

AN INTRODUCTION TO ELLIPTIC CURVES AND THEIR DIOPHANTINE GEOMETRY — MORDELL CURVES

KATSUYA MIYAKE

RÉSUMÉ. Nous décrivons d’abord la conjecture de Birch et Swinnerton-Dyer et indiquons l’importance de la géométrie diophantienne des courbes elliptiques. Puis nous passons en revue l’histoire des courbes de Mordell $y^2 = x^3 + k$, $k \in \mathbb{Q}$. Ensuite, nous nous concentrons sur la géométrie des courbes elliptiques sur $\mathbb{C}$ et sur l’arithmétique des courbes elliptiques à multiplication complexe. La dernière section est consacrée au survol des travaux récents de l’auteur sur la géométrie diophantienne des courbes de Mordell de la forme

$$M : y^2 = x^3 - B^2(B + 3), \quad \text{où } B = \frac{4b}{9} \text{ avec } b \in \mathbb{Q},$$

associées aux corps cubiques déterminés par le polynôme $X^3 + bX + b$, $b \in \mathbb{Q}$.

ABSTRACT. We first give a brief description of the Birch and Swinnerton-Dyer conjecture and indicate the importance of the Diophantine geometry of elliptic curves. A brief historical review of the Mordell curves $y^2 = x^3 + k$, $k \in \mathbb{Q}$, is also given. Then we deal with the geometry of elliptic curves over $\mathbb{C}$ and with the arithmetic of those elliptic curves which have complex multiplication. The last section is devoted to a brief review of the author’s recent work on the Diophantine geometry of the Mordell curves of the form

$$M : y^2 = x^3 - B^2(B + 3), \quad \text{where } B = \frac{4b}{9} \text{ with } b \in \mathbb{Q}$$

associated to the cubic field defined by the polynomial $X^3 + bX + b$, $b \in \mathbb{Q}$.

1. Introduction.

1.1. One of the deepest and most interesting problems on the arithmetic of elliptic curves over the rational number field is certainly the Birch and Swinnerton-Dyer conjecture ([BS-63, BS-65]). It claims that certain basic analytic invariants of the Hasse-Weil L -function of an elliptic curve can be expressed via the periods and some algebraic invariants. A refined description of the conjecture looks quite analogous to the residue of the Dedekind zeta-function of an algebraic number field at the pole $s = 1$, although, at present, we cannot see any mathematical reasons for the resemblance.

Reçu le 4 janvier 2005 et, sous forme définitive, le 17 février 2005.

It has been proved by the epoch-making work of Andrew Wiles [Wi-95], complemented by C. Breuil, B. Conrad, F. Diamond and R. Taylor [BCDT-01], that *every elliptic curve over the rational number field $\mathbb{Q}$ is modular*, and hence that its Hasse-Weil L -function $L(s)$ coincides with the L -function of a related modular form. Therefore, $L(s)$ has a functional equation and can be analytically continued all over the complex plane as a meromorphic function. If the order of its zero at $s = 1$ is r , say, then the limit value $\lim_{s \rightarrow 1} (s - 1)^{-r} L(s)$ is well defined. This order r is called the analytic rank of the elliptic curve, and is conjectured to coincide with the Mordell-Weil rank of the curve, that is, the $\mathbb{Z}$ -rank of the free part of the $\mathbb{Z}$ -module of $\mathbb{Q}$ -rational points. (This is the easy-to-state part of the Birch and Swinnerton-Dyer conjecture. The precise description of the conjecture is, for example, found in the textbook of J. Silverman [Si-86].)

It should also be noted that the L -functions of two elliptic curves over $\mathbb{Q}$ coincide with each other if and only if the curves are isogenous over $\mathbb{Q}$. This is now an immediate conclusion of the isogeny theorem (for $\mathbb{Q}$) of the celebrated work [Fa-83, Fa-84] of G. Faltings in which he proved the theorem for every algebraic number field along the way to proving the Mordell conjecture.

The analytic basis of the Birch and Swinnerton-Dyer conjecture has thus been settled. It is however far beyond my task here to present anything substantial concerning that conjecture. My goal is to give a brief geometric background on elliptic curves and to introduce the Diophantine geometry of a certain family of Mordell curves.

1.2. In 1914 Mordell investigated integral solutions of the equation

$$M(k) : y^2 = x^3 + k$$

with $k \in \mathbb{Z}$ in his article [Mo-14]. Then Nagell [Na-24] studied rational points on the curve when k is a perfect cube. In his paper [Fu-30] Fueter worked on the equation by expressing it as $x^3 = y^2 + D$ and factorizing the right hand side in the quadratic field $\mathbb{Q}(\sqrt{-D})$. The papers [Ca-50] of J. W. S. Cassels and [Se-51, Se-54] of E. S. Selmer are to be considered as classic references. In 1998 J. Gebel, A. Pethő and H. G. Zimmer [GPZ-98] published their article “On Mordell’s Equation” after which I chose the terminology “*Mordell curves*” in this survey. As you see from the fact that they take the values of the parameter k in $\mathbb{Z}$ or in $\mathbb{Q}$, their main interest is in the Diophantine geometry of the equation. Indeed, the curve $M(-2^4 3^3)$ for $k = -2^4 3^3$ is a short form of the Fermat cubic curve $X^3 + Y^3 + Z^3 = 0$. Furthermore, the curve

$$M(-2^4 3^3 A^2) : y^2 = x^3 - 2^4 3^3 A^2$$

with $A \in \mathbb{Q} - \{0\}$ is a short form of the cubic twist

$$F(A) : X^3 + Y^3 = AZ^3$$

of the Fermat cubic curve; they transform into each other over $\mathbb{Q}$; see [Ca-50] for example.

In Chapter 2, we briefly review the geometry of elliptic curves given by the short Weierstrass forms $y^2 = 4x^3 - g_2x - g_3$ over the field $\mathbb{C}$ of complex numbers. (If we

replace y, g_2 , and g_3 , respectively, by $2y, g_2/4$, and $g_3/4$, then we can transform it to a form with the leading coefficient of the right hand side equal to 1.) Then our curve $M(k)$ has complex multiplication by the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$, and its j -invariant is equal to 0. The book [Co-89] of D. A. Cox is a fine classic introduction to complex multiplication.

In Chapter 3, we study some Diophantine relations between a family of elliptic curves given by a general cubic polynomial and a subfamily of our Mordell curves. The set of $\mathbb{Q}$ -rational points of each member of the subfamily is described by a certain subset of the related cubic field. We also illustrate a Diophantine way to obtain short forms of the elliptic curves with the help of Mordell's celebrated book [Mo-69]; (see [Mi-03-1,2]).

The basic references on our present subject are the books [Si-86] and [Si-94] of J. Silverman, and [ST-92] of J. Silverman and J. Tate.

2. Elliptic curves over $\mathbb{C}$.

2.1. The algebraic curve defined by a short form. Let us call an equation in x and y of the form

$$E : y^2 = P(x) := ax^3 + bx^2 + cx + d, \quad a, b, c, d \in \mathbb{C},$$

a *short form*. The set $E[\mathbb{C}]$ of those pairs (x, y) of complex numbers which satisfy the equation E forms an algebraic curve:

$$E[\mathbb{C}] := \{(x, y) \mid x, y \in \mathbb{C}, y^2 = ax^3 + bx^2 + cx + d\}.$$

We assume $a \neq 0$ to obtain an elliptic curve. Then by replacing x and y by ax and a^2y , respectively, we may assume that the leading coefficient of the cubic polynomial $P(x)$ is equal to 1: $a = 1$. Next we replace x by $x - b/3$. Then the coefficient of x^2 vanishes. Hence we may assume without losing generality that the short form is given as

$$E : y^2 = P(x) := x^3 + cx + d, \quad c, d \in \mathbb{C}.$$

The curve $E[\mathbb{C}]$ is embedded in the projective space $\mathbb{P}^2(\mathbb{C})$ with the homogeneous coordinate system $(X : Y : Z)$ by putting $x = X/Z$ and $y = Y/Z$. Then we have the homogeneous equation

$$\bar{E} : Y^2Z = X^3 + cXZ^2 + dZ^3.$$

Since the hyperplane at infinity is given by $Z = 0$, $\bar{E}[\mathbb{C}]$ has just one point at infinity $P_\infty = (0 : 1 : 0)$. We have

$$\bar{E}[\mathbb{C}] = E[\mathbb{C}] \cup \{P_\infty\}.$$

To obtain an elliptic curve such as $\bar{E}[\mathbb{C}]$, we need one more condition. Let $\Delta(P(x)) := -(4c^3 + 27d^2)$ be the discriminant of the cubic polynomial $P(x) = x^3 + cx + d$. Then $P(x)$ has a multiple root if and only if $\Delta(P(x)) = 0$. In this case, furthermore, the curve $\bar{E}[\mathbb{C}]$ is rational because its function field $\mathbb{C}(x, y)$ is equal to the rational function field $\mathbb{C}(u)$, $u = y/(x - \alpha)$ where α is a multiple root. Hence we assume $\Delta(P(x)) = -(4c^3 + 27d^2) \neq 0$.

2.2. The j -Invariant. One of the most important invariants of the elliptic curve E is

$$j(E) := -\frac{1728(4c)^3}{16\Delta(P(x))} = \frac{108(4c)^3}{4c^3 + 27d^2}.$$

We also define the discriminant

$$\Delta(E) := 16\Delta(P(x)) = -16(4c^3 + 27d^2)$$

of E as an important quantity for the elliptic curve E .

Proposition 2.2.1. (i) *The projective curve defined by the short form*

$$E : y^2 = x^3 + cx + d, \quad (c, d \in \mathbb{C}),$$

is non-singular if and only if $\Delta(E) \neq 0$. In this case the curve is an elliptic curve.

(ii) *Let $E' : y^2 = x^3 + c'x + d'$ be another elliptic curve and let K be a common field of definition of E and E' . Then E and E' are isomorphic (over the algebraic closure of K) if and only if $j(E) = j(E')$.*

(iii) *For every $j_0 \in \mathbb{C}$ there is an elliptic curve defined over $\mathbb{Q}(j_0)$ with j -invariant equal to j_0 .*

For the proof see [Si-86, III, §1].

Remarks. (1) The curves $M(k) : y^2 = x^3 + k$ ($k \in \mathbb{C}, k \neq 0$) are nothing but those elliptic curves which have j -invariant equal to 0.

(2) Let $d = 0$. Then for $E : y^2 = x^3 + cx$ we have $j(E) = 1728$. Therefore E is isomorphic to $E_0 : y^2 = x^3 + x$ over $\mathbb{C}$.

(3) Suppose $cd \neq 0$ and put $t = c^3/d^2$. Then replacing x and y by dx/c and $\sqrt{(d/c)^3}y$, respectively, we have the equation

$$E(t) : y^2 = x^3 + tx + t.$$

Then

$$j(E(t)) = 1728 \cdot \frac{4t}{4t + 27} \quad \text{and} \quad 4t = \frac{27j(E(t))}{1728 - j(E(t))}.$$

This shows that we can find t , and hence an elliptic curve $E(t)$, with $j(E(t)) = j_0$ for a given j_0 .

2.3. The universal covering of $\bar{E}[\mathbb{C}]$. We show that the universal covering of $\bar{E}[\mathbb{C}]$ is the complex plane $\mathbb{C}$ by use of the Weierstrass $\wp$ -function. Then we also see that $\bar{E}[\mathbb{C}]$ is biholomorphic to a complex torus of the form $\mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, with $\omega_1, \omega_2 \in \mathbb{C}$, is a lattice in $\mathbb{C}$. (Our basic reference is [Si-86, VI].)

Let ω_1 and ω_2 be two complex numbers independent over the field $\mathbb{R}$ of real numbers. We may assume that the imaginary part of $\tau := \omega_1/\omega_2$ is positive by exchanging the indices if necessary. Then τ belongs to the upper half complex plane $\mathfrak{H}$. Conversely, every τ on $\mathfrak{H}$ corresponds to a lattice with $\omega_1 = \alpha\tau$ and $\omega_2 = \alpha$, with $\alpha \in \mathbb{C} - \mathbb{R}$.

For such a lattice Λ we define the Weierstrass $\wp$ -function by the series

$$\wp(z; \Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left\{ \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right\}.$$

This converges absolutely and uniformly on every compact subset of $\mathbb{C} - \Lambda$, and defines a meromorphic function on $\mathbb{C}$ with a double pole with residue 0 at each lattice point. It is clear that this is an even function: $\wp(-z; \Lambda) = \wp(z; \Lambda)$. Its derivative

$$\wp'(z; \Lambda) := -2 \sum_{\omega \in \Lambda} \frac{1}{(z - \omega)^3}$$

is also a meromorphic function on $\mathbb{C}$ with a triple pole with residue 0 at each lattice point. We have $\wp'(-z; \Lambda) = -\wp'(z; \Lambda)$.

We need some Eisenstein series associated to the lattice Λ , namely the series

$$G_{2k}(\Lambda) := \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^{2k}}$$

which converges absolutely for each natural number $k > 1$.

Theorem 2.3.1. (i) *Both $\wp(z; \Lambda)$ and $\wp'(z; \Lambda)$ are periodic with respect to the set Λ of the periods: for each $\omega \in \Lambda$,*

$$\wp(z + \omega; \Lambda) = \wp(z; \Lambda), \quad \wp'(z + \omega; \Lambda) = \wp'(z; \Lambda).$$

Moreover, every meromorphic function on $\mathbb{C}$, which is periodic for all elements of Λ , is a rational combination of $\wp(z; \Lambda)$ and $\wp'(z; \Lambda)$.

(ii) *The two functions $\wp(z; \Lambda)$ and $\wp'(z; \Lambda)$ satisfy the equation*

$$\wp'(z; \Lambda)^2 = 4\wp(z; \Lambda)^3 - 60G_4(\Lambda)\wp(z; \Lambda) - 140G_6(\Lambda).$$

We define a map Ψ from $\mathbb{C} - \Lambda$ to $\mathbb{P}^2(\mathbb{C})$ by

$$\Psi(z) = (\wp(z; \Lambda) : \frac{1}{2}\wp'(z; \Lambda) : 1), \quad z \in \mathbb{C} - \Lambda.$$

Then this can naturally be extended to a map

$$\Psi : \mathbb{C} \longrightarrow \mathbb{P}^2(\mathbb{C})$$

by setting

$$\Psi(z) = \left(\frac{2\wp(z; \Lambda)}{\wp'(z; \Lambda)} : 1 : \frac{2}{\wp'(z; \Lambda)} \right) = (0 : 1 : 0)$$

for $z = \omega \in \Lambda$. Put

$$g_2 = g_2(\Lambda) := 60G_4(\Lambda), \quad g_3 = g_3(\Lambda) := 140G_6(\Lambda), \quad c := -\frac{1}{4}g_2, \quad d := -\frac{1}{4}g_3.$$

Then it follows from Theorem 2.3.1(ii) that the image of Ψ is contained in the curve $\bar{E}[\mathbb{C}]$ for the equation

$$E : y^2 = P(x) := x^3 + cx + d.$$

Hence we have an injective map

$$\bar{\Psi} : \mathbb{C}/\Lambda \longrightarrow \bar{E}[\mathbb{C}]$$

from the complex torus $\mathbb{C}/\Lambda$ into $\bar{E}[\mathbb{C}]$. (Note that Ψ maps 0 to the point at infinity $P_\infty = (0 : 1 : 0)$ of $\bar{E}[\mathbb{C}]$.) This $\bar{\Psi}$ is actually an analytic isomorphism. Indeed, we have the following theorem (see [Si-94, I, §4]).

Theorem 2.3.2. (*Uniformization Theorem for elliptic curves over $\mathbb{C}$.*) Let c, d be a pair of complex numbers which satisfies $4c^3 + 27d^2 \neq 0$. Then there exists a unique lattice Λ on $\mathbb{C}$ for which we have

$$g_2(\Lambda) = 60G_4(\Lambda) = -4c, \quad g_3(\Lambda) = 140G_6(\Lambda) = -4d.$$

Moreover the map $\bar{\Psi} : \mathbb{C}/\Lambda \longrightarrow \bar{E}[\mathbb{C}]$ for

$$E : y^2 = x^3 + cx + d$$

is a complex analytic isomorphism.

Remark. It is easy to see that the j -invariant of the elliptic curve of Theorem 2.3.2 is a function of $\tau = \omega_1/\omega_2 \in \mathfrak{H}$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. This is the so-called *elliptic modular function*, and this is an automorphic function for the linear fractional action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$; that is

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau) \quad \text{for} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

This corresponds to a basis change of the lattice Λ by a matrix.

2.4. Complex multiplication. Let $f(z)$ be an elliptic function. This means that $f(z)$ is a meromorphic function on $\mathbb{C}$ with two independent periods. Suppose that $f(z)$ is not a constant function, and put

$$\Lambda(f) := \{\omega \mid \omega \in \mathbb{C}, f(z + \omega) = f(z)\}.$$

Then there exists a pair of elements $\omega_1, \omega_2 \in \Lambda(f)$ such that we have $\Lambda(f) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. It follows from Theorem 2.3.1(i) that $f(z)$ belongs to the function field

$$K_{\Lambda(f)} := \mathbb{C}(\wp(z; \Lambda(f)), \wp'(z; \Lambda(f))).$$

For $n \in \mathbb{Z}, n \neq 0$, put $g(z) := f(nz)$. Then $g(z)$ is also an elliptic function; it is clear that $\Lambda(g) = n^{-1} \cdot \Lambda(f)$. Since $\Lambda(g)$ contains $\Lambda(f)$ in this case, $K_{\Lambda(g)}$ is a subfield of $K_{\Lambda(f)}$. Therefore, $g(z)$ is expressed as a rational combination of $\wp(z; \Lambda(f))$ and $\wp'(z; \Lambda(f))$. The field $K_{\Lambda(f)}$ is a finite algebraic extension of the subfield $\mathbb{C}(f(z))$. Hence $f(z)$ and $g(z)$ have an algebraic relation.

In his celebrated paper [Ab-1827], N. Abel was much interested in the case where $f(z)$ and $g(z) := f(\mu z)$ have an algebraic relation for some complex number μ different

from a rational number. Suppose that this is the case. We say that $f(z)$ has complex multiplication by μ .

Let $P(X, Y)$ be a polynomial in two variables X and Y over $\mathbb{C}$, and assume $P(g(z), f(z)) = 0$ as a function of z . Then for each $\omega \in \Lambda(f)$, we have

$$P(g(z + \omega), f(z + \omega)) = P(g(z + \omega), f(z)) = 0.$$

Therefore, $g(z + \omega)$ is also a root of the polynomial $P(X, f(z))$ over $K_{\Lambda(f)}$. Since all meromorphic functions over $\mathbb{C}$ form a field, the polynomial $P(X, f(z))$ has only a finite number of roots in the field; actually, the number is less than or equal to the degree. Hence we easily see that the set

$$S := \{\omega \in \Lambda(f) \mid g(z + \omega) = g(z)\} = \Lambda(f) \cap \Lambda(g)$$

is a submodule of $\Lambda(f)$ of finite index. Hence the $\mathbb{Z}$ -rank of S is 2, and S is a submodule of $\Lambda(g) = \mu^{-1} \cdot \Lambda(f)$ of finite index. Then there is a natural number $N > 0$ such that we have $N\mu^{-1} \cdot \Lambda(f) \subset S \subset \Lambda(f)$. Put $\alpha := N\mu^{-1}$. Then $\alpha \cdot \Lambda(f) \subset \Lambda(f)$. This relation is expressed with the basis elements ω_1 and ω_2 of $\Lambda(f)$ as

$$\alpha \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix},$$

where $a, b, c, d \in \mathbb{Z}$ with $ad - bc \neq 0$. Therefore α is an eigenvalue of the 2×2 matrix with rational entries, and hence a quadratic irrational number. By dividing both sides of the equation by ω_2 , we see that each of α and τ , and hence $\mu = N\alpha^{-1}$, generates the same imaginary quadratic field. Since $\alpha \cdot \Lambda(f) \subset \Lambda(f)$, multiplication by α induces a holomorphic endomorphism φ_α of the complex torus $\mathbb{C}/\Lambda(f)$ to itself.

Proposition 2.4.1. (i) *An endomorphism of a complex torus $\mathbb{C}/\Lambda$ which maps 0 to itself is always given as φ_α for some $\alpha \in \mathbb{C}$ which satisfies the condition $\alpha \cdot \Lambda \subset \Lambda$.*

(ii) *A complex torus $\mathbb{C}/\Lambda$ admits complex multiplication if and only if the element $\tau = \omega_1/\omega_2 \in \mathfrak{H}$, for a basis ω_1 and ω_2 of the lattice Λ , generates an imaginary quadratic field.*

For a proof of Proposition 2.3.3(i), see [Si-86, VI, §4]. The proof of (ii) will easily follow from the above arguments.

Example. Let us consider the curve defined by

$$E : y^2 = x^3 + d, \quad d \in \mathbb{C}.$$

By Theorem 2.3.2 the curve is isomorphic to a complex torus $\mathbb{C}/\Lambda$ for some lattice Λ ; the origin 0 of the abelian group $\mathbb{C}/\Lambda$ is mapped to the point P_∞ at infinity. Put $\zeta := (-1 + \sqrt{-3})/2$ where $\zeta^3 = 1$. Then the automorphism φ defined by sending (x, y) to $(\zeta x, y)$ fixes P_∞ . Therefore this curve has complex multiplication by the elements of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$.

Conversely, suppose that the complex torus $T := \mathbb{C}/\Lambda$ has complex multiplication by ζ . Then we may assume that $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ for some $\tau \in \mathbb{Q}(\sqrt{-3})$ because we may replace T by the isomorphic torus obtained by multiplying by some ω_2^{-1} . As is well

known, the ring of integers $\mathfrak{O}$ of $\mathbb{Q}(\sqrt{-3})$ is equal to $\mathbb{Z}[\zeta]$. Therefore the $\mathbb{Z}$ -module Λ is an $\mathfrak{O}$ -module because $\zeta \cdot \Lambda \subset \Lambda$. Hence Λ is a (fractional) ideal of $\mathbb{Q}(\sqrt{-3})$. Since the class number of $\mathbb{Q}(\sqrt{-3})$ is equal to 1, this ideal is principal; that is, there is an element $\lambda \in \mathbb{Q}(\sqrt{-3})$ such that we have $\Lambda = \lambda \cdot \mathfrak{O}$. Then the isomorphism of the tori, obtained by multiplying by λ^{-1} , sends T to $\mathbb{C}/\mathfrak{O}$ for which we see $\tau = \zeta$. Hence we conclude that $j(\zeta) = 0$ (see [Si-94, Appendix A, §3]). By Theorem 2.3.1(ii), T is isomorphic to a curve defined by an equation of the form $E : y^2 = x^3 + d$ for some $d \in \mathbb{C}$.

3. Mordell curves and cubic fields.

3.1. Introduction. In this section we study those elliptic curves which are defined over the rational number field $\mathbb{Q}$ and whose rational points over $\mathbb{Q}$ are described by certain subsets of the associated cubic fields. The curve $E = E(P(u))$ we are interested in is defined by the equation

$$E : w^3 = P(u) := u^3 + au^2 + bu + c$$

where $P(u)$ is an irreducible cubic polynomial in u over $\mathbb{Q}$. Note that the left hand side of the equation is w^3 in this part. We show, however, that its short form is a Mordell curve we introduced in Section 1.2. One of the points at infinity is rational over $\mathbb{Q}$ (although the two others are not). Hence we have an elliptic curve defined over $\mathbb{Q}$. Let $E[\mathbb{Q}]$ denote the set of all rational points of E over $\mathbb{Q}$. For a more detailed treatment, we refer to [Mi-03-2].

Take a root ξ of $P(u)$ in the complex number field $\mathbb{C}$, and let $K = \mathbb{Q}(\xi)$ be the cubic field generated by ξ . Put

$$\mathcal{W}(\xi) = \{ \alpha = a\xi + b \mid a, b \in \mathbb{Q}, N_{K/\mathbb{Q}}(\alpha) = 1 \}.$$

Then there is a bijective map from $\mathcal{W}(\xi)$ onto $E[\mathbb{Q}]$ which maps $1 \in \mathcal{W}(\xi)$ to the point at infinity in $E[\mathbb{Q}]$. This fact will be proved in Proposition 3.2.2. Note that the subset of $K^\times$ is not well determined by the cubic field K itself but depends on ξ or, we may say, on the polynomial $P(u)$; indeed, the isomorphism between the cubic fields K and $\mathbb{Q}(\eta)$ bijectively maps $\mathcal{W}(\xi)$ to $\mathcal{W}(\eta)$ if we take another root η of $P(u)$. In this way, we can completely describe the set of all rational points of E over $\mathbb{Q}$ by the subset $\mathcal{W}(\xi)$ of the cubic field K .

It is clear that $\mathcal{W}(\xi) = \mathcal{W}(s\xi + t)$ for all $s, t \in \mathbb{Q}$, $s \neq 0$. Hence the affine transformation $u \mapsto s^{-1}u - s^{-1}t$, for $s, t \in \mathbb{Q}$, gives a bijective correspondence between the sets of rational points of the curves over $\mathbb{Q}$. Then in Section 3.3 we shall reduce via affine transformations the curve $E(P(u))$ to two typical elliptic curves $F_0(a)$ and $E_0(b)$ which are defined as

$$\begin{cases} F_0(a) & : w^3 = u^3 + a, \\ E_0(b) & : w^3 = R(b; u) := u^3 + bu + b, \end{cases}$$

and respectively parametrized by $a, b \in \mathbb{Q}^\times$. The first curve $F_0(a)$ is isomorphic to the well known pure cubic twist $X^3 + Y^3 + aZ^3 = 0$ of the cubic Fermat curve. Its short form is a Mordell curve $M_5(a)$ defined as

$$M_5(a) : y^2 = x^3 - 2^4 3^3 a^2$$

(see, for example, Cassels [Ca-50]). In Section 3.4, we will show in a standard manner that a short form of $E_0(b)$ is

$$M_7(B) : y^2 = x^3 - B^2(B + 3), \quad B = \frac{4b}{9}.$$

(We use the indices of the curves here in such a way that they are consistent with the ones in [Mi-03-1].)

3.2. Miscellaneous elements. Let $P(u) = eu^3 + au^2 + bu + c$ be an irreducible cubic polynomial in u over $\mathbb{Q}$, and let $E = E(P(u))$ be a curve defined by the equation

$$E(P(u)) : w^3 = P(u) = eu^3 + au^2 + bu + c.$$

Proposition 3.2.1. *One of the points of E at infinity is rational over $\mathbb{Q}$ if and only if the leading coefficient e of $P(u)$ is a cube in $\mathbb{Q}$ (other than 0). In this case, the two other points of E at infinity are not rational over $\mathbb{Q}$ but over $\mathbb{Q}(\sqrt{-3})$.*

As we stated it in the introduction, we suppose that one of the points of $E(P(u))$ at infinity is rational over $\mathbb{Q}$. Then by the last proposition we have $e = r^3$, $r \in \mathbb{Q}^\times$. Replacing the variable w in the defining equation of E by rw , we may hereafter assume $e = 1$.

Let ξ be a root of $P(u)$ in the complex number field $\mathbb{C}$, and let $K = \mathbb{Q}(\xi)$ be the cubic field generated by ξ . Furthermore, let $\mathcal{W}(\xi)$ be the subset of $K^\times$ defined in Section 3.1.

Proposition 3.2.2. *There exists a bijective map from $\mathcal{W}(\xi)$ onto $E[\mathbb{Q}]$ which maps $1 \in \mathcal{W}(\xi)$ to the point at infinity in $E[\mathbb{Q}]$.*

Proof. Let ξ, ξ' and ξ'' be the three roots of $P(u)$ in $\mathbb{C}$. Then we have

$$P(u) = (u - \xi)(u - \xi')(u - \xi'').$$

Hence for $r \in \mathbb{Q}$, we have $P(r) = N_{K/\mathbb{Q}}(r - \xi)$. For $\alpha = a\xi + b \in \mathcal{W}(\xi)$ with $a \neq 0$, put $u = -b/a$ and $w = -1/a$. Then we have $w^3 = P(u)$ because $N_{K/\mathbb{Q}}(\alpha) = 1$; that is, we have a point $(u, w) = (-b/a, -1/a)$ of $E[\mathbb{Q}]$. For $\alpha = b \in \mathbb{Q}$,

$$N_{K/\mathbb{Q}}(\alpha) = b^3 = 1 \text{ if and only if } \alpha = 1.$$

Define a map $\rho : \mathcal{W}(\xi) \rightarrow E[\mathbb{Q}]$ by $\rho(\alpha) := (-b/a, -1/a)$ for $\alpha = a\xi + b \in \mathbb{Q}$ with $a \neq 0$ and put $\rho(1) :=$ the point at infinity in $E[\mathbb{Q}]$. It is clear that ρ is well defined and injective. There is only one point at infinity in $E[\mathbb{Q}]$. Let $(u, w) = (r, s)$, with $r, s \in \mathbb{Q}$, be a point of $E[\mathbb{Q}]$. Then we have $s^3 = P(r)$ and hence $s \neq 0$ because $P(u)$ is irreducible over $\mathbb{Q}$. Therefore $(r, s) = \rho(\alpha)$ with $\alpha = (-1/s)\xi + r/s \in \mathcal{W}(\xi)$. The proof is completed.

Lemma 3.2.3. *For all $s, t \in \mathbb{Q}$ with $s \neq 0$, $\mathcal{W}(\xi) = \mathcal{W}(s\xi + t)$.*

3.3. The curves $F_0(a)$ and $E_0(b)$. Let us see how our curve $E(P(u))$ for the cubic polynomial $P(u) = u^3 + au^2 + bu + c$ can be isomorphically reduced to either $F_0(a)$ or $E_0(b)$ as defined in Section 3.1 without changing the set $\mathcal{W}(\xi)$. First put $x = u + a/3$. Then we have $P(u) = x^3 + b'x + c'$ with

$$b' = -a^2/3 + b \quad \text{and} \quad c' = 2a^3/27 - ab/3 + c.$$

Since $P(u)$ is irreducible over $\mathbb{Q}$, c' is not equal to 0. If $b' = 0$, then we have the curve

$$F_0(a) : w^3 = u^3 + a;$$

here we replaced x and c' by the letters u and a , respectively, for simplicity.

Suppose now $b' \neq 0$. Put $y = \frac{b'}{c'} \cdot x$. Then we see

$$\left(\frac{b'}{c'}\right)^3 \cdot P(u) = y^3 + \frac{b'^3}{c'^2} \cdot y + \frac{b'^3}{c'^2}.$$

We have therefore the curve

$$E_0(b) : w^3 = R(b; u) = u^3 + bu + b;$$

here, for simplicity, we replaced $\frac{b'}{c'} \cdot w$, y and $\frac{b'^3}{c'^2}$ by the letters w , u and b , respectively. We easily see by Lemma 3.2.3 that the original $\mathcal{W}(\xi)$ coincides with either $\mathcal{W}(\sqrt[3]{a})$ for $F_0(a)$ or $\mathcal{W}(\eta)$ for $E_0(b)$ where η is a root of $R(b; u)$.

Proposition 3.3.1. *The elliptic curve $E(P(u))$ is isomorphic over $\mathbb{Q}$ to either $F_0(a)$ or $E_0(b)$ for some a or b in $\mathbb{Q}$ with the same subset $\mathcal{W}(\xi)$ of the cubic field $\mathbb{Q}(\xi)$.*

Remark. In our previous work [Mi-03-1], we studied the family of elliptic curves

$$E_1(c) : w^3 = P(c; u) := u^3 + u^2 + c$$

where $P(c; u)$ is an irreducible cubic polynomial in $\mathbb{Q}[u]$. This polynomial is related to $R(b; u) := u^3 + bu + b$ as follows: as before let ξ be a fixed root of $R(b; u)$. Then ξ^{-1} is a root of $P(c; u)$ with $c = b^{-1}$. This relation may give us a morphism between the two algebraic curves $E_0(b)$ and $E_1(c)$. If we try to pick up such one, however, it may not be defined over $\mathbb{Q}$ as we don't see a natural correspondence between $\mathcal{W}(\xi)$ and $\mathcal{W}(\xi^{-1})$. Hence we should initiate the reduction process of this section if we want a homomorphism of elliptic curves defined over $\mathbb{Q}$.

3.4. The short form of $E_0(b)$. In this final section, we prove our main result on $E_0(b)$. The author is indebted to M. Imaoka for a portion of the calculation.

Theorem 3.4.1. (i) *For $b \in \mathbb{Q} - \{0, -27/4\}$, the short form of $E_0(b)$ is $M_7(B)$, $B = 4b/9 \in \mathbb{Q} - \{0, -3\}$ and is defined by the equation*

$$M_7(B) : y^2 = x^3 - B^2(B + 3) \quad \text{for } B = \frac{4b}{9} \in \mathbb{Q} - \{0, -3\}.$$

(ii) *$M_7(B)$ has a rational point*

$$(x_0, y_0) = (B + 4, 3B + 8).$$

This is not a torsion point unless either $B = -4$ or $B = -8/3$, and hence its Mordell-Weil rank is greater than or equal to 1 if $B \neq -4, -8/3$.

(iii) The exceptional curves

$$M_7(-4) : y^2 = x^3 + 16 \quad \text{and} \quad M_7(-8/3) : y^2 = x^3 - (4/3)^3$$

have Mordell-Weil rank = 0. Its torsion group is of order 3 and 2, respectively, and is generated by the point $(x_0, y_0) = (0, -4)$ and $(x_0, y_0) = (4/3, 0)$, respectively.

Proof. (i) Put $W = w + u$. Then we obtain

$$3Wu^2 + (3W^2 - b)u = -W^3 + b$$

from the equation $w^3 = u^2 + bu + b$. To make a perfect square out of the left-hand side, multiply both sides by $12W$, and get

$$(6Wu + 3W^2 - b)^2 = -3W^4 - 6bW^2 + 12bW + b^2.$$

The constant term of the right-hand side is a square. Hence by multiplying both sides by b^2/W^4 , we obtain

$$\begin{aligned} Y^2 &= (X - 3)^4 + 12(X - 3)^3 - 6b(X - 3)^2 - 3b^2 \\ &= X^4 - 6(b + 9)X^2 + 36(b + 6)X - 3(b + 9)^2 \end{aligned}$$

if we put

$$Y = \frac{b(6Wu + 3W^2 - b)}{W^2} = -\frac{b^2}{W^2} + \frac{6bu}{W} + 3b \quad \text{and} \quad X = \frac{b}{W} + 3.$$

Then we utilize the method of Mordell [Mo-69, Ch.10, Th.2]. If we put $\alpha = b + 9$, $\beta = 9(b + 6)$, and $\gamma = -3(b + 9)$, then we have $3\alpha^2 + \gamma = 0$ and $-\alpha\gamma - \beta^2 + \alpha^3 = b^2(4b + 27)$. Therefore we easily obtain

$$y^2 = x^3 - (4b)^2(4b + 27)$$

if we put

$$x = 2X^2 + 2Y - 2\alpha \quad \text{and} \quad y = 4X(X^2 + Y - 3\alpha) + 4\gamma.$$

If we divide both sides of the equation by 27^2 , then we have

$$\left(\frac{y}{27}\right)^2 = \left(\frac{x}{9}\right)^3 - \left(\frac{4b}{9}\right)^2 \cdot \left(\frac{4b}{9} + 3\right).$$

Hence we obtain part (i) of the theorem by replacing $x/9$ and $y/27$ by x and y , respectively.

(ii) The former half is confirmed by a direct calculation. For the latter half, put $P = (x_0, y_0)$ for simplicity and suppose that it is of finite order. We know by Fueter [Fu-30] (also see [GPZ-98, Proposition 1]) that the torsion part of the rational points of

a Mordell curve is cyclic and of order 1, 2, 3 or 6; furthermore, a rational point on it is of order 2 or 3 if and only if its y -coordinate is equal to 0 or its x -coordinate is equal to 0, respectively. We see immediately that $y_0 = 0$ if and only if $B = -8/3$; in this case, we have $M(-8/3) : y^2 = x^3 - (4/3)^3$ and the point P is of order 2. It is also clear that $x_0 = 0$ if and only if $B = -4$; in this case, we have $M(-4) : y^2 = x^3 + 16$ and the order of P is 3.

Let us now check if P might be of order 6. Suppose that $x_0 \neq 0$ and $y_0 \neq 0$. The x -coordinate $x(2P)$ of $2P = P + P$ on $M_7(B)$ is given by

$$x(2P) = \frac{x_0(x_0^3 - 8 \cdot B^2(B+3))}{4 \cdot y_0^2};$$

see, for example, Silverman and Tate [ST-92]. We know that $x_0 \neq 0$. Hence

$$\begin{aligned} x(2P) = 0 &\iff x_0^3 - 8 \cdot B^2(B+3) = -7B^3 - 12B^2 + 48B + 64 = 0 \\ &\iff (7B)^3 + 12(7B)^2 - 48 \cdot 7 \cdot (7B) - 64 \cdot 7^2 = 0. \end{aligned}$$

Since the algebraic integer $7B$ is contained in $\mathbb{Q}$, it is a rational integer which divides the constant term $-64 \cdot 7^2$. Such a divisor is, however, unable to make the cubic polynomial equal to 0 as is easily checked. Therefore we conclude that the point P is not of order 6. This completes the proof of (ii).

(iii) It is sufficient to show that the Mordell-Weil ranks of the curves

$$M(-8/3) : y^2 = x^3 - (4/3)^3 \quad \text{and} \quad M(-4) : y^2 = x^3 + 16$$

are equal to 0. The latter curve is in Table 1 of Cassels [Ca-50]; as to the former, it is isomorphic to $y^2 = x^3 - 3^3 \cdot 2^6$ which is also in the table.

The theorem is now completely proved.

Acknowledgment. The author was partly supported by the Grant-in-Aid for Scientific Research (C) (2) No. 14540037, Japan Society for the Promotion of Science, while he prepared this article.

Résumé substantiel en français. Cet article se veut une courte introduction à la géométrie diophantienne des courbes de Mordell de la forme

$$M : y^2 = x^3 - B^2(B+3), \quad B = \frac{4b}{9} \text{ avec } b \in \mathbb{Q}.$$

Ce sont probablement les courbes les plus standard parmi les courbes de Mordell récemment étudiées en relation avec les corps cubiques. L'ensemble $M[\mathbb{Q}]$ des points rationnels de M sur $\mathbb{Q}$ (incluant le point à l'infini) est décrit au moyen d'un sous-ensemble du corps cubique défini par le polynôme $X^3 + bX + b$. Il s'avère qu'il y a une bijection naturelle entre $M[\mathbb{Q}]$ et

$$\mathcal{W}(\xi) = \{\alpha = a\xi + b \mid N_{K/\mathbb{Q}}(\alpha) = 1, a, b \in \mathbb{Q}\}$$

où ξ est une racine complexe de $X^3 + bX + b$ qui engendre $K = \mathbb{Q}(\xi)$.

Nous donnons dans l'introduction une courte description de la conjecture de Birch et Swinnerton-Dyer, mettant en valeur l'importance de la géométrie diophantienne des courbes elliptiques, et faisons un survol historique des courbes de Mordell $y^2 = x^3 + k$, $k \in \mathbb{Q}$. L'invariant j de ces courbes est égal à 0, de sorte que ces courbes sont isomorphes sur le corps $\mathbb{C}$ des complexes à la courbe $y^2 = x^3 + 1$. Elles sont à multiplication complexe via une racine troisième de l'unité du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-3})$. Ces propriétés sont typiques des courbes de Mordell parmi les courbes elliptiques définies sur $\mathbb{Q}$ sous la forme de Weierstrass, ce qui explique que la géométrie des courbes elliptiques sur $\mathbb{C}$ et leur géométrie diophantienne sur $\mathbb{Q}$ sont tout à fait différentes.

Au chapitre 2, nous passons en revue ce qui a trait à la géométrie des courbes elliptiques sur $\mathbb{C}$. À la Section 2.4, on rencontrera l'aspect arithmétique de ces courbes elliptiques à multiplication complexe. Vraiment, ceci fut à l'origine de l'importance de la théorie algébrique des nombres au 19^e siècle, et au cours des vingt premières années du 20^e siècle alors que Takagi a finalement réussi à établir la théorie du corps de classes. Le chapitre 3 est explicitement consacré à un court survol de la géométrie diophantienne des courbes de Mordell.

REFERENCES

- [Ab-1827] N. H. Abel, *Recherches sur les fonctions elliptiques*, J. Reine Angew. Math. Bd. 2 (1827), 101–181; Bd. 3 (1828), 160–190; *Œuvres complètes I*, 263–388.
- [BS-63] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on Elliptic Curves I*, J. Reine Angew. Math. **212** (1963), 7–25.
- [BS-65] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on Elliptic Curves II*, J. Reine Angew. Math. **218** (1965), 79–108.
- [BCDT-01] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001); no. 4, 843–939 (electronic).
- [Ca-50] J. W. S. Cassels, *The rational solutions of the Diophantine equation $y^2 = x^3 - D$* , Acta Math. **82** (1950), 243–273.
- [Co-89] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*, John Wiley & Sons, Inc., New York, 1989.
- [Fa-83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
- [Fa-84] G. Faltings, *Erratum: “Finiteness theorems for abelian varieties over number fields”*, Invent. Math. **75** (1984), 381.
- [Fu-30] R. Fueter, *Über kubische diophantische Gleichungen*, Comment. Math. Helv. **2** (1930), 69–89.
- [GPZ-98] J. Gebel, A. Pethő and H. G. Zimmer, *On Mordell's Equation*, Compositio Math. **110** (1998), 335–367.
- [Me-92] J.-F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), 919–922.
- [Me-95] J.-F. Mestre, *Rang de courbes elliptiques d'invariant nul*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), 1235–1236.
- [Mi-03-1] K. Miyake, *Some families of Mordell curves associated to cubic fields*, J. Comput. Appl. Math. **160** (2003), 217–231.
- [Mi-03-2] K. Miyake, *Cubic fields and Mordell curves*, Tokyo Metropolitan Univ. Math. Preprint Series **15** (Sept. 2003).

- [Mo-14] L. J. Mordell, *The Diophantine equation $y^2 - k = x^3$* , Proc. London Math. Soc. **13** (1914), 60–80.
- [Mo-69] L. J. Mordell, *Diophantine equations*, Pure and Applied Mathematics, vol. 30, Academic Press, London-New York, 1969.
- [Na-24] T. Nagell, *Über die rationalen Punkte auf einigen kubischen Kurven*, Tôhoku Math. J. **24** (1924), 48–53.
- [Se-51] E. S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$* , Acta Math. **85** (1951), 203–362.
- [Se-54] E. S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. Completion of the tables*, Acta Math. **92** (1954), 191–197.
- [Si-86] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
- [Si-94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
- [ST-92] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1992.
- [Wi-95] A. Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), 443–551.

K. MIYAKE

DEPARTMENT OF MATHEMATICAL SCIENCE

WASEDA UNIVERSITY

OHKUBO 3-4-1, SHINJUKU-KU

TOKYO, 169-8555

JAPAN

E-MAIL: miyakek@aoni.waseda.jp