

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.
DOI: <https://doi.org/10.5169/seals-45377>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. 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. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

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. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

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. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 09.07.2025

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:

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

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

Or, on peut écrire:

$$(3) \quad \sum_{x \in k} \phi(x^3 - Dx) = \sum_{x \in k} (1 + \phi(x)) (\phi(x^2 - D)) - \sum_{x \in k} \phi(x^2 - D).$$

D'autre part:

Lemme 2: On a l'égalité
$$\sum_{x \in k} (1 + \phi(x)) \phi(x^2 - D) = \sum_{x \in k} \phi(x^4 - D).$$

Preuve: Remarquons que $\phi(0) = 0$; il en résulte que la contribution de 0 à chacune des deux sommes étudiées est la même: $\phi(-D)$. On peut donc se borner à prouver que $S = S'$, en posant

$$S = \sum_{x \in k^*} (1 + \phi(x)) \phi(x^2 - D) \quad \text{et} \quad S' = \sum_{x \in k^*} \phi(x^4 - D).$$

Désignons par V l'image de k^* par l'application $x \rightarrow x^4 - D$. Cette application se « factorise » à travers k^{*2} , ce qui nous conduit à envisager 2 cas:

a) $p \equiv 1 \pmod{4}$ — Dans ce cas on a $(k^* : k^{*2}) = (k^{*2} : k^{*4}) = 2$. Il en résulte que $S' = 4 \sum_{y \in V} \phi(y) = 2 \sum_{x \in k^{*2}} \phi(x^2 - D)$, puisqu'un élément $y \in V$ fixé est alors l'image de quatre éléments distincts de k^* , ou de deux éléments distincts de k^{*2} .

b) $p \equiv 3 \pmod{4}$ — Dans ce cas $k^{*2} = k^{*4}$, et l'application $k^{*2} \rightarrow V$ qui factorise $k^* \rightarrow V$ est une bijection. On en déduit, ici encore, que $S' = 2 \sum_{x \in k^{*2}} \phi(x^2 - D)$, puisque tout élément de V provient d'un élément de k^{*2} unique, lequel est l'image de deux éléments distincts de k^* .

Donc, dans tous les cas, $S' = 2 \sum_{x \in k^{*2}} \phi(x^2 - D)$. Or, il est évident que $S = 2 \sum_{x \in k^{*2}} \phi(x^2 - D)$ puisque $\phi(x) = 1$ si $x \in k^{*2}$ et $\phi(x) = -1$ si $x \notin k^{*2}$. On a donc bien $S = S'$, ce qui achève la démonstration.

Compte tenu du lemme 2 et de la formule (3), la formule (1) devient alors:

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

Or, de façon claire, $N_\infty = N'_\infty = 1$; d'après (2) on obtient donc

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

Il ne reste plus qu'à calculer $\sum_{x \in k} \phi(x^2 - D)$. Cela peut se faire de deux façons.

3) Calcul « géométrique » de la somme $\sum_{x \in k} \phi(x^2 - D)$.

L'hyperbole $y^2 = x^2 - D$ est birationnellement équivalente sur k à la droite projective définie sur k ; elle a donc $p + 1$ points rationnels sur k . Comme elle a deux points à l'infini, le lemme 1 nous donne :

$$\sum_{x \in k} \phi(x^2 - D) = p + 1 - 2 - p = -1.$$

4) Calcul « arithmétique » de la somme $\sum_{x \in k} \phi(x^2 - D)$.

Distinguons deux cas :

a) D n'est pas résidu quadratique modulo p ; alors $x^2 - D$ n'est jamais nul, et si l'on désigne par A (resp. par B) l'ensemble des $x \in k$ tels que $x^2 - D \in k^{*2}$ (resp. $\notin k^{*2}$) on a : $\sum_{x \in k} \phi(x^2 - D) = \text{card}(A) - \text{card}(B)$.

Mais c'est un exercice élémentaire de vérifier que :

$$\text{card}(A) = \frac{p-1}{2}, \quad \text{card}(B) = \frac{p+1}{2};$$

$$\text{d'où } \sum_{x \in k} \phi(x^2 - D) = \frac{p-1}{2} - \frac{p+1}{2} = -1$$

b) D est résidu quadratique modulo p ; la méthode est la même qu'en a), mais ici $x^2 - D$ s'annule pour deux valeurs de x , si bien que l'on a :

$$\text{card}(A) = \frac{p-3}{2}, \quad \text{card}(B) = \frac{p-1}{2};$$

$$\text{d'où encore } \sum_{x \in k} \phi(x^2 - D) = -1.$$

5) D'une manière ou d'une autre, on a établi le résultat suivant :

Lemme 3 : On a l'égalité $\sum_{x \in k} \phi(x^2 - D) = -1$.

On peut alors conclure, en reportant cette valeur dans (4), que $N = N' + 1$, ce qui achève la démonstration de la proposition 1.

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:

Lemme 4 : On a $\pi(\phi, \phi) = -1$.

(Rappelons brièvement la démonstration de ce résultat. On voit facilement, compte tenu de la définition de $\pi(\phi, \phi)$ et de la relation $\phi^2 = 1$, que

$$\pi(\phi, \phi) = \sum_{\substack{x \in k \\ x \neq 1}} \phi\left(\frac{x}{1-x}\right) = \sum_{\substack{y \in k \\ y \neq -1}} \phi(y) = \sum_{y \in k} \phi(y) - \phi(-1);$$

Comme $\phi(0) = 0$ et que $\sum_{y \in k^*} \phi(y) = 0$ (somme des valeurs d'un caractère

non trivial), on a bien $\pi(\phi, \phi) = -\phi(-1) = -(-1)^{\frac{p-1}{2}} = -1$, puisque $p \equiv 1 \pmod{4}$).

Le lemme 4, la formule (5), et le fait que $\Psi^3 = \bar{\psi}$, donnent alors:

$$(6) \quad N'_a = p - 1 + \bar{\psi}(D) \pi(\Psi, \phi) + \Psi(D) \pi(\bar{\psi}, \phi).$$

2) *Calcul des sommes de Jacobi $\pi(\Psi, \phi)$ et $\pi(\bar{\psi}, \phi)$.*

PROPOSITION 3: On a les égalités $\pi(\Psi, \phi) = -\lambda$ et $\pi(\bar{\psi}, \phi) = -\bar{\lambda}$.

Il suffit d'établir la première de ces égalités. Commençons par prouver ici:

Lemme 5 : On a la congruence $\pi(\Psi, \phi) \equiv 0 \pmod{\lambda}$.

Preuve : En effet, on a, par définition de ϕ et Ψ :

$$\pi(\Psi, \phi) \equiv \sum_{x \in k} (1-x)^{\frac{p-1}{4}} x^{\frac{p-1}{2}} \pmod{\lambda};$$

mais le polynôme $P(X) = (1-X)^{\frac{p-1}{4}} X^{\frac{p-1}{2}}$ et de degré $\frac{3}{4}(p-1) < p$,

et on sait (voir [8], p. 12) que, dans ces conditions, $\sum_{x \in k} P(x) = 0$. Le

lemme 5 est ainsi démontré.

Remarquons maintenant que, ainsi qu'il est bien connu (« module d'une somme de Jacobi »: voir [4], p. 463, ou [5], chap. 5, prop. 9, cor. 1, ou [9], p. 502):

$$(7) \quad |\pi(\Psi, \phi)|^2 = p;$$

cette formule prouve que $\pi(\Psi, \phi)$ est un diviseur de p dans $\mathbf{Z}[i]$. Compte tenu du lemme 5, il suffit, pour démontrer la proposition 3, de prouver le résultat suivant:

Lemme 6 : On a la congruence $\pi(\Psi, \phi) \equiv -1 \pmod{2+2i}$.

Preuve : Posons à priori $\pi(\Psi, \phi) = a + ib$. La formule (7) nous donne :

$$(8) \quad a^2 + b^2 = p.$$

Par ailleurs, la courbe affine $y^2 + X^4 = 1$ a sur k un nombre de points rationnels donné par :

$$(9) \quad M = p + \pi(\phi, \phi) + \pi(\Psi, \phi) + \pi(\bar{\Psi}, \phi)$$

(même méthode que pour établir (6)).

On a donc :

$$(10) \quad M = p - 1 + 2a.$$

Comme k contient les racines carrées et quatrième de l'unité (puisque $p \equiv 1 \pmod{4}$) on voit facilement en faisant opérer ces racines de l'unité sur les coordonnées des points de la courbe que ces derniers se répartissent comme suit : six points sur les axes (quatre sur celui des x , deux sur celui des y), les autres points se regroupant huit par huit. Ainsi, M est de la forme $6 + 8h$, soit encore $M \equiv 6 \pmod{8}$, ou $p - 1 + 2a \equiv 6 \pmod{8}$; finalement :

$$(11) \quad -a \equiv \frac{p+1}{2} \pmod{4}.$$

Distinguons alors 2 cas :

- a) $p \equiv 1 \pmod{8}$; on a alors $-a \equiv 1 \pmod{4}$, et, d'après (8), $b \equiv 0 \pmod{4}$. Dans ce cas, $-(a+ib)$ est donc de la forme $1 + 4(s+it)$, avec s et $t \in \mathbf{Z}$.
- b) $p \equiv 5 \pmod{4}$; on a alors $-a \equiv 3 \pmod{4}$ et, d'après (8), $b \equiv 2 \pmod{4}$. Dans ce cas $-(a+ib)$ est donc de la forme $(3+2i) + 4(s+it)$, avec s et $t \in \mathbf{Z}$.

Comme $4 = -2(1+i)^2 i$, on voit que, dans les deux cas, on a $-(a+ib) \equiv 1 \pmod{2+2i}$, c'est-à-dire $\pi(\Psi, \phi) \equiv -1 \pmod{2+2i}$. Le lemme 6 est démontré. On a déjà dit que cela achevait de prouver la proposition 3.

3) *Conclusion* :

Compte tenu de la proposition 3, la formule (6) devient :

$$N'_a = p - 1 + \bar{\psi}(D)(-\lambda) + \Psi(D)(-\bar{\lambda});$$

avec l'identification signalée au début,

$$\Psi(D) = \left(\frac{D}{\lambda}\right)_4 \quad \text{et} \quad \bar{\Psi}(D) = \left(\frac{D}{\bar{\lambda}}\right)_4.$$

Donc :

$$N'_a = p - 1 - \lambda \left(\frac{D}{\bar{\lambda}}\right)_4 - \bar{\lambda} \left(\frac{D}{\lambda}\right)_4.$$

Tenant compte du point à l'infini et de la proposition 1, on trouve donc enfin :

PROPOSITION 4: *Dans le cas $p \equiv 1 \pmod{4}$, on a*

$$N = p + 1 - \lambda \left(\frac{D}{\bar{\lambda}}\right)_4 - \bar{\lambda} \left(\frac{D}{\lambda}\right)_4.$$

La conjonction des propositions 2 et 4 démontre le théorème 1.

BIBLIOGRAPHIE

- [1] CASSELS, J. W. S., « Diophantine equations with special reference to elliptic curves », *J. London Math. Soc.*, 41 (1966), pp. 193-291.
- [2] ——— and A. FRÖHLICH. Algebraic number theory. Academic Press, 1967.
- [3] DAVENPORT, H. und H. HASSE. « Die Nullstellen der Kongruenzetafunktionen in gewissen zyklischen Fällen », *J. reine angew. Math.*, 172 (1934), pp. 151-182.
- [4] HASSE, H. Vorlesungen über Zahlentheorie, Springer, 1964.
- [5] JOLY, J. R. « Equations et variétés algébriques sur un corps fini », *Enseign. Math.* (à paraître).
- [6] MORLAYE, B. « Equations diagonales non homogènes sur un corps fini », *C. R. Acad. Sci. Paris*, 271 (1971), pp. 1545-1548.
- [7] RAJWADE, A. R. « A note on the number of solutions N_p of the Congruence $y^2 \equiv x^3 - Dx \pmod{p}$ », *Proc. Cambridge Phil. Soc.*, 67 (1970), pp. 603-605.
- [8] SERRE, J. P. Cours d'arithmétique, P.U.F., 1970.
- [9] WEIL, A. « Numbers of solutions of equations in finite fields », *Bull. Amer. Math. Soc.*, 55 (1949), pp. 497-508.

(Reçu le 26 septembre 1972)

B. Morlaye,
21, rue des Tilleuls,
F - 73 - Barberaz.