

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: III. Le cas $p \equiv -1 \pmod{4}$
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: 27.01.2025

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

6) *Remarque.*

On peut trouver de la proposition 1 une démonstration géométrique directe et très rapide; indiquons-en les grandes lignes: la courbe $y^2 = x^4 - D$ a pour modèle de Weierstrass (qui lui est donc birationnellement équivalent) la courbe $y^2 = 4x^3 + Dx$. Or, la « division par deux » de cette dernière courbe montre qu'elle est isogène à la courbe $y^2 = 4x^3 - 4Dx$, laquelle enfin est birationnellement équivalente à la courbe $y^2 = x^3 - Dx$, comme on le voit tout de suite. Or, deux courbes isogènes ont le même nombre de points rationnels (voir [1], p. 242); un petit calcul laissé au lecteur conduit alors à la formule $N = N' + 1$.

III. LE CAS $p \equiv -1 \pmod{4}$

C'est le cas « facile » du théorème. Il suffit de remarquer que l'on a (si $p \equiv -1 \pmod{4}$): $(p-1, 4) = (p-1, 2) = 2$. On en déduit que les courbes affines $y^2 = x^4 - D$ et $y^2 = x^2 - D$ ont le même nombre de points rationnels sur k (voir par exemple [6], hyp. (H_0)). Mais on a déjà vu dans la démonstration du lemme 3 que ce nombre est $p - 1$. On peut donc énoncer, compte tenu des points à l'infini et de la proposition 1:

PROPOSITION 2: *Lorsque $p \equiv -1 \pmod{4}$, on a $N = p + 1$.*

IV. LE CAS $p \equiv 1 \pmod{4}$

Nous supposons dorénavant $p \equiv 1 \pmod{4}$.

1) *Formule donnant le nombre de points de la courbe affine $y^2 = x^4 - D$.*

La courbe $y^2 = x^4 - D$ a une équation *diagonale*. On sait, dans ce cas, calculer le nombre de ses points rationnels sur k (voir [5], chap. 6, et [8]). En particulier, on peut appliquer le théorème 2 de [5], chap. 6, et écrire:

$$(5) \quad N'_a = p + \bar{\psi}(D) \pi(\Psi, \phi) + \pi(\Psi^2, \phi) + \Psi(D) \pi(\Psi^3, \phi),$$

en désignant par N'_a le nombre de points de la courbe *affine* (c'est-à-dire sans les points à l'infini) $y^2 = x^4 - D$, et par $\pi(\Psi, \phi)$ (par exemple) la somme de Jacobi $\sum_{\substack{u, v \in k \\ u+v=1}} \Psi(u) \phi(v)$ associée aux deux caractères Ψ et ϕ

(voir [4], p. 460, ou [5], chap. 5, § 3). Remarquons que $\Psi^2 = \phi$, si bien que $\pi(\Psi^2, \phi) = \pi(\phi, \phi)$. De plus: