IV. Le cas p 1(mod 4)

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 supposerons 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:

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

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 $\Psi^3 = \overline{\psi}$, donnent alors:

$$N_a' = p - 1 + \overline{\psi}(D)\,\pi(\Psi, \phi) + \Psi(D)\,\pi(\overline{\psi}, \phi). \tag{6}$$

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

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

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 ou 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):

$$|\pi(\Psi, \phi)|^2 = p; \tag{7}$$

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 $\pi(\Psi, \phi) \equiv -1 \bmod (2+2i)$.

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

8) $$a^2 + b^2 = p.$$

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

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

(même méthode que pour établir (6)).

On a donc:

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

Comme k contient les racines carrées et quatrièmes 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) $$-a \equiv \frac{p+1}{2} \pmod 4.$$

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 $-(a+ib) \equiv 1 \mod (2+2i)$, c'est-à-dire $\pi(\Psi, \phi) \equiv -1 \mod (2+2i)$. 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 Kongruenzzetafunktionen in gewissen zyklischen Fallen », *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.