

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 13 (1967)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUR L'ORGANISATION D'UN COURS D'ARITHMÉTIQUE
Autor: Samuel, Pierre
Kapitel: III. L'ordre (b), (c), (a)
DOI: <https://doi.org/10.5169/seals-41545>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 08.07.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

THÉOREME. Soient a, b deux entiers ≥ 1 . Les assertions suivantes sont équivalentes :

- a) a et b sont premiers entre eux;
- b) la classe $\bar{b}$ de b est inversible dans $\mathbb{Z}/a\mathbb{Z}$;
- c) il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Esquisse de démonstration. On raisonne « en cercle » : $a) \Rightarrow b) \Rightarrow c) \Rightarrow a)$. Supposons $a)$; la relation $\bar{b}\bar{x} = 0$ dans $\mathbb{Z}/a\mathbb{Z}$ veut dire $a|bx$, d'où $a|x$ par Euclide, et $\bar{x} = 0$; on en déduit, par différence, que, dans $\mathbb{Z}/a\mathbb{Z}$, la multiplication par $\bar{b}$ est injective ; elle est donc bijective (cf. I), d'où l'inversibilité de $\bar{b}$. Si $b)$ est vraie, il existe $v \in \mathbb{Z}$ tel que $bv \equiv 1 \pmod{a}$, et ceci équivaut à $c)$. Enfin $c) \Rightarrow a)$ est immédiat.

III. L'ORDRE (b), (c), (a)

1) On commence par l'existence de la décomposition en facteurs premiers comme dans le 2) du § II. Pour l'unicité, on peut utiliser l'ingénieuse démonstration suivante, due à E. Zermelo :

On montre, par récurrence sur n , que la décomposition de n en facteurs premiers est unique. Facile (mais inutile) départ pour $n = 1$ ou 2 . On suppose l'unicité vraie pour tout entier naturel $n' < n$. Considérons deux décompositions de n en facteurs premiers

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t.$$

et supposons les distinctes. Alors chacun des p_i est distinct de chacun des q_j : sinon l'on diviserait par ce facteur premier commun p_k et on obtiendrait deux décompositions distinctes du nombre n/p_k , contrairement à l'hypothèse de récurrence. On a donc, par exemple, $p_1 < q_1$; écrivons $n = p_1 p' = q_1 q'$ avec $p' = p_2 \dots p_s$ et $q' = q_2 \dots q_t$; alors $q' < p'$. Considérons le nombre $n' = (q_1 - p_1) q' = p_1 (p' - q')$. On a $n' < n$, de sorte que la décomposition en facteurs premiers de n' est unique. Or, comme $n' = p_1 (p' - q')$, p_1 figure dans cette décomposition ; écrivons alors $n' = (q_1 - p_1) q'$; comme p_1 est distinct de tous les facteurs premiers q_j de la décomposition $q' = q_2 \dots q_t$, et que celle-ci est unique par l'hypothèse de récurrence, p_1 doit figurer dans la décomposition (unique encore) de $q_1 - p_1$. Mais alors p_1 divise $q_1 - p_1$, donc aussi q_1 . Contradiction. C.Q.F.D.

2) L'étude purement multiplicative des diviseurs et multiples peut alors procéder comme dans le 3) du § II. Pour l'identité de Bezout, il semble préférable d'avoir la théorie des congruences.

3) Jusqu'au théorème disant que Z/pZ est un corps lorsque p est premier (exclus), on procède comme dans le 1) du § II. Mais il n'est pas avantageux de démontrer directement ce théorème; en effet on en sait suffisamment pour démontrer un théorème plus fort, à savoir le dernier théorème du § II relatif à l'identité de Bezout. Alors l'énoncé relatif à Z/pZ (p premier) vient en corollaire; en effet un élément non nul de Z/pZ est la classe d'un entier premier à p , et est donc inversible dans Z/pZ d'après l'assertion $b)$ du théorème.

IV. L'ORDRE CLASSIQUE (c), (b), (a)

1) L'exemple de l'ensemble nZ des multiples de n introduit la notion d'*idéal* de Z (et, plus généralement, d'un anneau commutatif quelconque). La division euclidienne permet alors de montrer le:

THÉORÈME. *Tout idéal I de Z est « principal », c'est-à-dire de la forme nZ .*

C'est clair si I est réduit à 0. Sinon I contient des éléments > 0 , donc un plus petit élément > 0 , soit n . Par division euclidienne de $x \in I$ par n , soit $x = nq + r$ avec $0 \leq r \leq n - 1$, on voit que $r \in I$, donc $r = 0$; ainsi $x \in nZ$, et $I = nZ$. C.Q.F.D.

L'existence du *ppcm* de deux entiers a et b est alors immédiate: en effet $Za \cap Zb$ est un idéal de Z , donc est de la forme Zm . Pour le *pgcd* on peut le déduire du *ppcm*, en vérifiant que l'entier $d = ab/\text{ppcm}(a, b)$, d'une part divise a et b , d'autre part est multiple de tout diviseur commun à a et b . Mais il est plus fructueux et plus classique de noter que tout diviseur commun à a et b divise tous les éléments de l'idéal $Za + Zb$ (ensemble des sommes $ua + vb$, où u et v parcourent Z); or cet idéal est de la forme Zd ; comme $Za \subset Zd$, on voit que d divise a , et de même d divise b . Ainsi d a les propriétés classiques du *pgcd*; de plus il s'écrit

$$d = ua + vb \quad (u, v \in Z) \tag{3}$$

N. B. Il sera bon de dire que les mots « plus grand » et « plus petit » (dans « plus grand commun diviseur » et « plus petit commun multiple ») ne se rapportent qu'incidemment à la relation d'ordre usuelle de N ,