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)]
$A_w, B_w \in k.$

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

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

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

(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.

that rank $E(k)$ is positive for each member $\boldsymbol{E}$ of it.

(2.1) **Theorem.** *Let $E: Y^2 = X^3 + AX^2 + BX$ be an elliptic curve such that A, B belong to $\mathfrak{o}$. If* (i) *A is even and* (ii) *there is an integer $C \in \mathfrak{o}$ such that $(A-1)^2 - 4B = C^2$, then $P_0 = (x_0, y_0)$, with $x_0 = (C/2)^2$, $y_0 = (C/2)(C^2 + 2(A-1))/4$, is a point of infinite order in $E(k)$.*

Proof. First of all, P_0 belongs to $E(k)$ by (ii) and (1.6). Next, assume, on the contrary, that P_0 is of order $m \geq 2$. If $m = 2$, then P_0 is a 2-torsion point; so $y_0 = 0$. By (i), let $\mathfrak{p}$ be a prime over 2 such that $\nu_{\mathfrak{p}}(A) > 0$. Then, by (ii), we have $\nu_{\mathfrak{p}}(C) = 0$; in particular, $C \neq 0$. Hence the relation $0 = y_0 = (C/2)(C^2 + 2(A-1))/4$ implies that $C^2 = 2(A-1)$, contradicting $\nu_{\mathfrak{p}}(C) = 0$. Thus we may assume that $m > 2$. From this point on, we need a generalization of the Nagell-Lutz theorem ([3] p. 220, Theorem 7.1).[5] This theorem, when applied to our $P_0 = (x_0, y_0)$, says:

(a) *If m is not a prime power, then $x_0, y_0 \in \mathfrak{o}$.*

(b) *If $m = l^n$ is a prime power, for each prime ideal $\mathfrak{q}$ of $\mathfrak{o}$ let*

$r_{\mathfrak{q}} = [\nu_{\mathfrak{q}}(l)/(l^n - l^{n-1})]$ ([ ] = *the integral part*).

Then $\nu_{\mathfrak{q}}(x_0) \geq -2r_{\mathfrak{q}}$ and $\nu_{\mathfrak{q}}(y_0) \geq -3r_{\mathfrak{q}}$. In particular, x_0 and y_0 are $\mathfrak{q}$-integral if $\nu_{\mathfrak{q}}(l) = 0$.

Now, as we saw $\nu_{\mathfrak{p}}(C) = 0$ for a $\mathfrak{p}$ above 2, we have $\nu_{\mathfrak{p}}(x_0) = -2\nu_{\mathfrak{p}}(2) < 0$; hence $x_0 \notin \mathfrak{o}$, showing that the case (a) does not occur. Next, for the case (b), assume first that $l \neq 2$. Then for that prime $\mathfrak{p}$ over 2 we have $\nu_{\mathfrak{p}}(l) = 0$ and so, by the last italicized sentence in (b), $0 \leq \nu_{\mathfrak{p}}(x_0) = -2\nu_{\mathfrak{p}}(2) < 0$, and the case $l \neq 2$ does not occur also. Finally, it remains the case $m = 2^n$, $n \geq 2$. Again for that $\mathfrak{p}$, put $e = \nu_{\mathfrak{p}}(2)$. If we write $e = s2^{n-1} + r$, with $0 \leq r \leq 2^{n-1}$, we have $r_{\mathfrak{p}} = s$. Hence (b) implies that $-2s \leq \nu_{\mathfrak{p}}(x_0) = 2\nu_{\mathfrak{p}}(C) - 2\nu_{\mathfrak{p}}(2) = -2\nu_{\mathfrak{p}}(2) = -2e$; so $s \geq e \geq s2^{n-1}$, which is impossible because $n \geq 2$. Q.E.D.

§3. Algebraically closed fields. Assume that our basic field k is algebraically closed of characteristic $\neq 2$. Let q be the ternary quadratic form on $v = k^3$ defined by $q(x) = x_1^2 + x_2^2 - x_3^2$. We have defined a set W in $V \times V$, (1.1). Now call $\boldsymbol{E}$ the totality of elliptic curves E over k of the form (1.4). Then, by (1.2), (1.3), we have a map $\pi: W \rightarrow \boldsymbol{E}$ given by

(3.1) $\pi(w) = E_w: Y^2 = X^3 + A_w X^2 + B_w X$.

We know that π is surjective by (1.5). On the other hand, to describe fibres of π, it is convenient to limit ourselves to the case where k is algebraically closed. Denote by $O(q)$ the orthogonal group of q. We need also the following group:

(3.2) $$G(q) = k^\times \times O(q).$$

This group $G(q)$ acts on W by the rule:

(3.3) $$(a, s)w = (asu, a^{-1}sv),$$
$$a \in k^\times,\ s \in O(q),\ w = (u, v) \in W.$$

One checks easily that

(3.4) $$\pi(gw) = \pi(w), \quad g \in G(q).$$

Passing to the quotient, the map $\pi: w \rightarrow \boldsymbol{E}$ induces a map

(3.5) $$\tilde{\pi}: \tilde{W} = G(q)\backslash W \rightarrow \boldsymbol{E}$$

which is surjective.

(3.6) **Theorem.** *The map $\tilde{\pi}$ is a bijection: $\tilde{W} = G(q)\backslash w \xrightarrow{\sim} \boldsymbol{E}$.*

Proof. We have only to check that $\tilde{\pi}$ is injective. So take two points $w, w' \in W$ such that $E_w = E_{w'}$, i.e., $A_w = A_{w'}$ and $B_w = B_{w'}$. In other words, consider $w = (u, v)$, $w' = (u', v') \in W$ such that

(3.7) $$\langle u, v\rangle = \langle u', v'\rangle \text{ and}$$
$$\langle u, v\rangle^2 - q(u)q(v) = \langle u', v'\rangle^2 - q(u')q(v'),$$

or

(3.8) $\langle u, v\rangle = \langle u', v'\rangle$ and $q(u)q(v) = q(u')q(v')$.

Since k is algebraically closed and $q(u)q(v) \neq 0$, there is an $a \in k^\times$ so that $q(au) = q(u')$; hence $q(av') = q(v)$ by (3.8). Therefore, (3.8) amounts to the condition:

(3.9) $$\langle au, v\rangle = \langle u', av'\rangle,\ q(au) = q(u') \text{ and } q(v) = q(av').$$

Our assertion then follows from (3.9), the independence of u, v and the SAS-theorem on triangles in the metric space (V, q).[6] Q.E.D.

(3.10) **Corollary.** *Let k be an algebraically closed field of characteristic $\neq 2$ and let E be an elliptic curve $Y^2 = X^3 + AX^2 + BX$ over k, $B(A^2 - 4B) \neq 0$.. Then, for any $a \in k^\times$, the point $P_a = (x_a, y_a)$ belongs to $E(k)$, where*

$$\begin{cases} x_a = (a^2 + a^{-2}(A^2 - 4B) - 2A)/4, \\ y_a = x_a^{\frac{1}{2}}(a^2 - a^{-2}(A^2 - 4B))/4. \end{cases}$$

Proof. We know that $w = (e, Ae + h)$, with

5) This portion of the proof is the same as in the proof of (2.3) in [1]. In view of the change of situation, however, we find it convenient to repeat it.

6) Namely, take an $s \in GL(V)$ so that $sau = u'$, $sv = sv'$. Then (3.9) implies $s \in O(q)$.

$q_H(h) = -4B$, is a point in W such that $\pi(w) = E$, ((1.5)). By (3.6), any other point w' such that $\pi(w') = E$ is of the form $w' = gw$, with $g = (a, s) \in G(q)$. Our assertion follows if one computes the coordinates x_0, y_0 of the point P_0 in $E_{w'} = E$ by making use of the explicit formula in (1.7) of (I). Q.E.D.

(3.11) **Remark.** Needless to say, one verifies (3.10) derectly. Be that as it may, it is nice to have found a (double valued) map $a \mapsto P_a = (x_a, y_a)$ form $k^\times$ to E in (3.10), (end of remark).

Since k is algebraically closed, one should classify $\boldsymbol{E}$ according to isomorphisms over k. If $E, E' \in \boldsymbol{E}$ are given by Weierstrass form of type (1.4) with coefficients (A, B), (A', B'), respectively, then, as is well-known, we have

(3.12) $E \simeq E' \Leftrightarrow$

$$\begin{cases} u^2A' = A + 3r, \\ u^4B' = B + 2Ar + 3r^2, \\ 0 = r(B + Ar + r^2),\ u(\neq 0),\ r \in k, \end{cases}$$
$$\Leftrightarrow j(E) = j(E'),$$

where

(3.13) $j(E) = 2^8(A^2 - 3B)^3/(B^2(A^2 - 4B))$.

In view of (3.6), we can view j as a function of $w = (u, v) \in W$:

(3.14) $$j(\pi(w)) = 2^6(\langle u, v\rangle^2 + 3q(u)q(v))^3 /(q(u)q(v)(\langle u, v\rangle^2 - q(u)q(v))^2).$$

In particular,

(3.15) $$j(\pi(w)) = 2^6 3^3 \Leftrightarrow \langle u, v\rangle = 0 \text{ or } \pm 3(q(u)q(v))^{\frac{1}{2}}.$$

§4. Real number field. Taking $V = \boldsymbol{R}^2$, consider the standard quadratic form $q(x) = x_1^2 + x_2^2$, $x = (x_1, x_2)$. Hence the metric space (V, q) is the space of plane Euclidean geometry. Here, the set W is nothing but the set of pairs $w = (u, v)$ of independent vectors; namely triangles (a, b, c) such that $a^2 = q(u)$, $b^2 = q(v)$ and $c^2 = q(u - v) = q(u) + q(v) - 2\langle u, v\rangle$, (the law of cosine). We have

(4.1) $$\begin{cases} A_w = \langle u, v\rangle = \dfrac{1}{2}(a^2 + b^2 - c^2) \\ B_w = (\langle u, v\rangle^2 - q(u)q(v))/4 = \\ \qquad -s(s-a)(s-b)(s-c). \end{cases}$$

The elliptic curve E_w is the one introduced in [1] in connection with the antique congruent number problem. Needless to say, if we pursue an analogous theme for (V, q) with $V = \boldsymbol{R}^3$, $q(x) = x_1^2 + x_2^2 + x_3^2$ (resp. $q(x) = x_1^2 + x_2^2 - x_3^2$), then we will be led to triangles on the sphere $q(x) = 1$ (resp. on the upper half of the hyperboloid of two sheets $q(x) = -1$). We hope to come back sometime to the study of such a relationship between non-Euclidean geometry and elliptic curves.

References

[1] T. Ono: Triangles and elliptic curves. Proc. Japan Acad., **70A**, 106–108 (1994).

[2] T. Ono: Quadratic forms and elliptic curves. Proc. Japan Acad., **72A**, 156–158 (1996).

[3] J. H. Silverman: The Arithmetic of Elliptic Curves. Springer, New York (1986).