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

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

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

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

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

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

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

which satisfies the required property

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

Finally, consider the set

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

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

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

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

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).

special but an interesting example, we shall consider the case $k = \boldsymbol{Q}$, $V = Z = \boldsymbol{Q}^2 = X \oplus Y$, $X = Y = \boldsymbol{Q}$, $q_X(x) = x^2$, $q_Y(y) = ny^2$, $n \geq 1$, $q(z) = q_Z(z) = x^2 + ny^2$, $z = (x, y)$. Let $\varepsilon = (1,0)$, $\eta = (0,1)$. Hence $U = \boldsymbol{Q}\eta \approx \boldsymbol{Q}$, $q_U(y\eta) = q_Y(y) = ny^2$. As a bilinear form we adopt the map $\beta : Z \rightarrow U$ defined by $\beta(x, y) = xy\eta$. One verifies that $q_U(\beta(x, y)) = nx^2y^2 = q_X(x)q_Y(y)$. Then the Hopf map $h : Z = \boldsymbol{Q}^2 \rightarrow V = \boldsymbol{Q}^2$ is given by

(2.1) $h(x, y) = (x^2 - ny^2, 2xy)$.

Note that

(2.2) $\varepsilon + h(z) = (1 + x^2 - ny^2, 2xy)$.

Since $q(x, y) = x^2 + ny^2$, the set (1.6) boils down to

(2.3) $Z^* = \{z = (x, y) \in \boldsymbol{Q}^2 ; x \neq 0, y \neq 0\}$.

Given an integer $n \geq 1$, let p be a prime number $\not| \, 2n$ such that $p = a^2 + nb^2$ with positive integers a, b.[4] Let us set, for each $n \geq 1$,

(2.4) $E_n = \{p ; p \not| \, 2n, p = a^2 + nb^2, a, b > 0\}$.

We know that E_n contains infinitely many primes. To be more precise, let L be the ring class field of the order $\mathcal{O} = \boldsymbol{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \boldsymbol{Q}(\sqrt{-n})$. As is well-known, we have

(2.5) $p \in E_n \Leftrightarrow p$ splits completely in L.[5]

Since $L/\boldsymbol{Q}$ is galois of degree $2h(-n)$, $h(-n)$ being the class number of the order $\mathcal{O}$, the Dirichlet density of E_n is $(2h(-n))^{-1}$.

3. Subset F_n of E_n. We need a subset F_n of the set E_n (2.4) to state a theorem in 4. As F_n is interesting by itself, we insert here a brief comment on it. Set

(3.1) $F_n = \{p ; \text{prime}, p = a^2 + nb^2 = 4a^2 + 1, \quad a, b > 0\}$.[6]

In case $n = 1$, by the uniqueness of (x, y) such that $p = x^2 + y^2$, we find $a = 1$, $b = 2$, $p = 5$, i.e., $F_1 = \{5\}$. More generally, if n is square, $n = r^2$, then one verifies again by the uniqueness for $p = x^2 + y^2$ that $F_4 = \{5\}$ and $F_n = \phi$ for $r \geq 3$. Note that, since $nb^2 = 3a^2 + 1$, we have $F_n = \phi$ unless $n \equiv 1 \pmod 3$ and $\left(\frac{-3}{q}\right) = 1$ for any odd prime factor q of n. So it is enough to determine the set F_n for $n = 7, 13, 19, 28, \ldots$. For $n = 7$, we find $37 \in F_7$ with $a = 3$, $b = 2$. However machine computation shows that the next smallest $p \in F_7$ (if any) should be $> 10^{10}$. On the other hand some F_n contain at least two primes: e.g., $17, 41617 \in F_{13}$, $257, 152176897 \in F_{193}$ and $401, 578883601 \in F_{301}$. It would be nice if one could determine the (possibly finite) set F_n.[7]

In the Table below, the smallest primes p in F_n are shown.

n	p	a	b
1	5	1	2
4	5	1	1
7	37	3	2
13	17	2	1
19	101	5	2
28	37	3	1
31	8101	45	14
37	197	7	2
76	101	5	1
124	8101	45	7
127	677	13	2
148	197	7	1
193	257	8	1
301	401	10	1
433	577	12	1
508	677	13	1
547	2917	27	2
817	4357	33	2
973	1297	18	1
1027	5477	37	2
1201	1601	20	1
1519	8101	45	2
1657	8837	47	2
2188	2917	27	1
2269	12101	55	2
2353	3137	28	1
2977	15877	63	2
3169	16901	65	2
3268	4357	33	1
3367	17957	67	2
3997	21317	73	2
4108	5477	37	1
4219	22501	75	2
5293	7057	42	1
5419	28901	85	2
6076	8101	45	1
6628	8837	47	1
9076	12101	55	1

4) If $n \geq 2$, the ordered pair (a, b) is uniquely determined by p. (see, e.g., [2, p. 188, Theorem 101].) If $n = 1$, we assume that a is odd to secure the uniqueness.

5) See [1, p.181, Theorem 9.4]. [1] is an excellent exposition on primes of the said form.

6) We agree with the convention in 4). Note that the condition $p \not| \, 2n$ follows automatically from (3.1).

7) By the way, one verifies easily the following properties of F_n: (i) $n = mr^2 \Rightarrow F_n \subseteq F_m$. (ii) $p \in F_n \Rightarrow \left(\frac{n}{p}\right) = 1$. (iii) The set $\{p ; p = 1 + x^2, x \in \boldsymbol{Z}\} = \bigcup_n F_n$ (disjoint union, n : squarefree).

4. Elliptic curves attached to $p = x^2 + ny^2$. Back to the situation in **2**, for an $n \geq 1$, take a prime p in the set E_n (2.4). The pair (a, b) such that $p = a^2 + nb^2$ is uniquely determined by p. (see footnote 4)). For $z = (a, b)$, we have $h(z) = (x^2 - ny^2, 2xy)$ by (2.1), z belongs to Z^* ((1.6), (2.3)) and $w = (\varepsilon, \varepsilon + h(z)) = ((1,0), (1 + a^2 - nb^2, 2ab))$ belongs to W (1.1). Since w is determined by p, we can write $E_w = E_{n,p}$. In view of (1.7), to each $p \in E_n$, we associate an elliptic curve:

$$(4.1)\quad \begin{cases} E_{n,p} : Y^2 = X^3 + A_p X^2 + B_p X, \\ A_{n,p} = -2(1 + a^2 - nb^2), \\ B_{n,p} = 1 + 2(a^2 - nb^2) + p^2. \end{cases}$$

From (1.8), it follows that the point $(1, p)$ belongs to $E_{n,p}(\boldsymbol{Q})$. Let $D_{n,p}$ denote the discriminant of the cubic polynomial in (4.1). Then, by (1.9), we have, with $S = a^2 + nb^2 = p$, $T = a^2 - nb^2 = 2a^2 - p$,

$$(4.2)\quad D = D_{n,p} = 4(1 + 2T + S^2)^2(T^2 - S^2) \equiv 4(1 + 2T)^2 T^2 \pmod{p^2}.$$

Since $p \nmid T$ and $1 + 2T \equiv 4a^2 + 1 \pmod p$, we have

$$p^2 \mid D \Leftrightarrow p \mid (1 + 2T) \Leftrightarrow p \mid (4a^2 + 1) \Leftrightarrow$$
$$\exists\ c > 0 \text{ such that } (a^2 + nb^2)c = 4a^2 + 1 \Leftrightarrow$$
$$a^2 + nb^2 = 4a^2 + 1.^{8)}$$

In other words, by (3.1), we have

$$(4.3)\quad p^2 \mid D_{n,p} \Leftrightarrow p \in F_n.$$

Consider now the point $P_0 = (1, p) \in E_{n,p}(\boldsymbol{Q})$. If P_0 is of finite order, then, by the (strong) Nagell-Lutz theorem ([4, p.56, p.62]), p^2 divides $D_{n,p}$, and hence p belongs to F_n by (4.3). Summarizing our argument, we obtain

(4.4) **Theorem.** *For a positive integer n, let E_n, F_n be sets of primes defined by*

$$E_n = \{p\,;\, p \nmid 2n,\ p = a^2 + nb^2\},$$
$$F_n = \{p\,;\, p = a^2 + nb^2 = 4a^2 + 1\},$$

where a, b are positive integers. For $p \in E_n$, the point $P_0 = (1, p)$ lies on the elliptic curve

$$E_{n,p} : Y^2 = X^3 - 2(1 + a^2 - nb^2)X^2 + (1 + 2(a^2 - nb^2) + p^2)X.$$

If P_0 is a torsion point, then p belongs to F_n.

(4.5) **Remark.** If $F_n = \phi$, e.g. if $n \not\equiv 1 \pmod 3$, then $(1, p)$ is of infinite order for all $p \in E_n$. In view of comment after (2.4) we get in this way a natural family of elliptic curves of positive rank parametrized by a set of primes of density > 0. Next, let $n = 1$. We know that $F_1 = \{5\}$, so for all $p \geq 13$, $p \equiv 1 \pmod 4$, the point $P_0 = (1, p)$ is of infinite order. As for $p = 5$, however, we have $E_{1,5} : Y^2 = X^3 + 4X^2 + 20X$. Since the torsion subgroup of $E_{1,5}(\boldsymbol{Q})$ is of order 2, $P_0 = (1,5)$ is of infinite order, too. Therefore (0.1) is proved.

8) Note first that $c \leq 3$. Then eliminate cases $c = 2,3$ by taking mod 2, mod 3, respectively.

References

[1] D. Cox: Primes of the Form $x^2 + ny^2$. John Wiley & Sons, New York (1989).
[2] T. Nagell: Introduction to Number Theory. Chelsea, New York (1969).
[3] T. Ono: Quadratic forms and elliptic curves. I, II, III (with K. Ono). Proc. Japan Acad., **72A**, 156–158 (1996); **72A**, 194–196 (1996); **72A**, 204–205 (1996).
[4] J. H. Silverman and J. Tate: Rational Points on Elliptic Curves. Springer, New York (1992).