MARKOFF EQUATION AND NILPOTENT MATRICES

Norbert Riedel

Abstract A triple \((a, b, c)\) of positive integers is called a Markoff triple iff it satisfies the Diophantine equation

\[ a^2 + b^2 + c^2 = abc. \]

Recasting the Markoff tree, whose vertices are Markoff triples, in the framework of integral upper triangular 3x3 matrices, it will be shown that the largest member of such a triple determines the other two uniquely. This answers a question which has been open for almost 100 years.

Introduction

Markoff numbers, the solutions of the Markoff Diophantine equation, have captured the imagination of mathematicians for over a century. Rooted in A.A. Markoff’s late 19th century work on binary quadratic forms and their connection to the top hierarchy of the worst approximable (quadratic) numbers by rationals, these numbers have found their place in seemingly unrelated endeavors of mathematical activity, such as 4-dimensional manifolds ([HZ]), quantum field theory ([CV]), hyperbolic geometry ([S]), combinatorics ([Po]), group and semi group theory ([Co],[Re]). Two in-depth treatments of the classical aspects of the theory ([Ca], [CF]) bracket almost four decades. One problem that has resisted a conclusive solution so far is the question whether the largest number of a Markoff triple determines uniquely the other two. F.G. Frobenius posed this question in 1913 ([F]). It was restated most recently by M.Waldschmidt in ([W]). Also fairly recent, various contributions appeared which established (essentially) that the answer is affirmative if the largest number in a Markoff triple is a prime power. For the relevant references as well as an elementary proof of this fact see [Zh]. A brief discussion of the uniqueness question is included in the recent exposition of Markoff’s theory by E. Bombieri [B]. In the sequel it will be shown by methods very much within the grasp of Frobenius, that the answer is affirmative throughout. The basic idea for the proof of this fact is to encode every Markoff triple in a (upper) triangular 3x3 matrix, with 1’s in the diagonal, and then to determine an explicit form for the “isomorphs’ of these matrices’. More specifically, given any pair of such matrices, the connectedness of the Markoff tree gives rise to an integral unimodular matrix transforming one into the other, in the same vein as equivalent quadratic forms are related. A (integral) nilpotent rank 2 matrix, which is associated (essentially uniquely) with each of the aforementioned triangular matrices, and which holds all the
relevant information, is then seen to be conjugate to the corresponding matrix associated with any other Markoff triple via that same unimodular matrix. Being of rank 2, these nilpotent matrices provide enough constraints to lead the assumption of two distinct Markoff triples with a common largest member to a contradiction. To summarize, the following statement will be proved:

**Theorem** Given two triples of positive integers, \((a_1, b_1, c_1)\) and \((a_2, b_2, c_2)\), such that

\[ a_k < b_k < c_k , \quad \text{and} \quad a_k^2 + b_k^2 + c_k^2 = a_k b_k c_k , \quad k \in \{1, 2\} , \]

it follows that \( c_1 = c_2 \) implies \( a_1 = a_2 \) and \( b_1 = b_2 \).

Finally, we note that this theorem also answers a conjecture by A. N. Tyurin in complex geometry, stating that a representative exceptional bundle on the complex projective plane is uniquely determined by its rank. For details see A. N. Rudakov’s article [Ru].

1 Markoff tree and triangular 3x3 matrices

Since the matrix manipulations employed in the sequel render the more common version of the Markoff equation

\[ a^2 + b^2 + c^2 = 3abc , \quad a, b, c \in \mathbb{N} \]

impractical, we shall use throughout the alternative form

\[ a^2 + b^2 + c^2 = abc , \]

where \( a = 3a, b = 3b, c = 3c \). It is also common to represent the three numbers as the components of a triple, arranged in increasing order from the left to the right, for instance. This arrangement is unsuitable for the present purpose. While still referring to this arrangement as a Markoff triple, and the largest number as the dominant member, we will supplement this notion by the following, denoting by \( M_n(\mathbb{Z}) \) the set of \( n \times n \) matrices whose entries are integers (non-negative integers).

1.1 Definition A MT-matrix is a matrix in \( M_3(\mathbb{Z}) \) of the form

\[
\begin{pmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1 \\
\end{pmatrix},
\]

where \( a^2 + b^2 + c^2 = abc \), and \( \max\{a, b, c\} \in \{a, c\} \).

For each Markoff triple, with the exception of \((3, 3, 3)\) and \((3, 3, 6)\), there are exactly four MT-matrices. We shall use the notation

\[
M(a, b, c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}
\]
for arbitrary entries $a, b, c$. Throughout this work, a matrix followed by an upper right exponent $t$ denotes the corresponding transposed matrix.

1.2 Proposition For any two MT-matrices $M(a_1, b_1, c_1)$ and $M(a_2, b_2, c_2)$ there exists $N \in \text{SL}(3, \mathbb{Z})$ such that

$$N^t M(a_2, b_2, c_2) N = M(a_1, b_1, c_1),$$

and

$$N^t \begin{pmatrix} c_2 \\ a_2c_2 - b_2 \\ a_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ a_1c_1 - b_1 \\ a_1 \end{pmatrix}.$$

Proof: If

$$P(x) = \begin{pmatrix} 0 & -1 & 0 \\ 1 & x & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Q(y) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & y & 1 \\ 0 & -1 & 0 \end{pmatrix},$$

then $P(x), Q(y) \in \text{SL}(3, \mathbb{Z})$ for $x, y \in \mathbb{Z}$, and

$$P(a)^t M(a, b, c) P(a) = M(a, c, ac - b)$$

$$Q(c)^t M(a, b, c) Q(c) = M(ac - b, a, c).$$

If $M(a, b, c)$ is a MT-matrix, then the matrices on the right hand side are also MT-matrices, and both are associated with the same neighbor of the Markoff triple corresponding to the MT-matrix on the left hand side. Here the word neighbor refers to two adjacent Markoff triples in the so-called Markoff tree. By the very definition of MT-matrices the Markoff triple associated with the right hand side is further removed from the root of the tree than the corresponding triple on the left hand side. Furthermore, application of transposition and conjugation by

$$\mathcal{J} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

to the two identities above leads to new identities:

$$Q(a)^t M(c, b, a) Q(a) = M(ac - b, c, a),$$

$$P(c)^t M(c, b, a) P(c) = M(c, a, ac - b).$$

So, on the right hand side of these four identities combined, we obtain exactly the four MT-matrices associated with a common Markoff triple. It follows that, through repeated applications of the four identities, the claimed statement is true in case $a_1 = b_1 = c_1 = 3$. Notice that it is vital that there is only one MT-matrix associated with the root of the Markoff tree! The claim in the general
case now follows immediately by combining the special case applied to $M(a_1, b_1, c_1)$ and to $M(a_2, b_2, c_2)$ separately.

**Remarks**

1) The first two of the identities in the proof of Proposition 1.1 give rise to the definition of neighbors in a binary tree with MT-matrices serving as vertices. The Markoff tree, which is not entirely binary, can be recovered from this tree simply by identifying the four MT-matrices with the Markoff triple they are associated with.

2) If 

$$N^tM(3,3,3)N = M(a,b,c), N^t \begin{pmatrix} 3 \\ 6 \\ 3 \end{pmatrix} = \begin{pmatrix} c \\ ac-b \\ a \end{pmatrix}, N \in \mathcal{G},$$

then

$$N^{-1}M(-3,6,-3)(N^{-1})^t = M(-a,ac-b,-c).$$

Therefore, if

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (N^{-1})^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

then

$$(N)^tM(3,6,3)N = M(a,ac-b,c), N^t \begin{pmatrix} c \\ b-ac \\ a \end{pmatrix} = \begin{pmatrix} 3 \\ -6 \\ 3 \end{pmatrix}.$$

Since

$$P(3)^tM(3,6,3)P(3) = Q^t(3)M(3,6,3)Q(3) = M(3,3,3),$$

it follows that, given any two Markoff triples, any permutation of the first, $(a_1, b_1, c_1)$ say, and any permutation of the second, $(a_2, b_2, c_2)$ say, there exists $N \in \text{SL}(3,\mathbb{Z})$, such that

$$N^tM(a_2,b_2,c_2)N = M(a_1,b_1,c_1).$$

3) Markoff triples have also been associated with triples of integral unimodular matrices, exploiting two of the so-called Fricke identities. For an in-depth survey of this approach, mostly due to H. Cohn, see [Pe]. The connection between that approach and the present one is as follows: Let

$$A_0 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } B_0 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$ 

We say that $(A_0, A_0B_0, B_0)$ is an admissible triple. New admissible triples can be generated out of given ones by the rule, that if $(A, AB, B)$ is an admissible triple, then so are $(A, A^2B, AB)$ and $(AB, AB^2, B)$. Fricke’s identities ensure that the corresponding triple of traces associated with an admissible triple solves
the Markoff equation. Moreover, the lower left entry of each matrix is one-third of its trace. So, once again with the notion of neighbor defined in a natural way, the admissible triples represent nothing but the vertices of the Markoff tree. However, since \((\text{Tr}(A_0), \text{Tr}(A_0B_0), \text{Tr}(B_0)) = (3, 6, 3)\), the first Markoff triple \((3, 3, 3)\) is missing from the picture. As pointed out in the proof of Proposition 1.2, its availability in the present approach is crucial, due to the fact that it is the only Markoff triple for which all components are equal. Exploiting the fact that a matrix solves its own characteristic equation, one can easily see that each matrix in an admissible triple can be written as a linear combination of the matrices \(A_0, A_0B_0\) and \(B_0\) with integral coefficients. If \(a_2 = b_2 = c_2 = 3\) in Proposition 1.2, and if \(N\) is the matrix exhibited in its proof, then the coefficient vectors for the admissible triple associated with \((c_1, a_1c_1-b_1, a_1)\) are exactly the columns of the matrix \(N\) in the order of their appearance. The 1’s in the diagonal of the matrix \(M(a_1, b_1, c_1)\) reflect the unimodularity of the 2×2 matrices in the corresponding admissible triple. Other choices for the basis \(A_0, A_0B_0\) and \(B_0\) appear in the literature, mostly motivated by the desire to connect them to the continued fraction expansion of the quadratic irrationals, which are at the core Markoff’s original work. That all these choices are connected via a single integral nilpotent 3×3 matrix, and that this matrix holds the key to the uniqueness question of the Markoff triples, is the central observation in the present work.

2. Markoff triples and nilpotent matrices

The statement of Proposition 1.1 raises the issue of “automorphs”, to borrow a notion from the theory of quadratic forms. More specifically, what can be said about the matrices \(N \in \text{SL}(3, \mathbb{Z})\) which leave \(M\) invariant, i.e.

\[
N^tM(a, b, c)N = M(a, b, c)?
\]

There are two natural candidates that could serve as generators. While defining them, we will temporarily relinquish the requirement that \(a, b \text{ and } c\) are in \(\mathbb{Z}\). A commutative ring will do. Let

\[
H(a, b, c) = M(a, b, c)^{-1}M(a, b, c)^t.
\]

If possible, we will suppress the arguments.

2.1 Proposition a) \(H^tMH=M\)

b) If \(N\) is invertible and \(N^tM(a_2, b_2, c_2)N = M(a_1, b_1, c_1)\), then

\[
N^{-1}H(a_2, b_2, c_2)N = H(a_1, b_1, c_1).
\]

Proof: a)

\[
H^t MH = M(M^{-1})^tMM^{-1}M^t = M.
\]

b) Writing

\[
M_k = M(a_k, b_k, c_k), H_k = M_k^{-1}M_k^t, k \in \{1, 2\},
\]
\[ N^t M_2 N = M_1 \text{ implies} \]
\[ N^t M_2 N = M_1^t \text{ and } N^{-1} M_2^{-1} (N^t)^{-1} = M_1^{-1}, \]
so,
\[ N^{-1} H_2 N = N^{-1} M_2^{-1} M_1^t N = N^{-1} M_2^{-1} (N^t)^{-1} N^t M_2^t N = M_1^{-1} M_1^t = H_1 \]
\[ \square \]

The explicit form of \( H \) is
\[
H(a, b, c) = \begin{pmatrix}
1 - (a^2 + b^2 - abc) & ac^2 - bc - a & ac - b \\
1 - a^2 & 1 - c^2 & -c \\
1 - b^2 & c & 1
\end{pmatrix}
\]

Its characteristic polynomial is given by
\[
\det(H - \lambda E) = - (\lambda - 1)^3 - d(\lambda - 1)^2 - d(\lambda - 1),
\]
d = a^2 + b^2 + c^2 - abc

**Remark** The matrix \( H \) has a place in quantum field theory ([CV]). More specifically \( H \) (or rather its inverse), is the monodromy matrix for the so-called \( \mathbb{CP}^2 \) \( \sigma \)-model. This is a model with \( N=2 \) superconformal symmetry and Witten index \( n=3 \).

The other candidate is related to a matrix \( R \epsilon M_3(\mathbb{Z}) \) which solves the matrix equation
\[ R^t M + MR = 0 \]
This matrix is unique up to a multiplicative constant. We can choose
\[
R = \begin{pmatrix}
a^2 + b^2 - abc & 2a + bc - ac^2 & 2b - ac \\
bc - 2a & c^2 - a^2 & 2c - ab \\
ac - 2b & -2c - ab + a^2c & abc - b^2 - c^2
\end{pmatrix}
\]

Its characteristic polynomial is
\[
\det(R - \lambda E) = -\lambda^3 + d(d - 4)\lambda, d = a^2 + b^2 + c^2 - abc
\]

In the context of real numbers we can state the following:

**2.2 Proposition** For any \( x \in \mathbb{R} \), \( (e^x R)^t M e^x R = M \).

**Proof** Since \( (R^t)^k M = (-1)^k M R^k \) for all \( k \in \mathbb{N} \),
\[
(e^x R)^t M e^x R = \sum_{k,l=0}^{\infty} x^{k+l} (R^t)^k M R^l = \sum_{k,l=0}^{\infty} (-1)^k x^{k+l} M R^{k+l} = M e^{-R e^R} = M.
\]
\[ \square \]
Remark In reference to Remark 3 in Section 1, the conjugation of $N$ by $e^{-\frac{1}{d} R}$ corresponds to the conjugation of the components of the related admissible triple by the matrix

$$
\begin{pmatrix}
1 & x \\
0 & 1
\end{pmatrix}.
$$

The matrices $H$ and $R$ commute, and so they share common eigenvectors. Let us briefly consider $R$ in the context of the ring $P_\mathbb{Z}[X]$, the polynomials with integral coefficients. There are exactly two cases in which $R$ is nilpotent, namely $d=0$ and $d=4$. The case $d=0$ leads us to Markoff triples, while the case $d=4$ leads us to triples of Tchebycheff polynomials. These are monic polynomials which are mutually orthogonal with respect to a certain probability measure derived from classical potential theory. The triples of integers representing the degrees of these polynomials form the vertices of the so-called “Euclid tree”. While the kinship between the cases $d=0$ and $d=4$ goes well beyond the shared nilpotence of $R$, a fact which has been exploited by Zagier in [Z] with profit in deriving an asymptotic bound for Markoff numbers through comparison of the two cases, the uniqueness question, which is the subject of the present investigation, has clearly a negative answer in the case $d=4$. The crucial difference that accounts for the opposite answers to this question is the fact that, while $R$ is of rank 2 in the case $d=0$, it is of rank 1 in the case $d=4$. Notice also that, while $H - E$ is nilpotent for $d=0$, it still has two equal but non-vanishing eigenvalues for $d=4$.

From now on we will be exclusively concerned with Markoff triples. Let

$$
S = H - E,
$$

where $E$ denotes the unit matrix.

2.3 Proposition a) $H = e^{-\frac{R}{d}} = E - \frac{1}{d} R + \frac{1}{d^2} R^2$

b) $S^2 = \begin{pmatrix} c & -b \\ -b & a \end{pmatrix} (c, ac - b, a)$

The proof is obtained through straightforward manipulations, involving repeated employment of the Markoff property. Proposition 2.3 shows that we are essentially dealing with a single nilpotent matrix of rank 2. It will follow from our subsequent discussion that all “automorphs” have the form $e^{sR}$ for a suitable rational parameter $s$. Since the matrix $R$ has some mild redundancies, thus making manipulations a bit more lengthy, and since these redundancies are not shared by the matrix $S$, we will be working in the sequel with $S$ only.

3 Proof of the Theorem

If the dominant member $m$ of a Markoff triple is either 3 or 6, then the claim is obviously true. Therefore we shall assume henceforth that $m \neq 3$ and $m \neq 6$. 

7
First we construct a matrix $T$ which conjugates $S$ to its Jordan form. Starting with an eigenvector for $S$, yields

\[
S \begin{pmatrix} c \\ ac - b \\ a \end{pmatrix} = ac \begin{pmatrix} ac^2 - bc - a \\ -e^2 \\ c \end{pmatrix}
\]

Notice that the vector on the right hand side is nothing but the second column of $S$ multiplied by $ac$. Applying $S$ to its second column yields by virtue of the Markoff property

\[
(ac - b) \begin{pmatrix} c \\ -b \\ a \end{pmatrix},
\]

which is in the kernel of $S$. So, if we define

\[
T = \begin{pmatrix}
  c & ac(ac^2 - bc - a) & ac(ac - b)c \\
  ac - b & ac(-c^2) & ac(ac - b)(-b) \\
  a & acc & ac(ac - b)a
\end{pmatrix}
\]

then we have

\[
ST = T \begin{pmatrix}
  0 & 0 & 0 \\
  1 & 0 & 0 \\
  0 & 1 & 0
\end{pmatrix}.
\]

Furthermore,

\[
\det(T) = -[ac(ac - b)]^3
\]

In order to manage the manipulations involving this matrix efficiently, we will use a suitable factorization. If

\[
A = \begin{pmatrix}
  0 & c(ac - b) - a & c \\
  1 & -e^2 & -b \\
  0 & c & a
\end{pmatrix},
\]

\[
B = \begin{pmatrix}
  ac & 0 & 0 \\
  0 & 1 & 0 \\
  0 & 0 & 1
\end{pmatrix}
\]

\[
C = \begin{pmatrix}
  1 & 0 & 0 \\
  0 & 1 & 0 \\
  0 & 1 & 1
\end{pmatrix},
\]

\[
D = \begin{pmatrix}
  1 & 0 & 0 \\
  0 & ac & 0 \\
  0 & 0 & ac(ac - b)
\end{pmatrix},
\]

then $T = ABCD$. Moreover

\[
A^{-1} = \frac{1}{(ac - b)^2} \begin{pmatrix}
  -(ac - b) & -(ac - b)^2 & -a(ac - b) \\
  -a & 0 & c \\
  c & 0 & a - c(ac - b)
\end{pmatrix}
\]
\[= \frac{1}{(ac - b)^2} FKL,\]

where
\[F = \begin{pmatrix} ac - b & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\]
\[K = \begin{pmatrix} c & 1 & a \\ a & 0 & -c \\ -c & 0 & c(ac - b) - a \end{pmatrix},\]
\[L = \begin{pmatrix} 1 & 0 & 0 \\ 0 & ac - b & 0 \\ 0 & 0 & 1 \end{pmatrix}.\]

We shall also need the matrix
\[U = MT = VBCD,\]

where
\[V = \begin{pmatrix} a & -a & c \\ 1 & 0 & m \\ 0 & c & a \end{pmatrix},\]
\[V^{-1} = \frac{1}{(ac - b)^2} \begin{pmatrix} c(ac - b) & -b(ac - b) & a(ac - b) \\ a & -a^2 & a(ac - b) - c \\ -c & ac & -a \end{pmatrix}.\]

Now consider two Markoff triples (at this point not necessarily distinct) with a common dominant member \(m\). We assume that
\[m = a_1c_1 - b_1 = a_2c_2 - b_2,\]
where \(a_k, b_k\) and \(c_k\) are the components of the unique neighbor closer to the root of the Markoff tree, for \(k = 1\) and \(k = 2\), respectively. This arrangement accommodates all vertices of the Markoff tree except for the root. In order to make use of the matrices introduced above in the present context, we adopt the convention of attaching an index 1 or 2 to their names, depending on the Markoff triple in reference. Let
\[N = T_2T_1^{-1}, r = \frac{a_1c_1}{a_2c_2}.\]

Then
\[\det(rN) = 1\]

By Proposition 1.1 there exists a matrix \(N \in \mathcal{G}\) such that
\[(3.1)\]
\[N^tM(a_2, b_2, c_2)N = M(a_1, b_1, c_1).\]
By Proposition 2.1(b) \[ N^{-1}S_2N = S_1 \]

Since \((N)_{N^{-1}}S_2N = S_1\), it follows that \(N(N^{-1})_N = S_1\) and \(S_2\) commute. Since \(S_2\) has rank 2, this implies that there exist rational numbers \(s\) and \(t\), such that

\[ \tag{3.2} \]

\[ N = r(E + sS_2 + tS_2^2)N = rT_2 \begin{pmatrix} 1 & 0 & 0 \\ s & 1 & 0 \\ t & s & 1 \end{pmatrix} T_1^{-1}eM_3(\mathbb{Z}). \]

Substituting (3.2) into (3.1) yields the identity

\[ \tag{3.3} \]

\[ r(T_1')^{-1} \begin{pmatrix} 1 & s & t \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} T_2' = r^{-1}(M(a_2, b_2, c_2)T_2 \begin{pmatrix} 1 & 0 & 0 \\ s & 1 & 0 \\ t & s & 1 \end{pmatrix}) (M(a_1, b_1, c_1)T_1)^{-1} = \]

\[ r^{-1}U_1 \begin{pmatrix} 1 & 0 & 0 \\ -s & 1 & 0 \\ s^2 - t & -s & 1 \end{pmatrix} U_2^{-1} \]

We are now going to evaluate the three terms in (3.2). Writing \(F, L\) in place of \(F_1, L_1\), respectively,

\[ rm^2N = rA_2B_2C_2D_1D_2^{-1}C_1^{-1}B_1^{-1}FK_1L = \]

\[ A_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{a_2c_2} - \frac{1}{a_1c_1} & 0 & 1 \end{pmatrix} FK_1L = \]

\[ \begin{pmatrix} c_2(a_2c_2 - \frac{1}{a_2a_1})m & c_2m - a_2 & c_2 \\ (1 - b_2(a_2c_2 - \frac{1}{a_2a_1}))m & -c_2^2 - b_2 & c_2 \\ a_2(a_2c_2 - \frac{1}{a_2a_1})m & c_2 & a_2 \end{pmatrix} K_1L = \]

\[ \Gamma_0 + mG_1 + m^2G_2, \]

where,

\[ \Gamma_0 = \begin{pmatrix} -(a_1a_2 + c_1c_2) & 0 & -(a_1c_2 - c_1a_2) \\ -(a_1c_2 - c_1a_2)c_2 & 0 & (a_1c_2 - c_1a_2)a_2 \\ a_1c_2 - c_1a_2 & 0 & -(a_1a_2 + c_1c_2) \end{pmatrix} + m \begin{pmatrix} a_1c_2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & c_1a_2 \end{pmatrix} \]

\[ \Gamma_1 = \left( \frac{1}{a_2c_2} - \frac{1}{a_1c_1} \right) \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} \]
\[ \Gamma_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \]

Since
\[ m^2 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} T^{-1} = a^{-1} c^{-1} \begin{pmatrix} 0 & 0 & 0 \\ m & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} KL = a^{-1} c^{-1} L \begin{pmatrix} 0 & 0 & 0 \\ c & 1 & a \\ a & 0 & -c \end{pmatrix} L, \]
we get for the second term
\[ mrS_2N = mrT_2 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} T_1^{-1} = A_2 \begin{pmatrix} 0 & 0 & 0 \\ c_1 & 1 & a \\ a_1 & 0 & -c_1 \end{pmatrix} L = \Omega_0 + m \Omega_1, \]
where
\[ \Omega_0 = \begin{pmatrix} a_1 c_2 - c_1 a_2 & 0 & -(a_1 a_2 + c_1 c_2) \\ -(a_1 a_2 + c_1 c_2) c_2 & 0 & -(a_1 c_2 - c_1 a_2) c_2 \\ a_1 a_2 + c_1 c_2 & 0 & a_1 c_2 - c_1 a_2 \end{pmatrix}, \]
\[ \Omega_1 = \begin{pmatrix} 0 & -a_2 & 0 \\ a_1 & -c_2 & -c_1 \\ 0 & c_2 & 0 \end{pmatrix} + c_2 \begin{pmatrix} c_1 & m & a_1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \]
Finally, for the third term
\[ rS_2N^\sim = \Phi^t = \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} (c_1, m, a_1). \]
In order to manipulate the identity (3.3) we shall need a similar decomposition involving the matrix \( U \).
\[ r^{-1} m^2 U_1 U_2^{-1} = V_1 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\left(\frac{1}{a_2 c_2} - \frac{1}{a_1 c_1}\right) & 0 & 1 \end{pmatrix} \begin{pmatrix} c_2 m & -b_2 m & a_2 m \\ a_2 & -a_2^2 & a_2 m - c_2 \\ -c_2 & a_2 c_2 & -a_2 \end{pmatrix} = \Theta_0 + m \Theta_1 + m^2 \Theta_2, \]
where
\[ \Theta_0 = \begin{pmatrix} -(a_1 a_2 + c_1 c_2) & -(a_1 c_2 - c_1 a_2) c_2 & a_1 c_2 - c_1 a_2 \\ 0 & 0 & 0 \\ -(a_1 c_2 - c_1 a_2) & (a_1 c_2 - c_1 a_2) a_2 & -(a_1 a_2 + c_1 c_2) \end{pmatrix}, \]
\[ +m \begin{pmatrix} a_1 c_2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & c_1 a_2 \end{pmatrix}, \]

11
\[
\Theta_1 = -\left( \frac{1}{a_2c_2} - \frac{1}{a_1c_1} \right) \begin{pmatrix} c_1 \\ m \\ a_1 \end{pmatrix} (c_2, -b_2, a_2),
\]
\[
\Theta_2 = \Gamma_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.
\]

Since
\[
m^2 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} U^{-1} = a^{-1} c^{-1} \begin{pmatrix} 0 & 0 & 0 \\ cm & -bm & am \\ a & -a^2 & am - c \end{pmatrix},
\]
we get
\[
r^{-1} m U_1 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} U_2^{-1} = V_1 \begin{pmatrix} 0 & 0 & 0 \\ c_2 & -b_2 & a_2 \\ a_2 & -a_2^2 & a_2 m - c_2 \end{pmatrix}
\]
\[
= \Lambda_0 + m \Lambda_1,
\]
where
\[
\Lambda_0 = \begin{pmatrix} -(a_1c_2 - c_1a_2) & (a_1c_2 - c_1a_2)a_2 & -(a_1a_2 + c_1c_2) \\ 0 & 0 & 0 \\ a_1a_2 + c_1c_2 & -(a_1a_2 + c_1c_2)a_2 & -(a_1c_2 - c_1a_2) \end{pmatrix},
\]
\[
\Lambda_1 = \begin{pmatrix} 0 & -a_1 & 0 \\ a_2 & -a_2^2 & -c_2 \\ 0 & c_1 & 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 & 0 & c_1 \\ 0 & 0 & m \\ 0 & 0 & a_1 \end{pmatrix}.
\]

Finally,
\[
r^{-1} U_1 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} U_2^{-1} = \Phi
\]

Let
\[
N(s) = re^{-\frac{b_2 s}{m}} N^\sim - \frac{1}{m} \left( \frac{1}{a_2c_2} - \frac{1}{a_1c_1} \right) \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} (c_1, m, a_1) =
\]
\[
rN^\sim e^{-\frac{b_2 s}{m}} - \frac{1}{m} \left( \frac{1}{a_2c_2} - \frac{1}{a_1c_1} \right) \begin{pmatrix} c_2 \\ -b_2 \\ a_2 \end{pmatrix} (c_1, m, a_1)
\]

Then we have the following crucial representation of all "rational isomorphs".

3.1 Proposition If \( Q \in \text{SL}(3, \mathbb{Q}) \), then
(3.5) \[ Q^t M_2 Q = M_1, \]
if and only if there exists a rational number \( s \) such that \( Q = N(s) \).

**Proof** First, by our discussion above, we know that if (3.5) holds true, then there exist rational numbers \( s \) and \( t \), such that

\[ Q = r(E + sS_2 + tS_2^2)N. \]

Now given this representation, \( Q \) satisfies (3.5) if and only if

\[
(3.6) r(T_1^{-1})^{-1} \begin{pmatrix} 1 & s & t \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} T_2^t - r^{-1}U_1 \begin{pmatrix} 1 & 0 & 0 \\ -s & 1 & 0 \\ s^2 - t & -s & 1 \end{pmatrix} U_2^{-1} = 0.
\]

Employing the above decompositions, the left hand side of (3.6) turns into

\[
\frac{1}{m^2} \Gamma_0^t + \frac{1}{m} \Gamma_1^t + \Gamma_2^t + s \Omega_0^t + s \Omega_1^t + t \Phi - \frac{1}{m^2} \Theta_0 - \frac{1}{m} \Theta_1 - \Theta_2 + \frac{1}{m} \Lambda_0 + s \Lambda_1 = (s^2 - t) \Phi.
\]

Since

\[
\Gamma_0^t = \Theta_0, \Gamma_1^t = -\Theta_1 = \left( \frac{1}{a_2 c_2} - \frac{1}{a_1 c_1} \right) \Phi, \Gamma_2^t = \Theta_2,
\]

the left hand side of (3.6) simplifies to

\[
\frac{s}{m} (\Omega_0^t + \Lambda_0) + s (\Omega_1^t + \Lambda_1) + (2 \left( \frac{1}{m} \left( \frac{1}{a_2 c_2} - \frac{1}{a_1 c_1} \right) \Phi + \frac{1}{m^2} \right) + t) - s^2) \Phi.
\]

But

\[
\Omega_1^t + \Lambda_1 = \Phi + \begin{pmatrix} 0 & c_1 b_2 & 0 \\ 0 & 0 & 0 \\ 0 & a_1 b_2 & 0 \end{pmatrix},
\]

while

\[
\Omega_0^t + \Lambda_0 = -m \begin{pmatrix} 0 & c_1 b_2 & 0 \\ 0 & 0 & 0 \\ 0 & a_1 b_2 & 0 \end{pmatrix},
\]

so that the left hand side of (3.6) finally takes the form

\[
(2 \left( \frac{1}{m} \left( \frac{1}{a_2 c_2} - \frac{1}{a_1 c_1} \right) \Phi + \frac{1}{m^2} \right) + t) - s^2) \Phi.
\]

This expression is equal to zero if and only if

\[
t = \frac{1}{2} (s^2 - s) - \frac{1}{m} \left( \frac{1}{a_2 c_2} - \frac{1}{a_1 c_1} \right),
\]

which is equivalent with \( Q = N(s) \). □

**Remark** (a) If \( a_1 = a_2, c_1 = c_2 \), then the proof of Proposition 3.1 shows that all “automorphs” of an MT-matrix are of the form \( e^{\pi s} \) for some integer \( s \).
(b) If \( a_1 = c_2, c_1 = a_2 \), then (3.4) provides an explicit form of the “isomorphs” for the corresponding MT-matrices, and as such could be useful in further studies of Markoff triples and their applications.

c) All integral “isomorphs” are actually contained in a proper congruence subgroup of \( \text{SL}(3, \mathbb{Z}) \), namely the matrices which are orthogonal modulo 3.

d) Notice that due to cancellation the matrix \( N(s) \) can be written more compactly as follows,

\[
N(s) = \frac{1}{m^2} \Gamma_0 + \Gamma_2 + \frac{s}{m} (\Omega_0 + m\Omega_1) + \frac{s^2 - s}{2} \Phi^t.
\]

In order to exploit the number theoretic features of the representation (3.4), we shall need the following sequence of lemmas, culminating with the factorization of \( m \) stated in Corollary 3.5 below.

**3.2 Lemma** If \( q \neq 2, 3 \) is a prime factor of \( m \), then \( q \) does not divide at least one of the following two terms

\[ a_1a_2 + c_1c_2, a_1a_2 - c_1c_2. \]

The same conclusion holds for the terms

\[ a_1c_2 + c_1a_2, a_1c_2 - c_1a_2. \]

**Proof** Suppose the first statement were not true, i.e. both terms are divisible by \( q \). Then \( q \) also divides

\[ (a_1a_2 + c_1c_2) + (a_1a_2 - c_1a_2) = 2a_1a_2. \]

Since \( q \neq 2, 3 \), neither \( a_1 \) nor \( a_2 \) is divisible by \( q \), and so this is impossible. The same argument proves the second statement. \( \square \)

**3.3 Lemma** If \( q \neq 3 \) is a prime factor of \( m \), then

a) \( q \) divides \( a_1c_2 - c_1a_2 \) if and only if it divides \( a_1a_2 + c_1c_2 \),

b) \( q \) divides \( a_1a_2 - c_1c_2 \) if and only if it divides \( a_1c_2 + c_1a_2 \).

**Proof** a) If \( q \) divides \( c_2 - c_1a_2 \), then

\[
a_1 = \frac{a_1}{a_2} a_2 \text{ and } c_1 = \frac{a_1}{a_2} c_2 \text{ modulo } q.
\]

Hence

\[
0 = mb_1 = a_1^2 + c_1^2 = \frac{a_1}{a_2} (a_1a_2 + c_1c_2) \text{ modulo } q,
\]

which in turn implies

\[
a_1a_2 + c_1c_2 = 0 \text{ modulo } q.
\]
If, on the other hand, $q$ divides $a_1a_2 + c_1c_2$, then

$$a_1 = \frac{a_1}{c_2}c_2 \text{ and } c_1 = -\frac{a_1}{c_2} \text{ modulo } q.$$  

Hence

$$0 = mb_1 = a_1^2 + c_1^2 = \frac{a_1}{c_2}(a_1c_2 - c_1a_2) \text{ modulo } q,$$

which in turn implies

$$a_1c_2 - c_1a_2 = 0 \text{ modulo } q.$$  

b) All one has to do is switch $a_1$ and $c_1$, or equivalently, $a_2$ and $c_2$, and copy the proof for part a). □

3.4 Lemma Suppose that $m = nq^l$, $q \neq 2, 3$ is a prime factor, and $n, q$ relatively prime. Then

either $q^2$ divides $a_1c_2 - c_1a_2$ or $q^2$ divides $a_1a_2 - c_1c_2$.

Proof We shall need the following:

\begin{equation}
(3.7) \quad (a_1c_2 - c_1a_2)(a_1a_2 - c_1c_2) = m^2(b_1 - b_2)
\end{equation}

To see this, we employ Markoff’s property.

$$(a_1c_2 - c_1a_2)(a_1a_2 - c_1c_2) = (a_1^2 + c_1^2)a_2c_2 - (a_2^2 + c_2^2)a_1c_1 = m(b_1a_2c_2 - b_2a_1c_1) = m[(b_1-a_1c_1)a_2c_2-(b_2-a_2c_2)a_1c_1] = m^2((a_1c_1-a_2c_2)+m^2((b_1-a_1c_1-a_2c_2)) = m^2(b_1 - b_2).$$

If $b_1 - b_2 = 0$, then the claim is obviously true, because one of the two terms is zero, while the other one and $q$ are relatively prime. Now suppose that $b_1 - b_2 \neq 0$, and that $q$ divides $a_1c_2 - c_1a_2$ and $a_1a_2 - c_1c_2$. Then by Lemma 3.3 $q$ divides $a_1a_2 + c_1c_2$ and $a_1c_2 + c_1a_2$ as well. By Lemma 3.2 this is impossible. In conclusion, (3.7) implies that $q^2$ divides either $a_1c_2 - c_1a_2$ or $a_1a_2 - c_1c_2$, as claimed. □

3.5 Corollary There exists a unique factorization of $m = \frac{m}{3}$ if $m$ is odd, and of $m = \frac{m}{q}$ if $m$ is even, $m = fg$ say, where and $f$ and $g$ are positive, relatively prime integers, such that

$f^2$ divides $a_1c_2 - c_1a_2$ and $g^2$ divides $a_1a_2 - c_1c_2$.

Moreover, $f$ is relatively prime to $a_1a_2 - c_1c_2$, while $g$ is relatively prime to $a_1c_2 - c_1a_2$.

Proof This follows immediately from Lemma 3.3 and 3.4. □

Remark Notice that the the factorization in Corollary 3.5 is trivial if $\{a_1,c_1\} = \{a_2,c_2\}$. In this case we have $\{f,g\} = \{1,m\}$.  

15
From now on we shall assume that we have two distinct Markoff triples with a common dominant member. So we suppose that
\[ \{a_1, c_1\} \cap \{a_2, c_2\} = \emptyset \]
This implies that \(a_1c_1 - a_2c_2 = b_1 - b_2 \neq 0\), and hence \(a_1c_2 - c_1a_2 \neq 0\), \(a_1a_2 - c_1c_2 \neq 0\), by (3.7).

3.6 Lemma Both, \(f\) and \(g\) have at least one prime factor which is not equal to 2 or 3, respectively.

Proof Suppose that one of the two factors, \(g\) say, does not have a prime factor other than 2 or 3. If \(m\) is odd, then \(m^2\) divides \(a_1c_2 - c_1a_2\), which is non-zero by our assumption. This implies \(m^2 < a_1c_2\) or \(m^2 < c_1a_2\). In either case, \(m\) is smaller than at least one of the four numbers \(a_1, c_1, a_2, c_2\), which is impossible. If \(m\) is even, then \(a_1, c_1, a_2, c_2\) are odd, and so \(a_1c_2 - c_1a_2\) is even. It follows that \(\frac{a_1c_2}{2}\) divides \(a_1c_2 - c_1a_2\). As in the reasoning above we infer that \(\frac{a_1c_2}{2}\) is less than at least one of the four numbers \(a_1, c_1, a_2, c_2\), which is impossible since the dominant member of a Markoff triple exceeds the others by at least a factor 6. Finally, if \(f\) does not have a prime factor other than 2 or 3, we apply the same line of reasoning to \(a_1a_2 - c_1c_2\), which is also non-zero by our assumption, thus leading to a contradiction as well. \(\Box\)

We shall now return to the representation (3.4), introducing the following notation. Writing temporarily
\[ N(a_1, b_1, c_1, a_2, b_2, c_2, s) = N(s), \]
we define for \(i, j \in \{\pm 1, \pm 2\},\)
\[ N(i, j)(s) = \begin{cases} N(a_i, b_i, c_i, a_j, b_j, c_j, s) & \text{if } i, j > 0 \\ N(c_i, b_i, a_i, a_j, b_j, c_j, s) & \text{if } i > 0, j < 0 \\ N(a_i, b_i, c_i, c_j, b_j, a_j, s) & \text{if } i > 0, j < 0 \\ N(c_i, b_i, a_i, c_j, b_j, a_j, s) & \text{if } i, j < 0 \end{cases} \]
Also, writing for \(i \in \{1, 2\}\)
\[ T(a_i, b_i, c_i) = T_i, \]
we define
\[ T_{-i} = T(c_i, b_i, a_i). \]
Finally, we define the matrices \(R_{-i}\) and \(S_{-i}\) in a similar fashion.

Remarks 1) Recalling that \(\mathcal{J} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\), one can show that \(\mathcal{J}_i = \mathcal{J} \mathcal{N}(i, -1)(0)\) is nothing but the involution which is uniquely determined by the identities \(\mathcal{J}_i R_i \mathcal{J}_i = -R_i, \mathcal{J}_i \mathcal{J} = \mathcal{J} \mathcal{J}_{-i} \).

2) If \(a_2 = c_1, b_2 = b_1, c_2 = a_1\) in Proposition 1.2, then the connection outlined in the last remark in section 1 suggests, that for the matrix \(\mathcal{N}\) constructed in
we conclude

Since for any 

Proposition 1.2 one has \( N_{(1,-1)}(s) = N \), where either \( s \) or \( -s \) is the number closest to zero with the property \( N_{(1,-1)}(s) \in \text{SL}(3, \mathbb{Z}) \).

**Lemma 3.7** For \( i, j \in \{\pm 1, \pm 2\} \), and for any two rational numbers \( s, t \), the following identities hold:

\[
e^{-rac{R_i}{T}(s+t)} = N_{(i,i)}(s+t) = N_{(j,j)}(s)N_{(i,j)}(t), N_{(i,-i)}(s+t) = N_{(j,-i)}(s)N_{(i,j)}(t).
\]

**Proof** Since for any \( i, j \in \{\pm 1, \pm 2\} \), and for any rational number \( s \)

\[
N_{(i,j)}(s) = e^{-rac{R_i}{T}(s)}N_{(i,j)}(0) = N_{(i,j)}(0)e^{-rac{R_i}{T}(s)},
\]

it suffices to prove the identities for \( s = t = 0 \) only. Consider the case \( i = 1, j = 2 \) for the second identity. Writing

\[
\alpha = \frac{1}{a_2c_2} - \frac{1}{a_1c_1},
\]

we obtain

\[
N_{(2,-1)}(0)N_{(1,2)}(0) =
\]

\[
(r^{-1}T_1T_2^{-1} + \frac{\alpha}{m} \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right) (c_2, m, a_2 ))(rT_2T_1^{-1} - \frac{\alpha}{m} \left( \begin{array}{c} c_2 \\ -b_2 \\ a_2 \end{array} \right) (c_1, m, a_1 ) =
\]

\[
T^{-1}T_1^{-1} + \frac{r\alpha}{m} \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right) (c_2, m, a_2 ) T_2T_1^{-1} - \frac{\alpha}{rm} T^{-1}T_2^{-1} \left( \begin{array}{c} c_2 \\ -b_2 \\ a_2 \end{array} \right) (c_1, m, a_1 )
\]

\[
-\frac{\alpha^2}{m^2} \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right) (c_2, m, a_2 ) \left( \begin{array}{c} c_2 \\ -b_2 \\ a_2 \end{array} \right) (c_1, m, a_1 ).
\]

Since

\[
( c_2, m, a_2 ) T_2T_1^{-1} = ma_2c_2(1, 0, 0)T_1^{-1} = \frac{ma_2c_2}{ma_1c_1} (c_1, m, a_1 ) = \frac{1}{r} (c_1, m, a_1 ),
\]

\[
T^{-1}T_2^{-1} \left( \begin{array}{c} c_2 \\ -b_2 \\ a_2 \end{array} \right) = \frac{1}{ma_2c_2} T^{-1} \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right) = \frac{ma_1c_1}{ma_2c_2} \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right) = r \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right),
\]

\[
( c_2, m, a_2 ) \left( \begin{array}{c} c_2 \\ -b_2 \\ a_2 \end{array} \right) = 0,
\]

we conclude

\[
N_{(2,-1)}(0)N_{(1,2)}(0) = T^{-1}T_1^{-1} + \frac{\alpha}{m} (r^{-1} \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right) (c_1, m, a_1 ) - \frac{1}{r} \left( \begin{array}{c} a_1 \\ -b_1 \\ c_1 \end{array} \right) (c_1, m, a_1 )) =
\]

17
\[ N_{(1,-1)}(0), \]

as claimed. The remaining identities can be shown in a similar fashion. It is worth noting, however, that in the proof of the identities involving the matrices \( N_{(i,i)}(0) \) the two terms in the middle vanish. □

**Lemma 3.8** For \( i, j \in \{\pm 1, \pm 2\} \) we have

a) \( N_{(-i,-j)}(s) = JN_{(i,j)}(-s)J \)
b) \( N_{(j,i)}(s) = N_{(i,j)}(-s)^{-1} \)

**Proof** The validity of a) is seen by observing that

\[ JN_{(i,j)}(0)J = N_{(-i,-j)}(0), \]

\( JR_iJ = -R_{-i} \) and \( N_{(i,j)}(s) = N_{(i,j)}(0)e^{-\frac{2\pi}{3}(s)}. \) Letting \( s = t = 0 \) in the first identity of Lemma 3.7 shows that

\[ N_{(j,i)}(0) = N_{(i,j)}(0)^{-1}, \]

which in turn implies b). □

**Lemma 3.9** If \( N_{(2,-1)}(s^+), N_{(1,2)}(s^-) \in \text{SL}(3,\mathbb{Z}), \) for some \( s^+, s^- \in \mathbb{Q}, \) and

\[ s_1 = s^+ + s^-, \quad s_2 = s^+ - s^-, \]

then \( N_{(1,-2)}(s^+) \in \text{SL}(3,\mathbb{Z}), \) \( N_{(2,1)}(-s^-) \in \text{SL}(3,\mathbb{Z}), \) and therefore

\[ N_{(1,-1)}(s_1) = N_{(2,-1)}(s^+)N_{(1,2)}(s^-) \in \text{SL}(3,\mathbb{Z}), \]

\( N_{(2,-2)}(s_2) = N_{(1,-2)}(s^+)N_{(2,1)}(-s^-) \in \text{SL}(3,\mathbb{Z}). \)

**Proof** An application of part a) of Lemma 3.8 to \( N_{(2,-1)}(s^+) \) followed by an application of part b) shows that \( N_{(1,-2)}(s^+) \in \text{SL}(3,\mathbb{Z}). \) Application of part a) of Lemma 3.8 to \( N_{(1,2)}(s^-) \) shows that \( N_{(2,1)}(-s^-) \in \text{SL}(3,\mathbb{Z}). \) Finally, since \( \text{SL}(3,\mathbb{Z}) \) is a group, an application of Lemma 3.7 establishes the second part of the claim. □

**3.10 Lemma** If \( N_{(i,j)}(s) \in M_3(\mathbb{Z}) \) for some \( i, j \in \{\pm 1, \pm 2\}, \) then

\[ s = \frac{n}{9m} \text{ if } ij = -1 \text{ or } ij = -4; \]

\[ s = \frac{n}{9g} \text{ if } ij = 2, \]

\[ s = \frac{n}{9f} \text{ if } ij = -2, \]

where \( n \) is relatively prime to \( m, g, f, \) respectively.

**Proof** Consider, for instance, the case \( i = 1, j = 2. \) The assumption \( N_{(1,2)}(s) = N(s) \in M_3(\mathbb{Z}) \) implies

\[ S_2N(s) = \frac{1}{m}(\Omega_0 + m\Omega_1) + s\Phi^t\epsilon M_3(\mathbb{Z}), \]

hence

\[ \frac{1}{m}\Omega_0 + s\Phi^t\epsilon M_3(\mathbb{Z}). \]
Since each entry of $\Omega_0$ is divisible by 9 in case $m$ is odd, and by 18 in case $m$ is even, it follows from Corollary 3.5 and Lemma 3.3 a)

$$\frac{1}{g} \Omega_0 + s \Phi^t \epsilon M_3(\mathbb{Z})$$

and this implies

$$s \Phi^t \frac{1}{g} M_3(\mathbb{Z}).$$

Since the greatest common divisor of all the entries of the matrix $\Phi^t$ is 9, we infer that $s \frac{1}{g} \epsilon 9$, as claimed. Since Corollary 3.5 shows that the entries of $\Omega_0$ and $g$ are relatively prime, the claim follows in this particular case. The other cases can be proved in the same way. □

In light of Lemma 3.10 we introduce the following notation within the context of Lemma 3.9:

$$s_i = \frac{n_i}{9m} \text{ for } i = 1, 2; s^+ = \frac{n^+}{9f}, s^- = \frac{n^-}{9g}$$

Then Lemma 3.9 implies $n_i = n^+ g + n^- f$, $n_2 = n^+ g - n^- f$.

**Remark** It is not difficult to show that $n_i \equiv -\frac{2a_i c_i}{\epsilon (9m)}$ modulo $3f$, $n^- \equiv -\frac{2a_i f_i}{\epsilon (9m)}$ modulo $3g$. But these specific representations will not be used in the sequel.

The proof of the Theorem can now be accomplished as follows. For convenience we shall assume that $m$ is odd. The case when $m$ is even necessitates some minor factor 2 adjustments. By Proposition 1.2 and Proposition 3.1 there exist $s^+, s^- \epsilon Q$ such that $N_{2,-1}(s^+), N_{1,2}(s^-) \epsilon SL(3,\mathbb{Z})$. Then, with the notation introduced above, we obtain

$$m^2 N_{1,2}(s^-) = m^2 N_{1,2}(s^+ - s_2) =$$

$$\Gamma_0 + m^2 \Gamma_2 + \frac{1}{3}(\Omega_0 + m\Omega_1)(n^+ g - n_2) + \frac{1}{9}(n^+ g - n_2)^2 - \frac{1}{3}(n^+ g - n_2)m)\Phi^t =$$

$$\Gamma_0 + m^2 \Gamma_2 - (\Omega_0 + m\Omega_1)\frac{n_2}{3} + \frac{1}{2}((\frac{n_2}{3})^2 + \frac{n_2}{3})\Phi^t +$$

$$\frac{1}{2}((\frac{n_2}{3})^2 - n^+ f)g^2 \Phi^t + \frac{1}{3}(\Omega_0 + m\Omega_1 - \frac{n_2}{3}\Phi^t)n^+ g =$$

$$\mathcal{A} + \mathcal{B} + \mathcal{C} + \mathcal{D},$$

where

$$\mathcal{A} = m^2 N_{1,2}(s_2) = \Gamma_0 + m^2 \Gamma_2 + (\Omega_0 + m\Omega_1)\frac{n_2}{3} + \frac{1}{2}((\frac{n_2}{3})^2 - \frac{n_2}{3})m)\Phi^t,$$

$$\mathcal{B} = \frac{1}{2}((\frac{n_2}{3})^2 - n^+ f)g^2 \Phi^t,$$

$$\mathcal{C} = \frac{1}{3}(\Omega_0 + m\Omega_1 - \frac{n_2}{3}\Phi^t)n^+ g - 2fg\Omega_1 n_2 + n_2 fg \Phi^t,$$

$$\mathcal{D} =$$
\[ \mathcal{D} = -\Omega_0 \frac{2n_2}{3} \]

Since, by Corollary 3.5, \( a_2 = \frac{2}{a_1} c_1 \) modulo \( g^2 \), and since obviously \( c_2 = \frac{2}{a_1} a_1 \), each entry in the matrix \( \mathfrak{A} \) is equal to the corresponding entry in \( m^2 N_{(2,-2)}(s_2) \) modulo \( g^2 \). Since \( N_{(2,-2)}(s_2) \) is an integral matrix by Lemma 3.9, it follows that \( \mathfrak{A} \) is the null matrix modulo \( g^2 \). Since \( \mathfrak{B} \) is also the null matrix modulo \( g^2 \), and since \( \mathfrak{C} \) is the null matrix modulo \( g \), we have

\[ m^2 N_{(1,2)}(s^-) = \mathcal{D} \mod g. \]

Since \( n_2 \) and \( g \) are relatively prime, Corollary 3.5 shows that the right hand side is not the null matrix modulo \( g \). This implies that \( N_{(1,2)}(s^-) \) is not in \( M_3(\mathbb{Z}) \), contradicting the choice of \( s^- \).

**Remark** The crux of the argument is of course the fact that the second term in the expression \( s^+ - s_2 \) at the beginning of this last sequence of manipulations has the “wrong sign”. Since changing that sign leads to the opposite conclusion, one can construct an alternative proof of the Theorem, which does not rely on Proposition 1.2. First, choosing \( s_1 = \frac{n_1}{m} \) such that \( N_{(-1,1)}(s_1) \in \text{Sl}(3,\mathbb{Z}) \), one shows that there exist integers \( n^+ \) and \( n^- \) satisfying the identity \( n_1 = n^+ g + n^- f \). Then, letting \( s^+ = \frac{n^+}{m}, \ s^- = \frac{n^-}{m} \), and following a similar line of reasoning as above, but working with \( s_1 - s^+ \) and \( s_1 - s^- \), respectively, rather than with \( s^+ - s_2 \), one shows that both, \( m^2 N_{(1,2)}(s^-) \) and \( m^2 N_{(2,-1)}(s^+) \) are equal to the null matrix modulo \( g^2 \). One can then show by related manipulations that \( m^2 N_{(1,2)}(s^-) \) and \( m^2 N_{(2,-1)}(s^+) \) are equal to the null matrix modulo \( f^2 \) as well. The indicated proofs exploit the full strength of Corollary 3.5. These two facts taken together show that \( N_{(1,2)}(s^-) \in M_3(\mathbb{Z}) \). Invoking finally once again the last part in the above proof, leads to the same contradiction.

**References**

[B] E. Bombieri, “Continued fractions and the Markoff tree”, Expositiones Mathematicae 25 (3) (2007), 187-213

[Ca] J.W.S. Cassels, “An introduction to Diophantine Approximation”, Cambridge Univ. Press, 1957 (Chapter II)

[CV] S. Cecotti, C. Vafa, “On the classification of N=2 Supersymmetric Theories”, Commun. Math. Phys. 158 (1993), 569-644

[Co] H. Cohn, “Markoff Forms and Primitive Words”, Math. Ann. 196 (1972), 8-22

[CF] T.W. Cusick, M.E. Flahive, “The Markoff and Lagrange spectra”, Mathematical Surveys and Monographs, 30, American Mathematical Society (1989)

[F] F.G. Frobenius “Über die Markoffschen Zahlen”, Sitzungsberichte der Koeniglichen Preussischen Akademie der Wissenschaften zu Berlin (1913), 458-487 (p. 461) [Gesammelte Abhandlungen, Band III, Springer Verlag, (p.601)]

20
[HZ] F. Hirzebruch, D. Zagier, “The Atiyah-Singer Theorem and Elementary Number Theory”, Publish or Perish (1974)

[Pe] S. Perrine, “L’interpretation matricielle de la theory de Markoff classique”, Int. J. Math. Math. Sci. 32 (2002).no.4, 193-262

[Po] J.Popp, “The combinatorics of frieze patterns and Markoff numbers”, arXiv:math/0511633

[Re] C. Reutenauer, “On Markoff’s property and Sturmian words”, Math. Ann. 336 (1) (2006), 1-12

[Ru] A. N. Rudakov, “The Markov numbers and exceptional bundles on $P^2$ “, Math. USSR. Izv., 32(1) (1989), 99-102

[S] C. Series, “The geometry of Markoff numbers”, Math. Intelligencer 7 (1985), no.3, 20-29

[W] M. Waldschmidt, “Open Diophantine Problems”, Moscow Mathematical Journal 4 (2004), no.1, 245-305

[Za] D. Zagier, “On the Number of Markoff Numbers Below a Given Bound”, Mathematics of Computation, 39 (1982), no.160, 709-723

[Zh] Y. Zhang, “An elementary proof of Markoff conjecture for prime powers” arXiv:math.NT/0606283

Department of Mathematics
Tulane University
New Orleans, LA 70118

e-mail: nriedel@tulane.edu