The Uniqueness of Some Markoff Numbers

By
Shih-Hsun Chung

Advisor
Yu-ching Hung

Department of Mathematics,
National Taiwan Normal University
Taipei, Taiwan.
June, 2008

Abstract

In this thesis, we use some simple facts about congruence to show that if (a, b, c) and (a', b', c) are non-singular Markoff triples with $a, a' \geq \frac{k+1}{3}$, where k is a positive odd integer, then the Markoff conjecture holds if $3c-2$ or $3c+2$ is k times an odd prime power.

中文摘要

於此篇論文中, 我們將用一些數論上同餘的理論去證明: 設 (a, b, c) 與 (a', b', c) 皆爲馬可夫方程式的正整數解, 且 $a, a' \geq \frac{k+1}{3}$, 其中 k 是一個正奇數. 若 c 滿足 $3c-2$ 或 $3c+2 = kp^n$, 則馬可夫猜想是成立的.

Contents

1 Introduction

The Diophantine equation

$$x^2 + y^2 + z^2 = 3xyz \tag{1}$$

was first examined in detail by A.A.Markoff [1] [2] in 1879 and 1880 when he was studying the theory of quadratic forms. Now (1) is hte well-known Markoff equation.

All the triples (a, b, c) of positive integers satisfying (1) are called Markoff triples. For convenience, we shall not distinguish a Markoff triple from those obtained by permuting its entries, that is, without considering the permutation of the entries of the Markoff triples. Usually, we rearrange the entries of the solution triple in ascending order. Therefore, if we say that (a, b, c) is a Markoff triple, it usually means that (a, b, c) is a solution of (1) and $a \leq b \leq c$. In ascending order of their largest elements, the first 14 Markoff triples are: $(1, 1, 1)$, $(1, 1, 2)$, $(1, 2, 5)$, $(1, 5, 13)$, $(2, 5, 29)$, $(1, 13, 34)$, $(1, 34, 89)$, $(2, 29, 169)$, $(5, 13, 194)$, $(1, 89, 233)$, $(5, 29, 433)$, $(1, 233, 610)$, $(2, 169, 985)$, $(13, 34, 1325)$.

All the entries of the Markoff triple are particularly important in the works of Markoff and hence G.Frobenius [3] called them the Markoff numbers. The first few Markoff numbers are: 1, 2, 5, 13, 29, 34, 89, 169, 194, 233, 433, 610, 985, 1325. See more in [8].

An old well-known problem for this Diophantine equation is the Markoff conjecture, which was first mentioned by G.Frobenius [3] in 1913.

Markoff Conjecture: If (a, b, c) and (a', b', c) are Markoff triples with $a \leq b \leq c$ and $a' \leq b' \leq c$, then we have $a = a'$ and $b = b'$.

In other words, it asserts that a Markoff triple up to permutation is determined uniquely by its largest entry. Sometimes we simply say that a Markoff number c is unique if the above conjecture holds for c.

A book by Cassels [7] published in 1957 provided a comprehensive introduction and brought the conjecture to the attention of many mathematicians. However, this conjecture is still open. It has been proved only for the Markoff triples of some rather special forms. For example, J. Button [6] proved the conjecture for the prime number c by using algebraic number theory and P.Schmutz [10] used the hyperbolic geometry to establish the conjecture for the prime power c (but the proof works also for 2 times a prime power). Another simple, short proof using hyperbolic geometry is recently posted by M. L. Lang and S. P. Tan [9] for a prime power (but the proof still works for 2 times a power and 5 times a power). A stronger result for the unicity conjecture is provided by J. Button [5] for the Markoff number c which are products of a prime power and a "small" factor k, where k is any number such that $k^4 \leq c$.

Baragar [3] has also proven the conjecture for the Markoff number c if either $3c-2$ or $3c+2$ is a prime number, or 2 times a prime or 4 times a prime. Recently, Y. Zhang [11] established the uniqueness for those Markoff number c where one of $3c-2$ or $3c+2$ is a prime power, or 4 times a prime power, or 8 times a prime power.

In this thesis, we use some simple facts about congruence to show that if (a, b, c) and (a', b', c) are non-singular Markoff triples with $a, a' \geq \frac{k+1}{3}$, where k is a positive odd integer, then the Markoff conjecture holds if $3c-2$ or $3c+2$ is k times an odd prime power. We expect that this result can be helpful to find many more Markoff numbers for which the Markoff conjecture is true.

2 Preliminary

We shall call the two Markoff triples $(1, 1, 1)$ and $(1, 1, 2)$ **singular**, while all the others **non-singular**.

Proposition 1 ([12]): The entries of a non-singular Markoff triple are all distinct.

Proof: Let (a, b, c) be a non-singular Markoff triple. First, we suppose $b = c$. Then (1) can be written as $a^2 + b^2 + b^2 = 3ab^2$, i.e. $a^2 = b^2(3a - 2)$. This implies that $b \mid a$. However, a and b are positive integers with $a \leq b$, so we have $a = b$. Hence we obtain $3a - 2 = 1$, which implies $a = b = c = 1$, and this leads to a contradiction. Secondly, we suppose $a = b$. Then (1) can be written as $b^2 + b^2 + c^2 = 3b^2c$, i.e. $c^2 = b^2(3c-2)$. This implies that $b \mid c$. So we can let $c = nb$ for some positive integer n. Then we have $n^2b^2 = b^2(3nb - 2)$, i.e. $2 = n(3b - n)$, which leads to $n \mid 2$ and hence $n = 1$ or 2. So $3c - 2 = (\frac{c}{b})^2 = n^2 = 1$ or 4; that is, $c = 1$ or 2. Therefore we conclude that $(a, b, c) = (1, 1, 1)$ or $(1, 1, 2)$, a contradiction again. Consequently, the entries of a non-singular Markoff triples are all distinct and this completes the proof.

The following two lemmas from elementary number theory will be used in the proof of Theorem 4.

Lemma 2 ([13]): The Diophantine equation $x^2 + y^2 + z^2 = kxyz$ has no positive integer solution if the integer $k > 3$.

Lemma 3: If m and n are coprime integers, then every odd factor of $m^2 + n^2$ is congruent 1 modulo 4.

Proof: Let $t \neq 1$ ($t = 1$ certainly holds) be an odd factor of $m^2 + n^2$ and let p be any prime factor of t. Then we have $m^2 + n^2 \equiv 0 \pmod{p}$. Notice that m and n are coprime, so $p \nmid m$ and $p \nmid n$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, we can multiply the congruence equation by $(m^{-1})^2$ to get $(nm^{-1})^2 \equiv -1 \pmod{p}$, which implies that -1 is a quadratic residue modulo a prime p. By elementary number theory we know that $p \equiv 1 \pmod{4}$. Therefore, t is also congruent 1 modulo 4 since every prime factor of t is congruent 1 modulo 4. This completes the proof.

The following theorem gives some useful properties about Markoff triples and Markoff numbers.

Theorem 4:([4],[11])

(a) The entries of a Markoff triple are pairwise coprime.

(b) Every odd Markoff number is congruent 1 modulo 4.

(c) Every even Markoff number is congruent 2 modulo 32.

Proof of Theorem 4:

(a) Let (a, b, c) be any Markoff triple. Suppose $\gcd(a, b) \neq 1$ and hence there exists a prime number p such that $p \,|\, \gcd(a, b)$. Then we can let $a = pa_1$ and $b = pb_1$ for some positive integers a_1 and b_1. So (1) can be expressed as $(pa_1)^2 + (pb_1)^2 + c^2 = 3(pa_1)(pb_1)c$ and it follows that $p \,|\, c$ since p is a prime number. Hence we let $c = pc_1$ for some positive integer c_1 and immediately it leads to $a_1^2 + b_1^2 + c_1^2 = (3p)a_1b_1c_1$. By Lemma 2, it is a contradiction. Hence we have $\gcd(a, b) = 1$. Similarly, we can also obtain $\gcd(b, c) = \gcd(c, a) = 1$. Therefore, the entries of a Markoff triple are pairwise coprime.

(b) Without loss of generality, suppose (a, b, c) is any Markoff triple with odd a. Since (1) can be transformed to $b^2 + c^2 = a(3bc - a)$ and $\gcd(b, c) = 1$, by Lemma 3 we immediately have a is congruent 1 modulo 4. As a result, every odd Markoff number is congruent 1 modulo 4.

(c) Suppose (a, b, c) is any Markoff triple with even c. By (a)(b) we have $a \equiv b \equiv 1 \pmod 4$. Notice that (1) can be transformed to $c(3ab - c) = a^2 + b^2$, and it follows that $c \equiv 2 \pmod 8$ by checking $c = 8k$, $8k + 2$, $8k + 4$ or $8k + 6$, respectly. So $\frac{b-a}{2}$ is even, $\frac{c}{2} \equiv 1 \pmod 4$ and $3c - 2 \equiv 4 \pmod 8$, which implies that $\frac{3c-2}{4}$ is odd. Therefore, the Markoff equation can be written as the form: $(\frac{b-a}{2})^2 + (\frac{c}{2})^2 = ab(\frac{3c-2}{4})$. Moreover, since $\gcd(a, \frac{c}{2}) = \gcd(b, \frac{c}{2}) = \gcd(\frac{c}{2}, \frac{3c-2}{4}) = 1$, we may conclude that $\frac{b-a}{2}$ and $\frac{c}{2}$ are coprime. By Lemma 3 it follows that $\frac{3c-2}{4} \equiv 1 \pmod 4$, which implies that $c \equiv 2 \pmod{16}$ by checking $c = 16k$, $16k + 2$, $16k + 4$, ..., $16k + 10$, respectly. Then $3c + 2 \equiv 8 \pmod{16}$

and hence $\frac{3c+2}{8}$ is odd. Similarly, since the Markoff equation can be expressed as $(\frac{b+a}{2})^2 + (\frac{c}{2})^2 = 2ab(\frac{3c+2}{8})$ and $\gcd(a, \frac{c}{2}) = \gcd(b, \frac{c}{2}) = \gcd(\frac{c}{2}, \frac{3c+2}{8}) = 1$, so $\frac{b-a}{2}$ and $\frac{c}{2}$ are coprime and apply Lemma 3 again, we have $\frac{3c+2}{8} \equiv 1 \pmod 4$. Consequently, by checking c in detail, we conclude that $c \equiv 2 \pmod{32}$ and the proof is completed.

3 Main Theorem

In this section, we shall first introduce some useful lemmas for proving our main theorem of this paper.

The following lemma is the key for our main theorem.

Lemma 5: Suppose $m = kp^n$ for an odd prime number p and positive integers k and n. Then, for any integer r coprime to m, the quadratic residue

$$x^2 \equiv r \pmod{m} \tag{2}$$

has at most one solution with $0 < u < \frac{m}{2k}$.

Remark: It has been shown in [11] for $k = 1$.

Proof of Lemma 5:

Suppose the quadratic residue $x^2 \equiv r \,(\text{mod } m)$ has two solutions u and u' such that

$$0 < u < u' < \frac{m}{2k}$$

Then clearly we have $u^2 \equiv r \equiv (u')^2 \,(\text{mod } m)$ and hence obtain $m \,|\, (u')^2 - u^2$; that is,

$$kp^n \,|\, (u' + u)(u' - u)$$

Note that

$$0 < u' + u < \frac{m}{k} = \frac{kp^n}{k} = p^n$$
$$0 < u' - u < \frac{m}{2k} = \frac{kp^n}{2k} = \frac{p^n}{2}$$

If both $u' + u$ and $u' - u$ have a common divisor p; that is, $p \,|\, u' + u$ and $p \,|\, u' - u$, it then follows that $p \,|\, 2u$ and hence implies $p \,|\, u$ since p is an odd prime number. In addition, since u is a solution for (2), we obtain $kp^n \,|\, u^2 - r$. Consequently, we have $p \,|\, r$. This contradicts the choice of r which is coprime to m. Thus $u' + u$ and $u' - u$ do not have a common divisor p; that is, we must have either $p^n \,|\, u' + u$ or

$p^n \mid u' - u$. However, $0 < u' + u < p^n$ and $0 < u' - u < \frac{p^n}{2}$ make the divisibilities above fail, which is again a contradiction. Therefore, (2) indeed has at most one solution u with $0 < u < \frac{m}{2k}$ and the proof is completed.

Remark 6: It's already known that if (a, b, c) is a non-singular Markoff triple, we have $b > 2a$. Moreover, if a non-singular Markoff triple $(a, b, c) \neq (1, 2, 5)$, we have $c > 2b$. See [11].

The following lemma gives further property in some particular condition for Markoff triples.

Lemma 7: Suppose (a, b, c) is a non-singular Markoff triple. If $a \geq \frac{k+1}{3}$ for a positive integer k, then we have $c > kb$.

Proof: Note that the Markoff equation can be rewritten as the form

$$c^2 - 3abc + a^2 + b^2 = 0$$

and therfore c can be regarded as a solution for the quadratic equation

$$x^2 - (3ab)x + (a^2 + b^2) = 0. \tag{3}$$

Suppose c' is another solution for (3), then we obtain

$$\begin{aligned} c + c' &= 3ab \\ cc' &= a^2 + b^2. \end{aligned}$$

Now we consider the following:

$$\begin{aligned} (c - b)(c' - b) &= cc' - (c + c')b + b^2 \\ &= (a^2 + b^2) - (3ab)b + b^2 \\ &= a^2 + 2b^2 - 3ab^2 \\ &= (a^2 - ab^2) + (2b^2 - 2ab^2) \\ &= a(a - b^2) + 2b^2(1 - a). \end{aligned} \tag{4}$$

Since (a, b, c) is a non-singular Markoff triple, clearly we have $a - b^2 < 0$ and $1 - a \leq 0$ in (4). Therefore, $(c - b)(c' - b) < 0$ and immediately we obtain $c' < b$. Moreover, since $a \geq \frac{k+1}{3}$, we have

$$c = 3ab - c' \geq (k+1)b - c' > (k+1)b - b = kb,$$

which is what we want and thus we complete the proof.

Remark: Lemma 5 in [11] is a special case of Lemma 7 for $k = 2$.

Theorem 8: Let (a, b, c) and (a', b', c) be non-singular Markoff triples with $a, a' \geq \frac{k+1}{3}$, where k is a positive odd integer. If either $3c + 2$ or $3c - 2$ is k times an odd prime power, then $a = a'$ and $b = b'$.

Proof of Theorem 8:

Case 1: Suppose $3c + 2 = kp^n$. For convenience, we write $m = 3c + 2$. Note that the Markoff equation can be rewritten as the form

$$(a + b)^2 + c^2 = ab(3c + 2). \tag{5}$$

So we have

$$(a + b)^2 + c^2 = abm \equiv 0 \pmod{m}$$

Thus, $a + b$ is a solution of the quadratic residue $x^2 + r \equiv 0 \,(\mathrm{mod}\ m)$, where $r = c^2$. Let $\gcd(c, m) = \gcd(c, 3c + 2) = d$. Clearly we have $d|c$ and $d \,|\, 3c + 2$, which leads to obtain $d \,|\, 2$. Since c is an odd number in this case, we immediately have $d = 1$ and conclude that r and m are coprime. In addition, since $a \geq \frac{k+1}{3}$, by Remark 6 and Lemma 7,

$$0 < a + b \leq \frac{3}{2}b \leq \frac{3c}{2k} < \frac{3c+2}{2k} = \frac{m}{2k}.$$

Similarly as the above method, $a' + b'$ is also a solution for the same quadratic residue $x^2 + r \equiv 0 \,(\mathrm{mod}\ m)$ with $\gcd(r, m) = 1$ and $0 < a' + b' < \frac{m}{2k}$. By Lemma 5, it implies that $a + b = a' + b'$. Substituting this result back into the equation (5), one then obtains

$$ab(3c + 2) = (a + b)^2 + c^2 = (a' + b')^2 + c^2 = a'b'(3c + 2),$$

which implies that $ab = a'b'$. Hence both {a,b} and {a',b'} are the roots of the same quadratic equation and this goes to $a = a'$ and $b = b'$.

Case 2: Assume $3c-2=kp^n$. To simply the notation again, let $m=3c-2$. Similarly as the Case 1 , we rewrite the Markoff equation as the form

$$(a-b)^2+c^2=ab(3c-2) \tag{6}$$

and immediately obtain

$$(b-a)^2+c^2=abm\equiv 0 \pmod{m}$$

So that $b-a$ is a solution of the quadratic residue $x^2+r\equiv 0 \,(\mathrm{mod}\ m)$, where $r=c^2$ and $\gcd(r,m)=1$. Moreover, since $a\geq \frac{k+1}{3}$ and (a,b,c) are non-singular Markoff triples, by Lemma 7 again,

$$0<b-a\leq \frac{c}{k}-a<\frac{2c}{2k}<\frac{3c-2}{2k}=\frac{m}{2k}.$$

The same argument is also for the non-singular Markoff triple (a',b',c'); that is, $a'+b'$ is also a solution for the same quadratic residue $x^2+r\equiv 0\,(\mathrm{mod}\ m)$ with $\gcd(r,m)=1$ and $0<b'-a'<\frac{m}{2k}$. Now applying Lemma 5, it implies that $b-a=b'-a'$. Substituting this relation back into the equation (6),

$$ab(3c-2)=(b-a)^2+c^2=(b'-a')^2+c^2=a'b'(3c-2)$$

and hence we have $ab=a'b'$. Again, it follows that $a=a'$ and $b=b'$. This completes the proof of Theorem 8.

Remark: Take $k=1$ in Therem 7, then we have the following statement: If one of $3c+2$ and $3c-2$ is a prime power, the Markoff Conjecture holds for the non-singular Markoff triples (a,b,c) and (a',b',c); that is, $a=a'$ and $b=b'$. This is part of the results in the [11].

Reference

[1] A.A Markoff, *Sur les forme quadratiques binaires indéfinies. I*, Math. Ann. 15 (1879), 381-409.

[2] A.A Markoff, *Sur les forme quadratiques binaires indéfinies. II*, Math. Ann. 17 (1880), 379-399.

[3] A. Baragar, *On the unicity conjecture for Markoff numbers*, Canad. Math. Bull. 39 (1996), no. 1, 3-9.

[4] G. Frobenius, *über die Markoffschen Zhalen*, Press. Akad. Wiss. Sitzungsberichte, 1913, 458-487; Ges. Abh. Vol.III, Springer-Verlag,Berlin, 1968, pp. 598-627.

[5] J. O. Button, *Markoff numbers, principal ideals and continued fraction expansions*, Journal of Number Theory 87 (2001), no. 1, 77-95

[6] J. O. Button, *The uniqueness of the prime Markoff numbers*, J. London Math. Soc. (2) 58 (1998), no. 1, 9-17.

[7] J.W.S Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathem-Atics and Mathematical Physics, 45, Cambridge University Press, New York (1957).

[8] N. J. A. Sloane, Sequence A00259 in "The On-Line Encyclopedia of Integer Sequences".

[9] M. L. Lang and S. P. Tan, *A simple proof of Markoff conjecture for prime powers*, preprint, arXiv: math.NT/0508443.

[10] P. Schmutz, *Syotles of arithmetic surfaces and the Markoff spectrum*, Math. Ann. 305 (1996), no. 1, 191-203.

[11] Y. Zhang, *Congruence and uniquencess of certaion Markoff numbers*, preprint, arXiv: math. no. NT/0612620 (version 2), (2006)

[12] 沈雅引, *On the Solutions of Certain Markoff Numbers*, 國立臺灣師範大學數學系碩士論文 (2007)

[13] 林志穎, *On the Diophantine Equations* $x^2 + y^2 + z^2 = kxyz$, 國立臺灣師範大學數學系碩士論文 (2007)