Quadratic Forms and Elliptic Curves. II

By Takashi ONO

Department of Mathematics, The Johns Hopkins University, U.S.A.

(Communicated by Shokichi IYANAGA., M. J. A., Oct. 14, 1996)

This is a continuation of my preceding paper [2] which will be referred to as (I) in this paper. In (I), to each quadratic space (V, q) over any field k of characteristic $\neq 2$ and a pair $w = (u, v)$ of independent and nonisotropic vectors in V, we associated an elliptic curve E_w over k:

(0.1) $$E_w : Y^2 = X^3 + A_w X^2 + B_w X.,^{1)} \quad A_w, B_w \in k.$$

In this paper, we shall consider the converse problem. Thus, let E be an elliptic curve over k:

(0.2) $$E : Y^2 = X^3 + AX^2 + BX, \quad A, B \in k, B(A^2 - 4B) \neq 0.$$

We shall show that there is a quadratic space (V, q) over k and a pair $w = (u, v)$ as above so that

(0.3) $E = E_w$. (Main Theorem).

(In fact, we can choose $V = k^3$ and $q(x) = x_1^2 + x_2^2 - x_3^2$). Since E_w is provided with a point $P_w = (x_w, y_w)$,[2] so is E, i.e., we can write down a point on $E(\bar{k})$ explicitly. When k is a number field, we can find easily a point of infinite order in $E(k)$ under simple conditions on A, B. On the other hand, statement like (0.3) may be viewed as an analogue (over any field k of characteristic $\neq 2$) of "Uniformization theorem of elliptic curves over $\boldsymbol{C}$".

§1. Field of characteristic $\neq 2$. Let (V, q) be a quadratic space over a field of characteristic $\neq 2$. Consider a subset W of $V \times V$ given by

(1.1) $W = \{(u, v) \in V \times V\,; u, v$ are independent and nonisotropic$\}$.

To each $w \in W$, we associate an elliptic curve E_w:

(1.2) $$E_w : Y^2 = X^3 + A_w X^2 + B_w X$$

with

(1.3) $$A_w = \langle u, v\rangle = \frac{1}{2}(q(u + v) - q(u) - q(v)),$$
$$B_w = (\langle u, v\rangle^2 - q(u)q(v))/4.$$

Conversely, let E be an elliptic curve over k of the form:

(1.4) $$E : Y^2 = X^3 + AX^2 + BX \quad A, B \in k, \quad B(A^2 - 4B) \neq 0.$$

(1.5) **Main theorem.** *Let k be a field, $ch(k) \neq 2$, and q be a ternary quadratic form on the vector space $V = k^3$ given by $q(x) = x_1^2 + x_2^2 - x_3^2$, $x = (x_1, x_2, x_3)$. Let $e = (1,0,0)$ and $H = \{h = (0, h_2, h_3)\,; h_2, h_3 \in k\}$.*[3] *For any elliptic curve E of the form* (1.4), *let h be a vector in H such that $q_H(h) = -4B$.*[4] *Then the pair $w = (e, Ae + h)$ belongs to W in* (1.1) *and we have $E = E_w$,* ((1.2), (1.3)).

Proof. Put $w = (u, v)$ with $u = e$, $v = Ae + h$, where $h \in H$ is a vector such that $q_H(h) = -4B$. Since $(V, q) = ke \oplus (H, q_H)$, an orthogonal direct sum with $q(e) = 1$, we have $A_w = \langle u, v\rangle = \langle e, Ae + h\rangle = A$ and $B_w = (\langle u, v\rangle^2 - q(u)q(v))/4 = (A^2 - q(e)q(Ae + h))/4 = (A^2 - (A^2 - 4B))/4 = B$. Since A, B are coefficients of E, we have $0 \neq B(A^2 - 4B) = B_w(A_w^2 - 4B_w)$ and hence $w = (u, v) \in W$. Q.E.D.

(1.6) **Corollary.** *Let E be an elliptic curve of the form* (1.4) *over k. Then $E(\bar{k})$ contains a point $P = (x, y)$ with*
$$x = ((A - 1)^2 - 4B)/4, y = x^{\frac{1}{2}}(A^2 - 4B - 1)/4.$$

Proof. Using notation in the proof of (1.5), we find $q(e - v) = q(e) + q(v) - 2\langle e, v\rangle = 1 + A^2 - 4B - 2A$ and $q(v) - q(e) = A^2 - 4B - 1$. Our assertion follows from (1.5) and (1.7) of (I). Q.E.D.

§2. Number fields. Let k be a number field of finite degree over $\boldsymbol{Q}$ and $\mathfrak{o}$ be the ring of integers of k. For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, we denote by $\nu_{\mathfrak{p}}$ the order function on k at $\mathfrak{p}$. An element $a \in o$ is said to be *even* if $\nu_{\mathfrak{p}}(a) > 0$ for some $\mathfrak{p}$ which lies above 2. The next theorem provides us with a family of elliptic curves over k such

1) In this paper we shall write A_w, B_w instead of P_w, Q_w in (I).We shalll also use $\langle u, v\rangle$ for inner product instead of $B(u, v)$.

2) We wrote $P_0 = (x_0, y_0)$ in (I) for $P_w = (x_w, y_w)$.

3) By abuse of notation we shall identify H with the hyperbolic plane k^2 with the metric form $q_H(h) = h_2^2 - h_3^2$, $h = (h_2, h_3) \in k^2$.

4) Since q_H is isotropic, it can represent any element of k.