Canad. Math. Bull. Vol. 39 (1), 1996 pp. 3–9

ON THE UNICITY CONJECTURE FOR MARKOFF NUMBERS

ARTHUR BARAGAR

ABSTRACT. In 1913 Frobenius conjectured that for any positive integer m, there exists at most one pair of integers (x, y) with $0 \leq x \leq y \leq m$ such that (x, y, m) is a solution to the Markoff equation: $x^2 + y^2 + m^2 = 3xym$. We show this is true if either m, $3m - 2$ or $3m + 2$ is prime, twice a prime or four times a prime.

0. **Introduction.** Markoff (1879) [M] studied the equation

$$x^2 + y^2 + z^2 = 3xyz, \tag{0.1}$$

and showed its set of integral solutions is the orbit of the fundamental solution $(1, 1, 1)$ under the action of the group of automorphisms $\mathcal{G}$ generated by the permutations S_3 on $\{x, y, z\}$, the sign change

$$\rho \colon (x, y, z) \longrightarrow (-x, -y, z),$$

and

$$\phi_3 \colon (x, y, z) \longrightarrow (x, y, 3xy - z).$$

Further, the positive ordered integral solutions (the *Markoff triples*) all lie in the tree rooted at $(1, 1, 1)$ with branching operations

$$\phi_2 \colon (x, y, z) \longrightarrow (x, z, 3xz - y)$$

$$\phi_1 \colon (x, y, z) \longrightarrow (y, z, 3yz - x).$$

This tree has appeared frequently in the literature (see [C], [Z].)

Frobenius (1913) [F] conjectured that any Markoff number m appears uniquely as the maximal element of a Markoff triple, *i.e.*, if (x_1, y_1, m) and (x_2, y_2, m) are both integral solutions to (0.1), and $0 \leq x_i \leq y_i \leq m$, then $x_1 = x_2$ and $y_1 = y_2$.

In this paper, we prove a weaker result:

THEOREM 0.1. *If either m, $3m - 2$ or $3m + 2$ is a prime, twice a prime or four times a prime, then there exists at most one integer pair (x, y) so that (x, y, m) is a Markoff triple.*

This result was independently proved by Zagier a number of years ago, though his results were never published. The general approach—to look at the factorization of ideals in orders—was also known to Harvey Cohn, and may be 'well known', but only recently appeared in print [B].

Received by the editors January 4, 1995.
AMS subject classification: 11D25.

1. **A Reformulation.** Our approach is to fix a Markoff number m, and consider the resulting quadratic equation as a norm equation in a real quadratic field. We identify an integer solution to the Markoff equation with a solution to the norm equation that lies in a certain order. The details are easiest to check if the order in question is the ring of integers, but the theory works with orders too, though we must consider the problem in two parts— the case with m odd, and the case with m even.

We first fix m odd, and consider the equation

$$x^2 + y^2 - 3mxy = -m^2. \tag{1.1}$$

We can rewrite (1.1) as

$$N_{K/\mathbb{Q}}(x + \omega y) = -m^2$$

where $K = \mathbb{Q}(\omega)$ and ω is the larger number that satisfies $\omega^2 + 3m\omega + 1 = 0$. Hence there is a one-to-one correspondence between integer solutions (x, y) of (1.1) and elements β in the order $R = \mathbb{Z} + \omega\mathbb{Z}$ that satisfy

$$N_{K/\mathbb{Q}}(\beta) = -m^2. \tag{1.2}$$

There is a natural subgroup H of $\mathcal{G}$ that acts on (1.1), holding m fixed. This is the group generated by

$$\begin{aligned} \sigma &: (x, y, m) \longmapsto (y, x, m) \\ \rho &: (x, y, m) \longmapsto (-x, \ -y, m) \\ \phi &: (x, y, m) \longmapsto (y, 3ym - x, m). \end{aligned}$$

We would like to describe this as the subgroup that fixes m, but that is precisely the unicity conjecture.

These automorphisms have natural interpretations in R. The sign change ρ is multiplication by -1; ϕ is multiplication by the unit $-\omega$; and the permutation σ is conjugation followed by multiplication by ω. Furthermore, if $m \neq 1$, then ω is a fundamental unit. Hence, there is a one-to-one correspondence between orbits of integral solutions to (1.1) and pairs of principal ideals $\{\beta R, \bar{\beta} R\}$ generated by a $\beta \in R$ that satisfies (1.2).

Thus we may reformulate the unicity conjecture:

THEOREM 1.1. *If m is an odd Markoff number, then m is the maximal element of a unique Markoff triple if and only if there exists exactly one pair of principal ideals $\{\beta R, \bar{\beta} R\}$ in R such that β satisfies* (1.2).

In the following, we consider the prime factorization of the ideal βR in R. Since its norm $\mathrm{N}(\beta R) = m^2$ is relatively prime to the discriminant $\Delta = \operatorname{disc}(R) = 9m^2 - 4$, and is therefore coprime to the conductor, which divides Δ, we know this factorization is unique.

Note also that if (x, y, m) is a Markoff triple, then $\gcd(x, y) = 1$, so βR is a *primitive* ideal (*i.e.*, it has no $\mathbb{Z}$ factors.)

COROLLARY 1.2. *If m is an odd prime Markoff number, then m is the maximal element of a unique Markoff triple.*

PROOF. Since m is prime, mR either remains prime in K or has two prime factors: $mR = \mathfrak{p}\bar{\mathfrak{p}}$. Since βR is primitive, $\beta R \neq mR$, so we must have $mR = \mathfrak{p}\bar{\mathfrak{p}}$ and either $\beta R = \mathfrak{p}^2$ or $\beta R = \bar{\mathfrak{p}}^2$. Thus, by Theorem 1.1, m is the maximal element of a unique Markoff triple.

Now, suppose there are two elements β and γ in R that satisfy (1.2) but generate different pairs of ideals. Then we can factor the ideals βR and γR into prime ideals, some of which are common to both, the rest of which must be conjugates, since βR and γR have the same norm. Thus

$$\beta R = \mathfrak{a}_1\mathfrak{a}_2$$

$$\gamma R = \mathfrak{a}_1\bar{\mathfrak{a}}_2,$$

where neither $\mathfrak{a}_1$ nor $\mathfrak{a}_2$ is all of R. Multiplying these together, we get

$$\beta\gamma R = \mathfrak{a}_1^2\mathfrak{a}_2\bar{\mathfrak{a}}_2,$$

so

$$\mathfrak{a}_1^2 \overset{+}{\sim} R$$

where $\overset{+}{\sim}$ is narrow class equivalence. Similarly, by multiplying βR and $\bar{\gamma} R$ together, we get $\mathfrak{a}_2^2 \overset{+}{\sim} R$. One of these two ideals satisfies $\mathrm{N}(\mathfrak{a}_i) < m < \frac{1}{2}\sqrt{\Delta}$.

For any fixed value of m, it is possible to classify all 'small', primitive ideals I whose square is equivalent to R. Our main tool is the theory of continued fractions, which can be thought of as a means of finding good rational approximations. This is the subject of the next section.

2. **A Classification of Certain Ideals.**

In this section, we describe a procedure to find all ideals I in K which are primitive, have norm $\mathrm{N}(I) < \frac{1}{2}\sqrt{\Delta}$, and satisfy $I \overset{+}{\sim} \bar{I}$ (*i.e.*, $I^2 \overset{+}{\sim} R$.) In particular, we show that if either $3m-2$ or $3m+2$ is prime, then $\mathrm{N}(I)$ divides Δ. Thus, in these two cases, the ideal $\mathfrak{a}_i$ cannot exist.

We begin with a couple of useful results which are easy enough to prove:

LEMMA 2.1. *If I is primitive, then there exists a basis over $\mathbb{Z}$ of I of the form $\{r+\omega, \mathrm{N}(I)\}$ for some $r \in \mathbb{Z}$. Furthermore, we may choose r so that*

$$\sqrt{\Delta} - \mathrm{N}(I) < r + \omega \leq \sqrt{\Delta}, \tag{2.1}$$

since this interval has length $\mathrm{N}(I)$.

COROLLARY 2.2. *If J is a primitive ideal and $J = \bar{J}$, then $\mathrm{N}(J)$ divides Δ.*

LEMMA 2.3. *Suppose $I \overset{+}{\sim} \bar{I}$. Then there exists an ideal J in R such that J is primitive, $\mathrm{N}(J)$ divides Δ, and $I \sim J$ where $\sim$ is class equivalence.*

PROOF. Since $I \overset{+}{\sim} \bar{I}$, there exist elements $\alpha_1, \alpha_2 \in R$ such that $\mathrm{N}(\alpha_1), \mathrm{N}(\alpha_2) > 0$ and

$$\alpha_1 I = \alpha_2 \bar{I}.$$

Thus, $\mathrm{N}\left(\frac{\alpha_1}{\alpha_2}\right) = 1$ and by Hilbert's Theorem 90, there exists a $\sigma \in K$ such that

$$\frac{\alpha_1}{\alpha_2} = \frac{\sigma}{\bar{\sigma}}.$$

Furthermore, by multiplying by an appropriate integer, we can insure that $\sigma \in R$. Then we get

$$\sigma I = \bar{\sigma}\bar{I}.$$

Let n be the largest factor of σI in $\mathbb{Z}$, and let $nJ = \sigma I$. Then J is primitive, and $J = \bar{J}$, so by Corollary 2.2, $\mathrm{N}(J)$ divides Δ.

Since $nJ = \sigma I$, there exists an integer matrix A with $\det A = \pm 1$ such that

$$A\begin{bmatrix} n(s+\omega) \\ n\,\mathrm{N}(J) \end{bmatrix} = \begin{bmatrix} \sigma(r+\omega) \\ \sigma\,\mathrm{N}(I) \end{bmatrix},$$

where $J = (s+\omega)\mathbb{Z} \times \mathrm{N}(J)\mathbb{Z}$. Choose $E = \begin{bmatrix} \pm 1 & 0 \\ 0 & 1 \end{bmatrix}$ so that $\hat{A} = EA \in \mathrm{Sl}_2(\mathbb{Z})$. Then we can think of $\hat{A}$ as a fractional linear transformation, and

$$\hat{A}\left(\frac{s+\omega}{\mathrm{N}(J)}\right) = \pm\frac{r+\omega}{\mathrm{N}(I)}.$$

Let us set

$$x_I = \frac{r+\omega}{\mathrm{N}(I)} \quad \text{and} \quad x_J = \frac{s+\omega}{\mathrm{N}(J)}.$$

We now use some results from the theory of continued fractions [N-Z, Ch. 7]. If two real quadratic numbers differ by a fractional linear transformation, then they have the same repeating part. Furthermore, if a real quadratic number $x > 1$ satisfies $-1 < \bar{x} < 0$, then x has a periodic continued fraction. That is to say,

$$x = \langle \overline{a_0, \ldots, a_n} \rangle.$$

Lemma 2.4. *Suppose a primitive ideal I satisfies $\mathrm{N}(I) < \frac{1}{2}\sqrt{\Delta}$. Then x_I has a periodic continued fraction expansion.*

Proof. Since $\mathrm{N}(I) < \frac{1}{2}\sqrt{\Delta}$, we get from (2.1) that

$$1 < x_I;$$

and since $\omega - \bar{\omega} = \sqrt{\Delta}$,

$$-1 < \bar{x}_I = \frac{r+\bar{\omega}}{\mathrm{N}(I)} = \frac{r+\omega-\sqrt{\Delta}}{\mathrm{N}(I)} < 0.$$

Thus, we can find all such ideals I by finding the periodic part of the continued fraction expansion of x_J for all J whose norm divides Δ. For a fixed m, this is of course possible, but for arbitrary m, this approach may be of little use. There are however a couple of exceptions.

LEMMA 2.5. *Suppose* $\mathrm{N}(J) = t$ *and* $tu = 3m - 2$ *with* $u \in \mathbb{Z}$. *That is, suppose* $\mathrm{N}(J)$ *divides* $3m - 2$. *Then* $\mathrm{N}(I) = t$ *or* u.

PROOF. Note that

$$J = \left(\frac{tu + \sqrt{\Delta}}{2}\right)\mathbb{Z} + t\mathbb{Z} = \left(\frac{tu - 3m}{2} + \omega\right)\mathbb{Z} + t\mathbb{Z}$$

and

$$\frac{tu + \sqrt{\Delta}}{2t} = \langle \overline{u, t} \rangle,$$

so $\mathrm{N}(I) = t$ or u.

This also shows that if $\mathrm{N}(J) = 3m-2$, then $J \sim R$, since $u = 1$. That is, J is principal.

LEMMA 2.6. *Suppose* $\mathrm{N}(J) = t$ *and* $tu = 3m + 2$ *with* $u \in \mathbb{Z}$ *and* $m > 3$. *Then* $\mathrm{N}(I) = t$ *or* u.

PROOF. Note that

$$J = \left(\frac{tu - 2t + \sqrt{\Delta}}{2}\right)\mathbb{Z} + t\mathbb{Z}$$

and if t and u are greater than 2, then

$$\frac{tu - 2t + \sqrt{\Delta}}{2t} = \langle \overline{u - 2, 1, t - 2, 1} \rangle,$$

so $\mathrm{N}(I) = t$, u or $tu - t - u$. The last is in fact not possible: Since t and u are odd, and not 1, we have $t, u \geq 3$, so

$$tu - t - u > 3m + 2 - 3 - \frac{3m + 2}{3} > \frac{2}{3}\sqrt{\Delta} - \frac{5}{3} > \frac{1}{2}\sqrt{\Delta}.$$

The last inequality follows for $m > 3$. Finally, if $t = 1$ we use Lemma 2.5, and if $t = 3m + 2$, then

$$\frac{-t + \sqrt{\Delta}}{2t} = \langle -1, 1, 3m - 1, \overline{1, 3m - 2} \rangle,$$

so again $\mathrm{N}(I) = 1$ or t. Further, if $\mathrm{N}(J) = 3m + 2$, then J is principal.

The restriction $m > 3$ is not stringent at all, since m is odd, 3 is not a Markoff number, and it is clear there is only one Markoff triple with maximal element equal to 1.

COROLLARY 2.7. *Suppose* $p = 3m - 2$ *or* $3m + 2$ *is prime, and* p *divides* $\mathrm{N}(J)$. *Then there exists a* J' *so that* $J \sim J'$ *and* $\mathrm{N}(J')$ *divides* Δ/p.

PROOF. There exists an ideal $\mathfrak{p} = \left(\frac{p+\sqrt{\Delta}}{2}\right)\mathbb{Z} \times p\mathbb{Z}$ with norm p. By Lemmas 2.5 and 2.6, $\mathfrak{p}$ is principal. Thus

$$J \sim J\mathfrak{p}.$$

But $\mathrm{N}(J\mathfrak{p})$ does not divide Δ, since p^2 cannot divide Δ, so $J\mathfrak{p}$ is not primitive. Furthermore, p must divide the largest factor n of $J\mathfrak{p}$ in $\mathbb{Z}$. Let J' be the ideal such that $nJ' = J\mathfrak{p}$. Then $J' \sim J$ and $\mathrm{N}(J')$ divides $\Delta p/p^2 = \Delta/p$.

Thus, if either $3m - 2$ or $3m + 2$ is prime, then $\mathrm{N}(I)$ divides Δ.

3. **The Even Case.** Finally, we address the possibility that m is even. The argument is almost identical, so we only draw attention to the differences.

Modulo four, the Markoff tree collapses to

$$(1,1,1) \text{——} (1,1,2), \tag{3.1}$$

so m is never 0 modulo 4, and neither $3m-2$ nor $3m+2$ is ever 2 modulo 4. Thus part of the statement of Theorem 0.1 is vacuous.

We also have from (3.1) that when m is even, both x and y are odd, and we can write $m = 2r$ with r odd. Hence, we can rewrite (1.1) as

$$(x-3ry)^2 - (9r^2-1)y^2 = -4r^2,$$

where now $x - 3ry$ is even and $9r^2 - 1 \equiv 0 \pmod 4$, so we can divide through by four to get

$$v^2 - \alpha^2 y^2 = -r^2,$$

where $v = \frac{x-3ry}{2} \in \mathbb{Z}$, $\alpha^2 = \frac{9r^2-1}{4}$, $R = \mathbb{Z} + \alpha\mathbb{Z}$, and $\Delta = \operatorname{disc} R = 9r^2 - 1$. We proceed as before, and discover $\omega = -3r + \sqrt{9r^2-1}$. Again, $\gcd(r, \Delta) = 1$, so we have unique factorization of the ideals that divide r^2R. Assuming the existence of β and γ, we find the ideal $\mathfrak{a}_i$ with $\mathrm{N}(\mathfrak{a}_i) < r$, and investigate the possible ideals I with $\mathrm{N}(I) < r < \frac{1}{2}\sqrt{\Delta}$.

When $\mathrm{N}(J) = t$ and $tu = \frac{3r-1}{2}$, we find

$$J = (tu+\alpha)\mathbb{Z} + t\mathbb{Z}$$

and

$$\frac{tu+\alpha}{t} = \langle \overline{2u, 2t} \rangle$$

so $\mathrm{N}(I) = t$ or u. Again we note that if $\mathrm{N}(J) = \frac{3r-1}{2}$, then $u = 1$ and we find J is principal.

When $\mathrm{N}(J) = t$ and $tu = \frac{3r+1}{2}$, with $t, u \geq 2$, we find

$$J = (tu - t + \alpha)\mathbb{Z} + t\mathbb{Z}$$

and

$$\frac{tu-t+\alpha}{t} = \langle \overline{2u-2, 1, 2t-2, 1} \rangle,$$

so $\mathrm{N}(I) = t$, u or $2tu - t - u$. This time, we get

$$2tu - t - u \geq (3r+1) - 2 - \frac{3r+1}{4} > \frac{3}{4}\sqrt{\Delta} - \frac{5}{4} > \frac{1}{2}\sqrt{\Delta},$$

so again, we get that $\mathrm{N}(I)$ must divide Δ.

If $t = \frac{3r+1}{2}$, then

$$\frac{\alpha}{t} = \langle 0, 1, \overline{2, 3r-1} \rangle,$$

and again we have J principal.

Thus, if either $3m-2$ or $3m+2$ is four times a prime, then $\mathrm{N}(I)$ divides Δ, so $\mathfrak{a}_1$ cannot exist.

4. **An Experiment.** If m is a Markoff number, then m is never four times a prime, and neither $3m - 2$ nor $3m + 2$ is ever twice a prime. Thus, one might wonder whether Theorem 0.1 ever has substance. The number of Markoff numbers below 10^{140} is 18906. Of them, 1197 (or roughly 6%) satisfy the conditions of Theorem 0.1. This was found using Maple's probabilistic primality test, and about ten hours of computing time. This ratio decreases as the bound increases, and empirical evidence suggests it decreases like a constant over the log of the bound, but the data is not very convincing. Heuristic arguments suggest it should not decrease so quickly, since every factor of a Markoff number is equivalent to 1 or 2 modulo 4, and thus the ratio is expected to decrease like a constant over the square root of the log of the bound.

We also note that there are no contradictions to the unicity conjecture among all Markoff triples whose maximal element is less than 10^{140}.

References

[B] A. Baragar, *The Hurwitz Equations*, Number Theory with an Emphasis on the Markoff Spectrum, Lecture Notes in Pure and Applied Mathematics, (A. Pollington and W. Moran), Marcel Dekker, New York **147**(1993), 1–8.

[C] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Chapter II, Cambridge Univ. Press, Cambridge, 1957.

[F] G. Frobenius, *Über die Markoffschen Zahlen*, Akad. Wiss. Sitzungaber, (1913), 458–493.

[G] R. Guy, *Unsolved Problems in Number Theory*, New York, (1981).

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

[N-Z] I. Niven and H. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 1980.

[R-P] D. Rosen and G. Patterson, Jr., *Some Numerical Evidence Concerning the Uniqueness of the Markov Numbers* Math. Comp. **25**(1971), 919–921.

[R] G. Rosenberger, *The Uniqueness of the Markoff Numbers*, but see MR **53** #280, Math. Comp. **30**(1976), 361–365.

[Z] D. Zagier, *On the Number of Markoff Numbers Below a Given Bound*, Math. Comp. **39**(1982), 709–723.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
N2L 3G1
e-mail: abaragar@watdragon.uwaterloo.ca