels

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}.$$

Les entiers naturels servent essentiellement à compter les objets. Toutefois, pour nos utilisations mathématiques, on se heurte très rapidement à des difficultés conceptuelles en travaillant uniquement dans $\mathbb{N}$. Par exemple l'équation

$$2 + x = 5$$

admet une solution dans $\mathbb{N}$, à savoir $x = 3$. Néanmoins, l'équation $5 + x = 2$, semblable à la première n'admet pas de solution dans $\mathbb{N}$, pour la simple raison, qu'en travaillant chez les entiers naturels $5 + x \geq 5$ et donc ne pourra jamais atteindre 2. Nous avons donc besoin d'un ensemble plus grand que $\mathbb{N}$, celui des entiers relatifs qu'on dénote

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\},$$

où la lettre $\mathbb{Z}$ fait référence ici au mot *Zahlen*, signifiant nombres en allemand. L'équation $5 + x = 2$ devient alors résoluble dans $\mathbb{Z}$ et sa solution vaut $x = -3$. Toutefois, l'équation $2x = 4$ admet une solution dans $\mathbb{Z}$ mais l'équation similaire $4x = 2$ n'en admet pas. Nous avons donc besoin de construire un ensemble de nombres plus grand que $\mathbb{Z}$, à savoir cette fois-ci l'ensemble des nombres rationnels (les fractions)

$$\mathbb{Q} = \left\{ \frac{p}{q}, (p, q) \in \mathbb{Z} \times \mathbb{N}^* \right\}.$$

L'ensemble $\mathbb{Q}$ suffit-il alors pour résoudre toute équation à coefficients entiers ? L'équation $x^2 = 2$ est à coefficients entiers et pourtant elle n'admet pas de solutions dans $\mathbb{Q}$, puisqu'on a vu ensemble que $\sqrt{2}$ n'est pas un nombre rationnel. On aimerait alors étendre $\mathbb{Q}$ à un ensemble plus grand permettant de résoudre par exemple les équations du type $x^2 = a$.

Pour ce faire, nous allons utiliser le développement décimal d'un nombre. Le développement décimale d'une fraction est toujours périodique, mais mieux encore tout nombre avec un développement décimal périodique est forcément une fraction. Par exemple,

$$\frac{3}{7} = 0.428571\ 428571\ 428571 \cdots$$

on voit aisément que $3/7$ admet un développement décimal périodique et que plus généralement le développement décimale de n'importe quelle fraction est périodique à partir d'un certain rang (pourquoi ?). Réciproquement, tout nombre dont le développement décimal est périodique à partir d'un certain rang est une fraction. Regardons ensemble ce qui se passe sur un exemple. Soit x le nombre

$$x = 0.12345\ 345\ 345\ldots.$$

En multipliant x par 10^2 on obtient

$$10^2 x = 12.345\ 345\ 345\ldots.$$

De même, en le multipliant par 10^5 on obtient $10^5 x = 12345.345\ 345\ldots$. L'égalité

$$(10^5 - 10^2)x = 12345 - 12$$

en découle et il s'en suit donc que x est une fraction égale à $12333/99900$. Ce procédé se généralise bien facilement et notre réciproque tombe ainsi comme une pomme mûre. Notez alors que les premières décimales de $\sqrt{2}$ sont

$$\sqrt{2} = 1.41421356237309504880168872420969807856967187537694807317667 9\cdots$$

et que a priori ce développement n'est pas périodique. En réalité il ne peut pas l'être car on a montré que $\sqrt{2}$ ne s'écrit pas sous la forme d'une fraction et que seules les fractions admettent cette propriété.

Cette remarque suggère une idée d'une possible extension de $\mathbb{Q}$. Puisque ce dernier est l'ensemble des nombres dont le développement décimal est périodique à partir d'un certain rang, il suffit de prendre de façon informelle l'ensemble de tous les développements décimaux possibles. On obtient ainsi

$$\mathbb{R} = \text{ensemble de tous les développements décimaux.}$$

L'ensemble des nombres réels permet donc de résoudre davantage d'équations, même à coefficients réels. On sait par exemple que si $\Delta = b^2 - 4ac \geq 0$, l'équation générale

$$ax^2 + bx + c = 0, \quad \text{où } a \neq 0,$$

admet deux solutions (comptées avec multiplicité), à savoir $x_{1,2} = (-b \pm \sqrt{\Delta})/2a$. On se demande alors très naturellement si maintenant toutes les équations à coefficients réels admettent des solutions dans $\mathbb{R}$. Vous n'êtes pas sans savoir que l'équation $x^2+1 = 0$ n'admet pas de solution réelle, car dans $\mathbb{R}$, $x^2 + 1 \geq 1$ et donc n'atteint jamais 0. Nous avons là encore besoin de créer de façon un peu artificielle un ensemble de nombres contenant $\mathbb{R}$ et un nombre imaginaire i vérifiant

$$i^2 = -1.$$

Autrement dit, on considère un nombre i solution de l'équation $x^2 + 1 = 0$. On obtient à partir de là l'ensemble des nombres complexes $\mathbb{C}$. Nous avons ainsi introduit plusieurs ensembles de nombres tels que

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

afin de pouvoir résoudre davantage d'équations. Mais ce procédé s'arrêtera-t-il un jour ? Ou doit-on encore construire un ensemble plus grand que $\mathbb{C}$ contenant des racines d'équations à coefficients dans $\mathbb{C}$. Aussi surprenant que cela puisse paraître, $\mathbb{C}$ contient les racines de n'importe quelle équation à coefficients dans cet ensemble ! Et donc on n'a plus besoin d'élargir nos ensembles afin de résoudre nos équations. Ce fameux théorème s'appelle le **théorème fondamental de l'algèbre** et il dit que tout polynôme non constant à coefficients dans $\mathbb{C}$ admet une racine dans $\mathbb{C}$. On dit alors que $\mathbb{C}$ est algébriquement clos. La preuve de ce théorème dépasse un peu le cadre de notre cours.

11.2.2 Racines entières et rationnelles d'un polynôme

Dans la suite nous nous intéressons aux ensembles $\mathbb{Z}$ et $\mathbb{Q}$. Nous souhaitons trouver les solutions entières du polynôme

$$P(x) = 3x^3 - 11x^2 - 24x + 20.$$

Si $n \in \mathbb{Z}$ tel que $P(n) = 0$ alors on peut affirmer que

$$n(3n^2 - 11n - 24) = -20.$$

Puisque tout se passe dans $\mathbb{Z}$, cela signifie que si n est racine de P alors n doit diviser (-20) ou encore que

$$n \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$$

Il s'agit donc d'essayer un nombre fini de valeurs pour voir si l'une d'entre elles est solution de notre équation. Après plusieurs essais, on voit que les solutions de P habitant dans $\mathbb{Z}$ sont (-2) et 5. Or P est de degré 3, donc il doit admettre une troisième solution, possiblement vivant dans $\mathbb{Q}$. Soit donc $r = p/q \in \mathbb{Q}$ tel que $P(r) = 0$ et $(p, q) = 1$. Cette dernière égalité s'écrit

$$3\left(\frac{p}{q}\right)^3 - 11\left(\frac{p}{q}\right)^2 - 24\left(\frac{p}{q}\right) + 20 = 0.$$

On obtient donc en multipliant par q^3 l'égalité dans $\mathbb{Z}$, $3p^3 - 11p^2q - 24pq^2 + 20q^3 = 0$. Par conséquent

$$p(3p^2 - 11pq - 24q^2) = -20q^3 \quad \text{et} \quad q(20q^2 - 24pq - 11p^2) = -3p^3.$$

Ceci signifie que p divise $-20q^3$ et q divise $-3p^3$. Je prétends que c'est quasiment fini puisque d'après le lemme de Gauss p doit diviser -20 et q doit de son côté diviser (-3). On en déduit donc que

$$p \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\} \quad \text{et} \quad q \in \{\pm 1, \pm 3\}.$$

Après divers essais, on voit que la dernière solution de P est $r = 2/3$. Notez alors qu'on aurait pu trouver cette dernière solution bien plus facilement en effectuant la division euclidienne du polynôme P par le polynôme $(x + 2)(x - 5)$ et P s'écrit ainsi sous la forme

$$P(x) = 3(x - 2)(x + 5)(x - 2/3).$$

Cet exemple se généralise facilement et je vous invite à démontrer que si P est un polynôme de degré $n \geq 1$ défini par l'expression

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

où $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ et si $r = p/q$ est une fraction irréductible vérifiant $P(r) = 0$ alors le lemme de Gauss nous permet d'affirmer que p divise a_0 et que q divise a_n.

Pour finir cette section, nous donnons une preuve alternative de l'irrationalité de $\sqrt{2}$ en montrant que le polynôme $P(x) = x^2 - 2$ n'admet pas de racines rationnelles. En effet, si $r = p/q$ est irréductible telle que $P(r) = 0$ alors p et q doivent diviser respectivement 2 et 1. Ainsi $r = \pm 2$, mais $2^2 - 2 = (-2)^2 - 2 = 2 \neq 0$. Ainsi P n'admet aucune solution rationnelle. Ceci achève notre super preuve.

12 Le théorème fondamental de l'arithmétique

Nous sommes maintenant à même de décortiquer et démontrer le fameux théorème fondamental de l'arithmétique. Il affirme en effet qu'à permutation près, tout entier naturel ≥ 2 se décompose de façon unique en produit de facteurs premiers. Ainsi, le nombre 140 se décompose sous la forme

$$140 = 2 \cdot 70 = 2 \cdot 2 \cdot 35 = 2^2 \cdot 5 \cdot 7.$$

On voit alors qu'on ne peut pas casser les nombres davantage puisque 2, 5 et 7 sont premiers. Remarquez aussi que l'on peut écrire

$$140 = 2^2 \cdot 5 \cdot 7 = 5 \cdot 2^2 \cdot 7,$$

c'est à dire permuter les positions des nombres premiers dans la décomposition en facteurs premiers, mais jamais on ne pourra trouver une décomposition de 140 faisant intervenir des nombres premiers différents de 2, 5 et 7. Ce résultat semble donc évident, mais comme je l'ai déjà souligné, rien n'est bien évident trop longtemps en mathématiques et il nécessite ainsi une démonstration correcte. On peut alors penser que notre théorème est vrai car quand on tombe sur un nombre premier en faisant la décomposition, on ne peut plus décomposer davantage. Cette intuition est fausse comme on peut le voir sur le contre-exemple suivant.

Nous nous intéressons au monde des entiers naturels s'écrivant sous la forme $3x + 1$, à savoir

$$1, 4, 7, 10, 13, 16, 19, 22, 25 \cdots$$

Quand on multiplie deux entiers de cette forme, on tombe sur un entier de la même forme. Par exemple,

$$7 \cdot 10 = 70 = 3 \cdot 23 + 1,$$

qui est donc de la forme $3x + 1$. Plus généralement,

$$\begin{aligned}(3x+1)(3y+1) &= 3x \cdot 3y + 3x + 3y + 1 \\ &= 3(3xy + x + y) + 1 \\ &= 3X + 1,\end{aligned}$$

où $X = 3xy + x + y$. Cela signifie en clair que la multiplication laisse stable l'ensemble des entiers naturels de la forme $3x + 1$. Autrement dit, en multipliant deux entiers naturels de cet ensemble, le résultat n'en sort pas. Dans ce monde de nombres, 52 est un nombre composé puisque $52 = 4 \cdot 13$, 28 l'est aussi car $28 = 4 \cdot 7$. Toutefois, 22 ne se décompose plus en produit de nombres de la forme $3x + 1$ et donc on peut considérer que dans ce monde 22

est premier. Notez alors que 100 est un nombre de notre nouveau monde se décomposant en

$$100 = 10 \cdot 10 = 4 \cdot 25,$$

où 10, 4 et 25 ne se décomposent plus en produit de nombres entiers de la forme $3x+1$. Moralité de cette histoire, 100 admet deux décompositions en produit de facteurs indécomposables dans notre monde et donc l'unicité de la décomposition en facteurs premiers chez les entiers naturel tout court ne découle pas de l'indécomposibilité des nombres premiers. Si c'était le cas pour les entiers ce serait aussi le cas pour les entiers de la forme $3x+1$.

On peut être tenté de penser que l'unicité de la décomposition en facteurs premiers chez les entiers est une conséquence de la possibilité de décomposer de tels nombres. Dans la suite, nous étudierons un contre-exemple un peu plus savant que le premier. Nous nous intéressons alors aux nombres complexes de la forme $a+ib\sqrt{5}$, où a et b sont des entiers. Pour commencer, on remarque que non seulement cet ensemble est stable par multiplication mais aussi par addition. On se rapproche ainsi de la structure algébrique des entiers naturels. En effet,

$$(a+ib\sqrt{5})+(c+id\sqrt{5}) = (a+b)+i(c+d)\sqrt{5},$$

et

$$\begin{aligned}(a+ib\sqrt{5})(c+id\sqrt{5}) &= ac+iad\sqrt{5}+ibc\sqrt{5}-5bd \\ &= (ac-5bd)+i(ad+bc)\sqrt{5}.\end{aligned}$$

On remarque alors qu'ici 21 se décompose sous plusieurs formes

$$\begin{aligned}21 &= 3\cdot 7 \\ &= (1+i2\sqrt{5})(1-i2\sqrt{5}) \\ &= (4+i\sqrt{5})(4-i\sqrt{5}).\end{aligned}$$

À ce stade, la question que l'on se pose naturellement est si ces nombres figurant dans la décomposition de 21 sont premiers ou sont-ils encore décomposables dans le monde des nombres de la forme $a+ib\sqrt{5}$. Regardons du côté de 3 et supposons qu'il l'est, c'est à dire

$$\begin{aligned}3 &= (a+ib\sqrt{5})(c+id\sqrt{5}) \\ &= (ac-5bd)+i(ad+bc)\sqrt{5}.\end{aligned}$$

Par identification [17], cette dernière égalité implique que $ad+bc=0$. Par conséquent on peut aussi écrire

$$\begin{aligned}3 &= (a-ib\sqrt{5})(c-id\sqrt{5}) \\ &= (ac-5bd)-i(ad+bc)\sqrt{5}.\end{aligned}$$

On en déduit que

$$\begin{aligned}9 &= (a+ib\sqrt{5})(a-ib\sqrt{5})(c+id\sqrt{5})(c-id\sqrt{5}) \\ &= (a^2+5b^2)(c^2+5d^2).\end{aligned}$$

17. Partie réelle et partie imaginaire

Cette relation signifie donc que a^2+5b^2 et c^2+5d^2 sont des diviseurs positifs de 9 et par conséquent

$$a^2+5b^2, c^2+5d^2 \in \{1,3,9\}.$$

Si par exemple $a^2+5b^2=1$ alors $c^2+5d^2=9$. Dans ce cas $a=\pm 1$, $b=0$, $c=\pm 3$ et $d=0$ ou $c=\pm 2$ et $d=\pm 1$. Dans tous les cas, ces entiers ne donnent jamais $(a+ib\sqrt{5})(c+id\sqrt{5})=3$. Le cas $a^2+5b^2=9$ et $c^2+5d^2=1$ se traite de la même manière et je vous laisse vérifier que le cas $a^2+5b^2=c^2+5d^2=3$ est impossible. Ainsi, dans le monde des nombres de la forme $a+ib\sqrt{5}$, 3 ne peut pas se décomposer davantage.

Ce même raisonnement permet de démontrer que 7 est premier dans ce nouveau monde et que $4+i\sqrt{5}$ l'est aussi. À vous de jouer ! On a ainsi trouvé un ensemble de nombres dans lequel on peut additionner, multiplier et décomposer en produit de facteurs premiers sans pour autant garantir l'unicité de cette décomposition. On peut alors se demander quelle raison y a-t-il derrière l'unicité de la décomposition en produit de facteurs premiers chez les entiers naturels ? Quelle propriété possèdent-ils permettant d'avoir cette caractéristique ?

L'unicité de la décomposition en facteurs premiers repose sur un lemme clef, connu sous le nom du **lemme d'Euclide**. Ce fameux résultat affirme que si p est un nombre premier divisant le produit de deux entiers ab, alors p doit diviser a ou b. Pour nous, ce lemme est un cas particulier du lemme de Gauss. Toutefois, ce qui est surprenant, les Grecs ont compris toutes ses subtilités sans forcément disposer de contre-exemples pertinents. Nous allons donc suivre le raisonnement d'Euclide afin de parvenir à la démonstration de son lemme. Tout d'abord, notre ancêtre savant démontre l'énoncé suivant

Proposition 20-Livre VII : Si l'on a une fraction $\frac{a}{b}$ et si a et b sont les plus petits dans ce rapport, autrement dit si $\frac{c}{d}$ est une autre fraction égale à a/b alors $a \leq c$ et $b \leq d$, alors il existe un entier k tel que $c=ak$ et $d=bk$.

Ce résultat semble évident mais il nécessite là encore une démonstration. En effet, en divisant c par a et d par b on obtient les relations $c=ak+r$ et $d=bk'+s$ avec $0 \leq r < a$ et $0 \leq s < b$. On souhaite démontrer que $k=k'$ et $r=s=0$. D'abord on peut écrire

$$\begin{aligned} ad &= a(bk'+s) \\ &= abk'+as \end{aligned}$$

et

$$\begin{aligned} bc &= b(ak+r) \\ &= bak+br. \end{aligned}$$

L'égalité $a/b=c/d$ implique alors que $ad=bc$ ou encore que $m := abk'+as=abk+br$ [18]. Mais comme on a $as<ab$ et $br<ab$, les deux expressions définissant l'entier m sont en réalité deux divisions euclidiennes de m par ab. Par unicité du quotient et du reste de la division euclidienne, on a $k=k'$ et $as=br$. Les entiers r et s sont tous les deux nuls car sinon si $s \neq 0$ alors $a/b=r/s$, ce qui contredit la minimalité de a et b. Le résultat en découle.

Le lemme d'Euclide est alors une conséquence de cette proposition. En effet, si p divise ab alors on peut écrire $ab=pc$ ou encore que $a/p=c/b$. Si p ne divise pas a alors a et p

18. Le signe := signifie l'entier m est défini par.

sont premiers entre eux et sont donc les plus petits entiers représentant la fraction a/p. La proposition 20 implique alors qu'il existe un entier k tel que $c = ak$ et $b = pk$. Le nombre premier p divise donc b. Notez alors que le lemme d'Euclide n'est plus valable dans le monde des nombres de la forme $a+ib\sqrt{5}$. Nous avons en effet vu que $21 = 3\cdot 7 = (4+i\sqrt{5})(4-i\sqrt{5})$, 3 divise donc $(4+i\sqrt{5})(4-i\sqrt{5})$ sans diviser aucun des facteurs.

Venons-en maintenant à la preuve de l'unicité de la décomposition chez les entiers. Supposons que l'entier n admette deux décompositions possibles en produit de facteurs premiers, de sorte que

$$n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_r.$$

Cela signifie en particulier que p_1 divise $q_1 q_2 \cdots q_r$, mais puisque tous les q sont premiers, le lemme d'Euclide implique que p_1 doit diviser l'un deux, disons q_1. Par conséquent $p_1 = q_1$ et $p_2 p_3 \cdots p_t = q_2 q_3 \cdots q_r$. En réitirant ce même procédé avec cette nouvelle égalité, le théorème fondamental de l'arithmétique tombe comme une pomme mûre.

Avant de terminer cette section, nous donnons une démonstration de plus de l'irrationalité de $\sqrt{2}$. On n'en a pas fini avec ce petit monstre. D'abord, d'après le TFA [19], tout entier $n \geq 2$ s'écrit sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

où $p_1 < p_2 < \cdots < p_r$ et $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 1$. Supposons maintenant qu'on peut écrire $\sqrt{2} = m/n$, ou encore que $2n^2 = m^2$. D'après ce qui précède, on peut écrire

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{et} \quad m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t},$$

avec $p_1 < p_2 < \cdots < p_r$ et $q_1 < q_2 < \cdots < q_t$. Ceci implique en particulier la relation

$$2p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} = q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_t^{2\beta_t}.$$

Or d'après l'unicité de la décomposition en facteurs premiers on peut affirmer que $2 = q_1$. On en déduit que la puissance de 2 à droite est $2^{2\beta_1} \geq 2^2$, car $\beta_1 \geq 1$. Ainsi 4 doit diviser le membre de gauche et l'on doit donc avoir $p_1 = 2$. La puissance de 2 à gauche vaut donc $2\alpha_1 + 1 = 2\beta_1$. Contradiction [20].

13 Retour sur les triplets Pythagoriciens

Euclide a utilisé sa théorie de la divisibilité afin de trouver tous les triplets pythagoriciens, à savoir les triplets d'entiers (x, y, z) vérifiant l'équation $x^2 + y^2 = z^2$. Avant de nous lancer dans cette quête, nous allons démontrer deux lemmes importants.

13.1 Deux lemmes techniques

Lemme 1 : Si le produit deux entiers naturels premiers entre est un carré parfait alors chacun de ces entiers est un carré parfait. De façon équivalente, si x, y et z sont trois entiers naturels tels que

$$xy = z^2 \quad \text{et} \quad (x, y) = 1,$$

19. Théorème Fondamental de l'Arithmétique.
20. Un nombre pair ne peut pas être égal à un nombre impair.

alors il existe deux entiers naturels u et v tels que $x = u^2$ et $y = v^2$.

Lemme 2 : Si d^2 divise z^2 alors d divise z.

Ces deux lemmes sont des conséquences du TFA. Nous pouvons ainsi utiliser les valuations p-adique afin de les démontrer. Soit ainsi $x \in \mathbb{N}^*$ et p un nombre premier. La valuation p-adique de x qu'on note $v_p(x)$ est la plus grande puissance de p divisant x. En d'autres termes,

$$v_p(x) = \max\{\alpha \in \mathbb{N}, p^\alpha \text{ divise } x\}.$$

Par exemple

$$280 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 = 2^3 \cdot 5 \cdot 7.$$

Ainsi la plus grande puissance de 2 divisant 280 est 3 et donc $v_2(280) = 3$. De même, on voit que $v_5(280) = v_7(280) = 1$ et $v_{11}(280) = 0$. Notez alors que la valuation p-adique vérifie la fameuse relation logarithmique

$$v_p(xy) = v_p(x) + v_p(y),$$

qui est une conséquence directe du TFA. La valuation est un outil efficace pour démontrer certains résultats en arithmétique et remarquer alors que pour montrer que m divise n, il suffit de montrer que pour tout nombre premier p, $v_p(m) \leq v_p(n)$. Nos deux lemmes deviennent alors deux conséquences triviales de cette histoire.

- Lemme 1 : Si $xy = z^2$ et $(x, y) = 1$ alors $v_p(xy) = v_p(z^2)$, ce qui implique par la relation logarithmique que $v_p(x) + v_p(y) = 2v_p(z)$. Puisque x et y sont premiers entre eux, il vient que $(v_p(x) \neq 0 \implies v_p(y) = 0)$. Ainsi, $v_p(x) = 2v_p(z)$. Cette dernière égalité est vérifiée pour tout nombre premier p, toute valuation de x est paire, donc x est un carré parfait. Le même raisonnement s'applique sur y.
- Lemme 2 : Si d^2 divise z^2 alors $v_p(d^2) \leq v_p(z^2)$ pour tout nombre premier p. La relation logarithmique là encore implique que $2v_p(d) \leq 2v_p(z)$ ou encore que $v_p(d) \leq v_p(z)$. $\mathscr{C}\mathscr{Q}\mathscr{F}\mathscr{D}$.

13.2 Triplets pythagoriciens primitifs et similarité

Soit $\Delta = (x, y, z)$ un triangle pythagoricien, ce qui signifie que x, y et z sont des entiers naturels vérifiant l'égalité $x^2 + y^2 = z^2$. Si chacun des côtés de ce triangle est multiplié par un entier naturel k, on obtient un triangle pythagoricien semblable au premier.
De la même manière, on obtient une infinité de triangles pythagoriciens semblables, de la forme $k\Delta = (kx, ky, ky)$. Nous avons vu ensemble que le triangle $\Delta = (3, 4, 5)$ est pythagoricien, à partir duquel on peut extraire une infinité d'autres tels que $(6, 8, 10)$, $(9, 12, 15)$, $(12, 16, 20)$, etc. Il est alors trivial de voir que parmi tous les triangles pythagoriciens semblables, il en existe un plus petit ayant les deux côtés x et y premiers entre eux. En effet, si x et y ne le sont pas alors ils admettent un diviseur commun $d > 1$. Cela implique que $x = dx_1$ et $y = dy_1$, où x_1 et y_1 désignent deux entiers naturels. On obtient ainsi la relation

$$z^2 = x^2 + y^2 = (dx_1)^2 + (dy_1)^2 = d^2(x_1^2 + y_1^2),$$

ce qui montre que d^2 divise z^2. D'après notre deuxième lemme technique, d doit diviser z et par conséquent $z = dz_1$. En divisant le tout par d^2 on obtient la relation

$$x_1^2 + y_1^2 = z_1^2,$$

ce qui prouve que (x_1, y_1, z_1) est un triangle pythagoricien semblable et plus petit que (x, y, z). Moralité : parmi les triangles pythagoriciens semblables, le plus petit a les côtés x et y premiers entre eux.

Réciproquement, si dans un triangle pythagoricien $\Delta = (x, y, z)$, les côtés x et y sont premiers entre eux alors il n'existe de triangle pythagoricien semblable et plus petit que Δ. Si $\Delta_1 = (x_1, y_1, z_1)$ était un tel triangle, la similarité avec Δ impliquerait la relation $x/x_1 = y/y_1$ ou encore que $x/y = x_1/y_1$. Puisque x/y est une fraction irréductible (car x et y sont premiers entre eux), on obtient que $x_1 \geq x$ et $y_1 \geq y$ ce qui contredit l'hypothèse de minimalité vérifiée par Δ_1 par rapport à Δ. On dira dorénavant que le triplet (x, y, z) est primitif lorsque $(x, y) = 1$.

13.3 La chasse des triplets primitifs

Il est évident maintenant que la quête des triplets pythagoriciens revient à trouver ceux qui sont primitifs. Soit alors $\Delta = (x, y, z)$ un triplet primitif. Dans ce cas, x et y ne peuvent pas être tous les deux pairs car ils sont premiers entre eux. Nous montrons dans ce qui suit qu'ils ne peuvent pas être tous les deux impairs. Pour se faire, nous démontrons que le carré d'un nombre impair laisse un reste égal à 1 dans sa division euclidienne par 8. Soit a un nombre impair de la forme $a = 2k + 1$, où $k \in \mathbb{N}$. On obtient alors

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

À ce stade, il suffit de montrer que $k(k + 1)$ est toujours un nombre pair. Ceci est trivial car dans un produit de deux entiers consécutifs, l'un des facteurs est pair et donc le produit l'est aussi. Revenons à nos moutons, si x et y étaient tous les deux impairs, le reste de la division euclidienne de $x^2 + y^2 = z^2$ par 8 serait égal à 2. Cette dernière affirmation est impossible car le carré d'un nombre pair est divisible par 4 [21].

Sans perte de généralité, on peut supposer que l'entier y est pair. Il en résulte que x et z sont tous les deux impairs. L'équation de Pythagore peut s'écrire sous la forme

$$y^2 = z^2 - x^2 = (z - x)(z + x).$$

Étant la somme et la différence de deux entiers impairs, les deux entiers $z - x$ et $z + x$ sont pairs, par conséquent peuvent s'écrire sous la forme

$$z + x = 2a, \quad z - x = 2b.$$

On en déduit en particulier que $z = a + b$ et $x = a - b$. Ces deux dernières égalités impliquent que a et b sont premiers entre eux. En effet, si d était un facteur en commun à a et b, il serait aussi facteur en commun à z et x et donc à $z + x$ et $z - x$. Cela signifie que d^2 divise y^2, ou encore que d divise y. Ceci implique donc que $d = 1$ car x et y sont premiers entre eux. Par ailleurs, l'entier y peut s'écrire sous la forme $y = 2c$ et l'équation $y^2 = (z - x)(z + x)$ devient alors $4c^2 = 2a \cdot 2c$ ou encore

$$c^2 = ab.$$

21. Je vous laisse le soin de détailler ces raisonnements afin de vous en convaincre.

Cette identité est géniale car elle nous rappelle notre Lemme 1. On en déduit que a et b sont deux carrés parfaits, c'est-à-dire $a = u^2$ et $b = v^2$, où u et v sont premiers entre eux (car ils divisent deux nombres premiers entre eux). Il s'en suit que

$$z = u^2 + v^2, \quad x = u^2 - v^2, \quad \text{et} \quad y = 2uv.$$

Il est alors immédiat que

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2.$$

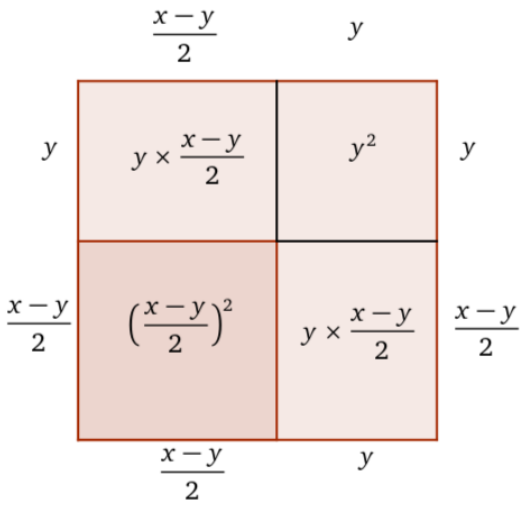
J'espère que cette jolie identité vous rappelle la même, retrouvée dans les travaux de Diophante et contournant complètement le théorème fondamental de l'arithmétique. Notez de plus que pour garantir le caractère primitif de nos triplets, u et v ne peuvent pas être tous les deux pairs, ni impairs d'ailleurs. Dans le cas contraire, $x = u^2 - v^2$ serait pair, ce qui contredit notre hypothèse du départ.

Réciproquement, on aimerait savoir si $u > v$ sont deux entiers naturels premiers entre eux dont l'un est pair et le deuxième impair, alors notre fameuse formule produit bien un triplet primitif, autrement dit les entiers $x = u^2 - v^2$ et $y = 2uv$ sont premiers entre eux. En effet, si $d > 1$ était un facteur en commun à x et y, il aurait la même parité que x, mais d est aussi facteur de $z = u^2 + v^2$, ce qui implique que d est facteur de $z + x = 2u^2$ et $z - x = 2v^2$. La parité de d implique qu'il est facteur en commun de u^2 et v^2. Ceci nous conduit à une contradiction car u^2 et v^2 sont premiers entre eux puisque u et v le sont.

Ainsi, nous avons montré que tous les triplets pythagoriciens primitifs sont de la forme $\Delta = (u^2 - v^2, 2uv, u^2 + v^2)$, où $u > v$ sont deux entiers naturels premiers entre eux dont l'un est pair et l'autre est impair. Dans sa recherche des triplets pythagoriciens, Euclide a utilisé une approche légèrement différente. En effet, notre ancêtre savant a utilisé l'identité algébrique

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

En gardant en tête qu'Euclide était essentiellement géomètre, comment a-t-il pu donc penser à sa formule ? Ci-dessous une façon de faire[22] (légèrement différente là encore de celle d'Euclide)



22. Ce beau dessin m'a été suggéré par un élève. L'idée originale d'Euclide se trouve dans ses Éléments, Livre II, Proposition 5.

En calculant l'aire du grand carré de deux façons, on obtient le résultat voulu. D'une part, le côté de ce carré vaut

$$\frac{x-y}{2}+y=\frac{x+y}{2},$$

ce qui implique que son aire vaut $\left(\frac{x+y}{2}\right)^2$. D'autre part, cette même aire vaut

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

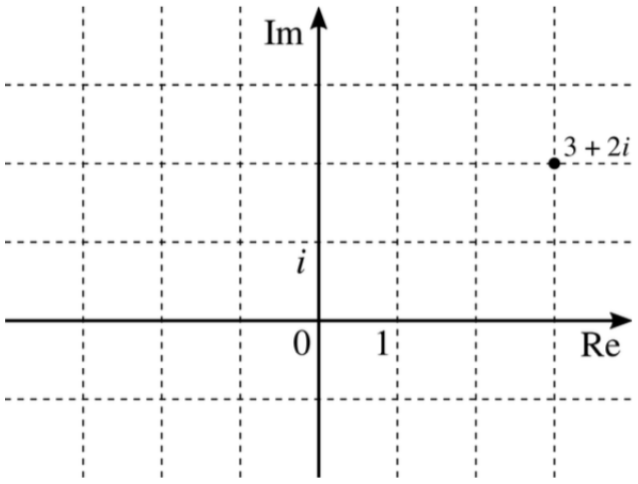
D'où la relation euclidienne. Revenons maintenant à notre problème. Euclide a observé qu'il était suffisant de prendre x et y tels que xy soit un carré parfait afin de générer des triplets pythagoriciens. Pour se faire, x et y doivent être deux entiers **semblables**, c'est-à-dire $x=u^2w$ et $y=v^2w$. Le mot semblable a une interprétation géométrique dans ce contexte, il signifie que si un rectangle d'aire w est dilaté par u ou v (pour les deux dimensions) alors l'aire est respectivement dilatée d'un facteur u^2 ou v^2. L'identité algébrique d'Euclide devient alors

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

Euclide va même un peu plus loin et montre que la façon de produire des triplets pythagoriciens est de prendre x et y des entiers semblables. En d'autres termes, xy est un carré parfait si et seulement si x et y sont deux entiers semblables [23]. Sans perte de généralité, on peut supposer que x et y sont premiers entre eux. La proposition d'Euclide est tout simplement notre Lemme 1. Le résultat en découle.

13.4 Les entiers de Gauss

Une autre approche pour trouver les triplets pythagoriciens est celle des entiers de Gauss. L'idée géniale de notre ancêtre est de travailler chez les entiers complexes $a+ib$, où a et b sont dans $\mathbb{Z}$. On dénote cet ensemble de nombres $\mathbb{Z}[i]$. Géométriquement, cet ensemble correspond aux points du plan ayant des coordonnées entières.



L'idée de Gauss était de factoriser l'équation $z^2=x^2+y^2$ dans l'ensemble $\mathbb{Z}[i]$. Nous avons en effet

$$z^2=x^2-(iy)^2=(x-iy)(x+iy).$$

23. Voir Livre IX, Proposition 2.

On espère alors à ce stade pouvoir conclure avec un lemme fonctionnant dans $\mathbb{Z}[i]$ et ressemblant à notre Lemme 1 (fonctionnant dans $\mathbb{Z}$). En effet, si x et y sont premiers entre eux alors $x-iy$ et $x+iy$ semblent être premiers entre eux, mais qu'est ce que cela peut bien signifier dans $\mathbb{Z}[i]$? En tout cas, si c'est le cas, on pourra dire que $x+iy$ est un carré parfait dans $\mathbb{Z}[i]$. Par conséquent, il existe $u=a+ib\in\mathbb{Z}[i]$ tel que

$$x+iy=u^2=(a+ib)^2=a^2-b^2+i(2ab).$$

En prenant les carrés des modules de ces nombres complexes, on obtient l'égalité

$$|x+iy|^2=|(a+ib)^2|^2=|a^2-b^2+i(2ab)|^2,$$

ou encore

$$z^2=x^2+y^2=(a^2+b^2)^2=(a^2-b^2)^2+(2ab)^2,$$

qui est bien le résultat tant recherché ! Quelle incroyable simplicité ! La structure de $\mathbb{Z}[i]$ tient donc le secret de l'équation de Pythagore.

L'outil efficace ayant permis nos conclusions dans le cas de $\mathbb{Z}$ et de $\mathbb{Z}[i]$ est une similarité structurelle entre les deux ensembles. Ils possèdent tous les deux une division euclidienne. Je vous rappelle le théorème de la division euclidienne dans $\mathbb{Z}$.

Théorème : Soient $a\in\mathbb{Z}$ et $b\in\mathbb{N}^*$. Il existe un unique couple $(q,r)\in\mathbb{Z}\times\mathbb{N}$ tel que

$$a=bq+r \quad \text{et} \quad 0\leq r<b.$$

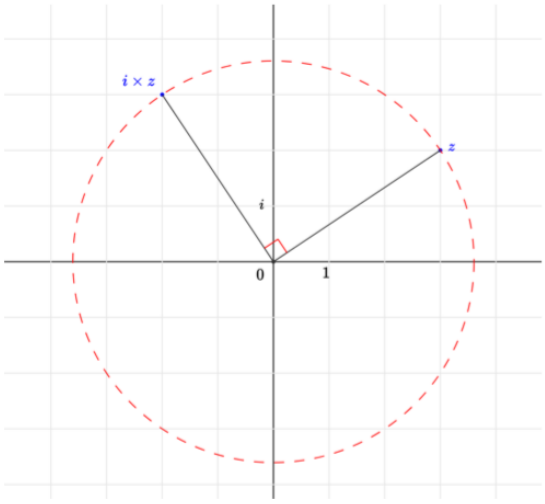
Dans $\mathbb{Z}[i]$, on a le théorème de la division euclidienne suivant

Théorème : Soient α et β deux entiers de Gauss, $\beta\neq 0$. Il existe au moins (pas d'unicité ici) deux entiers de Gauss τ et ρ vérifiant

$$\alpha=\beta\tau+\rho \quad \text{avec} \quad 0\leq|\rho|<|\beta|.$$

Comment peut-on alors imaginer un tel théorème ? En tout cas, il a une conséquence capitale, à savoir impliquer l'unicité de la décomposition en facteurs premiers chez les entiers de Gauss et donc deux lemmes équivalents à nos Lemmes 1 et 2.

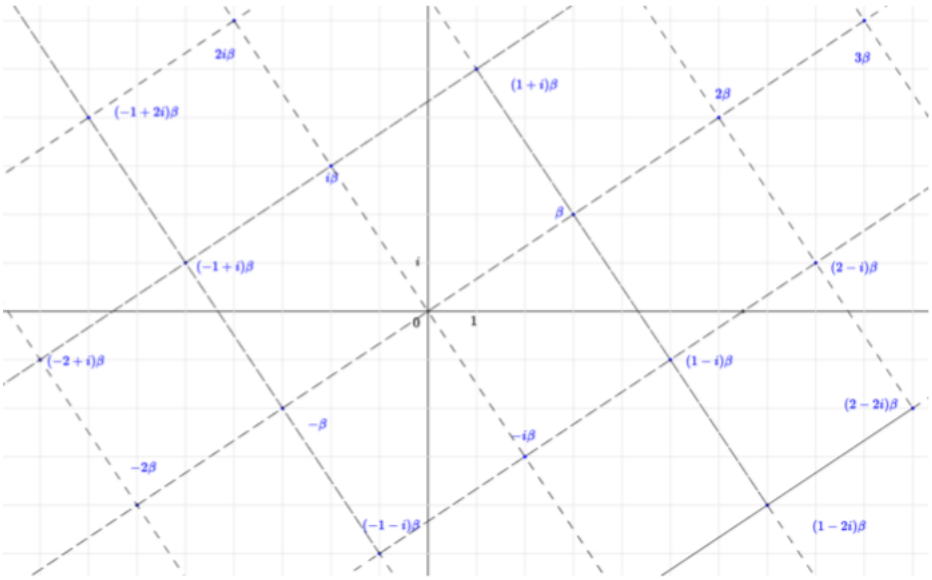
Afin de bien comprendre le théorème de la division euclidienne dans $\mathbb{Z}[i]$, plaçons-nous dans le cadre géométrique. Accrochez-vous hein !



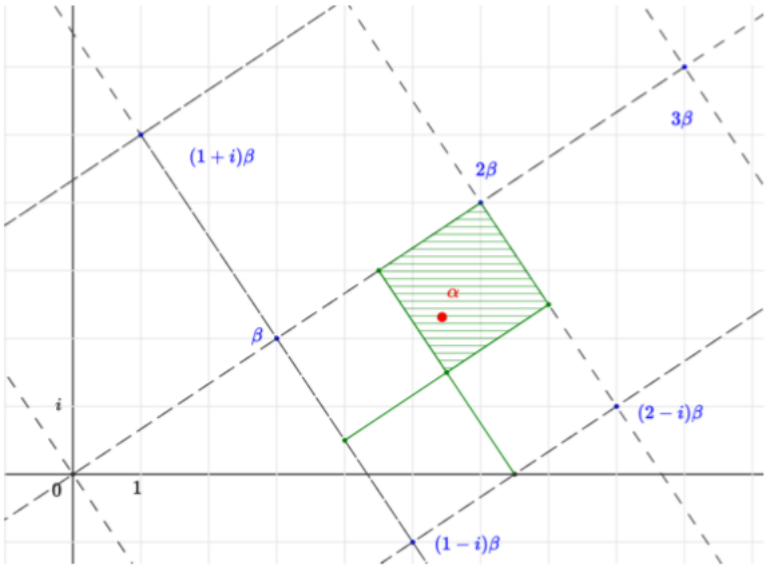
On remarque d'abord que multiplier un nombre complexe z par i revient à prendre le nombre complexe qui lui est perpendiculaire, comme le montre la figure ci-dessus. Or, multiplier β par l'entier de Gauss $c+id$ donne

$$\beta(c+id) = \beta c + i\beta d = c(\beta) + d(i\beta),$$

qui est un nouveau point exprimé dans la base $(\beta, i\beta)$. On obtient ainsi le réseau ci-dessous.



Par conséquent, tout point α est à l'intérieur de l'un des carrés formés par ce réseau de points. En divisant chacun des carrés en 4 zones et en déterminant à quelle zone α appartient on obtient la figure :



On prend alors le point le plus proche du réseau à cette zone, égal à $\beta\tau$ pour un certain $\tau \in \mathbb{Z}[i]$ et l'on vérifie aisément que $|\alpha - \beta\tau|$, c'est-à-dire la distance entre α et ce point, est strictement plus petite que le côté du grand carré, à savoir $|\beta|$. La preuve en découle en prenant $\rho = \alpha - \beta\tau$. Prenons un exemple.

Exemple : Soient $\alpha = 2+3i$ et $\beta = 1-2i$. Alors

$$\begin{aligned}\frac{2+3i}{1-2i} &= \frac{(2+3i)(1+2i)}{(1-2i)(1+2i)}\\ &= \frac{2+4i+3i-6}{1+4}\\ &= \frac{-4+7i}{5}.\end{aligned}$$

Il suffit alors de prendre $\tau = x+iy$ où

$$\left|x-(-4/5)\right| \leq \frac{1}{2} \quad \text{et} \quad \left|y-7/5\right| \leq \frac{1}{2}.$$

L'entier de Gauss $\tau = -1+i$ vérifie les deux inégalités et on a bien $\alpha = \beta\tau+\rho$, où $\rho = 1$. Je vous laisse vérifier la condition sur le module. La preuve formelle du théorème de la division euclidienne dans $\mathbb{Z}[i]$ est une généralisation de cet exemple. En effet, soient α et $\beta \in \mathbb{Z}[i]$ tels que $\beta \neq 0$. Soient $x, y \in \mathbb{Q}$ tels que $\alpha/\beta = x+iy$. Prenons deux entiers $p, q \in \mathbb{Z}$ tels que $|x-p| \leq 1/2$ et $|y-q| \leq 1/2$. On pose alors $\tau = p+iq$ et $\rho = \alpha-\beta\tau$. Il s'ensuit

$$\begin{aligned}|\rho|^2 &= |\alpha-\beta\tau|^2\\ &= \left|\beta\left(\frac{\alpha}{\beta}-\tau\right)\right|^2\\ &= |\beta|^2\left|\frac{\alpha}{\beta}-\tau\right|^2\\ &= |\beta|^2|(x-p)+i(y-q)|^2\\ &\leq |\beta|^2(1/4+1/4)\\ &< |\beta|^2.\end{aligned}$$

Cela achève notre preuve.

Avant de terminer cette section, donnons encore une méthode permettant de trouver les triplets pythagoriciens. Cette méthode se base sur l'identité **des deux carrés** donnée par son éminence Abu Jafar Muhammed Al-Khazin, mathématicien perse du 10ème siècle.

L'identité des deux carrés : Le produit de deux sommes de deux carrés est la somme de deux carrés. En d'autres termes

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2.$$

En effet

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (a-ib)(a+ib)(c-id)(c+id)\\ &= (a-ib)(c-id)(a+ib)(c+id)\\ &= [(ac-bd)-i(ad+bc)][(ac-bd)+i(ad+bc)]\\ &= (ac-bd)^2+(ad+bc)^2.\end{aligned}$$

Maintenant en prenant $a = c$ et $b = d$, on obtient

$$(a^2+b^2)(a^2+b^2) = (a^2-b^2)^2+(2ab)^2.$$

Oh ! Incroyable, c'est encore notre fameuse formule ! Toutefois, cette approche n'implique pas que tous les triplets pythagoriciens sont de cette forme. Cela termine donc notre quête des triplets de Pythagore.

13.5 Retour sur le Grand Théorème de Fermat pour $n = 4$

Nous sommes maintenant capables de démontrer le Grand Théorème de Fermat dans le cas $n = 4$. Je vous rappelle que cela revient à démontrer en utilisant la descente infinie qu'il n'existe pas de triangle pythagoricien dont l'aire est un carré parfait. Supposons qu'il existe $\Delta = (a, b, c)$ un triangle pythagoricien dont l'aire est un carré parfait, autrement dit

$$a^2 + b^2 = c^2 \quad \text{et} \quad \frac{1}{2}ab \text{ est un carré parfait.}$$

Sans perte de généralité, on peut supposer le triplet (a, b, c) primitif, ce qui signifie que a et b sont premiers entre eux. D'après ce qui précède, il existe deux entiers $u > v$, premiers entre eux et de parités opposées [24] tels que

$$a = u^2 - v^2, \quad b = 2uv \quad \text{et} \quad c = u^2 + v^2.$$

Dans ce cas, l'aire de Δ vaut

$$\begin{aligned} \frac{1}{2}ab &= \frac{1}{2}(u^2 - v^2) \cdot 2uv \\ &= (u - v)(u + v)uv. \end{aligned}$$

Cette égalité implique que $(u-v)(u+v)uv$ est un carré parfait, car $(1/2)ab$ l'est aussi. Or $u-v$, $u+v$, u et v sont deux à deux premiers entre eux [25] et donc d'après le Lemme 1, ils sont tous des carrés parfaits. Je vous rappelle que l'on souhaite démontrer l'existence d'un triangle pythagoricien strictement plus petit que Δ dont l'aire est un carré parfait. Ceci nous conduira à une contradiction. En effet, $(u-v)(u+v)$ est un carré parfait et donc s'écrit sous la forme

$$(u - v)(u + v) = u^2 - v^2 = p^2,$$

ou encore $p^2 + v^2 = u^2$. Or $u^2 - v^2 = a$ et si l'on prend a impair alors p l'est aussi. Si de plus u est impair alors v doit être pair. On pourra alors montrer facilement que p et v sont premiers entre eux, ce qui implique que $\delta = (p, v, u)$ est un nouveau triplet pythagoricien primitif. Il existe alors deux entiers $u_1 > v_1$ premiers entre eux et de parités opposées tels que

$$p = u_1^2 - v_1^2, \quad v = 2u_1v_1 \quad \text{et} \quad u = u_1^2 + v_1^2.$$

Or $v = 2u_1v_1$ est un carré parfait donc u_1 ou v_1 est un carré impair tandis que le deuxième est le double d'un carré(*). Par ailleurs, u est un carré parfait et s'écrit donc sous la forme $u = n^2$, ce qui implique que $n^2 = u_1^2 + v_1^2$. Par conséquent $\Gamma = (u_1, v_1, n)$ est un nouveau triangle pythagoricien dont l'aire $(1/2)u_1v_1$ doit être un carré parfait d'après (*). Il nous reste donc à montrer que le triangle Γ est plus petit que le triangle Δ. En effet

$$n = \sqrt{u} < u < u^2 < u^2 + v^2 = c.$$

Le résultat en découle !

24. L'un est pair, l'autre est impair

25. Par exemple, si d divise u et $u-v$ alors d doit diviser leur différence, à savoir v, il en résulte que $d = 1$. Je vous laisse le soin de montrer le résultat pour les autres cas.

14 Les congruences

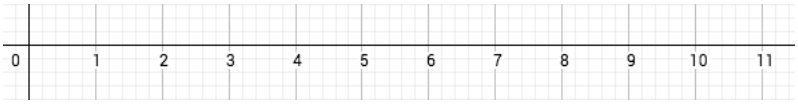
14.1 Définition et premières propriétés

Avant de définir formellement les congruences, nous allons inspecter ensemble quelques exemples concrets afin de nous rendre compte de la puissance de cet outil.

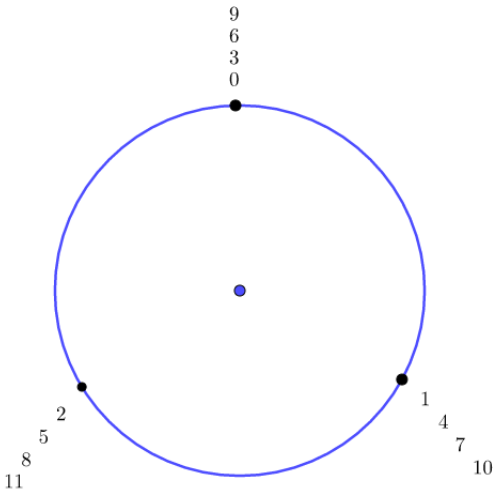
Exemple 1 : Nous souhaitons démontrer dans ce premier exemple que si a est un entier alors $a^3 - a$ est toujours multiple de 3. Regardons ce que cela donne sur quelques valeurs.

a	$a^3 - a$
0	$0^3 - 0 = 0 = 3 \cdot 0$
1	$1^3 - 1 = 0 = 3 \cdot 0$
2	$2^3 - 2 = 6 = 3 \cdot 2$
3	$3^3 - 3 = 24 = 3 \cdot 8$
4	$4^3 - 4 = 60 = 3 \cdot 20$
5	$5^3 - 5 = 120 = 3 \cdot 40$
$\vdots$	$\vdots$

On voit alors que notre résultat est vérifié pour les premières valeurs de a et l'on peut alors conjecturer sa véracité pour tout a. Afin de prouver cette conjecture, nous allons introduire une nouvelle façon de représenter les nombres, à savoir l'horloge de Gauss. Nous avons alors l'habitude de représenter les entiers naturels mentalement sous la forme d'une suite de nombres situés sur une demi-droite comme ci-dessous



Au lieu de ça, nous pouvons enrouler cette demi-droite sur une horloge de 3 heures de la manière suivante



On voit alors que les entiers 3, 6 et 9 pointent sur l'heure 0 et plus généralement tout multiple de 3 est situé sur cette heure. Si a pointe sur 0 dans une horloge de 3 heures, on écrit

$$a \equiv 0 \pmod 3$$

et on lit a est **congru** à 0 **modulo** 3. De même, 4, 7 et 10 pointent sur 1 et tout nombre entier a de la forme $3x+1$ pointe sur 1. Dans ce cas on écrit

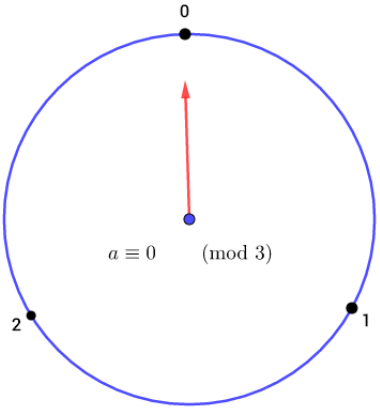
$$a \equiv 1 \pmod 3$$

et finalement 5, 8 et 11 pointent sur 2 heures et tout entier a de la forme $3k+2$ pointe sur 2, auquel cas on écrit $a \equiv 2 \pmod 3$. Maintenant pour montrer que $a^3 - a$ est un multiple de 3 pour tout a, il suffit de montrer que cette expression pointera toujours sur 0 dans une horloge de 3 heures, ou encore que

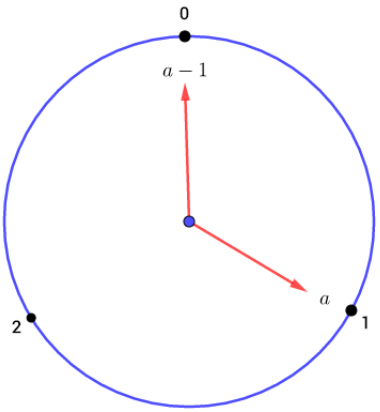
$$a^3 - a \equiv 0 \pmod 3.$$

L'expression $a^3 - a$ se factorise sous la forme $a(a-1)(a+1)$, cela nous conduit donc à distinguer 3 cas :

- Si a est un multiple de 3, autrement dit, si a pointe sur l'heure 0 sur une horloge de 3 heures, alors il en est de même pour l'expression $a(a-1)(a+1)$ car l'un de ses facteurs est un multiple de 3. En d'autres termes, si $a \equiv 0 \pmod 3$ alors $a^3 - a \equiv 0 \pmod 3$.



- Si a est de la forme $3x+1$, c'est à dire si a pointe sur 1 heure, ou encore que $a \equiv 1 \pmod 3$ alors $a-1$ pointe naturellement sur 0, ce qui s'écrit $a-1 \equiv 0 \pmod 3$ [26]. Par conséquent l'expression $a^3 - a = a(a-1)(a+1)$ pointe elle aussi sur 0, ce qui signifie qu'elle est multiple de 3.

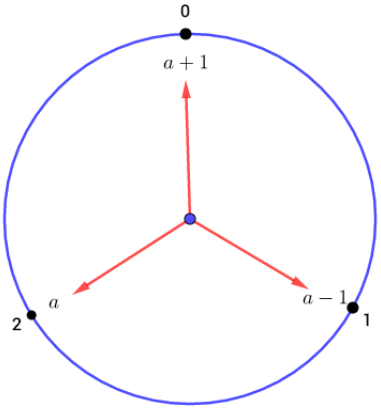


26. Remarquer ici que "$\equiv$" se comporte comme une vraie égalité dans laquelle on a effectué une simple soustraction, à savoir

$$a \equiv 1 \pmod 3 \implies a-1 \equiv 1-1 \equiv 0 \pmod 3.$$

- Dernier cas, si a pointe sur 2 heures, alors cette fois $a-1$ pointe sur 1 heure, ce qui n'est pas d'une grande aide pour nous. Toutefois, $a+1$ pointe sur 0. Avec les congruences, on écrit $a \equiv 2 \pmod 3$ implique que $a-1 \equiv 1 \pmod 3$ mais que

$$a+1 \equiv 2+1 \equiv 3 \equiv 0 \pmod 3.$$

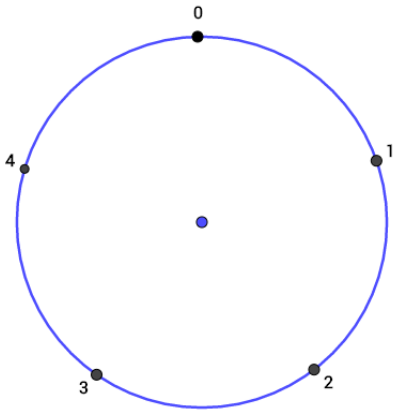


Ha ! On se rend compte que raisonner sur l'horloge rend la tâche bien plus facile. Prenons un deuxième exemple pour se fixer les idées.

Exemple 2 : Nous nous intéressons dans cet exemple à un énoncé similaire au premier. On souhaite démontrer que pour tout entier naturel a, $a^5 - a$ est un multiple de 5. Les premiers essais donnent

a	$a^5 - a$
0	$0^5 - 0 = 0 = 5 \cdot 0$
1	$1^5 - 1 = 0 = 5 \cdot 0$
2	$2^5 - 2 = 30 = 5 \cdot 6$
3	$3^5 - 3 = 240 = 5 \cdot 48$
4	$4^5 - 4 = 1020 = 5 \cdot 204$
5	$5^5 - 5 = 3120 = 5 \cdot 624$
$\vdots$	$\vdots$

Curieux ! N'est ce pas ? Je vous invite à prendre davantage de valeurs afin de vous en convaincre. Cette fois-ci, nous allons enrouler notre demi-droite sur une horloge de 5 heures comme ci-dessous.



Sans surprise, dans une horloge de 5 heures, tous les multiples de 5 pointent sur 0 et si a désigne un multiple de 5 on écrit

$$a \equiv 0 \pmod 5.$$

Les nombres a de la forme $5x+1$ pointent sur 1 heure, ce qui s'écrit naturellement $a \equiv 1 \pmod 5$ etc. Afin de montrer que $a^5 - a$ est un multiple de 5, il suffit de montrer qu'elle pointera sur 0 pour tout a. Remarquons tout d'abord que

$$\begin{aligned} a^5 - a &= a(a^4-1) \\ &= a(a^2-1)(a^2+1) \\ &= a(a-1)(a+1)(a^2+1). \end{aligned}$$

On distingue alors plusieurs cas :

- Si $a \equiv 0 \pmod 5$, alors il en est de même pour $a^5 - a = a(a-1)(a+1)(a^2+1)$ car l'un de ses facteurs est multiple de 5.
- Si $a \equiv 1 \pmod 5$, alors $a - 1 \equiv 0 \pmod 5$. Le résultat en découle.
- Si $a \equiv 2 \pmod 5$, alors $a - 1 \equiv 1 \pmod 5$, $a + 1 \equiv 3 \pmod 5$ mais

$$a^2 + 1 \equiv 2^2 + 1 \equiv 5 \equiv 0 \pmod 5.$$

- Si $a \equiv 3 \pmod 5$, alors de même

$$a^2 + 1 \equiv 3^2 + 1 \equiv 10 \equiv 0 \pmod 5.$$

- Si $a \equiv 4 \pmod 5$, alors

$$a + 1 \equiv 4 + 1 \equiv 5 \equiv 0 \pmod 5.$$

Dans tous les cas, l'un des facteurs de $a^5 - a$ est un multiple de 5. Remarquez là encore que l'horloge simplifie considérablement les raisonnements.

Vous pouvez montrer seul que $a^7 - a$ est un multiple de 7 pour tout entier a. Il s'agit en réalité de cas particuliers du *petit théorème de Fermat*, affirmant que si p est un nombre premier alors p divise $a^p - a$, ce qui s'écrit $a^p - a \equiv 0 \pmod p$ ou encore, si on considère le signe "$\equiv$" comme une vraie égalité entre nombres,

$$a^p \equiv a \pmod p$$ [27].

Exemple 3 : Prenons un exemple de plus afin de mieux apprécier les congruences. On souhaite démontrer que si $p \geq 5$ est un nombre premier alors 24 divise $p^2 - 1$. C'est curieux, mais comme toujours, une petite expérimentation s'impose :

27. Nous démontrerons ce théorème central plus loin.

p	p^2-1
5	$5^2-1=24=24\cdot 1$
7	$7^2-1=48=24\cdot 2$
11	$11^2-1=120=24\cdot 5$
13	$13^2-1=168=24\cdot 7$
17	$17^2-1=288=24\cdot 12$
19	$19^2-1=360=24\cdot 15$
$\vdots$	$\vdots$

Afin de prouver ce résultat, au lieu de montrer que 24 divise p^2-1, il suffit de montrer que 3 et 8 divisent p^2-1. On pourra alors conclure que $3\cdot 8=24$ divise p^2-1. Attention alors à ce passage subtil, cette implication ne fonctionne que parce que 3 et 8 sont premiers entre eux. On sait par exemple que 3 divise 12 et 6 divise 12 mais pourtant $3\cdot 6=18$ ne divise pas 12. Notre affirmation nécessite donc une démonstration et on aimerait prouver plus généralement que si a et b divisent c et si de plus a et b sont premiers entre eux alors $a\cdot b$ divise c. En effet, c peut s'écrire sous la forme $c=a\cdot k=b\cdot k'$. Puisque a et b sont premiers entre eux, le lemme de Gauss implique que a doit diviser k' ce qui signifie que $k'=a\cdot x$. On en déduit que

$$c=bk'=b(ax)=ab\cdot x.$$

Le résultat en découle. Revenons maintenant à nos moutons, on souhaite d'abord démontrer que $p^2-1\equiv 0 \pmod 3$. On distingue alors 3 cas :

- La congruence $p\equiv 0 \pmod 3$ signifie que 3 divise p, ce qui est impossible car p est un nombre premier différent de 3, donc ne peut pas être divisible par 3.
- Si $p\equiv 1 \pmod 3$ alors $p^2\equiv 1^2\equiv 1 \pmod 3$ et donc $p^2-1\equiv 0 \pmod 3$. Ainsi 3 divise p^2-1.
- Si $p\equiv 2 \pmod 3$ alors $p^2\equiv 2^2\equiv 4\equiv 1 \pmod 3$ et donc $p^2-1\equiv 0 \pmod 3$.

Ainsi, on voit que dans tous les cas, 3 divise p^2-1. Nous démontrons maintenant que 8 divise p^2-1. Nous avons de même plusieurs cas :

- Pour les mêmes raisons, la congruence $p\equiv 0 \pmod 8$ est impossible.
- Si $p\equiv 1 \pmod 8$ alors $p^2\equiv 1^2\equiv 1 \pmod 8$, ce qui implique que $p^2-1\equiv 0 \pmod 8$.
- La congruence $p\equiv 2 \pmod 8$ est impossible car dans ce cas $p=2+8k=2(1+4k)$ et cela signifie que 2 divise p.
- Si $p\equiv 3 \pmod 8$ alors $p^2\equiv 3^2\equiv 9\equiv 1 \pmod 8$. Le résultat en découle.
- La congruence $p\equiv 4 \pmod 8$ est elle aussi impossible, à vous de voir pourquoi.
- Si $p\equiv 5 \pmod 8$ alors $p^2\equiv 5^2\equiv 25\equiv 1 \pmod 8$. Dans ce cas aussi, $p^2-1\equiv 0 \pmod 8$.
- Le cas $p\equiv 6 \pmod 8$ est impossible par primalité de p.
- Le dernier cas $p\equiv 7 \pmod 8$ implique que $p^2\equiv 7^2\equiv 49\equiv 1+8\cdot 6\equiv 1 \pmod 8$.

Ainsi, dans tous les cas 8 divise p^2-1. D'où notre assertion.

Dans nos trois exemples, au lieu de vérifier une infinité de cas (ce qui est impossible) afin de montrer nos résultats, penser dans l'horloge nous a permis de conclure rapidement en vérifiant uniquement un nombre fini de cas. L'idée de réduire nos identités dans une horloge est d'une importance capitale dans la théorie de la divisibilité. Par ailleurs, nous avons utilisé l'addition et la multiplication dans une horloge sans toucher un mot, de leur réelle signification pour notre nouveau symbole " $\equiv$ ", ni pourquoi sont-elles bien définies ? Dans la suite, nous allons répondre à ces questions formellement afin de travailler la conscience tranquille avec notre super outil " $\equiv$ ".

On sait alors que modulo 5, on a les congruences

$$16 \equiv 1 \pmod 5 \quad \text{et} \quad 13 \equiv 3 \pmod 5.$$

On aimerait alors additionner $16 \pmod 5$ et $13 \pmod 5$ mais pour que l'addition soit bien définie il faudrait que cette somme soit égale à $1+3 \pmod 5$. En effet

$$16+13 \equiv 29 \equiv 4 \pmod 5 \quad \text{et} \quad 1+3 \equiv 4 \pmod 5.$$

Ainsi on obtient bien $16+13 \equiv 1+3 \pmod 5$. Plus généralement on souhaite démontrer que si

$$\begin{aligned} a &\equiv b \pmod n \\ c &\equiv d \pmod n, \end{aligned}$$

alors $a+c \equiv b+d \pmod n$. La même question se pose pour la multiplication et on aimerait là aussi avoir $16 \cdot 13 \equiv 1 \cdot 3 \pmod 5$. Je vous laisse vérifier que c'est bien le cas. De façon générale, on souhaite démontrer que sous les mêmes conditions, on a aussi $ac \equiv bd \pmod n$. Commençons tout d'abord par donner une définition rigoureuse de la congruence. En effet, on dit que a est congru à b modulo n et on note

$$a \equiv b \pmod n,$$

si a et b ont même reste de la division euclidienne par n. Cette idée correspond bien à l'idée d'une horloge sur laquelle deux nombres se correspondent s'ils pointent sur une même heure. Nous démontrons dans la suite que d'une façon équivalente, a est congru à b modulo n si et seulement si $a-b$ est un multiple de n. En effet

- Si a et b ont même reste de la division euclidienne par n alors on peut écrire $a = nk+r$ et $b = nk'+r$. Ainsi $a-b = n(k-k')$, qui est bien un multiple de n.
- Réciproquement, si $a-b$ est un multiple de n, alors a et b admettent le même reste dans la division euclidienne par n. En effet, on peut écrire $a = nk+r$ et $b = nk'+r'$ et sans perte de généralité on peut supposer $r' \leq r$. On obtient alors

  $$a-b = n(k-k')+(r-r'),$$

  ce qui implique que $r-r' = (a-b)-n(k-k')$. Puisque $a-b$ est un multiple de n, cette dernière égalité implique que $r-r'$ est divisible par n. Or $0 \leq r < n$ et $0 \leq r' < n$ donc leur différence $0 \leq r-r' < n$. Le seul multiple de n strictement plus petit que n étant 0, on obtient que $r-r' = 0$. D'où notre affirmation.

Revenons à notre histoire d'addition et de multiplication. On souhaite démontrer que si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors

$$a+c \equiv b+d \pmod{n} \quad \text{et} \quad ac \equiv bd \pmod{n}.$$

- Montrer que $a+c \equiv b+d \pmod{n}$ revient à montrer que $(a+c)-(b+d)$ est un multiple de n. En effet

$$(a+c)-(b+d) = \underbrace{(a-b)}_{\in n\mathbb{Z}} + \underbrace{(c-d)}_{\in n\mathbb{Z}}.$$ [28]

  Il s'agit donc de la somme de deux multiples de n, qui par conséquent est un multiple de n. Notez que $a-b$ et $c-d$ sont des multiples de n car par hypothèse $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$.

- De même, montrer que $ac \equiv bd \pmod{n}$ revient à montrer que $ac-bd$ est un multiple de n. On sait que $a-b$ et $c-d$ le sont et on va donc forcer leur apparition dans l'expression $ac-bd$. On commence alors par $a(c-d)+\cdots$ et pour conserver la même expression du départ on doit y rajouter ad. On obtient ainsi

$$ac-bd = a(c-d)+ad-bd = a\underbrace{(c-d)}_{\in n\mathbb{Z}} + d\underbrace{(a-b)}_{\in n\mathbb{Z}}.$$

  On voit ainsi que $ac-bd$ est combinaison de deux multiples de n, donc est un multiple de n. Le résultat en découle.

Dans le cas particulier de $a=c$ et $b=d$ on obtient

$$a^2 \equiv b^2 \pmod{n}.$$

Si on réitère le même procédé, on obtient de même $a^3 \equiv b^3 \pmod{n}$ et plus généralement

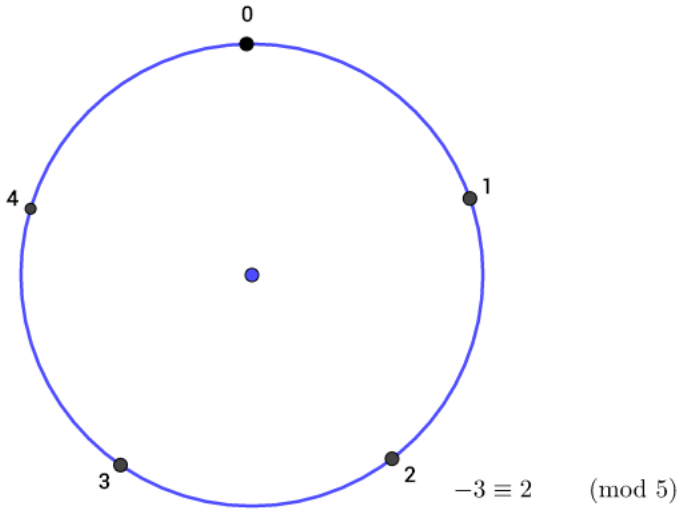
$$a^m \equiv b^m \pmod{n}.$$

Ainsi " $\equiv$ " se comporte comme une vraie égalité, dans laquelle on peut multiplier et donc passer à n'importe quelle puissance entière positive. Toutefois, on verra que certaines opérations sur les congruences se comportent plus subtilement que dans le monde usuel des nombres.

Avant de passer à davantage d'applications de cet outil, tâchons de comprendre et de définir la soustraction sur une horloge. En d'autres mots, quelle est la signification de la congruence $a-b \pmod{n}$? Cela devrait être la même chose que $a+(-b) \pmod{n}$, mais du coup comment peut-on définir l'opposé de $b \pmod{n}$? Sur une horloge de n heures, $-b \pmod{n}$ devrait signifier aller en arrière de b heures dans le sens inverse des aiguilles d'une montre, bien sûr en partant de l'heure 0. Algébriquement, cela veut dire que $-b \pmod{n}$ est l'heure qu'on ajoute à $b \pmod{n}$ afin d'avoir $0 \pmod{n}$.

Un exemple vaut mieux qu'un long discours. Prenons une horloge de 5 heures comme ci-dessous.

28. $n\mathbb{Z}$ signifie l'ensemble des multiples de n.



Reculer de 3 sur cette horloge ou encore considérer l'heure $-3 \pmod 5$ revient à considérer le nombre $2 \pmod 5$ et on voit alors que algébriquement $3+2 \pmod 5 \equiv 0 \pmod 5$. On écrit ainsi

$$-3 \equiv 2 \pmod 5.$$

De même, si on cherche l'opposé de 4 sur une horloge de 7 heures, il s'agit de l'heure qu'on ajoute à 4 afin de tomber sur 0. On voit ainsi que

$$-4 \equiv (7-4) \pmod 7 \equiv 3 \pmod 7.$$

Plus généralement, si $0 \leq b < n$ alors

$$-b \equiv (n-b) \pmod n,$$

car $b+(n-b) \equiv n \equiv 0 \pmod n$ et $n-b > 0$. Passons maintenant à quelques applications concrètes utilisant les congruences.

14.2 Quelques applications

Application 1 : On souhaite savoir si le nombre $6^{2021}-1$ est divisible par 5 et 7 et si ce n'est pas le cas, trouver le reste de la division euclidienne par ces deux entiers. Bien évidemment, il ne s'agit pas ici de calculer ce nombre monstrueux, ni d'effectuer la division euclidienne à la main. Nous utiliserons les propriétés des congruences afin d'y arriver bien plus facilement.

- On sait en effet que dans une horloge de 5 heures on a $6 \equiv 1 \pmod 5$. En élévant de part et d'autre à la puissance 2021 on obtient

$$\begin{aligned} 6^{2021} &\equiv 1^{2021} \pmod 5 \\ &\equiv 1 \pmod 5. \end{aligned}$$

  On en déduit donc que $6^{2021}-1 \equiv 0 \pmod 5$, ce qui signifie que 5 divise $6^{2021}-1$.

- Dans une horloge de 7 heures et pour simplifier le calcul des puissances, on peut écrire que $6 \equiv -1 \pmod 7$. Ainsi on obtient

$$\begin{aligned} 6^{2021} &\equiv (-1)^{2021} \pmod 7 \\ &\equiv -1 \pmod 7, \end{aligned}$$

car 2021 est un entier impair. Il s'ensuit donc que

$$6^{2021} - 1 \equiv -1 - 1 \pmod 7 \equiv -2 \pmod 7 \equiv 5 \pmod 7.$$

On en déduit que 7 ne divise pas $6^{2021} - 1$ et que le reste de sa division euclidienne par 7 vaut 5. Incroyable, quelle puissance !

Remarquer alors que dans les deux cas, on calcule avec le symbole " $\equiv$ " comme avec le signe usuel " $=$ ".

Application 2 : Dans ce deuxième exemple, nous souhaitons calculer le reste de la division euclidienne de 12! par 13. Je vous rappelle que

$$12! = 12 \cdot 11 \cdot 10 \cdots 3 \cdot 2 \cdot 1.$$

Un calcul direct montre que $12! = 479\,001\,600$. En effectuant la division euclidienne de ce nombre par 13 on obtient

$$12! = 36846276 \cdot 13 + 12.$$

Ainsi le reste de la division euclidienne de 12 ! par 13 vaut 12. Imaginez maintenant qu'on ne dispose pas de calculatrice, les congruences vont nous permettre d'arriver au même résultat, avec très peu de travail. En effet,

$$\begin{aligned} 12! &\equiv 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \pmod{13} \\ &\equiv \underbrace{(-1) \cdot (-2) \cdot (-3) \cdot (-4)}_{24} \cdot (-5) \cdot (-6) \cdot 6 \cdot 5 \cdot \underbrace{4 \cdot 3 \cdot 2}_{24} \pmod{13} \\ &\equiv 24 \cdot 24 \cdot 25 \cdot 36 \pmod{13} \\ &\equiv 11 \cdot 11 \cdot 12 \cdot 10 \pmod{13} \\ &\equiv (-2) \cdot (-2) \cdot (-1) \cdot (-3) \pmod{13} \\ &\equiv 12 \pmod{13}. \end{aligned}$$

Voilà donc sans beaucoup de peine.

Application 3 : On souhaite trouver le reste de la division euclidienne de 2^{2021} par 11. Pour se faire, commençons par calculer quelques petites puissances de 2 modulo 11.

n	2^n
2	$2^2 \equiv 4 \pmod{11}$
3	$2^3 \equiv 8 \pmod{11}$
4	$2^4 \equiv 16 \equiv 5 \pmod{11}$
5	$2^5 \equiv 2^4 \cdot 2 \equiv 5 \cdot 2 \equiv 10 \pmod{11}$
6	$2^6 \equiv 2^5 \cdot 2 \equiv 10 \cdot 2 \equiv 9 \pmod{11}$
7	$2^7 \equiv 2^6 \cdot 2 \equiv 9 \cdot 2 \equiv 7 \pmod{11}$
8	$2^8 \equiv 2^7 \cdot 2 \equiv 7 \cdot 2 \equiv 3 \pmod{11}$
9	$2^9 \equiv 2^8 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \pmod{11}$
10	$2^{10} \equiv 2^9 \cdot 2 \equiv 6 \cdot 2 \equiv 1 \pmod{11}$

Bingo ! On a donc obtenu une puissance de 2 qui donne 1 (mod 11), à savoir

$$2^{10} \equiv 1 \pmod{11}.$$

Remarquez alors qu'on aurait pu obtenir ce résultat en remarquant que $2^5 \equiv 10 \equiv -1 \pmod{11}$ et donc en élévant au carré on obtient

$$(2^5)^2 \equiv (-1)^2 \equiv 1 \pmod{11}.$$

Par ailleurs, $2021 = 202 \cdot 10 + 1$, ceci implique que

$$\begin{aligned} 2^{2021} &\equiv 2^{202\cdot 10+1} \pmod{11} \\ &\equiv \left(2^{10}\right)^{202} \cdot 2^1 \pmod{11} \\ &\equiv 1^{202} \cdot 2 \pmod{11} \\ &\equiv 2 \pmod{11}. \end{aligned}$$

Ainsi, le reste de la division euclidienne de 2^{2021} par 11 vaut 2. Le secret de cette recette est l'existence d'une puissance de 2 égale à 1 modulo 11, car il est trivial de calculer les puissances de 1.

Application 4 : (À la chasse des 9) Le critère de divisibilité par 9 sert aussi à vérifier l'exactitude des grands calculs de façon relativement rapide, sans devoir les répéter. Prenons par exemple le calcul

$$4027 \cdot 45 = 181215.$$

On aimerait savoir si ce calcul est plutôt bon ou pas. La méthode de la chasse des 9 repose sur le fait que dans une horloge de 9 heures, un nombre pointe sur la somme de ses chiffres. En effet, si on prend un nombre à 4 chiffres de la forme ABCD, on peut l'écrire sous la forme

$$ABCD = A \cdot 10^3 + B \cdot 10^2 + C \cdot 10 + D.$$

Par exemple on a $9425 = 9 \cdot 10^3 + 4 \cdot 10^2 + 2 \cdot 10 + 5$. Or on sait que $10 \equiv 1 \pmod{9}$, ce qui implique que $10^n \equiv 1^n \equiv 1 \pmod{9}$. On obtient ainsi

$$\begin{aligned} 9425 &= 9 \cdot 10^3 + 4 \cdot 10^2 + 2 \cdot 10 + 5 \\ &\equiv 9 \cdot 1 + 4 \cdot 1 + 2 \cdot 1 + 5 \pmod{9} \\ &\equiv 9 + 4 + 2 + 5 \pmod{9}. \end{aligned}$$

Ainsi, 9425 est congru à la somme de ses chiffres modulo 9. De même

$$\begin{aligned} ABCD &= A \cdot 10^3 + B \cdot 10^2 + C \cdot 10 + D \\ &\equiv A \cdot 1 + B \cdot 1 + C \cdot 1 + D \pmod{9} \\ &\equiv A + B + C + D \pmod{9}. \end{aligned}$$

Pour les sceptiques, on peut vérifier à la main que pour les premières valeurs de n, $10^n \equiv 1 \pmod{9}$. En effet,

$$10^2 = 100 = 99 + 1 \equiv 9 \cdot 11 + 1 \pmod{9} \equiv 1 \pmod{9}.$$

De même, $10^3 = 1000 = 999 + 1 \equiv 1 \pmod 9$ car 999 pointe sur 0 sur une horloge de 9 heures. Revenons à notre opération du départ $4027 \cdot 45 = 181215$. En réduisant modulo 9, on obtient

$$\begin{aligned} 4027 \cdot 45 &\equiv (4+0+2+7) \cdot (4+5) \pmod 9 \\ &\equiv 13 \cdot 9 \pmod 9 \\ &\equiv 0 \pmod 9. \end{aligned}$$

Maintenant si $181215 \equiv 0 \pmod 9$ alors on peut espérer que notre calcul est bon. En effet

$$\begin{aligned} 181215 &\equiv 1+8+1+2+1+5 \pmod 9 \\ &\equiv 18 \pmod 9 \\ &\equiv 0 \pmod 9. \end{aligned}$$

Bingo ! Toutefois, je tiens à vous mettre en garde, cette méthode ne garantit pas l'exactitude des calculs, mais elle indique seulement si le calcul est plutôt bon ou pas. Pour s'en convaincre, prenons le calcul

$$12527 \cdot 35 = 438436.$$

D'une part,

$$\begin{aligned} 12527 \cdot 35 &\equiv (1+2+5+2+7) \cdot (3+5) \pmod 9 \\ &\equiv 17 \cdot 8 \pmod 9 \\ &\equiv 8 \cdot 8 \pmod 9 \\ &\equiv (-1) \cdot (-1) \pmod 9 \\ &\equiv 1 \pmod 9. \end{aligned}$$

D'autre part,

$$\begin{aligned} 438436 &\equiv 4+3+8+4+\underbrace{3+6}_{0} \pmod 9 \\ &\equiv 19 \pmod 9 \\ &\equiv 1 \pmod 9. \end{aligned}$$

On voit ainsi que les deux membres donnent le même résultat et pourtant $12527 \cdot 35 \neq 438436$. En d'autres mots, cela signifie

$$12527 \cdot 35 \equiv 438436 \pmod 9 \not\Rightarrow 12527 \cdot 35 = 438436.$$

Je vous laisse alors vérifier que le bon résultat est $12527 \cdot 35 = 438445$.

Application 5 : Il est relativement facile de reconnaître un multiple de 2 car ces nombres se terminent par 0, 2, 4, 6 ou 8. Il est tout aussi facile de reconnaître un multiple de 5 car là encore le chiffre des unités vaut 0 ou 5. Comment peut-on alors reconnaître un multiple de 11 ? En effet, un nombre n est divisible par 11 si la somme alternée de ses chiffres est divisible par 11. Par exemple, un nombre de la forme ABCD est divisible par 11 si $D - C + B - A$ est divisible par 11. Le mot "alternée" signifie donc qu'on alterne les signe $+$ et $-$. Par exemple si $n = 52118$ alors la somme alternée de ses chiffres vaut $8 - 1 + 1 - 2 + 5 = 11 \equiv 0 \pmod{11}$. On peut donc conclure que n est un multiple de 11. Rien de plus facile, n'est-ce

pas ? Ce résultat fonctionne car si par exemple n est de la forme ABCD alors là encore la décomposition de ce nombre en base 10 s'écrit $ABCD = A\cdot 10^3 + B\cdot 10^2 + C\cdot 10 + D$. Or $10 \equiv -1 \pmod{11}$ ce qui implique que $10^n \equiv (-1)^n \pmod{11}$. En particulier, $10^3 \equiv (-1) \pmod{11}$ et $10^2 \equiv 1 \pmod{11}$, ainsi

$$\begin{aligned} ABCD &= A\cdot 10^3 + B\cdot 10^2 + C\cdot 10 + D \\ &\equiv A\cdot(-1) + B\cdot 1 + C\cdot(-1) + D \pmod{11} \\ &\equiv -A + B - C + D \pmod{11}. \end{aligned}$$

Cette petite preuve se généralise trivialement à n'importe quel entier. On remarque alors que les critères de divisibilité sont des moyens très efficaces pour déterminer si un entier est multiple d'un autre, sans passer par exemple par la division euclidienne, on voit à titre d'exemple que la division de 52118 par 11 est plus pénible que le calcul de la somme alternée de ses chiffres, d'où l'efficacité.

Application 6 : Les congruences ont été introduites par Gauss afin de pouvoir trouver les solutions entières d'équations polynomiales connues sous le nom d'équations diophantiennes. Regardons ensemble le fonctionnement des congruences sur une équation diophantienne particulière. On aimerait montrer que l'équation $x^2 - 7y^3 = 3$ n'admet pas de solutions entières. Autrement dit, il n'existe aucun couple d'entiers (x, y) vérifiant cette égalité. En effet, si $x^2 - 7y^3 = 3$ alors dans une horloge de 7 heures cette équation devient $x^2 - \underbrace{7y^3}_{0} \equiv 3 \pmod{7}$, ou encore $x^2 \equiv 3 \pmod{7}$. Tout ce qu'il nous reste à faire est de prouver que la congruence $x^2 \equiv 3 \pmod{7}$ est impossible. Les congruences sont forts sympathiques car elle réduisent le travail à un nombre fini de cas, relativement facile à vérifier. En effet

- Si $x \equiv 0 \pmod{7}$ alors $x^2 \equiv 0^2 \equiv 0 \pmod{7} \not\equiv 3 \pmod{7}$.
- Si $x \equiv 1 \pmod{7}$ alors $x^2 \equiv 1^2 \equiv 1 \pmod{7} \not\equiv 3 \pmod{7}$.
- Si $x \equiv 2 \pmod{7}$ alors $x^2 \equiv 2^2 \equiv 4 \pmod{7} \not\equiv 3 \pmod{7}$.
- Si $x \equiv 3 \pmod{7}$ alors $x^2 \equiv 3^2 \equiv 9 \equiv 2 \pmod{7} \not\equiv 3 \pmod{7}$.
- Si $x \equiv 4 \pmod{7}$ alors $x^2 \equiv 4^2 \equiv 16 \equiv 2 \pmod{7} \not\equiv 3 \pmod{7}$.
- Si $x \equiv 5 \pmod{7}$ alors $x^2 \equiv 5^2 \equiv 25 \equiv 4 \pmod{7} \not\equiv 3 \pmod{7}$.
- Si $x \equiv 6 \pmod{7}$ alors $x^2 \equiv 6^2 \equiv 36 \equiv 1 \pmod{7} \not\equiv 3 \pmod{7}$.

Ainsi, dans tous les cas $x^2 \not\equiv 3 \pmod{7}$! Avouons-le, c'est d'une incroyable ingéniosité !

14.3 Une propriété utile chez les congruences

Dans le monde des nombres réels, quand on dispose d'une égalité de la forme $a\cdot b = a\cdot c$ et si de plus $a \neq 0$ alors on peut simplifier par a

$$\not{a}\cdot b = \not{a}\cdot c$$

et affirmer que $b = c$. Cette simplification fonctionne dans $\mathbb{R}$ car $ab = ac$ implique que $ab - ac = 0$ ou encore $a(b-c) = 0$. Or si le produit de deux nombres réels est nul alors l'un

des facteurs est nul. Autrement dit si $xy = 0$ alors $x = 0$ ou $y = 0$. Puisque dans notre cas $a \neq 0$, on en déduit que $b - c = 0$, c'est-à-dire $b = c$.

Les choses se passent moins bien pour les congruences car si $a \cdot b \equiv 0 \pmod{n}$ alors rien ne garantit que $a \equiv 0 \pmod{n}$ ou $b \equiv 0 \pmod{n}$. Par exemple, dans une horloge de 6 heures, $2 \not\equiv 0 \pmod{6}$, $3 \not\equiv 0 \pmod{6}$ et pourtant $2 \cdot 3 \equiv 0 \pmod{6}$. Ainsi on a deux nombres non nuls sur l'horloge dont le produit est nul. Pas de chance ! On aimerait alors savoir à quelle condition peut-on simplifier de part et d'autre dans une congruence ? En d'autres termes, si $a \cdot b \equiv a \cdot c \pmod{n}$, quand peut-on dire que $b \equiv c \pmod{n}$? Regardons ce qui se passe sur un exemple concret. On peut facilement vérifier que

$$2 \cdot 7 \equiv 2 \cdot 3 \pmod{8} \quad \text{car} \quad 14 \equiv 6 \pmod{8}.$$

Toutefois, on ne peut pas simplifier par 2 car cela impliquerait la congruence $7 \equiv 3 \pmod{8}$, ce qui est évidemment faux. On vérifie de même que $5 \cdot 3 \equiv 5 \cdot 11 \pmod{8}$ car 15 et 55 pointent tous les deux sur 7 (mod 8). Dans ce cas, la simplification par 5 s'effectue correctement, car on a bien $3 \equiv 11 \pmod{8}$. On remarque alors que la simplification fonctionne, mais pas dans tous les cas ! Nous allons démontrer alors que

$$\text{Si } ab \equiv ac \pmod{n} \text{ et si } (a,n) = 1 \text{ [29] alors } b = c \pmod{n}.$$

Pour se faire, nous démontrerons un résultat un peu plus général affirmant que si $ab \equiv ac \pmod{n}$ alors

$$b \equiv c \pmod{n/(a,n)}.$$

En effet, $ab \equiv ac \pmod{n}$ implique que $a(b-c) \equiv 0 \pmod{n}$. En particulier n divise $a(b-c)$ et on a un entier k pour lequel $a(b-c) = n \cdot k$. Notons $d = (a,n)$, on peut alors écrire $a = d \cdot a'$ et $n = d \cdot n'$, où a' et n' sont deux entiers premiers entre eux [30]. L'égalité $a(b-c) = n \cdot k$ s'écrit alors

$$da'(b-c) = dn'k,$$

ou encore $a'(b-c) = n'k$. Ainsi, $n' = n/(a,n)$ divise $a'(b-c)$, le lemme de Gauss permet alors d'affirmer que $n/(a,n)$ divise $b-c$, ou encore que

$$b - c \equiv 0 \pmod{n/(a,n)}.$$

Le résultat en découle. Cette propriété de simplification chez les congruences a des conséquences importantes. Par exemple si n est un nombre premier alors la condition $a \not\equiv 0 \pmod{n}$ implique que $(a,n) = 1$. Dans ce cas, si $ab \equiv ac \pmod{n}$ et $a \not\equiv 0 \pmod{n}$, on peut directement conclure que $b \equiv c \pmod{n}$. C'est surprenant car cela signifie qu'une horloge contenant un nombre d'heures premier se comporte comme le monde des réels pour l'opération de la simplification. De surcroît, si n est premier alors

$$ab \equiv 0 \pmod{n} \Longrightarrow a \equiv 0 \pmod{n} \quad \text{ou} \quad b \equiv 0 \pmod{n}.$$

Incroyable surprise ! Les nombres premiers font de l'horloge un endroit privilégié pour y conduire des calculs sur la divisibilité ! Ce résultat se justifie rapidement car $ab \equiv 0 \pmod{n}$ s'écrit aussi $ab \equiv a \cdot 0 \pmod{n}$. Donc si $a \not\equiv 0 \pmod{n}$ alors on peut simplifier par a pour

29. Je vous rappelle que (a,n) signifie le pgcd de a et de n.
30. Les entiers n' et a' ne peuvent pas partager un diviseur différent de 1 car d est le plus grand diviseur en commun entre a et n.

obtenir $b \equiv 0 \pmod{n}$. Passons maintenant sur le terrain et regardons ce que cela donne avec des équations modulaires.

Exemple 1 : On souhaite résoudre l'équation $x^2 \equiv 4 \pmod 7$. Une solution évidente est $x = 2 \pmod 7$ car $2^2 \equiv 4 \pmod 7$. Cette équation admet une deuxième solution qu'on peut trouver en essayant toutes les valeurs modulo 7. Cette méthode fonctionne bien quand l'horloge contient peu d'heures mais si $n = 53$ par exemple, alors les vérifications deviennent longues et pénibles. Plutôt que d'appliquer cette méthode, nous allons utiliser la propriété de simplification chez les nombres premiers. En effet,

$$\begin{aligned} x^2 \equiv 4 \pmod 7 &\Longrightarrow x^2 - 2^2 \equiv 0 \pmod 7 \\ &\Longrightarrow (x-2)(x+2) \equiv 0 \pmod 7 \\ &\Longrightarrow x-2 \equiv 0 \pmod 7 \quad \text{ou} \quad x+2 \equiv 0 \pmod 7 \\ &\Longrightarrow x \equiv 2 \pmod 7 \quad \text{ou} \quad x \equiv -2 \equiv 5 \pmod 7. \end{aligned}$$

On vérifie alors aisément que $5^2 \equiv 25 \equiv 4 \pmod 7$ et $5 \pmod 7$ est bien solution de notre équation $x^2 \equiv 4 \pmod 7$.

Exemple 2 : Dans cet exemple, on souhaite résoudre l'équation $x^2 \equiv 16 \pmod{53}$. Une solution évidente est $x \equiv 4 \pmod{53}$. Comme je viens de le préciser, il serait bien pénible de vérifier le carré de chacune des horloges dans ce cas et nous allons donc procéder comme ci-dessus. En effet, 53 est un nombre premier, donc

$$\begin{aligned} x^2 \equiv 16 \pmod{53} &\Longrightarrow x^2 - 4^2 \equiv 0 \pmod{53} \\ &\Longrightarrow (x-4)(x+4) \equiv 0 \pmod{53} \\ &\Longrightarrow x-4 \equiv 0 \pmod{53} \quad \text{ou} \quad x+4 \equiv 0 \pmod{53} \\ &\Longrightarrow x \equiv 4 \pmod{53} \quad \text{ou} \quad x \equiv -4 \equiv 49 \pmod{53}. \end{aligned}$$

On peut alors vérifier que réciproquement, on a bien $49^2 \equiv 16 \pmod{53}$. On aurait pu voir directement que $-4 \pmod{53}$ est solution de notre équation car $(-4)^2 \equiv 4^2 \equiv 16 \pmod{53}$. Notez alors que notre méthode dit aussi que 4 et (-4) sont non seulement solutions mais il s'agit des seules solutions modulo 53.

15 Le petit théorème de Fermat

Nous sommes maintenant à même de comprendre le premier théorème non-trivial sur les congruences, à savoir *le petit théorème de Fermat*. Ce théorème central en arithmétique affirme que si p est un nombre premier alors p doit diviser $a^p - a$ pour tout entier a. Dans le monde des congruences, cet énoncé dit que $a^p - a \equiv 0 \pmod p$ ou encore que

$$a^p \equiv a \pmod p.$$

Je vous rappelle alors qu'on a démontré ce résultat dans les cas particuliers de $p = 3$ et $p = 5$ en factorisant les expressions $a^3 - a = a(a-1)(a+1)$ et $a^5 - a = a(a-1)(a+1)(a^2+1)$. Il n'est pas alors évident comment généraliser cette idée à tout nombre premier p. Nous verrons dans cette section un point de vue différent permettant d'aboutir au résultat général.

Avant de nous plonger dans les détails techniques de ce théorème, tâchons de savoir un peu plus sur son histoire. Il paraît que Fermat a découvert son théorème en investiguant **les nombres parfaits**, ce qui nous renvoie à l'antiquité. Un entier naturel est dit parfait s'il est la somme de tous ses diviseurs sauf lui-même. Le premier nombre parfait est 6 car ses diviseurs (sauf lui-même) sont 1, 2 et 3 et on a bien

$$6 = 1 + 2 + 3.$$

Le deuxième nombre parfait est 28 car ses diviseurs, là encore sauf lui-même, sont 1, 2, 4, 7 et 14 et on peut vérifier facilement que

$$28 = 1 + 2 + 4 + 7 + 14.$$

Nos ancêtres donnaient des significations mystiques à de tels nombres et l'on peut lire dans Saint Augustin "La cité de Dieu" :

"Six est un nombre parfait en lui même, non parce que Dieu a créé toutes choses en six jours, mais Dieu a créé toutes choses en six jours parce que ce nombre est parfait."

Les nombres parfaits font leur apparition aussi dans l'oeuvre d'Euclide dans laquelle il donne une formule permettant de les générer. En effet, le nombre N donné par

$$N = 2^{n-1}(2^n - 1)$$

est parfait si $p = 2^n - 1$ est premier. D'ailleurs, il s'agit de la seule façon connue à ce jour pour produire des nombres parfaits et l'on verra qu'Euler a démontré que tout nombre parfait pair est de la forme euclidienne. Puisque p est premier, les diviseurs de N sont

$$1, 2, 2^2, 2^3, \ldots, 2^{n-1} \quad \text{et} \quad p, 2p, 2^2p, 2^3p, \ldots, 2^{n-1}p = N.$$

Ceci implique que la somme des diviseurs de N, sauf lui-même, vaut

$$\begin{aligned}
\underbrace{1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1}}_{\text{somme géométrique}} + p + 2p + 2^2p + \cdots + 2^{n-2}p &= \frac{2^n - 1}{2 - 1} + \underbrace{(1 + 2 + \cdots + 2^{n-2})}_{\text{somme géométrique}} p \\
&= \underbrace{2^n - 1}_{=p} + \frac{2^{n-1} - 1}{2 - 1} p \\
&= p + \underbrace{2^{n-1}p}_{=N} - p \\
&= N.
\end{aligned}$$

Cela montre donc que N est parfait quand p est un nombre premier. Ainsi, afin de trouver des nombres parfaits, il suffit de trouver des nombres premiers de la forme 2^n-1, ce qui n'est pas tâche facile. Les nombres premiers de cette forme sont appelés les nombres premiers de notre ancêtre Mersenne. Les premières valeurs de n pour lesquelles p est premier et N est parfait sont données dans le tableau suivant

n	p	N
2	$2^2-1=3$	$2^{2-1}\cdot 3=6$
3	$2^3-1=7$	$2^{3-1}\cdot 7=28$
5	$2^5-1=31$	$2^{5-1}\cdot 31=496$
7	$2^7-1=127$	$2^{7-1}\cdot 127=8128$
$\vdots$	$\vdots$	$\vdots$

Notez alors que tous les nombres premiers parfaits de la forme euclidienne sont pairs et à ce jour personne n'a trouvé un nombre parfait impair. On pense d'ailleurs qu'il n'en existe pas. Je vous mets alors en garde, si n est premier 2^n-1 ne l'est pas forcément. Trop beau pour que ce soit vrai. Par exemple si $n=11$, $2^{11}-1=2047$ est divisible par 23. Toutefois, si 2^n-1 est premier alors n est forcément premier. Cela signifie que pour chercher les nombres premiers de la forme 2^n-1, inutile de s'intéresser aux nombres n composés. En effet, si $n=ab$ avec $1<a\leq b<n$ alors 2^a-1 est un diviseur non-trivial [31] de $2^{ab}-1=2^n-1$. Pour le voir, il suffit de remarquer que $2^a-1\equiv 0 \pmod{2^a-1}$, ce qui s'écrit

$$2^a\equiv 1 \pmod{2^a-1}.$$

En élévant de part et d'autre à la puissance b on obtient $(2^a)^b\equiv 1^b \pmod{2^a-1}$ ou encore

$$2^{ab}\equiv 1 \pmod{2^a-1}.$$

Ainsi $2^n-1\equiv 0 \pmod{2^a-1}$. On peut arriver au même résultat en remarquant l'identité

$$x^b-y^b=(x-y)(x^{b-1}+x^{b-2}y+x^{b-3}y^2+\cdots+y^{b-1}).$$

Il suffit alors de l'appliquer à $x=2^a$ et $y=1$.

En 1640, Bernard Frénicle de Bessy a demandé à Pierre de Fermat de trouver un nombre parfait $10^{20}<N<10^{22}$. La seule forme de nombres parfaits étant la forme euclidienne, cette question est équivalente à trouver un nombre n tel que

$$10^{20}<2^{n-1}(2^n-1)<10^{22}.$$

L'entier n doit être compris entre 34 et 37. Pour le voir, on peut écrire

$$\begin{aligned}2^{n-1}(2^n-1)&=2^{n-1}2^n-2^{n-1}\\&=2^{2n-1}-2^{n-1}\\&<2^{2n-1}.\end{aligned}$$

Ainsi, pour avoir $2^{n-1}(2^n-1)<10^{22}$, il suffit d'avoir $2^{2n-1}<10^{22}$ ou encore

$$n\leq E\left(\frac{\frac{22\ln(10)}{\ln(2)}+1}{2}\right)=37,$$

31. Diviseur non-trivial de n signifie un diviseur différent de 1 et de n.

où E désigne la partie entière d'un nombre. Pour la deuxième inégalité, il suffit de voir que

$$2^{n-1}(2^n-1) > 2^{n-1}(2^n-2^{n-2}) = 2^{n-1}\cdot 2^{n-2}(2^2-1) = 3\cdot 2^{2n-3}.$$

Donc pour avoir $2^{n-1}(2^n-1) > 10^{20}$, il suffit d'avoir $3\cdot 2^{2n-3} > 10^{20}$ ou encore

$$n \geq E\left(\frac{\frac{20\ln(10)-\ln(3)}{\ln(2)}+3}{2}\right)+1 = 34.$$

Pour résumer, ce qu'on a montré ici c'est que si $34 \leq n \leq 37$ alors

$$10^{20} < 2^{n-1}(2^n-1) < 10^{22}.$$

En réalité, les deux assertions sont équivalentes car si on essaie l'expression au milieu des inégalités avec $n = 33$ ou $n = 38$, on voit qu'on dépasse de part et d'autre notre plage de nombres.

Je vous rappelle que Fermat était à la recherche d'un nombre $34 \leq n \leq 37$ tel que $p = 2^n - 1$ soit premier. Puisqu'on ne peut pas prendre n composé, le seul bon candidat est $n = 37$. La question difficile maintenant est de décider si $2^{37}-1$ est bien premier. Fermat démontre alors qu'il est divisible par 223 et on a

$$\begin{aligned} 2^{37}-1 &= 137438953471 \\ &= 223\cdot 616318177. \end{aligned}$$

Ne me dites pas que tout va bien ! Comment Fermat a-t-il pu voir que ce nombre est divisible par 223 ? Pour se faire, notre éminent savant utilise une conséquence directe de son petit théorème affirmant que

si n est un nombre premier et p un nombre premier diviseur de 2^n-1 alors $p-1$ est un multiple de n.

Dans le monde des congruences, cela se traduit par si $2^n - 1 \equiv 0 \pmod{p}$ alors $p \equiv 1 \pmod{n}$. Avant de voir une preuve de cette proposition, tâchons de comprendre comment elle sert à factoriser $2^{37}-1$. Si p est un nombre premier divisant $2^{37}-1$ alors d'après la proposition ci-dessus, 37 doit diviser $p-1$, auquel cas $p-1 = 37k$. Or $p-1$ est un nombre pair car p est impair puisqu'il divise un nombre impair. On en déduit que

$$p-1 = 37k = 37\cdot 2\cdot k' = 74k'.$$

En résumé, si p divise $2^{37}-1$ alors il doit être de la forme $74k+1$. Il suffit maintenant de prendre quelques valeurs de k et vérifier si le nombre obtenu divise bien $2^{37}-1$.

- Si $k = 1$ alors $p = 75$, or 75 n'est pas un nombre premier.
- Si $k = 2$ alors $p = 149$ qui est bien premier. Toutefois, la division euclidienne de $2^{37}-1$ par 149 donne
$$2^{37}-1 = 149\cdot 922409083 + 104.$$
- Maintenant si on prend $k = 3$, on obtient le nombre premier $p = 223$ et la bonne décomposition.

À titre personnel, je trouve cette méthode d'une ingéniosité incroyable, qu'en dites-vous ?

Une erreur de Fermat : Pierre de Fermat a voulu factoriser les nombres de la forme $a^{2n}-1$. On remarque tout d'abord que

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

Ceci conduit notre ancêtre à chercher la factorisation de a^n+1. En particulier, si $a=2$, il s'est demandé quand 2^n+1 produit-elle un nombre premier ? Notez alors que si n admet un diviseur $d>1$ impair alors 2^n+1 ne peut pas être premier. En effet, on peut écrire

$$\begin{aligned}2^n+1&=2^{dk}+1\\&=(2^k)^d-(-1)^d\\&=(2^k-(-1))(\cdots).\end{aligned}$$

Ainsi 2^n+1 est divisible par $2^k+1>1$. Donc pour que 2^n+1 soit un nombre premier, n ne peut pas contenir un diviseur impair >1. On en déduit que n est une puissance de 2 et s'écrit donc sous la forme $n=2^m$. Dans ce cas, on obtient

$$2^n+1=2^{2^m}+1=F_m,$$

et l'on reconnaît ici les fameux nombres de Fermat. Nous avons vu que ces nombres sont tous premiers entre eux mais qu'ils ne sont pas tous premiers. Fermat a conjecturé leur primalité mais Euler l'a refuté en montrant que F_5 est divisible par 641. Ce qui est surprenant, la preuve de la non-primalité de F_5 n'était pas au dessus des capacités techniques de Fermat. En effet, afin de trouver 641, Euler utilise la procédure de Fermat et affirme que les diviseurs premiers de $2^{32}+1$ sont de la forme $p=64k+1$, ce qui donne les candidats 193, 257, 449, 577 et 641. On pense alors que Fermat a effectué la division euclidienne de $2^{32}+1$ par 641 mais qu'au passage il a fait une erreur de calcul sans s'en rendre compte.

Revenons maintenant au petit théorème de Fermat. Je vous rappelle que notre savant était à la recherche de diviseurs premiers des nombres de la forme 2^n-1. Naivement, on peut essayer tous les nombres premiers en dessous de $\sqrt{2^n-1}$ [32]. Si $n=37$, on a

$$\sqrt{2^{37}-1}\simeq 370727 \quad \text{et} \quad \pi(370727)=31579,$$

où $\pi(x)$ désigne le nombre de nombres premiers en dessous d'un nombre x. On voit alors que si on manque de chance, on peut passer énormément de temps à chercher un diviseur premier de $2^{37}-1$. L'idée géniale du grand Fermat était de tourner la question autrement. Au lieu de chercher les diviseurs premiers p de 2^n-1 pour un n fixé, il fixait un nombre premier p et regardait pour quels entiers n a-t-on

$$2^n\equiv 1 \pmod p.$$

L'arithmétique est basée sur l'expérimentation, regardons donc ce qui se passe quand $p=17$. Nous allons chercher le premier exposant [33] strictement positif pour lequel la puissance correspondante de 2 est congru à 1 modulo 17. On peut faire cela à la main pour se rendre

32. J'utilise ici le fait que si n est composé alors son plus petit diviseur premier est plus petit que $\sqrt{n}$. Donc si aucun nombre premier $\leq\sqrt{n}$ ne divise n, alors on peut affirmer que n est premier. Je vous laisse le soin de démontrer ce petit résultat.

33. S'il existe.

compte de la mécanique sous-jacente au calcul sur les congruences [34], mais nous allons utiliser un petit algorithme écrit en Python permettant de calculer les puissances de n'importe quel entier a modulo un entier p.

```
def power(a, p):
    power_lst = [1]
    for i in range(1, p):
        x = power_lst[i - 1]*a % p
        power_lst.append(x)
    return power_lst
```

La liste power_lst contiendra donc les p premières puissances de a modulo p. En effectuant l'exécution avec $a = 2$ et $p = 17$ on obtient

```
>>> power(2,17)
[1, 2, 4, 8, 16, 15, 13, 9, 1, 2, 4, 8, 16, 15, 13, 9, 1]
```

On voit alors que la première puissance de 2, dont l'exposant est non nul et donnant 1 modulo 17 est d'exposant égal à 8. Par conséquent

$$2^8 \equiv 1 \pmod{17}.$$

En exécutant notre algorithme avec $a = 3$ et $p = 17$ on obtient la liste

```
>>> power(3, 17)
[1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1]
```

Dans ce cas, 16 est le plus petit exposant non nul dont la puissance de 3 correspondante donne 1 modulo 17 et on a $3^{16} \equiv 1 \pmod{17}$. Notez alors que ce résultat ressemble au petit théorème de Fermat, car en multipliant cette dernière congruence par 3 on obtient bien $3^{17} \equiv 3 \pmod{17}$. Maintenant en prenant $a = 4$ et $p = 17$ on obtient la liste

```
>>> power(4, 17)
[1, 4, 16, 13, 1, 4, 16, 13, 1, 4, 16, 13, 1, 4, 16, 13, 1]
```

.

On voit alors que la liste des puissances est répétitive, dès qu'on tombe sur 1, on retombe après sur 4, 16, 13 puis encore 1. Ce phénomène est tout à fait normal et je vous le laisse en exercice. Il se passe davantage de choses sur une horloge et je vous invite à aller sur Python, afin d'en découvrir par vous-même. Un dernier constat à voir ici et qui a été utilisé par Fermat est que a^{p-1} pointe toujours sur 1 sur une horloge de p heures, sauf si a pointe sur 0 et que $p-1$ est multiple du plus petit exposant non nul donnant une puissance de a congru à $1 \pmod{p}$. Par exemple, pour $a = 2$ et $p = 17$, ce plus petit exposant vaut 8 et on a bien $16 = p-1 = 8 \cdot 2$. Allez, soyons fou et prenons un autre nombre premier. Si $a = 5$ et $p = 13$, la liste des puissances successives de 5 modulo 13 est

```
>>> power(5, 13)
[1, 5, 12, 8, 1, 5, 12, 8, 1, 5, 12, 8, 1]
```

Le plus petit exposant non nul n donnant $5^n \equiv 1 \pmod{13}$ vaut 4 et on a bien $12 = p-1 = 4 \cdot 3$. C'est fou, non ? En réalité, il est facile de voir pourquoi si $a \not\equiv 0 \pmod{p}$ alors il existe toujours une puissance de a égale à $1 \pmod{p}$. En effet, les puissances successives donnent

34. Je vous conseille de le faire d'abord à la main.

des restes modulo p. Puisqu'il n'existe qu'un nombre fini de restes possibles, il existe deux entiers $n > m$ tels que

$$a^n \equiv a^m \pmod{p}.$$

En particulier, $a^{n-m} \equiv 1 \pmod{p}$ [35]. On aimerait montrer maintenant que si $d \neq 0$ est le plus petit exposant vérifiant $a^d \equiv 1 \pmod{p}$ alors d doit diviser $p-1$. D'après le petit théorème de Fermat (qu'on n'a pas encore démontré), si $a \not\equiv 0 \pmod{p}$ alors $a^{p-1} \equiv 1 \pmod{p}$. La division euclidienne de $p-1$ par d nous fournit deux entiers q et r tels que $p-1 = d \cdot q + r$ et $0 \leq r < d$. On souhaite alors montrer que $r = 0$. En effet,

$$\begin{aligned} a^{p-1} &\equiv a^{dq+r} \pmod{p} \\ &\equiv (a^d)^q a^r \pmod{p} \\ &\equiv 1^q a^r \pmod{p} \\ &\equiv a^r \pmod{p}. \end{aligned}$$

Ainsi, $a^r \equiv 1 \pmod{p}$ et puisque d est le plus entier naturel non nul vérifiant cette propriété, l'inégalité $r < d$ implique que $r = 0$. Cela démontre donc au passage la proposition utilisée par Fermat pour factoriser $2^{37} - 1$.

Avant de démontrer notre théorème, tâchons de comprendre un dernier phénomène sur une horloge de p heures, où p désigne toujours un nombre premier. Si $a \not\equiv 0 \pmod{p}$ alors en multipliant a par toutes les heures de l'horloge, sauf 0, on obtient là encore toutes les heures de notre horloge. Un exemple vaut mieux qu'un long discours. Prenons $p = 7$ et $a = 5$, en multipliant a par les heures, de 1 à 6 on obtient le tableau suivant

n	$a \cdot n \pmod{p}$
1	$a \cdot 1 \equiv 5 \cdot 1 \equiv 5 \pmod{7}$
2	$a \cdot 2 \equiv 5 \cdot 2 \equiv 3 \pmod{7}$
3	$a \cdot 3 \equiv 5 \cdot 3 \equiv 1 \pmod{7}$
4	$a \cdot 4 \equiv 5 \cdot 4 \equiv 6 \pmod{7}$
5	$a \cdot 5 \equiv 5 \cdot 5 \equiv 4 \pmod{7}$
6	$a \cdot 6 \equiv 5 \cdot 6 \equiv 2 \pmod{7}$

On remarque alors que $5 \cdot n \pmod{7}$ est une permutation des heures sur notre horloge, sans que deux heures différentes donnent la même heure en appliquant la formule $5 \cdot n \pmod{7}$. Ce phénomène est vrai pour tout nombre premier p et tout $a \not\equiv 0 \pmod{p}$. Pour s'en rendre compte, on peut passer sur Python afin d'y faire quelques expérimentations. L'algorithme ci-dessous

```
def multiplication(a, p):
    mult_lst = []
    for i in range(1, p):
        x = (a*i)%p
        mult_lst.append(x)
    return mult_lst
```

renvoie une liste contenant tous les nombres $a \cdot i \pmod{p}$ pour i allant de 1 à $p-1$. En exécutant ce programme avec $p = 7$ et $a = 5$ comme ci-dessus, on obtient la même liste, à savoir

35. Notez que ce passage nécessite de multiplier de part et d'autre par $a^{-m} \pmod{p}$ et qu'on n'a pas encore défini la signification d'une puissance négative sur une horloge. Cela ne saurait tarder.

```
>>> multiplication(5, 7)
[5, 3, 1, 6, 4, 2]
```

En prenant maintenant $p = 19$ et $a = 6$, on voit là encore qu'on obtient une permutation de toutes les heures modulo 19 (sauf 0 bien-sûr).

```
>>> multiplication(6, 19)
[6, 12, 18, 5, 11, 17, 4, 10, 16, 3, 9, 15, 2, 8, 14, 1, 7, 13]
```

Autrement dit, on obtient tous les nombres de 1 à 18. La preuve de ce résultat est relativement simple. Il suffit de montrer que si $0 < i < j \leq p-1$ alors $a \cdot i \not\equiv a \cdot j \pmod{p}$. En d'autres mots, deux heures différentes ne donnent pas la même heure par multiplication par $a \not\equiv 0 \pmod{p}$. En effet, si

$$a \cdot i \equiv a \cdot j \pmod{p}$$

alors on peut simplifier de part et d'autre par a car a est premier avec p. Cela implique donc que $i \equiv j \pmod{p}$. Les inégalités $0 < i < j \leq p-1$ implique alors que $i = j$. Le résultat en découle.

Nous sommes maintenant à même de démontrer le petit théorème de Fermat. Soit $a \not\equiv 0 \pmod{p}$ et prenons le nombre $(a \cdot 1)(a \cdot 2)(a \cdot 3) \cdots (a \cdot (p-1))$. Par ce que nous venons de voir, les facteurs de ce produit est une permutation des nombres modulo p. Ainsi

$$\begin{aligned}(a \cdot 1)(a \cdot 2)(a \cdot 3) \cdots (a \cdot (p-1)) &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ &\equiv (p-1)! \pmod{p}.\end{aligned}$$

Or

$$\begin{aligned}(a \cdot 1)(a \cdot 2)(a \cdot 3) \cdots (a \cdot (p-1)) &= 1 \cdot 2 \cdot 3 \cdots (p-1) \underbrace{a \cdot a \cdot a \cdots a}_{p-1 \text{ fois}} \\ &= (p-1)! a^{p-1}\end{aligned}$$

Ainsi, on obtient $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. En simplifiant de part et d'autre par $(p-1)!$ (car premier avec p), on obtient le résultat souhaité, à savoir

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ingénieux, n'est-ce pas ? Notez alors que cela implique en multipliant par a que $a^p \equiv a \pmod{p}$. Cette dernière congruence est valable même si $a \equiv 0 \pmod{p}$ car $0^p \equiv 0 \pmod{p}$. Toutefois, $a^p \equiv 1 \pmod{p}$ n'est valable que si $a \not\equiv 0 \pmod{p}$.

16 Euler, l'incroyable génie

Le mathématicien suisse Leonhard Euler a révolutionné les mathématiques à bien des égards. Dans cette section nous lui rendons un petit hommage [36] en nous intéresssant à deux de ses exploits en arithmétique. Nous donnons tout d'abord sa preuve du petit théorème de Fermat [37] et ensuite une partie de ses travaux sur les nombres parfaits.

36. Pas à la hauteur de son génie. Il lui faudra au moins une dizaine de livres.
37. Notez alors qu'il s'agit de la première preuve connue de ce théorème.

Leonhard Euler

16.1 Euler et le petit théorème de Fermat

Euler était le premier à démontrer le petit théorème de Fermat. Pour se faire, il remarque tout d'abord que le nombre

$$(a+1)^p - (a^p+1)$$

est toujours divisible par p. En d'autres mots, $(a+1)^p \equiv a^p + 1 \pmod{p}$. Inspectons ce résultat sur un exemple. Si $p = 3$ et $a = 2$ alors

$$(a+1)^p = (2+1)^3 \equiv 3^3 \equiv 27 \equiv 0 \pmod{3}.$$

Par ailleurs $2^3 + 1 \equiv 9 \equiv 0 \pmod{3}$. On voit alors que dans ce cas, on a bien $(a+1)^p \equiv a^p + 1 \pmod{p}$. Afin de faire l'expérimentation de façon plus simple, je vous ai écrit un petit algorithme en Python, qui renvoie True si la congruence est bonne et False sinon. Évidemment, il ne donnera jamais False, puisqu'on démontrera ce petit lemme dans tous les cas. Voici donc l'algorithme

```
def cong_test (a, p):
    x = ((a+1)**p) % p
    y = (a**p + 1) % p
    return x == y
```

Allez, j'en ai marre de faire l'expérimentation à votre place, je vous laisse aller sur Python seul afin de vous en convaincre. Venons-en à la démonstration du constat d'Euler. Je vous rappelle la formule du binôme de Newton

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n,$$

où $\binom{n}{k}$ désigne le choix de k éléments parmi n. Je vous rappelle de plus que ce choix est donné par la formule

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Je vous laisse là encore le soin d'appliquer cette formule dans les cas particuliers de $n = 2$ et $n = 3$ pour obtenir les fameuses formules

$$(a+b)^2 = a^2 + 2ab + b^2 \quad \text{et} \quad (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Euler a utilisé le binôme de Newton pour montrer que

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1,$$

en prenant $b=1$. Ainsi, pour montrer que $(a+1)^p-(a^p+1)$ est divisible par p, il suffit de montrer que p divise

$$\binom{p}{1}a^{p-1}+\binom{p}{2}a^{p-2}+\cdots+\binom{p}{p-1}a.$$

Montrer que p divise chacun des $\binom{p}{k}$ pour $1\leq k\leq p-1$ suffira donc pour conclure. Regardons si c'est le cas sur deux exemples.

- Si $p=3$ alors

$$\binom{3}{1}=\frac{3!}{1!(3-1)!}=\frac{3!}{2!}=3.$$

  Ainsi $\binom{3}{1}=3$ est bien divisible par $p=3$. De même

$$\binom{3}{2}=\frac{3!}{2!(3-2)!}=\frac{3!}{2!}=3.$$

  Même conclusion pour ce calcul.

- Si $p=5$ alors

$$\binom{5}{1}=5,\quad \binom{5}{2}=5\cdot 2,\quad \binom{5}{3}=5\cdot 2\quad \text{et}\quad \binom{5}{4}=5.$$

  On voit là encore que $p=5$ divise $\binom{5}{k}$ pour $1\leq k\leq 4$.

Dans le cas général, montrons tout d'abord que p divise $k!\cdot\binom{p}{k}$ quand $1\leq k\leq p-1$. En effet

$$k!\binom{p}{k}=k!\frac{p!}{k!(p-k)!}=\frac{p!}{(p-k)!}=p\frac{(p-1)!}{(p-k)!}.$$

On voit alors que la condition $1\leq k\leq p-1$ implique que $(p-1)!/(p-k)!$ est un nombre entier. On en déduit que p divise $k!\binom{p}{k}$. Or p ne peut pas diviser $k!$, donc d'après le lemme de Gauss p divise $\binom{p}{k}$. Notre résultat en découle.

Maintenant une petite récurrence sur a suffit pour montrer le petit théorème de Fermat. En effet,

- **Initialisation :** Pour $a=0$, le résultat est trivial.
- **Hérédité :** Supposons que le résultat est vrai pour $a\in\mathbb{N}$. Autrement dit, on suppose que $a^p\equiv a\pmod p$ et montrons que $(a+1)^p\equiv a+1\pmod p$. En effet, d'après ce qui précède on a

$$(a+1)^p\equiv a^p+1\pmod p\equiv \underbrace{a}_{HR}+1\pmod p.$$

  D'où le résultat. Pour le montrer pour tout $a\in\mathbb{Z}$, il suffit de remarquer que pour un nombre premier p impair on a $(-a)^p\equiv -a^p\equiv -a\pmod p$. Si $p=2$, la congruence $1\equiv -1\pmod 2$ implique que $(-a)^2\equiv a^2\equiv a\equiv -a\pmod 2$.

Rien de bien ingénieux allez-vous me dire ! Attendez de voir sa manipulation des nombres parfaits pour comprendre son génie.

16.2 Euler et les nombres parfaits pairs

Avant de nous intéresser aux travaux d'Euler sur les nombres parfaits pairs, il est important de s'arrêter un petit instant sur ceux d'Euclide. À l'époque de ce dernier, les seuls nombres parfaits connus étaient 6, 28, 496 et 8128. Euclide a su alors déceler à partir de si peu d'exemples une forme générale permettant de les générer, à savoir

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

où $2^k - 1$ est un nombre premier. Je trouve cela incroyable à titre personnel ! Euclide mérite qu'on l'applaudisse encore une fois, pour sa rigueur et sa compréhension profonde de la nature des nombres.

Venons-en maintenant à notre savant éminent Euler. Ce dernier s'est intéressé à la théorie des nombres sous l'influence du fameux Christian Goldbach.

Christian Goldbach

Goldbach a rencontré le jeune Euler en 1727 à Saint Petersbourg. Il a ainsi porté à son attention les travaux de Fermat autour de la théorie des nombres. Peu après, Euler a su refuter la conjecture de Fermat sur ses nombres F_n et a montré au passage que F_5 est divisible par 641. Mais ce n'est que le début qu'une aventure magique dans l'esprit génial du grand maître. Euler s'est intéressé ensuite aux nombres parfaits en regardant du côté des nombres **amiables**. Deux entiers m et n sont dits amiables lorsque la somme des diviseurs propres de m vaut n et vice versa. Les nombres amiables sont rares et les plus petits sont $m = 220$ et $n = 284$. Avant qu'Euler entre en scène, seuls trois couples de nombres amiables étaient connus. Notre ancêtre savant a trouvé à lui seul 59 couples supplémentaires ! Pour étudier ces nombres et les nombres parfaits, il introduit une nouvelle fonction qu'on appelle σ définie par

$$\sigma(N) = \sum_{d|N} d.$$

En d'autres mots, $\sigma(N)$ est tout simplement la somme des diviseurs de N, N inclus. Notez alors que cette fonction est légèrement différente de celle d'Euclide, car ce dernier fait la somme des diviseurs de N, N exclu. Euler inclut N pour des raisons bien profondes que l'on va découvrir ensemble. Avant de nous plonger dans les détails techniques, prenons quelques exemples. Si $N = 6$ alors

$$\sigma(6) = 1 + 2 + 3 + 6 = 12.$$

Si $N = 7$ alors $\sigma(7) = 1 + 7 = 8$ et si $N = 28$ alors

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28 = 56.$$

Bien sûr, nous pouvons passer sur Python afin d'écrire une fonction permettant de calculer σ et voilà ce qu'on obtient

```
def divisors(n):
    list_div = []
    for d in range(1, n+1):
        if n % d == 0:
            list_div.append(d)
    return list_div

def sigma(n):
    s = 0
    for d in divisors(n):
        s += d
    return s
```

La fonction *divisors* renvoie la liste des diviseurs de n et à partir de cette liste la fonction *sigma* calcule la somme des diviseurs de n. Je vous laisse aller sur le Shell afin de vérifier que tout fonctionne bien. Les choses deviennent intéressantes quand Euler caractérise les nombres premiers et les nombres parfaits avec sa fonction σ. En effet, nous avons

1. Un entier p est premier si et seulement si $\sigma(p) = p + 1$.
2. Un entier N est parfait si et seulement si $\sigma(N) = 2N$.

Cela déplace ainsi notre problème sur les nombres parfaits à l'étude de la fonction σ. Cette dernière a des propriétés très intéressantes, à savoir

1. Si p est un nombre premier alors
$$\sigma(p^r) = \frac{p^{r+1}-1}{p-1}.$$
2. La fonction σ a une propriété multiplicative intéressante, à savoir si p et q sont deux nombres premiers distincts alors
$$\sigma(pq) = \sigma(p)\sigma(q).$$
3. En réalité, on peut généraliser cette dernière propriété à n'importe quels entiers a et b premiers entre eux, auquel cas on obtient $\sigma(ab) = \sigma(a)\sigma(b)$. Nous verrons alors que cette généralisation est l'une des clefs de l'étude de notre fonction.

La preuve de la première propriété est triviale. En effet, les diviseurs de p^r sont tous de la forme p^s où $0 \leq s \leq r$. Ainsi
$$\sigma(p^r) = 1 + p + p^2 + \cdots + p^r = \frac{p^{r+1}-1}{p-1},$$
car il s'agit d'une somme géométrique de raison égale à p. De cette formule, nous pouvons déduire que le nombre $N = 2^r$ n'est jamais parfait. En effet, d'après notre première propriété
$$\begin{aligned}
\sigma(\underbrace{2^r}_{N}) &= \frac{2^{r+1}-1}{2-1} \\
&= 2^{r+1} - 1 \\
&= 2 \cdot \underbrace{2^r}_{N} - 1 \\
&= 2N - 1 \\
&\neq 2N.
\end{aligned}$$

Voyez-vous maintenant à quel point la fonction σ est incroyable ? Et ce n'est que le début. Avant de prouver notre deuxième assertion, regardons ce que cela donne sur Python. En prenant $p = 7$ et $q = 5$ on trouve

```
>>> sigma(7)
8
>>> sigma(5)
6
```

Maintenant en calculant $\sigma(7 \cdot 5)$ on tombe sur

```
>>> sigma(7*5)
48
```

et il s'agit bien de $8 \cdot 6$. On voit ainsi que $\sigma(7 \cdot 5) = \sigma(7) \cdot \sigma(5)$. Plus généralement, si p et q sont premiers alors $\sigma(p) = p + 1$ et $\sigma(q) = q + 1$. Or les diviseurs de pq sont 1, p, q et pq. Ainsi

$$\begin{aligned}\sigma(pq) &= 1 + p + q + pq \\ &= (p+1)(q+1) \\ &= \sigma(p)\sigma(q).\end{aligned}$$

Je vous laisse le soin de démontrer la troisième propriété, facilement déductible des deux premières. Remarquez maintenant qu'il devient bien facile de calculer la fonction σ. En effet, si $N = 90$ alors nos trois propriétés impliquent

$$\begin{aligned}\sigma(90) &= \sigma(2^3 \cdot 3 \cdot 5) \\ &= \sigma(2^3)\sigma(3)\sigma(5) \\ &= (2^4 - 1) \cdot 4 \cdot 6 \\ &= 360.\end{aligned}$$

Voilà donc, nous avons su calculer la somme des diviseurs de 90, sans même les connaître. Nous sommes maintenant prêt à démontrer le résultat d'Euler, à savoir si N est un nombre parfait pair alors il doit être de la forme euclidienne $N = 2^{n-1}(2^n - 1)$. Puisque N est pair, nous pouvons l'écrire sous la forme $N = 2^{n-1}k$, où k est un entier impair. En d'autres mots, 2^{n-1} est la plus grande puissance de 2 divisant N. Notez alors que la parité de N implique que $n > 1$. Par ailleurs, N est parfait donc

$$\begin{aligned}\sigma(N) &= 2N \\ &= 2 \cdot 2^{n-1}k \\ &= 2^n k.\end{aligned}$$

Or 2^{n-1} et k sont premiers entre eux donc

$$\begin{aligned}\sigma(N) &= \sigma(2^{n-1}k) \\ &= \sigma(2^{n-1})\sigma(k) \\ &= (2^n - 1)\sigma(k).\end{aligned}$$

Ainsi, $2^n k = (2^n - 1)\sigma(k)$. Euler a pu en déduire que 2^n doit diviser $\sigma(k)$ car il est premier avec $2^n - 1$. Cela implique donc l'existence d'un entier b tel que

$$\sigma(k) = b \cdot 2^n.$$

L'égalité $2^n k = (2^n - 1)\sigma(k)$ s'écrit alors $2^n k = (2^n - 1) \cdot b \cdot 2^n$, ce qui implique que

$$k = b(2^n - 1).$$

Si vous êtes un peu perdu, je vous rappelle qu'on cherche à écrire le nombre parfait N sous la forme $2^{n-1}(2^n - 1)$, où $2^n - 1$ désigne un nombre premier. On a commencé par écrire $N = 2^{n-1}k$ et on a obtenu que k est de la forme $k = b \cdot (2^n - 1)$. Il suffit maintenant de démontrer que $b = 1$ et que $2^n - 1$ est premier.

Supposons par l'absurde que $b > 1$. Les entiers 1, b, $2^n - 1$ et k sont des diviseurs de $k = b(2^n - 1)$. Je prétends alors que tous ces diviseurs sont distincts. Pour se faire, nous allons montrer qu'ils sont deux à deux distincts.

1. $k \neq 1$ car dans ce cas $N = 2^{n-1}k = 2^{n-1}$, ce qui est impossible car on a vu qu'une puissance de 2 ne peut jamais être un nombre parfait.

2. $b \neq 1$ car par hypothèse $b > 1$.

3. $2^n - 1 \neq 1$ car dans le cas contraire on obtient $2^n = 2$ ou encore que $2^{n-1} = 1$ ce qui implique que $N = 2^{n-1}k = k$. Là encore c'est impossible car k est un entier impair tandis que N est un nombre parfait pair.

4. $k \neq b$ car l'égalité $k = b(2^n - 1)$ implique que $2^n - 1 = 1$ ce qui est impossible d'après le cas ci-dessus.

5. $k \neq 2^n - 1$ car dans ce cas $b = 1$, ce qui est exclu par hypothèse.

6. Dernier cas $b \neq 2^n - 1$. En effet, dans le cas contraire on obtient $k = b^2$ et donc k admet au moins 3 diviseurs distincts, à savoir 1, b et b^2 (car $b > 1$). Ainsi

   $$\sigma(k) \geq 1 + b + b^2.$$

   Par ailleurs on sait que

   $$\begin{aligned}\sigma(k) &= b \cdot 2^n \\ &= b(2^n - 1 + 1) \\ &= b(b + 1) \\ &= b^2 + b \\ &< 1 + b + b^2.\end{aligned}$$

   Contradiction.

Nous avons ainsi démontré que 1, b, $2^n - 1$ et k sont deux à deux distincts, donc

$$\begin{aligned}\sigma(k) \geq 1 + b + 2^n - 1 + k &= b + 2^n + k \\ &= b + 2^n + b(2^n - 1) \\ &= 2^n(b + 1) \\ &> 2^n b = \sigma(k).\end{aligned}$$

Au final, on obtient $\sigma(k) > \sigma(k)$. Ceci est évidemment une contradiction. L'hypothèse du départ $b > 1$ ne tient donc pas la route, donc $b = 1$ et par conséquent $k = 2^n - 1$. Il nous reste à démontrer que $2^n - 1$ est un nombre premier. En effet,

$$\sigma(k) = b \cdot 2^n = 2^n = 2^n - 1 + 1 = k + 1.$$

Le résultat en découle car un nombre p est premier si et seulement si $\sigma(p) = p + 1$. Bingo ! Avant de conclure cette section, je tiens à vous faire remarquer que cette preuve n'était pas au dessus des capacités techniques d'Euclide. Toutefois, Euler a su poser le bon outil, clef des nombres parfaits pairs, en sommant tous les diviseurs au lieu d'exclure N. Cela peut sembler anodin, mais nous avons vu que ce petit changement a permis de faire tomber notre problème comme la pomme de Newton !

17 Où sont les nombres parfaits impairs ?

La question de chercher les nombres parfaits impairs est tout à fait légitime. On peut alors demander à Python de nous calculer les premières valeurs de σ pour N impair. Pour se faire, nous pouvons utiliser l'algorithme suivant [38]

```
def sigma_odd(n):
    liste = []
    for i in range(3, n+1, 2):
        liste.append(sigma(i))
    return liste
```

En effectuant l'exécution avec $n = 40$ on obtient la liste

```
>>> sigma_odd(40)
[4, 6, 8, 13, 12, 14, 24, 18, 20, 32, 24, 31, 40, 30, 32, 48, 48, 38, 56]
```

Cela signifie que $\sigma(3) = 4, \sigma(5) = 6, \sigma(7) = 8, \sigma(9) = 13 \ldots$ et $\sigma(39) = 56$. On remarque alors que pour ces premières valeurs $\sigma(N) < 2N$. Après tout, ce phénomène est plutôt plausible. Contrairement aux nombres pairs, pour lesquels l'un des diviseurs est déjà la moitié du nombre donné, un nombre impair n'a pas cette chance. En effet, le nombre 8128 est divisible par $8128/2 = 4064$ tandis que le plus grand diviseur propre de 8129 vaut seulement 739 ! Pour arriver à la perfection, les autres diviseurs propres de 8128 doivent rectifier un déficit de $8128 - 4064 = 4064$. Ceci est le cas puisqu'on sait que 8128 est parfait. Toutefois, les choses se passent mal pour 8129, ce nombre est bien loin de la perfection car ses autres diviseurs propres doivent s'additionner pour donner $8129 - 739 = 7390$. Notez alors que nous sommes bien loin du compte.

À ce stade, nous pouvons penser que pour N impair, on aura toujours $\sigma(N) < 2N$. Revenons donc à notre outil génialissime Python. L'algorithme suivant permettra de renvoyer, s'il existe, le premier nombre impair N pour lequel on n'a pas $\sigma(N) < 2N$.

```
def sigma_test():
    i = 3
    while sigma(i) < 2*i:
        i += 2
    return i, sigma(i)
```

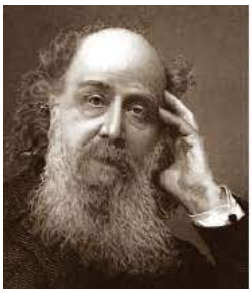
38. Je vous conseille de le faire à la main aussi.

En effectuant l'exécution de ce bout de code on obtient

```
>>> sigma_test()
(945, 1920)
```

On a bien $\sigma(945) = 1920 > 2 \cdot 945$. Notre première intuition n'est donc pas bonne. Il existe dans la nature des nombres impairs pour lesquels $\sigma(N) > 2N$. Puisqu'il existe des entiers impairs pour lesquels $\sigma(N) < 2N$ et d'autres pour lesquels $\sigma(N) > 2N$, rien n'empêche l'existence de nombres impairs N pour lesquels $\sigma(N) = 2N$. Nos nombres impairs ne sont donc plus disqualifiés et reviennent ainsi dans la course.

À ce jour, personne n'a su trouver un nombre parfait impair et personne n'a su refuter leur existence. Euler en parle comme un problème extrêmement difficile et si lui dit que c'est difficile alors ça l'est véritablement. Pour prouver l'impossibilité de l'existence de tels entiers, certains mathématiciens ont tenté de trouver des propriétés impossibles à ces nombres. En vain, toutefois on a progressé un peu sur la question. L'un des résultats allant dans ce sens est un théorème dû à James Jospeh Sylvester.



J-J Sylvester

Son théorème affirme qu'un nombre parfait impair doit avoir au moins 3 facteurs premiers distincts. Sylvester démontre ce résultat avec beaucoup d'élégance. En effet, si N est un nombre parfait impair admettant un seul diviseur premier alors $N = p^r$, où p désigne un nombre premier impair et $r \geq 1$, alors $2N = \sigma(N)$ et

$$2p^r = \sigma(p^r) = \frac{p^{r+1} - 1}{p - 1}.$$

Ceci donne l'égalité $2p^r - p^{r+1} = 1$, qui est une contradiction car p ne peut pas diviser 1. Ainsi, un nombre parfait impair ne peut pas avoir un seul facteur premier. Qu'en est-il de deux facteurs premiers ? Supposons que $N = p^r q^s$, où $p < q$ désignent deux nombres premiers impairs. On sait dans ce cas que

$$2N = \sigma(N) = \sigma(p^r q^s) = \sigma(p^r)\sigma(q^s).$$

En d'autres termes, nous avons que

$$2N = (1 + p + p^2 + \cdots + p^r)(1 + q + q^2 + \cdots + q^s).$$

En divisant cette égalité de part et d'autre par $N = p^r q^s$ et en simplfiant on obtient la relation

$$\begin{aligned} 2 &= \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^r}\right)\left(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots + \frac{1}{q^s}\right) \\ &\leq \left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^r}\right)\left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots \frac{1}{5^s}\right). \end{aligned}$$

Cette inégalité est valide car p est un nombre premier impair donc doit être égal au moins à 3. L'entier q étant premier plus grand que p, il est au moins égal à 5. Par passage à l'infini dans ces deux séries géométriques on obtient l'inégalité

$$2 \leq \sum_{k=0}^{\infty} \frac{1}{3^k} \cdot \sum_{k=0}^{\infty} \frac{1}{5^k} = \frac{3}{2} \cdot \frac{5}{4} = \frac{15}{8}.$$

Ceci est une contradiction ! Ainsi un entier parfait impair ne peut pas avoir seulement deux facteurs premiers disctincts. Quelle ingéniosité, quel talent ! Il est donc inutile de chercher des nombres parfaits impairs comme 10125 car sa décomposition en facteurs premiers, à savoir $3^4 \cdot 5^3$, contient uniquement deux facteurs premiers. Sylvester ne s'est pas arrêté ici et a aussi montré qu'un nombre parfait impair admet au moins 4 facteurs premiers distincts puis au moins 5.

18 Résolution de congruences linéaires

Dans cette partie, nous allons nous intéresser aux congruences linéaires. En d'autres termes, on aimerait pouvoir résoudre les équations de la forme

$$ax + b \equiv 0 \pmod{n}.$$

Je vous rappelle que pour résoudre l'équation $ax + b = 0$ dans $\mathbb{R}$, on soustrait d'abord b de part et d'autre de l'égalité pour obtenir $ax + \not{b} - \not{b} = -b$, ce qui s'écrit encore $ax = -b$. Maintenant pour trouver le nombre x vérifiant l'égalité précédente, on la multiplie de part et d'autre par l'inverse de a pour avoir

$$\frac{1}{a} \cdot ax = \frac{1}{a} \cdot (-b).$$

Ainsi, on obtient $x = -b/a$. Tout va bien à condition d'avoir $a \neq 0$. C'est cette condition qui garantit l'existence d'un inverse du nombre a. Autrement, l'existence d'un nombre c vérifiant l'égalité

$$a \cdot c = 1.$$

Il s'avère que dans $\mathbb{R}$, tout nombre non nul admet un inverse. Peut-on faire la même chose sur une horloge de n heures ? Évidemment, si $ax + b \equiv 0 \pmod{n}$ alors on peut soustraire b pour obtenir $ax \equiv -b \pmod{n}$. Diviser par a dans une horloge ne signifie pas grand-chose, ainsi pour se débarrasser du a, nous avons besoin d'un c vérifiant

$$c \cdot a \equiv 1 \pmod{n}.$$

Dans ce cas, en multipliant notre congruence $ax \equiv -b \pmod{n}$ de part et d'autre par c on obtient

$$\underbrace{c \cdot a}_{1 \pmod{n}} \; x \equiv c \cdot (-b) \pmod{n}.$$

Puisque $ca \equiv 1 \pmod{n}$, ce procédé implique que $x \equiv -bc \pmod{n}$. Super ! Toutefois, il y reste une zone d'ombre ! Comment peut-on trouver un tel c ? D'ailleurs, existe-t-il toujours ? Nous verrons alors qu'un tel entier modulo n n'existe pas tout le temps. En tout cas, s'il existe, retenez qu'on dit que a est **inversible** modulo n d'inverse égal à $c \pmod{n}$.

Regardons ce qui se passe sur un exemple concret. On aimerait savoir si 2 est inversible modulo 7. Autrement dit, on cherche un nombre x pour lequel

$$2x \equiv 1 \pmod 7.$$

Après quelques essaies, on voit que $2 \cdot 4 \equiv 1 \pmod 7$. Ainsi, 2 est inversible modulo 7 et son inverse vaut 4 (mod 7). Maintenant, si on souhaite par exemple résoudre l'équation $2x \equiv 3 \pmod 7$, il suffit de multiplier de part et d'autre par 4 (mod 7) pour obtenir

$$\underbrace{4 \cdot 2}_{1 \pmod 7} x \equiv 4 \cdot 3 \pmod 7.$$

La solution de notre congruence linéaire $2x \equiv 3 \pmod 7$ est donc $x \equiv 5 \pmod 7$. Vous pouvez vérifier facilement qu'en effet, on a bien $2 \cdot 5 \equiv 3 \pmod 7$. Very nice !

Regardons maintenant ce qui se passe sur un autre exemple. On souhaite alors résoudre l'équation $2x \equiv 1 \pmod 6$. Cela revient à savoir si 2 est inversible modulo 6. On pourra essayer toutes les valeurs de x possibles et voir qu'aucune ne donne 1 (mod 6). Mais notez que l'on peut s'en rendre compte avec un petit raisonnement. En effet, on sait que $2 \cdot 3 \equiv 0 \pmod 6$. Cela implique donc que s'il existe x vérifiant $2x \equiv 1 \pmod 6$ alors en multipliant cette congruence de part et d'autre par 3 on obtient

$$\underbrace{3 \cdot 2}_{0 \pmod 6} x \equiv 3 \cdot 1 \pmod 6,$$

ou encore que $0 \equiv 3 \pmod 6$, ce qui est une contradiction. Ainsi, l'équation $2x \equiv 1 \pmod 6$ n'admet pas de solution modulo 6. Moralité de cette histoire, dans $\mathbb{R}$, la condition $a \neq 0$ suffit pour trouver l'inverse de a alors que sur une horloge, $a \neq 0 \pmod n$ ne suffit pas pour inverser a, comme on vient de le voir avec 2 (mod 6).

La question toute naturelle qui nous vient à l'esprit à ce stade est, à quelle condition alors un nombre $a \pmod n$ est-il inversible modulo n ? Nous allons nous intéresser dans la suite à une question plus générale, à savoir à quelles conditions sur a, b et n, l'équation

$$ax \equiv b \pmod n$$

admet-elle une solution ? En effet, $ax \equiv b \pmod n$ si et seulement si il existe un entier k tel que $ax = b + nk$, ce qui s'écrit encore $ax - nk = b$. Autrement dit $ax \equiv b \pmod n$ si et seulement si la droite d'équation $ax + ny = b$ admet un point à coordonnées entières. Je vous rappelle que ceci est le cas si et seulement si le pgcd de a et de n divise b.

Ainsi, pour résoudre l'équation $ax \equiv b \pmod n$, il suffit de résoudre l'équation diophantienne $ax + ny = b$, à condition que (a,n)[39] divise b, et ce en utilisant l'algorithme d'Euclide étendu. Notez au passage qu'un nombre a est inversible modulo n si et seulement si $(a,n) = 1$. Prenons un exemple. On souhaite résoudre l'équation $21x \equiv 14 \pmod{35}$. La suite des divisions euclidiennes successives donne

$$\begin{aligned} 35 &= 21 \cdot 1 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= 7 \cdot 2 + 0. \end{aligned}$$

39. Je vous rappelle que (a,n) désigne le pgcd de a et de n.

On en déduit que $(35,21)=7$ et en remontant les opérations on obtient

$$\begin{aligned}7&=21-14\cdot 1\\&=21-(35-21\cdot 1)\cdot 1\\&=21\cdot 2-35\cdot 1.\end{aligned}$$

Je prétends que c'est quasiment fini car dans le monde des congruences cela s'écrit

$$21\cdot 2\equiv 7 \pmod{35}.$$

En multipliant cette congruence de part et d'autre par 2, on obtient $21\cdot 4\equiv 14 \pmod{35}$. Cela affirme donc que $x\equiv 4 \pmod{35}$ est une solution de l'équation $21x\equiv 14 \pmod{35}$. En réalité, il ne s'agit pas de la seule solution modulo 35 et il en existe exactement $7=(35,21)$.

Pour trouver les autres solutions, revenons à l'égalité $7=21\cdot 2-35\cdot 1$. En multipliant par 2 on obtient

$$14=21\cdot 4-35\cdot 2,$$

ce qui signifie que le point $(4,-2)$ est un point intégral sur la droite d'équation $14=21x+35y$. Je vous laisse résoudre cette équation avec la méthode classique pour voir que x doit être de la forme $x=4-5k$, où k désigne un entier. Autrement dit si x est solution de l'équation $21x\equiv 14 \pmod{35}$ alors $x\equiv 4 \pmod 5$. Modulo 35, cela nous donne les nombres 4, 9, 14, 19, 24, 29 et 34. Ils sont bien au nombre de 7 et les sceptiques peuvent vérifier qu'ils sont tous solutions de notre équation du départ. Plus généralement, je vous laisse montrer seul que si (a,n) divise b alors l'équation $ax\equiv b \pmod n$ admet (a,n) solutions. Notez alors que cela implique que si a est inversible modulo n alors cet inverse est unique.

19 Résolution de systèmes de congruences linéaires

Dans cette section nous nous intéressons aux systèmes constitués de congruences linéaires en x. Prenons un premier exemple. Soit à résoudre le système

$$\begin{cases}x &\equiv 3 \pmod 5\\ x &\equiv 2 \pmod 7.\end{cases}$$

En français, cela signifie que nous sommes à la recherche des nombres x qui laissent un reste égal à 3 modulo 5 et égal à 2 modulo 7. La première équation implique alors que x doit être de la forme $x=3+5k$ pour un entier k et la deuxième force l'égalité $x=2+7k'$ pour un autre entier k'. Notez alors que les entiers $x=3+5k$ ne laissent pas tous un reste égal à 2 modulo 7. Si par exemple $k=1$, cette formule produit $x=8$ et le reste de la division euclidienne de 8 par 7 vaut $1\neq 2$. De même, la formule $x=2+7k'$ ne produit pas forcément des entiers laissant un reste égal à 3 modulo 5.

Nous sommes donc à la recherche d'une seule formule permettant de générer tous les entiers x vérifiant à la fois la permière équation et la deuxième équation. Pour se faire, nous procéderons de deux manières différentes.

Première méthode : Les égalités $x = 3 + 5k$ et $x = 2 + 7k'$ impliquent que

$$3 + 5k = 2 + 7k',$$

ou encore $7k' - 5k = 1$. Autrement dit le couple $(k', -k)$ est solution entière de l'équation diophantienne $7u + 5v = 1$. Oh ! C'est quasiment plié du coup ! La question tombe dans notre machine diophantienne et n'en sortira donc que résolue ! En appliquant l'algorithme d'Euclide étendu on obtient la suite des divisions euclidiennes

$$\begin{aligned} 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Cela implique que le pgcd de 7 et 5 vaut 1 et en remontant ces opérations on obtient

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 5 \cdot 1) \\ &= 5 \cdot 3 - 2 \cdot 7. \end{aligned}$$

Ainsi $(-2, 3)$ est une solution particulière de l'équation $7u + 5v = 1$ et en résolvant donc celle-ci avec la manière classique on trouve $u = -2 + 5t$, où t désigne un entier. L'égalité $x = 2 + 7k'$ s'écrit alors

$$x = 2 + 7(-2 + 5t) = -12 + 35t.$$

Dans le monde des congruences, cela s'écrit $x \equiv -12 \pmod{35} \equiv 23 \pmod{35}$. On voit alors que 23 est la première solution positive de notre système car $23 \equiv 3 \pmod 5$ et $23 \equiv 2 \pmod 7$. La deuxième solution positive de notre système est $x = 23 + 35 = 58$ et je vous laisse le vérifier seul. Plus généralement, $x \equiv 23 \pmod{35}$ est solution de notre système car

$$x \equiv 23 \pmod{35} \equiv 23 \pmod 5 \equiv 3 \pmod 5$$

et

$$x \equiv 23 \pmod{35} \equiv 23 \pmod 7 \equiv 2 \pmod 7.$$

On a donc obtenu notre formule permettant de générer les solutions de notre système. Cette méthode fonctionne très bien sur un système de deux équations mais n'est plus efficace avec des systèmes comportant davantage d'équations. Nous aborderons donc dans la suite une méthode bien plus efficace, inspirée du fameux **théorème des restes chinois**.

Deuxième méthode : Reprenons donc le même système de notre exemple précédent

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

Afin de résoudre ce système, nous allons nous intéresser à deux systèmes sous-jacents, à savoir

$$\begin{cases} x_1 \equiv 1 \pmod 5 \\ x_1 \equiv 0 \pmod 7 \end{cases} \quad ; \quad \begin{cases} x_2 \equiv 0 \pmod 5 \\ x_2 \equiv 1 \pmod 7 \end{cases}$$

Je prétends alors que si on arrive à résoudre ces deux systèmes, la solution du système initial s'en déduit trivialement. En effet, si x_1 est solution du premier système et x_2 est solution du deuxième système alors

$$x \equiv 3 \cdot x_1 + 2 \cdot x_2 \pmod{5 \cdot 7}$$

est la solution recherchée. Voyez-vous pourquoi ? En effet,

$$\begin{aligned} x &\equiv 3 \cdot x_1 + 2 \cdot x_2 \pmod{5 \cdot 7} \\ &\equiv 3 \cdot x_1 + 2 \cdot x_2 \pmod{5} \\ &\equiv 3 \cdot 1 + 2 \cdot 0 \pmod{5} \\ &\equiv 3 \pmod{5}, \end{aligned}$$

car $x_1 \equiv 1 \pmod{5}$ et $x_2 \equiv 0 \pmod{5}$. De même, ce x est solution de la deuxième équation car

$$\begin{aligned} x &\equiv 3 \cdot x_1 + 2 \cdot x_2 \pmod{5 \cdot 7} \\ &\equiv 3 \cdot x_1 + 2 \cdot x_2 \pmod{7} \\ &\equiv 3 \cdot 0 + 2 \cdot 1 \pmod{7} \\ &\equiv 2 \pmod{7}, \end{aligned}$$

car $x_1 \equiv 0 \pmod{7}$ et $x_2 \equiv 1 \pmod{7}$. Il nous reste maintenant à résoudre les deux systèmes

$$\begin{cases} x_1 \equiv 1 \pmod{5} \\ x_1 \equiv 0 \pmod{7} \end{cases} \quad ; \quad \begin{cases} x_2 \equiv 0 \pmod{5} \\ x_2 \equiv 1 \pmod{7} \end{cases}$$

Cela peut paraitre plus laborieux car on résout deux systèmes au lieu d'en résoudre qu'un seul, mais en réalité ce n'en est rien. Allons-y donc ! On sait que $x_1 \equiv 0 \pmod{7}$, donc x_1 s'écrit sous la forme $x_1 = 7m$, où m désigne un entier. Par ailleurs $x_1 \equiv 1 \pmod{5}$, cela implique en particulier que $7m \equiv 1 \pmod{5}$ et donc qu'il existe un n tel que $7m + 5n = 1$. Or d'après la résolution de cette équation diophantienne, on sait que $m = -2 + 5t$, pour un entier t. Par conséquent

$$x_1 = 7m = 7(-2 + 5t) = -14 + 35t,$$

ou encore $x_1 \equiv -14 \pmod{35} \equiv 21 \pmod{35}$. En inspectant maintenant le deuxième système, la congruence $x_2 \equiv 0 \pmod{5}$ implique l'existence d'un n tel que $x_2 = 5n$. La deuxième équation de ce système s'écrit donc $5n \equiv 1 \pmod{7}$, d'où l'existence d'un entier m tel que $7m + 5n = 1$! Hoo, mais il s'agit de la même équation diophantienne dont la résolution donne $n = 3 - 7t$. On en déduit donc que

$$x_2 = 5(3 - 7t) = 15 - 35t,$$

ou encore $x_2 \equiv 15 \pmod{35}$. On voit alors avec un simple calcul que

$$\begin{aligned} x &\equiv 3 \cdot x_1 + 2 \cdot x_2 \pmod{35} \\ &\equiv 3 \cdot 21 + 2 \cdot 15 \pmod{35} \\ &\equiv 23 \pmod{35}. \end{aligned}$$

Et il s'agit bien de la solution retrouvée avec la première méthode, Bingo ! Il reste toutefois une question en suspens. Nous avons montré que la solution des deux systèmes auxiliaires

donnait une solution du système initial. Néanmoins nous n'avons pas montré qu'il s'agit de la seule solution. Rien ne garantit a priori que les deux systèmes auxiliaires sont équivalents au système initial.

Nous verrons plus loin que le théorème des restes chinois affirme que cette méthode fournit toutes les solutions de notre système d'équations. Ce théorème met au clair aussi les conditions à vérifier pour qu'un tel système admette des solutions. Il existe en effet des systèmes impossibles à résoudre tels que

$$\begin{cases} x & \equiv 1 \pmod 2 \\ x & \equiv 4 \pmod 6. \end{cases}$$

La deuxième équation de ce système est incompatible avec la première car

$$\begin{aligned} x &\equiv 4 \pmod 6 \\ &\equiv 4 \pmod 2 \\ &\equiv 0 \pmod 2. \end{aligned}$$

Ainsi $x \equiv 0 \pmod 2$ et $x \equiv 1 \pmod 2$, ce qui est impossible. Dans la suite de cette section, nous allons nous intéresser à un problème posé par le mathématicien chinois *Sun Zi* au IVème siècle.

Sun Zi

Nous disposons d'un certain nombre x de chevaux qu'on souhaite compter tel que $x \leq 100$. Pour se faire, en les comptant 3 par 3, il reste un cheval seul. En les comptant 5 par 5 et 7 par 7 , il en reste 3 à chaque fois. Peut-on alors trouver le nombre exact des chevaux ? Ce problème est équivalent à la résolution du système

$$\begin{cases} x & \equiv 1 \pmod 3 \\ x & \equiv 3 \pmod 5 \\ x & \equiv 3 \pmod 7 \end{cases}$$

Afin de le résoudre, nous considérons trois systèmes auxiliaires, à savoir

$$\begin{cases} x_1 \equiv 1 \pmod 3 \\ x_1 \equiv 0 \pmod 5 \\ x_1 \equiv 0 \pmod 7 \end{cases} \quad ; \quad \begin{cases} x_2 \equiv 0 \pmod 3 \\ x_2 \equiv 1 \pmod 5 \\ x_2 \equiv 0 \pmod 7 \end{cases} \quad ; \quad \begin{cases} x_3 \equiv 0 \pmod 3 \\ x_3 \equiv 0 \pmod 5 \\ x_3 \equiv 1 \pmod 7 \end{cases}$$

Modulo la résolution de ces trois systèmes, la solution x de notre système initial sera donnée par

$$x \equiv 1 \cdot x_1 + 3 \cdot x_2 + 3 \cdot x_3 \pmod{3 \cdot 5 \cdot 7}.$$

Je vous laisse alors vérifier seul que cette combinaison est bien solution du système initial. Pour trouver x_1, on remarque que $x_1 \equiv 0 \pmod 5$ et $x_1 \equiv 0 \pmod 7$ implique que $x_1 \equiv 0 \pmod{35}$ car 5 et 7 sont premiers entre eux. Autrement dit, il existe un entier k_1 tel que $x_1 = 35k_1$. La congruence $x_1 \equiv 1 \pmod 3$ implique alors que $35k_1 \equiv 1 \pmod 3$. En réduisant 35 modulo 3 on obtient la congruence

$$2k_1 \equiv 1 \pmod 3,$$

car $35 \equiv 2 \pmod 3$. En multipliant la congruence $2k_1 \equiv 1 \pmod 3$ par 2 on obtient $4k_1 \equiv 2 \pmod 3$, ce qui s'écrit encore $k_1 \equiv 2 \pmod 3$ car $4 \equiv 1 \pmod 3$. On peut alors affirmer que k_1 est de la forme $k_1 = 2 + 3n_1$, où n_1 désigne un entier. L'égalité $x_1 = 35k_1$ s'écrit donc

$$x_1 = 35k_1 = 35(2 + 3n_1) = 70 + 105n_1 \equiv 70 \pmod{105}.$$

De même, $x_2 \equiv 0 \pmod 3$ et $x_2 \equiv 0 \pmod 7$ implique que $x_2 = 21k_2$, où k_2 désigne un entier. La congruence $x_2 \equiv 1 \pmod 5$ s'écrit donc $21k_2 \equiv 1 \pmod 5$. Or $21 \equiv 1 \pmod 5$. On obtient ainsi

$$k_2 \equiv 1 \pmod 5.$$

En multipliant par 21, on obtient que $x_2 \equiv 21 \pmod{105}$[40]. Pour trouver x_3 , on remarque de même que $x_3 \equiv 0 \pmod{15}$, ou encore que $x_3 = 15k_3$. La troisième congruence implique donc que $15k_3 \equiv 1 \pmod 7$. Tout va bien car $15 \equiv 1 \pmod 7$ et donc

$$k_3 \equiv 1 \pmod 7.$$

En multipliant cette congruence par 15 on obtient $x_3 \equiv 15 \pmod{105}$. Voilà, c'est terminé ! Notre nombre x recherché vérifie donc

$$\begin{aligned} x &\equiv 1 \cdot x_1 + 3 \cdot x_2 + 3 \cdot x_3 \pmod{105} \\ &\equiv 70 + 3 \cdot 21 + 3 \cdot 15 \pmod{105} \\ &\equiv 73 \pmod{105}. \end{aligned}$$

Puisque cette congruence admet une seule solution en dessous de 100, on peut en déduire que $x = 73$ est notre nombre recherché. Vous pouvez alors vérifier à la main que 73 est bien solution de notre système.

20 Le théorème des restes chinois

Le fameux théorème des restes chinois permettra d'affirmer l'unicité de la solution des systèmes de la forme

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

Nous prendrons ici m_1 et m_2 premiers entre eux. Notre théorème affirme en d'autres termes que chacun des nombres $0 \leq x < m_1 m_2$ admet une unique représentation (r_1, r_2), où r_1 et r_2 désignent respectivement les restes de x modulo m_1 et modulo m_2. Un exemple, comme toujours, vaut bien mieux qu'un long discours. Prenons les entiers $x = 0, 1, \ldots, 19$ et regardons leurs restes $x \pmod 4$ et $x \pmod 5$. En effet, nous avons le tableau

40. J'utilise ici la propriété évidente $a \equiv b \pmod n$ implique que $ma \equiv mb \pmod{mn}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$x \pmod 4$	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
$x \pmod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

Nous pouvons voir dans ce tableau que chaque $0 \leq x < 20$ est représenté de façon unique par le couple

$$(x \pmod 4, x \pmod 5).$$

Par exemple, le couple $(1,0)$ ne représente que le nombre 5, $(3,1)$ correspond uniquement à 11 et $(3,0)$ à 15 etc. Il est relativement facile de voir la raison pour laquelle cela fonctionne. D'abord $x \pmod 4$ décrit la séquence $01230123\ldots$ de façon périodique de période égale à 4. De même $x \pmod 5$ décrit la séquence $0123401234\ldots$ avec une période égale à 5. Ainsi, aucune paire ne se répète avant le **ppcm**[41] de $(4,5)$, à savoir $4 \cdot 5 = 20$.

Plus généralement,

- $x \pmod{m_1}$ prend les valeurs $012\ldots(m_1-1)012\ldots(m_1-1)\ldots$ de façon périodique de période égale à m_1.
- De même, $x \pmod{m_2}$ décrit la suite $012\ldots(m_2-1)012\ldots(m_2-1)\ldots$ de période égale à m_2.
- Ainsi, aucune paire ne se répète avant le $\text{ppcm}(m_1,m_2) = m_1 m_2$, car le pgcd de m_1 et m_2 vaut 1.[42]

Revenons maintenant au cas d'un système contenant n équations, s'écrivant sous la forme

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \\ & \vdots \\ x & \equiv a_n \pmod{m_n} \end{cases}$$

où les m_i sont deux à deux premiers entre eux, c'est-à-dire pour tous $i \neq j$, le pgcd de m_i et de m_j vaut 1. Le théorème chinois affirme que ce système admet une unique solution

$$x \equiv a \pmod{m_1 \cdot m_2 \cdots m_n}.$$

Nous avons vu ensemble l'algorithme permettant de trouver un tel a, que nous allons généraliser dans la suite dans le but de mieux comprendre son fonctionnement. On sait alors que pour se faire, il suffit de résoudre les n systèmes auxiliaires

$$\begin{cases} x_1 \equiv 1 \pmod{m_1} \\ x_1 \equiv 0 \pmod{m_i} \quad i \neq 1 \end{cases}; \begin{cases} x_2 \equiv 1 \pmod{m_2} \\ x_2 \equiv 0 \pmod{m_i} \quad i \neq 2 \end{cases}; \ldots \begin{cases} x_n \equiv 1 \pmod{m_n} \\ x_n \equiv 0 \pmod{m_i} \quad i \neq n \end{cases}$$

Résolvons ensemble le premier système. Les congruences $x_1 \equiv 0 \pmod{m_i}$ pour tout $i \neq 1$ signifient que chacun des m_i divise x_1. Puisqu'ils sont deux à deux premiers entre eux, on peut en déduire que le nombre $M_1 = m_2 \cdot m_3 \cdots m_n$ divise x_1. Il existe donc un entier k_1 tel que $x_1 = M_1 k_1$. La congruence $x_1 \equiv 1 \pmod{m_1}$ devient alors

$$M_1 k_1 \equiv 1 \pmod{m_1}.$$

41. Le mot ppcm désigne le plus petit commun multiple.
42. J'utilise ici la fameuse identité $\text{pgcd}(a,b) \times \text{ppcm}(a,b) = ab$, où a et b désignent deux entiers naturels.

La question revient donc à inverser M_1 modulo m_1. D'abord, est-il inversible ? Bien sûr que oui puisque le pgcd de M_1 et de m_1 vaut 1 [43]. Pour trouver cet inverse, le tout revient à utiliser l'algorithme d'Euclide étendu, d'où la résolubilité de notre premier système.

Les choses se passent de la même manière pour un système quelconque

$$\begin{cases} x_i & \equiv 1 \pmod{m_i} \\ x_i & \equiv 0 \pmod{m_j} \quad j \neq i \end{cases}$$

Dans ce cas, le nombre $M_i = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_n$ doit diviser x_i, auquel cas il existe un entier k_i tel que $x_i = M_i k_i$. La résolution de notre système revient alors à résoudre la congruence

$$M_i k_i \equiv 1 \pmod{m_i},$$

ce qui revient à inverser le nombre inversible M_i. Une fois les n systèmes résolus, notre solution sera donnée par

$$x \equiv a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \pmod{M},$$

où $M = m_1 m_2 \cdots m_n$. [44] En ce qui concerne l'unicité de cette solution modulo M, si y est une deuxième solution de notre système, c'est-à-dire si $y \equiv a_i \pmod{m_i}$ pour tout i alors

$$x \equiv y \pmod{m_i},$$

ce qui implique naturellement que $x \equiv y \pmod{M}$, voyez-vous pourquoi ? Passons maintenant aux choses exotiques et donc à la programmation de notre algorithme sur Python.

```
def euc_ext(a,mod):
    x = 1 ; xx = 0
    y = 0 ; yy = 1
    while mod != 0:
        q = a // mod
        a, mod = mod, (a % mod)
        xx, x = x - q*xx , xx
        yy, y = y - q*yy , yy
    return x

def Chinese(lst_a, lst_mod):
    n = len(lst_a)
    modulus = 1
    sol = 0
    for i in range(n):
        modulus = modulus * lst_mod[i]
    lst = [modulus//lst_mod[i] for i in range(n)]
    for i in range(n):
        inv = euc_ext(lst[i]%(lst_mod[i]), lst_mod[i])
        sol += lst_a[i]*(inv % lst_mod[i])*lst[i]
    return sol%modulus
```

L'algorithme euc_ext est tout simplement l'algorithme d'Euclide étendu, permettant de résoudre l'équation $ax \equiv 1 (\text{mod})$, à condition que a et mod soient premiers entre eux. L'algorithme principal Chinese prend deux listes en argument, lst_a contiendra les a_i et lst_mod

43. Je vous rappelle qu'un nombre a est inversible modulo n si et seulement si le pgcd de a et de n vaut 1.
44. Il est intéressant de noter que $M_i = M/m_i$. Cette remarque nous sera utile dans la programmation de l'algorithme chinois sur Python.

les m_i. La première boucle *for* permet de calculer le nombre $M = m_1 m_2 \cdots m_n$. L'algorithme crée par la suite la liste lst contenant les M_i. La deuxième boucle *for* fait appel à euc_ext afin d'inverser chacun des M_i modulo m_i et calcule par la même occasion la solution de notre système.

Essayons notre algorithme avec le système

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

Je vous rappelle alors qu'on a résolu ce système auparavant, pour lequel $x \equiv 23 \pmod{35}$ est la solution. L'exécution donne

```
>>> Chinese([3, 2], [5, 7])
23
```

Bingo ! Quelle satisfaction quand tout tourne bien ! Pour s'en convaincre davantage, nous allons prendre un deuxième exemple. Soit le système

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

Remarquez que l'on peut résoudre ce système astucieusement et sans l'algorithme de nos ancêtres chinois. Il est en effet équivalent au système

$$\begin{cases} x \equiv -1 \pmod 3 \\ x \equiv -1 \pmod 5 \\ x \equiv -1 \pmod 7 \end{cases}$$

Une solution triviale de ce système est donc $x \equiv -1 \pmod{3 \cdot 5 \cdot 7} \equiv 104 \pmod{105}$. Regardons alors si c'est bien le cas sur Python.

```
>>> Chinese([2, 4, 6], [3, 5, 7])
104
```

Yesss ! Je vous invite à résoudre davantage de systèmes à la main et à aller sur Python afin de vérifier vos résultats.

21 Le théorème d'Euler

Le théorème d'Euler est une généralisation du petit théorème de Fermat, affirmant que si p est un nombre premier et $a \not\equiv 0 \pmod p$ alors

$$a^{p-1} \equiv 1 \pmod p.$$

En effet, la congruence ci-dessus dit ce qui se passe modulo un nombre premier p mais ne précise pas ce qui se déroule pour un entier naturel n quelconque. Par exemple, si $n = 9$ et $a = 2$ alors

$$a^{n-1} = 2^{9-1} = 256 \equiv 4 \pmod 9 \not\equiv 1 \pmod 9.$$

On voit alors que le petit théorème de Fermat n'est plus valide quand n n'est pas un nombre premier. Toutefois, il permet de conclure si par exemple $n = pq$, où p et q désignent deux nombres premiers distincts. Par exemple si $(a, 21) = 1$ alors on peut conclure que $a^{12} \equiv 1 \pmod{21}$. Pour s'en convaincre, remarquons tout d'abord que

$$a^{12} \equiv 1 \pmod{21} \iff \big(a^{12} \equiv 1 \pmod{3} \quad \text{et} \quad a^{12} \equiv 1 \pmod{7}\big),$$

car 3 et 7 sont premiers entre eux. Les deux dernières congruences se déduisent trivialement du PTF [45]. En effet, $a \not\equiv 0 \pmod{3}$ car $(a, 21) = 1$, donc

$$a^2 \equiv 1 \pmod{3}.$$

Par conséquent $a^{12} \equiv (a^2)^6 \equiv 1 \pmod{3}$. Le même argument fonctionne pour $a^{12} \equiv 1 \pmod{7}$. Le résultat en découle. Toutefois, le PTF ne permet pas de conclure quand n est un carré parfait, comme par exemple avec 9. Regardons ensemble ce qui se passe modulo un entier naturel n avec Python.

```
def power(n):
    for a in range(1, n):
        lst = [(a**i)%n for i in range(1, n)]
        print(lst)
```

Cet algorithme permet d'afficher les puissances successives d'un entier a modulo n. En exécutant avec $n = 9$ on obtient

```
>>> power(9)
[1, 1, 1, 1, 1, 1, 1, 1]
[2, 4, 8, 7, 5, 1, 2, 4]
[3, 0, 0, 0, 0, 0, 0, 0]
[4, 7, 1, 4, 7, 1, 4, 7]
[5, 7, 8, 4, 2, 1, 5, 7]
[6, 0, 0, 0, 0, 0, 0, 0]
[7, 4, 1, 7, 4, 1, 7, 4]
[8, 1, 8, 1, 8, 1, 8, 1]
```

Quelques commentaires s'imposent ici. La première liste contient les puissances de $a = 1$ et il est tout à fait naturel d'avoir des 1 partout. La deuxième liste contient les puissances successives de $a = 2$. On voit alors que le premier exposant m pour lequel $2^m \equiv 1 \pmod{9}$ est $m = 6$. On voit dans la troisième liste qu'aucune puissance de 3 ne donne 1 modulo 9, le même phénomène se produit pour $a = 6$. Par ailleurs, on remarque que pour tout a tel que le pgcd de a et de 9 vaut 1

$$a^6 \equiv 1 \pmod{9}.$$

Nous allons montrer ce résultat en suivant les pas d'Euler. Nous commençons tout d'abord par trouver les éléments inversibles modulo 9. Je vous rappelle qu'un nombre x est inversible modulo 9 si et seulement s'il existe y tel que $xy \equiv 1 \pmod{9}$, si et seulement si le pgcd de x et de 9 vaut 1. Les nombres $0 < x < 9$ vérifiant cette dernière condition sont

$$\{1, 2, 4, 5, 7, 8\}.$$

Les entiers 3 et 6 ne font pas partie de la liste car ils ne sont pas premiers avec 9. Notez alors qu'il existe, comme par hasard, exactement 6 éléments inversibles modulo 9. Si a est premier avec 9 on a

$$(a \cdot 1)(a \cdot 2)(a \cdot 4)(a \cdot 5)(a \cdot 7)(a \cdot 8) \equiv (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)a^6 \pmod{9}$$

45. PTF est une abbréviation du petit théorème de Fermat.

Notez alors qu'on a pris le produit des $a \cdot u$, où u parcourt la liste des nombres inversibles modulo 9. Les $a \cdot u$ sont tous inversibles et distincts donc ce produit est une permutation des nombres inversibles modulo 9. Ainsi on obtient

$$(a \cdot 1)(a \cdot 2)(a \cdot 4)(a \cdot 5)(a \cdot 7)(a \cdot 8) \equiv 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \pmod 9.$$

En notant N le nombre $1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8$ on obtient la congruence

$$Na^6 \equiv N \pmod 9.$$

Or le nombre N est inversible donc on peut simplifier par N de part et d'autre pour obtenir

$$a^6 \equiv 1 \pmod 9.$$

Le cas général se traite de la même manière et il suffit de compter à chaque fois le nombre d'éléments inversibles modulo un nombre n. Pour se faire, nous allons considérer une nouvelle fonction, la fameuse **fonction indicatrice d'Euler**, qu'on dénote φ. Ainsi, $\varphi(n)$ désignera le nombre d'éléments inversibles modulo n. En d'autres termes, nous allons compter le nombre de a premier avec n, ce qui signifie que

$$\varphi(n) = \#\{1 \leq a \leq n-1, \quad (a,n) = 1\},$$

où $\#E$ désigne le cardinal de l'ensemble E. Le théorème d'Euler dit alors que si le pgcd de a et n vaut 1 alors

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Ce théorème est une généralisation du petit théorème de Fermat car si n est un nombre premier alors $\varphi(n) = n-1$, car le seul élément non inversible dans ce cas est 0. On obtient bien du coup $a^{n-1} \equiv 1 \pmod n$ si $a \not\equiv 0 \pmod n$. Venons-en maintenant à la démonstration du théorème d'Euler. Notons $u_1, u_2, \ldots, u_{\varphi(n)}$ les éléments inversibles modulo n. D'une part, on a

$$(a \cdot u_1)(a \cdot u_2) \cdots (a \cdot u_{\varphi(n)}) \equiv (u_1 \cdot u_2 \cdots u_{\varphi(n)})a^{\varphi(n)} \pmod n.$$

Par ailleurs, les $a \cdot u_i$ sont distincts et inversibles. Il s'ensuit que

$$(a \cdot u_1)(a \cdot u_2) \cdots (a \cdot u_{\varphi(n)}) \equiv u_1 \cdot u_2 \cdots u_{\varphi(n)} \pmod n.$$

On obtient ainsi la congruence $Na^{\varphi(n)} \equiv N \pmod n$, où $N = u_1 \cdot u_2 \cdots u_{\varphi(n)}$. L'entier N étant inversible, on obtient

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Avant de terminer cette section, montrons tout de même que les $a \cdot u_i$ sont deux à deux distincts et qu'ils sont inversibles. En effet, pour la première assertion si $au_i \equiv au_j \pmod n$ alors on peut simplifier de part et d'autre par a car cet élément est inversible par hypothèse. On en déduit alors que $u_i \equiv u_j \pmod n$. En ce qui concerne l'inversibilité de $a \cdot u_i$, il s'agit d'une propriété générale sur les éléments inversibles. Si x et y sont deux éléments inversibles alors xy l'est aussi. En effet, en notant x^{-1} et y^{-1} les inverses respectifs de x et de y, l'inverse de xy est $y^{-1}x^{-1}$ car

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &\equiv x(yy^{-1})x^{-1} \pmod n \\ &\equiv xx^{-1} \pmod n \quad \text{car } yy^{-1} \equiv 1 \pmod n \\ &\equiv 1 \pmod n.\end{aligned}$$

Le résultat en découle. Prenons maintenant un exemple du théorème d'Euler. Si $n = 8$ et a est premier avec 8, notre théorème affirme que

$$a^{\varphi(8)} \equiv 1 \pmod 8.$$

Mais combien vaut $\varphi(8)$ dans ce cas ? Les nombres $1 \leq x \leq 7$ premiers avec 8 sont

$$\{1, 3, 5, 7\}.$$

Ainsi $\varphi(8) = 4$ et donc $a^4 \equiv 1 \pmod 8$. Magique ! Cela fonctionne-t-il vraiment ? Sur Python, l'exécution de notre fonction power donne

```
>>> power(8)
[1, 1, 1, 1, 1, 1, 1]
[2, 4, 0, 0, 0, 0, 0]
[3, 1, 3, 1, 3, 1, 3]
[4, 0, 0, 0, 0, 0, 0]
[5, 1, 5, 1, 5, 1, 5]
[6, 4, 0, 0, 0, 0, 0]
[7, 1, 7, 1, 7, 1, 7]
```

Incroyable !