ACTA ARITHMETICA
128.3 (2007)

Congruence and uniqueness of certain Markoff numbers

by

Ying Zhang (Yangzhou)

1. Introduction. It is A. A. Markoff who first studied the Diophantine equation (now known as the *Markoff equation*)

$$a^2 + b^2 + c^2 = 3abc \tag{1}$$

in the late 1870s in his famous work [11] on the minima of real, indefinite, binary quadratic forms. (For interpretations of Markoff's work, see [8], [4] and [7]. For its relation to the hyperbolic geometry of the modular torus, see [5] and [13].)

The positive integers a, b, c satisfying (1) are particularly important in the work of Markoff, and Frobenius [9] called them the *Markoff numbers*. The solution triples (a, b, c) of positive integers are called the *Markoff triples*. For convenience, we shall not distinguish a Markoff triple from others obtained by permuting its elements, i.e., from its permutation class, and when convenient, usually arrange its elements in ascending order. We shall call the two Markoff triples $(1, 1, 1)$ and $(1, 1, 2)$ *singular*, while all the others *non-singular*. It is easy to show that the elements of a non-singular Markoff triple are all distinct.

In ascending order of their largest elements, the first 12 Markoff triples are: $(1, 1, 1)$, $(1, 1, 2)$, $(1, 2, 5)$, $(1, 5, 13)$, $(2, 5, 29)$, $(1, 13, 34)$, $(1, 34, 89)$, $(2, 29, 169)$, $(5, 13, 194)$, $(1, 89, 233)$, $(5, 29, 433)$, $(89, 233, 610)$. And the first 40 Markoff numbers are recorded in [14].

The particular interest of the Markoff equation lies in the fact that it is a quadratic equation in each of a, b and c, and hence new solutions can be obtained by a simple process from any given one, (a, b, c). To see this, keep a and b fixed and let c' be the other root of (1), regarded as a quadratic equation in c. Since (1) can be rewritten as $c^2 - 3abc + (a^2 + b^2) = 0$, we have $c + c' = 3ab$ and $cc' = a^2 + b^2$. Thus $c' = 3ab - c$ is a positive integer

2000 *Mathematics Subject Classification*: Primary 11D45; Secondary 11A07.
Supported by a CNPq-TWAS Postdoctoral Fellowship and in part by NKBRF (China) grant no. G1999075104 and NSFC grant no. 10671171.

 © Instytut Matematyczny PAN, 2007

and (a, b, c') is another solution triple to (1) in positive integers, that is, a Markoff triple. Similarly, we obtain two other Markoff triples (a', b, c) and (a, b', c). We call the three new Markoff triples thus obtained the *neighbors* of the given one.

In [11], Markoff demonstrated that every Markoff triple can be obtained from $(1, 1, 1)$ by repeatedly generating new neighbors.

THEOREM A (Markoff [11]). *Every Markoff triple can be traced back to* $(1, 1, 1)$ *by repeatedly performing the following operation on Markoff triples*:

$$(a, b, c) \mapsto (a, b, c') := (a, b, 3ab - c), \tag{2}$$

where the elements of (a, b, c) *are arranged so that* $a \le b \le c$, *and the elements of* (a, b, c') *need to be rearranged in ascending order to perform the next operation.*

Markoff's proof of Theorem A can be found in [11, pp. 397–398]. A different, simple proof can be found in [4, pp. 27–28]; see also [7, pp. 17–18]. Another slightly different proof is given by the author in [15].

The idea of the proof given in [4] is that operation (2) above reduces the largest elements of Markoff triples as long as the input triple is non-singular. Indeed, if $a < b < c$ then $(c-b)(c'-b) = cc' - (c+c')b + b^2 = a^2 + 2b^2 - 3ab^2 < 0$, and hence $c' < b$. Therefore, after a finite number of steps of reduction, the process will stop at a singular Markoff triple, which is in fact $(1, 1, 2)$. Applying operation (2) another time then gives $(1, 1, 1)$.

As an immediate corollary of Theorem A, we have

THEOREM B (Frobenius [9]).

(a) *The elements of a Markoff triple are pairwise coprime.*
(b) *Every odd Markoff number is* $\equiv 1 \pmod 4$.
(c) *Every even Markoff number is* $\equiv 2 \pmod 8$.

Proof. By (1), $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = \gcd(a, b, c)$, and by Theorem A, $\gcd(a, b, c) = \gcd(a, b, 3ab - c) = \cdots = \gcd(1, 1, 1) = 1$. This proves (a).

Since $c(3ab - c) = a^2 + b^2$ and $\gcd(a, b) = 1$, c is not a multiple of 4, and for each prime factor p, -1 is a quadratic residue modulo p. Since it is well known that -1 is not a quadratic residue modulo a prime $\equiv 3 \pmod 4$, each odd prime factor of c is $\equiv 1 \pmod 4$, from which (b) and (c) follow. ∎

The following conjecture on the uniqueness of Markoff numbers or Markoff triples was somewhat hidden in the work of Markoff and was first mentioned explicitly as a question by G. Frobenius in his 1913 paper [9]. It asserts that a Markoff triple is uniquely determined by its largest element. We shall simply say that a Markoff number c is *unique* if the following holds for c.

THE UNICITY CONJECTURE. *Suppose* (a, b, c) *and* $(\widetilde{a}, \widetilde{b}, c)$ *are Markoff triples with* $a \le b \le c$ *and* $\widetilde{a} \le \widetilde{b} \le c$. *Then* $a = \widetilde{a}$ *and* $b = \widetilde{b}$.

The conjecture has become widely known when Cassels mentioned it in [4, p. 33]; see also [7, p. 11, p. 26] and [6, p. 188]. It has been proved only for some rather special subsets of the Markoff numbers. The following result for Markoff numbers which are prime powers or 2 times prime powers was first proved independently and partly by Baragar [1] (for primes and 2 times primes), Button [2] (for primes but can be easily extended to prime powers) and Schmutz [12] (for prime powers but the proof works also for 2 times prime powers) using either algebraic number theory ([1], [2]) or hyperbolic geometry ([12]). A simple, short proof using the hyperbolic geometry of the modular torus as used by Cohn in [5] has been obtained a bit later but only recently posted by Lang and Tan [10]. See [15] for a completely elementary proof which uses neither hyperbolic geometry nor algebraic number theory. A stronger result along the same lines has been obtained by Button in [3]; in particular, the Markoff numbers which are "small" ($\le 10^{35}$) multiples of prime powers are unique.

THEOREM C (Baragar [1]; Button [2]; Schmutz [12]). *A Markoff number is unique if it is a prime power or* 2 *times a prime power.*

In this paper we first obtain the following simple but sharper congruence for all even Markoff numbers.

THEOREM 1. *If* c *is an even Markoff number then* $c \equiv 2 \pmod{32}$.

This congruence is best possible since the first two even Markoff numbers are 2 and 34. And it seems only the congruence $c \equiv 2 \pmod 8$ has been previously observed by Frobenius [9]. As a consequence of Theorem 1, we see that for an even Markoff number c,

$$3c - 2 \equiv 4 \pmod{32} \quad \text{and} \quad 3c + 2 \equiv 8 \pmod{32};$$

hence $3c-2$ and $3c+2$ are respectively 4 times and 8 times an odd number.

As the other main result of this paper, we then have the following

THEOREM 2. *A Markoff number* c *is unique if one of* $3c+2$ *and* $3c-2$ *is a prime power*, 4 *times a prime power*, *or* 8 *times a prime power.*

In the case where one of $3c+2$ and $3c-2$ is a prime or 4 times a prime, this has been obtained by Baragar in [1] (and earlier by D. Zagier but not published).

The proofs of Theorems 1 and 2 will be given in §3. Our method is completely self-contained and elementary in the sense that it uses nothing but very basic facts on congruence, which we list as Lemmas 3 and 4 in §2 and include proofs. It is most important for us to note that Markoff's equation (1)

can be rewritten as

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

$$(a+b)^2 + c^2 = ab(3c+2). \tag{4}$$

Actually, the result in Theorem 2 came to the author's mind immediately after he saw (3) and (4) printed in [9, p. 601].

2. Lemmas. The following two basic facts from elementary number theory will be used in the proofs of the theorems. We include their proofs to make the paper self-contained.

LEMMA 3. *If x and y are coprime integers then every odd factor of x^2+y^2 is $\equiv 1 \pmod 4$.*

Proof. It is shown in the proof of Theorem B that every odd prime factor of x^2+y^2 is $\equiv 1 \pmod 4$, from which the conclusion of the lemma follows. ∎

LEMMA 4. *Suppose $m = p^n$ or $2p^n$ for an odd prime p and an integer $n \ge 1$. Then, for any integer r coprime to m, the binomial quadratic equation*

$$x^2 + r \equiv 0 \pmod m \tag{5}$$

has at most one integer solution x with $0 < x < m/2$.

Proof. We prove the lemma for $m = 2p^n$ only; the proof for $m = p^n$ is similar and actually a bit simpler. Suppose (5) has two integer solutions x and $\widetilde{x}$ such that $0 < x < \widetilde{x} < m/2$. Then $2p^n \mid (\widetilde{x}+x)(\widetilde{x}-x)$. Note that $0 < \widetilde{x}+x < 2p^n$ and $0 < \widetilde{x}-x < p^n$. If $p \mid \widetilde{x}+x$ and $p \mid \widetilde{x}-x$ then $p \mid 2x$; hence $p \mid x$, and consequently $p \mid r$, a contradiction. Therefore we must have $p^n \mid \widetilde{x}+x$ and $2 \mid \widetilde{x}-x$. But then $\widetilde{x}+x = p^n$ and $\widetilde{x} \equiv x \pmod 2$, which implies that p^n is even, again a contradiction. This completes the proof of Lemma 4. ∎

REMARK. One may give a direct proof for Lemma 4 using the fact that in this case there is a primitive root of m.

For the proof of Theorem 2, we shall also need the following rough comparison among the elements of a non-singular Markoff triple.

LEMMA 5. *Suppose $(a,b,c) \ne (1,2,5)$ is a Markoff triple with $a < b < c$. Then*

$$c > 2ab \quad \text{and} \quad b > 2c'a, \tag{6}$$

where $c' = 3ab - c$; in particular, $c > 2b$ and $b > 2a$.

Proof. By Theorem A, every Markoff triple $(a,b,c) \ne (1,2,5)$ can be obtained by repeatedly generating new neighbors starting from $(1,2,5)$. Hence we only need to show that if (6) holds for (a,b,c) then it also holds for the two new neighbors (a',b,c) and (a,b',c), where $a' = 3bc-a$ and $b' = 3ca-b$.

For this we only need to check $a' > 2bc$ and $b' > 2ca$, which are very easy. This proves Lemma 5. ∎

REMARK. It can be seen from the above proof that the result of Lemma 5 can be improved, say, as $c > 5ab/2$ and $b > 5c'a/2$ if $(a,b,c) \neq (1,2,5)$, $(2,5,29)$; actually, this was already known to Frobenius [9] with a different proof. But for our purposes in this paper the weaker result that $c > 2b$ and $b > 2a$ is enough.

3. Proof of Theorems 1 and 2

Proof of Theorem 1. Suppose (a,b,c) is a Markoff triple with $a < b < c$ such that c is even. By Theorem B, $a \equiv b \equiv 1 \pmod 4$ and $c \equiv 2 \pmod 8$, hence $(a-b)/2$ is even and $c/2 \equiv 1 \pmod 4$. Since $3c-2 \equiv 4 \pmod 8$, we know that $(3c-2)/4$ is odd. Then (3) gives

$$((b-a)/2)^2 + (c/2)^2 = ab(3c-2)/4. \tag{7}$$

Since $\gcd(c/2,a) = \gcd(c/2,b) = 1$ and $\gcd(c/2,(3c-2)/4) = 1$, we know that $c/2$ is coprime with $ab(3c-2)/4$, and consequently, $(b-a)/2$ and $c/2$ are coprime. Then Lemma 3 implies $(3c-2)/4 \equiv 1 \pmod 4$, from which it follows that $c \equiv 2 \pmod{16}$.

Then $3c+2 \equiv 8 \pmod{16}$ and hence $(3c+2)/8$ is odd. Now (4) gives

$$((a+b)/2)^2 + (c/2)^2 = 2ab(3c+2)/8. \tag{8}$$

Since $\gcd(c/2,a) = \gcd(c/2,b) = 1$ and $\gcd(c/2,(3c+2)/4) = 1$, we know that $c/2$ is coprime with $ab(3c+2)/4$, and consequently, $(a+b)/2$ and $c/2$ are coprime. Then Lemma 3 implies $(3c+2)/8 \equiv 1 \pmod 4$, which yields $c \equiv 2 \pmod{32}$. This proves Theorem 1. ∎

Proof of Theorem 2. Suppose (a,b,c) and $(\widetilde{a},\widetilde{b},c)$ are Markoff triples with $a \le b \le c$ and $\widetilde{a} \le \widetilde{b} \le c$. We proceed to show that if $3c-2$ or $3c+2$ is of the form p^n, $4p^n$ or $8p^n$ for an odd prime p and an integer $n \ge 1$ then $a = \widetilde{a}$ and $b = \widetilde{b}$.

CASE 1: *c is odd.*

SUBCASE 1.1: Suppose $3c-2 = p^n$. Write $m = 3c-2$. Then (3) gives

$$(b-a)^2 + c^2 = abm \equiv 0 \pmod m. \tag{9}$$

Note that $\gcd(c,m) = 1$ since $\gcd(c,m) \mid 2$ and c is odd. By Lemma 5,

$$0 < b-a < c/2 - 1 < (3c-2)/2 = m/2. \tag{10}$$

Since (9) and (10) are also true for $(\widetilde{a},\widetilde{b},c)$, Lemma 4 implies $b-a = \widetilde{b}-\widetilde{a}$. Substituting this relation back into (9) and its analog for $(\widetilde{a},\widetilde{b},c)$, one then obtains $ab = \widetilde{a}\widetilde{b}$. Hence both $\{-a,b\}$ and $\{-\widetilde{a},\widetilde{b}\}$ are the roots of the same quadratic equation. This implies $a = \widetilde{a}$ and $b = \widetilde{b}$.

SUBCASE 1.2: Suppose $3c+2=p^n$. Write $m=3c+2$. The proof is similar to that of Subcase 1.1, with the use of

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

and $0<a+b<3c/4<(3c+2)/2=m/2$.

CASE 2: *c is even.* By Theorem 1, $3c-2$ is 4 times an odd and $3c+2$ is 8 times an odd. And by Theorem B, $a\equiv b\equiv 1 \pmod 4$ and $\widetilde{a}\equiv\widetilde{b}\equiv 1 \pmod 4$.

SUBCASE 2.1: Suppose $3c-2=4p^n$. Write $m=(3c-2)/4=p^n$. Then (3) gives

$$((b-a)/2)^2+(c/2)^2=abm\equiv 0 \pmod m. \tag{11}$$

Since $\gcd(c,3c-2)=2$, we have $\gcd(c/2,m)=1$. By Lemma 5,

$$0<(b-a)/2<c/4<(3c-2)/8=m/2. \tag{12}$$

Since (11) and (12) are also true for $(\widetilde{a},\widetilde{b},c)$, Lemma 4 implies that $b-a=\widetilde{b}-\widetilde{a}$, and consequently, $ab=\widetilde{a}\widetilde{b}$. Therefore $a=\widetilde{a}$ and $b=\widetilde{b}$.

SUBCASE 2.2: Suppose $3c+2=8p^n$. Write $m=(3c+2)/4=2p^n$. The proof is similar to that of Subcase 2.1, with the use of

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

again $\gcd(c/2,m)=1$, and $0<(a+b)/2<3c/8<(3c+2)/8=m/2$.

This completes the proof of Theorem 2. ∎

Acknowledgements. The author would like to thank Ser Peow Tan for very helpful conversations and suggestions during his visit to IMPA, Rio de Janeiro in mid-December, 2006.

References

[1] A. Baragar, *On the unicity conjecture for Markoff numbers*, Canad. Math. Bull. 39 (1996), 3–9.

[2] J. O. Button, *The uniqueness of the prime Markoff numbers*, J. London Math. Soc. (2) 58 (1998), 9–17.

[3] —, *Markoff numbers, principal ideals and continued fraction expansions*, J. Number Theory 87 (2001), 77–95.

[4] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge Tracts in Math. Math. Phys. 45, Cambridge Univ. Press, New York, 1957.

[5] H. Cohn, *Approach to Markoff's minimal forms through modular functions*, Ann. of Math. (2) 61 (1955), 1–12.

[6] J. H. Conway and R. K. Guy, *The Book of Numbers*, Copernicus Press, New York, 1996.

[7] T. W. Cusick and M. E. Flahive, *The Markoff and Lagrange Spectra*, Math. Surveys Monogr. 30, Amer. Math. Soc., Providence, RI, 1989.

[8] L. E. Dickson, *Studies in the Theory of Numbers*, The Univ. of Chicago Press, Chicago, 1930.

[9] G. Frobenius, *Über die Markoffschen Zahlen*, Preuss. Akad. Wiss. Sitzungsber. 1913, 458–487; Ges. Abh., vol. III, Springer, Berlin, 1968, 598–627.

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

[11] A. A. Markoff, *Sur les formes quadratiques binaires indéfinies. II*, Math. Ann. 17 (1880), 379–399.

[12] P. Schmutz, *Systoles of arithmetic surfaces and the Markoff spectrum*, ibid. 305 (1996), 191–203.

[13] C. Series, *The geometry of Markoff numbers*, Math. Intelligencer 7 (1985), no. 3, 20–29.

[14] N. J. A. Sloane, Sequence A002559 in "The On-Line Encyclopedia of Integer Sequences".

[15] Y. Zhang, *An elementary proof of uniqueness of Markoff numbers which are prime powers*, preprint, arXiv:math.NT/0606283 (version 2).

School of Mathematical Sciences
Yangzhou University
Yangzhou, Jiangsu 225002, China
E-mail: yingzhang@alumni.nus.edu.sg

Received on 31.1.2007 (5384)