Nihonkai Math. J.
Vol. 12(2001), 75-88

On Certain Rational Cuboid Problems

Norihiko Narumiya and Hironori Shiga

0 Introduction

In this paper we study a certain kind of generalization of the congruent number problem. Namely, we mainly discuss the rational solutions of the equation (0.5) stated below, and we show how to generate all the solutions. The complete set of the solutions is given via the congruent number problem (see Theorem 1.2). We shall also discuss the similar equation (0.4).

The congruent number problem asks to find a criterion for the existence of a rectangle with rational sides and a rational diagonal having a given even integral area (saying $2N$). If there exists such a rectangle, we say N is a congruent number.

By putting x, y and z to be the sides and the diagonal, respectively, we can formulate this problem to find an non-trivial rational solution (that is $xyz \neq 0$) for the system of equations:

$$\begin{cases} x^2 + y^2 = z^2 \\ xy = 2N. \end{cases} \tag{0.1}$$

This is a famous problem origined in the ancient Arabic time. We can reformulate the problem by a slight modification of variables. By putting $x = 1 - t^2, y = 2t, z = 1 + t^2$ with $t \in \mathbf{Q}$ (0.1) is deformed to a single equation

$$z^2 t(1 - t^2) = N(1 + t^2)^2.$$

So we obtain an elliptic curve

$$V^2 = U^3 - N^2 U \tag{0.2}$$

by putting $U = -Nt, V = N^2(1 + t^2)/z$. By this transformation we obtain a bijective correspondence between the nontrivial rational solutions of (0.1) and those of (0.2) (that means $V \neq 0$). In 1983 Tunnell has discovered a nice criterion for the congruent number (see Tunnell [T]). So we study the analogous problem for a cuboid instead of a rectangle. Let us consider a cuboid K with the sides x, y and z. We say K to be a rational cuboid if x, y and z are rational numbers. We suppose K is situated in the (x, y, z)-space with the sides lying on the corresponding axis. We denote the diagonals on the (x, y)-surface, (y, z)-surface and (z, x)-surface by p, q and r, respectively, and we denote the inner diagonal by w.

Now we can set our problems:

Problem 0 (Perfect rational cuboid problem):

Does there exist a rational cuboid K with rational diagonals p, q, r and w ?

Problem 1:

Let N be a positive integer. Find a criterion that N to be a volume of a rational cuboid with rational diagonals p, q and r.

Problem 2:

Let N be a positive integer. Find a criterion that N to be a volume of a rational cuboid with rational diagonals p, q and w.

By using above notation we can formulate the Problem 0 as finding a nontrivial (that means $xyz \neq 0$) rational solution of the system of equations

$$\begin{cases} x^2 + y^2 = p^2 \\ y^2 + z^2 = q^2 \\ z^2 + x^2 = r^2 \\ x^2 + y^2 + z^2 = w^2. \end{cases} \tag{0.3}$$

It is not found any example of perfect rational cuboid still now, and we do not make the argument on (0.3) in this paper. If we neglect the condition for N, we get the following formulations of Problem 1 and Problem 2, respectively:

$$\begin{cases} x^2 + y^2 = p^2 \\ y^2 + z^2 = q^2 \\ z^2 + x^2 = r^2, \end{cases} \tag{0.4}$$

and

$$\begin{cases} x^2 + y^2 = p^2 \\ y^2 + z^2 = q^2 \\ x^2 + y^2 + z^2 = w^2. \end{cases} \tag{0.5}$$

0.1 Preliminaries

To proceed further considerations we need some classical transformations.

Lemma 0.1 *Let us consider the following elliptic curves $F(M, N)$ and $C(M, N)$ determined by complex parameters M, N with $MN(M - N) \neq 0$:*

$$F(M, N) =$$

$$\{[x_0, x_1, x_2, x_3] \in \mathbf{P}^3(\mathbf{C}) : x_0^2 + Mx_1^2 = x_2^2, x_0^2 + Nx_1^2 = x_3^2\} \tag{0.6}$$

$$C(M, N) = \{[x, y, z] \in \mathbf{P}^2(\mathbf{C}) : zy^2 = x(x + Mz)(x + Nz)\}. \tag{0.7}$$

Then $F(M,N)$ is isomorphic to $C(M,N)$ by the following map $\psi : F(M,N) \to C(M,N)$

$$\begin{cases} x = x_3 - x_2, \\ y = (N-M)x_1, \\ z = \frac{1}{MN}\{(M-N)x_0 + Nx_2 - Mx_3\}. \end{cases} \tag{0.8}$$

The inverse map of ψ is given by $\varphi : C(M,N) \to F(M,N)$

$$\begin{cases} x_0 = (x+Mz)\{y^2 - M(x+Nz)^2\}, \\ x_1 = 2(x+Nz)(x+Mz)y, \\ x_2 = (x+Mz)\{y^2 + M(x+Nz)^2\}, \\ x_3 = (x+Nz)\{y^2 + N(x+Mz)^2\} \end{cases} . \tag{0.9}$$

These isomorphisms become to be **Q**-*isomorphisms provided $M, N \in \mathbf{Q}$.*

Lemma 0.2 *Let us consider an elliptic curve*

$$y^2 = x^4 + cx^2 + dx + e$$

with rational coefficients c, d and e. By the birational transformation

$$x = \frac{v - 27d}{6u + 36c}, y = u/18 - c/6 - x^2 \tag{0.10}$$

we obtain a **Q**-*isomorphic Weierstrass equation*

$$v^2 = u^3 - 27(c^2 + 12e)u + 27(2c^3 + 27d^2 - 72ce).$$

The inverse transformation is given by

$$u = 3(6x^2 + 6y + c), v = 27(4x^3 + 4xy + 2cx + d). \tag{0.11}$$

Lemma 0.3 *Suppose $a, b \in \mathbf{Q}$. Then two elliptic curves*

$$E_1 : y^2 = x^3 + ax^2 + bx$$

and

$$E_2 : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$$

are isogenous with the following isogeny maps (of degree 2):

$$\begin{array}{rcl} \varphi : E_1 & \to & E_2 \\ (x,y) & \mapsto & \left(\dfrac{y^2}{x^2}, \dfrac{y(b-x^2)}{x^2}\right), \\ \psi : E_2 & \to & E_1 \\ (X,Y) & \mapsto & \left(\dfrac{Y^2}{4X^2}, \dfrac{Y(a^2-4b-X^2)}{8X^2}\right). \end{array}$$

1 The rational cuboid problem of Euler type

In this section we discuss the nontrivial rational solution of

$$\begin{cases} x^2 + y^2 = p^2 \\ y^2 + z^2 = q^2 \\ x^2 + y^2 + z^2 = w^2. \end{cases}$$

By putting $X = x/p, Y = y/p, Z = z/p, Q = q/p$ and $W = w/p$, this system of equations is transformed to

$$\begin{cases} X^2 + Y^2 = 1 \\ Y^2 + Z^2 = Q^2 \\ 1 + Z^2 = W^2. \end{cases} \tag{1.1}$$

The nontrivial rational solutions of the first equation in (1.1) are parametrized by

$$\begin{cases} X = \dfrac{1-t^2}{1+t^2} \\ Y = \dfrac{2t}{1+t^2} \end{cases}$$

with $t \in \mathbf{Q} - \{0, \pm 1\}$. By the same way the solutions of the third equation are given by

$$\begin{cases} Z = \dfrac{2s}{1-s^2} \\ W = \dfrac{1+s^2}{1-s^2} \end{cases}$$

with $s \in \mathbf{Q} - \{0, \pm 1\}$. So we obtain an equation

$$Q^2 = \frac{4t^2}{(1+t^2)^2} + \frac{4s^2}{(1-s^2)^2}$$

that is birationally equivalent with (1.1) over $\mathbf{Q}$.

By putting

$$u = (1+t^2)(1-s^2)Q/2$$

we obtain the equation

$$u^2 = (s^2t^2 + 1)(s^2 + t^2). \tag{1.2}$$

Now our problem is rearranged to find the rational solutions of (1.2).

For this purpose we construct the nonsingular complex surface S_1 determined by (1.2) as the following.

First we note that (1.2) determines a double covering complex variety V_1 over the product of s-sphere and t-sphere. It contains twelve rational double points of type A_1 at

$$(s,t) = (0,0), (0,\infty), (\infty,0), (\infty,\infty),$$
$$(1,\pm i), (-1,\pm i), (i,\pm 1), (-1,\pm 1).$$

After the resolution of these singularities we obtain the required surface S_1. We denote the exceptional curve obtained by the resolution at the point (a,b) by $\Theta_{a,b}$ (see the conceptional Figure 1).

For each value $s = a$ of the set $\{0, \pm 1, \pm i, \infty\}$ we obtain two rational curves over the complex line $\{s = a\}$ in (s,t)-space. We denote them $D_a^{\pm}$ with the index of s-coordinate. By the same way we determine $C_b^{\pm}$ for the complex line $\{t = b\}$ with $b \in \{0, \pm 1, \pm i, \infty\}$.

Remark 1.1 *We note that all the trivial complex solutions of (1.1) are contained in the union Λ_1 of the rational curves*

$$C_0^{\pm}, C_{\infty}^{\pm}, C_1^{\pm}, C_{-1}^{\pm}, D_0^{\pm}, D_{\infty}^{\pm}, D_1^{\pm}, D_{-1}^{\pm}$$

via the above correspondence.

Theorem 1.1 *The algebraic surface S_1 given by (1.2) is birationally equivalent over* $\mathbf{Q}$ *with*

$$S_2 \ : \ y^2 = z(z^2+4)x(x^2-1).$$

The birational map is given by

$$\phi \ : \ S_1 \longrightarrow S_2$$

$$\begin{cases} x = \dfrac{t+u+s^2t}{s(t-1)^2} \\ y = \dfrac{4t(t+u+s^2+s^2tu+s^2t^3+s^4t^2)}{s(t-1)^3} \\ z = 2st \end{cases} \tag{1.3}$$

and

$$\psi \ : \ S_2 \longrightarrow S_1$$

$$\begin{cases} s = \dfrac{z(-4x+y-2z)}{2(y+2z+xz^2)} \\ t = \dfrac{y+2z+xz^2}{-4x+y-2z} \\ u = (4y^2-32x^3z+16yz+16z^2-48x^2z^2+y^2z^2-16x^3z^3-4yz^3+4z^4-12x^2z^4-2x^3z^5) \\ \qquad /(4(4x-y+2z)(y+2z+xz^2)) \ . \end{cases} \tag{1.4}$$

Remark 1.2 *We obtain the following seven curves on S_2 corresponding to Λ_1 on S_1 mentioned above :*

$$\begin{aligned} &\{x=y=0\}, \{z=y=0\} \\ &\{x=\pm 1 \ , \ y=0\}, \\ &\{x=(z^2+4)/4z \ , \ y=(z^2-4)(z^2+4)/8z\} \\ &\{x=(z+2)^2/(z-2) \ , \ y=4z(z+2)(z^2+4)/(z-2)^3\} \\ &\{x=-(z-2)^2/(z+2)^2 \ , \ y=4z(z-2)(z^2+4)/(z+2)^3\} \ . \end{aligned}$$

We denote by Λ_2 the union of these curves on S_2.

Proof: We get the above transformation as the composition of the following transformations:

First transform:

$$T_1(s,\ t,\ u) = (v_1,\ t_1,\ u_1) = (st,\ t,\ tu).$$

By T_1 we obtain the transformed equation

$$u_1^2 = (v_1^2+1)(t_1^4+v_1^2). \tag{1.5}$$

We can regard (1.5) as an elliptic fibered surface over v_1-space. That has four singular fibers over $v_1 = 0, \pm i, \infty$ of type I_0^* using the notation of Kodaira. Next we proceed

$$T_2(v_1,\ t_1,\ u_1) = (v_2,\ t_2,\ u_2) = (v_1,\ 1/(t_1-1),\ u_1/(t_1-1)^2)$$

to get rid the section

$$\sigma(v_1) = (v_1,\ t_1,\ u_1) = (v_1,\ 1,\ v_1^2+1)$$

to the section at infinity. Then we get the equation. To get a monic form of the right hand side we proceed

$$T_3(v_2,\ t_2,\ u_2) = (v_3,\ t_3,\ u_3) = (v_2,\ (v_2^2+1)t_2,\ (v_2^2+1)u_2).$$

Then we get

$$u_3^2 = t_3^4 + 4t_3^3 + 6(v_3^2+1)t_3^2 + 4(v_3^2+1)t_3 + (v_3^2+1)^3\ . \tag{1.6}$$

To cancel the term of t_3^3 we proceed

$$T_4(v_3,\ t_3,\ u_3) = (v_4,\ t_4,\ u_4) = (v_3,\ t_3+1,\ u_3).$$

Then we get

$$u_4^2 = t_4^4 + 6v_4^2t_4^2 + 4v_4^2(v_4^2-1)t_4 + v_4^2(v_4^4-v_4^2+1)\ . \tag{1.7}$$

Now we put

$$\begin{cases} c(v_4) = 6v_4^2 \\ d(v_4) = 4v_4^2(v_4^2-1) \\ e(v_4) = v_4^2(v_4^4-v_4^2+1)\ . \end{cases}$$

According to Lemma 0.2 we can shift the quartic polynomial of t_4 in (1.6) to a cubic polynomial. In fact, by the transform

$$\begin{cases} x_1 = 18(u_4+t_4^2+v_4^2) \\ y_1 = 108(t_4^3+t_4u_4-v_4^2+3t_4v_4^2+v_4^4) \\ z_1 = v_4 \end{cases}$$

we get

$$y_1^2 = x_1^3 - 3^4(2z_1(z_1^2+1))^2x_1\ . \tag{1.8}$$

So we perform the final transform

$$\begin{cases} x_2 = \dfrac{x_1}{18z_1(z_1^2+1)} \\ y_2 = \dfrac{y_1}{27z_1(z_1^2+1)} \\ z_2 = 2z_1\ . \end{cases}$$

Then we obtain the required form

$$y_2^2 = z_2(z_2^2+4)x_2(x_2^2-1)\ . \tag{1.9}$$

By the composition of the above transformations we obtain the transformation ϕ.

Q.E.D.

By this theorem we can obtain all the nontrivial rational solution of (1.1) from the set of ratioal points $S_2(\mathbf{Q})$ on the vriety S_2. So we discuss how to generates $S_2(\mathbf{Q})$.

Let us cosider the elliptic curves

$$\begin{aligned} E_1 \ :\ w_1^2 &= x(x^2-1) \\ E_2 \ :\ w_2^2 &= z(z^2+4) \quad . \end{aligned}$$

The product type abelian variety $E_1 \times E_2$ admits an involution

$$\iota \ :\ ((x,\ w_1),\ (z,\ w_2)) \mapsto ((-x,\ -w_1),\ (-z,\ -w_2)).$$

The surface S_2 is identified as the Kummer surface $E_1 \times E_2/\iota$.

Remark 1.3 *We note that E_1 and E_2 are isogenous, and the isogeny is given as follows:*

$$\begin{aligned} f_1 \ :\ E_1 &\ \to\ E_2 \\ (x, w_1) &\ \mapsto\ (w_1^2/x^2, -w_1(x^2+1)/x^2)\ . \end{aligned}$$

The dual isogeny is given by

$$\begin{aligned} f_2 \ :\ E_2 &\ \to\ E_1 \\ (z, w_2) &\ \mapsto\ (w_2^2/4z^2, w_2(4-z^2)/(8z^2))\ . \end{aligned}$$

This is the consequence of Lemmma1.3

According to this isogeny our problem is reduced to the rational points on the rational points on the Kummer surface of product type

$$Kum_1 \ :\ \eta^2 = \xi(\xi^2-1)\zeta(\zeta^2-1) \tag{1.10}$$

that can be considered as $E_1 \times E_1/\iota$, where ι indicates the involution $P \mapsto -P$ on the abelian variety. In fact the following transformations give two to one correspondences between S_2 and Kum_1:

$$\Phi \ :\ \begin{cases} \xi = x \\ \eta = \dfrac{y(4-z^2)}{8z^2} \\ \zeta = \dfrac{y^2}{4x(x^2-1)z^2} \end{cases}$$

and

$$\Psi \ :\ \begin{cases} x = \xi \\ y = -\dfrac{\eta(1+\zeta^2)}{\zeta^2} \\ z = \dfrac{\eta^2}{\zeta^2\xi(\xi^2-1)} \ . \end{cases}$$

Remark 1.4 *Now we set the following curves on* Kum_1*:*

$$\begin{aligned}\Gamma_1^{\pm} &= \{\xi = \pm 1, \eta = 0\},\\ \Gamma_2^{\pm} &= \{\xi - \zeta = 0, \eta = \pm\xi(\xi^2 - 1)\},\\ \Gamma_3^{\pm} &= \{\eta = \pm 2\xi\zeta\},\end{aligned}$$

and we set

$$\Lambda_3 = \Gamma_1^+ \cup \Gamma_1^- \cup \Gamma_2^+ \cup \Gamma_2^- \cup \Gamma_3^+ \cup \Gamma_3^- .$$

The rational points on Λ_3 *correspond to the trivial solution of (1,2).*

It is well known that $E_1(\mathbf{Q}) = \{(0,0), (\pm 1, 0), \mathbf{O} = (\infty, \infty)\}$. So the abelian variety dose not induce any nontrivial rational point on Kum_1.

Now we suppose a rational point (ξ, ζ, η) on Kum_1. Let us make the prime decomposition of $\xi(\xi^2 - 1)$ as

$$\xi^3 - \xi = p_1 p_2 \cdots p_k \times s^2 ,$$

where s indicates a certain number in $\mathbf{Q}$. To get a square number η^2 it must hold also

$$\zeta^3 - \zeta = p_1 p_2 \cdots p_k \times u^2 ,$$

with a certain number u in $\mathbf{Q}$. By putting $N = p_1 \cdots p_k$, $\xi = X/N$, $s = Y/N^2$ in the former equality we obtain

$$Y^2 = X^3 - N^2 X. \tag{1.11}$$

By putting $\zeta = Z/N$, $u = W/N^2$ in the latter we have

$$W^2 = Z^3 - N^2 Z \tag{1.12}$$

by the same way. As we stated in Section 1 (0.2) the above equations (1.11) and (1.12) take the form of the classical congruent number equation. As the consequence of the above investigation we have the following:

Proposition 1.1 *Let* N *be a congruent number, and let* (X, Y), (Z, W) *be nontrivial solutions of the congruent number equation (1.11) and (1.12), respectively. By putting*

$$(\xi, \zeta, \eta) = (X/N, Z/N, YW/N^3),$$

we obtain a rational point (ξ, ζ, η) *of* Kum_1. *Conversely, every nontrivial rational point of* Kum_1 *is obtained in this way.*

As the consequence of Theorem 1.1 and the above arguments we have:

Theorem 1.2 *There is a* $2:1$ *correspondence* $\psi \circ \Psi$ *from the set of rational points on* Kum_1 *to the set of nontrivial solutions of 1.2 outside the divisor* Λ_3. *The composite* $\Phi \circ \phi$ *gives the* $2:1$ *correspondence of the converse direction.*

Now we know that the rational solution of our original problem 0.5 is given via the pair of rational points on the elliptic curve 0.2 with the same congruent number N.

2 The Problem SRC and its variation

Concerning the equation (0.4) we can proceed the similar consideration, and we can get an analogous result. By putting $X = x/p$, $Y = y/p$, $Z = z/p$, $Q = q/p$ and $R = r/p$ we can deduce the following system of equations from (0.4):

$$\begin{cases} X^2 + Y^2 = 1 \\ Y^2 + Z^2 = Q^2 \\ Z^2 + X^2 = R^2 \ . \end{cases} \tag{2.1}$$

Theorem 2.1 *The variety defined by (2.1) is birationally equivalent over* $\mathbf{Q}(\sqrt{2})$ *with*

$$S \ : \ y^2 = x(x^2 - 4x + 2)z(z^2 + 8z + 8). \tag{2.2}$$

Remark 2.1 *The above surface* S *is a Kummer surface induced from the product type ablian variety* $T_1 \times T_2$ *with*

$$\begin{aligned} T_1 \ : \ y_1^2 &= x_1(x_1^2 - 4x_1 + 2), \\ T_2 \ : \ y_2^2 &= x_2(x_2^2 + 8x_2 + 8) \ . \end{aligned}$$

Moreover T_1 *and* T_2 *are isogenous over* $\mathbf{Q}$ *with the isogeny stated in Lemma 0.3.*

Remark 2.2 *Two elliptic curves* T_1 *and* T_2 *are isomorphic over the real quadratic field* $\mathbf{Q}(\sqrt{2})$*, and they are isomorphic with the torus* $\mathbf{C}/(\mathbf{Z}+\sqrt{-2}\mathbf{Z})$ *as a complex curve. So they are examined to be modular curves and with Mordell-Weil rank 0 (see Cremona[C]). Hence by the similar argument as in Section 1 we have two to one correspondence defined over* $\mathbf{Q}(\sqrt{2})$ *between the set of non-trivial* $\mathbf{Q}(\sqrt{2})$*-rational points on the surface (2.2) and that of the self product Kummer surface*

$$T^2 = U(U^2 - 2U + \frac{1}{2})V(V^2 - 2V + \frac{1}{2}) \tag{2.3}$$

outside a certain divisor.

Here we describe the exact process to get the equivalence in Theorem 2.1.

-First step-

By putting

$$\begin{cases} X = \dfrac{1 - u^2}{1 + u^2} \\ Y = \dfrac{2u}{1 + u^2} \end{cases}$$

we can reduce the variety (2.1) to the equation

$$\begin{cases} x_0^2 + \dfrac{4u^2}{(1 + u^2)^2}\tilde{x}_1^2 = x_2^2 \\ x_0^2 + \dfrac{(1 - u^2)^2}{(1 + u^2)^2}\tilde{x}_1^2 = x_3^2 \ . \end{cases} \tag{2.4}$$

By considering $\tilde{x}_1/(1+u^2)$ a new variable x_1 we get a parametrized family of space elliptic curves $F(4u^2,\ (1-u^2)^2)$ in Lemma 0.1. Hence we can transform it to the family of plane elliptic curves of the following form:

$$\Sigma\ :\ t^2 = s(s^2+4u^2)(s+(1-u^2)^2)\ .$$

It determines an elliptic surface over u-sphere. It has the singular fibers of type I_4 over $u = 0,\ \pm 1,\ \infty$ and those of type I_2 over $u = \pm\sqrt{2}+1,\ \pm\sqrt{2}-1$.

-Second step-

We define an intermediate surface

$$K_1\ :\ w_1^2 = (2x_1^2-4x_1+1)(u_1^4-4x_1u_1^2+2x_1^2). \tag{2.5}$$

That is obtained by looking for the another elliptic fibration for Σ. We can regard K_1 as an elliptic surface over x_1-sphere with singular fibers of type I_0^* over $x_1 = 0,\ \infty,\ 1\pm 1/\sqrt{2}$. This configuration shows that it is a product type Kummer surface. In fact the transformation

$$\begin{cases} x_1 = \dfrac{u^2s+2(\sqrt{2}+1)u^2(u^2-1)}{\sqrt{2}(\sqrt{2}+1)s+2\sqrt{2}u^2(u^2-1)} \\ w_1 = \dfrac{u^2(u^2-1)(u^2-3-2\sqrt{2})t}{2\{(\sqrt{2}+1)s+2u^4-2u^2\}^2} \\ u_1 = u \end{cases} \tag{2.6}$$

gives the equivalence from Σ to K_1.

-Third step-

The elliptic surface K_1 has a global section $u_1 = 1,\ w_1 = 2x_1^2-4x_1+1$ defined over $\mathbf{Q}$. So we get rid it to the section at infinity. After that we make the routine work of the transformation in Lemma 0.2. The above process is realized by the transformation

$$\begin{cases} x = x_1 \\ y = 8(u_1^3+u_1w_1-2u_1x_1-2u_1^2x_1-4u_1^3x_1-2w_1x_1-2u_1w_1x_1+2x_1^2+ \\ \qquad 8u_1x_1^2+8u_1^2x_1^2+2u_1^3x_1^2+2w_1x_1^2-8x_1^3-4u_1x_1^3-4u_1^2x_1^3+4x_1^4)/(x_1(u_1-1)^3) \\ z = \dfrac{2(u_1^2+w_1-2x_1-2u_1^2x_1+2x_1^2)}{x_1(u_1-1)^2} \end{cases} \tag{2.7}$$

gives the equivalence between K_1 and S.

(The variation of the Problem SRC) As we have studied we can not get an equivalence defined over $\mathbf{Q}$ from (2.1) to a product type Kummer surface. So we perform a slight modification of the problem to get a nice description of the rational points. Let us consider the variety

$$\begin{cases} X^2+Y^2 = 1 \\ 2Y^2+Z^2 = Q^2 \\ Z^2+2X^2 = R^2\ . \end{cases} \tag{2.8}$$

Proposition 2.1 *We get an equivalence between (2.8) and the surface (2.2) defined over* $\mathbf{Q}$.

We can obtain this equivalence by the similar method as in Theorem 2.1.

-First step-

By putting

$$\begin{cases} X = \dfrac{1-u^2}{1+u^2} \\ Y = \dfrac{2u}{1+u^2} \end{cases}$$

we can reduce the variety (2.8) to the equation

$$\begin{cases} x_0^2 + 2 \cdot \dfrac{4u^2}{(1+u^2)^2}\tilde{x}_1^2 = x_2^2 \\ x_0^2 + 2 \cdot \dfrac{(1-u^2)^2}{(1+u^2)^2}\tilde{x}_1^2 = x_3^2 \ . \end{cases}$$

By considering $\tilde{x}_1/(1+u^2)$ to be a new variable x_1, we get a parametrized family of space elliptic curves $F(8u^2,\ 2(1-u^2)^2)$ in Lemma 0.1. Hence we can transform it to the family of plane elliptic curves of the following form:

$$\Sigma' \ : \ t^2 = s(s+8u^2)(s+2(1-u^2)^2).$$

It determines an elliptic surface over u-sphere.

-Second step-

We consider again the intermediate surface

$$K_1 \ : \ w_1^2 = (2x_1^2 - 4x_1 + 1)(u_1^4 - 4x_1u_1^2 + 2x_1^2).$$

We can find the birational $\mathbf{Q}$-equivalence between K_1 and Σ' as the following:

$$\begin{cases} x_1 = \dfrac{2s+t+2su^2}{4(-2+s+4u^2-2u^4)} \\ w_1 = (-8s - 4s^2 + 2s^3 - 8t - t^2 - 32u^2 + 16s^2u^2 + 8tu^2 + 128u^4 + 16su^4 - \\ \qquad 4s^2u^4 + 8tu^4 - 192u^6 - 8tu^6 + 128u^8 - 8su^8 - 32u^{10})/(8(-2+s+4u^2-2u^4)^2) \\ u_1 = u \end{cases}$$

and

$$\begin{cases} s = 4(u_1^2 + w_1 - 2x_1 - 2u_1^2x_1 + 2x_1^2) \\ t = 8(-u_1^2 - u_1^4 - w_1 - u_1^2w_1 + x_1 + 8u_1^2x_1 + u_1^4x_1 + 2w_1x_1 - 6x_1^2 - 6u_1^2x_1^2 + 4x_1^3) \\ u = u_1 \end{cases} \quad .$$

-Third step- This is the exactly same as the third step in Theorem 2.1.

Finally we can state certain systems of rational solutions of (1,4).

Proposition 2.2

$$\begin{cases} x = -2(k^2-4k+5)^2(k^2-5k+5)(k^2-5) \\ y = -4k(k-2)(2k-5)(k^2-4k+5)(k^2-5k+5) \\ z = k(k-1)(k-2)(k-3)(k-5)(2k-5)(3k-5) \\ p = -2(k^2-4k+5)(k^2-5k+5)(k^4-4k^3+8k^2-20k+25) \\ q = k(k-2)(2k-5)(-5k^4+48k^3-166k^2+240k-125) \\ r = 2k^8 - 26k^7 + 14k^6 - 446k^5 + 1066k^4 - 2230k^3 + 3525k^2 - 3250k + 1250 \ . \end{cases} \tag{2.9}$$

$$\begin{cases} x = -8k(2k^2+1)(48k^8-16k^6+4k^2-3) \\ y = (4k^4-12k^2+1)(48k^8-16k^6+4k^2-3) \\ z = 4(64k^{12}-80k^{10}+80k^8-120k^6+20k^4-5k^2+1) \\ p = -(4k^4+20k^2+1)(48k^8-16k^6+4k^2-3) \\ q = 320k^{12}-640k^{10}+560k^8-64k^6+140k^4-40k^2+5 \\ r = 4(64k^{12}+208k^{10}-112k^8+56k^6-28k^4+13k^2+1)\ . \end{cases} \tag{2.10}$$

$$\begin{cases} x = 2b(4a^4+3a^2+1)(4a^4+a^2-1) \\ y = 4ab(2a^2+1)(4a^4+a^2-1) \\ z = (2a^2+1)(16a^8+8a^6-15a^4-10a^2+1) \\ p = 2b(4a^4+5a^2+1)(4a^4+a^2-1) \\ q = -(2a^2+1)(16a^8+8a^6+a^4+6a^2+1) \\ r = 32a^{10}+64a^8+26a^6-a^4+4a^2+3 \\ \textit{where,a, b satisfy } b^2 = 2(a^2+1)\ . \end{cases} \tag{2.11}$$

$$\begin{cases} x = 4a(2b^2-b+1)(2b^2+b+1)(4b^4+b^2-1) \\ y = -8ab(2b^2+1)(4b^4+b^2-1) \\ z = (2b^2+1)(4b^4+b^2+4ab-1)(4b^4+b^2-4ab-1) \\ p = 4a(b^2+1)(4b^2+1)(4b^4+b^2-1) \\ q = -(2b^2+1)(16b^8+8b^6-7b^4+16a^2b^2-2b^2+1) \\ r = 64a^2b^8+16b^8+32a^2b^6+24b^6-28a^2b^4+17b^4-8a^2b^2+6b^2+4a^2+1 \\ \textit{where,a, b satisfy } 2a^2 = b^2+1\ . \end{cases} \tag{2.12}$$

Proof. We obtain 4 rational curves on Σ as the lifting of the following curves on s, u-plane corresponding to each parametrization (2.9), (2.10), (2.11) and (2.12), respectively:

$$\begin{aligned} &s = u^2-1 \\ &s = 4u^2(2u^2-1) \\ &s^2+4u^2s+16u^6 = 0 \\ &s^2+12u^2s+32u^4+32u^6 = 0 \end{aligned}$$

Q.E.D.

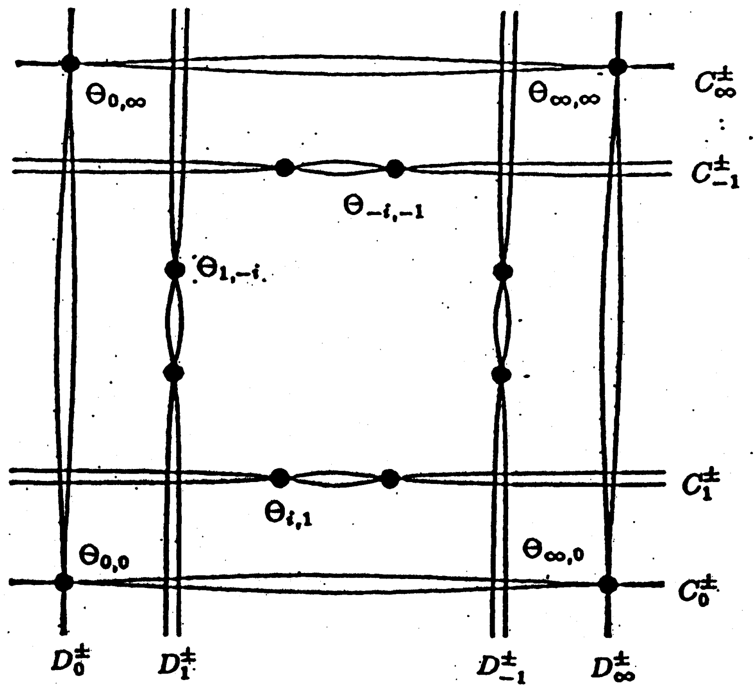
$\Theta_{0,\infty}$
$\Theta_{\infty,\infty}$
$C^{\pm}_{\infty}$
$C^{\pm}_{-1}$
$\Theta_{-i,-1}$
$\Theta_{1,-i}$
$C^{\pm}_{1}$
$\Theta_{i,1}$
$\Theta_{0,0}$
$\Theta_{\infty,0}$
$C^{\pm}_{0}$
$D^{\pm}_{0}$
$D^{\pm}_{1}$
$D^{\pm}_{-1}$
$D^{\pm}_{\infty}$

Fig. 1

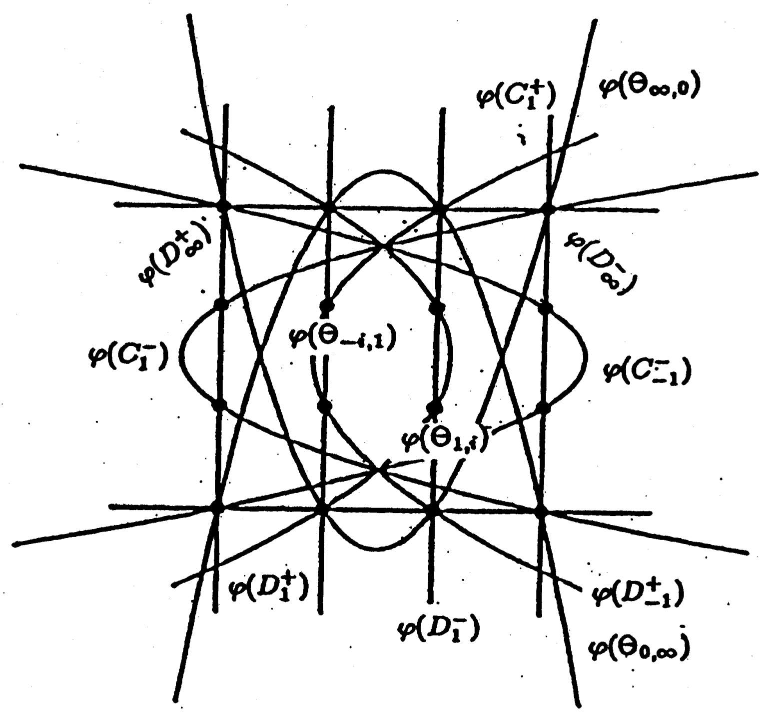
$\varphi(C^{+}_{1})$
$\varphi(\Theta_{\infty,0})$
$\varphi(D^{+}_{\infty})$
$\varphi(D^{-}_{\infty})$
$\varphi(\Theta_{-i,1})$
$\varphi(C^{-}_{1})$
$\varphi(C^{-}_{-1})$
$\varphi(\Theta_{1,i})$
$\varphi(D^{+}_{1})$
$\varphi(D^{+}_{-1})$
$\varphi(D^{-}_{1})$
$\varphi(\Theta_{0,\infty})$

Fig. 2

References

[ABS] Abo, N. Sasakura and T. Terasoma, Quadratic residue graph and Shioda elliptic modular surfaces $S(4)$, Tokyo J. Math., 19(1996), 263 - 288.

[A] N. Adachi, On Pythagorean Elliptic Curves. Proc. Japan Acad., vol. 70(1994), 226 - 229.

[B-G] F. Beukers and B. van Geemen, Rational cuboids,preprint(1995).

[C] J.E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge U.P., 1992.

[Kz] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, 1984.

[L] J. Leech, The rational cuboid revisited, Amer. Math. Monthly, 84(1977), 518 - 533.

[Mi] M. Mizukami, Birational mappings from the quartic surfaces to the Kummer surfaces, Masterthesis Univ. of Tokyo, 1976, in Japanese.

[N] N. Narumiya, Studies on the rational cuboid problems from an algebro-geometric view point, Masterthesis Chiba Univ., 1995.

[O] T. Ono, Variations on the theme of Euler, Jikkyo Shuppan Pub., 1980, in Japanese.

[S] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

[Ta] S. Tajima, On a certain Mordell-Weil group and its application, Masterthesis Chiba Univ., 1989.

[T] J. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, Inv. Math., 72(1983), 323 - 334.

Norihiko Narumiya and Hironori Shiga
Graduate School of Science and Technology, Chiba University
Yayoi-cho 1-33, Inage-ku, 263-8522 Chiba, Japan
shiga@math.s.chiba-u.ac.jp

Received December 18, 2000