

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: I. Préliminaires
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>

SUR L'ORGANISATION D'UN COURS D'ARITHMÉTIQUE

par Pierre SAMUEL (Paris)

Malgré la prétendue difficulté de ce sujet, il est très fructueux d'enseigner de l'Arithmétique à de grands élèves scientifiques de l'enseignement secondaire. Par exemple, en France, les programmes de la classe de « Terminale C » (correspondant à l'ancienne « Mathématiques élémentaires ») en comportent. L'intérêt de l'Arithmétique est d'autant plus grand qu'elle permet d'illustrer, par des exemples nombreux et concrets, les notions d'Algèbre dite « moderne » (groupes, anneaux, corps, homomorphismes) qui prennent progressivement leur place dans les programmes de l'enseignement secondaire.

Les programmes français comprennent, très raisonnablement, les trois blocs suivants :

- (a) Congruences, anneaux $\mathbb{Z}/n\mathbb{Z}$;
- (b) L'unique décomposition des entiers en facteurs premiers;
- (c) L'étude des diviseurs (resp. multiples) communs à deux ou plusieurs nombres, et du p.g.c.d. (resp. p.p.c.m.).

Le but de cet article est de montrer qu'on peut mettre ces trois blocs dans un ordre à peu près arbitraire. Cependant quelques définitions et faits préliminaires sont nécessaires.

I. PRÉLIMINAIRES

On utilise les notations classiques N pour l'ensemble des entiers naturels et $\mathbb{Z}$ pour l'anneau des entiers relatifs. On commence par définir la relation de divisibilité dans $\mathbb{Z}$; on introduit les mots « divise », « diviseur », « multiple », et la très commode notation $x \mid y$. On remarque que la restriction à N de la relation $x \mid y$ est une relation d'ordre. On définit enfin un nombre premier comme un nombre $p > 1$ dont les seuls diviseurs (dans N) sont p et 1. On notera qu'il y a grand intérêt à entendre la relation de divisibilité au sens large (ainsi x divise x), et qu'il n'est pas recommandé de considérer 1 comme un nombre premier.

A propos des ensembles finis, on aura mis en évidence l'importante propriété suivante: toute application injective (resp. surjective) d'un ensemble fini dans lui-même est *bijjective*. On pourra dire aux élèves que cette propriété caractérise les ensembles finis, et leur montrer une application injective (resp. surjective) f de N dans lui-même qui n'est pas bijective; par exemple $f(n) = 2n$ (resp. $f(n) = n - 1$ pour $n \geq 1$ et $f(0) = 0$).

Enfin, étant donnés un groupe G (commutatif pour simplifier, et noté additivement) et un sous-groupe H de G , on aura montré que la relation $x - y \in H$ est une relation d'équivalence dans G (bien entendu des exemples seront les bienvenus ici, les congruences si l'on veut). La classe de x est l'ensemble traditionnellement noté $x + H$, et est en correspondance biunivoque avec H . Avec la notation $\text{card}(E)$ pour le nombre d'éléments d'un ensemble fini E , on en déduit aussitôt:

THÉORÈME. *Si G est un groupe commutatif fini et si H est un sous-groupe de G , alors $\text{card}(H)$ divise $\text{card}(G)$.*

Bien entendu l'hypothèse de commutativité est inutile.

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

1) Soit $n \geq 1$ un entier naturel. Les multiples de n forment un sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$. La relation d'équivalence $x - y \in n\mathbb{Z}$ dans $\mathbb{Z}$ est appelée la relation de *congruence modulo n* , et est notée $x \equiv y \pmod{n}$. On définit, sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ de ces classes d'équivalence, une structure de groupe additif, puis une structure d'*anneau*, déduites de celles de $\mathbb{Z}$. Tout ceci est bien classique.

On démontre alors le théorème de la *division euclidienne* (« tout entier $x \in \mathbb{Z}$ s'écrit, d'une façon et d'une seule, sous la forme $x = bn + r$ avec $b, r \in \mathbb{Z}$ et $0 \leq r \leq n - 1$ »). On en déduit aussitôt que $\mathbb{Z}/n\mathbb{Z}$ a *exactement n éléments*, à savoir les classes de $0, 1, \dots, n - 1$. On illustre ici le cours par des exercices de calculs modulo de petits entiers n , et par l'établissement des tables d'addition et de multiplication de $\mathbb{Z}/n\mathbb{Z}$ correspondantes. La recherche d'inverses dans ces tables de multiplication amène très naturellement au théorème suivant:

THÉORÈME. *Soit p un entier ≥ 2 . Alors « p premier » équivaut à « $\mathbb{Z}/p\mathbb{Z}$ est un corps ».*

Esquisse de démonstration: Si p n'est pas premier, on écrit $p = ab$ avec $a, b > 1$, et la classe de a dans $\mathbb{Z}/p\mathbb{Z}$ n'est pas inversible. Si p est