COLLOQUIUM MATHEMATICUM

VOL. 115 2009 NO. 1

ON INTEGRAL SIMILITUDE MATRICES

BY

J. BRZEZIŃSKI and T. WEIBULL (Göteborg)

Abstract. We study integral similitude 3×3-matrices and those positive integers which occur as products of their row elements, when matrices are symmetric with the same numbers in each row. It turns out that integers for which nontrivial matrices of this type exist define elliptic curves of nonzero rank and are closely related to generalized cubic Fermat equations.

1. Introduction. Let A be a rational $n \times n$-matrix. We say that A is a *similitude matrix* if its rows have the same length l and are pairwise orthogonal, that is, $AA^t = l^2 I$, where A^t is the transpose of A and I the identity matrix. Of course, also the columns of A have the same length and are pairwise orthogonal. We say that an integral matrix $A = [a_{ij}]$ ($a_{ij} \in \mathbb{Z}$) is *primitive* if the greatest common divisor of the a_{ij} equals 1. Since $\det(A) = l^n$, the number l must be an integer when n is odd (as l^2 is an integer). For simplicity, we will consider only similitude matrices with positive determinant. When $n = 2$, then, of course,

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

where $a^2 + b^2 = l^2$ and a, b are relatively prime integers, is a general form of primitive similitude matrices. In the special case when (a, b) has integer length, that is, $l = c$ for a positive integer c, we have a Pythagorean triple (a, b, c) and assuming that a is even,

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 2rs & r^2 - s^2 \\ s^2 - r^2 & 2rs \end{pmatrix},$$

where $\gcd(r, s) = 1$ and r, s are of different parities.

Notice that integral similitude 2×2-matrices can be considered as *integral square frames* by which we mean a pair of orthogonal vectors in $\mathbb{R}^2$ with integral coordinates spanning a square. The products of the coordinates of such

2000 *Mathematics Subject Classification*: Primary 11C20, 11G05; Secondary 11D25.
Key words and phrases: similitude matrix, congruent number, cuboid number, elliptic curve.

DOI: 10.4064/cm115-1-1

vectors lead to interesting questions in number theory: The area of the right triangle is $S = \frac{1}{2}ab = mk^2$, where m is square-free and k is an integer. The number m is called a *congruent number* (see e.g. [K, p. 52]). For example, it is well known that $1, 2, 3$ are not, but $5, 6$ are congruent. Characterization of congruent numbers is a difficult problem on which a considerable progress has been achieved using the theory of elliptic curves and modular forms (see [Tu]). In fact, m is a congruent number if and only if the elliptic curve

$$y^2 = x^3 - m^2x$$

has non-zero rank (see [K, p. 110]).

The purpose of this note is to study similar questions concerning *integral cubic frames*, that is, triples of integral orthogonal vectors in $\mathbb{R}^3$ which span cubes. In other words, we are concerned with 3×3 integral similitude matrices. The Pythagorean triples may be considered as a special case of such integral cubic frames (when the matrices A above are extended to 3×3-matrices by a row and column consisting of $0, 0, c$).

First of all, in Section 2, we recall a parametrization of all primitive similitude 3×3-matrices, which, in principle, was already known to Euler (see [D, p. 530]). In Section 3, we study symmetric matrices of this type, and in Section 4, those integral cubic frames in which coordinates of the vectors are permuted. This case is in some sense a natural analogue of the case of Pythagorean triangles and opens for natural questions concerning *cuboid numbers*, which are defined by an analogy to the congruent numbers. The primitive permutational similitude matrices have the following form:

$$A = \begin{pmatrix} -rs & rs - r^2 & rs - s^2 \\ rs - r^2 & rs - s^2 & -rs \\ rs - s^2 & -rs & rs - r^2 \end{pmatrix},$$

where r, s are relatively prime integers (see (4.1)). The product of the row elements of A is always a square, and the *cuboid numbers* are those positive integers whose squares appear as such products. Somewhat simpler, a positive integer m is a cuboid number if $m = \alpha\beta(\alpha - \beta)\gamma^3$, where α, β, γ are rational numbers (m is congruent if $m = \alpha\beta(\alpha^2 - \beta^2)\gamma^2$). It turns out that $m \neq 2$ is a cuboid number if and only if the elliptic curve $y^2 = x^3 + 16m^2$ has non-zero rank (see Proposition 4.4). This result identifies the cuboid numbers as those for which the generalized Fermat equation $x^3 + y^3 = mz^3$ has a non-trivial solution (see Proposition 4.5). Thus the problem of construction of integral similitude matrices is related to a vast literature concerning generalized Fermat equations $m_1x^3 + m_2y^3 + m_3z^3 = 0$, where m_i are integers such that $m_1m_2m_3 = m$ (see [C1], [ZK], and especially [S] with a long list of references on this problem).

In the last Section 5, we give some numerical examples constructing primitive similitude matrices for all cuboid numbers $m \le 50$.

2. Similitude transformations in three dimensions. Assume now that $n = 3$. We want to find a general form of primitive similitude matrices of dimension 3 (with positive determinant). Let $A = [a_{ij}]$ be such a matrix. Let $q : \mathbb{Q}^3 \to \mathbb{Q}$, where $q(x) = x_1^2 + x_2^2 + x_3^2$. Then $\varphi(x) = Ax$ for a (column) vector $x \in \mathbb{Q}^3$ is a linear transformation for which $q(Ax) = l^2 q(x)$. Hence $(1/l)\varphi$ is an orthogonal transformation of $(\mathbb{Q}^3, q)$.

Consider the Hamiltonian quaternion algebra $\mathbb{H}$ over the rational numbers, that is, $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, where $i^2 = j^2 = -1$, $ij + ji = 0$ and $k = ij$. For a quaternion $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{H}$, where $x_i \in \mathbb{Q}$, we denote by $\bar{x} = x_0 - x_1 i - x_2 j - x_3 k$ its conjugate. The trace $\mathrm{Tr}(x) = x + \bar{x}$ and the norm $\mathrm{Nr}(x) = x\bar{x}$ of $x \in \mathbb{H}$ are elements of $\mathbb{Q}$. The subspace $\mathbb{H}^0$ consisting of the pure quaternions, that is, quaternions with $\mathrm{Tr}(x) = 0$, has dimension 3 over $\mathbb{Q}$ and $\mathrm{Nr}(x) = x_1^2 + x_2^2 + x_3^2$. Thus $(1/l)\varphi$ can be considered as an orthogonal transformation of $(\mathbb{H}^0, \mathrm{Nr})$, whose matrix in the basis i, j, k is $(1/l)[a_{ij}]$. The following well-known result gives a parametrization of all orthogonal transformation of this space (see [O'M, 57:13]):

Proposition 2.1. *Every rotation of* $\mathbb{H}^0$ *has the form* $\sigma(x) = \alpha x \alpha^{-1}$ *for some* $\alpha \in \mathbb{H}$.

In fact, let $\alpha = a + bi + cj + dk$, where $a, b, c, d \in \mathbb{Q}$. In the basis i, j, k, the transformation $(1/l)\varphi = \alpha x \alpha^{-1}$ has the following matrix:

$$(1/l)[a_{ij}] = \frac{1}{a^2 + b^2 + c^2 + d^2} \times \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2bc - 2ad & 2bd + 2ac \\ 2bc + 2ad & a^2 - b^2 + c^2 - d^2 & 2cd - 2ab \\ 2bd - 2ac & 2cd + 2ab & a^2 - b^2 - c^2 + d^2 \end{pmatrix}.$$

The matrix on the right uniquely determines a primitive integral matrix with positive determinant, that is, the numbers a_{ij} and the factor $1/l$. Multiplying the rational numbers a, b, c, d by their least common denominator, we may assume that these numbers are relatively prime integers. Then we get the following result (see [D, p. 530] and the references given there, in particular to L. Euler):

Proposition 2.2. *Every primitive similitude* 3×3*-matrix* (*with positive determinant*) *has the form* $2^{-\kappa} A(a, b, c, d)$, *where*

$$(2.1)\quad A(a,b,c,d) = \begin{pmatrix} a^2+b^2-c^2-d^2 & 2bc-2ad & 2bd+2ac \\ 2bc+2ad & a^2-b^2+c^2-d^2 & 2cd-2ab \\ 2bd-2ac & 2cd+2ab & a^2-b^2-c^2+d^2 \end{pmatrix},$$

a,b,c,d are relatively prime integers and

- (a) $\kappa = 0$ *when exactly one of a,b,c,d is odd or exactly one is even*;
- (b) $\kappa = 1$ *when exactly two of a,b,c,d are odd*;
- (c) $\kappa = 2$ *when all a,b,c,d are odd.*

Moreover, the length of the rows of $2^{-\kappa}A(a,b,c,d)$ equals $l = 2^{-\kappa}(a^2+b^2+c^2+d^2)$ and the determinant of this matrix equals l^3.

Proof. Let $A = [a_{ij}]$ be a primitive similitude 3×3-matrix (with positive determinant) with row length l. Then according to the arguments above,

$$[a_{ij}] = \frac{l}{a^2+b^2+c^2+d^2} A(a,b,c,d),$$

where a,b,c,d are relatively prime integers. It is easy to see that the greatest common divisor of all the elements of the matrix $A(a,b,c,d)$ must be a power of 2. In fact, if an odd prime p divides all the elements of this matrix, then an easy computation modulo p shows that p must divide all a,b,c,d, which contradicts our assumption. Thus the only possibility is that all the elements of the matrix are divisible by a power of 2.

In case (a) and only in this case, the diagonal elements of $A(a,b,c,d)$ are odd. Hence the matrix is primitive and we have $l = a^2+b^2+c^2+d^2$.

In case (b), $l = a^2+b^2+c^2+d^2 \equiv 2 \pmod 4$ and all the elements of $A(a,b,c,d)$ are even. An easy computation modulo 4 shows that they are not all divisible by 4. Hence their greatest common divisor is 2. Dividing the elements of this matrix by 2, we get a primitive matrix, and at the same time we get $2l = a^2+b^2+c^2+d^2$.

Finally, in case (c), $l = a^2+b^2+c^2+d^2 \equiv 4 \pmod 8$ and, as in case (b), the elements of $A(a,b,c,d)$ are even. But now they are all divisible by 4, but not all by 8. Dividing these elements by 4, we get a primitive matrix and the equality $4l = a^2+b^2+c^2+d^2$. ■

Corollary 2.3. *There exist primitive similitude matrices with row length l if and only if l is odd.*

Proof. If l is odd, then l has a primitive representation as a sum of four integer squares (see [C2, p. 144]). Of course, exactly one or three of these squares are odd, so according to Proposition 2.2(a), there is a primitive similitude matrix whose length of rows (columns) equals l. Conversely, if such a matrix exists, then by Proposition 2.2, l is odd (case (a)) or $2l \equiv 2$

(mod 4) (case (b)) or $4l \equiv 4 \pmod 8$ (case (c)), so l must be odd in all cases. ∎

3. Symmetric similitude matrices. The aim of this section is to prove the following result:

PROPOSITION 3.1. *For every positive odd integer l there exists a primitive symmetric similitude matrix with length of rows* (*columns*) *equal to l. If $A \neq I$ is such a matrix, then for some $\kappa \in \{0,1\}$, $2^\kappa A$ has the form*

$$\begin{pmatrix} b^2-c^2-d^2 & 2bc & 2bd \\ 2bc & -b^2+c^2-d^2 & 2cd \\ 2bd & 2cd & -b^2-c^2+d^2 \end{pmatrix}, \tag{3.1}$$

where b, c, d are relatively prime.

Proof. Recall that according to the well known theorem of Gauss a positive integer is a sum of three squares if and only if it is not of the form $2^{2r}(8s+7)$, where r, s are non-negative integers. Moreover, if the integer is not congruent to 0, 4 or 7 modulo 8, it has a primitive representation, that is, it is a sum of three relatively prime squares (see [C2, p. 144]).

Thus if l is a positive odd integer such that $l \not\equiv 7 \pmod 8$, then $l = b^2+c^2+d^2$, where b, c, d are relatively prime. Then if we choose $a = 0$, the matrix (2.1) is symmetric and primitive according to Proposition 2.2(a).

If $l \equiv 7 \pmod 8$, then $2l$ is a sum of three integer squares. Let $2l = b^2+c^2+d^2$, where b, c, d are relatively prime. Exactly one of b, c, d must be even. If we choose $a = 0$, then the matrix $2^{-1}A(a, b, c, d)$ is symmetric and primitive according to Proposition 2.2(b).

This proves the first part of the proposition. The second part follows immediately from Proposition 2.2 on noting that the matrix (2.1), if not equal to $a^2 I$, is symmetric if and only if $a = 0$. ∎

REMARK 3.2. Notice that if l is odd, then $2l$ is a sum of three squares if and only if l is represented by the quadratic form $x^2+y^2+2z^2$. In fact, as noted above, $2l = b^2+c^2+d^2$ implies that exactly one of b, c, d is even, say $d = 2z$. Since then both b, c are odd, we can find integers x, y (of different parities) such that $b = x+y$ and $c = x-y$. Then $l = x^2+y^2+2z^2$. Conversely, the last equality implies that $2l = 2x^2+2y^2+4z^2 = (x+y)^2+(x-y)^2+(2z)^2$ is a sum of three squares. Thus in Proposition 3.1, we have the first case when l is represented by $x^2+y^2+z^2$, and the second when l is represented by $x^2+y^2+2z^2$ (of course, it may happen that l is represented by both forms).

4. Cubic integral frames with permuted coordinates. In this section, we study the integral similitude 3×3-matrices in which all rows are permutations of the first one. As we show below, this case is in some sense similar to the case of 2×2-matrices and Pythagorean triples and similarly leads to an analog of congruent numbers, which are also governed by rational points on some elliptic curves.

Call two integral matrices of the same size *equivalent* if they differ by a permutation of rows or columns, or by a change of sign of all elements in a number of rows or columns. We denote the equivalence class of A with respect to this relation by $[A]$. Any matrix in which all rows are permutations of the first one will be called *permutational.* Recall that as before, for simplicity of formulations, we limit our considerations to matrices with positive determinant. First of all, we have the following result:

PROPOSITION 4.1. (a) *Every primitive similitude* 3×3 *permutational matrix is equivalent to a symmetric matrix*

$$\begin{pmatrix} -rs & rs-r^2 & rs-s^2 \\ rs-r^2 & rs-s^2 & -rs \\ rs-s^2 & -rs & rs-r^2 \end{pmatrix}, \tag{4.1}$$

where r, s *are relatively prime integers. Moreover*, *the length of the rows* (*columns*) *equals* $l = r^2 - rs + s^2$, *the determinant of this matrix equals* l^3, *and the product of the row* (*column*) *elements is a square* $r^2s^2(r-s)^2$.

(b) *A permutational primitive similitude matrix whose rows* (*columns*) *have length* l *exists if and only if* $l = 1$ *or all the prime factors of* l *or of* $l/3$ *are primes congruent to* 1 *modulo* 3.

Proof. (a) Let A be a permutational primitive similitude matrix. Then, looking at possible configurations of elements in A, it is easy to notice that A is equivalent to a symmetric matrix. Hence the elements of A or $2A$ are given by (3.1), where the second and the third rows are permutations of the first one. This condition easily implies the equality $b + c + d = 0$. Dividing by 2 (notice that we have case (b) of (2.2)) and suitably changing the names of the parameters, we get the desired matrix.

(b) We find that the length of rows of A equals r^2-rs+s^2. It is well known that the integers primitively represented by the quadratic form $r^2 - rs + s^2$ are exactly 1, the products of primes congruent to 1 modulo 3, or 3 times such a product. ∎

Finally, in connection with 3×3 permutational integral similitude matrices, we want to discuss "cuboid" numbers, which appear in a natural way as a three-dimensional analogue of congruent numbers.

Recall that a congruent number is an integer expressing the area of a rational right triangle. If a, b, c are the sides of such a triangle, then multiplying these numbers by their least common denominator k, we may assume that a, b, c are relatively prime positive integers. The area of the right triangle is $S = \frac{1}{2}ab = mk^2$, where m is a square-free congruent number and k a positive integer. It is well known that $a = 2rs$, $b = r^2-s^2$, $c = r^2+s^2$, where $r > s > 0$, $\gcd(r, s) = 1$ and r, s have different parities. Hence $S = rs(r^2-s^2)$ and the congruent numbers m satisfy

$$rs(r^2 - s^2) = mk^2. \tag{4.2}$$

It is well known (see e.g. [K, p. 53]) that m is congruent if and only if there exists a $\mathbb{Q}$-rational point on the elliptic curve

$$y^2 = x^3 - m^2x,$$

which is different from $(0, 0), (\pm m, 0)$ and ∞. The rows of the 2×2-matrix

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 2rs & r^2 - s^2 \\ s^2 - r^2 & 2rs \end{pmatrix}$$

form an integral square frame in $\mathbb{R}^2$, that is, a pair of orthogonal vectors in $\mathbb{R}^2$ with integer coordinates and of integer length, which span a square. The products of the coordinates of these vectors (row elements in A) define congruent numbers.

Similarly, if

$$A = \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}, \qquad ab + bc + ca = 0,$$

is a permutational rational similitude 3×3-matrix, then its rows form a rational cubic frame in $\mathbb{R}^3$, that is, a triple of orthogonal vectors in $\mathbb{R}^3$ with rational coordinates (and of rational length), which span a cube. According to (4.1), if we multiply the elements of A by their least common denominator, say k_0, and assume that $\det A > 0$, we can assume that the first row of A is $-rs,\ rs - r^2,\ rs - s^2$, where r, s are relatively prime integers. Then the product of the row elements in such a matrix is a square. Therefore, we adopt the following:

Definition 4.2. A positive integer m is called *cuboid* if there exists a rational permutational similitude matrix for which the product of the row elements equals m^2.

If for the matrix A, the product of the row elements is a square, that is, $abc = m^2$, then for

$$a = -\frac{rs}{k_0}, \qquad b = \frac{rs - r^2}{k_0}, \qquad c = \frac{rs - s^2}{k_0},$$

we have

$$rs(r - s) = mk^3, \tag{4.3}$$

where r, s are relatively prime integers and $k_0 = k^2$ for a positive integer k. Of course, studying cuboid numbers, we can restrict our attention to cube-free positive integers m. It is easy to see that $m = 1$ is not cuboid. In fact, assuming $m = 1$, the equation (4.3) implies that $r, s, r - s$ are cubes of natural numbers, so existence of r, s contradicts Fermat's Last Theorem for exponent 3. Of course, $m = 2$ is a cuboid number. In general, we have the following result:

Proposition 4.3. *If m is a cube-free positive integer, then the following are equivalent*:

(a) *m is a cuboid number*;
(b) *$m = \alpha\beta(\alpha - \beta)$, where α, β are rational numbers*;
(c) *there exists a $\mathbb{Q}$-rational point on the elliptic curve*

$$y^2 = x^3 + 16m^2$$

other than $(0, \pm 4m)$ and ∞;
(d) *there is a factorization $m = m_1m_2m_3$ such that m_i are pairwise relatively prime and the Diophantine equation*

$$m_1x^3 + m_2y^3 = m_3z^3$$

has a solution (x, y, z) with $xyz \neq 0$.

Proof. The equivalence of (a) and (b) follows directly from the text preceding the proposition.

In order to prove equivalence of (a) and (c), notice that the equality (4.3) implies

$$\left(\frac{r}{s}\right)^2 - \frac{r}{s} = m\left(\frac{k}{s}\right)^3,$$

so setting $x_1 = k/s$, $y_1 = r/s$, we get $y_1^2 - y_1 = mx_1^3$. Now easy computations show that this equation can be transformed into the equivalent form

$$y^2 = x^3 + 16m^2,$$

where

$$x = \frac{4mk}{s}, \qquad y = \frac{4m(2r - s)}{s}.$$

Conversely,

$$r = \frac{(y + 4m)k}{2x}, \qquad s = \frac{4mk}{x}$$

is a solution of the equation $rs(r - s) = mk^3$ if a rational point (x, y) on the elliptic curve $y^2 = x^3 + 16m^2$ is given with $x \neq 0$.

Finally, the equation $m_1x^3 + m_2y^3 = m_3z^3$ in (d) gives $r = m_3z^3, s = m_1x^3$, which satisfy $rs(r-s) = mk^3$ (with $k = xyz$), which is (a). Conversely, the equality $rs(r - s) = mk^3$ with $r, s, r - s$ pairwise relatively prime implies that $m = m_1 m_2 m_3$ and $k = xyz$ for a suitable choice of m_1, m_2, m_3 and x, y, z, so that $r = m_3 z^3, s = m_1 x^3$ and $r - s = m_2 y^3$. ■

Let us denote by $[[a, b, c]]$ the symmetric permutational matrix whose first row is a, b, c (of course, there is only one such matrix).

The torsion groups of the equations $y^2 = x^3 - D$ are well known thanks to the Feuter–Billing theorem (see e.g. [C1, p. 246]). From this result, it follows immediately that the torsion group $E(\mathbb{Q})_{\mathrm{tors}}$ of $y^2 = x^3 + 16m^2$ for cube-free $m \neq 2$ consists of three elements: $(0, \pm 4m)$ and ∞. If $m = 2$, then the rank of $y^2 = x^3 + 64$ is 0, and the group of rational points $E(\mathbb{Q})_{\mathrm{tors}} = \{(0, \pm 8), (-4, 0), (8, \pm 24), \infty\}$ has order 6. A non-trivial symmetric permutational matrix $[[-2, -2, 1]]$ corresponds to the torsion point $(8, 24)$, which gives $r = 2, s = 1$ (for $k = 1$; the remaining torsion points with $x \neq 0$ give the same matrix). Hence, using Proposition 4.3, we can characterize the cuboid numbers in the following way:

Proposition 4.4. *A cube-free number $m \neq 2$ is cuboid if and only if the rank of the elliptic curve $y^2 = x^3 + 16m^2$ is non-zero, which means that there exists a finite rational point with $x \neq 0$ on this curve.*

According to Proposition 4.3(d), the solvability of the equation $x^3 + y^3 = mz^3$ with $xyz \neq 0$ implies, of course, that m is a cuboid number. But, in fact, the following, somewhat unexpected, result holds:

Proposition 4.5. *A* (*cube-free*) *number m is cuboid if and only if the Diophantine equation $x^3 + y^3 = mz^3$ has a non-trivial solution* (*that is, such that $xyz \neq 0$*).

Proof. It remains to prove that for a cuboid number m, the equation $x^3 + y^3 = mz^3$ has a non-trivial solution. If $m \neq 2$ is cuboid, then by Proposition 4.4, the rank of $y^2 = x^3 + 16m^2$ is at least 1. Thus the number of $\mathbb{Q}$-rational points on this curve is infinite and according to the proof of equivalence of (a) and (c) in Proposition 4.3, it is clear that they produce infinitely many solutions (r, s, k) of the equation (4.3). According to the proof of the equivalence (a) and (d) in Proposition 4.3, these solutions give infinitely many solutions to the equations $m_1 x^3 + m_2 y^3 = m_3 z^3$, where $m_1 m_2 m_3 = m$. By [S, Theorem I, p. 210], this implies that the equation $x^3 + y^3 = mz^3$ has a non-trivial integral solution (and, in fact, infinitely many such solutions).

If $m = 2$, then, of course, the equation $x^3 + y^3 = 2z^3$ has a non-trivial solution. ■

Notice that each non-trivial solution (x, y, z) of the equation $x^3 + y^3 = mz^3$ (that is, with $xyz \neq 0$) gives a rational point on the elliptic curve

$$Y^2 = X^3 - 2^4 3^3 m^2. \tag{4.4}$$

In fact,

$$X = \frac{12mz}{x+y}, \qquad Y = \frac{36m(x-y)}{x+y}$$

is such a point when $x+y \neq 0$, that is, $z \neq 0$. Conversely,

$$x = \frac{(36m+Y)z}{6X}, \qquad y = \frac{(36m-Y)z}{6X}$$

gives a rational point on $x^3+y^3 = mz^3$ (notice that $X \neq 0$; for a less formal argument see [ST, p. 24]). Thus Proposition 4.5 implies:

PROPOSITION 4.6. *A* (*cube-free*) *number* $m \neq 1, 2$ *is cuboid if and only if the rank of the elliptic curve* $Y^2 = X^3 - 2^4 3^3 m^2$ *is non-zero*, *which means that there exists a rational point different from* ∞ *on this curve.*

Proof. According to the Fueter–Billing theorem ([C1, Theorem VI, p. 246]), the group of torsion points on the curve $Y^2 = X^3 - 2^4 3^3 m^2$ over $\mathbb{Q}$ is trivial when $m \neq 1, 2$. If $m = 1$ this group has order 3 and is generated by $(12, 36)$, while for $m = 2$, its order is 2 and the generator is $(0, 12)$. In both cases ($m = 1, 2$), it is well known that these two curves have rank 0.

Thus, if m is cuboid, then by Proposition 4.5, there is a non-trivial point on the curve $x^3+y^3 = mz^3$ and the birational transformation above gives a finite rational point on the curve $Y^2 = X^3 - 2^4 3^3 m^2$. By the Fueter–Billing theorem, the curve has non-zero rank if $m \neq 1, 2$. Conversely, if there is a finite rational point on the curve $Y^2 = X^3 - 2^4 3^3 m^2$ and $m \neq 1, 2$, then the Fueter–Billing theorem and the formulae for x, y above show that $xy \neq 0$, so the equation $x^3+y^3 = mz^3$ has a non-trivial solution. ∎

Concerning relations between the elliptic curves $y^2 = x^3 + 16m^2$ and $Y^2 = X^3 - 2^4 3^3 m^2$, which were pointed out by Billing, see [S, 1.2.2 and 1.2.5]. Notice also that Propositions 4.4–4.6 and a part of 4.3 are essentially contained in [ZK, p. 53] (in order to get (ii) in [ZK], m in 4.3(b) may be replaced by $-m$ noting that m and $-m$ are cuboid simultaneously).

5. Examples. In this final section, we want to exemplify the results concerning relations between the cuboid numbers and permutational primitive similitude matrices. Thanks to the results of Proposition 4.5, the sequence of cuboid numbers is well identified and its terms are computed in several places (see [SE, sequence A020897], [ZK] and also the tables in Selmer's paper [S]). Our intention is to give examples of permutational primitive similitude matrices $[[a, b, c]]$ corresponding to the cuboid numbers $1 < m \leq 50$. In order to construct such a matrix, we find a rational point (in fact, integral, with the exception of $m = 31$, when it is impossible) of infinite order (if $m \neq 2$) on the elliptic curve $y^2 = x^3 + 16m^2$ (in case $m = 31$, we use the minimal model $y^2 + y = x^3 + 240$ and the free generator for rational points on this rank 1 curve given in Cremona's tables [C] in order to find a rational point of infinite order on $y^2 = x^3 + 16 \cdot 31^2$). If $m = r(r-1)$, then the situation is very easy, since in this case, $(4r, 4r(r+1))$ is a point on the curve $y^2 = x^3 + 16m^2$ of infinite order if $r > 2$. The corresponding matrix is then $[[-r(r-1), -r, r-1]]$. However, in all cases in the table, we try to choose examples with $\max(|a|, |b|, |c|)$ as small as possible.

Table. Cuboid numbers $m \leq 50$ and corresponding primitive similitude matrices

Cuboid number	Rational point on	(r, s)	Matrix
m	$y^2 = x^3 + 16m^2$		
2	$(8, 24)$	$(2, 1)$	$[[-2, -2, 1]]$
6	$(12, 48)$	$(3, 2)$	$[[-6, -3, 2]]$
7	$(8, 36)$	$(8, 7)$	$[[-56, -8, 7]]$
9	$(9, 45)$	$(9, 8)$	$[[-72, -9, 8]]$
12	$(16, 80)$	$(4, 3)$	$[[-12, -4, 3]]$
13	$(273, 4511)$	$(351, 8)$	$[[-2808, -120393, 2744]]$
15	$(24, 132)$	$(8, 5)$	$[[-24, -40, 15]]$
17	$(8568, 793084)$	$(5832, 1)$	$[[-5832, -34006392, 5831]]$
19	$(24, 140)$	$(27, 19)$	$[[-513, -216, 152]]$
20	$(20, 120)$	$(5, 4)$	$[[-20, -5, 4]]$
22	$(33, 209)$	$(27, 16)$	$[[-432, -297, 176]]$
26	$(12, 112)$	$(27, 26)$	$[[-702, -27, 26]]$
28	$(336, 6160)$	$(28, 1)$	$[[-28, -756, 27]]$
30	$(40{,}280)$	$(5, 3)$	$[[-15, -10, 6]]$
31	$(\frac{8905}{441}, \frac{1422989}{9261})$	$(31 \cdot 42^3, 137^3)$	$[[-5905698432984, 630738927000, -706157817625]]$
33	$(33{,}231)$	$(11, 8)$	$[[-88, -33, 24]]$
34	$(17{,}153)$	$(17, 16)$	$[[-272, -17, 16]]$
35	$(105{,}1085)$	$(35, 8)$	$[[-280, -945, 216]]$
37	$(48{,}364)$	$(64, 37)$	$[[-2368, -1728, 999]]$
42	$(28{,}224)$	$(7, 6)$	$[[-42, -7, 6]]$
43	$(2408{,}118164)$	$(344, 1)$	$[[-344, -117992, 343]]$
49	$(1617{,}65023)$	$(1331, 8)$	$[[-10648, -1760913, 10584]]$
50	$(24{,}232)$	$(27, 25)$	$[[-54, -675, 50]]$

Acknowledgements. We express our thanks to J. Browkin and P. Kurlberg for several useful comments and references on the problem in the literature.

REFERENCES

[C1] J. W. S. Cassels, *The rational solutions of the Diophantine equation* $Y^2 = X^3 - D$, Acta Math. 82 (1950), 243–273.

[C2] —, *Rational Quadratic Forms*, Academic Press, London, 1978.

[C] J. Cremona, *Elliptic curve data*, http://www.maths.nott.ac.uk/personal/jec/ftp/data/.

[D] L. Dickson, *History of the Theory of Numbers*, vol. II, Chelsea, New York, 1952.

[K] A. W. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, NJ, 1992.

[O'M] O. T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren Math. Wiss. 117, Springer, Berlin, 1973.

[S] E. S. Selmer, *The Diophantine equation* $ax^3+by^3+cz^3 = 0$, Acta Math. 85 (1951), 203–362.

[SE] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/∼njas/sequences.

[ST] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, 1992.

[Tu] J. Tunel, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. 72 (1983), 323–334.

[ZK] D. Zagier and G. Kramarz, *Numerical investigations related to L-series of certain elliptic curves*, J. Indian Math. Soc. 52 (1987), 51–69.

Mathematical Sciences
University of Gothenburg
SE-41296 Göteborg, Sweden
E-mail: jub@chalmers.se

Mathematical Sciences
Chalmers University of Technology
SE-41296 Göteborg, Sweden
E-mail: weibull@chalmers.se

Received 15 June 2007 (4934)