Les nombres entiers premiers sont-ils toujours premiers ?

Autor(en): **Moine, Jean-Marie**

Objekttyp: **Article**

Zeitschrift: **Actes de la Société jurassienne d'émulation**

Band (Jahr): **97 (1994)**

PDF erstellt am: **20.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-555325

Les nombres entiers premiers sont-ils toujours premiers?

Par Jean-Marie Moine

INTRODUCTION

Les mathématiques font partie de ce qu'on appelle la culture générale, au même titre que la musique, la peinture, etc. Or vous conviendrez avec moi, que cet aspect culturel est souvent délaissé. Pour quelles raisons?

– Malheureusement, les mathématiques ne sont souvent considérées et appréciées que par nécessité pratique. Si on a besoin d'elles, on les étudie, mais... juste ce qu'il faut!

– Avant d'apprécier les mathématiques, il faut faire un effort, car aucun des cinq sens naturels de l'homme n'est à même de lui faire éprouver une sensation en face d'une page de mathématiques, ou à l'écoute de la lecture de celle-ci. Il en va tout autrement de la musique par exemple: on peut très bien apprécier un concert sans rien connaître de la musique.

– Selon un préjugé bien ancré dans les esprits, les mathématiques sont abstraites, donc...! C'est certainement vrai lorsqu'elles sont exposées d'une certaine façon (je pense à la façon bourbachique; le mot est du mathématicien français Jean Dieudonné). Cependant on rencontre l'abstraction en peinture par exemple, ce qui n'empêche pas bon nombre de visiteurs d'un musée, qui ignorent tout de la peinture, d'apprécier voire d'aimer des tableaux dits abstraits.

Il me semble que trop rares sont les mathématiciens qui font un effort pour essayer de faire comprendre aux non-mathématiciens, donc presque à «Monsieur tout le monde», ce qu'ils font afin d'en faire apprécier la beauté. Et, à l'espèce de mépris (le mot est sans doute un peu trop fort) qu'ont certains mathématiciens pour ceux qui ne comprennent pas, «Monsieur tout le monde» sait répondre par une indifférence totale et non dissimulée!

Les lignes qui suivent s'adressent en priorité à «Monsieur tout le monde», et n'exigent pour leur compréhension qu'un petit effort d'attention, en plus des connaissances mathématiques que chacun a acquises à l'école primaire ou à l'école secondaire.

J'espère que ce n'est pas une utopie d'essayer de vous faire comprendre et apprécier l'une des plus belles découvertes de la théorie des nombres, faite au cours de la seconde moitié du siècle passé.

Les numéros suivis d'une parenthèse renvoient aux notes figurant en fin d'exposé. Les numéros affectés d'un astérisque sont destinés aux lecteurs ayant poursuivi des études en mathématiques après l'école secondaire, aux étudiants en mathématiques, et pourquoi pas, aux mathématiciens eux-mêmes.

PLAN DE L'EXPOSÉ

I) Rappel d'une «chaîne» d'ensembles intuitivement connus.

$\boldsymbol{N}$	——	$\boldsymbol{Z}$	——	$\boldsymbol{Q}$	——	$\boldsymbol{R}$
décomposition unique		décomposition presque unique		décomposition presque unique		décomposition «anarchique»

II) Introduction d'idéaux de $\boldsymbol{Z}$ pour assurer la décomposition unique.

Ensemble des idéaux de $\boldsymbol{Z}$

décomposition unique

III) $\boldsymbol{R}$ étant trop grand, on considère une autre «chaîne» d'ensembles.

$$\boldsymbol{N} \text{ —— } \boldsymbol{Z} \text{ —— } \boldsymbol{Z}[\sqrt{3}]$$

IV) Introduction d'idéaux de $\boldsymbol{Z}$ $[\sqrt{3}]$ pour assurer la décomposition unique.

Ensemble des idéaux de $\boldsymbol{Z}$	Ensemble des idéaux de $\boldsymbol{Z}[\sqrt{3}]$
décomposition unique	décomposition unique

L'avis que vous avez reçu vous indique que je n'ai pas l'intention de vous exposer une théorie. Néanmoins, tout exposé de mathématique, pour qu'il soit jugé sérieux, doit comporter au moins une démonstration. J'ose donc, pour que cet exposé paraisse sérieux, vous démontrer une formule d'algèbre, la seule d'ailleurs dont nous aurons besoin aujourd'hui. C'est une formule que vous savez tous démontrer, mais laissez-

moi le plaisir d'en faire la démonstration. Ainsi les... (pardonnez-moi), les esprits chagrins seront satisfaits.

$$a^2 - b^2 = [a + b] \,.\, [a - b]$$ [1)]

L'homme a toujours été fasciné par les nombres, par les nombres premiers en particulier. Mais il se bute sans cesse à des difficultés qu'il ne sait pas surmonter et qui restent plantées dans sa chair comme des échardes destinées à lui rappeler la modestie.

Un illustre mathématicien (je crois que c'est Dedekind, mais je n'en suis pas certain) a dit un jour: «Dieu a créé les nombres entiers, l'homme a fait le reste !»

J'ouvre une parenthèse pour vous soumettre une question: L'homme a-t-il alors bien décidé de ce qu'est un nombre premier? Permettez-moi de ne pas pouvoir répondre. Mais, la découverte d'une formule qui fournirait explicitement la valeur du n-ième nombre premier n'a toujours pas été trouvée, et ce problème restera peut-être à jamais sans solution!

Avec le même respect que celui qu'avait notre illustre mathématicien, acceptons l'œuvre de Dieu, acceptons donc les nombres entiers.

EXPOSÉ PROPREMENT-DIT

I) «CHAÎNE» D'ENSEMBLES INTUITIVEMENT CONNUS.

a) **Ensemble des nombres entiers naturels.**

$\boldsymbol{N} = \{0, 1, 2, \ldots\ldots, n, \ldots\ldots\}$ [2)]

Dans l'ensemble $\boldsymbol{N}$, l'homme a défini une addition, un produit, puis une soustraction et une division (ces deux dernières opérations ne sont pas toujours possibles dans $\boldsymbol{N}$).

L'élément zéro étant égoïste pour la multiplication, impossible pour la division, on a décidé de l'exclure et de considérer l'ensemble [3)]

$\boldsymbol{N}^* = \{1, 2, 3, \ldots\ldots, n, \ldots\ldots\}$ [4*)]

[Chaque fois que l'élément zéro sera gênant, on l'éliminera. Cette élimination sera indiquée par un astérisque.]

L'homme a ensuite défini:

Nombre entier naturel non nul, supérieur à 1, premier: c'est un entier naturel divisible seulement par 1 et par lui-même.

2 est premier
3 est premier
4 n'est pas premier, puisqu'il est divisible par 1, par 4, mais aussi par 2.

Résultat important: Tout nombre entier naturel non nul et différent de 1 s'écrit de **façon unique à l'ordre des facteurs près**, sous la forme d'un produit de nombres entiers naturels premiers supérieurs à 1.

Exemples:
$14 = 2.7 = 7.2$
$45 = 3.3.5 = 3.5.3 = 5.3.3$

b) Ensemble des nombres entiers relatifs.

Dans $\boldsymbol{N}$, la soustraction n'est pas toujours possible. D'où la nécessité de définir un nouvel ensemble.

On appelle **entier relatif**, un nombre qui est ou bien égal à un entier naturel, ou bien égal à un nombre entier naturel précédé du signe moins. L'ensemble des nombres entiers relatifs est:

$\boldsymbol{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\ldots, n, -n, \ldots\ldots\}$ [5*)]

Lorsque le nombre entier relatif zéro gênera, on considérera l'ensemble

$\boldsymbol{Z^*} = \{1, -1, 2, -2, 3, -3, \ldots\ldots, n, -n, \ldots\ldots\}$

Résultat important: Un nombre entier relatif non nul et différent de 1 ou de –1 s'écrit de **façon unique à l'ordre des facteurs près**,

soit sous la forme d'un produit de nombres entiers naturels premiers,

soit sous la forme d'un produit de nombres entiers naturels premiers et de –1.

Exemples:
$75 = 3.5.5 = 5.5.3 = 5.3.5$
$-77 = [-1].7.11 = [-1].11.7 = 7.[-1].11 = 11.[-1].7 = 7.11.[-1] = 11.7.[-1]$

Remarque: On constate que le dernier résultat important est moins «élégant» que le résultat «analogue» concernant la décomposition d'un entier naturel, ceci, à cause du .... soit..... soit..... Nous reviendrons sur ce problème un peu plus tard. Pour l'instant, suivons le développement historique de l'apport de l'homme à la théorie des nombres.

c) Ensemble des nombres rationnels.

Dans $\boldsymbol{N}$, dans $\boldsymbol{Z}$ aussi, la division n'est pas toujours possible. Il faut donc définir un nouvel ensemble.

On appelle **nombre rationnel** (fraction), le résultat du quotient (division) d'un nombre entier relatif par un autre nombre entier relatif **non nul** (on ne divise jamais par zéro).

L'ensemble des nombres rationnels est l'ensemble:

$\boldsymbol{Q} = \{p/q \mid p \text{ élément de } \boldsymbol{Z}, q \text{ élément de } \boldsymbol{Z^*}\}$ [6*)]

Lorsque le nombre rationnel zéro gênera, on considérera l'ensemble

$\boldsymbol{Q^*} = \{p/q \mid p \text{ élément de } \boldsymbol{Z^*}, q \text{ élément de } \boldsymbol{Z^*}\}$

Résultat important: Un nombre rationnel non nul, simplifié au maximum, s'écrit de **façon unique à l'ordre des facteurs près**, sous la forme d'un quotient du produit d'un nombre fini d'entiers naturels premiers (produit éventuellement par –1) par le produit d'un nombre fini d'entiers naturels premiers.

Exemples:

$$\frac{10}{21} = \frac{2.5}{7.3} = \frac{5.2}{7.3} = \frac{2.5}{3.7} = \frac{5.2}{3.7}$$

$$\frac{-5}{6} = \frac{[-1].5}{2.3} = \frac{[-1].5}{3.2} = \frac{5.[-1]}{2.3} = \frac{5.[-1]}{3.2}$$

Remarque: Ici aussi (à cause du produit éventuel par –1), le résultat important n'est pas très «élégant». Cela n'aura pas d'importance pour la suite de l'exposé.

d) **Ensemble des nombres réels.**

Cependant, les nombres rationnels ne suffisent pas. L'homme a eu besoin de considérer de nouveaux nombres tels $\sqrt{2}$, $\sqrt{3}$ ....., π (pi),..., etc. qu'il a appelés nombres réels. [7)]

π = 3,141592653590..... (on ne peut pas l'écrire «jusqu'au bout», il n'y a pas de fin!)

L'ensemble des nombres réels est désigné par $\boldsymbol{R}$. [8*)]

Mais alors, que deviennent nos «résultats importants» dans $\boldsymbol{R}$?

Examinons un exemple:

$481 = 13.37$

$481 = [41 + 20\sqrt{3}] . [41 - 20\sqrt{3}]$

$481 = [26 + 13\sqrt{3}] . [74 - 37\sqrt{3}]$

$481 = [24 + \sqrt{95}] . [24 - \sqrt{95}]$

$481 = [27 + 2\sqrt{62}] . [27 - 2\sqrt{62}]$

Aïe, aïe, aïe ! On trouverait encore d'autres décompositions différentes de 481, même, une infinité !

Dans $\boldsymbol{R}$, la décomposition semble anarchique. **Elle n'est pas unique.** [9)]

II) AMÉLIORATION DU RÉSULTAT IMPORTANT CONCERNANT LA DÉCOMPOSITION D'UN NOMBRE ENTIER RELATIF.

Idéal de $\boldsymbol{Z}$.

Pour chaque entier naturel n, on peut considérer l'ensemble de tous les nombres entiers relatifs égaux au produit de n par un entier relatif.

Cet ensemble constitue un **idéal de $\boldsymbol{Z}$**, noté (n).

(n) = {0, n, –n, 2n, –2n, 3n, –3n, ...}

Exemples.

L'idéal (2) de $\boldsymbol{Z}$ est l'ensemble constitué des nombres entiers relatifs

0, 2, –2, 4, –4, 6, –6, ...

On écrit: (2) = {0, 2, –2, 4, –4, 6, –6, ...}

L'idéal (3) de $\boldsymbol{Z}$ est l'ensemble constitué des nombres entiers relatifs

0, 3, –3, 6, –6, 9, –9, ...

On écrit: (3) = {0, 3, –3, 6, –6, 9, –9, ...}

L'idéal (6) de $\boldsymbol{Z}$ est l'ensemble constitué des nombres entiers relatifs

0, 6, –6, 12, –12, 18, –18, ...

On écrit: (6) = {0, 6, –6, 12, –12, 18, –18, ...}

Produit de deux idéaux.

Le produit de l'idéal (p) par l'idéal (q) est l'idéal (pq), constitué par l'ensemble des nombres entiers relatifs égaux aux produits d'un nombre de (p) par un nombre de (q).

Exemple.

Le produit de l'idéal (2) par l'idéal (3) est égal à l'idéal (6).
On écrit : (2) . (3) = (6)

En effet,
0, élément de (6) est égal au produit de l'élément 0 de (2) par l'élément 0 de (3);
6, élément de (6) est égal au produit de l'élément 2 de (2) par l'élément 3 de (3);
–6, élément de (6) est égal au produit de l'élément 2 de (2) par l'élément – 3 de (3);
etc.

Idéal premier.

Un idéal (n) de $\boldsymbol{Z}$ est dit premier si n est un nombre entier naturel non nul, supérieur à 1, premier.

Exemples.

(2) est un idéal premier de $\boldsymbol{Z}$.[10)]
(3) est un idéal premier de $\boldsymbol{Z}$.
(6) est un idéal de $\boldsymbol{Z}$, mais il n'est pas premier.
(5) est un idéal premier de $\boldsymbol{Z}$.
(10) est un idéal de $\boldsymbol{Z}$, mais il n'est pas premier.

Résultat important: Tout idéal de $\boldsymbol{Z}$ s'écrit **de façon unique**, à l'ordre des facteurs près, sous la forme d'un produit d'idéaux premiers de $\boldsymbol{Z}$.

Exemples.

(6) = (2) . (3), ou dans un ordre différent (6) = (3) . (2) .[11)]
(30) = (2) . (3) . (5), ou dans des ordres différents (30) = (2) . (5) . (3)
(30) = (3) . (2) . (5)
(30) = (3) . (5) . (2)
(30) = (5) . (2) . (3)
(30) = (5) . (3) . (2)

III) L'IDÉE GÉNIALE DE DEDEKIND ET DE KUMMER.

Dedekind Richard, mathématicien allemand (Brunswick 1831- id. 1916).
Kummer Ernst Eduard, mathématicien allemand (Sorau 1810- Berlin 1893).

J'ai associé ces deux illustres mathématiciens et leur ai attribué la paternité de cette idée géniale, sans vraiment chercher ce qui revenait à l'un et ce qui revenait à l'autre. J'aurais d'ailleurs pu citer les noms d'autres mathématiciens célèbres qui ont apporté, au milieu du siècle dernier, une contribution importante à la théorie des nombres.

L'idée fondamentale.

> Si la décomposition en facteurs premiers n'est pas unique, on doit pouvoir représenter les nombres comme objets d'un nouvel ensemble muni d'une multiplication et dans lequel la décomposition en facteurs premiers est cette fois définie de manière unique.

(Voir par exemple: Théorie des nombres par Z. I. Borevitch et I. R. Chafarevitch, page 186. Les auteurs attribuent cette idée à Kummer.)

Comment concrétiser techniquement cette idée?

Intéressons-nous aux décompositions du seul nombre 481.

Nous avons vu que dans $\boldsymbol{R}$, on pouvait obtenir une infinité de décompositions de 481. Les décompositions que nous avons indiquées font intervenir $\sqrt{3}$, $\sqrt{95}$ ou $\sqrt{62}$.

L'ensemble $\boldsymbol{R}$ est donc trop grand !

Limitons-nous aux décompositions qui ne font intervenir que $\sqrt{3}$. [12*)]

Avec Kummer et Dedekind, fabriquons un sous-ensemble de $\boldsymbol{R}$, constitué de tous les nombres réels qu'on peut écrire sous la forme $a + b\sqrt{3}$, où a et b sont des nombres entiers relatifs.

Cet ensemble est noté $\boldsymbol{Z}[\sqrt{3}]$. [13*)]

$\boldsymbol{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a$ élément de $\boldsymbol{Z}$, b élément de $\boldsymbol{Z}\}$ [14)]

Les éléments de $\boldsymbol{Z}[\sqrt{3}]$ sont appelés des entiers algébriques.

$\boldsymbol{Z}[\sqrt{3}]$ est un ensemble d'**entiers algébriques**.

Les entiers algébriques premiers de $\boldsymbol{Z}[\sqrt{3}]$ •

Parmi les entiers algébriques de $\boldsymbol{Z}[\sqrt{3}]$, certains sont premiers (les mathématiciens disent **irréductibles**), d'autres ne le sont pas. Permettez-moi de ne pas préciser ce qu'est un élément irréductible de $\boldsymbol{Z}[\sqrt{3}]$. La

définitition de tels éléments repose sur des notions mathématiques que je ne peux exposer ici. [15*)]

IV) IDÉAL DE $\boldsymbol{Z}[\sqrt{3}]$.

Dans le cas qui nous intéresse (mais ce n'est pas toujours aussi simple qu'ici) [16*)] nous pouvons construire les idéaux de $\boldsymbol{Z}[\sqrt{3}]$ en procédant comme nous l'avons fait pour construire les idéaux de $\boldsymbol{Z}$.

Pour chaque entier algébrique de $\boldsymbol{Z}[\sqrt{3}]$, c'est-à-dire pour chaque élément $\alpha = a + b\sqrt{3}$, où a et b sont des nombres entiers relatifs, on peut considérer l'ensemble de tous les entiers algébriques égaux au produit de α par un entier algébrique de $\boldsymbol{Z}[\sqrt{3}]$. Cet ensemble constitue un **idéal de $\boldsymbol{Z}[\sqrt{3}]$**, noté (α).

Exemples.

2 est un entier algébrique de $\boldsymbol{Z}[\sqrt{3}]$.
L'idéal (2) de $\boldsymbol{Z}[\sqrt{3}]$ contient donc tous les nombres
0, 2, –2, 4, –4, 6, –6, ...
Mais attention, cet idéal contient beaucoup d'autres nombres, par exemple:
$2 . \sqrt{3}$
$2 . [5 + \sqrt{3}]$, c'est-à-dire $10 + 2\sqrt{3}$,
$2 . [-3 + 7\sqrt{3}]$, c'est-à-dire $-6 + 14\sqrt{3}$,
etc. [17)]

3 est un entier algébrique de $\boldsymbol{Z}[\sqrt{3}]$.
L'idéal (3) de $\boldsymbol{Z}[\sqrt{3}]$ contient beaucoup de nombres, par exemple:
$3 . [2\sqrt{3}]$, c'est-à-dire $6\sqrt{3}$,
$3 . [1-\sqrt{3}]$, c'est-à-dire $3 - 3\sqrt{3}$,
$3 . [-7 +\sqrt{3}]$, c'est-à-dire $-21 + 3\sqrt{3}$,
etc.

$4 + \sqrt{3}$ est un entier algébrique de $\boldsymbol{Z}[\sqrt{3}]$.
L'idéal $(4 + \sqrt{3})$ de $\boldsymbol{Z}[\sqrt{3}]$ contient donc tous les nombres
$0, 4 +\sqrt{3}, [-1] . [4 + \sqrt{3}], 2 . [4 + \sqrt{3}], [-2] . [4 + \sqrt{3}]$, ...
Mais attention, cet idéal contient beaucoup d'autres nombres, par exemple:
$\sqrt{3} . [4 + \sqrt{3}]$, c'est-à-dire $3 + 4\sqrt{3}$,
$[8 + 3\sqrt{3}] . [4 + \sqrt{3}]$, c'est-à-dire $41 + 20\sqrt{3}$,
$[1 + \sqrt{3}] . [4 + \sqrt{3}]$, c'est-à-dire $7 + 5\sqrt{3}$,
etc.

Produit de deux idéaux de $Z[\sqrt{3}]$.

Nous pouvons aussi définir le produit de deux idéaux comme nous l'avons fait pour le produit de deux idéaux de Z.

Donc, le produit de l'idéal (α) de $Z[\sqrt{3}]$ par l'idéal (β) de $Z[\sqrt{3}]$ est l'idéal $(\alpha . \beta)$ de $Z[\sqrt{3}]$, constitué par l'ensemble des entiers algébriques de $Z[\sqrt{3}]$ égaux aux produits d'un élément de (α) par un élément de (β).

Ainsi, $(\alpha . \beta) = (\alpha) . (\beta)$. [18)]

Idéal premier de $Z[\sqrt{3}]$. [19*)]

Je ne définirai pas cette notion puisque je ne vous ai pas dit ce qu'était un entier algébrique premier de $Z[\sqrt{3}]$.

Croyez-moi s'il vous plaît, si je vous dis que les idéaux suivants de $Z[\sqrt{3}]$ sont premiers:

$\mathcal{P}_1 = (4 + \sqrt{3})$, $\mathcal{P}_2 = (4 - \sqrt{3})$, $\mathcal{P}_3 = (8 + 3\sqrt{3})$, $\mathcal{P}_4 = (8 - 3\sqrt{3})$.

Observez qu'on a désigné l'idéal $(4 + \sqrt{3})$ par $\mathcal{P}_1$, l'idéal $(4 - \sqrt{3})$ par $\mathcal{P}_2$, etc.

Résultat important: Dans $Z[\sqrt{3}]$, tout idéal se décompose **de façon unique** à l'ordre des facteurs près, sous la forme d'un produit d'idéaux premiers. (C'est le résultat fondamental de Dedekind et de Kummer).

Illustrons ce résultat important en reprenant les décompositions du nombre 481 faisant intervenir $\sqrt{3}$, indiquées à la page 74.

Attention: Pour éviter toute confusion, les crochets [ ] sont réservés à l'écriture des nombres alors que les idéaux sont toujours écrits entre parenthèses ( ).

Première décomposition. (voir page 74)

En langage de nombres:

$481 = 13.37$

Mais, $13 = [4 + \sqrt{3}] . [4 - \sqrt{3}]$ et $37 = [8 + 3\sqrt{3}] . [8 - 3\sqrt{3}]$

Donc $481 = \underbrace{[4+\sqrt{3}]}_{\text{nombre}} . \underbrace{[4-\sqrt{3}]}_{\text{nombre}} . \underbrace{[8+3\sqrt{3}]}_{\text{nombre}} . \underbrace{[8-3\sqrt{3}]}_{\text{nombre}}$

En langage d'idéaux:

Le nombre 481 appartient à l'idéal (481) qui n'est pas premier;
le nombre $4 + \sqrt{3}$ appartient à l'idéal premier $(4 + \sqrt{3})$ qu'on écrit aussi $\mathcal{P}_1$;
le nombre $4 - \sqrt{3}$ appartient à l'idéal premier $(4 - \sqrt{3})$ qu'on écrit aussi $\mathcal{P}_2$;
le nombre $8 + 3\sqrt{3}$ appartient à l'idéal premier $(8 + 3\sqrt{3})$ qu'on écrit aussi $\mathcal{P}_3$;
le nombre $8 - 3\sqrt{3}$ appartient à l'idéal premier $(8 - 3\sqrt{3})$ qu'on écrit aussi $\mathcal{P}_4$.

L'idéal (481) peut donc être décomposé en produit d'idéaux:

$$(481) = \underbrace{(4+\sqrt{3})}_{\substack{\text{idéal}\\\text{premier}}} . \underbrace{(4-\sqrt{3})}_{\substack{\text{idéal}\\\text{premier}}} . \underbrace{(8+3\sqrt{3})}_{\substack{\text{idéal}\\\text{premier}}} . \underbrace{(8-3\sqrt{3})}_{\substack{\text{idéal}\\\text{premier}}} = \mathcal{P}_1 . \mathcal{P}_2 . \mathcal{P}_3 . \mathcal{P}_4$$

Deuxième décomposition. (voir page 74)

En langage de nombres:

$481 = [41 + 20\sqrt{3}] . [41 - 20\sqrt{3}]$
Mais, $41 + 20\sqrt{3} = [4 + \sqrt{3}] . [8 + 3\sqrt{3}]$ et $41 - 20\sqrt{3} = [4 - \sqrt{3}] . [8 - 3\sqrt{3}]$

Donc $481 = \underbrace{[4+\sqrt{3}]}_{\text{nombre}} . \underbrace{[8+3\sqrt{3}]}_{\text{nombre}} . \underbrace{[4-\sqrt{3}]}_{\text{nombre}} . \underbrace{[8-3\sqrt{3}]}_{\text{nombre}}$

En langage d'idéaux:

Le nombre 481 appartient à l'idéal (481) qui n'est pas premier;
le nombre $4 + \sqrt{3}$ appartient à l'idéal premier $(4 + \sqrt{3})$ qu'on écrit aussi $\mathcal{P}_1$;
le nombre $8 + 3\sqrt{3}$ appartient à l'idéal premier $(8 + 3\sqrt{3})$ qu'on écrit aussi $\mathcal{P}_3$;
le nombre $4 - \sqrt{3}$ appartient à l'idéal premier $(4 - \sqrt{3})$ qu'on écrit aussi $\mathcal{P}_2$;
le nombre $8 - 3\sqrt{3}$ appartient à l'idéal premier $(8 - 3\sqrt{3})$ qu'on écrit aussi $\mathcal{P}_4$.

L'idéal (481) peut donc être décomposé en produit d'idéaux:

$$(481) = \underbrace{(4+\sqrt{3})}_{\text{idéal premier}} . \underbrace{(8+3\sqrt{3})}_{\text{idéal premier}} . \underbrace{(4-\sqrt{3})}_{\text{idéal premier}} . \underbrace{(8-3\sqrt{3})}_{\text{idéal premier}} = \mathcal{P}_1 . \mathcal{P}_3 . \mathcal{P}_2 . \mathcal{P}_4$$

Troisième décomposition. (voir page 74)

En langage de nombres:

$481 = [26 + 13\sqrt{3}] . [74 - 37\sqrt{3}]$

Mais, $26 + 13\sqrt{3} = 13 . [2 + \sqrt{3}] = \underbrace{[4 + \sqrt{3}] . [4 - \sqrt{3}]}_{\text{nombre 13}} . [2 + \sqrt{3}]$

et $74 - 37\sqrt{3} = 37 . [2 - \sqrt{3}] = \underbrace{[8 + 3\sqrt{3}] . [8 - 3\sqrt{3}]}_{\text{nombre 37}} . [2 - \sqrt{3}]$

Donc $481 = \underbrace{[4+\sqrt{3}]}_{\text{nombre}} . \underbrace{[4-\sqrt{3}]}_{\text{nombre}} . \underbrace{[2+\sqrt{3}]}_{\text{nombre}} . \underbrace{[8+3\sqrt{3}]}_{\text{nombre}} . \underbrace{[8-3\sqrt{3}]}_{\text{nombre}} . \underbrace{[2-\sqrt{3}]}_{\text{nombre}}$

$\underbrace{\qquad\qquad}_{\text{nombre}} \qquad\qquad \underbrace{\qquad\qquad}_{\text{nombre}}$

En langage d'idéaux:

Le nombre 481 appartient à l'idéal (481) qui n'est pas premier;
le nombre $4 + \sqrt{3}$ appartient à l'idéal premier $(4 + \sqrt{3})$ qu'on écrit aussi $\mathcal{P}_1$;
le nombre $[4 - \sqrt{3}] . [2 + \sqrt{3}]$ appartient à l'idéal premier $(4 - \sqrt{3})$ désigné aussi par $\mathcal{P}_2$;
le nombre $8 + 3\sqrt{3}$ appartient à l'idéal premier $(8 + 3\sqrt{3})$ qu'on écrit aussi $\mathcal{P}_3$;
le nombre $[8 - 3\sqrt{3}] . [2 - \sqrt{3}]$ appartient à l'idéal premier $(8 - 3\sqrt{3})$ désigné par $\mathcal{P}_4$.

L'idéal (481) peut donc être décomposé en produit d'idéaux:

$$(481) = \underbrace{(4+\sqrt{3})}_{\text{idéal premier}} . \underbrace{(4-\sqrt{3})}_{\text{idéal premier}} . \underbrace{(8+3\sqrt{3})}_{\text{idéal premier}} . \underbrace{(8-3\sqrt{3})}_{\text{idéal premier}} = \mathcal{P}_1 . \mathcal{P}_2 . \mathcal{P}_3 . \mathcal{P}_4$$

Conclusion: L'idéal (481) a toujours pu être décomposé de **façon unique** à l'ordre des facteurs près, sous la forme du produit des idéaux

premiers $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, $\mathcal{P}_4$. C'est le beau résultat de Dedekind et de Kummer.

Notes: Les notes indiquées par un nombre suivi d'un astérisque sont surtout destinées aux lecteurs ayant poursuivi des études de mathématiques après l'école secondaire, aux étudiants en mathématiques, et, pourquoi pas, aux mathématiciens eux-mêmes.

[1)] Démonstration: $[a + b] . [a - b] = a.a + a.[-b] + b.a + b.[-b]$
$= a.a - [a.b] + a.b - [b.b] = a.a - b.b = a^2 - b^2$

[2)] On note un ensemble de nombres en écrivant les nombres de cet ensemble entre des accolades.

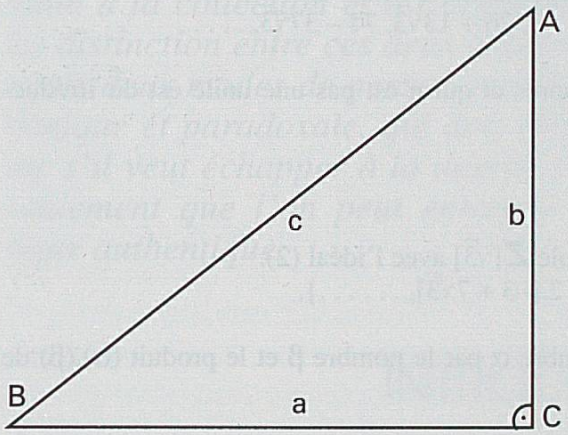
[3)] Dire que zéro est «égoïste» signifie qu'il «ramène tout à lui».
Exemples: Zéro fois trois égale zéro.
Zéro fois cinq égale zéro.
Dire que zéro est impossible pour la division signifie qu'on ne peut pas diviser par zéro.

[4*)] $\boldsymbol{N^*}$ est un demi-groupe (ou un semi-groupe, ou un monoïde) pour la multiplication.

[5*)] $\boldsymbol{Z}$ est le symétrisé de $\boldsymbol{N}$. $\boldsymbol{Z}$ est un anneau factoriel. 1 et –1 sont les unités de $\boldsymbol{Z}$.

[6*)] $\boldsymbol{Q}$ est le corps des fractions de l'anneau $\boldsymbol{Z}$ des entiers relatifs.

[7)]



Considérons par exemple le triangle rectangle en C. Soit a = 5 cm, la longueur du côté BC.
Soit b = 4cm, la longueur du côté AC.
La longueur du côté AB est donnée par le théorème de Pythagore qui dit que $c^2 = a^2 + b^2$.

Donc $c = \sqrt{a^2 + b^2}$
$= \sqrt{5.5 + 4.4} = \sqrt{25 + 16} = \sqrt{41}$.

$\sqrt{41}$ vaut à peu près 6,403.
$\sqrt{41}$ n'est pas un nombre entier.
$\sqrt{41}$ ne peut pas être écrit sous la forme du quotient de deux nombres entiers. Les mathématiciens disent que $\sqrt{41}$ est un nombre réel.

[8*)] On peut définir $\boldsymbol{R}$ par le procédé des coupures, par exemple. (Dedekind)

[9)] Le nombre réel 481 peut s'écrire de nombreuses façons sous la forme du produit de deux nombres réels. Si on reprend les trois premières décompositions du nombre 481 (indiquées au haut de la page 74), on voit que:
481 est égal au produit du nombre réel 13 par le nombre réel 37.
481 est égal au produit du nombre réel $41 + 20\sqrt{3}$ par le nombre réel $41 - 20\sqrt{3}$.
481 est égal au produit du nombre réel $26 + 13\sqrt{3}$ par le nombre réel $74 - 37\sqrt{3}$.

[10)] **Attention.** Ne pas confondre le nombre entier 2 avec l'idéal (2) de $\boldsymbol{Z}$.
2 représente le nombre entier «deux» que chacun connaît.
(2) représente l'idéal «deux». (2) est l'ensemble de tous les nombres entiers relatifs, multiples du nombre entier 2.

[11] **Attention.** Ne pas confondre 2.3, produit du nombre entier 2 par le nombre entier 3, avec le produit (2) . (3).
(2) . (3) est le produit de l'idéal (2), par l'idéal (3).
Rappelons qu'un idéal est un ensemble de nombres!

[12*] Ici, on se place dans l'extension quadratique $\mathbb{Q}[\sqrt{3}]$, obtenue par l'adjonction à $\mathbb{Q}$ de l'élément $\sqrt{3}$.
Cette extension est $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$

[13*] $\mathbb{Z}[\sqrt{3}]$ est l'ensemble de tous les entiers algébriques du corps $\mathbb{Q}[\sqrt{3}]$. On appelle entier algébrique sur $\mathbb{Z}$, tout nombre complexe (il peut être réel) qui est racine d'une équation du type

$$x^n + a_{n-1}x^{n-1} + \ldots\ldots\ldots + a_1 x + a_0 = 0$$

tous les a_i , $0 \leq i \leq n-1$ étant des éléments de $\mathbb{Z}$.

Soit $d \in \mathbb{Z}^*$, $d \neq 1$.
L'ensemble des entiers algébriques du corps $\mathbb{Q}[\sqrt{d}]$ est constitué de tous les entiers algébriques sur $\mathbb{Z}$, contenus dans $\mathbb{Q}[\sqrt{d}]$.
C'est un anneau qui est un $\mathbb{Z}$–module de base:
$1, \sqrt{d}$, si $d \equiv 2$ ou $d \equiv 3 \pmod 4$

$1, \dfrac{1+\sqrt{d}}{2}$, si $d \equiv 1 \pmod 4$.

[14] L'ensemble $\mathbb{Z}[\sqrt{3}]$ contient beaucoup de nombres réels, par exemple
0, 1, –1, 2, –2, 3, –3, ... (tous les entiers relatifs), mais aussi
$1 + \sqrt{3}, 5 - \sqrt{3}, \ldots\ldots, 41 + 20\sqrt{3}, 41 - 20\sqrt{3}, \ldots, 26 + 13\sqrt{3}, 74 - 37\sqrt{3}, \ldots\ldots$

[15*] Un élément n'ayant pas de diviseurs propres et qui n'est pas une unité est dit irréductible.

[16*] $\mathbb{Z}[\sqrt{3}]$ est un anneau principal.

[17] Ne pas confondre le nombre 2 de l'ensemble $\mathbb{Z}[\sqrt{3}]$ avec l'idéal (2).
$(2) = \{0, 2, -2, \ldots\ldots, 2.3, 2.[5 + \sqrt{3}], \ldots\ldots, 2.[-3 + 7\sqrt{3}], \ldots\ldots\}$.

[18] Ne pas confondre le produit α . β du nombre α par le nombre β et le produit $(\alpha).(\beta)$ de l'idéal (α) par l'idéal (β).

[19*] Un idéal $\mathcal{P}$ de l'anneau A tel que l'anneau-quotient $A/\mathcal{P}$ soit un domaine d'intégrité est par définition un idéal premier.

Jean-Marie Moine (La Chaux-de-Fonds), docteur en mathématiques, est professeur à l'Ecole d'ingénieurs du canton de Neuchâtel au Locle.