ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

T. G. BERRY

Points at rational distance from the corners of a unit square

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4^e série, tome 17, n^o 4 (1990), p. 505-529

<http://www.numdam.org/item?id=ASNSP_1990_4_17_4_505_0>

Points at Rational Distance from the Corners of a Unit Square

T.G. BERRY

Introduction

This paper is mainly concerned with the study, using algebro-geometric techniques, of the diophantine equation

$$2(Y^4 + T^4) + X^4 + Z^4 = 2(X^2 + Z^2)(Y^2 + T^2). \tag{1}$$

We also give a few, negative, results on the possible simultaneous rational solutions of (1) and

$$U^2 + Y^2 = X^2 + Z^2. \tag{2}$$

Equations (1) and (2) occur in the old problems of finding a point in the plane of a unit square whose distances to three or to all four corners of the square are rational (these are called the three and four distance problems respectively). Indeed (1) is the necessary and sufficient condition that three non-negative reals be the distances of a point in the plane of a square of side T to three given corners of the square, and, when (1) is satisfied, (2) gives the fourth distance (c.f. Fig. 1).

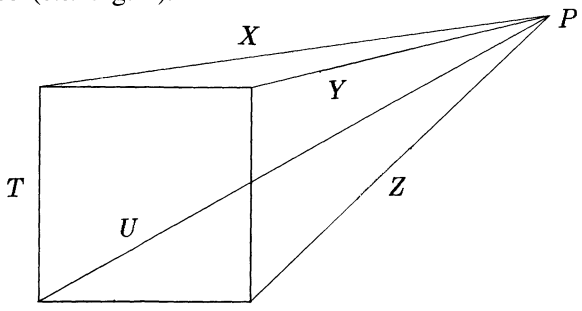


Fig. 1

Pervenuto alla Redazione il 12 Maggio 1988 e in forma definitiva il 6 Febbraio 1990.

The three and four distance problems are reviewed in §D19 of R.K. Guy's collection [8], and the three-distance problem (or an equivalent problem) is studied in [5] and [9] - the latter contains an extensive historical review. According to these references no solutions of the four distance problem are known. For a long time the three-distance problem was conjectured to have no solutions except when the point P lies on a side of the square. However, in 1967 a one-parameter family of solutions was found by J.H. Hunter. This family was rediscovered later by J. Leech, J.H. Conway and M.K. Guy, and Leech showed how to generate infinitely many one-parameter families of solutions starting from this one. Subsequently other solutions not lying in the Hunter-Leech one-parameter families have been found, mainly by studying certain elliptic curves associated with the problem. All this is reviewed in [9], and details are given in [5]. Our results complement these by studying the one-parameter families of solutions of the three-distance problem.

We now describe the main results of this paper. It should be stated at the outset that we have not settled the four distance problem: we neither produce a solution nor prove that there is none. Our main result is that there is an extraordinary abundance of solutions of the three distance problem. We show in fact that there are infinitely many one-parameter families of rational integer solutions of (1). We give explicitly families parametrized by polynomials of degree 2, 4, 6, and 8, these being the lowest degrees that occur, and show that our list is complete for degrees 2 and 4. We also give an iterative procedure that generates an infinite set of one-parameter families starting from the families of degrees two and four, but we show that this procedure does not generate all the one-parameter families of solutions of (1). The degree 4 solution is (up to a reparametrization) the Hunter-Leech-Conway-Guy solution, and our iterative method, applied to this family, presumably coincides with Leech's, though we have not verified this explicitly. All the other solutions we give are new, and in particular there are infinitely many one-parameter families of solutions outside the Hunter-Leech families.

As for the four distance problem, we prove that there is no simultaneous integer solution of (1) and (2) contained in the one-parameter families of solutions of (1) of degrees 2 and 4. We give reasons, but no proof, for believing that the same is true for the families of higher degree.

Our technique consists in viewing (1) as the homogeneous equation of a surface S in $\mathbb{P}^3(\mathbb{C})$. It turns out that S is a Kummer surface, i.e. it is a quartic surface with exactly sixteen singular points. One-parameter families of solutions of (1) correspond to parametrizable curves on S. (By parametrizable we always mean parametrizable by rational functions with rational coefficients). The parametrizable curves of degrees 2 and 4 are certain plane sections of S. From these we generate parametrizable curves of higher degree by projecting away from nodes of S. We show that infinitely many distinct parametrizable curves can be obtained in this way by showing that the composition of projections from two distinct nodes corresponds to translation by an element of infinite order in the elliptic pencil cut out on S by planes through the two nodes. A study of

this elliptic pencil also yields the Néron-Severi group of S. This theoretically allows one to find all parametrizable curves on S of given degree whose proper transforms are non-singular on a desingularisation of S. We use it to show that our list of parametrizable curves of degrees 2 and 4 is complete, and that there are more parametrizable curves of degrees 6 and 8 than can be accounted for by projecting curves of lower degree from nodes.

It is worth mentioning that our methods can be applied to the problem of finding points at rational distance from the vertices of any triangle. The results are very similar to those just described.

Equations (1) and (2) together define a surface R in $\mathbb{P}^4(\mathbb{C})$ which is a double cover of S. Our meagre results on the four distance problem come from a study of the ramification of this double cover. R turns out to be a regular surface of general type, which perhaps accounts for the difficulty of the four distance problem: there is not even the beginning of a diophantine theory for these surfaces.

Studies of diophantine properties of quartic surfaces in $\mathbb{P}^3$, and more generally of K_3 surfaces in higher-dimensional spaces, have been made by Swinnerton-Dyer [16] and Bremner [2], [3], [4]. Our techniques are, naturally, similar to those of Bremner and Swinnerton-Dyer, but the fact that we are working with a Kummer, which is a very particular type of K_3 surface, alleviates many technical difficulties, particularly with regard to the calculation of the Néron-Severi group.

I am very grateful to John Tyrrell for pointing out the problem itself and the fact that S is Kummer, and for much ingenious help with the computations.

1. - The geometric background

All the properties of Kummer surfaces that we use can be found in [1], Chap. 8.

We continue with the terminology of the introduction. The singularities of S can be found directly by calculating the simultaneous zeroes of the partial derivatives of the L.H.S. of (1). This presents no difficulty and one finds sixteen singular points, which are listed in Table 2 (see Appendix). With hindsight this seems reasonable, since it gives singular points whenever the point P of Fig. 1 is at a corner of the square. Since it has precisely sixteen singular points, S is a Kummer surface and each singular point is a node, i.e. a double point whose Zariski tangent cone is an irreducible quadratic cone.

The sixteen nodes of a Kummer surface define a 16_6 configuration i.e. there are sixteen planes, called the singular tangent planes, each of which contains six nodes, while each node lies on six of the planes. Table 3 gives the singular tangent planes (see Appendix). Table 1 (which is taken from [6], p. 161) is the incidence diagram of the 16_6 configuration: if the numbers in the top row of

Table 1 are taken as naming planes, then the columns name the nodes that lie on those planes, and dually (see Appendix).

Each singular tangent plane cuts out, doubly, a conic on S. These conics are called "tropes" (one imagines something like the rim of a volcano). We shall denote by C_i the trope lying in singular tangent plane i. In Table 3 the quadratic equations, together with the equations of the plane i, give the C_i.

Equation (1) possesses some obvious symmetries, defined over $\mathbb{Q}$; namely, one can change the sign of any of the variables, or interchange X and Z, or Y and T. Using these symmetries, it is trivial to construct Table 3 once one has spotted one singular tangent plane and calculated the corresponding trope. Moreover, any solution to (1), even if some of the coordinates are negative, gives a solution of the three distance problem, by changing the signs of the negative coordinates, and from any solution of the three distance problem one obtains others by use of the symmetries. We shall therefore only give one representative for each orbit of a solution under the symmetries, and we shall not concern ourselves with possible negative signs in our solutions.

2. - The Néron-Severi group

Let $\tilde{S}$ denote the minimal non-singular model of S. Thus the inverse image on $\tilde{S}$ of each node of S is a non-singular rational curve of self-intersection 2.

In this section we calculate the Néron-Severi group of $\tilde{S}$. Let us first fix some notation. We do not distinguish between a divisor and its class in the Néron-Severi group. The symbol "$\approx$" means algebraic equivalence. If X is any non-singular surface then $NS(X)$, $\rho(X)$, $d(X)$, will denote the Néron-Severi group of X, the rank of $NS(X)$, and the discriminant of $NS(X)$, respectively (when $NS(X)$ is free, the only case we need, $d(X)$ is the determinant of the intersection matrix of a $\mathbb{Z}$-basis of $NS(X)$).

Our strategy is as follows. We first prove, using the double cover of S by an Abelian surface, that $\rho(\tilde{S}) = 19$ and $d(\tilde{S}) = 64$. Then, by studying a pencil of elliptic curves on $\tilde{S}$, we find a set of seventeen curves on $\tilde{S}$ which can be completed to a basis of $NS(\tilde{S})$ by adjoining two curves which generate the free part of the group of sections of the elliptic pencil. A result of Cox [7] then allows us to use our knowledge of $d(\tilde{S})$ to verify that a guess at the two generators is correct. In all this we lean heavily on results of Shioda ([14] and [15]).

Let $p : A \to S$ be the canonical double cover of S by an Abelian surface. We recall that p is ramified over the sixteen nodes of S and that A is the Jacobian of the curve of genus 2 defined as the double cover of any trope ramified over the six nodes on that trope (c.f. [1] Chap. 8).

PROPOSITION 2.1. *$\rho(A) = 3$ and $d(A) = 8$.*

PROOF. We shall get at $NS(A)$ via the classical theory of Riemann matrices and the principal matrices attached to them. The results we need are all in [11].

In fact, we arrive easily at the result that A is isogenous to a product $E \times E$, where E is an elliptic curve without complex multiplication, whence $\rho(A) = \rho(E \times E) = 3$, since ρ is invariant under isogeny. However, the discriminant is not invariant under isogeny, and we could find no quicker way of getting at $d(A)$ than the direct attack via principal matrices.

Before embarking on the explicit calculations, we give a resume of the theory, and explain how one can use the principal matrices to calculate intersection numbers on A.

Let W be a Riemann matrix for A. W is a 2×4 complex matrix whose columns generate a lattice L of $\mathbb{C}^2$ and $A = \mathbb{C}^2/L$. One can replace W by any matrix obtained from W by performing any sequence of elementary row operations and column operations, provided that the column operations correspond to postmultiplying by an element of $GL(4, \mathbb{Z})$.

$NS(A)$ is isomorphic to the additive group of Hermitian forms whose imaginary parts are integral on $L \times L$; in this isomorphism the positive-definite forms correspond to (classes of) ample divisors, while degenerate forms correspond to divisors which are pull-backs via a map from A to an elliptic curve. In matrix terms, the ample divisors correspond, by taking the imaginary part of the corresponding Hermitian form, to non-singular skew-symmetric integer matrices P which satisfy $WP^{-1}W^t = 0$, $-iWP^{-1}\overline{W}^t > 0$; such matrices are called principal matrices (for W). If C is an ample curve on A and P is the corresponding principal matrix then $H^0(A, O_A(C)) = \sqrt{\det P}$; by the Kodaira vanishing theorem, $\chi(A, O_A(C)) = \sqrt{\det P}$ also. On the other hand if P is a singular matrix in the group generated by the principal matrices, then as noted above a corresponding divisor C is supported on fibres of a map from A to a curve, and thus $C^2 = 0$. Riemann-Roch on A then implies $\chi(A, O_A(C)) = 0$. These results allow us to calculate the intersection pairing on $NS(A)$ from principal matrices, via the formula, valid on any non-singular surface A (in our case $\chi(O_A) = 0$, of course),

$$C \cdot C' = \chi(O_A) - \chi(C) - \chi(C') + \chi(C + C'),$$

where we have written $\chi(C)$ instead of $\chi(A, O_A(C))$ etc.

We shall now calculate a Riemann matrix of A. This matrix is, by definition of the Jacobian of a curve, the period matrix $\left(\int_{\gamma_i} \omega_j\right)$ of any curve of which A is the Jacobian, where the ω_j are a basis for differentials of first kind on the curve and the γ_i form a homology basis for the first homology of the curve.

A can be taken to be the Jacobian of a curve C, which is the double cover of trope C_7, ramified over the nodes that lie on this trope. A short computation shows that C has equation

$$y^2 = x(x - 1)(x + 1)(x^2 + 2x - 1).$$

The branch points of $C \to \mathbb{P}^1$ are

$$0,\ 1,\ \infty,\ \alpha = -1 - \sqrt{2},\ \beta = -1 + \sqrt{2},\ \alpha\beta = -1.$$

This type of curve, ramified over 0, 1, ∞, α, β, $\alpha\beta$, always admits degree 2 maps to elliptic curves. Indeed, if constants C_+, C_- are defined by

$$C_\pm = -\frac{(\sqrt{\alpha} \pm \sqrt{\beta})^2}{(1-\alpha)(1-\beta)},$$

then such a curve maps to the elliptic curves E_+, E_-, defined by

$$v^2 = u(1-u)(1-C_\pm u),$$

the explicit formulae being

$$u = \frac{(1-\alpha)(1-\beta)x}{(\alpha - x)(\beta - x)},$$

$$v = \frac{\sqrt{(1-\alpha)(1-\beta)}(x \pm \sqrt{\alpha\beta})}{(\alpha - x)^2(\beta - x)^2} y;$$

we shall denote the maps to E_+ and E_- by π_+ and π_-, respectively. Finally, one has

$$\frac{k + \ell x}{y} dx = \frac{1}{2\sqrt{(1-\alpha)(1-\beta)}} \left\{ \left(\frac{k}{\sqrt{\alpha\beta}} - \ell \right) \pi_+^* \omega - \left(\frac{k}{\sqrt{\alpha\beta}} + \ell \right) \pi_-^* \omega \right\}$$

where ω denotes the differential of first kind $\frac{du}{v}$, on E_+ or E_-. It follows that $\pi_+^*\omega$, $\pi_-^*\omega$ are a basis for the differentials of first kind on C.

A convenient reference for the foregoing classical formulae is [10] Chap. XI.

In our case we find $C_\pm = 1 \mp i$, and calculation shows that E_+ and E_- are isomorphic via the isomorphism induced by $u \mapsto 1 - u$, and the j-invariant of both curves is 2^7. This is not one of the thirteen integer values of j for which the corresponding curve has complex multiplication, so $E_\pm$ do not have complex multiplication. Thus, if $2^7 = j(\tau)$ and $\mathrm{Im}(\tau) > 0$ then τ is transcendental.

In view of the preceding remarks, the period matrix for C can be taken as

$$\begin{pmatrix} \pi_+^*\ \omega(\gamma) \\ \pi_-^*\ \omega(\gamma) \end{pmatrix},$$

where γ runs over a homology basis of C and we have written $\omega(\gamma)$ for $\int_\gamma \omega$, ω a differential form and γ a 1-cycle. This matrix is equal to

$$\begin{pmatrix} \omega(\pi_+\ (\gamma)) \\ \omega(\pi_-\ (\gamma)) \end{pmatrix},$$

so it remains to calculate the effects of $\pi_\pm$ on homology. To this end we take homology bases $\{a_1, a_2, a_3, a_4\}$ on C and $\{\theta_\pm, \eta_\pm\}$ on $E_\pm$ which are liftings of the cycles shown in figs. 2 and 3.

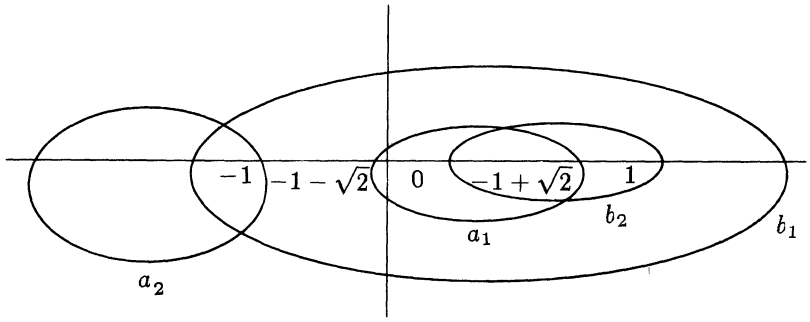


Fig. 2

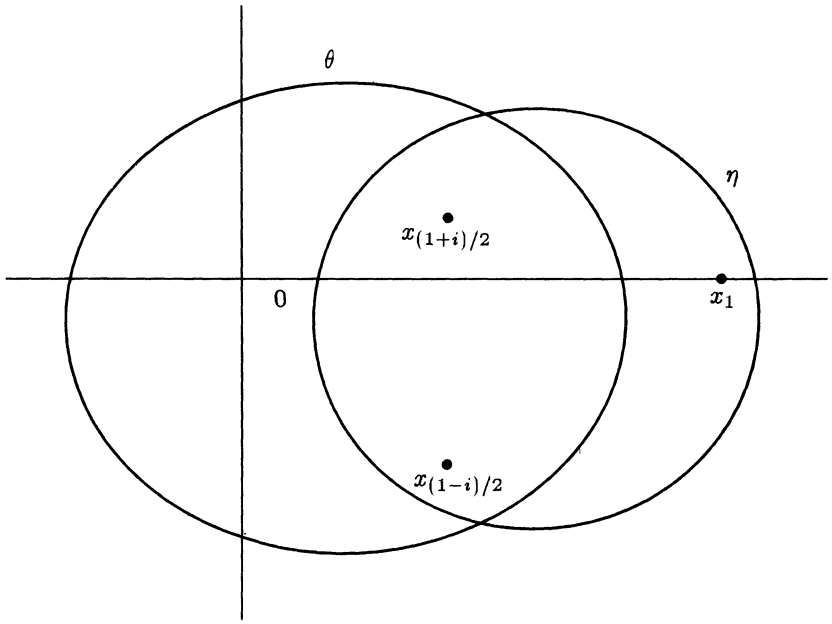


Fig. 3

Now if we introduce the involution $T : C \to C$ defined by

$$T(x) = \frac{\alpha\beta}{x} = \frac{-1}{x}, \qquad T(y) = \frac{iy}{x^3},$$

we find $T(a_1) = -b_1$, $T(a_2) = b_2$ (here "=" means "is homologous to"). Moreover $\pi_+ \circ T = \pi_+$, while $\pi_- \circ T = \sigma \circ \pi_-$, where σ is the sheet- changing involution on E_-. Finally $\pi_+(a_1) = \eta_+$ by a direct calculation. From this we obtain the following table

γ	a_1	$b_1 = -T(a_1)$	a_2	$b_2 = T(a_2)$
$\pi_+(\gamma)$	η_+	$-\eta_+$	θ_+	θ_+
$\pi_-(\gamma)$	η_-	η_-	θ_-	θ_-

hence a period matrix

$$\begin{bmatrix} \omega_+(\eta_+) & -\omega_+(\eta_+) & \omega_+(\theta_+) & \omega_+(\theta_+) \\ \omega_-(\eta_-) & \omega_-(\eta_-) & \omega_-(\theta_-) & -\omega_-(\theta_-) \end{bmatrix}.$$

There is an isomorphism $E_- \to E_+$ induced by $u \to 1 - u$ and sending ω_- to $\sqrt{i}\omega_+$ for a fixed choice of $\sqrt{i}$. In homology this sends $\eta_- \to \theta_+$, $\theta_- \to \eta_+$. We use these to put everything in terms of E_+, and find, after some obvious (and permissible) row and column operations, the matrix

$$\begin{bmatrix} \omega_+(\eta_+) & 0 & \omega_+(\theta_+) & 2\omega_+(\theta_+) \\ \omega_+(\theta_+) & 2\omega_+(\theta_+) & \omega_+(\eta_+) & 0 \end{bmatrix}$$

which reduces to give the period matrix W:

$$\begin{bmatrix} 1 & 0 & \tau & 1/2 \\ 0 & 1 & 1/2 & \tau \end{bmatrix}$$

where $2\tau = \omega_+/\omega_-$. This is a period matrix for C, and so a Riemann matrix for A. We may assume $\mathrm{Im}(\tau) > 0$. We calculate the principal matrices by calculating first their inverses, and find, without difficulty, and using of course the fact that τ is transcendental, that the principal matrices are matrices of the form

$$\begin{bmatrix} 0 & R \\ -R & Q \end{bmatrix},$$

where

$$R = \begin{bmatrix} p & r \\ r & s \end{bmatrix}, \quad Q = \begin{bmatrix} 0 & -(p-s)/2 \\ (p-s)/2 & 0 \end{bmatrix}$$

and p, r, s are integers with $p \equiv s \pmod 2$ and $p > 0$, $\det R > 0$.

$NS(A)$ is isomorphic to the group generated by the principal matrices, and so finally we conclude that $NS(A)$ is isomorphic to the additive group generated by the three matrices

$$\begin{bmatrix} 0 & R \\ -R & Q \end{bmatrix}$$

with Q related to R as above, and

$$R = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

and we recover $\rho(A) = 3$.

Finally, calling the curves, corresponding to the above matrices, C, θ, C' respectively, we use the technique describe at the beginning of the proof to derive the intersection matrix

	C	θ	C'
C	0	2	2
θ	2	2	2
C'	2	2	0

whence $d(A) = 8$ and the proof is finished.

COROLLARY 2.2. $\rho(\tilde{S}) = 19$ *and* $d(\tilde{S}) = 64$.

PROOF. Shioda ([15], Prop. 3.1) has proved

$$\rho(\tilde{S}) = 16 + \rho(A), \quad d(\tilde{S}) = 2^{6-\rho} d(A).$$

We shall now find a set of generators of $NS(\tilde{S})$. We use the following theorem.

THEOREM 2.3. *Let* $f : X \to B$ *be an elliptic fibration, where* X *is a non-singular surface and* B *a non-singular curve.*

Let $\sigma : B \to X$ *be the zero section. Then* $NS(X)$ *is generated by the following curves:*

(a) σ *(i.e.* $\sigma(B)$*. We identify sections and their images on* X*).*

(b) *A non-singular fibre of* f.

(c) *Generators of the group of sections of* f.

(d) *The components of singular fibres of* f *that do not meet* σ.

There are at most two relations, which correspond to generators of the torsion part of the group of sections.

A proof of the theorem and explicit formulae for the relations can be found in Shioda [14], Theorem 1.1 and Cor. 1.5.

It follows from Theorem 2.3 that

$$\rho(X) = r + 2 + \sum_{v \in B} (m_v - 1) \tag{3}$$

where r is the rank of the group of sections and m_v denotes the number of components of $f^{-1}(v)$.

We shall apply the theorem to the elliptic fibration on $\tilde{S}$ which is the proper transform of the pencil of binodal plane quartics cut on S by the pencil of planes which pass through nodes 1 and 2.

Let us fix some more notation. Let $f : \tilde{S} \to \mathbb{P}^1$ be the elliptic pencil, and F a general fibre. Let E_i be the inverse image of node i on $\tilde{S}$. We shall not distinguish in notation between curves on S and their proper transforms on $\tilde{S}$; the context will determine which we mean. In particular, intersections are always to be taken on $\tilde{S}$. Thus, for example, $E_i \cdot E_j = C_i \cdot C_j = -2\delta_{ij}$ (recall the C_i are the tropes) while $E_i \cdot C_j = 1$ or 0 according as i does or does not occur in column j of Table 1 (we use these numbers frequently, whence the utility of Table 1). Finally Q_i denotes the curve (a trinodal quartic on S, but non-singular on $\tilde{S}$) cut out by the plane through nodes 1, 2, and i, for $i = 9, 10, 13, 14$; Q and Q' denote the conics cut out on S by the plane $Y = 0$, and H denotes a general plane section of S. Let us observe that $H \approx F + E_1 + E_2$, and that $H \cdot C = \deg C$, the degree of C in $\mathbb{P}^3$, for any $C \in S$.

Any one of the tropes C_i, which passes through one of nodes 1 and 2 but not both, is a section of f, since by an easy calculation $C_i \cdot F = 1$. We may therefore take C_1 as the zero for the group law on the sections of f. With this choice the other tropes through node 1 but not 2, namely C_6, C_9, C_{13}, are 2-torsion elements in the group of sections. This can be seen, for example, by considering a generic fibre on S; the group law is equivalent to the group on a binodal plane quartic with zero chosen as the point of contact of a tangent drawn from one of the nodes. The elliptic involution is the projection away from this node, and the branch points are the 2-torsion elements.

We may take $\lambda Y + (X - T) = 0$ as the equation of the pencil of planes through nodes 1 and 2, where λ is the parameter. We claim that the singular fibres of f are as shown in Fig. 4. It is easy to show that the given values of λ define singular fibres as shown, and it only remains to show that there are no further singular fibres. This follows from Noether's formula, which in the case of an elliptic pencil, states that the topological Euler-Poincare characteristic of the surface is the sum of the topological Euler-Poincare characteristics of the singular fibres. The Euler-Poincare characteristic of S is $c_2(S) = 24$. Thus we see that a singular fibre occurs when and only when the plane of the fibre passes through a node additional to 1 and 2.

In Fig. 4 the ˜ marks the component of the singular fibre that meets the 0-section, C_1.

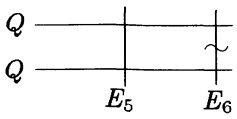
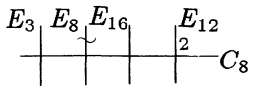
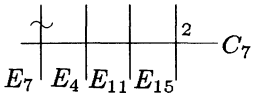
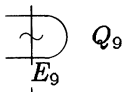
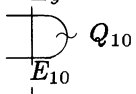
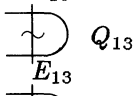
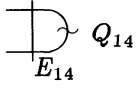
Singularity	Kodaira Name	Euler-Poincaré Characteristic	λ
	I_4	4	∞
	I_0^*	6	-1
	I_0^*	6	1
	I_2	2	$\sqrt{2}-1$
	I_2	2	$-(\sqrt{2}-1)$
	I_2	2	$-(\sqrt{2}+1)$
	I_2	2	$(\sqrt{2}+1)$

Fig. 4

COROLLARY 2.4. *The torsion in the group of sections of f is $\mathbb{Z}/2 \times \mathbb{Z}/2$ and consists of C_1, C_6, C_9 and C_{13}.*

PROOF. The fibre over $\lambda = 1$ is of type I_0^*. The group of non-singular points in a fibre of this type has torsion $\mathbb{Z}/2 \times \mathbb{Z}/2$, and the torsion in the group of sections injects into this group (c.f. Tate's article in [12]). But we have already detected a group $\mathbb{Z}/2 \times \mathbb{Z}/2$ in the group of sections, and the result follows.

Applying formula (3) gives

PROPOSITION 2.5. *The group of sections of f has rank 2.*

Now let us note that the plane $X = Z$ passes through the four nodes 1, 4, 5, 8 and no others, and therefore cuts out a pair of conics on S. Let P be one of these conics. We do not need the equations of P, but we note that it is defined over $\mathbb{Q}(\sqrt{2})$, and not over $\mathbb{Q}$.

PROPOSITION 2.6. *P and C_2 generate the free part of the group of sections of f.*

PROOF. We use the criterion of Cox [7]. This states that sections $s_1, \ldots, s_r$ of an elliptic fibration $f : X \to B$ generate mod. torsion if and only if

$$\det\langle s_i, s_j\rangle = \frac{d(X) \cdot (^{\#}\text{tors})^2}{\prod_{b \in B} m(b)} \tag{4}$$

where $m(b)$ denotes the number of components of multiplicity one in the fibre over $b \in B$, $^{\#}$tors is the order of the torsion subgroup of the group of sections, and $\langle\ ,\ \rangle$ is the Cox pairing whose definition is briefly recalled below. Applying corollaries 2 and 4, we find that the value of the R.H.S. of (4) is $64 \cdot 4^2/(4 \cdot 4 \cdot 4 \cdot 2 \cdot 2 \cdot 2 \cdot 2) = 1$.

The Cox pairing is given by

$$\langle C, C'\rangle = -(C - C_1) \cdot (C' - C_1) - (\text{correction term})$$

where the correction term depends on the intersections of C and C' with the singular fibres. Full details can be found in [7]. We need only the following: the correction term is a sum over singular fibres. If C or C' meets the same component of a fibre as C_1, the zero section, then the contribution to correction is 0; if this does not happen, then the contribution to correction for a fibre of type I_2 is $1/2$, for a fibre of type I_0^* or I_4 is 1, provided C and C' meet the same component of the fibre, and in case that this component does not meet the zero-section.

The intersections of C_2 and P with fibre components are given in Fig. 5.

λ	∞	-1	1	$\sqrt{2}-1$	$-(\sqrt{2}-1)$	$-(\sqrt{2}+1)$	$(\sqrt{2}+1)$
P	E_5	E_8	E_4	Q_9	Q_{10}	Q_{13}	Q_{14}
C_2	E_5	E_8	E_7	Q_9	E_{10}	Q_{13}	E_{14}

Fig. 5

Thus, for example, we compute

$$-\langle P, C_2\rangle = (P - C_1)(C_2 - C_1) + 1 + 0 + 0 + \frac{1}{2} + 0 + \frac{1}{2} + 0 = 0.$$

Similarly $\langle P, P\rangle = 1$, $\langle C_2, C_2\rangle = 1$. Thus the discriminant of the Cox pairing is 1, and the proposition is proved.

REMARK. Computations similar to the above, though easier, show that a generic Kummer has $\rho = 17$, $d = 64$, and C_2 generates the group of sections. This motivates our guess of P as the second generator, since it is a section of a type which does not occur in the generic case. Moreover, if we knew that the discriminant of a Kummer surface were upper semi-continuous under deformations, then we could avoid the tedious explicit computation of $d(\tilde{S})$. We would compute $\rho(\tilde{S})$, make a guess at a basis as above, and then calculate - by machine! - the discriminant of the putative basis. This turns out to be 64 and $d(\tilde{S})$ cannot be less that 64; this being the generic value, it follows $d(\tilde{S}) = 64$ and we have a basis. However, we have not managed to prove - or disprove - the upper semi-continuity of the discriminant.

We now apply Theorem 3 and find the following set of generators for $NS(\tilde{S})$:

$$F, C_1, C_2, P, C_6, C_9, Q, Q', E_5, E_3, E_{16},$$

$$E_{12}, C_8, E_4, E_{11}, E_{15}, C_7, Q_9, E_{10}, Q_{13}, E_{14}.$$

There are two relations:

$$2C_6 \approx 4F + 2C_1 + (\text{components of singular fibres})$$

and a similar expression for C_9. Using Shioda's explicit formulae ([14], Th. 1.1) we find that Q_9 occurs with multiplicity -1 in the relation for C_6, and Q_{13} does not appear in the relation, while, in the relation for C_9, Q_{13} appears with multiplicity -1 and Q_9 does not appear. Thus we can drop Q_9 and Q_{13} and the curves that remain form a free basis for $NS(\tilde{S})$. However, when H is expressed in terms of this basis (a machine calculation) one finds that E_{11} occurs with multiplicity -1. We therefore replace E_{11} by H in our list of basis vectors to obtain:

PROPOSITION 2.7. *$NS(\tilde{S})$ is freely generated by the 19 curves*

$$H, E_3, E_4, E_5, E_{10}, E_{12}, E_{14}, E_{16}, C_1, C_2,$$

$$C_6, C_7, C_8, C_9, Q, Q', F, P, E_{15}.$$

COROLLARY 2.8. *All curves on S have even degree.*

PROOF. Let $G \subseteq NS(\tilde{S})$ be the subgroup generated by the E_i, $F - H$, and $2C - H$, where C is any curve of the basis other than H, F or one of the E_i. Then G is orthogonal to H in the intersection pairing on $NS(\tilde{S})$, and, for any curve D of S,

$$2D \approx nH + g$$

for some $n \in Z$ and $g \in G$. Intersecting both sides with H gives $2D \cdot H = 2 \deg D = 4n$, and the result follows.

This result is well-known for a generic Kummer surface.

THEOREM 2.9. *$NS(\tilde{S}, \mathbb{Q})$, i.e. the subgroup of $NS(\tilde{S})$ of divisors defined over $\mathbb{Q}$, is freely generated by the thirteen curves*

$$H,\ E_3,\ E_4,\ E_5,\ E_{10}+E_{14},\ E_{12}+E_{16},$$

$$C_1,\ C_2,\ C_6,\ C_7,\ C_8,\ Q+Q',\ F.$$

PROOF. $NS(\tilde{S})$ is defined over $\mathbb{Q}(\sqrt{2}, i)$ so take invariants under the Galois group of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$.

The intersection matrix of this basis is given in Fig. 6.

		1	2	3	4	5	6	7	8	9	10	11	12	13
		H	E_3	E_4	E_5	$E_{10}+E_{14}$	$E_{12}+E_{16}$	C_1	C_2	C_6	C_7	C_8	$Q+Q'$	F
1	H	4						2	2	2	2	2	4	4
2	E_3		−2							1		1		
3	E_4			−2						1	1			
4	E_5				−2				1				2	
5	$E_{10}+E_{14}$					−4			2	2				
6	$E_{12}+E_{16}$						−4					2		
7	C_1							−2						1
8	C_2								−2					1
9	C_6									−2				1
10	C_7										−2			
11	C_8											−2		
12	$Q+Q'$												−4	
13	F													

Fig. 6 - Intersection matrix of a basis of $NS(\tilde{S}, \mathbb{Q})$

Let us recall how one uses the Néron-Severi group to find curves of virtual genus 0 and given degree. One forms a subgroup $G' \subseteq NS(\tilde{S}, \mathbb{Q})$ in a manner analogous to the formation of $G \subset NS(\tilde{S})$, and finds, for a curve D defined over $\mathbb{Q}$,

$$2D \approx nH + g, \tag{5}$$

for some $g \in G'$ (Fig. 7 gives the intersection matrix of G').

	1	2	3	4	5	6	7	8	9	10	11	12
	E_3	E_4	E_5	$E_{10}+E_{14}$	$E_{12}+E_{16}$	$2C_1-H$	$2C_2-H$	$2C_6-H$	$2C_7-H$	$2C_8-H$	$Q+Q'-H$	$F-H$
1	−2							2		2		
2		−2						2	2			
3			−2				2				2	
4				−4			4	4				
5					−4					4		
6						−12	−4	−4	−4	−4	−4	−2
7							−12	−4	−4	−4	−4	−2
8								−12	−4	−4	−4	−2
9									−12	−4	−4	−4
10										−12	−4	−4
11											−8	−4
12												−4

Fig. 7 - Intersection matrix of G', an orthogonal of H in $NS(\tilde{S}, \mathbb{Q}) \otimes \mathbb{Q}$

Now, on any K_3 surface, the virtual genus of a divisor D is given by p has $(D) = \frac{D^2}{2} + 1$, so that an irreducible curve has virtual genus 0 if and only if it has self-intersection -2. Thus, the only irreducible curves with negative self-intersection are the non-singular rational curves.

From (5) one obtains, intersecting both sides with D,

$$2D^2 = n \cdot (\deg D) + g \cdot D;$$

while intersecting with g yields $2D \cdot g = g \cdot g$. Thus if D is rational, then

$$-g \cdot g = (\deg D)^2 + 8. \tag{6}$$

By the Hodge index theorem, the intersection pairing restricted to G is negative-definite, so (6) has only a finite number of solutions for any given value of $\deg D$. Each of these solutions corresponds to a divisor of self-intersection -2, and, by Riemann-Roch on $\tilde{S}$, any such divisor of non-negative degree is linearly equivalent to an effective divisor. However this divisor may be reducible. The reducible divisors are detected as follows; if D is reducible, let $D = D_1 + \ldots + D_k$, where the D_i are irreducible, not necessarily distinct. Then, intersecting with D, $-2 = D^2 = \sum_1^k D \cdot D_i$, so that, for at least one index i, $D \cdot D_i < 0$. It follows that $D_i^2 < 0$ (for certainly $D_i \cdot D_j \geq 0$ if $D_j \neq D_i$) so that

D_i is an irreducible curve of virtual genus 0. Thus D is reducible if and only if it has negative intersection number with some irreducible rational curve of lesser degree, and thus one can generate all irreducible curves of virtual genus zero by iteration on the degree.

The above procedure may fail to detect reducible divisors when working over $\mathbb{Q}$. A typical example is given by $C_9+C_{13}+E_1$. This is a reducible divisor defined over $\mathbb{Q}$, of self-intersection -2, and degree 4 but it has non-negative intersection with all $\mathbb{Q}$-rational conics and all E_i; it will not therefore be detected as reducible by the algorithm described in the previous paragraph. The most satisfactory solution to this difficulty would be to work with the full Néron-Severi group and then discard divisors not defined over $\mathbb{Q}$. This is not practical in the present case, unfortunately, as the complexity of solving (6) increases exponentially with the rank of the group G. We adopted the ad hoc device of testing divisors output as solutions of (6) not only against all previously admitted solutions, but also against all the E_i, $1 \leq i \leq 16$, and all conics forming part of a $\mathbb{Q}$-conjugate pair on S. These conics are easy to find, as we explain in the next section. This is enough to make the irreducibility test work in degree ≤ 6, as one sees by considering possible $\mathbb{Q}$-conjugate components of a divisor output by the modified algorithm.

Further difficulties arise when one tries to solve (6) for a given value of $\deg D$. The only feasible method of attack seems to be to diagonalise the quadratic form $-g \cdot g$ over $\mathbb{Q}$, clear denominators, to obtain an equation of the form $\sum a_i x_i^2 = b$, where the a_i and b are positive integers, and to find solutions of this equation by exhaustive search.

For any solution of the diagonalised equation, one must first check that it corresponds to an integral solution of (6), and then test for irreducibility; all this is extremely time-consuming, which makes the procedure impracticable for values of $\deg D$ larger than eight and for G of high rank. I owe to the referee the following suggestion. For our purpose it is only necessary to look at those divisors whose degree is not decreased by projection away from a rational node (the others are obtained by projecting curves of lower degree from nodes, c.f. §3). This provides a set of linear inequalities which narrows the search region considerably.

A final difficulty is that there is no good algorithm for diagonalising the quadratic form; naively completing the square leads to very large denominators. For the form $g \cdot g = \sum a_{ij} x_i x_j$ whose matrix (a_{ij}) is given in Fig. 7, we obtain, by luck more than judgement, the diagonalisation

$$\begin{aligned} -g \cdot g = {} & 2(x_1 - x_8 + x_{10})^2 + 2(x_2 - x_8 - x_9)^2 + 2(x_3 - x_7 - x_{11})^2 \\ & + 4(x_4 - x_7 - x_8)^2 + 4(x_5 - x_{10})^2 + 4x_6^2 + 2(x_6 + x_7 + x_9)^2 \\ & + (x_6 - x_7 + x_8)^2 + 4x_9^2 + 2(x_6 + x_7 + x_{10})^2 + 2(x_6 + x_8 + x_{11})^2 \\ & + (x_6 + x_7 + x_8 + 2x_9 + 2x_{10} + 2x_{11} + 2x_{12})^2. \end{aligned}$$

Finally, we observe that our algorithm finds curves of virtual genus 0 on

$\tilde{S}$, i.e. it finds the non-singular rational curves (c.f. [4]). It does not find the possible singular rational curves of $\tilde{S}$, as these have positive virtual genus.

3. - The three distance problem

Our knowledge of the three distance problem is summed up in the following two theorems.

THEOREM 3.1. *The curves given in Table* 4 *(see Appendix) are parametrized curves on* S. *Up to symmetry, there are no further parametrizable curves on* S *of degrees* 2 *or* 4.

THEOREM 3.2. *Infinitely many parametrizable curves can be obtained starting from* C_2, *by successive projections from nodes* 1 *and* 2.

Before giving the proofs of these theorems we show how Table 4 was obtained, and describe the results of applying the algorithm of Section 2. Of course one can verify by direct computation that the parametrized curves of Table 4 do indeed lie on S.

The conic of Table 4 is the trope C_7. The quartic is the section of S by the plane $2T = X+Z$. This plane passes through the nodes 1, 3, 7 and no others and so cuts out on S a three-nodal plane quartic. Three-nodal quartics have geometric genus zero. To be parametrizable our curve must have a non-singular $\mathbb{Q}$-rational point. We find (1, 4, 5, 3) is such a point (the reader is invited to locate this point in the plane of Fig. 1). We may then parametrize the curve by the classical method of taking the pencil of conics through the three nodes and the rational point. There remains just one free intersection of a conic of the pencil with the quartic, whose coordinates must be rational functions of the parameter of the pencil, whence the parametrization.

The conics and three-nodal quartics provide the obvious curves of geometric genus zero on S (there are in fact eight parametrizable three-nodal quartics but they form a single orbit under the symmetries). To find others, we project known curves away from nodes. This means the following: projection away from a node N is the map that sends $P \in S$ to the fourth point of intersection of the line PN with S. This defines an involutory birational self-transformation of S which induces a biregular self-transformation of $\tilde{S}$. All nodes other than N are fixed, and N itself is blown up into the intersection of the Zariski tangent cone at N with S. The sextic of Table 4 is the projection of the trope C_7 from node 5, while the octavic is the intersection of the Zariski tangent cone at node 1 with S.

We now turn to the algorithm of section 2, to search for curves of virtual genus zero on $\tilde{S}$. A computer implementation found only the tropes $C_1 \ldots C_8$ in degree 2, and the (proper transforms of the) three-nodal quartics in degree 4 (we

note that up to symmetry this gives just one conic and one three-nodal quartic). However, in degree 6, the algorithm finds not only the 32 sextics obtained by projecting parametrizable tropes from nodes, but also 24 new sextics. These sextics, to be parametrizable, must have a non-singular $\mathbb{Q}$-rational point. The algorithm of course outputs curves as integer-linear combinations of the basis of the Néron-Severi group. This allows one to calculate intersection numbers. Calculating intersections with the E_i, $i = 1, \ldots, 8$, one finds that every one of the 24 sextics has intersection number 1 with precisely 4 of the E_i. This means that the curve passes simply through the corresponding node, and we have our non-singular $\mathbb{Q}$-rational point. For example, one of the sextics is given as $(3\ -2\ -2\ 0\ -5\ 1\ 2\ -4\ -6\ 2\ 3\ 2\ -2)$ and has intersection number 1 with E_i, $i = 1, 2, 3, 8$.

We have not parametrized these sextics. One method of doing so would be to project from a node through which a sextic passes onto a plane. The image of the sextic is a plane quintic whose equation can be found. Another method, suggested by the referee, would be to find a pencil of elliptic curves whose general curve has intersection number 1 with the sextic. This is a computation in $NS(\tilde{S})$ similar to those already described. From this a parametrization of the sextic can be deduced by straighforward manipulations on the generic curve of the pencil.

Since we are leaning so heavily on a computer program, it is perhaps worth mentioning that it is easy to find all the conics on S. This provides a slight check on the correctness of the program. In fact, any conic of S must pass through at least four nodes; if not, its inverse image on the Abelian surface A would be rational, and an Abelian variety cannot contain any rational variety. Thus one has only to search for sets of four coplanar nodes of S. One finds only the singular tangent planes and (the orbits under the symmetries of) the planes $X = Z$, $Y = 0$. Thus the only conics on S defined over $\mathbb{Q}$ are the tropes C_i, $i = 1 \ldots 8$, verifying the result of the computer program.

We now turn to the proofs of 3.1 and 3.2.

PROOF OF THEOREM 3.1. As already stated, the algorithm of Section 2 yields only tropes and proper transforms of three-nodal quartics as curves on $\tilde{S}$ of virtual genus zero of degrees 2 and 4. These are orbits under the symmetries of the conic and quartic of Table 4. However, there remains the possibility of a rational curve of positive virtual genus. Such a curve remains singular on $\tilde{S}$. Conics are non-singular, so the only case to consider is that of a singular rational quartic on S whose proper transform is singular on $\tilde{S}$. We leave to the reader the task of excluding the plane quartics, and now show that, while space quartics with these properties do exist on S, none is defined over $\mathbb{Q}$.

It is well-known that a space quartic, either has virtual genus 0, in which case it is certainly non-singular, or it has virtual genus 1, is the complete intersection of two quadrics, and may have a unique singular point. We are therefore led to consider elliptic quartics on S. By Riemann-Roch any such curve moves in a pencil; thus a singular space quartic on S is a singular fibre

of a pencil of elliptic quartics on S. We use the Néron-Severi group to find all classes of elliptic quartics on $\tilde{S}$; i.e. we use our algorithm to find divisors of degree 4 and self-intersection 0. It turns out that, as well as the 32 pencils of plane elliptic curves cut out by planes through pairs of nodes, there are 14 other elliptic pencils on S, defined over $\mathbb{Q}$. These fall into five orbits under the symmetries. Representatives of these orbits are the linear systems

$$|C_2 + C_6 + E_{10} + E_{14}|, \ |C_9 + C_{13} + E_1 + E_5|, \ |C_1 + C_6 + E_1 + E_6|,$$
$$|C_2 + C_8 + E_2 + E_8|, \ |C_1 + C_8 + E_1 + E_8|.$$

The first two are invariant under the symmetries, the remainder belong to orbits of four elements apiece. Each defines an elliptic pencil on S which certainly has singular fibres, and our affirmation is that no irreducible singular fibre is defined over $\mathbb{Q}$. This is established by finding equations for each elliptic pencil. In fact, for each pencil we can find quadrics $Q_1(\lambda)$ and $Q_2(\lambda)$, depending on $\lambda \in \mathbb{P}_1$ such that the curves of the pencil are given by $Q_1(\lambda) \cap Q_2(\lambda)$. It is known that a space quartic given as the complete intersection of two quadrics $Q_1 = 0$ and $Q_2 = 0$ is singular if and only if the quartic in t, $\det(Q_1 + t\,Q_2)$ has repeated roots, and so we can determine the singular fibres of the pencil from the discriminant of this polynomial.

Consider for example the third pencil of the list. Calculating intersections with the E_i we find that the pencil has on S eight base points, namely nodes 3, 4, 7, 8, 9, 10, 13, 14. We find also that the divisor $C_2 + C_5 + E_2 + E_5$ is a reducible fibre. The eight nodes are the basepoints of a net of quadrics with basis $T_1T_6 = 0$, $T_2T_5 = 0$, $F = 0$, where $T_i = 0$ is the equation of singular tangent plane i, and F is $Y^2 - X^2 + T^2$. Now $F = 0$ intersects S in $C_1 + C_2 + C_5 + C_6$, so that the pencil of quadrics $T_1T_6 + \lambda F = 0$ has $C_1 + C_6$ as base divisor. This pencil of quadrics cuts out on S, residual to $C_1 + C_6$, a pencil of quartics which contains in particular $C_1 + C_6$ (for $\lambda = 0$) and $C_2 + C_5$ (for $\lambda = \infty$). It therefore cuts out the elliptic pencil under consideration. Similarly, $T_2T_5 + \mu F = 0$ cuts out, residual to $C_2 + C_5$, the same pencil. This defines a projective correspondance between λ and μ; namely, any value of λ determines a curve of the pencil and this determines a corresponding μ. The pairs $(0, \infty)$, $(\infty, 0)$, $(\sqrt{2} + 1, \sqrt{2} - 1)$ correspond in this projectivity, (the last pair comes from considering the curve of the pencil through node 11). We conclude that the projectivity is $\lambda\mu = 1$ and any member of our elliptic pencil is the complete intersection of the quadrics $Q_1(\lambda) = T_1T_6 + \lambda F = 0$, $Q_2(\lambda) = \lambda T_2T_5 + F = 0$, for a unique $\lambda \in \mathbb{P}_1$. Thus the singular fibres of the pencil are given by those values of λ for which $\det(Q_1 + t\,Q_2) = 0$ has repeated roots. A calculation yields $\det(Q_1 + t\,Q_2) = (t+\lambda)((\lambda-1)t + \lambda + 1)(\lambda t^2 + (\lambda^2 - 4\lambda - 1)t - \lambda)$ and the discriminant of this quartic in t is

$$\lambda^4(\lambda^2 - 2\lambda - 1)^2(\lambda^4 - 4\lambda^3 - 6\lambda^2 + 4\lambda + 1)^2((\lambda^2 - 4\lambda - 1)^2 + 4\lambda^2).$$

One sees rational roots only at $0, \infty$. Thus the only singular fibres of

$|C_1 + C_6 + E_1 + E_6|$ defined over $\mathbb{Q}$ are the reducible singular fibres which we already know about, and we are done. The remaining elliptic pencils are dealt with similarly, though the computations for the last two on the list are difficult and we were obliged to use REDUCE.

The proof of Theorem 3.1 is now complete.

PROOF OF THEOREM 3.2. Projection from node 2 followed by projection from node 1 induces, in the group of sections of the elliptic pencil studied in Section 2, a map which is just translation by the section C_2. This is easily seen by considering the group law on the generic fibre. But, by Corollary 2.4, C_2 is an element of infinite order in the group of sections, and Theorem 3.2 follows.

Perhaps it is worth noting that the proof of Theorem 3.2 only uses the fact that C_2 has infinite order in the group of sections, and not the more difficult result that it is in fact a generator of the group.

REMARK. The surfaces considered in [2], [3], and [16], have the property that there exist a finite set of parametrizable curves and a finitely generated group of automorphisms of the surface, such that every parametrizable curve on the surface can be obtained from the given set of parametrizable curves by means of an automorphism of the group. In our case, however, in view of the abundance of parametrizable curves on S of degree 6, and also of degree 8, (though we have not completely analysed this latter case), it seems unlikely that any such result holds.

4. - The four distance problem

The equations (1) and (2) of the introduction, taken together, define a surface R in the space $\mathbb{P}^5$ of homogeneous coordinates (X, Y, Z, T, U). R is a double cover of S by projection onto $U = 0$, and the rational points of R, if any, are the solutions of the four distance problem.

Let $\pi : R \to S$ denote the projection, so $\pi(X, Y, Z, T, U) = (X, Y, Z, T)$. The branch locus of π is evidently the intersection of the quadric

$$X^2 - Y^2 + Z^2 = 0$$

with S. Let B denote this branch locus.

PROPOSITION 4.1. *$B = B_1 + B_2$, where B_1 and B_2 are elliptic quartics conjugate over $\mathbb{Q}$ and defined over $\mathbb{Q}(i)$, which intersect each other in the eight points* $(\pm 1, \pm\sqrt{2}, \pm 1, \pm 1)$.

PROOF. Substitute $X^2 + Z^2$ for Y^2 in (1) and factorize. The equations of

B_1 and B_2 turn out to be

$$B_1 : X^2 - Y^2 + Z^2 = 0, \qquad iX^2 + Z^2 - (1+i)T^2 = 0$$
$$B_2 : X^2 - Y^2 + Z^2 = 0, \quad -iX^2 + Z^2 - (1-i)T^2 = 0$$

and it is well-known that the complete intersections of two quadrics is an elliptic quartic.

COROLLARY 4.2. *R is a regular surface of general type, of geometric genus* 5, *and with only ordinary nodes as singularities.*

PROOF. This follows from the standard theory of double covers, (c.f. [13]); we have $2H \equiv B$, so that $h^i(R, \underline{O}_R)$ is given by $h^i(S, \underline{O}_S) + h^i(S, O_S(-H))$, $0 \leq i \leq 2$.

The only singularities of B are the intersections of B_1 and B_2, which are transversal as is easy to verify, so the only singularities of R are nodes lying over the singularities of B and also nodes lying in pairs over the singularities of S. Because the singularities are rational we may apply the formula $K_R \equiv \pi^*(K_S+H)$ for the canonical class of the double cover, and conclude $K_R = \pi^*(H)$, so that K_R is ample and R is therefore of general type, and is canonically embedded in $\mathbb{P}^5$.

Unfortunately there is no Diophantine Theory of surfaces of general type. It does not even seem to be known whether a regular surface of general type can carry infinitely many rational curves (an irregular surface cannot because of the Albanese map), so that Corollary 4.2 does not even exclude the possibility of infinitely many one parameter families of solutions to the four-distance problem! Our only general result is the following.

PROPOSITION 4.3. *There is no irreducible rational curve on R of the form π^*C, where C is one of the rational curves on S generated from rational conics and quartics by the prescription of Theorem* 3.2.

PROOF. Suppose there were such a curve $C' = \pi^*C$. Then $\pi|C' : C' \to C$ has at most two branch points, since C' is rational, which, since C' is non-singular except possibly at nodes of R, must occur at transversal intersections of C with B. The remaining intersections of C with B must occur at nodes of B. Now C is defined over $\mathbb{Q}$ while B_1 and B_2 are interchanged by complex conjugation. It follows that $C \cdot B_1 = C \cdot B_2$. Moreover C is non-singular at non-singular points of S; we conclude that if C passes through a node of B it cannot be tangent to either B_1 or B_2 there, for if it were it would be tangent to both B_1 and B_2 and thus singular. Therefore if C passes through a node of B the intersection multiplicity of C and B at the node is 2. Hence

$$C \cdot B = 2 \cdot (\text{number of nodes of } B \text{ through which } C \text{ passes}) + b$$

where b, the number of branch points of $C' \to B$, is 0 or 2.

On the other hand we have $2H \equiv B$ so that $B \cdot C = 2 \deg C$.

Thus $\deg C$ = (number of nodes of B through which C passes) $+b/2$. Since B has eight nodes, and C has even degree, we conclude $\deg C \leq 8$. But now one verifies, quite explicitly, using the equations given in §3, that the curves of degrees 2, 6, 8 of Table 5 (and curves obtained from them by the symmetries) do not pass through any node of B, while curves of degree 4 pass through at most two nodes. Thus for all these curves $b \geq 4$ so that C' cannot be rational and the proof is complete.

For degrees 2 and 4 we find far better results.

PROPOSITION 4.4. *The one-parameter families of degree* 2 *and* 4 *of solutions of the three-distance problem do not contain any solution of the four-distance problem.*

PROOF. In degree 2, trope C_7 gives a solution of the four-distance problem if and only if

$$U^2 = X^2 - Y^2 + Z^2, \qquad Z^2 = (X+Y)^2 + Y^2$$

have a simultaneous solution, and it is already noted in [8] that they do not. Similarly for the other rational tropes.

In degree 4, we substitute the parametrization in equation (2) and obtain

$$U^2 = (t^2 - 8)^2(2 \cdot 5 \cdot t^4 - 2^7 \cdot t^3 + 2^5 \cdot 19t^2 - 2^{10}t + 5 \cdot 2^7).$$

The quadratic factor occurs because the degree 4 curve passes through the nodes $(1, \pm\sqrt{2}, 1, 1)$ of B. This seems promising, but it is entirely elementary to show that there is no rational solution!

Substitute $t = 2^k \frac{p}{q}$, where p and q are odd integers, and clear denominators. One sees immediately that there is no value of $k \in \mathbb{Z}$ which makes it possible for both sides of the resulting equation to be divisible by the same power of 2. This completes the proof.

The sextic of Table 5 gives, on substituting in (2).

$$U^2 = t^{12} - 4t^{11} - 62t^{10} + 68t^9 + 1647t^8 + 4184t^7 + 2716t^6$$
$$- 376t^5 + 623t^4 - 788t^3 + 194t^2 - 12t + 1.$$

The R.H.S. of this equation is square-free, as one sees by reducing mod 3. The curve is of genus 5. A small scale computer search did not find any rational points except $t = 0$, $U = \pm 1$, but we have not proved anything.

The above and a similar calculation in degree 8 seem to show that what one expects to happen on R actually does happen, namely, that rational curves on S meet B transversally and away from nodes of B, so that the inverse images of these curves have high genus on R. One does not expect to find rational points on curves of high genus. This lends some weight to the conjecture that the four distance problem has no solution, though the algebro-geometric techniques of this paper are unlikely to yield a proof.

Appendix

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
13	14	15	16	9	10	11	12	5	6	7	8	1	2	3	4
8	7	6	5	4	3	2	1	16	15	14	13	12	11	10	9
7	8	5	6	3	4	1	2	15	16	13	14	11	12	9	10
6	5	8	7	2	1	4	3	14	13	16	15	10	9	12	11

Table 1 - The 16_6 *Configuration*

1.	(1	0	1	1)	9.	($\sqrt{2}$	-1	0	1)
2.	(1	0	-1	1)	10.	($\sqrt{2}$	1	0	1)
3.	(1	1	-1	0)	11.	(0	1	$-\sqrt{2}$	1)
4.	(1	-1	1	0)	12.	(0	-1	$\sqrt{2}$	1)
5.	(1	0	1	-1)	13.	($\sqrt{2}$	1	0	-1)
6.	(-1	0	1	1)	14.	($-\sqrt{2}$	1	0	1)
7.	(-1	1	1	0)	15.	(0	1	$\sqrt{2}$	1)
8.	(1	1	1	0)	16.	(0	1	$\sqrt{2}$	-1)

Table 2 - The nodes of S

1.	Z	$=$	$Y+T$	;	$X^2=Y^2+T^2$
2.	Y	$=$	$Z+T$	;	$X^2=Y^2+T^2$
3.	Y	$=$	$X+T$	;	$Z^2=Y^2+T^2$
4.	$-Y$	$=$	$X+T$	;	$Z^2=Y^2+T^2$
5.	$-Y$	$=$	$Z+T$	;	$X^2=Y^2+T^2$
6.	T	$=$	$Z+Y$	;	$X^2=Y^2+T^2$
7.	T	$=$	$X+Y$	;	$Z^2=Y^2+T^2$
8.	X	$=$	$Y+T$	;	$Z^2=Y^2+T^2$
9.	Z	$=$	$X+\sqrt{2}Y$	;	$T^2=X^2+Y^2+\sqrt{2}XY$
10.	$\sqrt{2}Y$	$=$	$X+Z$	;	$T^2=X^2+Y^2-\sqrt{2}XY$
11.	$-\sqrt{2}T$	$=$	$X+Z$	;	$Y^2=X^2+T^2-\sqrt{2}XT$
12.	Z	$=$	$X+\sqrt{2}T$	;	$Y^2=X^2+T^2+\sqrt{2}XT$
13.	X	$=$	$Z+\sqrt{2}Y$	;	$T^2=X^2+Y^2-\sqrt{2}XY$
14.	$-X$	$=$	$Z+\sqrt{2}Y$	;	$T^2=X^2+Y^2+\sqrt{2}XY$
15.	$\sqrt{2}T$	$=$	$X+Z$	;	$Y^2=X^2+T^2-\sqrt{2}XT$
16.	X	$=$	$Z+\sqrt{2}T$	;	$Y^2=X^2+T^2-\sqrt{2}XT$

Table 3 - Singular tangent planes of S, and corresponding tropes

Degree 2.	$X=$	$t^2+2t-1,$
	$Y=$	$1-t^2,$
	$Z=$	$t^2+1,$
	$T=$	$X+Y$
Degree 4.	$X=$	$5t^4-48t^3+144t^2-128t+64$
	$Y=$	$4t^4-48t^3+192t^2-384t+256$
	$Z=$	$t^4-16t^3+144t^2-384t+320$
	$T=$	$\frac{1}{2}(X+Z)$
Degree 6.	$X=$	$t^6+6t^5+29t^4+44t^3-13t^2-2t-1$
	$Y=$	$t^6+12t^5+21t^4-16t^3-21t^2+4t-1$
	$Z=$	$t^6+4t^5+7t^4+24t^3+39t^2-12t+1$
	$T=$	$10t^5+40t^4+28t^3-24t^2+10t$
Degree 8.	$X=$	$t^8-8t^7+12t^6+24t^5-10t^4-24t^3+12t^2+8t+1$
	$Y=$	$8t^7-16t^6-8t^5-8t^3+16t^2+8t$
	$Z=$	$t^8+12t^6-32t^5-10t^4+32t^3+12t^2+1$
	$T=$	$t^8-4t^6+22t^4-4t^2+1$

Table 4 - Parametrizable curves of degree ≤ 8

REFERENCES

[1] A. BEAUVILLE, *Surface Algébriques Complexes*. Astérisque **54**, 1978.

[2] S.A. BREMNER, *Pythagorean triangles and a quartic surface*. J. Reine Angew. Math. **318**, 1980, 120-125.

[3] S.A. BREMNER, *A geometric approach to equal sums of fifth powers*. J. Number Theory **13**, 1981, 337-354.

[4] S.A. BREMNER, *A geometric approach to equal sums of sixth powers*. Proc. London Math. Soc. **43**, 1981, 544-581.

[5] S.A. BREMNER - R.K. GUY, *The delta-lambda configurations in tiling the square*. J. Number Theory **32**, 1989, 263-280.

[6] A. CAYLEY, *Collected Papers*. Vol. 10. CUP Cambridge, 1898.

[7] D.A. COX, *Solutions of Weierstrass equations*. Algebraic Geometry, Proceedings, Copenhagen 1976. Springer Lecture Notes in Mathematics **732**, 43-59. Springer Verlag, Berlin 1976.

[8] R.K. GUY, *Unsolved Problems in number theory*. Springer Verlag, Berlin 1981.

[9] R.K. GUY, *Tiling the square with rational triangles*. Acta Arithmetica. To appear.

[10] A. KRAZER, *Lehrbuch der Thetafunctionen*. Chelsea, N.Y. 1970.

[11] S. LANG, *Introduction to algebraic and Abelian functions*. Springer Verlag, Berlin 1982.

[12] S. LANG, *Modular Functions of one variable IV*. Springer Lecture Notes in Mathematics **732**. Springer Verlag, Berlin 1978.

[13] U. PERSSON, *Double coverings and surfaces of general type*. Algebraic Geometry Proceedings, Tromso, Norway, 1977. Springer Lecture Notes in Mathematics **687**. Springer Verlag, Berlin 1979.

[14] T. SHIODA, *On Elliptic Modular Surfaces*. J. Mat. Soc. Japan, **24**, 1972, 20-59.

[15] T. SHIODA, *Supersingular K_3 surfaces*. Algebraic Geometry, Proceedings, Copenhagen 1976. Springer Lecture Notes in Mathematics **732**, 544-591. Springer Verlag, Berlin 1976.

[16] H.P.F. SWINNERTON-DYER, *Applications of Algebraic Geometry to Number Theory*. Proc. Symp. Pure Math. **20**, AMS, Providence, Rhode Island, 1970.

Departamento de Matemáticas
y Ciencia de la Computación
Universidad Simón Bolívar
Caracas, Venezuela