

# I. Préliminaires

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **13 (1967)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

# 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  $Z/nZ$ ;
- (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  $Z$  pour l'anneau des entiers relatifs. On commence par définir la relation de divisibilité dans  $Z$ ; 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 donné 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  $nZ$  de  $Z$ . La relation d'équivalence  $x - y \in nZ$  dans  $Z$  est appelée la relation de *congruence modulo  $n$* , et est notée  $x \equiv y \pmod{n}$ . On définit, sur l'ensemble  $Z/nZ$  de ces classes d'équivalence, une structure de groupe additif, puis une structure d'*anneau*, déduites de celles de  $Z$ . Tout ceci est bien classique.

On démontre alors le théorème de la *division euclidienne* (« tout entier  $x \in Z$  s'écrit, d'une façon et d'une seule, sous la forme  $x = bn + r$  avec  $b, r \in Z$  et  $0 \leq r \leq n - 1$  »). On en déduit aussitôt que  $Z/nZ$  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  $Z/nZ$  correspondantes. La recherche d'inverses dans ces tables de multiplication amène très naturellement au théorème suivant:

**THÉORÈME.** *Soit  $p$  un entier  $\geq 2$ . Alors «  $p$  premier » équivaut à «  $Z/pZ$  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  $Z/pZ$  n'est pas inversible. Si  $p$  est