

5. CONGRUENCES ET CORPS FINIS

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **8 (1962)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **22.09.2024**

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.

ou (équations homogènes):

$$x^2 + y^2 = z^2, \quad y^2 z - x^3 = 0, \dots$$

Une première catégorie de problèmes est la recherche des *points à coordonnées entières*, ou à *coordonnées rationnelles* (en abrégé points entiers, ou points rationnels) sur des courbes algébriques à coefficients entiers.

Par exemple: recherche de x, y, z entiers tels que:

$$x^2 + y^2 = z^2$$

(points rationnels sur un cercle); $x/y = t$ est rationnel et $x/z, y/z$ s'en déduisent par les formules:

$$\frac{x}{z} = \frac{1 - t^2}{1 + t^2} \quad \frac{y}{z} = \frac{2t}{1 + t^2}$$

ou encore x, y, z sont proportionnels à

$$\lambda^2 - \rho^2, \quad 2\lambda\rho, \quad \lambda^2 + \rho^2$$

avec λ, ρ entiers premiers entre eux.

Plus généralement, on peut chercher les points entiers, ou les points rationnels, sur des *surfaces*, ou sur des *variétés algébriques* déterminées par des relations à coefficients entiers.

Ces problèmes ont donné lieu à de nombreuses recherches dispersées et à des solutions de fortune, notamment de FERMAT, EULER, LAGRANGE. Des recherches plus systématiques ont été entreprises dans ces dernières années, surtout par H. POINCARÉ et A. WEIL.

Bibliographie: 4, 12, 15, 23, 29, 33, 38, 41.

5. CONGRUENCES ET CORPS FINIS

L'étude du problème de Fermat ont conduit EULER, LAGRANGE, LEGENDRE, JACOBI à établir une théorie qui a été mise au point par GAUSS. Elle a été exposée dans les *Disquisitiones arithmeticae* parus en latin en 1801 et traduite depuis en français.

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 polynôme $x^{p-1} - 1$ est nul pour toute valeur x du corps, sans être identiquement nul; plus généralement un polynôme $F(x^p)$ 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 polynôme 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, trouvé les p .