(a) $d \equiv 1\ (4)$: $d = 3\times 7^{**}, 3\times 23, 7\times 11^{**}, 3\times 31, 3\times 71, 3\times 79, 7\times 59, 19\times 23^{**}, 3\times 151, 3\times 239, 3\times 359, 11\times 103$ *et* 7×179.

(b) $d \equiv 2, 3\ (4)$: $d = 3^{*}, 2\times 3, 7, 11, 2\times 7, 23, 2\times 19, 47, 2\times 31, 83, 167, 227$ *et* 2×199.

(3) $N(\varepsilon_0) = +1$ *et* $h(d) = 2$:

(a) $d \equiv 1\ (4)$: $d = 3\times 5\times 11^{**}, 3\times 5\times 19^{**}, 3\times 7\times 17^{**}, 3\times 11\times 29^{**}, 5\times 7\times 31^{**}, 3\times 5\times 131, 3\times 5\times 139$ *et* $3\times 17\times 47^{**}$.

(b) $d \equiv 2, 3\ (4)$: $d = 3\times 5^{*}, 2\times 3\times 5, 5\times 7^{*}, 2\times 3\times 7, 3\times 29, 2\times 5\times 11, 2\times 3\times 23, 11\times 13^{*}, 2\times 7\times 13, 5\times 43, 2\times 3\times 53, 3\times 149$ *et* 5×127.

(4) $N(\varepsilon_0) = +1$ *et* $h(d) = 4$:

$d \equiv 2, 3\ (4)$: $d = 3\times 5\times 13^{*}, 3\times 5\times 17^{*}, 3\times 7\times 23^{*}, 2\times 3\times 5\times 31, 5\times 7\times 37^{*}$ *et* $2\times 3\times 7\times 41$.

Références

[1] H. Amara, *Cycles canoniques d'idéaux réduits et nombres de classes de certains corps quadratiques réels*, Nagoya Math. J. 103 (1986), 127–132.

[2] T. Azuhata, *On the fundamental units and the class numbers of real quadratic fields*, Proc. Japan Acad., Ser. A, 62 (1986), 97–100.

[3] A. Chatelet, *L'arithmétique des corps quadratiques*, L'enseignement des mathématiques, N° 9; Genève 1962.

[4] H. Hasse, *Vorlesungen über Zahlentheorie*, §16, Berechnung der Grundeinheit, Springer-Verlag, 1964.

[5] M. Kutsuna, *On a criterion for the class number of a quadratic number field to be one*, Nagoya Math. J. 79 (1980), 123–129.

[6] G. Lachaud, *Sur les corps quadratiques réels principaux*. Séminaire de théorie de nombres, Paris 1984–85, Progress in Mathematics, Vol. 63, p. 165–175.

[7] S. Louboutin, *Continued fractions and real quadratic fields*, J. Number Theory 3 (1988), 167–176.

[8] R. A. Mollin and H. C. Williams, *On prime valued polynomials and class number of real quadratic fields*, Research paper N° 653, July 1987; University of Calgary.

[9] — —*A conjecture of S. Chowla via the generalized Riemann hypothesis*, Proc. Amer. Math. Soc. 102 (1988), 794–796.

[10] R. A. Mollin, *Class number one criteria for real quadratic fields*, Proc. Japan Acad., Ser. A, 63 (1987), I, 121–125; II, 162–164.

[11] Y. Yamamoto, *Real quadratic number fields with large fundamental units*, Osaka J. Math. 8 (1971), 261–270.

UNIVERSITÉ PARIS VII
UER DE MATHÉMATIQUES ET INFORMATIQUE
UNITÉ ASSOCIÉE AU CNRS N°212
Tour 45 55, 5ème étage;
2 Place Jussieu
75251 Paris Cedex 05
France

Reçu le 3.2.1988
et dans la forme modifiée le 28.4.1988 (1782)

ACTA ARITHMETICA
LIV (1989)

Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique

par

ALAIN KRAUS (Paris)

A. Introduction. Soit K un corps de caractéristique nulle muni d'une valuation discrète v normalisée par $v(K^*) = \mathbf{Z}$.

On introduit les notations suivantes:

O_K l'anneau de valuation;

p la caractéristique résiduelle;

e la valuation de p.

À une équation de Weierstrass affine (W) à coefficients dans O_K:

$$(W) \qquad y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,$$

on associe des invariants c_4, c_6 et Δ que l'on calcule par le procédé suivant [1]:

$$\begin{aligned}
b_2 &= a_1^2+4a_2,\\
b_4 &= a_1a_3+2a_4,\\
b_6 &= a_3^2+4a_6,\\
b_8 &= a_1^2a_6-a_1a_3a_4+4a_2a_6+a_2a_3^2-a_4^2,\\
c_4 &= b_2^2-24b_4,\\
c_6 &= -b_2^3+36b_2b_4-216b_6,\\
\Delta &= -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6.
\end{aligned}$$

Ces grandeurs sont reliées par:

$$4b_8 = b_2b_6-b_4^2, \qquad 1728\Delta = c_4^3-c_6^2.$$

La cubique définie par l'équation (W) est non singulière si et seulement si Δ est non nul.

Étant donnés des éléments c_4, c_6 et Δ de O_K satisfaisant à

$$(*) \qquad c_4^3-c_6^2 = 1728\Delta \quad \text{et} \quad \Delta \neq 0$$

on se propose de déterminer des conditions nécessaires et suffisantes simples pour que c_4, c_6 et Δ puissent être réalisés comme les invariants $c_4(W)$, $c_6(W)$ et $\Delta(W)$ d'une équation de Weierstrass (W) définie sur O_K. Si tel est le cas, on écrira $c_4 = c_4(W)$, $c_6 = c_6(W)$, $\Delta = \Delta(W)$.

S'il existe une telle équation, elle est unique à un changement de variables près de la forme:

$$\begin{cases} x = x' + r, \\ y = y' + sx' + t \end{cases}$$

où r, s, t sont des éléments de O_K.

Je tiens à remercier J. Oesterlé pour les conseils qu'il a bien voulu me donner.

B. Énoncé des résultats. Le cas où $p \geqslant 5$ est facile et rappelé pour mémoire:

PROPOSITION 1. *Supposons $p \geqslant 5$. Quels que soient c_4, c_6, Δ dans O_K satisfaisant (*), il existe une équation de Weierstrass (W) à coefficients dans O_K telle que $c_4 = c_4(W)$, $c_6 = c_6(W)$.*

Cas où $p = 3$.

THÉORÈME 1. *Supposons $p = 3$, et soient c_4, c_6, Δ dans O_K satisfaisant (*). Il existe une équation de Weierstrass (W) définie sur O_K telle que $c_4 = c_4(W)$, $c_6 = c_6(W)$ si et seulement si l'une des conditions suivantes est vérifiée:*

(a) *c_6 est une unité de O_K;*

(b) *on a $0 < v(c_6) < 3e$ et il existe x dans O_K tel que*

$$x^3 - 3xc_4 - 2c_6 \equiv 0 \bmod 27;$$

(c) *on a $c_6 \equiv 0 \bmod 27$.*

Remarque. Sous les hypothèses du théorème 1, et si la condition (b) est satisfaite par un élément x de O_K, on a

$$3v(x) = v(c_6), \quad x^2 \equiv c_4 \bmod 3 \quad \text{et} \quad xc_4 + c_6 \equiv 0 \bmod 3.$$

COROLLAIRE. *Supposons toujours $p = 3$, et de plus $e = 1$ (par exemple $K = \boldsymbol{Q}_3$); soient c_4, c_6, Δ dans O_K satisfaisant (*). Il existe une équation de Weierstrass définie sur O_K telle que $c_4 = c_4(W)$, $c_6 = c_6(W)$, si et seulement si $v(c_6) \neq 2$.*

Démonstration du corollaire. Par hypothèse, on a $c_4^3 - c_6^2 = 1728\Delta$, d'où $c_4^3 \equiv c_6^2 \bmod 27$. Il en résulte que l'on a $v(c_6) = 0$, $v(c_6) = 2$ ou $v(c_6) \geqslant 3$. Si $v(c_6) = 0$ ou $v(c_6) \geqslant 3$, l'existence de (W) est assurée par le théorème 1, (a) ou (c). Si $v(c_6) = 2$, le théorème 1(b) et la remarque qui le suit montrent qu'il n'existe pas d'équation (W) possédant les propriétés requises.

Cas où $p = 2$.

THÉORÈME 2. *Supposons $p = 2$, et soient c_4, c_6, Δ dans O_K satisfaisant (*). Il existe une équation de Weierstrass (W) définie sur O_k telle que $c_4 = c_4(W)$, $c_6 = c_6(W)$ si et seulement si l'une des conditions suivantes est vérifiée:*

(a) *c_4 est une unité de O_K et $-c_6$ est un carré modulo 4;*

(b) *$0 < v(c_4) < 4e$ et il existe x dans O_K tel que si $P(X) = -X^6 + 3X^2c_4 + 2c_6$, on ait:*

$$\begin{cases} 4x^2P(x) \equiv (x^4 - c_4)^2 \bmod 2^8, \\ P(x) \text{ est multiple de } 16, \\ P(x)/16 \text{ est un carré modulo } 4; \end{cases}$$

(c) *on a $c_4 \equiv 0 \bmod 16$ et il existe x dans O_K tel que $c_6 \equiv 8x^2 \bmod 32$.*

Remarque. Si la condition (b) du théorème 2 est satisfaite par un élément x de O_K, on a $v(c_4) = 4v(x)$.

COROLLAIRE. *Supposons toujours $p = 2$ et de plus $e = 1$; soient c_4, c_6, Δ dans O_K satisfaisant (*). Il existe une équation de Weierstrass (W) définie sur O_K telle que $c_4 = c_4(W)$, $c_6 = c_6(W)$ si et seulement si l'une des conditions suivantes est vérifiée:*

(a) *c_4 est une unité de O_K et $-c_6$ est un carré modulo 4;*

(b) *on a $c_4 \equiv 0 \bmod 16$ et il existe x dans O_K tel que $c_6 \equiv 8x^2 \bmod 32$.*

(Lorsque $K \equiv \boldsymbol{Q}_2$, ces conditions s'écrivent respectivement

(a) $c_6 \equiv -1 \bmod 4$,

(b) $v(c_4) \geqslant 4$ *et* $c_6 \equiv 0$ *ou* $8 \bmod 32$.)

Démonstration du corollaire. Si $0 < v(c_4) < 4$, le théorème 2(b) et la remarque précédente montrent qu'il n'existe pas d'équation (W) réalisant $c_4 = c_4(W)$ et $c_6 = c_6(W)$. Si $v(c_4) = 0$ ou $v(c_4) \geqslant 4$, le corollaire résulte du théorème 2, (a) et (c).

C. Démonstrations.

Cas où $p \geqslant 5$. L'équation (W): $y^2 = x^3 - (c_4/48)x - (c_6/864)$ est définie sur O_K si $p \geqslant 5$ avec $c_4 = c_4(W)$ et $c_6 = c_6(W)$, ce qui démontre la proposition.

Cas où $p = 3$. Montrons d'abord qu'il existe une équation (W) telle que $c_4 = c_4(W)$, $c_6 = c_6(W)$ si et seulement si il existe x dans O_K tel que

$$\text{(1)} \qquad \begin{cases} x^3 - 3xc_4 - 2c_6 \equiv 0 \bmod 27, \\ c_4 \equiv x^2 \bmod 3. \end{cases}$$

La nécessité de (1) résulte des définitions en prenant $x = b_2$; inversement pour un x de O_K satisfaisant (1), l'équation

$$\text{(W)} \qquad Y^2 = X^3 + (x/4)X^2 + (x^2 - c_4)/48X + (x^3 - 3xc_4 - 2c_6)/1728$$

réalise $c_4 = c_4(W)$ et $c_6 = c_6(W)$ et est à coefficients dans O_K. Étant donné un élément x de O_K, il résulte de l'identité

$$(x^2 - c_4)^3 = (x^3 - 3xc_4 - 2c_6)(x^3 + 2c_6) + 3(xc_4 + c_6)^2 + c_6^2 - c_4^3$$

que la condition (1) équivaut à

$$(2)\qquad \begin{cases} x^3-3xc_4-2c_6 \equiv 0 \bmod 27, \\ xc_4+c_6 \equiv 0 \bmod 3. \end{cases}$$

Plaçons nous dans la condition (a) du théorème 1, c'est à dire supposons que c_6 soit une unité de O_K. Posons $x = -c_6/c_4$; il est clair que x satisfait (2) puisque $c_4^3 \equiv c_6^2 \bmod 27$.

Supposons maintenant $0 < v(c_6) < 3e$. Considérons un élément x de O_K satisfaisant à $x^3-3xc_4-2c_6 \equiv 0 \bmod 27$. Vérifions qu'il satisfait aussi à $xc_4+c_6 \equiv 0 \bmod 3$. Pour cela, on remarque que les congruences $c_4^3 \equiv c_6^2 \bmod 27$ et $x^3 \equiv 3xc_4+2c_6 \bmod 27$ entraînent

$$(xc_4+c_6)^3 \equiv 3c_6(xc_4+c_6)^2 \bmod 27, \quad \text{d'où } xc_4+c_6 \equiv 0 \bmod 3.$$

Cela prouve l'assertion (b) du théorème 1. Posons alors $c_4 = x^2+3u$ (avec u dans O_K); on a $2x^3+9xu+2c_6 \equiv 0 \bmod 27$, d'où l'égalité $3v(x) = v(c_6)$ et la remarque qui suit le théorème 1.

Enfin, si $v(c_6) \geqslant 3e$, il est clair que $x = 0$ satisfait (2). Cela achève la démonstration du théorème 1.

Cas où $p = 2$. S'il existe une équation de Weierstrass (W) à coefficients dans O_K telle que $c_4 = c_4(W)$ et $c_6 = c_6(W)$, il en existe une aussi dont le coefficient a_2 soit nul. L'existence d'une telle équation équivaut alors par définition à l'existence d'éléments a_1 et a_3 de O_K tels que:

$$(3)\qquad \begin{cases} a_1^4-c_4 \equiv 8a_1a_3 \bmod 16, \\ P(a_1) \equiv 16a_3^2 \bmod 64 \end{cases}$$

où $P(X) = -X^6+3X^2c_4+2c_6$.

Cela équivaut encore à l'existence d'un élément x de O_K tel que:

$$\begin{cases} 4x^2P(x) \equiv (x^4-c_4)^2 \bmod 2^8, \\ P(x) \text{ est multiple de } 16, \\ P(x)/16 \text{ est un carré modulo } 4. \end{cases}$$

Ceci prouve en particulier l'assertion (b) du théorème 2. Quant à la remarque qui suit ce théorème, elle se déduit simplement du fait qu'un élément x de O_K vérifiant la condition (b) est tel que $v(x) < e$.

Supposons que c_4 soit une unité de O_K. Il en est alors de même de c_6. S'il existe (W) tel que $c_4 = c_4(W)$ et $c_6 = c_6(W)$, alors il résulte des définitions de b_2 et c_6 que $-c_6$ est un carré modulo 4. Inversement, soit t un élément de O_K tel que $-c_6 \equiv t^2 \bmod 4$; en utilisant le fait que $c_4^3 \equiv c_6^2 \bmod 64$, on constate que l'élément $x = c_4/t$ vérifie les deux congruences

$$\begin{cases} c_4 \equiv x^4 \bmod 8, \\ -c_6 \equiv x^6 \bmod 4. \end{cases}$$

Par conséquent, il existe des éléments u et v de O_K tels que

$$\begin{cases} c_4 = x^4+8v, \\ c_6 = -x^6+4u. \end{cases}$$

La congruence $c_4^3 \equiv c_6^2 \bmod 64$ s'écrit alors $3x^8v \equiv 2u^2-x^6u \bmod 8$. En se servant de cette congruence, il est facile de vérifier que les éléments $a_1 = x$ et $a_3 = u/x^3$ satisfont (3). Cela prouve l'assertion (a) du théorème 2.

Supposons maintenant $v(c_4) \geqslant 4e$. Si des éléments a_1 et a_3 de O_K satisfont (3), on a $v(a_1) \geqslant e$, d'où $P(a_1) \equiv 2c_6 \bmod 64$ et $c_6 \equiv 8a_3^2 \bmod 32$; réciproquement, s'il existe x dans O_K tel que $c_6 \equiv 8x^2 \bmod 32$ les éléments $a_1 = 0$ et $a_3 = x$ vérifient (3), ce qui démontre l'assertion (c) du théorème 2.

Remarques. Dans le cas où $p = 3$:

1. L'existence d'un élément x de O_K tel que

$$x^3-3c_4x-2c_6 \equiv 0 \bmod 27$$

est équivalente à l'existence d'un élément u de K tel que

$$u^3-(c_4/48)u-(c_6/864)$$

appartient à O_K.

De tels éléments existent par exemple si la courbe elliptique

$$y^2 = x^3-(c_4/48)x-(c_6/864)$$

possède un point d'ordre 2 défini sur K.

2. Supposons $0 < v(c_6) < 3e$; vu la remarque qui suit le théorème 1, si un élément x de O_K vérifie $x^3-3xc_4-2c_6 \equiv 0 \bmod 27$, il en est de même de $x+3u$ pour tout $u \in O_K$. Les solutions de cette congruence peuvent donc être recherchées modulo 3.

Dans le cas où $p = 2$:

1. Posons $K = Q_2(\pi)$ où $\pi^6 = 2$, $c_4 = 8\pi^2$, $c_6 = 8\pi^3$. On a $e = 6$, $v(c_4) = 20$ et $v(c_6) = 21$.

On constate que l'élément $x = \pi^5$ vérifie $4x^2P(x) \equiv (x^4-c_4)^2 \bmod 2^8$ bien que la congruence $P(x) \equiv 16z^2 \bmod 64$ soit sans solution dans O_K. En ce sens, la condition (b) du théorème 2 est minimale.

2. Si un élément x de O_K satisfait la condition (b) du théorème 2 il en est de même de $x+2u$ pour tout $u \in O_K$.

En effet, d'après la démonstration du théorème 2, cette condition est équivalente à l'existence d'un élément z de O_K tel que:

$$\begin{cases} x^4-c_4 \equiv 8xz \bmod 16, \\ P(x) \equiv 16z^2 \bmod 64. \end{cases}$$

Or si $u \in O_K$, on vérifie que:

$$\begin{cases}(x+2u)^4 - c_4 \equiv 8(x+2u)z' \bmod 16,\\ P(x+2u) \equiv 16(z')^2 \bmod 64,\end{cases}$$

où $z' = z + ux^2 + u^2x$.

Cela démontre l'assertion. Par conséquent, la solution x du système peut être recherchée modulo 2.

D. Conséquences.

1. Considérons E une courbe elliptique définie sur K. Soit (W) un modèle de E entier, et π une uniformisante de K. (W) est un modèle minimal pour E si et seulement si $c_4(W)/\pi^4$ et $c_6(W)/\pi^6$ ne sont pas les invariants $c_4(W')$ et $c_6(W')$ d'une équation de Weierstrass (W') définie sur O_K. Les résultats précédents permettent donc de déterminer si un modèle donné de E est minimal.

2. Désignons par $v_p(a)$ la valuation p-adique d'un entier relatif a.

PROPOSITION 2. *Soient c_4, c_6, Δ des éléments de $\mathbf{Z}$ tels que $c_4^3 - c_6^2 = 1728\,\Delta$ et $\Delta \neq 0$. Pour qu'il existe une équation de Weierstrass (W) à coefficients dans $\mathbf{Z}$ avec $c_4 = c_4(W)$, $c_6 = c_6(W)$ il faut et il suffit que l'on ait $v_3(c_6) \neq 2$ et*

$$\begin{cases} c_6 \equiv -1 \bmod 4\\ \textit{ou}\\ v_2(c_4) \geqslant 4 \quad \textit{et} \quad c_6 \equiv 0 \textit{ ou } 8 \bmod 32.\end{cases}$$

On a $c_4 = c_4(W)$, $c_6 = c_6(W)$ avec (W) une équation de Weierstrass définie sur $\mathbf{Z}$ si et seulement si il en est de même sur $\mathbf{Z}_2$ et $\mathbf{Z}_3$. Il suffit alors de récrire les corollaires des deux théorèmes pour obtenir le résultat.

Remarque. J. F. Mestre m'a communiqué l'énoncé de la proposition 2 qu'il avait obtenu auparavant mais qu'il n'a pas publié.

Bibliographie

[1] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*; in: *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer-Verlag, 1975, 33–52.

Reçu le 1.3.1988 (1795)

ACTA ARITHMETICA
LIV (1989)

Sur un théorème de M. Langevin

par

MAURICE MIGNOTTE (Strasbourg)

1. Introduction. Dans [4], Michel Langevin a démontré le résultat suivant.

THÉORÈME A. *Soit V un voisinage d'un point du cercle unité. Alors il existe une constante $C > 1$, effectivement calculable, telle que tout polynôme à coefficients entiers, irréductible et qui ne possède pas de zéro dans V a une mesure qui vérifie $M(P) \geqslant C^d$ lorsque le degré d du polynôme P est assez grand.*

La démonstration utilise la notion de diamètre transfini. L'étape principale consistant à prouver que le diamètre transfini du disque unité privé des points de V est < 1.

Nous allons donner une démonstration très différente de ce résultat. Cette démonstration s'effectue en deux étapes:

1°, construction d'un multiple du polynôme P de petite hauteur,

2°, application d'un théorème d'Erdős–Turán sur la répartition des racines d'un polynôme à coefficients complexes.

Par cette méthode nous obtenons un résultat général dont le théorème A est un corollaire (voir la remarque à la suite du corollaire 3).

Soit

$$F = \sum_{i=0}^{n} a_i X^i, \quad a_n \neq 0,$$

un polynôme à coefficients complexes. Rappelons les définitions suivantes: on pose

$$H(F) = \max_{0 \leqslant i \leqslant n} |a_i|, \quad \text{la hauteur de } F,$$

$$L(F) = \sum_{i=0}^{n} |a_i|, \quad \text{la longueur de } F.$$