Indag. Mathem., N.S., 11 (3), 419–435 September 25, 2000

# A singular $K3$ surface related to sums of consecutive cubes

by Masato Kuwata and Jaap Top

*Département de Mathématiques, Université de Caen, B.P. 5186, F-14032 Caen Cedex, France*
*e-mail: kuwata@math.unicaen.fr*
*Vakgroep Wiskunde Rijks Universiteit Groningen, P.O. Box 800, 9700 AV Groningen, the Netherlands*
*e-mail: top@math.rug.nl*

Communicated by Prof. R. Tijdeman at the meeting of March 27, 2000

## 1. INTRODUCTION

The well known formula

$$1^3 + 2^3 + \ldots + k^3 = (k(k+1)/2)^2$$

shows in particular that the sum of the first $k$ consecutive cubes is in fact a square. A lot of related diophantine problems have been studied. For instance, Stroeker [Str] considered the question, for which integers $m > 1$ one can find non-trivial solutions of $m^3 + (m+1)^3 + \ldots + (m+k-1)^3 = \ell^2$. In particular he found all solutions with $1 < m < 51$ and with $m = 98$. Several authors considered the question of finding sums of consecutive squares which are themselves squares; see, e.g., [P-R] and references given there. In our paper [K-T] we considered this problem from a geometric point of view by exploiting a connection between solutions and rational points on the rational elliptic surface given by $6y^2 = (x^3 - x) - (t^3 - t)$.

Here we present a similar treatment of the equation

$$(1.1) \qquad m^3 + (m+1)^3 + (m+2)^3 + \ldots + (m+k-1)^3 = l^3.$$

It turns out that (1.1) determines a so-called singular $K3$ surface. Although our emphasis will be on geometric and arithmetic algebraic properties of this surface, we will note some consequences for the diophantine equation. In particular, we show that infinitely many non-trivial solutions exist; a result that was

already known to C. Pagliani in 1829/30. Pagliani's solutions can be regarded as points on a rational curve in the $K3$ surface.
By putting

$$(1.2) \qquad x = k, \qquad y = 2m + k - 1, \qquad z = 2l,$$

the equation eq.mkl becomes

$$(1.3) \qquad xy(x^2 + y^2 - 1) = z^3.$$

This equation (1.3) determines an algebraic surface in the affine space $\mathbb{A}^3$. We consider the projective model of it, given by

$$S_0 : \{(X : Y : Z : W) \mid XY(X^2 + Y^2 - W^2) = Z^3 W\} \subset \mathbb{P}^3.$$

This surface has some singular points. Denote by $S$ the minimal non-singular model of $S_0$. We will show that the surface $S$ is a $K3$ surface whose Picard number is 20, which is maximal for a $K3$ surface defined over a field of characteristic 0. Such $K3$ surfaces with maximal Picard number have been classified by Shioda and Inose [S-I].

In sections 2 and 3 we study geometric properties of the surface $S$. We construct some elliptic fibrations on it and determine the Néron-Severi group of $S$. Moreover, we find the Shioda-Inose class of this surface. It turns out that he elliptic fibrations we construct, do not have sections which would produce infinitely many non-trivial solutions to the original diophantine equation. In section 4 we describe a base change of one of the elliptic pencils. Using this, we do find infinitely many non-trivial solutions to (1.1). It turns out that precisely the same solutions already appeared in 1829/30 in work of C. Pagliani.
Section 5 gives a description of the surface $S$ and the base change we present, in terms of the product of two curves. This is used in section 6 to determine the Hasse-Weil zeta function of $S$ over $\mathbb{Q}$.

## 2. ELEMENTARY PROPERTIES OF $S_0$

### 2.1. Symmetry

The original diophantine problem asks for solutions to (1.1) in *positive* integers. This restriction, however, is not an essential one. For example, $(m, k, l) = (-2, 8, 6)$ is a solution to eq.mkl. Then, observing

$$\underbrace{(-2)^3 + (-1)^3 + 0^3 + 1^3 + 2^3}_{0} + 3^3 + 4^3 + 5^3 = 6^3,$$

we find another solution $(m, k, l) = (3, 3, 6)$ corresponding to $3^3 + 4^3 + 5^3 = 6^3$. This reflects an instance of the action of a certain group of symmetries on the set of solutions; one can always find a nonnegative solution in the orbit of a solution. These symmetries are conveniently described in terms of the co-

ordinates introduced in (1.2). There are obvious involutions acting on (1.3), namely

$$\tau_1 : (x, y, z) \longmapsto (-x, y, -z),$$
$$\tau_2 : (x, y, z) \longmapsto (x, -y, -z),$$
$$\tau_3 : (x, y, z) \longmapsto (y, x, z).$$

These involutions generate a group of order 8, which is isomorphic to the dihedral group $D_4$. The symmetry may be seen clearly in Figure 1.

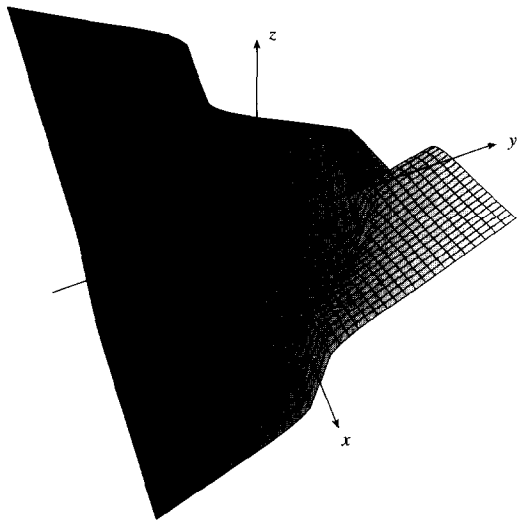


Figure 1

6

It is easy to see that $(m, k, l)$ is an integral solution to (1.1) if and only if $(x, y, z)$ is an integral solution to (1.3) such that $x$ and $y$ have different parity.

The surface $S_0$ admits another automorphism given by

$$\tau_4 : (x, y, z) \mapsto (x, y, \omega z),$$

where $\omega$ is a primitive third root of unity. We see that $\tau_4$ commutes with $\tau_1$, $\tau_2$ and $\tau_3$, and thus $\tau_1, \ldots, \tau_4$ forms a group isomorphic to $D_4 \times C_3$, where $C_3$ is the cyclic group of order 3. It is not difficult to see that these are the only automorphisms of $S_0$ induced from those of $\mathbb{P}^3$.

### 2.2. Singularities

The surface $S_0$ has the following five singular points

$$(X : Y : Z : W) = (0 : 0 : 0 : 1),\ (\pm 1 : 0 : 0 : 1),\ (0 : \pm 1 : 0 : 1),$$

all of whom are rational double points. These are the only singularities of $S_0$. Hence by the following result one concludes that the minimal non-singular model $S$ of $S_0$ is a $K3$ surface.

**Proposition 2.1.** [P-T-vdV, Proposition 2.1] *Any surface which is the minimal*

*resolution of singularities of a surface given by a degree four equation in projective 3-space with at most rational double points as singularities, is a K3 surface.*

Note that all of the singularities of $S_0$ are of type $A_2$, and thus the fibre of $S \to S_0$ above each singular point consists of two rational curves. This can be seen directly, but it also follows from the results in the next section since the resolution of singularities is built-in in Tate's algorithm for determining the singular fibers of an elliptic pencil.

### 2.3. Lines contained in $S_0$

The surface $S_0$ contains the following lines:

$$\ell_1 : \begin{cases} X = 0 \\ Z = 0 \end{cases} \qquad \ell_2 : \begin{cases} Y = 0 \\ Z = 0 \end{cases} \qquad \ell_3 : \begin{cases} X = 0 \\ W = 0 \end{cases}$$

$$\ell_4 : \begin{cases} Y = 0 \\ W = 0 \end{cases} \qquad \ell_5 : \begin{cases} X = iY \\ W = 0 \end{cases} \qquad \ell_6 : \begin{cases} X = -iY \\ W = 0 \end{cases}$$

$$\ell_7 : \begin{cases} X = W \\ Y = Z \end{cases} \qquad \ell_8 : \begin{cases} X = W \\ Y = \omega Z \end{cases} \qquad \ell_9 : \begin{cases} X = W \\ Y = \omega^2 Z \end{cases}$$

$$\ell_{10} : \begin{cases} X = -W \\ Y = -Z \end{cases} \qquad \ell_{11} : \begin{cases} X = -W \\ Y = -\omega Z \end{cases} \qquad \ell_{12} : \begin{cases} X = -W \\ Y = -\omega^2 Z \end{cases}$$

$$\ell_{13} : \begin{cases} Y = W \\ X = Z \end{cases} \qquad \ell_{14} : \begin{cases} Y = W \\ X = \omega Z \end{cases} \qquad \ell_{15} : \begin{cases} Y = W \\ X = \omega^2 Z \end{cases}$$

$$\ell_{16} : \begin{cases} Y = -W \\ X = -Z \end{cases} \qquad \ell_{17} : \begin{cases} Y = -W \\ X = -\omega Z \end{cases} \qquad \ell_{18} : \begin{cases} Y = -W \\ X = -\omega^2 Z. \end{cases}$$

The group of symmetries generated by $\{\tau_1, \ldots, \tau_4\}$ acts on this set of lines. It divides the set into four orbits: $\{\ell_1, \ell_2\}$, $\{\ell_3, \ell_4\}$, $\{\ell_5, \ell_6\}$ and $\{\ell_7, \ldots, \ell_{18}\}$. With the aid of the description of the Néron-Severi group of $S$ in terms of an elliptic fibration, one can in fact show that these are the only lines contained in $S_0$. However, we will not need this in the sequel.

## 3. ELLIPTIC FIBRATIONS ON $S$ AND THE NÉRON-SEVERI GROUP

By regarding $y$ as a constant in (1.3), one obtains a plane cubic curve in the $xz$-plane. It is easy to see that these cubic curves are nonsingular except for finitely many values of $y$. This implies that the map $S_0 \to \mathbb{A}^1$ given by $(x, y, z) \mapsto y$ determines an elliptic fibration $\varepsilon_1 : S \to \mathbb{P}^1$. Moreover, since $(x, z) = (0, 0)$ is a rational point on each fiber, $\varepsilon_1$ admits a section $\sigma_0 : \mathbb{P}^1 \to S$, which we designate as the 0-section.

Let $t$ be the generic point of the base curve $\mathbb{P}^1$, and let $E_t$ be the fiber of $\varepsilon_1$ at $t$. This is nothing but the curve defined over $\mathbb{Q}(t)$ obtained by replacing $y$ by $t$ in (1.3). Using the change of variables

$$\begin{cases} x_1 = \dfrac{(t^3 - t)z}{x} \\ y_1 = \dfrac{(t^3 - t)^2}{x}, \end{cases}$$

the curve $E_t$ can be written in the Weierstrass form

$$(3.4) \qquad E_t : \; y_1^2 = x_1^3 - t^4(t^2 - 1)^3.$$

The bad fibers of the fibration $\varepsilon_1$ are easily determined using Tate's algorithm. They are given in the table below. Here, we denote by $m_t$ (resp. $m_t^{(1)}$) the number of irreducible (resp. simple) components in the fiber of $E_t$ at $t$, and we denote by $\chi$ the (topological) Euler number of the bad fiber.

| $t$ | Kodaira type | $\chi$ | $m_t$ | $m_t^{(1)}$ | Group structure |
|---|---|---|---|---|---|
| 0 | IV* | 8 | 7 | 3 | $\mathbb{G}_a \times \mathbb{Z}/3\mathbb{Z}$ |
| $\pm 1$ | $I_0^*$ | 6 | 5 | 4 | $\mathbb{G}_a \times (\mathbb{Z}/2\mathbb{Z})^2$ |
| $\infty$ | IV | 4 | 3 | 3 | $\mathbb{G}_a \times \mathbb{Z}/3\mathbb{Z}$ |

Here group structure means the structure of a special fiber of the Néron model of $E_t/\mathbb{C}(t)$. In order to determine the Néron-Severi group of $S_{\mathbb{C}} = S \times_{\mathbb{Q}} \mathbb{C}$, we need to determine the Mordell-Weil group $E_t(\mathbb{C}(t))$. We observe that the image of the lines $\ell_1, \ldots, \ell_6$ in $S$ are components of bad fibers. It turns out that the lines $\ell_7, \ldots, \ell_{18}$ determine sections of $\varepsilon_1$. For example, $\ell_7$ is transformed to the section

$$\sigma_1 = \big(t^2(t^2 - 1), t^2(t^2 - 1)^2\big).$$

Note that this corresponds to the trivial parametric solution $(m, k, l) = (m, 0, m)$ to the original equation (1.1). Since the curve $E_t/\mathbb{C}(t)$ has complex multiplication by $\mathbb{Q}(\omega)$, we see that

$$[\omega]\sigma_1 = \big(\omega t^2(t^2 - 1), t^2(t^2 - 1)^2\big).$$

is also a section. It corresponds to the line $\ell_8$ in $S$.

**Proposition 3.1.**

*1.* The Mordell-Weil group $E_t(\mathbb{C}(t))$ is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$, and it is generated by $\sigma_1$ and $[\omega]\sigma_1$.

2 *The Mordell-Weil lattice of $E_t$ over $\mathbb{C}(t)$ is isomorphic to $A_2^*$, the dual lattice of the root lattice $A_2$.*

3 *The surface $S$ is a singular $K3$ surface. The determinant of its Néron-Severi lattice is* $-48$.

Recall that the Mordell-Weil lattice in the sense of Shioda [Shi] of an elliptic surface with section consists of the Mordell-Weil group modulo torsion of its generic fiber, together with twice the canonical height pairing on it. Also, a $K3$

surface in characteristic zero is called *singular* (or *exceptional*) if its Néron-Severi group has the maximal rank, which is 20.

**Proof.** We first determine the torsion subgroup $E_t(\mathbb{C}(t))_{\text{tors}}$. It is known that the specialization map $E_t^0(\mathbb{C}(t))_{\text{tors}} \to E_{t_0}^{\text{ns}}(\mathbb{C})$ for any $t_0 \in \mathbb{C}$ is always injective even when the fiber is a bad fiber (see [M-P, Lemma 1.1 (b)]); here $E_t^0(\mathbb{C}(t))$ denotes the subgroup of $E_t(\mathbb{C}(t))$ consisting of all points which specialize to smooth points in $E_{t_0}(\mathbb{C})$. Moreover, the notation $E_{t_0}^{\text{ns}}(\mathbb{C})$ is used for the group of smooth points in $E_{t_0}(\mathbb{C})$, which is also the connected component of zero of the fiber over $t_0$ in the Néron model of $E_t$. Considering the table of bad fibers above, one observes that $E_t(\mathbb{C}(t))_{\text{tors}}$ is a subgroup of both $\mathbb{C} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{C} \times (\mathbb{Z}/2\mathbb{Z})^2$. This implies that $E_t(\mathbb{C}(t))_{\text{tors}}$ is trivial.

Since $\sigma_1$ is not the zero section, we conclude that it has infinite order. Also, since the Mordell-Weil group is in fact a module over $\text{End}(E_t) \cong \mathbb{Z}[\omega]$, it follows that $\sigma_1$ and $[\omega]\sigma_1$ are independent.

The rank of the Néron-Severi group of $S$ and the rank of the Mordell-Weil group are related by the Shioda-Tate formula, which says that

$$\text{rank } NS(S) = 2 + \sum_t (m_t - 1) + \text{rank } E_t(\mathbb{C}(t)).$$

From the calculation of the bad fibers and the fact that rank $NS(S) \leq 20$ one concludes that the rank of $E_t(\mathbb{C}(t))$ is at most 2, hence equal to 2. It follows that the rank of $NS(S)$ is 20 and therefore $S$ is a singular $K3$ surface.

Next we compute the canonical height pairing for $\{\sigma_1, [\omega]\sigma_1\}$. This is easily done using [Kuw], and one finds the matrix

$$\begin{pmatrix} \frac{1}{3} & -\frac{1}{6} \\ -\frac{1}{6} & \frac{1}{3} \end{pmatrix}.$$

This shows again that $\sigma_1$ and $[\omega]\sigma_1$ are linearly independent. We use the computation to conclude that $\{\sigma_1, [\omega]\sigma_1\}$ generates the Mordell-Weil group. If the Mordell-Weil group $E_t(\mathbb{C}(t))$ would be strictly larger than the group generated by $\sigma_1$ and $[\omega]\sigma_1$, then $E_t(\mathbb{C}(t))$ must contain an element whose canonical height is less than $1/3$. However, the a priori lower bound for the canonical height calculated by using the method of [Kuw] is $1/3$ in the present case. Hence $\sigma_1$ and $[\omega]\sigma_1$ generate $E_t(\mathbb{C}(t))$.

Let us denote by $MW$ the Mordell-Weil lattice of $E_t$ in the sense of Shioda [Shi]. The pairing on $MW$ is given by twice the canonical height pairing; i.e., it is given by the matrix

$$\begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix}.$$

Hence, $MW$ is isomorphic to $A_2^*$, and we have

$$|\det NS(S)| = \frac{\prod m_t^{(1)} |\det MW|}{|E_t(\mathbb{C}(t))_{\text{tors}}|^2} = \frac{3 \cdot 4 \cdot 4 \cdot 3 \cdot \frac{1}{3}}{1} = 48.$$

Since by the Hodge index theorem $\det NS(S)$ is negative, one concludes that $\det NS(S) = -48$. □

According to the classification of Shioda-Inose [S-I], there are four non-isomorphic singular $K3$ surfaces whose Néron-Severi lattices have determinant $-48$. The transcendental lattice of such a surface is isomorphic to one of the lattices given by the Gram matrices

$$\begin{pmatrix} 2 & 0 \\ 0 & 24 \end{pmatrix}, \quad \begin{pmatrix} 4 & 0 \\ 0 & 12 \end{pmatrix}, \quad \begin{pmatrix} 6 & 0 \\ 0 & 8 \end{pmatrix}, \quad \begin{pmatrix} 8 & 4 \\ 4 & 8 \end{pmatrix}.$$

**Proposition 3.2.** *The surface $S$ is isomorphic over $\mathbb{Q}(i, \omega)$ to the quartic surface in $\mathbb{P}^3$ defined by the equation $S' : X'(X'^3 + Y'^3) = Z'(Z'^3 + W'^3)$. As a consequence, $S$ corresponds to the matrix $\left(\begin{smallmatrix} 8 & 4 \\ 4 & 8 \end{smallmatrix}\right)$ in the Shioda-Inose classification.*

**Proof.** Consider the family of planes passing through the line $\ell_5$. The intersection of $S_0$ and a plane in this family is $\ell_5$ and a plane cubic curve. This yields another elliptic fibration $\varepsilon_2 : S \to \mathbb{P}^1$. Setting $t = W/(X - iY)$ and using a standard algorithm we can convert the fiber at the generic point to the Weierstrass form

$$y^2 = x^3 - 432t^2(t-1)^2(t+1)^2(t^2+1)^2,$$

where the transformation is given by

$$\begin{aligned} X &= 72\sqrt{3}t(t^2+1)^2, & Y &= 3y - 36\sqrt{-3}t(t^4-1), \\ Z &= -6\sqrt{-3}(t^2+1)x, & W &= -t\big(3iy - 36\sqrt{3}t(t^2+3)(t^2+1)\big). \end{aligned}$$

This fibration has six fibers of type IV at $t = 0, \pm 1, \pm i, \infty$. The same fibration can be obtained by starting from the surface $S'$ given by

$$X'(X'^3 + Y'^3) = Z'(Z'^3 + W'^3).$$

Namely, with $t = Z'/X'$, using the transformation

$$\begin{aligned} X' &= -2(t^4+1)y - tx^2 + 12t^3x - 72t(t^4-1)^2, \\ Y' &= -2(2t^4-1)y + tx^2 - 12t^3(t^4-1)x + 72t(t^4-1), \\ Z' &= t\big(-2(t^4+1)y - tx^2 + 12t^3x - 72t(t^4-1)^2\big), \\ W' &= 2t(t^4-2)y + t^2x^2 + 12(t^4-1)x - 72t^6(t^4-1), \end{aligned}$$

one finds exactly the same Weierstrass equation. Since $S'$ is nonsingular and minimal, we conclude that $S$ and $S'$ are isomorphic.

A result of Inose [Ino] shows that $S'$ corresponds to the matrix $\left(\begin{smallmatrix} 8 & 4 \\ 4 & 8 \end{smallmatrix}\right)$ in the Shioda-Inose classification. This proves the assertion. □

**Remark 3.3.** The Shioda-Tate formula shows that the Mordell-Weil rank of the fibration $\varepsilon_2$ is $20 - 2 - 6 \times 2 = 6$. However, since the transformation from the $(X, Y, Z, W)$-coordinates to the affine $(x, y, t)$-coordinates used here is not de-

fined over $\mathbb{Q}$, one cannot expect sections of $\varepsilon_2$ to correspond to solutions to our original diophantine problem.

## 4. A POLYNOMIAL SOLUTION AND A BASE CHANGE

From Proposition 3.1 one deduces that $E_t(\mathbb{Q}(t))$ is generated by $\sigma_1$. A simple calculation shows that

$$[2]\sigma_1 = \left(\frac{1}{4}t^2(t^2+8), \frac{1}{8}t^2(t^4-20t^2-8)\right)$$

is a polynomial solution to (3.4), but this does not correspond to a polynomial solution to (1.3), as we have

$$(x,z) = \left(\frac{8(t^2-1)^2}{t^4-20t^2-8}, \frac{2t(t^2+8)(t^2-1)}{t^4-20t^2-8}\right).$$

Since $[3]\sigma_1$, $[4]\sigma_1$, etc., do not yield a polynomial solution to (1.3), we suspect that the elliptic fibration $E_t$ gives no non-trivial parametric solutions to the original question. In fact, we can prove the following by an elementary argument.

**Proposition 4.1.** *The only polynomial solutions of the form* $(f(t), t, g(t))$ *to the equation (1.3) are* $(\pm 1, t, t)$.

**Proof.** Suppose that a polynomial $p(t)$ which is relatively prime to $t(t-1)(t+1)$ divides $f(t)$. Since $p(t)$ does not divide $t(f(t)^2+t^2-1)$, its cube $p(t)^3$ divides $f(t)$. Thus, we may write $f(t) = t^\alpha(t-1)^\beta(t+1)^\gamma f_0(t)^3$ $(0 \le \alpha, \beta, \gamma \le 2)$. Since $f_0(t)$ divides $g(t)$, we write $g(t) = f_0(t)g_0(t)$. The polynomials $f_0(t)$ and $g_0(t)$ satisfy the equation

$$t^{3\alpha+1}(t-1)^{3\beta}(t+1)^{3\gamma}f_0(t)^6 + t^{\alpha+1}(t-1)^{\beta+1}(t+1)^{\gamma+1} = g_0(t)^3.$$

The degree of the left hand side is $\max\{3(\alpha+\beta+\gamma)+6\deg f_0+1, \alpha+\beta+\gamma+3\}$, but this equals $3(\alpha+\beta+\gamma)+6\deg f_0+1$ except in the case $\alpha=\beta=\gamma=\deg f_0=0$. Since the degree of the right hand side is a multiple of 3, the degree of the left hand side cannot equal $3(\alpha+\beta+\gamma)+6\deg f_0+1$. Thus, we have $\alpha=\beta=\gamma=\deg f_0=0$. In other words $f_0(t)$ must be a constant and the only possibilities for this constant are $\pm 1$, which lead to the solutions $(\pm 1, t, t)$.

Observe that if we set $t=u^3$ in (3.4), then we find a solution given as $(x_1, y_1) = (u^4(u^6-1), 0)$. This is a 2-torsion section of the elliptic surface corresponding to

$$y_1^2 = x_1^3 - u^{12}(u^6-1)^3.$$

Setting $y_2 = y_1/u^6$ and $x_2 = x_1/u^4$, a minimal Weierstrass equation

$$E_u' : y_2^2 = x_2^3 - (u^6-1)^3$$

is obtained. Let $\tau$ be the above torsion section and let $\sigma_1'$ be the section of $E_u'$ coming from $\sigma_1$. We have that

$$\tau = (u^6 - 1, 0)$$
$$\sigma_1' = \left(u^2(u^6 - 1), (u^6 - 1)^2\right),$$

and

$$\pm\sigma_1' + \tau = \left((u^2 + 2)(u^4 + u^2 + 1), \mp 3(u^4 + u^2 + 1)^2\right).$$

The latter sections correspond to

$$\begin{cases} x &= \pm\frac{1}{3}(u^2 - 1)^2 \\ y &= u^3 \\ z &= \pm\frac{1}{3}u(u^2 - 1)(u^2 + 2). \end{cases}$$

as solutions to the equation (1.3). Taking the positive sign, and interchanging $x$ and $y$, one obtains the following solution to (1.1):

$$\begin{cases} m &= \frac{1}{6}(u - 1)(u^3 - 2u^2 - 4u - 4) \\ k &= u^3 \\ l &= \frac{1}{6}u(u^2 - 1)(u^2 + 2). \end{cases}$$

For integer values of $u$ not divisible by 3, the $m$, $k$ and $l$ given above become integers. Thus, possibly after using the symmetries mentioned in section 2.1, they give (infinitely many nontrivial) solutions to the original diophantine problem. For instance, $u = 2$ leads to the solution $3^3 + 4^3 + 5^3 = 6^3$. It should be remarked here that this parametric solutions is in fact very old: according to [Di, p. 582] it already appeared in a paper by C. Pagliani which was published in 1829-1830.

Using a computer we found that (1.3) has precisely 32 solutions in integers $0 < y \leq x \leq 10^6$. Of these, 15 (almost half of them!) correspond to values of $u$ as above.

## 5. FURTHER PROPERTIES OF $S$

We will now study the geometry and arithmetic of the surface $S$ a bit more closely. To this end, the elliptic fibration $E_t$ and the base change $E_u'$ will be used. Denote by $E^-$ the elliptic curve over $\mathbb{Q}$ corresponding to the Weierstrass equation $y^2 = x^3 - 1$. Also, define a curve $C$ over $\mathbb{Q}$ by $s^2 = u^6 - 1$. Note that $C$ is hyperelliptic and of genus 2. The hyperelliptic involution on $C$ will be written as $\iota$; by definition $\iota(u, s) = (u, -s)$. Using the map $[-1]$ on $E^-$ as well, one obtains an involution $\langle \iota \times [-1] \rangle$ on the product $C \times E^-$.

**Proposition 5.1.** *With notations as introduced above, the quotient* $(C \times E^-)/\langle \iota \times [-1] \rangle$ *is birationally isomorphic over* $\mathbb{Q}$ *to* $E_u'$.

**Proof.** The function field of $C \times E^-$ over $\mathbb{Q}$ is $\mathbb{Q}(u,x)[s,y]$ (with the relations $y^2 = x^3 - 1$ and $s^2 = u^6 - 1$). The function field of the quotient by $\iota \times [-1]$ is the subfield of all functions invariant under $(u,x,s,y) \mapsto (u,x,-s,-y)$. Over $\mathbb{Q}$, these invariants are generated by $u, X' = s^2x$ and $Y' = s^3y$. The relation between these is $Y'^2 = X'^3 - (u^6-1)^3$, so one finds precisely the function field of $E'_u$ over $\mathbb{Q}$. □

Using a primitive cube root of unity $\omega \in \overline{\mathbb{Q}}$ one defines $[\omega] \in \mathrm{Aut}(E^-)$ by $[\omega](x,y) = (\omega x, y)$. Similarly we take $\varphi \in \mathrm{Aut}(C)$ given by $\varphi(u,s) = (\omega^2 u, s)$. Note that $[\omega]$ and $\varphi$ are not defined over $\mathbb{Q}$, but the finite groups of automorphisms they generate is. As a consequence, a quotient such as $(C \times E^-)/\langle \iota \times [-1], \varphi \times [\omega] \rangle$ is defined over $\mathbb{Q}$.

**Proposition 5.2.** *The surface $S$, or equivalently its elliptic fibration $E_t$, is birationally isomorphic over $\mathbb{Q}$ to $(C \times E^-)/\langle \iota \times [-1], \varphi \times [\omega] \rangle$.*

**Proof.** Consider the surjection $E'_u \to E_t$ given by

$$(u, X', Y') \mapsto (t, X, Y) = (u^3, u^4 X', u^6 Y').$$

This is in fact the quotient map for the group of automorphisms on $E'_u$ generated by $(u, X', Y') \mapsto (\omega^2 u, \omega X', Y')$. This generator can be lifted to the automorphism $\varphi \times [\omega]$ on $C \times E^-$. Using proposition 5.1 above now finishes the proof. □

In the next section it will be explained how the above description allows one to compute the number of $\mathbb{F}_{p^n}$-rational points on the reduction $S \bmod p$ in an easy way. As a preparation to that, we now consider the second cohomology group $H^2(S) = H^2(S, \mathbb{C})$. The cycle class map allows one to view the Néron-Severi group of $S$ as a part of $H^2(S$; it generates a linear subspace of dimension 20 in our case. The orthogonal complement (with respect to cup product) of this will be denoted $H^2_{\mathrm{tr}}(S)$. In terms of the Hodge decomposition of $H^2(S)$, since $S$ is a singular $K3$ surface, one has $H^2_{\mathrm{tr}}(S) = H^{2,0}(S) \oplus H^{0,2}(S)$ in the present situation. Using the relation between $S$ and $C \times E^-$ explained above, one regards $H^2_{\mathrm{tr}}(S)$ as the subspace of $H^2_{\mathrm{tr}}(C \times E^-)$ on which $\iota \times [-1]$ and $\varphi \times [\omega]$ act trivially. Since the Künneth components $H^2(C) \otimes H^0(E^-)$ and $H^0(C) \otimes H^2(E^-)$ of $H^2(C \times E^-)$ are algebraic, this means that $H^2_{\mathrm{tr}}(S)$ can be seen as a subspace of $H^1(C) \otimes H^1(E^-)$.

Note that the latter tensor product has dimension 8. To understand it even better we introduce the elliptic curve $E^+$, defined over $\mathbb{Q}$ by the equation $\eta^2 = \xi^3 + 1$. One has a morphism $\pi_1 : C \to E^+$, given by $\pi_1(u,s) = (\xi = -u^{-2}, \eta = su^{-3})$. The global differential given by $d\xi/\eta$ is pulled back to $2(du/s)$ under $\pi_1$. Hence it follows that under the pull back map $\pi_1^*$, the space $H^1(E^+)$ is mapped to the $-1$-eigenspace in $H^1(C)$ for the automorphism $\psi$ given by $\psi(u,s) = (-u,s)$. Similarly, using $\pi_2 : C \to E^-$ given by $\pi_2(u,s) = (x = u^2, y = s)$ one computes $\pi_2^*(dx/y) = 2u(du/s)$ and concludes that $\pi_2^*$ maps

$H^1(E^-)$ to the $+1$-eigenspace in $H^1(C)$ for $\psi$. Hence using $(\pi_1 \times \pi_2)^*$ one identifies

$$H^1(C) \otimes H^1(E^-) = \big(H^1(E^+) \otimes H^1(E^-)\big) \oplus \big(H^1(E^-) \otimes H^1(E^-)\big).$$

We claim that under this identification, the subspace $H^2_{\mathrm{tr}}(S)$ coincides with the transcendental part $H^2_{\mathrm{tr}}(E^+ \times E^-)$ inside $H^1(E^+) \otimes H^1(E^-)$. To see this, note that the latter transcendental part is generated by the holomorphic form $(d\xi/\eta) \otimes (dx/y)$ and its anti-holomorphic complex conjugate. Using $\pi_1^*$, this holomorphic form corresponds to $2(du/s) \otimes (dx/y)$, which is invariant under both $\iota \times [-1]$ and $\varphi \times [\omega]$, hence it (and its complex conjugate) is in $H^2_{\mathrm{tr}}(S)$. Since this space is 2-dimensional, the claim is proven.

**Remark.** The proofs provided in this section in fact describe an inclusion of function fields $\mathbb{Q}(C \times E^-) \supset \mathbb{Q}(E'_u) \supset \mathbb{Q}(E_t)$. It is easily verified that the composition of these inclusions corresponds to the finite (in fact, cyclic of degree 6) map $\psi : C \times E^- \to E_t = S$ which assigns to a point $(u, s)$, $(x_0, y_0) \in C \times E^-$ the point with coordinates $x = s/y_0, y = u^3, z = usx_0/y_0$ on $S$. The cyclic group of order 6 for which we take the quotient here, turns out to have precisely 16 orbits in $C \times E^-$ consisting of less than 6 points. Blowing up the quotient singularities obtained in this way, yields 16 (independent) elements in the Néron-Severi group of $S$. In fact this provides an alternative way to see that $S$ has Néron-Severi rank 20: One can lift the 4 generators of the Néron-Severi group of $E^- \times E^-$ to cycles in $C \times E^-$, and push them forward to $S$. In this way 20 independent elements are obtained, as follows immediately by computing their intersection numbers.

As a final remark, consider the morphism $C \to E^-$ given by $P \mapsto \pi_2(P) + (0, 1)$. The graph of this morphism defines a curve in $C \times E^-$, and the image in $E_t$ of this curve under $\psi$ is precisely the 'polynomial section' described by Pagliani in 1829/30 and by us in the previous section.

## 6. COUNTING POINTS ON $S$ OVER FINITE FIELDS

Since $S$ is a singular $K3$ surface, one knows from [S-I] that for sufficiently large extensions $K$ of the finite prime field $\mathbb{F}_p$ one can describe the number of $K$-rational points on the reduction of $S$ in terms of a Hecke character. However, it is not easy to describe, for which field extensions $K$ their result gives the number of points. For the present example, we present a Hecke character which gives the number of rational points over *all* finite fields. Although this does not seem to have an immediate relation to the problem of sums of consecutive cubes, it is included here because it is an interesting and nontrivial problem for singular $K3$'s over number fields in general, and not many interesting examples where this has been done have been published. One may note that the present case turns out to be much simpler than, e.g., the example described in [P-T-vdV].

To compute the number of points on $S$ over finite fields, the $\ell$-adic cohomology groups $H^i = H^i(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ are used. These spaces are $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-

modules. One knows $H^0 \cong \mathbb{Q}_\ell$, with the trivial Galois action and $H^4 \cong \mathbb{Q}_\ell(-2)$, which means that $H^4$ is a $\mathbb{Q}_\ell$-vector space of dimension 1 and a Frobenius element $\sigma_p \in G_\mathbb{Q}$ at a prime $p$ acts on it by multiplication by $p^2$. Furthermore, since $S$ is an elliptic surface with base $\mathbb{P}^1$ it follows that $H^1 = H^3 = (0)$. Given a Frobenius element $\sigma_p \in G_\mathbb{Q}$ at a 'good' prime $p \neq \ell$ (in our situation 'good' means that one of the equations defining $S$ gives a $K3$ surface over $\mathbb{F}_p$ as well; this happens when $p \neq 2, 3$), the number of points over $\mathbb{F}_{p^n}$ on the reduction mod $p$ of $S$ is given by the Lefschetz trace formula

$$\sum_{i=0}^{4} (-1)^i \operatorname{trace}(\sigma_p^n | H^i(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)) = 1 + p^{2n} + \operatorname{trace}(\sigma_p^n | H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)).$$

We will make this explicit by studying $H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$.

There exists a $G_\mathbb{Q}$-equivariant cycle class map which injects the Néron-Severi group of $S$ into $H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$, which is the same space $H^2$ but with a different Galois action: $\sigma_p$ acts on $H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ exactly as $p\sigma_p$ does on $H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$. Write $H^2_{\text{alg}}$. for the subspace of $H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ generated by the Néron-Severi group, and $H^2_{\text{tr}}$ for the orthogonal complement. Both spaces are $G_\mathbb{Q}$-invariant, and of course

$$\operatorname{trace}(\sigma_p^n | H^2(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)) = \operatorname{trace}(\sigma_p^n | H^2_{\text{alg}}) + \operatorname{trace}(\sigma_p^n | H^2_{\text{tr}}).$$

**Proposition 6.1.** *For $p \neq 2, 3, \ell$ prime and $\sigma_p \in G_\mathbb{Q}$ a Frobenius element at $p$, one has*

$$\operatorname{trace}(\sigma_p^n | H^2_{\text{alg}}) = 16p^n + 3\left(\frac{-3}{p}\right)^n p^n + \left(\frac{-4}{p}\right)^n p^n.$$

**Proof.** By what is said above, it suffices to compute the action of a Frobenius element $\sigma_p$ on a set of generators of the Néron-Severi group. Using the elliptic fibration $E_t$, we study such generators.

Firstly, there are the zero section and a fiber. On each of these $\sigma_p$ acts trivially, so they contribute $p^n + p^n = 2p^n$ to our trace.

Next we consider the sections $\sigma_1$ and $[\omega]\sigma_1$. Note that since $\sigma_1 + [\omega]\sigma_1 + [\overline{\omega}]\sigma_1 = 0$ in the group law, it follows that $\sigma_p([\omega]\sigma_1) = -\sigma_1 - [\omega]\sigma_1$ in case $\big((-3/p)\big) = -1$. On the other hand, $\sigma_1$ is fixed under every element of $G_\mathbb{Q}$. So it follows that these two sections contribute $\big(1 + (-3/p)^n\big)p^n$ to the trace.

It remains to compute the contributions from the irreducible components of the singular fibers, which do not meet the zero section. These fibers are over $t = 0$, $t = \pm 1$ and $t = \infty$. Over $t = 0$, the fibre is of type $IV^*$ and all its components turn out to be rational. Hence they contribute $6p^n$ to our trace.

Over $t = \pm 1$ one finds fibers of type $I_0^*$. Of the components not meeting the zero section, one is always rational. With $T$ a coordinate on this one, the other three meet it in points satisfying $T^3 - (\pm 2)^3 = 0$. Hence two of them are interchanged by $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ and the third one is rational. This means that one obtains

$$2\left(p^n+p^n+\left(1+\left(\frac{-3}{p}\right)^n\right)p^n\right)=6p^n+2\left(\frac{-3}{p}\right)^n p^n$$

from these fibers to the trace.

To study the fiber over $t=\infty$, one changes coordinates using $\tilde{y}=t^{-6}y, \tilde{x}=t^{-4}x$ and $s=t^{-1}$. The elliptic fibration $E_t$ is then given by $\tilde{y}^2=\tilde{x}^3-s^2(1-s^2)^3$. Over $t=\infty$, which corresponds to $s=0$, one finds a fiber of type IV. The two components not meeting the zero section are interchanged by $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Hence they add $(1+((-4/p))^n)p^n$ to the trace.

Summing all contributions now proves the proposition. □

The $G_{\mathbb{Q}}$-space $H^2_{\mathrm{tr}}$ will be our next object to study. Recall that we already showed it is related to $H^2_{\mathrm{tr}}(A_{\overline{\mathbb{Q}}},\mathbb{Q}_\ell)$ in which $A=E^+\times E^-$. In fact, this was only done for complex cohomology, but using a comparison theorem and noting that the morphisms $C\times E^-\to S$ and $C\to E^+\times E^-$ we used are defined over $\mathbb{Q}$, the same holds for $\ell$-adic cohomology. So one concludes

$$\mathrm{trace}(\sigma_p^n|H^2_{\mathrm{tr}})=\mathrm{trace}(\sigma_p^n|H^2_{\mathrm{tr}}(A_{\overline{\mathbb{Q}}},\mathbb{Q}_\ell)).$$

It is relatively standard how this latter trace is computed, as will be explained now.

It has been shown that $H^2_{\mathrm{tr}}\subset H^1(E^+)\otimes H^1(E^-)$. This Künneth component in $\ell$-adic cohomology is $G_{\mathbb{Q}}$-invariant, for instance because its orthogonal complement, which is generated by the cycle classes of $\{0\}\times E^-$ and $E^+\times\{0\}$, obviously is. Note that $\mathbb{Z}[\omega]$ is the endomorphism ring of both $E^+, E^-$, and all these endomorphisms are defined over $\mathbb{Q}(\omega)$. Hence the 2-dimensional $\mathbb{Q}_\ell$-vector spaces $H^1(E^\pm)$ are in fact free rank 1 modules over $\mathbb{Q}_\ell\otimes\mathbb{Z}[\omega]$. In particular, this means that when we restrict the Galois action to $G_{\mathbb{Q}(\omega)}=\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\omega))$, then it becomes abelian, i.e., it factors over the Galois group of the maximal abelian extension of $\mathbb{Q}(\omega)$. By class field theory this implies that our actions on $H^1(E^\pm)$ are given by Hecke characters, which will be denoted $\chi^+,\chi^-$, respectively. These characters will now be described.

Write $K=\mathbb{Q}(\omega)$. The Hecke characters $\chi^\pm$ can be thought of as products $\prod_v\chi_v^\pm$ in which the product is taken over all places of $K$ (including the infinite one). Here $\chi_v$ is a multiplicative character; for $v=\infty$ it is given by

$$\chi_\infty^\pm\ :\ \mathbb{C}^*\longrightarrow\mathbb{C}^*\ :\ z\mapsto\frac{1}{z}.$$

For finite places one has $\chi_v^\pm : K_v^*\to\mathbb{Q}(\omega)^*$. These characters have the property that for a place $v$ not dividing (2) or (3), and $v$ corresponding to a (principal) prime ideal $(\pi)$ of norm $q$ in $\mathbb{Z}[\omega]$, one has that $\chi_v^\pm$ sends any uniformizing element of $K_v$ to the generator of $(\pi)$ which as an element of the endomorphism ring of $E^\pm$ gives after reduction modulo $(\pi)$ the $q$th power endomorphism. In particular, for such $v$ one has that $\chi_v^\pm$ is 1 on all elements of $K_v$ which have valuation 0. If $\sigma_p\in G_{\mathbb{Q}}$ is a Frobenius element at a prime $p\neq 2,3$, then (for $n$ non-zero)

$$\operatorname{trace}(\sigma_p^{f_p n} | H^1(E^{\pm})) = \sum_{v|p} \chi_v^{\pm}(\pi_v)^n,$$

in which $\pi_v \in K_v$ is any uniformizing element and where $f_p$ is the degree of the extension $K_v/\mathbb{Q}_p$. Moreover, $\operatorname{trace}(\sigma_p^m | H^1(E^{\pm})) = 0$ when $f_p$ does not divide $m$.

An explicit description of the $\chi_v^{\pm}$ now boils down to finding the $q$th power endomorphism on $E^{\pm}$ over $\mathbb{F}_q$. In case $p \neq 2$ is a prime number $\equiv 2 \bmod 3$, the square of the $p$th power map has to be considered, and this equals $[-p]$ as endomorphism (the reduction of both $E^+, E^-$ is supersingular in this case). When $p \equiv 1 \bmod 3$, both primes above $p$ in $\mathbb{Z}[\omega]$ are primes of ordinary reduction for $E^{\pm}$. So here the full endomorphism ring in characteristic $p$ is $\mathbb{Z}[\omega]$, and we have to find out which element the $p$th power map corresponds to. Firstly, this map has degree $p$, so we look for an element of norm $p$. Next, the map is inseparable, so we want an element whose reduction modulo the prime of $\mathbb{Z}[\omega]$ under consideration is 0. This implies we want a generator $\pi$ of the prime ideal under consideration. To find out which generator, consider some torsion points on $E^{\pm}$. Note that since $p \equiv 1 \bmod 3$, all the 2-torsion points on both $E^{\pm}$ are rational over $\mathbb{F}_p$. Hence the $p$th power map $\pi$ fixes the 2-torsion, which implies that $2|(\pi - 1)$. Moreover, both $[\omega]$ and $[\overline{\omega}]$ act the same way (in fact, act trivially) on the points with $x-$ or $\xi$-coordinate 0. Hence these points are in the kernel of $[\omega - \overline{\omega}] = [\sqrt{-3}]$. This map has degree 3, so we found all the $[\sqrt{-3}]$-torsion. On $E^+$, these points are $\mathbb{F}_p$-rational, so it follows $\pi \equiv 1 \bmod 2\sqrt{-3}$ in this case. This determines $\pi$. For $E^-$, the $p$th power map acts as $[+1]$ on the $[\sqrt{-3}]$-torsion when $p \equiv 1 \bmod 12$, so in this case again $\pi$ is determined by $\pi \equiv 1 \bmod 2\sqrt{-3}$. However, when $p \equiv 7 \bmod 12$ then the $p$th power map acts as $[-1]$ on the $[\sqrt{-3}]$-torsion, hence $\pi$ is determined by $\pi \equiv -1 \bmod 2\sqrt{-3}$.

For completeness, and to allow us to relate $H^2_{\mathrm{tr}}$ to a modular form later on, we also describe the $\chi_v^{\pm}$ for $v|(2)(3)$. These can be found using that $\prod_v \chi_v(x) = 1$, where $x \in \mathbb{Q}(\omega)$ and where the product is over all places $v$ of $\mathbb{Q}(\omega)$. Furthermore, the local units $\mathbb{Z}_2[\omega]^*$ and $\mathbb{Z}_3[\omega]^*$ are known to have finite image, hence we know that this image has to be inside the 6th roots of unity. So in particular all sufficiently small subgroups $1 + 2^n\mathbb{Z}_2[\omega]$ resp. $1 + (\sqrt{-3})^m\mathbb{Z}_3[\omega]$, which consist of only 6th powers, are mapped to 1. Since there is only one prime above each of (2), (3), we denote the associated local characters by $\chi_2^{\pm}$ and $\chi_3^{\pm}$ respectively. One computes:

1 For $p = 3$ one identifies

$$\mathbb{Z}_3[\omega]^*/1 + (\sqrt{-3}) \cong (\mathbb{Z}_3[\omega]/\sqrt{-3})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \cong \{\pm 1\}.$$

Then both $\chi_3^+$ and $\chi_3^-$ are trivial on $1 + (\sqrt{-3})$, and on $\mathbb{Z}_3[\omega]^*$ they are given using the identification above. Next, $\chi_3^{\pm}(\sqrt{-3}) = \sqrt{-3}$.

2 For $p = 2$, identify

$$\mathbb{Z}_2[\omega]^*/1 + (2) \cong (\mathbb{Z}_2[\omega]/2)^* \cong \{1, \omega, \overline{\omega}\}.$$

Then $\chi_2^+$ is trivial on $1 + 2\mathbb{Z}_2[\omega]$, and it is given by this identification on $\mathbb{Z}_2[\omega]^*$. Moreover, $\chi_2^+(2) = -2$.

The character $\chi_2^-$ turns out to be trivial on $1+4\mathbb{Z}_2[\omega]$, and on $\mathbb{Z}_2[\omega]^*$ it is given by

$$\chi_2^-(u) = (-1)^{(u\bar{u}-1)/2}\chi_2^+(u)$$

Finally, $\chi_2^-(2) = -2$.

From the discussion above it is clear that the restriction to $G_{\mathbb{Q}(\omega)}$ of the $G_{\mathbb{Q}}$-representation $H^2_{\mathrm{tr}}(A)$ is given by the product $\chi = \chi^+\chi^-$. Namely, over $\mathbb{Q}(\omega, i)$ one finds two copies of $G_{\mathbb{Q}(\omega,i)}$-representation in $H^1(E^+) \otimes H^1(E^-)$, corresponding to the graph of an isomorphism between these elliptic curves, and the composition of that graph with $[\omega]$. These representations correspond to the Hecke character (in fact, Dirichlet character) $\chi^+\overline{\chi^-}$. Hence the remaining transcendental part corresponds to $\chi$.

The explicit description of $\chi^\pm$ shows that $\chi_3$ is in fact trivial on the units $\mathbb{Z}_3[\omega]^*$. In fact, one computes that $\chi$ is a Hecke character of conductor $(2)^4$. Since such Hecke characters are well known to be intimately related to modular forms, one concludes using e.g. [Top, Theorem 2.4.2] that the $L$-series attached to $H^2_{\mathrm{tr}}$, which equals

$$L(s,\chi) = \prod_{\substack{v \text{ finite} \\ v \neq 2}} (1 - \chi_v(\pi_v)N_v^{-s}\pi)^{-1},$$

is in fact the $L$-series of a cusp form of weight 3 and character $(\frac{-3}{\cdot})$ for $\Gamma_0(48)$.

If one works out the correspondence between this cusp form $f$ and the $L$-series in more detail, one finds that $f$ is given by the $q$-expansion

$$\frac{1}{6} \sum_{\substack{m,n \in \mathbf{Z} \\ (m,n) \not\equiv (0,0) \bmod 2}} (m+n\omega)^2 \chi_2(n+m\omega)^{-1} q^{m^2-mn+n^2}.$$

Hence one finds

$$f = q + 3q^3 - 2q^7 + 9q^9 - 22q^{13} - 26q^{19} - 6q^{21} + 25q^{25} + 27q^{27} + 46q^{31} + 26q^{37} - 66q^{39} + 22q^{43} - 45q^{49} \ldots$$

It was pointed out to us by Ken Ono that this cusp form has the following description. Denote by $\eta(z)$ the Dedekind eta-function, i.e., the function given by $\eta(z) = e^{2\pi iz/24}\prod_{n\geq 1}(1-e^{2\pi inz})$. Using the famous transformation rules for $\eta$ it is not hard to verify that

$$g(z) := \frac{\eta(12z)^9\eta(4z)^9}{\eta(2z)^3\eta(6z)^3\eta(8z)^3\eta(24z)^3}$$

is a modular form of weight 3 and character $(\frac{-3}{\cdot})$ for $\Gamma_0(48)$ as well. Comparing coefficients in fact shows that $f = g$, hence our $L$-series is the one associated with this product of eta-functions.

The above discussion allows one to compute the number of points on the somewhat abstractly defined variety $S$ over finite fields. However, since it is a

purely combinatorial matter (compare[vG-T]) to describe the difference between $S(\mathbb{F}_{p^n})$ and the set $\{(t,x,y) \in \mathbb{F}_{p^n}^{(3)} \mid y^2 = x^3 - t^4(t^2-1)^3\}$ we will for explicitness state the final result of the above discussion in terms of this explicit equation.

**Theorem 6.2.** *Suppose $p \geq 5$ is a prime number and $n > 0$ an integer. The number $N(p,n)$ of solutions $(t,x,y) \in \mathbb{F}_{p^n}^{(3)}$ to the equation $y^2 = x^3 - t^4(t^2-1)^3\}$ is given by*

$$N(p,n) = p^{2n} + p^n + (-3p)^n p^n + a_{p^n},$$

*in which $a_{p^n}$ is given by any of the two following descriptions.*

1 *$a_{p^n}$ is the coefficient of $q^{p^n}$ in the cusp form $f$ of weight 3 and character $(\frac{-3}{\cdot})$ for $\Gamma_0(48)$ given by*

$$q \prod_{n \geq 1} \frac{(1-q^{12n})^9 (1-q^{4n})^9}{(1-q^{2n})^3 (1-q^{6n})^3 (1-q^{8n})^3 (1-q^{24n})^3};$$

2 *For $p \equiv 2 \bmod 3$ one has $a_{p^n} = 0$ whenever $n$ is odd, and $a_{p^n} = p^n$ whenever $n$ is even.*

*For $p \equiv 1 \bmod 3$, write $p = m^2 - mn + n^2$. Then $a_{p^n} = \alpha^n + \overline{\alpha}^n$, in which $\alpha = (-4p)\omega^a (m + n\omega)^2$, and where the exponent $a$ is chosen such that $m + n\omega - w^a \in 2\mathbb{Z}[\omega]$.*

The first-named author would like to thank Joe Silverman for useful suggestions in regard to Proposition 4.1. He also thanks the Centre Interunivesitaire en Calcul Mathématique Algébrique at Concordia University for allowing him to use their computing facilities. We are grateful to the referee for pointing out the reference to Pagliani, and for some interesting remarks concerning the product of two curves we considered. Finally we thank Ken Ono for mentioning the formula for our cusp form in terms of eta-functions.

REFERENCES

[Di] Dickson, L.E. – History of the theory of numbers, Volume II. Washington: Carnegie Institution, (1920).

[Ino] Inose, H. – On certain Kummer surfaces which can be realized as non-singular quartic surfaces in $\mathbb{P}^3$, J. Fac. Sci. Univ. Tokyo **23**, 545–560 (1976).

[Kuw] Kuwata, M. – Canonical height and elliptic $K3$ surfaces, J. Number Theory **36**, 399–406 (1990).

[K-T] Kuwata, M. and J. Top – An elliptic surface related to sums of consecutive squares, Expos. Math. **12**, 181–192 (1994).

[M-P] Miranda, R. and U. Persson, – Torsion subgroup of elliptic surfaces, Compositio Math. **72**, 249–267 (1989).

[P-T-vdV] Peters, C., J. Top, and M. van der Vlugt, – The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes, J. Reine Angew. Math. **43** 2, 151–176 (1992).

[P-R] Platiel, S. and J. Rung, – Natürliche Zahlen als Summen aufeinander folgender Quadratzahlen, Expos. Math. **12**, 353–361 (1994).

[Shi] Shioda, T. – On the Mordell-Weil lattices, Comment. Math. Univ. Sancti Pauli **39**, 211–240 (1990).

[S-I] Shioda, T. and H. Inose, – On singular $K3$ surfaces, Complex Analysis and Algebraic Geometry, 119–136 (1977).

[Str] Stroeker, R.J. – On the sum of consecutive cubes being a perfect square, Compositio Math. **97**, 295–307 (1995).

[Top] Top, J. – Hecke $L$-series related with algebraic cycles or with Siegel modular forms, Ph.D. thesis, University of Utrecht, 1989.

[vG-T] van Geemen, van, B. and J. Top, – Selfdual and non-selfdual 3-dimensional Galois representations, Compositio Math. **97**, 51–70 (1995).

Received October 1999