Quadratic Forms and Elliptic Curves. IV

By Takashi ONO

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

(Communicated by Shokichi IYANAGA, M. J. A., June 12, 1997)

Introduction. This is a continuation of a series of papers [3] each of which will be referred to as (I), (II) and (III) in this paper. As in (I), we shall obtain, by the Hopf construction, a natural family of elliptic curves with canonical points defined over a given field k of rationality. For example, when $k = \boldsymbol{Q}$ and the Hopf map $h : \boldsymbol{Q}^2 \to \boldsymbol{Q}^2$ is given by $h(x, y) = (x^2 - y^2, 2xy)$, our method yields the following

(0.1) **Theorem.** *For a prime $p \equiv 1 \pmod 4$, let $p = a^2 + b^2$ be the unique expression of p by positive integers a, b with a odd. Let E_p be an elliptic curve given by*

$$(0.2)\quad E_p : Y^2 = X(X^2 - 2(1 + a^2 - b^2)X + (1 + 2(a^2 - b^2) + p^2)).$$

Then the point $P_0 = (1, p)$ is of infinite order in $E_p(\boldsymbol{Q})$.

1. Hopf construction. Let (V, q) be a nonsingular quadratic space over a field k of characteristic $\neq 2$. Let

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

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

$$(1.2)\quad \begin{cases} E_w : Y^2 = X^3 + A_w X^2 + B_w X, \\ A_w = -2\langle u, v\rangle = q(u) + q(v) - q(u + v) = q(v - u) - q(u) - q(v), \\ B_w = q(u)q(v).^{1)} \end{cases}$$

If we put $\alpha = q(u)$, $\beta = q(v)$, $\gamma = q(v - u)$, we have

$$(1.3)\quad E_w : Y^2 = X(X^2 - (\alpha + \beta - \gamma)X + \alpha\beta),$$

and nonsingularity of E_w (i.e., $w \in W$) amounts to the condition

$$\alpha\beta(\alpha^2 + \beta^2 + \gamma^2 - 2\alpha\beta - 2\beta\gamma - 2\gamma\alpha) \neq 0.$$

One verifies trivially that points $(\alpha, \alpha\sqrt{\gamma})$, $(\beta, \beta\sqrt{\gamma})$ belong to $E_w(k(\sqrt{\gamma}))$. If we want these points in $E_w(k)$, we need $w = (u, v) \in W$ such that $\gamma = q(v - u)$ is a square in k. The Hopf construction takes care of the matter. From now on, we assume that V has a unit vector ε, $q(\varepsilon) = 1$. Denote by U the orthogonal complement of the line $k\varepsilon$ and by q_U the restriction of q on U. Next, let $Z = X \oplus Y$ be an orthogonal direct sum decomposition of a nonsingular quadratic space (Z, q_Z) over k and q_X, q_Y be the restrictions of q_Z on X, Y, respectively. We assume further that there is a bilinear map $\beta : X \times Y \to U$ such that $q_U(B(x, y)) = q_X(x)q_Y(y)$. In this situation, we obtain a Hopf map $h : Z \to V$ given by

$$(1.4)\quad h(z) = (q_X(x) - q_Y(y))\varepsilon + 2\beta(x, y), \quad z = x + y \in Z,$$

which satisfies the required property

$$(1.5)\quad q(h(z)) = (q_Z(z))^2 = \text{a square}.$$

Finally, consider the set

$$(1.6)\quad Z^* = \{z = (x, y) \in Z = X \oplus Y ;\ x, y, \varepsilon + h(z) \text{ are all nonisotropic}\}.^{2)}$$

We know that $w = (u, v) = (\varepsilon, \varepsilon + h(z))$ belongs to W for all $z \in Z^*$.[3)]

Consequently, for this choice of w, we have

$$(1.7)\quad \begin{cases} E_w : Y^2 = X^3 + A_w X^2 + B_w X, \\ A_w = -2(1 + q_X(x) - q_Y(y)), \\ B_w = 1 + 2(q_X(x) - q_Y(y)) + (q_X(x) + q_Y(y))^2, \\ \alpha = q(u) = q(\varepsilon) = 1, \beta = q(v) = B_w, \\ \gamma = q(v - u) = q(h(z)) = (q_X(x) + q_Y(y))^2. \end{cases}$$

Furthermore, since $\alpha = 1$ and $\gamma = (q_X(x) + q_Y(y))^2$, we find

$$(1.8)\quad \text{the canonical point } (1, q_X(x) + q_Y(y)) \text{ belongs to } E_w(k).$$

In general, for a cubic curve $Y^2 = X(X^2 + AX + B)$, we denote by D the discriminant of the polynomial on the right side: $D = B^2(A^2 - 4B)$. For our elliptic curve E_w ((1.2), (1.7)), we have

$$(1.9)\quad D = 4(1 + 2T + S^2)^2(T^2 - S^2) \text{ with } S = q_X(x) + q_Y(y),\ T = q_X(x) - q_Y(y).$$

2. Primes of the form $x^2 + ny^2$. As a very

1) This E_w is a new one which is 2-isogenous to the curve in (I), (II) written by the same notation. Throughout this paper, we shall always mean by E_w the new curve given by (1.2).

2) In this paper, we shall not discuss the existence of Z^* in a general setting.

3) See (I), §2, after (2.5).