

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 18 (1972)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: DÉMONSTRATION ÉLÉMENTAIRE D'UN THÉORÈME DE DAVENPORT ET HASSE
Autor: Morlaye, B.
Kapitel: I. Introduction
DOI: <https://doi.org/10.5169/seals-45377>

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: 14.01.2025

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

DÉMONSTRATION ÉLÉMENTAIRE D'UN THÉORÈME DE DAVENPORT ET HASSE

Par B. MORLAYE

I. INTRODUCTION

Soient p un nombre premier impair et D un entier rationnel. Pour $p \equiv 1 \pmod{4}$, soient en outre λ et $\bar{\lambda}$ les facteurs irréductibles primaires de p dans $\mathbf{Z}[i]$, caractérisés par la double condition :

$$p = \lambda \bar{\lambda}, \quad \lambda \equiv \bar{\lambda} \equiv 1 \pmod{2+2i},$$

et désignons par $(\cdot/\lambda)_4$ et $(\cdot/\bar{\lambda})_4$ les symboles de restes biquadratiques modulo λ et $\bar{\lambda}$. Rappelons que si $x \in \mathbf{Z}[i]$, $(x/\lambda)_4$ vaut 0 si $\lambda \mid x$, et est égal, si $\lambda \nmid x$, à l'unique puissance i^α de i telle que $x^{(p-1)/4} \equiv i^\alpha \pmod{\lambda}$. Ce symbole est multiplicatif vis à vis de x , et est égal à 1 si et seulement si x est congru modulo λ à une puissance quatrième. Dans [3], p. 178, Davenport et Hasse démontrent :

THÉORÈME 1: *Soit N le nombre de solutions (y compris la solution « infinie ») de la congruence $y^2 \equiv x^3 - Dx \pmod{p}$. On a :*

$$N = p + 1 \text{ si } p \equiv -1 \pmod{4}$$

$$N = p + 1 - \lambda \left(\frac{D}{\bar{\lambda}} \right)_4 - \bar{\lambda} \left(\frac{D}{\lambda} \right)_4 \text{ si } p \equiv 1 \pmod{4}$$

Citant ce résultat dans [2], p. 284, Swinnerton-Dyer ajoute : « There is no easy proof of the full theorem ». Effectivement, la démonstration donnée dans [3] repose sur l'application de la théorie du corps de classes au corps des fonctions rationnelles sur certaines courbes de genre 1 définies sur \mathbf{F}_p , et ne peut donc guère être considérée comme « élémentaire ». Plus récemment, Rajwade [7] a publié une autre démonstration, qui utilise certains résultats de Deuring appliqués à la courbe $y^2 = x^3 - Dx$. Cette démonstration est également très « technique ».

Le but de cet article est de donner les grandes lignes d'une démonstration « élémentaire » du théorème 1. Le principe est le suivant :

Soient C' la courbe $y^2 = x^4 - D$ définie sur le corps F_p et C la courbe $y^2 = x^3 - Dx$, également définie sur F_p . Notons N' et N le nombre de points de C' et C , rationnels sur F_p , y compris les points à l'infini. On montre (prop. 1) que $N = N' + 1$. Pour $p \equiv -1 \pmod{4}$, N' se calcule aisément, et on obtient $N = p + 1$, d'où la première partie du théorème 1. Pour $p \equiv 1 \pmod{4}$, on identifie F_p à $Z[i]/(\lambda)$ et on note ϕ et Ψ les caractères multiplicatifs d'ordre 2 et 4 de F_p auxquels s'identifient respectivement les symboles $(\cdot/\lambda)_2$ et $(\cdot/\lambda)_4$. On introduit alors les sommes de Jacobi $\pi(\Psi, \phi)$, $\pi(\phi, \phi)$ et $\pi(\bar{\psi}, \phi)$, et on montre que: $N' = p + \bar{\psi}(D)\pi(\Psi, \phi) + \Psi(D)\pi(\bar{\psi}, \phi)$. Pour achever la démonstration de la deuxième partie du théorème 1, il ne reste plus qu'à prouver (prop. 3) que $\pi(\Psi, \phi) = -\lambda$ et $\pi(\bar{\psi}, \phi) = -\bar{\lambda}$.

II. LA FORMULE FONDAMENTALE

Notons désormais k le corps F_p .

PROPOSITION 1: Avec les notations précédemment introduites, on a $N = N' + 1$.

1) La première étape de la démonstration est constituée par le résultat suivant:

Lemme 1: Le nombre de points rationnels sur k de la courbe $y^2 = P(x)$, où $P(x)$ est un polynôme, est donné par:

$$N = N_\infty + p + \sum_{x \in k} \phi(P(x))$$

(N_∞ désigne le nombre de points à l'infini de la courbe).

Preuve: Pour $x_0 \in k$ fixé, l'équation $y^2 = P(x_0)$ a, comme on le vérifie sans peine, $1 + \phi(P(x_0))$ solutions dans k . Il ne reste plus qu'à faire parcourir à x_0 le corps k et à sommer pour trouver le nombre de points de la courbe (affine) rationnels sur k . Le lemme 1 en résulte tout de suite.

2) Le lemme 1, appliqué aux courbes C et C' , donne tout de suite:

$$(1) \quad N = N_\infty + p + \sum_{x \in k} \phi(x^3 - Dx).$$

$$(2) \quad N' = N'_\infty + p + \sum_{x \in k} \phi(x^4 - D).$$