Quadratic Forms and Elliptic Curves

By Takashi ONO

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

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1996)

Introduction. When an elliptic curve E over $\boldsymbol{Q}$ is given by a Weierstrass model like $Y^2 = X^3 + aX^2 + bX + c$, it is difficult to produce points of $E(\boldsymbol{Q})$ with certainty except some torsion points. To make such a plan work well, we might restrict ourselves to certain family of elliptic curves where the coefficients a, b, c are determined by a rule. Suggested by the antique congruent number problem for right triangles ([7], see also [1]), we obtained, using arbitrary triangles, a family of infinitely many elliptic curves each of which is provided with a 'canonical' nontorsion point $P_0 = (x_0, y_0)$ ([4], see also [2]).

In this paper, we shall pursue the same theme in a mere general setting whereby replacing triangles by quadratic forms. As is stated in the main theorem (1. 7), the canonical point P_0 might possibly belong to a quadratic extension of $\boldsymbol{Q}$, and so we needed to call up the Hopf maps to handle the matter.[1)]

§1. The set $\boldsymbol{W}$. Let k be a field of characteristic $\neq 2$, V a vector space of finite dimension over k, q a nondegenerate quadratic form on V and B a symmetric bilinear form corresponding to q. Hence we have the relations

(1.1) $$B(u, v) = \frac{1}{2}(q(u+v) - q(u) - q(v)),$$
$$q(u) = B(u, u),\ u, v \in V.$$

To each pair $w = (u, v) \in V \times V$, we set

(1.2) $$P_w = B(u, v),\ Q_w = \frac{1}{4}(B^2(u, v) - q(u)q(v)) = -\frac{1}{4}\begin{vmatrix} B(u, u) & B(u, v) \\ B(v, u) & B(v, v) \end{vmatrix}.$$

Note that

(1.3) $$P_w^2 - 4Q_w = q(u)q(v).$$

Consider a plane cubic given by

(1.4) $$E_w : y^2 = x^3 + P_w x^2 + Q_w x.$$

The discriminant of (1.4) is $\Delta = 16Q_w^2(P_w^2 - 4Q_w)$. Hence,

E_w is elliptic $\Leftrightarrow \Delta \neq 0$
$\Leftrightarrow (B^2(u, v) - q(u)q(v))q(u)q(v)) \neq 0.$

In view of the last equality in (1.2), we have

(1.5) E_w is elliptic $\Leftrightarrow U, V$ are independent and nonisotropic.

Let us introduce the set

(1.6) $W = \{w = (u, v) \in V \times V,\ E_w \text{ is elliptic}\}.$

(1.7) **Theorem.** *For $w = (u, v) \in W$, put*
$x_0 = q(u - v)/4,\ y_0 = q^{1/2}(u - v)(q(v) - q(u))/8.$[2)]
Then $P_0 = (x_0, y_0)$ belongs to $E_w(k(q^{1/2}(u - v)))$.

Proof. Straightforward calculation using (1.1), (1.2), (1.3).

(1.8) **Remark.** If we want the point P_0 in $E(k)$, we need $w = (u, v) \in W$ such that $q(u - v)$ is a square. This calls upon us to use a Hopf map.

§2. Hopf map $\boldsymbol{h}$. Notation being the same as in §1, we assume further that V has a vector ε such that $q(\varepsilon) = 1$. We shall fix this vector once for all and put $U = (k\varepsilon)^{\perp}$, the orthogonal complement of the line $k\varepsilon$. For a vector $v = a\varepsilon + u$, $a \in k$, $u \in U$, we have

(2.1) $$q(v) = a^2 + q_U(u)$$

where q_U denotes the restriction of q on U. Next, let $Z = X \oplus Y$ be an orthogonal direct sum decomposition of a nondegenerate quadratic space (Z, q_Z) over k, and let q_X, q_Y be the restrictions of q_Z on X, Y, respectively. We assume that there is a bilinear map $\beta : X \times Y \to U$ such that

(2.2) $$q_U(\beta(x, y)) = q_X(x)q_Y(y).$$

In this situation, we define the Hopf map $h : Z \to V$ by

(2.3) $$h(z) = (q_X(x) - q_Y(y))\varepsilon + 2\beta(x, y),$$
$$z = x + y \in Z.$$

One verifies easily, using (2.1), (2.2), (2.3), that

(2.4) $$q(h(z)) = q_Z^2(z).$$

The map h sends a sphere in Z to a sphere in V. Now we introduce a useful set:

(2.5) $Z^* = \{z = (x, y) \in Z = X \oplus Y;$

1) We hope there is a better way to evade quadratic extensions than employing Hopf maps. By the way, the relationship between Hopf maps and elliptic curves in this paper is logically irrelevant to the one described in [5].

2) For an element $a \in k$ we denote by $a^{\frac{1}{2}}$ any one of square roots of a. Here $q^{\frac{1}{2}}(u - v)$ means $(q(u - v))^{\frac{1}{2}}$.