MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 134
APRIL 1976, PAGES 361–365

# The Uniqueness of the Markoff Numbers

By Gerhard Rosenberger

*Dedicated to the 60th birthday of Professor Hel Braun*

**Abstract.** A Markoff triple is a set of three positive integers satisfying the diophantine equation $x^2 + y^2 + z^2 = 3xyz$. The maximum of the three numbers is called a Markoff number. We show: If there are Markoff triples $(x_1, y_1, z)$ and $(x_2, y_2, z)$ with the same Markoff number $z$, then $x_1 = x_2$ or $x_1 = y_2$.

A. A Markoff triple is a set of three positive integers satisfying the diophantine equation $x^2 + y^2 + z^2 = 3xyz$. The maximum of the three numbers is called a Markoff number. Here we will prove: If there are Markoff triples $(x_1, y_1, z)$ and $(x_2, y_2, z)$ with the Markoff number $z$, then $x_1 = x_2$ or $x_1 = y_2$. Some numerical evidence concerning the uniqueness of the Markoff numbers is given in [1] and [4].

*Definitions.*

$\{A, B\}$ is the group generated by $A$ and $B$.

$[A, B] = ABA^{-1}B^{-1}$ is the commutator of $A, B \in K$ ($K$ a group).

$\operatorname{tr} U$ is the trace of $U \in SL(2, \mathbf{C})$.

B. Lemma 1 (Nielsen [3]). *Let $K = \{A, B\}$ be a free group of rank two. Two elements $U, V$ of $K$ generate $K$ if and only if $[U, V]$ is conjugate over $K$ to $[A, B]^\epsilon$, $\epsilon = \pm 1$.*

We need the following facts about elements of $SL(2, \mathbf{C})$: For all $A, B \in SL(2, \mathbf{C})$ and $n \geqslant 1$

(a) $\operatorname{tr} AB = \operatorname{tr} A \cdot \operatorname{tr} B - \operatorname{tr} AB^{-1}$.

(b) $\operatorname{tr}[A, B] = (\operatorname{tr} A)^2 + (\operatorname{tr} B)^2 + (\operatorname{tr} AB)^2 - \operatorname{tr} A \cdot \operatorname{tr} B \cdot \operatorname{tr} AB - 2$.

(c) $A^n = S_nA - S_{n-1}I$, where $S_{-1} = -1, S_0 = 0, S_1 = 1, S_{n+1} = (\operatorname{tr} A) \cdot S_n - S_{n-1}$.

Now we fix the following notation:

$$T. = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad R. = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

$$A. = RTR^2T = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \quad B. = TR^2TR = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

It is known that

$$(*) \qquad A^{-1} = TRBR^{-1}T^{-1} = R^{-1}(AB)R$$

Received November 20, 1973.

*AMS (MOS) subject classifications* (1970). Primary 10B10, 10D05, 20H10.

and $\operatorname{tr}[A, B] = -2$. Because of $\operatorname{tr} A = 3$, we have $\operatorname{tr} A^n = \operatorname{tr} B^n = \operatorname{tr}(AB)^n > \operatorname{tr} A^m$ for $n > m > 0$.

The modular group $G$ is generated by $T$ and $R$, and it is

$$G = \{T, R | T^2 = R^3 = 1\} \qquad (G = PSL(2, \mathbf{Z})).$$

The commutator group $G' = [G, G]$ of $G$ is generated by $A$ and $B$; and $G'$ is a free group of rank two. By Lemma 1 we have $(\operatorname{tr} U)^2 + (\operatorname{tr} V)^2 + (\operatorname{tr} UV)^2 = \operatorname{tr} U \cdot \operatorname{tr} V \cdot \operatorname{tr} UV$ for any pair $(U, V)$ of generators of $G'$ (see (b)).

LEMMA 2. *For $n, m, r, s \in \mathbf{N}$ the following facts are true*:

(1) $\operatorname{tr} AB^n > \operatorname{tr} AB^m$ *for* $n > m$.

(2) $\operatorname{tr} AB^n > \operatorname{tr} AB^rAB^s$ *for* $n \geqslant 4$, $n \geqslant r + s$.

(3) $\operatorname{tr} AB^n < \operatorname{tr} AB^rAB^s$ *for* $r + s > n$.

(4) $\operatorname{tr} AB^nAB^m > \operatorname{tr} AB^rAB^s$ *for* $n + m > r + s$.

*Proof.* (1) $\operatorname{tr} AB^n = \operatorname{tr} A(S_nB - S_{n-1}I) = \operatorname{tr}(S_nAB - S_{n-1}A) = 3(S_n - S_{n-1}) > 3(S_m - S_{m-1}) = \operatorname{tr} AB^m$ for $n > m$.

(2) It is sufficient to prove this for $n = r + s$ and $s = 1$, i.e. $n = r + 1$, or $s = 2$. Let $s = 1$. Then, $\operatorname{tr} AB^rAB = \operatorname{tr}((S_rAB - S_{r-1}A)AB) = \operatorname{tr}(S_r(AB)^2 - S_{r-1}A^2B) = 7S_r - 6S_{r-1} < 3S_n - 3S_{n-1} = \operatorname{tr} AB^n$; because of $n \geqslant 4$. The proof for $s = 2$ is analogous.

(3) This is trivial for $r > n$ or $s > n$. Let us consider now $r \leqslant n$ and $s \leqslant n$. It is sufficient to prove this for $r + s = n + 1$ and $s = 1$, i.e. $n = r$. $\operatorname{tr} AB^nAB = 7S_n - 6S_{n-1} > 3(S_n - S_{n-1}) = \operatorname{tr} AB^n$.

(4) This is trivial for $n > r + s$ or $m > r + s$. Let us consider now $n \leqslant r + s$ and $m \leqslant r + s$. It is sufficient to prove this for $m + n = r + s + 1$. Then $m > r$, $m > s$, $n > r$ or $n > s$; say $m > s$. Now we may assume $s = 1$, i.e. $m + n = r + 2$.

(a) $n \geqslant r$. Then it is sufficient to prove this for $r = 1$; i.e. $m + n = 3$. Then $m = 2$ because of $m > s$. $\operatorname{tr} ABAB^2 = 15 > 7 = \operatorname{tr} ABAB$.

(b) $r \geqslant n$. Then it is sufficient to prove this for $n = 1$, i.e. $m = r + 1$; and therefore, we may assume $r = 1$, too, i.e. $m = 2$. $\operatorname{tr} ABAB^2 > \operatorname{tr} ABAB$. Q.E.D.

*Remark.* Some of our main arguments in this proof were, for instance, the following:

Let $n, m, r, s \in \mathbf{N}$.

(1) If $\operatorname{tr} AB^nAB^m < \operatorname{tr} AB^rAB^s$ for $n + m < r + s$, then $\operatorname{tr} AB^nAB^{m+1} < \operatorname{tr} AB^rAB^{s+1}$.

(2) If $\operatorname{tr} AB^n < \operatorname{tr} AB^rAB^s$, then $\operatorname{tr} AB^{n+1} < \operatorname{tr} AB^rAB^{s+1}$.

(3) If $\operatorname{tr} AB^n > \operatorname{tr} AB^rAB^s$, $n \geqslant 4$, then $\operatorname{tr} AB^{n+1} > \operatorname{tr} AB^rAB^{s+1}$.

With these and similar arguments, in connection with some suitable conjugations, we can construct the following lemma:

LEMMA 3. *Let* $C_1 = AB^{\epsilon_1} \cdots AB^{\epsilon_n}$, $2 \leqslant \epsilon_i$, *and* $C_2 = AB^{\alpha_1} \cdots AB^{\alpha_m}$, $2 \leqslant \alpha_j$. *Let* $k_1 = n + \Sigma_{i=1}^n \epsilon_i = n + s_1$, $k_2 = m + \Sigma_{j=1}^m \alpha_j = m + s_2$. *Let* $s_1 \geqslant s_2$ *for* $n < m$, *respectively*, $s_1 > s_2$ *for* $m \leqslant n$. *Then* $\operatorname{tr} C_1 > \operatorname{tr} C_2$.

*Proof.* We prove this lemma inductively over the possible quadruples $(s_1, s_2, n, m)$, where the quadruples $(s_1, s_2, n, m)$ are ordered by:

$$(s_1', s_2', n', m') < (s_1, s_2, n, m) \Leftrightarrow s_1' \leqslant s_1, \quad s_2' \leqslant s_2, \quad n' \leqslant n, \quad m' \leqslant m$$

and

$$s_1' + s_2' + n' + m' < s_1 + s_2 + n + m.$$

For suitable small quadruples $(s_1, s_2, n, m)$ the statement is true by Lemma 2.

Let $(s_1, s_2, n, m)$ be a possible quadruple. We assume the statement is true for all possible quadruples $(s_1', s_2', n', m')$ with $(s_1', s_2', n', m') < (s_1, s_2, n, m)$.

*Case* 1. $\epsilon_i = 2$ *for* $i = 1, \ldots, n$. Then $C_1 = (AB^2)^n$, $n \geqslant 2$ and $n > m$, i.e. $s_1 > s_2$ and $k_1 > k_2$. If $m \geqslant 2$, then it follows by assumption that $\operatorname{tr} AB^{s_2} > \operatorname{tr} C_2$. Therefore, the statement is true, if we can show $\operatorname{tr} C_1 > \operatorname{tr} AB^{s_2}$.

Obviously, the statement is true for $s_1 > s_2$, if we can show it for $2n = s_1 = s_2 + 1$. And we get

$$\begin{aligned}\operatorname{tr}(AB^2)^n &= \operatorname{tr}(AB^2) \cdot S_n(\operatorname{tr} AB^2) - 2S_{n-1}(\operatorname{tr} AB^2)\\ &= 6S_n(6) - 2S_{n-1}(6) > 3(S_{2n-1}(3) - S_{2n-2}(3))\\ &= 3(S_{2n-1}(\operatorname{tr} B) - S_{2n-2}(\operatorname{tr} B)) = \operatorname{tr} AB^{2n-1} \quad \text{by induction.}\end{aligned}$$

*Case* 2. $\alpha_j = 2$ *for* $j = 1, \ldots, m$. Then $C_2 = (AB^2)^m$.

Obviously, the statement is true for $m \leqslant n$.

Let us consider now $n < m$. Then $\epsilon_i \geqslant 3$ for some $i$. Obviously, the statement is true for $s_1 \geqslant s_2$, if we can show it for $s_1 = s_2 = 2m$.

Let us consider now $s_1 = s_2$. For $n = m - 1$ the statement is true by direct calculations. Let us consider now $n < m - 1$. It is $\operatorname{tr}(AB^2)^{m-2}AB^4 > \operatorname{tr}(AB^2)^m$; and therefore, it follows by assumption that

$$\operatorname{tr} C_1 > \operatorname{tr}(AB^2)^{m-2}AB^4 > \operatorname{tr} C_2.$$

*Case* 3. $\epsilon_i \geqslant 3$ *for some* $i$ *and* $\alpha_j \geqslant 3$ *for some* $j$. We may assume, perhaps after suitable conjugations, $\epsilon_n \geqslant 3$ and $\alpha_m \geqslant 3$. Let

$$C_1' = AB^{\epsilon_1} \cdots AB^{\epsilon_n - 1}, \qquad C_2' = AB^{\alpha_1} \cdots AB^{\alpha_m - 1}.$$

Then $\operatorname{tr} C_1' > \operatorname{tr} C_2'$ implies by a simple calculation

$$\operatorname{tr} C_1 = \operatorname{tr} C_1'B > \operatorname{tr} C_2'B = \operatorname{tr} C_2. \quad \text{Q.E.D.}$$

C. THEOREM. *Let* $(x_1, y_1, z)$ *and* $(x_2, y_2, z)$ *be Markoff triples with the same Markoff number* $z$. *Then* $x_1 = x_2$ *or* $x_1 = y_2$ (*and therefore,* $y_1 = y_2$ *or* $y_1 = x_2$).

*Proof.* If a triple $(x, y, z)$ of three positive integers is a solution of the diophantine equation $x^2 + y^2 + z^2 = xyz$, then $x, y, z \equiv 0 \pmod 3$, i.e.: With the integral solutions of $x^2 + y^2 + z^2 = xyz$ we have also the integral solutions of $x'^2 + y'^2 + z'^2 = 3x'y'z'$ and conversely. Therefore, the theorem is proved if we can show: If $(x_1, y_1, z)$ with $x_1, y_1 \leqslant z$ and $(x_2, y_2, z)$ with $x_2, y_2 \leqslant z$ are triples of positive integers satisfying the diophantine equation $x^2 + y^2 + z^2 = xyz$, then $x_1 = x_2$ or $x_1 = y_2$.

Let $(x_1, y_1, z)$ with $x_1, y_1 \leqslant z$ and $(x_2, y_2, z)$ with $x_2, y_2 \leqslant z$ be triples of positive integers satisfying the diophantine equation $x^2 + y^2 + z^2 = xyz$. The theorem is certainly true for $x_1 = z$, $x_2 = z$, $y_1 = z$ or $y_2 = z$.

Let us consider now $x_1, y_1, x_2, y_2 < z$. Especially, $z > 3$. By [2] and [5] there are generators $(A_1, B_1)$ and $(A_2, B_2)$ of the commutator group $G'$ of the modular group $G$ with

(1) $\operatorname{tr} A_1 = z$, $\operatorname{tr} B_1 = x_1$, $\operatorname{tr} A_1B_1 = y_1$, and

(2) $\operatorname{tr} A_2 = z$, $\operatorname{tr} B_2 = x_2$, $\operatorname{tr} A_2B_2 = y_2$.

Moreover, $\operatorname{tr}[A_1, B_1] = \operatorname{tr}[A_2, B_2] = -2$. By [2, Theorem 2.1], we may assume that $A_i$ is conjugate over $G'$ to an element $M_{r_i,s_i} = \Pi_{j=1}^{ri} AB^{a_{ij}+2}$ or its inverse, where $(r_i, s_i)$ an integer pair with $r_i > 0$, $s_i \geqslant 0$, $(r_i, s_i) = 1$ and $a_{ij} = [js_i/r_i] - [(j-1)s_i/r_i]$ $(i = 1, 2)$. By Lemma 3 we have $r_1 = r_2$, $s_1 = s_2$ and $a_{1j} = a_{2j}$ (here $\operatorname{tr} A_1 = \operatorname{tr} A_2$); that means we may assume that $A_1$ is conjugate over $G'$ to $A_2$ or its inverse. Now with regard to Lemma 1 and (*) we may assume, perhaps after a suitable conjugation,

(a) $A_2 = A_1^{\alpha}$, $\alpha = \pm 1$, and

(b) $[A_1, B_1] = [A_1^{\gamma}, B_2^{\delta}]$ or $[A_1, B_1] = [B_2^{\delta}, A_1^{\gamma}]$; $\gamma, \delta = \pm 1$.

*Case* 1. Let $[A_1, B_1] = [B_2^{\delta}, A_1^{\gamma}]$. Then we have necessarily $\gamma = -1$, because otherwise

$$B_2^{\delta} A_1 B_2^{-\delta} = A_1 B_1 A_1^{-1} B_1^{-1} A_1 \quad \text{and} \quad z = \operatorname{tr} A_1 = z \cdot \operatorname{tr}[A_1, B_1] - z = -3z.$$

We get $A_1 = B_1^{-1} A_1^{-1} B_2^{\delta} A_1 B_2^{-\delta} A_1 B_1$; i.e. $B_1^{-1} A_1^{-1} B_2^{\delta}$ and $A_1$ commute. Therefore, $B_1^{-1} A_1^{-1} B_2^{\delta}$ and $A_1$ have the same fixed points. Since the commutator subgroup $G'$ of the modular group is free, we have $B_2^{\delta} = A_1 B_1 A_1^{\beta}$. Assume $\beta \geqslant 1$. Then

$$x_2 = \operatorname{tr} B_1 A_1^{\beta+1} = y_1 S_{\beta+1} - x_1 S_\beta = (y_1 z - x_1) S_\beta - y_1 S_{\beta-1} > z,$$

and that is not true. Therefore, $\beta \leqslant 0$. Assume $\beta \leqslant -2$. Then $x_2 = \operatorname{tr} B_1 A_1^{\beta+1} = x_1 \cdot \operatorname{tr} A_1^{-\beta-1} - \operatorname{tr} B_1 A_1^{-\beta-1} = (x_1 z - y_1) S_{-\beta-1} > z$, and that is not true. Therefore, $\beta = 0$ or $\beta = -1$. We have $x_2 = y_2$ for $\beta = 0$ and $x_2 = x_1$ for $\beta = -1$.

*Case* 2. Let $[A_1, B_1] = [A_1^{\gamma}, B_2^{\delta}]$. Then we have necessarily $\gamma = 1$, because otherwise again $z = -3z$. We get $A_1 = B_1^{-1} B_2^{\delta} A_1 B_2^{-\delta} B_1$, i.e., $B_1^{-1} B_2^{\delta}$ and $A_1$ commute. Therefore $B_1^{-1} B_2^{\delta}$ and $A_1$ have the same fixed points. Since $G'$ is free, we have $B_2^{\delta} = B_1 A_1^{\beta}$. Assume $\beta \geqslant 2$. Then

$$x_2 = \operatorname{tr} B_1 A_1^{\beta} = y_1 S_\beta - x_1 S_{\beta-1} = (y_1 z - x_1) S_{\beta-1} - y_1 S_{\beta-2} > z,$$

and that is not true. Therefore, $\beta \leqslant 1$. Assume $\beta \leqslant -1$. Then $x_2 = \operatorname{tr} B_1 A_1^{\beta} = x_1 \operatorname{tr} A_1^{-\beta} - \operatorname{tr} B_1 A_1^{-\beta} = (x_1 z - y_1) S_{-\beta} > z$, and that is not true. Therefore, $\beta = 0$ or $\beta = 1$. We have $x_2 = x_1$ for $\beta = 0$ and $x_2 = y_1$ for $\beta = 1$. This completes the proof. Q.E.D.

Mathematisches Seminar der Universität
2 Hamburg 13
Bundesstr. 55
Federal Republic of Germany

1. I. BOROSH, "Numerical evidence on the uniqueness of Markoff numbers," *Notices Amer. Math. Soc.*, v. 21, 1974, p. A-55. Abstract #711-10-32.

2. H. COHN, "Markoff forms and primitive words," *Math. Ann.*, v. 196, 1972, pp. 8–22. MR **45** #6899.

3. J. NIELSEN, "Die Isomorphismen der allgemeinen unendlichen Gruppe mit zwei Erzeugenden," *Math. Ann.*, v. 78, 1918, pp. 385–397.

4. D. ROSEN & G. S. PATTERSON, JR., "Some numerical evidence concerning the uniqueness of the Markov numbers," *Math. Comp.*, v. 25, 1971, pp. 919–921. MR **46** #132.

5. G. ROSENBERGER, "Fuchssche Gruppen, die freies Produkt zweier zyklischer Gruppen sind, und die Gleichung $x^2 + y^2 + x^2 = xyz$," *Math. Ann.*, v. 199, 1972, pp. 213–227. MR **49** #5202.