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 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

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

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

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

Note that

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

Consider a plane cubic given by

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

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

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

(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 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

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

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

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

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

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

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

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

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

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

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 $(q(u - v))^{\frac{1}{2}}$.

$x, y, \varepsilon + h(z)$ are all nonisotropic}.

Then, for any $z \in Z^*$, $h(z)$ does not belong to the line $k\varepsilon$; in fact, if it did, we would have a relation $h(z) = a\varepsilon$, $a \in k$, and hence, by (2.2), (2.3), $q_X(x)q_Y(y) = q_U(\beta(x, y)) = q_U(0) = 0$, contradicting our assumption that x, y are both nonisotropic. Therefore, if we put $v = \varepsilon + h(z)$ for $z \in Z^*$, then $w = (\varepsilon, v) \in V \times V$ becomes a pair such that ε, v are independent and nonisotropic, i.e., E_w is elliptic by (1.5) and so $w \in W$ by (1.6). Since $q(\varepsilon - v) = q(h(z)) = q_Z^2(z)$, a square, we obtain (2.6) below which is a refinement of (1.7)

(2.6) **Theorem.** *Let k be a field of characteristic $\neq 2$, (V, q), (X, q_x), (Y, q_Y) be nondegenerate quadratic spaces over k, ε a vector in V such that $q(\varepsilon) = 1$, $(Z, q_Z) = (X, q_X) \oplus (Y, q_Y)$ and $h: Z \to V$ a Hopf map defined by* (2.3). *Then, for $z = (x, y) \in Z^*$ in* (2.5), *the pair $w = (\varepsilon, v)$, $v = \varepsilon + h(z)$, defines an elliptic curve E_w over k: $Y^2 = X^3 + P_wX^2 + Q_wX$, with $P_w = 1 + q_X(x) - q_Y(y)$, $Q_w = -q_X(x)q_Y(y)$.*[3] *Furthermore, the point $P_0 = (x_0, y_0)$ belongs to $E_w(k)$, where*

$$x_0 = q_Z^2(z)/4,$$
$$y_0 = q_Z(z)(q_Z^2(z) + 2(q_X(x) - q_Y(y)))/8.$$

(2.7) **Remark.** In the proof of (2.6), the following list of values of inner product B in (1.1), (1.2) is useful: $B(\varepsilon, \varepsilon) = 1$, $B(\varepsilon, v) = 1 + q_X(x) - q_Y(y)$, $B(v, v) = (1 + q_X(x) - q_Y(y))^2 + 4q_X(x)q_Y(y) = 1 + 2(q_X(x) - q_Y(y)) + (q_X(x) + q_Y(y))^2$.

§3. Classical Hopf maps over Q. We shall consider a special case of the situation described in (2.6). Namely, let $k = \boldsymbol{Q}$, $V = \boldsymbol{Q}^3$, $\varepsilon = (1, 0, 0)$, $X = Y = U = \boldsymbol{Q}^2$,[4] $q_X = q_Y = q_U = f_n$, with $f_n(x) = x_1^2 + nx_2^2$, $n \in \boldsymbol{Z}$, $n \neq 0$, $q(v) = v_0^2 + v_1^2 + nv_2^2$, $\beta(x, y) = (x_1y_1 + nx_2y_2, x_1y_2 - x_2y_1)$ and $h(x, y) = (x_1^2 + nx_2^2 - y_1^2 - ny_2^2, 2(x_1y_1 + nx_2y_2), 2(x_1y_2 - x_2y_1))$.

Since Z^* in (2.5) depends only on n, we may set $Z^* = Z_n$. Then, for $z = (x, y) \in \boldsymbol{Q}^4$, we have

(3.1) $z \in Z_n \Leftrightarrow f_n(x)f_n(y)(1 + 2(f_n(x) - f_n(y)) + (f_n(x) + f_n(y))^2) \neq 0.$

Notice that

(3.2) if f_n is positive (i.e., if $n > 0$) then $z = (x, y) \in Z_n \Leftrightarrow x \neq 0$ and $y \neq 0$.

Since $w = \varepsilon + h(z)$ is determined by $z = (x, y) \in Z_n$, we may write P_Z, Q_Z, E_Z instead of P_w, Q_w, E_w, respectively. Thus, with a binary form

(3.3) $f_n(x) = q_X(x) = x_1^2 + nx_2^2$, $n \in \boldsymbol{Z}$, $n \neq 0$,

we can associate an elliptic curve:

(3.4) $E_z: Y^2 = X^3 + P_zX^2 + Q_zX$,
$P_z = 1 + f_n(x) - f_n(y)$, $Q_z = -f_n(x)f_n(y)$

and a point $P_0 = (x_0, y_0)$ on it:

(3.5) $x_0 = (f_n(x) + f_n(y))^2/4$,
$y_0 = (f_n(x) + f_n(y))((f_n(x) + f_n(y))^2 + 2(f_n(x) - f_n(y)))/8.$

From now on, we shall restrict ourselves to the case where z is integral: $z = (x, y) \in \boldsymbol{Z}^4$. Therefore $f_n(x)$, $f_n(y)$ are integers, and so are P_z, Q_z, $z \in Z_n \cap \boldsymbol{Z}^4$. Now, for any $a \in \boldsymbol{Z}$, put

(3.6) $Z_n(a) = \{z \in Z_n \cap \boldsymbol{Z}^4;$
$P_z = 1 + f_n(x) - f_n(y) = a\}.$

From (3.1), (3.4), (3.5), we have

(3.7) $Z_n(a) = \{z = (x, y) \in \boldsymbol{Z}^4;$
$f_n(y) = f_n(x) + 1 - a, f_n(x)(f_n(x) + 1 - a) \times (4f_n^2(x) + 4f_n(x)(1 - a) + a^2) \neq 0\}.$

(3.8) $P_z = a$, $Q_z = -f_n(x)(f_n(x) + 1 - a)$,

$$(3.9)\quad \begin{cases} x_0 = \left(f_n(x) + \dfrac{1-a}{2}\right)^2 \\ y_0 = \left(f_n(x) + \dfrac{1-a}{2}\right) \times \\ \qquad \left(f_n^2(x) + f_n(x)(1-a) + \dfrac{a^2-1}{4}\right). \end{cases}$$

Therefore by the Nagell-Lutz theorem ([6], p. 56), we obtain

(3.10) **Theorem.** *Let $f_n(x) = x_1^2 + nx_2^2$, $n \in \boldsymbol{Z}$, $n \neq 0$. When a is even, for $z = (x, y) \in Z_n(a)$ in* (3.7), *the rank of the elliptic curve:*

$$E_z: Y^2 = X^3 + aX^2 - f_n(x)f_n(y)X$$

is positive and $P_0 = (x_0, y_0)$ in (3.9) *is a nontorsion point on $E_z(\boldsymbol{Q})$.*

§4. Comments and examples. The real heart of our problem is of course the determination of the set $Z_n(a)$. We will reserve it for another occasion. Here, we will consider some illustrative examples.

(4.1) Let us seek elliptic curves of the form $Y^2 = X^3 - AX$ with $A \in \boldsymbol{Z}$, $A \neq 0$. Therefore putting $a = 0$ in (3.10), we find from (3.7),

$$Z_n(0) = \{z = (x, y) \in \boldsymbol{Z}^4; f_n(y) = f_n(x) + 1, f_n(x)f_n(y) \neq 0\}.$$

If we choose $x = (0,1)$, $y = (1,1)$, then $f_n(x) = n$, $f_n(y) = n + 1$. Hence, for $n \neq 0, -1$, we have $z = (x, y) \in Z_n(0)$, and (3.10) implies that

3) I beg of readers to be generous with a crash of notation X, Y, occurring in (2.6).

4) Here $U = \boldsymbol{Q}^2$ means the orthogonal complement of $\varepsilon = (1, 0, 0)$ in $V = \boldsymbol{Q}^3$ with respect to the quadratic form $q(v) = v_0^2 + v_1^2 + nv_2^2$.

all elliptic curves $E_z: Y^2 = X^3 - n(n+1)X$, $n \neq 0, -1$, have positive rank. For each n, a non-torsion point $P_0 = (x_0, y_0)$ is given by

$$x_0 = \left(n + \frac{1}{2}\right)^2, \ y_0 = \left(n + \frac{1}{2}\right)\left(n^2 + n - \frac{1}{4}\right).$$

(4.2) As readers notice, we miss the elliptic curve $Y^2 = X^3 - 36X$ in the family of elliptic curves in (4.1). However, this curve is a lucky one because $q(u - v)$ in (1.7) is a square and so we do not need a help of the Hopf map. In fact, for $V = \boldsymbol{Q}^2$, $q(u) = u_1^2 + u_2^2$, put $u = (3,0)$, $v = (0,4)$. Then $q(u) = 9$, $q(v) = 16$ and since $B(u, v) = 0$, $q(u - v) = q(u) + q(v) = 25 = 5^2$, a square. Therefore, by (1.7), $P_0 = (x_0, y_0)$ belongs to the curve E_w, $w = (u, v)$,: $y^2 = X^3 - (1/4)q(u)q(v)X = X^3 - 36X$ with $x_0 = 25/4 \notin \boldsymbol{Z}$. Thus, by Nagell-Lutz, the rank of E_w is > 0.

References

[1] Koblitz, N.: Introduction to Elliptic Curves and Modular Forms. Springer, New York (1984).

[2] Kwon, S.: Elliptic curves related with triangles. Proc. Japan Acad., **72A**, 118–120 (1996).

[3] Ono, T.: On the Hopf fibration over $\boldsymbol{Z}$. Nagoya Math. J., **56**, 201–207 (1975).

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

[5] Ono, T.: Variations on a Theme of Euler. Plenum, New York (1994).

[6] Silverman, J. H., and Tate, J.: Rational Points on Elliptic Curves. Springer, New York (1992).

[7] Tunnell, J.: A classical diophantine problem and modular forms of weight 3/2. Inventiones Math., **72**, 323–334 (1983).