

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 8 (1962)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: BIBLIOGRAPHIE DE L'ARITHMÉTIQUE
Autor: Chatelet, Albert
Kapitel: 6. Formes quadratiques
DOI: <https://doi.org/10.5169/seals-37965>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. 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. [Siehe Rechtliche Hinweise.](#)

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. [Voir Informations légales.](#)

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. [See Legal notice.](#)

Download PDF: 18.04.2025

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

Cette théorie étudie l'arithmétique et l'algèbre des entiers définis à l'addition près d'un multiple d'un entier fixe p ; les relations obtenues sont appelées *congruences* suivant le module p . Les entiers, ainsi définis, ne déterminent qu'un nombre fini d'êtres, encore appelées classes de congruence.

Si l'entier p (caractéristique) est premier, l'ensemble des classes forme un corps, c'est-à-dire que les 4 opérations élémentaires sont possibles. Mais le polynome $x^{p-1} - 1$ est nul pour toute valeur x du corps, sans être identiquement nul; plus généralement un polynome $F(x^p)$ peut être irréductible et n'avoir que des racines multiples.

Dans une note assez brève, E. GALOIS complète ces résultats par l'introduction d'imaginaires. Il considère des êtres $f(i)$, définis suivant 2 modules p et $\varphi(i)$, où φ est un polynome irréductible de degré f . Il obtient ainsi p^f êtres, ou imaginaires de Galois; toute équation de degré f à coefficients rationnels est décomposable.

DICKSON a montré que les ensembles d'imaginaires de Galois forment tous les *corps* qui ne contiennent qu'un *nombre fini d'éléments* (corps finis). L'étude de ces corps est indispensable pour la résolution des équations diophantiennes.

HENSEL a introduit des corps (infinis) — les corps locaux ou p -adiques — qui permettent d'utiliser les propriétés des congruences suivant les modules puissances de nombres premiers. Un tel corps est constitué par les séries formelles $(a_0 + a_1p + \dots)$, où les a_i sont des entiers définis au module p près.

Bibliographie: 2, 3, 9, 12, 13, 14, 15, 18, 27, 30, 37.

6. FORMES QUADRATIQUES

L'équation congruentielle:

$$x^2 - q \equiv 0 \pmod{p}$$

a été particulièrement étudiée à 2 points de vue différents: p étant donné, trouver les q (appelés restes quadratiques mod. p); q étant donné, trouver les p .

La loi de réciprocité quadratique de GAUSS lie ces 2 points de vue.

Mais les diviseurs p de $x^2 - q$ sont les mêmes que ceux de $x^2 - qy^2$ (si ces diviseurs p sont sans facteurs carrés et premiers à q); cette dernière expression est un cas particulier d'une *forme quadratique binaire*

$$ax^2 + bxy + cy^2.$$

L'étude des formes quadratiques binaires a été débütée par GAUSS et continuée par HERMITE. On appelle formes *équivalentes* celles qui représentent les mêmes nombres; elles peuvent être déduites les unes des autres par des substitutions unimodulaires. Dans chaque classe de formes équivalentes, on cherche des formes *réduites*. Ces problèmes sont liés, en analyse, à l'étude des fonctions fuchsiennes.

L'étude des formes quadratiques à 3, 4, ... variables a donné lieu à de nombreux travaux, mais pose encore des problèmes importants. L'étude des formes de degré supérieur est seulement ébauchée.

L'étude des formes quadratiques binaires a été partiellement abandonnée et remplacée par celle des corps quadratiques, grâce à la relation:

$$ax^2 + bxy + cy^2 = (\alpha x + \beta y)(\alpha' x + \beta' y)$$

avec α, β nombres quadratiques.

Bibliographie: 15, 18, 21, 30, 34, 43.

7. APPROXIMATIONS DIOPHANTIENNES

Etant donné un nombre rationnel ou irrationnel, on peut chercher les fractions rationnelles à termes simples qui en diffèrent peu; c'est le problème des approximations diophantiennes.

La seule solution entièrement satisfaisante est celle des *fractions continues*. Il est remarquable qu'elle soit liée à la théorie des formes quadratiques binaires, du développement périodique des irrationnelles du second degré et aux substitutions unimodulaires.