Pour tout entier n, $\sqrt{n}$ est entier ou irrationnel

Une belle application du théorème de Gauss en Terminale.
Pourquoi pas un théorème d'Euclide ?

Michel Henry,
IREM de Franche-Comté

Sommaire

1 L'irrationalité de $\sqrt{2}$, conséquence immédiate du théorème de Gauss

1.1 $\sqrt{2}$ est irrationnel : la crise

L'irrationalité de $\sqrt{2}$ a illustré la « crise des irrationnelles[1] » dans la Grèce antique. L'Histoire a retenu la légende rapportant le désarroi de la secte pythagoricienne devant

[1] Il s'agit des « quantités irrationnelles ».

l'effondrement de sa conception réductrice du monde réel en termes de nombres entiers : Hippasos de Métaponte, celui qui vendit la mèche, fut englouti par les flots[2].

Le carré construit sur la diagonale d'un carré donné a une aire double de ce dernier, alors que leurs côtés ne sont pas dans un rapport exprimable avec les connaissances des Anciens. Cette construction de géométrie très élémentaire est exploitée par Socrate pour amener le serviteur de Ménon au constat de sa connaissance[3].

La preuve de l'incommensurabilité entre la diagonale et le côté d'un carré peut être purement géométrique :

> Si la diagonale et le côté étaient mesurés par une même unité (i.e. en seraient des multiples entiers), on pourrait construire un carré de côté plus petit que la moitié du précédent et qui serait mesuré par cette même unité. On peut itérer cette construction jusqu'à obtenir une longueur mesurée par une unité plus grande qu'elle !

Cette démonstration (dite par anthyphérèse[4]) met en œuvre l'opposition de nature entre les nombres (entiers), prototypiques du discret, et les grandeurs (au sens euclidien), représentatives du continu (i.e. divisibles à l'infini).

Une démonstration d'inspiration arithmétique figure dans la traduction de Peyrard (1819)[5] des *Éléments* d'Euclide, formulée dans le cadre géométrique (Livre X, prop. 117, cf. cette démonstration en annexe page 30)[6].

La preuve arithmétique était déjà donnée par Aristote[7] (384–322 av. J.-C.), inspirant la démonstration traditionnelle[8] que l'on peut décomposer ainsi (petit échauffement) :

- Supposons qu'il existe un nombre rationnel α dont le carré soit égal à 2. Notons que α n'est pas entier, puisque 2 ne figure pas dans la suite croissante des carrés parfaits.

[2] Jean Dhombres, dans *Nombre, mesure et continu* (CEDIC-Nathan, IREM de Nantes, 1978), rapporte le commentaire de Proclus (Ve siècle apr. J.-C.) : « Les auteurs de la légende ont voulu parler par allégorie. Ils ont voulu dire que tout ce qui est irrationnel et privé de formes doit demeurer caché. Que si quelque âme veut pénétrer dans cette région secrète et la laisser ouverte, alors elle est entraînée dans la mer du devenir et noyée dans l'incessant mouvement de ses courants ».

[3] Dialogue du *Ménon* de Platon (428–347 av. J.-C.).

[4] L'anthyphérèse de deux grandeurs est la suite des quotients successifs obtenus par l'algorithme d'Euclide (cf. section 2).

[5] *Les Œuvres d'Euclide, traduites littéralement par F. Peyrard*, réédité par la Librairie Blanchard, Paris, 1993.

[6] Le Livre X des *Éléments* traite des grandeurs incommensurables et propose une classification à base géométrique de l'irrationalité. Malgré les Livres d'arithmétique précédents (Livres VII à IX), les nombres considérés sont des mesures entières de grandeurs. Des recherches récentes (Bernard Vitrac : *Euclide, les Éléments*, vol. 3 p. 411, PUF, 1998) semblent indiquer que cette proposition 117 ne figurait pas dans l'original des *Éléments* (IIIe siècle av. J.-C.) et a été rajoutée par les premiers commentateurs avant le IVe siècle de notre ère, reprenant la démonstration d'Aristote.

[7] Notamment dans *Les Premiers Analytiques*, mais il l'évoque à plusieurs reprises comme une propriété familière de son lecteur. Sa réduction à l'absurde tient au fait qu'il n'existe aucun nombre qui soit à la fois pair et impair.

[8] Première question d'écrit au CAPES interne en 2000.

- Ce rationnel α peut être représenté par une fraction irréductible $\frac{a}{b}$.[9] D'après la remarque précédente, on a nécessairement : $b > 1$.
- Conservant avec l'existence de α les propriétés des opérations arithmétiques, on a :

$$a^2 = \alpha^2 b^2 = 2b^2.$$

- a^2 est donc pair. Mais comme le carré de tout nombre impair est impair (si $m = 2k+1$, alors $m^2 = 4k^2 + 4k + 1 = 2k' + 1$), a est nécessairement pair : c'est le principe du tiers exclu (un nombre ne peut être à la fois pair et impair, argument d'Aristote) appliqué à l'énoncé contraposé du précédent.
- On a donc $a = 2a'$, d'où $4a'^2 = 2b^2$ et $2a'^2 = b^2$. b^2 est donc pair, ce qui, comme précédemment, montre que b est pair.
- La fraction α n'est donc pas irréductible puisque a et b ont 2 pour diviseur commun ![10]

L'hypothèse que $\sqrt{2}$ est rationnel est donc à rejeter.

Si l'on veut considérer le rapport entre la diagonale et le côté d'un carré comme un *nombre* (que nous désignons par $\sqrt{2}$ en application du théorème de Pythagore), ce nombre ne peut donc être rationnel. Il ne fait pas partie des nombres concevables en tant que tels par les Grecs, et pourtant il est facilement constructible en géométrie.

La question générale de l'irrationalité de $\sqrt{n}$ ne semble pas se poser naturellement pour les Anciens, même si elle est à leur portée. Il est curieux de constater que tous les arguments nécessaires sont rassemblés dans le Livre VII des *Éléments* d'Euclide[11] (prop. 20 à 25), comme nous le verrons dans la deuxième partie de cet article, mais que cette conclusion n'y figure pas.

Cependant, les cas $n = 3, 5, \ldots, 17$ ont été résolus séparément[12]. Pourquoi produire autant de démonstrations (que d'entiers non carrés parfaits !), se ramenant de plus en plus laborieusement à l'argument aristotélicien de parité, alors que l'on peut aisément démontrer la propriété générale pour $\sqrt{n}$ avec les connaissances de l'époque, aujourd'hui enseignées en Terminale ? Il y a là une petite énigme historique.

[9] Ce raisonnement suppose donc que tout rationnel peut être représenté par une fraction irréductible, conséquence de l'existence du PGCD. L'existence, l'unicité et les propriétés de la fraction irréductible égale à une fraction (un rationnel) donnée fait l'objet de la deuxième partie de cet article.

[10] Le symbole ! à la fin d'une démonstration signifie la mise en évidence d'une contradiction avec une hypothèse introduite antérieurement. Le raisonnement « par l'absurde » permet alors de conclure que cette hypothèse est fausse, ceci en admettant la non contradiction du reste de la théorie.

[11] Bernard Vitrac (*Euclide, Les Éléments*, vol. 2, p. 288) indique que ce Livre VII est « attribué à des Pythagoriciens, de l'époque précédant Archytas » (Archytas de Tarente, 428–347 av. J.-C.).

[12] Jean Dhombres (op. cité) signale que Théodore de Cyrène (460–369 av. J.-C.) avait obtenu l'irrationalité de $\sqrt{3}$, $\sqrt{5}$, ... et cite le témoignage de Platon selon lequel Théétète disposait d'une démonstration de l'irrationalité de $\sqrt{17}$.

1.2 $\sqrt{n}$ est entier ou irrationnel

Nous allons voir que l'irrationalité de $\sqrt{n}$ pour n entier non carré parfait découle directement du théorème de Gauss[13], habituellement énoncé comme suit :

> *Soient a, b, c trois entiers naturels. Si a est premier avec b et si a divise le produit bc, alors a divise c.*[14]

Pour notre problème, nous utiliserons le cas particulier suivant, que l'on peut présenter comme conséquence directe du théorème de Gauss :

Lemme : *Si p premier divise a^2, alors p divise a.*[15]

> En effet, p étant premier, p et a ne peuvent avoir que p comme diviseur commun. Si p ne divisait pas a, alors p et a seraient premiers entre eux et, d'après le théorème de Gauss, p divisant le produit $a \times a$, p diviserait le second facteur a !

On peut obtenir l'irrationalité de $\sqrt{n}$ de deux manières différentes, aussi simples l'une que l'autre. On procède d'abord comme pour $\sqrt{2}$:

- Supposons que $\sqrt{n}$ soit rationnel non entier.
- Alors il existe un couple d'entiers non nuls (a, b), premiers entre eux, tels que $\sqrt{n} = \dfrac{a}{b}\cdot$
- Comme $\sqrt{n}$ n'est pas entier, $b > 1$, et par définition de $\sqrt{n}$, $a^2 = nb^2$.

À partir de cette égalité, il y a deux démarches possibles pour établir une contradiction : considérer a ou b comme diviseurs respectivement de nb^2 ou de a^2 (dans le cas de $\sqrt{2}$, on avait considéré 2 comme diviseur, ce qui se prête moins facilement aux généralisations) :

---

[13] Au programme de Terminale S, enseignement de spécialité. C'est un théorème pivot (osons le terme !) de l'arithmétique dans $\mathbb{N}$.

[14] On peut aussi retenir la forme particulière suivante, donnée par Euclide dans les *Éléments* (Livre VII, prop. 30), que l'on peut énoncer ainsi : *Si p premier divise un produit ab, alors p divise a ou divise b.*

[15] Ce lemme se trouve aussi dans les *Éléments* d'Euclide (Livre VII, prop. 25) sous une forme contraposée plus générale : *Si deux nombres sont premiers entre eux, le carré de l'un est premier avec l'autre* (cf. paragraphe 2.6).

Première démarche avec b :

- Soit p un diviseur premier de b.[16]
- Comme $a^2 = nb^2$, p divise a^2.
- Alors, d'après le lemme, p divise a.
- Mais a et b ont été supposés premiers entre eux, ils ne peuvent avoir p pour diviseur commun !

Deuxième démarche avec a :

- Comme a et b sont premiers entre eux, a^2 et b^2 le sont également, sinon, d'après le lemme, un diviseur premier commun à a^2 et b^2 serait un diviseur commun à a et b.
- Comme $a^2 = nb^2$, d'après le théorème de Gauss, a^2 divise n, ce qui implique $b = 1$!

l'hypothèse « $\sqrt{n}$ non entier et rationnel » est donc absurde, sa négation « $\sqrt{n}$ est entier ou irrationnel » est donc démontrée.

1.3 Place du Théorème de Gauss dans les deux progressions usuelles en arithmétique

Remarquons que la première démarche n'utilise en fait que notre lemme : « si p premier divise a^2, alors il divise a », que nous avons introduit comme application du théorème de Gauss.

Dans la progression des *Éléments* d'Euclide, le théorème de Gauss est directement issu des propriétés de la division euclidienne mises en œuvre dans l'algorithme d'Euclide[17] :

- Si a et b sont premiers entre eux, 1 est le dernier reste non nul dans l'algorithme d'Euclide engendré par a et b.
- En multipliant chaque égalité de cet algorithme par c, on obtient l'algorithme engendré par ac et bc, et le dernier reste non nul est c.
- a divise ac et bc, a divise donc tous les restes successifs de cet algorithme jusqu'au dernier non nul : a divise c.

Dans ce premier point de vue, le théorème de Gauss se présente comme un résultat précurseur du théorème fondamental de l'arithmétique[18] (sa démonstration n'est pas exigible en Terminale S) :

[16] Tout nombre $b \geqslant 2$ admet au moins un diviseur premier. En effet, l'ensemble de ses diviseurs est non vide (contenant b lui-même) et comme toute partie non vide de $\mathbb{N}$, il admet un plus petit élément p. p est donc un diviseur de b et p est premier, sinon un diviseur strict de p serait aussi diviseur de b et plus petit que p !

Cette remarque est à la base du théorème d'existence et d'unicité de la décomposition d'un entier en produit de facteurs premiers.

[17] Ayant $a = bq + r$, avec $0 \leqslant r < b$, si $r \neq 0$, l'algorithme d'Euclide consiste à diviser b par r, ce qui donne un reste $r_1 < r$, puis alternativement les restes successifs entre eux, strictement décroissants, jusqu'à obtenir le dernier reste non nul δ qui est alors divisible par tous les diviseurs communs à a et b. δ est le PGCD de a et b (Livre VII, prop. 2).

[18] Ce théorème a été énoncé explicitement par Gauss dans ses *Recherches Arithmétiques* (1801), mais il

Pour tout a supérieur ou égal à 2, il existe une famille finie unique $p_1, \ldots, p_k$ de nombres premiers distincts et une famille unique d'entiers non nuls $\mu_1, \ldots, \mu_k$ telles que $a = p_1^{\mu_1} \ldots p_k^{\mu_k}$.

On peut cependant inverser la progression et tirer le théorème de Gauss de l'existence et de l'unicité de cette décomposition, obtenue comme conséquence d'axiomes du type de ceux de Péano, comme certains traités d'arithmétique le présentent. La division euclidienne est alors impliquée par le théorème de Gauss[19].

Dans ce deuxième point de vue, notre lemme (« *si p premier divise a^2, alors il divise a* ») est une conséquence immédiate du théorème de décomposition :

> En effet, si $a = p_1^{\mu_1} \ldots p_k^{\mu_k}$, alors $a^2 = p_1^{2\mu_1} \ldots p_k^{2\mu_k}$, a et a^2 ont donc la même famille de facteurs premiers. p fait partie de la famille des facteurs premiers de a^2, donc de celle de a.

La progression d'Euclide met bien en évidence le rôle de fondement de l'arithmétique (dans $\mathbb{N}$) joué par la division euclidienne. Cette progression exploite largement toutes les propriétés de la division que les élèves ont trop tendance à négliger.

La démonstration que l'on trouve dans les *Éléments* semble moins simple que la démonstration « classique », car elle fait le détour par une proposition « clé »[20] qui revient à prouver l'existence et l'unicité de la fraction irréductible égale à une fraction donnée. Elle a cependant l'avantage d'éviter le raisonnement par récurrence (techniquement lourd à exposer) implicite dans la démonstration « classique ».

La démonstration d'Euclide est assez belle, je vous invite à la regarder, car elle peut suggérer un excellent thème de travail autour de la division euclidienne, en fin de compte seule responsable de l'irrationalité de $\sqrt{n}$ quand n n'est pas un carré parfait.

2 Le théorème de Gauss dans *Les Éléments* d'Euclide

2.1 La division euclidienne

Pour Euclide, toute l'arithmétique dans $\mathbb{N}^*$ repose sur cette division qui n'est pas présentée explicitement, tellement elle est « naturelle ». Du point de vue pédagogique,

---

est quasiment présent dans les *Éléments* d'Euclide (Livre VII, prop. 32) : « *Tout nombre est soit premier soit mesuré par un certain nombre premier* ». L'existence de la décomposition d'un entier en facteurs premiers en découle par divisions de cet entier par ses facteurs premiers successifs jusqu'à épuisement du sujet. L'unicité provient directement de la forme particulière du théorème de Gauss (prop. 30) citée en note 14.

[19] Pour comparer ces deux démarches, on pourra consulter l'excellente brochure de l'IREM d'Aquitaine : *Initiation à l'arithmétique*, 1999.

[20] Livre VII, prop. 20. Son étude fait l'objet de la deuxième partie de cet article.

nous en faisons le « **Théorème de la division euclidienne** » :

> *Pour tout couple d'entiers non nuls (a, b) tels que $a \geqslant b$, il existe un couple unique d'entiers (q, r) tel que : $a = bq + r$, avec $q \geqslant 1$ et $0 \leqslant r < b$.*

Résultat obtenu simplement en retranchant b de a autant de fois qu'il est possible. Le reste r est donc strictement inférieur à b, sinon on pourrait enlever b de $a - bq$ une fois de plus.

Dans notre formulation modernisée, r peut être nul : c'est le cas où a est divisible par b.[21]

Nous disons alors que « b divise a » au lieu de « b mesure a » comme le fait Euclide qui pense l'arithmétique dans le cadre géométrique.

2.2 La progression des *Éléments* d'Euclide

Le premier Livre d'arithmétique, le Livre VII, commence par ce que l'on appelle aujourd'hui « l'algorithme d'Euclide » (Livre VII, prop. 1)[22], puis applique cet algorithme à des recherches de PGCD (prop. 2).

Algorithme d'Euclide : « *Deux nombres inégaux étant proposés et le plus petit étant retranché du plus grand de façon réitérée et en alternance, si le reste ne mesure jamais le [reste] précédent jusqu'à ce qu'il subsiste une unité, les nombres initiaux seront premiers entre eux* ».

Euclide établit ensuite quelques propriétés élémentaires des opérations arithmétiques et des proportions, puis s'intéresse particulièrement aux couples d'entiers proportionnels pour lesquelles le premier couple est formé par des nombres premiers entre eux (prop. 20 à 23, que nous proposerons de rassembler sous l'appellation de « théorème d'Euclide »). Il en tire la proposition 24, proche du théorème de Gauss (cf. paragraphe 2.6) :

Proposition 24 : « *Si deux nombres sont premiers avec un certain nombre, leur produit sera aussi premier avec ce même [nombre]* ».

Traduisons : Si a est premier avec b et avec c, a est premier avec le produit bc.

D'où le cas particulier qui nous intéresse, car il implique notre lemme :

---

[21] Dans la suite, les nombres considérés sont des entiers naturels non nuls, sauf mention du contraire. Pour rester dans le cadre de l'arithmétique dans $\mathbb{N}^*$, nous éviterons les écritures fractionnaires. Le mot diviseur désigne un entier strictement supérieur à 1 : d est diviseur de a non nul s'il existe un quotient $q \geqslant 1$ tel que $a = dq$. Ainsi, deux nombres sont premiers entre eux s'ils n'ont pas de diviseur commun.

[22] Les énoncés qui suivent ainsi que la numérotation des propositions sont ceux de l'ouvrage de Bernard Vitrac : *Euclide, les Éléments*, vol. 2, PUF, 1994. Pour bien apprécier la démarche euclidienne, il est bon de disposer des énoncés authentiques donnés par Euclide. Nous interpréterons cependant au besoin ces énoncés dans des formulations qui nous sont aujourd'hui plus claires et synthétiques.

Proposition 25 : « *Si deux nombres sont premiers entre eux, le produit de l'un d'eux [par lui-même] sera premier avec celui qui reste* ».

Si a est premier avec b, alors a est premier avec b^2.

Il déduit enfin de la proposition 24 la forme particulière du théorème de Gauss, utile en pratique :

Proposition 30 : « *Si deux nombres se multipliant l'un l'autre produisent un certain [nombre] et si un certain nombre premier mesure leur produit, il mesurera aussi l'un des nombres initiaux* ».

Si p premier divise ab, il divise a ou il divise b.

2.3 Couples d'entiers en « même rapport »

Pour comparer des grandeurs de même espèce, Euclide introduit la notion de « raison » comme « *une certaine manière d'être de deux grandeurs homogènes, suivant la quantité* »[23]. S'il ne peut donner une définition claire de cette notion de « raison » (car il s'agit en fait de rapports de nombres réels lorsque les grandeurs sont mesurées par une unité commune), il donne par contre une définition très précise mais sophistiquée de la propriété pour deux couples de grandeurs d'être « en même raison » (i.e. proportionnelles : Livre V, déf. 6).

Transposée aux couples de nombres (entiers) susceptibles de se multiplier, cette notion correspond à leur « rapport » qu'Euclide ne définit pas. Par contre, comme pour comparer les raisons entre grandeurs, Euclide définit précisément l'égalité entre rapports de nombres (Livre VII, déf. 21) :

« *Des nombres sont en proportion quand le premier, du deuxième, et le troisième, du quatrième, sont équimultiples...* »

$\frac{a}{b} = \frac{c}{d}$ s'il existe deux entiers p et q tels que $qa = pb$ et $qc = pd$.

Nous l'utiliserons plutôt sous la forme suivante :

Les couples de nombres entiers non nuls (a, b) et (c, d) sont « en même rapport » si et seulement si ils forment une proportion, c'est-à-dire s'ils vérifient l'égalité : $ad = bc$.

Euclide énonce ainsi cette proportionnalité : « *a est à b comme c est à d* », locution qui sera symbolisée plus tard par « $a : b :: c : d$ ».

Cette notation est maintenant désuète, remplacée pour les nombres par $\frac{a}{b} = \frac{c}{d}$ (cela suppose d'avoir défini le rationnel représenté par ces fractions, ce qui n'est pas

[23]Dans sa traduction, Peyrard (op. cité) utilise le terme de « raison » plus vague que celui de « rapport » figurant dans le texte de Vitrac. Cette notion de raison est introduite dans le Livre V des *Éléments* comme fondement de la théorie des proportions entre grandeurs, dont la construction est vraisemblablement due à Eudoxe (408–355 av. J.-C.). Certains commentateurs prétendent que cette définition (Livre V, déf. 3) a été rajoutée par la suite.

nécessaire dans la suite), mais elle avait l'avantage d'être plus générale, concernant aussi bien des grandeurs que des entiers. Elle autorisait certaines pratiques et techniques de la proportionnalité entre couples de grandeurs non nécessairement commensurables et éventuellement de natures différentes : longueurs, aires, ... (dans ce cas, cette proportionnalité ne peut être exprimée en termes numériques sans une théorie de la mesure élaborée, supposant la construction des nombres réels).

Pour nous, un rationnel non nul est défini comme quotient de deux entiers (c, d) non nuls, représenté en écriture fractionnaire par $\frac{c}{d}\cdot$

Le fond de la démarche euclidienne est de remarquer que ce rationnel peut être représenté **de manière unique** par une fraction irréductible $\frac{a}{b}\cdot$ Cela revient à montrer qu'il existe un couple **unique** de nombres non nuls (a, b) premiers entre eux, qui sont dans le même rapport que (c, d) (i.e. $\frac{a}{b} = \frac{c}{d}$ où $\frac{a}{b}$ est irréductible)[24]. L'argument essentiel est que a et b sont les plus petits nombres parmi ceux qui sont dans le même rapport que c et d. Il s'en suit que pour tout autre couple (x, y) dans ce même rapport, x et y sont des équimultiples de a et b.

Remarquons que le résultat tire parti du lien entre la relation d'ordre naturel sur $\mathbb{N}^*$ et la relation de divisibilité. Ce lien sera finement exploité dans la démonstration d'Euclide que nous présentons dans le paragraphe suivant.

2.4 Le « théorème d'Euclide »

a) Les énoncés d'Euclide

Cette partie du Livre VII qui dégage les propriétés du couple minimal d'une proportion, comprend les trois propositions suivantes. Les énoncés donnés sont conformes au texte des *Éléments* puis interprétés :

Proposition 20, la clé de l'édifice :

« *Les plus petits nombres parmi ceux qui ont le même rapport qu'eux mesurent ceux qui ont le même rapport autant de fois, le plus grand le plus grand et le plus petit le plus petit* ».

> Si a et b sont deux entiers non nuls et si pour tout (c, d) formant avec (a, b) une proportion on a $a \leqslant c$ et $b \leqslant d$, alors il existe un entier q tel que $c = qa$ et $d = qb$.

[24] L'existence est immédiate, il suffit de considérer le PGCD δ de c et d, obtenu par exemple par l'algorithme d'Euclide, pour exhiber le couple (a, b) : posant $c = \delta a$ et $d = \delta b$, on a bien $ad = bc$, car chaque membre vaut $ab\delta$. De plus a et b sont premiers entre eux, car s'ils avaient un diviseur commun $q > 1$, alors $q\delta$ serait diviseur de c et d, et δ ne serait pas leur plus grand commun diviseur. L'unicité, implicitement, fait l'objet de la démonstration d'Euclide.

Proposition 21, la bonne remarque :

« *Les nombres premiers entre eux sont les plus petits parmi ceux qui ont le même rapport qu'eux* ».

Si a et b sont premiers entre eux, alors pour tout (c, d) formant avec (a, b) une proportion, on a $a \leqslant c$ et $b \leqslant d$.

Proposition 22, réciproque de la précédente :

« *Les nombres les plus petits parmi ceux qui ont le même rapport qu'eux sont premiers entre eux* ».

b) L'énoncé du « théorème d'Euclide »

De ces trois propositions, dégageons un énoncé synthétique plus moderne, que nous appelons le « **théorème d'Euclide** »[25] :

Soient (a, b) et (c, d) deux couples d'entiers non nuls en même rapport ($ad = bc$). Si a et b sont premiers entre eux, alors c et d sont équimultiples de a et b (i.e. il existe un entier q tel que $c = aq$ et $d = bq$).

L'existence d'une fraction irréductible égale à une fraction donnée (cf. note 22) est un résultat bien connu des élèves de collège (on peut rêver !) : « toute fraction non irréductible est simplifiable ». Mais le théorème d'Euclide apporte de plus l'unicité de la fraction réduite :

- Soit δ le PGCD de c et d, obtenu par l'algorithme d'Euclide initialisé par la division de c par d : on a $c = \delta\alpha$ et $d = \delta\beta$ où $\dfrac{\alpha}{\beta}$ est la fraction réduite égale à $\dfrac{c}{d}$.
- Si $\dfrac{a}{b}$ est une fraction irréductible égale à $\dfrac{c}{d}$, d'après le théorème, c et d sont des équimultiples de a et b : il existe q diviseur commun de c et d tel que $c = aq = \delta\alpha$ et $d = bq = \delta\beta$.
- q est un diviseur de δ : $\delta = q\delta'$, car dans l'algorithme d'Euclide, si q divise c et d, il divise les restes successifs jusqu'au dernier reste non nul δ.
- On a donc $a = \delta'\alpha$ et $b = \delta'\beta$, et comme a et b sont premiers entre eux, $\delta' = 1$, d'où l'unicité : $a = \alpha$ et $b = \beta$.

Pour résumer, le théorème d'Euclide peut être formulé en termes de fractions :

Étant donnée la fraction $\dfrac{c}{d}$, si la fraction $\dfrac{a}{b}$ est une fraction irréductible égale à $\dfrac{c}{d}$, alors $c = a\delta$ et $d = b\delta$, où δ est le PGCD de c et de d.

[25] Il est ainsi appelé dans certains pays étrangers.

c) Sa démonstration par Euclide

La démonstration qui suit est directement adaptée de celle des *Éléments*, dans des formulations condensées et une symbolique contemporaine à l'usage des élèves de Terminale[26].

L'idée est d'introduire le couple (a, b) des « plus petits entiers en même rapport » qu'un couple (c, d) donné (i.e. pour tout couple (x, y) en même rapport que (c, d), on a $a \leqslant x$ et $b \leqslant y$). Euclide en admet implicitement l'existence, mais cela ne va pas complètement de soi. En termes ensemblistes, on peut le voir ainsi :

> Soit E l'ensemble non vide des couples (x, y) d'entiers non nuls en même rapport que (c, d).
> Soit F l'ensemble des premières projections des éléments de E. F est une partie non vide de $\mathbb{N}^*$. Il existe donc dans F un plus petit élément a et par suite un couple (a, b) dans E tel que $ad = bc$.
> Pour tout autre couple (x, y) en même raison que (c, d), on a $ay = bx$ (car $xd = yc$ entraîne $bxd = bcy = ady$).
> Puisque a est le plus petit élément de F, on a $a \leqslant x$ et donc $b \leqslant y$ (sinon $ay < bx$!).

i. Voici d'abord la démonstration de la proposition 20, c'est le clou du spectacle :

- Supposons que a et b soient les nombres les plus petits de ceux qui sont en même rapport avec eux. Soit (c, d) en même rapport que (a, b), on a $ad = bc$ et $a \leqslant c$ et $b \leqslant d$.
- La division euclidienne de c par a et de d par b donne l'existence et l'unicité des couples (q, r) et (q', r') tels que :

$$(1) \begin{cases} c = aq + r \\ d = bq' + r' \end{cases} \text{avec} \begin{cases} q \geqslant 1 \\ q' \geqslant 1 \end{cases} \text{et} \begin{cases} 0 \leqslant r < a \\ 0 \leqslant r' < b \end{cases}$$

  d'où

$$(2) \begin{cases} bc = abq + br \\ ad = abq' + ar' \end{cases} \text{avec} \begin{cases} q \geqslant 1 \\ q' \geqslant 1 \end{cases} \text{et} \begin{cases} 0 \leqslant rb < ab \\ 0 \leqslant r'a < ab \end{cases}$$

- Par unicité de la division euclidienne de $bc = ad$ par ab, on a $q = q'$ et $br = ar'$.
- En reportant cela dans (1), il vient :

$$(1') \begin{cases} c = aq + r \\ d = bq + r' \end{cases} \text{avec } q \geqslant 1, \begin{cases} 0 \leqslant r < a \\ 0 \leqslant r' < b \end{cases} \text{et } ar' = br$$

- Supposons que $r \neq 0$. Comme $ar' = br$, $r' \neq 0$ et (r, r') sont en même rapport que (a, b). De plus $r < a$ et $r' < b$. Mais on avait supposé que a et b sont les plus petits nombres de ceux qui sont dans ce même rapport !

[26] Nous avons dans ce qui suit une mine d'exercices sur le raisonnement mathématique, avec des démonstrations par l'absurde, des contrapositions, des réciproques et des manipulations logiques d'énoncés de la forme P et $Q \Rightarrow R$!

- Donc $r = 0$ et comme $br = ar'$, on a $r' = 0$, d'où $\begin{cases} c = aq \\ d = bq \end{cases}$: a divise c et b divise d avec le même quotient q.

ii. On établit ensuite l'équivalence indiquée par les propositions 21 et 22 :

Les entiers a et b sont premiers entre eux si et seulement si a et b sont les plus petits nombres parmi les couples qui sont en même rapport qu'eux.

(a)

- Soient a et b deux entiers premiers entre eux et supposons qu'ils ne soient pas les plus petits qui sont en même rapport qu'eux.
- Soit (a', b') le couple des entiers les plus petits parmi ceux qui sont en même rapport que (a, b) : $ab' = ba'$ [l'existence de ce couple (a', b') a été montrée ci-dessus].
- D'après la proposition 20, a' divise a et b' divise b dans le même rapport q : $a = qa'$ et $b = qb'$. Si q était plus grand que 1, il serait diviseur commun de a et b qui ne seraient pas premiers entre eux !
- Donc $q = 1$ et a et b sont les plus petits entiers de ceux qui sont en même rapport qu'eux.

(b)

- Réciproquement, supposons que a et b sont les plus petits entiers de ceux qui sont en même rapport qu'eux.
- Supposons que a et b ne soient pas premiers entre eux.
- Soit $\delta > 1$ le PGCD de a et b (obtenu par exemple par l'algorithme d'Euclide). Soient a' et b' les quotients de a et b par δ. a' et b' sont premiers entre eux et comme $a = \delta a'$ et $b = \delta b'$, on a $a' < a$ et $b' < b$.
- Alors $ab' = \delta a'b' = a'b$. (a', b') sont donc en même rapport que (a, b) et plus petits qu'eux. Mais a et b sont les plus petits de ceux qui sont dans ce même rapport !
- a et b sont donc premiers entre eux.

Cette équivalence permet de remplacer l'hypothèse de la proposition 20 par « a et b premiers entre eux », ce qui donne notre théorème d'Euclide.

2.5 Équivalence entre le théorème d'Euclide et le théorème de Gauss

Le théorème de Gauss est une conséquence immédiate du théorème d'Euclide :

- Supposons que a divise bc et que a est premier avec b. Montrons que a divise c.

- Il existe donc d non nul tel que $ad = bc$. a et b sont donc premiers entre eux dans le même rapport que (c, d).

- D'après le théorème d'Euclide, a divise c.

Mais le théorème d'Euclide est aussi une conséquence immédiate du théorème de Gauss :

- Supposons que a et b sont premiers entre eux, en même rapport que (c, d). On a $ad = bc$.
- a divise donc bc et d'après le théorème de Gauss, a divise c : $c = aq$.
- De même, comme a et b sont premiers entre eux et comme b divise ad, alors (Gauss) b divise d : $d = bq'$.
- Comme $ad = bc$, on a : $abq' = baq$, d'où $q = q'$.
- c et d sont donc des équimultiples de a et b.

2.6 Le théorème de Gauss dans les *Éléments*

Le théorème de Gauss était donc à portée de la main. Mais Euclide lui a préféré sa proposition 24 (cf. paragraphe 2.2) que nous énonçons :

Si a est premier avec b et avec c, alors a est premier avec le produit bc.

La démonstration qu'en donne Euclide fait directement intervenir la proposition 20 :

- Supposons que a et bc ne soient pas premiers entre eux. Ils ont alors un diviseur commun $e > 1$.
- Comme e divise a et comme a est premier avec c, e est premier avec c (sinon un diviseur commun de e et c serait diviseur de a !).
- Comme e divise bc, il existe f tel que $bc = ef$. (e, c) et (b, f) sont en même rapport.
- Comme e et c sont premiers entre eux, ils sont les plus petits dans leur rapport (prop. 21) et par conséquent e divise b (prop. 20). Comme e divise a, a et b ne sont pas premiers entre eux !
- a et bc sont donc premiers entre eux.

La proposition 24 est très proche du théorème de Gauss. On le voit mieux sur la forme logiquement équivalente suivante, issue de l'énoncé contraposé :

Si a est premier avec b et si a et bc ont un diviseur commun, alors a et c ont un diviseur commun.

Cet énoncé semble plus général mais moins précis que celui de Gauss (via le théorème d'Euclide, il lui est équivalent).

En faisant $b = c$, Euclide en déduit son cas particulier (proposition 25, cf. paragraphe 2.2) :

si a est premier avec b, alors a est premier avec b^2, et notre lemme *(si p premier divise b^2, alors p divise b)* s'en déduit simplement par contraposition, en remarquant que si $a = p$ est premier, la négation de « p est premier avec b » est « p divise b ». C'est en effet l'objet de sa **proposition 29** :

« *Tout nombre premier est premier avec tout nombre qu'il ne mesure pas* ».

En effet, ces deux nombres ne peuvent pas avoir de diviseur commun, puisqu'un nombre premier n'en a pas d'autre que lui-même.

Euclide utilise enfin la proposition 24 pour obtenir l'énoncé particulier du théorème de Gauss :

Proposition 30 :
« *Si deux nombres se multipliant l'un l'autre produisent un certain [nombre] et si un certain nombre premier mesure leur produit, il mesurera aussi l'un des nombres initiaux* ».

Traduisons : si a est un nombre premier et divise le produit bc, il divise b ou il divise c.

C'est exactement la contraposée de la proposition 24, appliquée au cas où a est premier, moyennant la remarque précédente.

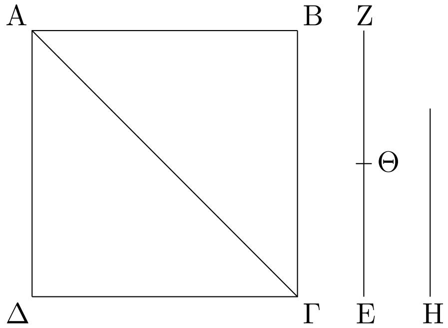
3 Annexe

Voici pour terminer la démonstration de l'incommensurabilité entre la diagonale et le côté d'un carré, inspirée par l'argument d'Aristote, telle qu'elle figure dans l'édition des *Éléments* par la librairie Blanchard (1993), issue de la traduction de François Peyrard (1819).

LE DIXIÈME LIVRE DES ÉLÉMENTS D'EUCLIDE PROPOSITION CXVII.

Qu'il nous soit proposé de démontrer que dans les figures quarrées la diagonale est incommensurable en longueur avec le côté.

Soit le quarré $\mathrm{AB\Gamma\Delta}$, et que $\mathrm{A\Gamma}$ soit sa diagonale ; je dis que la droite $\mathrm{A\Gamma}$ est incommensurable en longueur avec AB.



Qu'elle lui soit commensurable, si cela est possible ; je dis qu'il s'en suivrait qu'un même nombre serait pair et impair.

Or, il est évident que le quarré de $\mathrm{A\Gamma}$ est double du quarré de AB ; mais $\mathrm{A\Gamma}$ est commensurable avec AB ; la droite $\mathrm{A\Gamma}$ a donc avec la droite AB la raison qu'un nombre a avec un nombre. Que $\mathrm{A\Gamma}$ ait avec AB la raison que le nombre EZ a avec le nombre H, et que les nombres EZ, H soient les plus petits de ceux qui ont la même raison avec eux ; le nombre EZ ne sera pas l'unité. Car si EZ était l'unité, à cause que EZ a avec H la raison que $\mathrm{A\Gamma}$ a avec AB, et que $\mathrm{A\Gamma}$ est plus grand que AB, l'unité EZ serait plus grande que le nombre H, ce qui est absurde ; EZ n'est donc pas l'unité ; EZ est donc un nombre.

Et puisque $\mathrm{\Gamma A}$ est à AB comme EZ est à H, le quarré de $\mathrm{\Gamma A}$ sera au quarré de AB comme le quarré de EZ est au quarré de H.

Mais le quarré de $\mathrm{\Gamma A}$ est double du quarré de AB ; le quarré de EZ est donc double du quarré de H ; le quarré du nombre EZ est donc pair. Le nombre EZ est donc pair ; car s'il était impair, son quarré serait impair ; parce que si l'on ajoute tant de nombres impairs que l'on voudra, leur quantité étant impaire, leur somme est un nombre impair ; le nombre EZ est donc un nombre pair.

Partageons le nombre EZ en deux parties égales en Θ. Puisque les nombres EZ, H sont les plus petits de ceux qui ont la même raison avec eux, ces nombres seront premiers entr'eux. Mais le nombre EZ est pair ; le nombre H est donc impair. Car s'il était pair, les nombres EZ, H, qui sont premiers entr'eux, seraient mesurés par deux ; parce que tout nombre pair a une partie qui en est la moitié, ce qui est impossible. Le nombre H n'est donc pas un nombre pair ; il est donc impair.

Mais EZ est double de $\mathrm{E}\Theta$; le quarré de EZ est donc quadruple du quarré de $\mathrm{E}\Theta$. Mais le quarré de EZ est double du quarré de H ; le quarré de H est donc double du quarré de $\mathrm{E}\Theta$; le quarré de H est donc pair ; le nombre H est donc pair, d'après ce qui a été dit.

Mais il est aussi impair, ce qui est impossible ; la droite $\mathrm{A\Gamma}$ n'est donc pas commensurable en longueur avec AB ; elle lui est donc incommensurable.

Ce qu'il fallait démontrer.