JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Anitha SRINIVASAN

Markoff numbers and ambiguous classes

Tome 21, n° 3 (2009), p. 757-770.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_3_757_0>

Journal de Théorie des Nombres
de Bordeaux **21** (2009), 757-770

Markoff numbers and ambiguous classes

par Anitha SRINIVASAN

Résumé. La conjecture de Markoff dit qu'étant donné un entier positif c il existe au plus un triplet (a, b, c) d'entiers positifs tels que $a \leq b \leq c$ et satisfaisant l'équation $a^2 + b^2 + c^2 = 3abc$. La conjecture est vraie pour c une puissance d'un nombre premier ou deux fois une puissance d'un nombre premier. Nous présentons une preuve élémentaire de ce résultat. Nous montrons également que si, dans le groupe des classes des formes de discriminant $d = 9c^2 - 4$, toute forme ambige dans le genre principal correspond à un diviseur de $3c - 2$ alors la conjecture est vraie. Comme conséquence, nous obtenons un critère, en termes de symboles de Legendre des premiers divisant d, pour lequel la conjecture est vraie. Nous énonçons également une conjecture pour le corps quadratique $\mathbb{Q}(\sqrt{9c^2 - 4})$ qui est équivalente à la conjecture de Markoff pour c.

Abstract. The Markoff conjecture states that given a positive integer c, there is at most one triple (a, b, c) of positive integers with $a \leq b \leq c$ that satisfies the equation $a^2 + b^2 + c^2 = 3abc$. The conjecture is known to be true when c is a prime power or two times a prime power. We present an elementary proof of this result. We also show that if in the class group of forms of discriminant $d = 9c^2 - 4$, every ambiguous form in the principal genus corresponds to a divisor of $3c-2$, then the conjecture is true. As a result, we obtain criteria in terms of the Legendre symbols of primes dividing d under which the conjecture holds. We also state a conjecture for the quadratic field $\mathbb{Q}(\sqrt{9c^2 - 4})$ that is equivalent to the Markoff conjecture for c.

1. Introduction

A triple (a, b, c) of positive integers that satisfies the Markoff equation

$$a^2 + b^2 + c^2 = 3abc \tag{1.1}$$

is called a Markoff triple; the numbers a, b, and c are called Markoff numbers. The Markoff conjecture states that the maximal element of a Markoff triple uniquely determines the triple. In other words, if (a_1, b_1, c) and

Manuscrit reçu le 15 mai 2008.

(a_2, b_2, c) are two Markoff triples with $a_i \leq b_i \leq c,\ \ i = 1, 2$, then $a_1 = a_2$ and $b_1 = b_2$. In this case c is said to be unique.

This conjecture has fascinated mathematicians for over 100 years now. Markoff numbers made their first appearance in Markoff's famous paper on the least positive integer represented by an indefinite real binary quadratic form [9]. While the proof of the conjecture still eludes us, it has been settled in the case of Markoff numbers that are prime powers or two times a prime power. The first few results on this conjecture are by Baragar [1] for prime Markoff numbers and Button [4] and Schmutz [14] for those that are prime powers or two times a prime power. Recently other proofs [8] and [18] of this result have been given. We present here (Theorem 2.2) a short and completely elementary proof of this same result that uses only gcd considerations.

Many authors have proved uniqueness in special cases such as for example when one of $3c - 2$ or $3c + 2$ is a prime or a prime power as in [1] and [18]. J. Jimenez pointed out to the author yet another simple and short proof of this result (Theorem 2.3). For more interesting results on Markoff numbers and their generalizations, see Bombieri [2], Button [4], Zagier [16], Perrine [11], Perrine[12] and Srinivasan [15].

Here we show that when $d = 9c^2 - 4$ is odd, then c is unique if every ambiguous class in the class group of $\mathbb{Q}(\sqrt{d})$ that belongs to the principal genus (see Definition 3.1), corresponds to a divisor of $3c - 2$. As a result we obtain criteria for uniqueness that are given in terms of the Legendre symbols of the primes in d. In the particular case when $3c - 2$ and $3c + 2$ are both products of two primes we give an explicit criterion in terms of the four primes in d. As this criterion is applicable to cases where existing criteria do not apply, our result extends the collection of unique Markoff numbers.

It can be shown (see remark following the proof of Theorem 5.1) that if a positive integer c is not a prime power, then c is a Markoff number if and only if there is a form $f(x, y) = nx^2 + mxy + ly^2$ of discriminant d that represents $-p^2$ and q^2, for some coprime pair of positive integers p, q, both greater than 1 with $c = pq$. In Theorem 5.1 we show that if this form is not ambiguous then c is unique. This observation leads us to our uniqueness criterion (Theorem 5.4) and also enables us to state a conjecture for the quadratic field $\mathbb{Q}(\sqrt{9c^2 - 4})$ (Conjecture 5.2) that is equivalent to the Markoff conjecture for c: if p, q are coprime integers greater than 1 with $c = pq$, then there is no ambiguous form of discriminant d that represents both $-p^2$ and q^2.

2. Elementary proofs

In this section we present elementary proofs of the Markoff conjecture in the cases when c is a prime power or two times a prime power and when the greatest odd divisor of either $3c+2$ or $3c-2$ is a prime power. The proofs use three simple properties of Markoff numbers, namely, the three integers in every Markoff triple are mutually coprime, all odd Markoff numbers are congruent to 1 modulo 4 and if c is an even Markoff number, then c is congruent to 2 modulo 4 and $\frac{3c-2}{4}$ and $\frac{3c+2}{8}$ are odd integers. These results may be proved in an elementary manner. In Section 4 we state these results and give some alternative proofs. The following lemma is easy to verify.

Lemma 2.1. *Let (a_1, b_1, c) and (a_2, b_2, c) be two Markoff triples. Then*

$$(a_1a_2 - b_1b_2)(a_1b_2 - b_1a_2) = c^2(a_1b_1 - a_2b_2). \tag{2.1}$$

Theorem 2.2. *If c is a Markoff number that is an odd prime power or two times an odd prime power, then c is unique.*

Proof. Let (a_1, b_1, c) and (a_2, b_2, c) be two Markoff triples with $a_i \leq b_i \leq c$ for $i = 1, 2$. Assume that $a_1b_1 - a_2b_2 = 0$; then by Lemma 2.1 either $a_1a_2 = b_1b_2$ or $a_1b_2 = b_1a_2$. Let $a_1a_2 = b_1b_2$. As $\gcd(a_1, b_1) = \gcd(a_2, b_2) = 1$ we have $a_2 = b_1$ and $b_2 = a_1$. Similarly if $a_1b_2 = b_1a_2$ we have $a_2 = a_1$ and $b_2 = b_1$. Hence $a_1b_1 - a_2b_2 \neq 0$.

Let $g > 2$ be an odd prime divisor of c. We will show that g cannot divide both $a_1a_2 - b_1b_2$ and $a_1b_2 - b_1a_2$. Assume on the contrary that $a_1a_2 \equiv b_1b_2 \mod g$ and $a_1b_2 \equiv b_1a_2 \mod g$. On multiplication of the two congruences we obtain $a_1^2a_2b_2 \equiv b_1^2a_2b_2 \mod g$. It follows that $a_1^2 \equiv b_1^2 \mod g$ as $\gcd(a_2b_2, c) = 1$. However as $g|a_1^2 + b_1^2$ we have $g|b_1$ which is not true as $\gcd(c, b_1) = 1$. Therefore $\gcd(a_1a_2 - b_1b_2, a_1b_2 - b_1a_2, c') = 1$, where $c' = c$ when c is odd and $\frac{c}{2}$ when c is even. (Note that as mentioned at the begining of this section if c is even, then $\frac{c}{2}$ is odd). Hence $c = pq$ or $2pq$, depending on whether c is odd or even respectively where we have

$$a_1a_2 - b_1b_2 \equiv 0 \mod p^2 \text{ and } a_1b_2 - b_1a_2 \equiv 0 \mod q^2. \tag{2.2}$$

Now if c is an odd prime power or two times an odd prime power, we conclude that one of p or q say q, is equal to 1. Therefore $p = c$ or $\frac{c}{2}$ depending on whether c is odd or even respectively.

If c is odd we have $a_1a_2 - b_1b_2 \equiv 0 \mod c^2$. As $a_i, b_i \leq c$, it follows that $a_1a_2 - b_1b_2 = 0$ and hence $a_2 = b_1$ and $b_2 = a_1$ (as $\gcd(a_i, b_i) = 1$), which is not possible.

If c is even, then a_i, b_i are odd and as all odd Markoff numbers are congruent to 1 modulo 4 (see begining of this section), we have $a_1a_2 - b_1b_2 \equiv 0 \mod 4$. Also $a_1a_2 - b_1b_2 \equiv 0 \mod \frac{c^2}{4}$ (as $p = \frac{c}{2}$) and as $\frac{c^2}{4}$ is odd ($c \equiv 2 \mod 4$) it follows as in the case above, that $a_1a_2 - b_1b_2 \equiv 0 \mod c^2$ and the proof is complete. □

Theorem 2.3. *Let c be a Markoff number such that the greatest odd divisor of either $3c-2$ or $3c+2$ is a prime power. Then c is unique.*

Proof. Let (a_1, b_1, c) and (a_2, b_2, c) be two Markoff triples. Let $A_i = \frac{a_i+b_i}{2}$ and $B_i = \frac{a_i-b_i}{2}$, for $i = 1, 2$. Then the Markoff equation (1.1) gives

$$(2-3c)A_i^2 + (2+3c)B_i^2 = -c^2. \tag{2.3}$$

Subtracting the two equations for $i = 1, 2$ in (2.3) above we obtain

$$(3c-2)(A_1^2 - A_2^2) = (3c+2)(B_1^2 - B_2^2). \tag{2.4}$$

Suppose that c is odd and $(3c+2)$ is a power of a prime p. Assume that $p|\gcd(2(A_1+A_2), 2(A_1-A_2))$. Then $p|A_1$ and from (2.3) we have $p|c$, which is not possible. Therefore if $3c+2$ is a power of a prime then $3c+2|2(A_1+A_2)$ or $2(A_1-A_2)$. However this is not possible if $a_i \le b_i \le c$, since from (1.1) we have $ab \le c$, hence $a \le \sqrt{c}$ and therefore $3c+2 \le 2(A_1+A_2) \le 2(c-1)+2\sqrt{c}$. The case when $3c-2$ is a power of a prime is dealt with similarly.

Now assume that c is even. Then as mentioned at the start of this section, we have c is not divisible by 4 and $\frac{3c-2}{4}$ and $\frac{3c+2}{8}$ are odd integers. It follows from (2.3) that $2A_i$ is even and hence a_i, b_i are odd. Therefore A_i and B_i are integers and from (2.3) we have A_1, A_2 are odd integers. Since $B_i = A_i - b_i$ the integers B_i are even.

Let $\frac{3c-2}{4}$ be a prime power. From (2.3) we have

$$\frac{3c-2}{4}\frac{A_1^2 - A_2^2}{3c+2} = \frac{B_1^2 - B_2^2}{4},$$

which is not possible if $a_i \le b_i \le c$, as then $|\frac{B_1+B_2}{2}| \le \frac{c}{2}$.

The case when $\frac{3c+2}{8}$ is a prime power is similar. □

3. Binary quadratic forms and ideals

Henceforth $d \equiv 0$ or $1 \mod 4$ will be an integer that is not a square and R will be the unique quadratic order of discriminant d in $K = \mathbb{Q}(\sqrt{d})$.

The reader may refer to [13], [6] or [10] for details on forms, ideals and the correspondence between them.

3.1. Forms. A *primitive binary quadratic form* $f = (a, b, c)$ of discriminant d is a function $f(x, y) = ax^2 + bxy + cy^2$, where a, b, c are integers with $b^2 - 4ac = d$ and $\gcd(a, b, c) = 1$. All forms considered here are primitive binary quadratic forms and henceforth we shall refer to them simply as forms.

Two forms f and f' are said to be *equivalent*, written as $f \sim f'$, if for some $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ we have $f'(x, y) = f(\alpha x + \beta y, \gamma x + \delta y)$. It is easy to see that $\sim$ is an equivalence relation on the set of forms of

discriminant d. The equivalence classes form an abelian group called the *class group* with group law given by composition of forms which follows from the product formula for ideals given in the next section.

The *identity form* is defined as the form $(1, 0, \frac{-d}{4})$ or $(1, 1, \frac{1-d}{4})$ depending on whether d is even or odd, respectively. In the case when $d = 9c^2 - 4$ we define $e = (1, -3c, 1)$, which is equivalent to the identity form. (Note that $e(x + \frac{3c+1}{2}y, y) = (1, 1, \frac{1-d}{4})$.) The *inverse* of $f = (a, b, c)$, denoted by f^{-1}, is given by $(a, -b, c)$.

A form f is said to represent an integer m if there exist coprime integers x and y such that $f(x, y) = m$.

A form (a, b, c) is said to be *ambiguous* if a divides b. It follows then that a divides d. Conversely, if $d = rr'$ with $\gcd(r, r') = 1$, then there is an ambiguous form (r, x, y) with $r|x$. If (a, b, c) is an ambiguous form, we say that it corresponds to the divisor $|a|$ of d. An *ambiguous class* is one that contains an ambiguous form.

The form $-f = (-a, b, -c)$ is the *negative* of the form $f = (a, b, c)$.

Definition 3.1. (Generic values) Let $d \equiv 1 \mod 4$ have t distinct prime divisors given by $r_i, i = 1, 2, \cdots, t$. Let f be a form and Q be the equivalence class containing f. Let m with $\gcd(2d, m) = 1$ be any integer represented by f and let $(\frac{m}{r_i})$ denote the Legendre symbol. Then the t *generic values* associated to Q or f are given by $\theta_i(Q) = \theta_i(f) = (\frac{m}{r_i})$, $i = 1, 2, \cdots, t$. We define $\theta(Q) = \theta(f) = ((\frac{m}{r_1}), (\frac{m}{r_2}), \cdots, (\frac{m}{r_t}))$. The *principal genus* consists of all classes Q (or forms f) with $\theta(Q) = (1, 1, \cdots, 1)$.

It can be shown that the value of θ for a given class is independent of the integer m represented.

3.2. Ideals. For details of the results presented in this section the reader is directed to [6, Section 5.2 and 5.4.2]. A clear presentation of the arithmetic of ideals is also available in [10, Sections 1.2 and 1.3].

A primitive integral ideal I of R can be written in the form

$$I = a\mathbb{Z} + \frac{-b + \sqrt{d}}{2}\mathbb{Z}, \tag{3.1}$$

where a, b are integers such that $a > 0$ is the norm of the ideal and $4a$ divides $b^2 - d$.

If $c = \frac{b^2-d}{4a}$ and $\gcd(a, b, c) = 1$, then the ideal is invertible and the inverse is the ideal $\overline{I} = a\mathbb{Z} + \frac{b+\sqrt{d}}{2}\mathbb{Z}$. Note that $(a, b, c) = ax^2 + bxy + cy^2$ is a form of discriminant d. Indeed the invertible ideals are the ideals that correspond to forms.

Let F be the set of forms modulo the action of the group $\left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, m \in \mathbb{Z} \right\}$, where the forms (a, b, c) and $(a, b + 2am, c')$ are identified. Let $\mathbb{I}$ be the set

of fractional ideals modulo $\mathbb{Q}^*$. Then a map ψ from F to $\mathbb{I}$ is defined as

$$\psi(a,b,c) = \begin{cases} a\mathbb{Z} + \frac{-b+\sqrt{d}}{2}\mathbb{Z}, & \text{if } a > 0 \\ (a\mathbb{Z} + \frac{-b+\sqrt{d}}{2}\mathbb{Z})\sqrt{d}, & \text{if } a < 0. \end{cases}$$

The map ψ induces a bijection between the class group of forms and the narrow class group of R, where two ideals I and J are strictly equivalent, written as $I \approx J$, if there are algebraic integers α and β such that $\alpha I = \beta J$ and where the norms of α and β are of the same sign. To establish the bijection induced by ψ it is necessary to consider for each ideal an ordered basis $w_1\mathbb{Z} + w_2\mathbb{Z}$ that satisfies $\overline{w_2}w_1 - \overline{w_1}w_2 > 0$, where $\overline{w_1}$ represents the conjugate of w_1. Two ideals are said to be equivalent, written as $I \sim J$, if the ideal equality given above holds without the norm condition.

Observe that if $a > 0$ and $\psi(a,b,c) = I$, then $\psi(-a,b,-c) = I\sqrt{d}$.

In the following definition we present the formula for the product of ideals which leads to composition of forms.

Let $I_k = a_k\mathbb{Z} + \frac{-b_k+\sqrt{d}}{2}\mathbb{Z}$, $k = 1, 2$, be two primitive ideals. Let $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ be the corresponding binary quadratic forms of discriminant d.

Definition 3.2. Let $g = gcd(a_1, a_2, (b_1+b_2)/2)$ and let v_1, v_2, w be integers such that

$$v_1a_1 + v_2a_2 + w(b_1 + b_2)/2 = g.$$

If we define a_3 and b_3 as

$$a_3 = \frac{a_1a_2}{g^2},$$

$$b_3 = b_2 + 2\,\frac{a_2}{g}\,\left(\frac{b_1 - b_2}{2}\;v_2 - c_2w\right),$$

then $I_1 \cdot I_2$ is the ideal $a_3\mathbb{Z} + \frac{-b_3+\sqrt{d}}{2}\mathbb{Z}$. Further the composition of the forms (a_1, b_1, c_1) and (a_2, b_2, c_2) is the form (a_3, b_3, c_3), where c_3 is computed using the discriminant equation.

Note that this gives the multiplication in the class group.

3.3. Lemmas on binary quadratic forms.

Lemma 3.3. *Let f be a form of positive discriminant $d \equiv 1 \mod 4$.*

1. *$f \sim f^{-1}$ if and only if f is equivalent to an ambiguous form.*
2. *Let d be square-free. Then the number of ambiguous classes is equal to 2^{t-1}, where t is the number of distinct prime divisors of d.*

Proof. If f is an ambiguous form then it follows immediately from Definition 3.2 that $f \sim f^{-1}$.

For the converse, let $\psi(f) = I$. Then $I \approx \overline{I}$. It can be shown (as for example in [1, Lemma 2.3]) that there exists a primitive ideal J such that

$N(J) \mid d$ and $I \sim J$. It follows that either $I \approx J$ or $I \approx \sqrt{d}J$ [7, page 197]. In either case f is equivalent to an ambiguous form as the forms corresponding to the ideals J and $\sqrt{d}J$ are ambiguous.

For the details of part 2 the reader may refer to [13, page 143]. □

Lemma 3.4. *Let f be a form that represents integers m and m' with $\gcd(mm', 2d) = 1$. Then for each odd prime divisor r of d we have $(\frac{m}{r}) = (\frac{m'}{r})$.*

Proof. See [13, page 139]. □

4. Properties of Markoff numbers

The following lemma is an easy consequence of Markoff's early work [9] where he showed that all Markoff triples can be generated from $(1, 1, 1)$. The reader may refer to [5, page 28] for a proof.

Lemma 4.1. *If (a, b, c) is a Markoff triple, then $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$.*

In the next lemma we present some properties of Markoff numbers. Part 1 of the lemma follows from a classical result of numbers representable as a sum of two coprime squares and hence is well known. A short proof of part 2 is given in [15] and an elementary proof for the last part can be found in [17]; here we present alternative proofs for these two results.

Lemma 4.2. *Let c be a Markoff number and $d = 9c^2 - 4$.*

(1) *Every odd prime divisor of c is congruent to 1 modulo 4. If c is even then c is not divisible by 4.*
(2) *Every odd prime divisor of d is congruent to 1 modulo 4.*
(3) *If c is even then $\frac{3c-2}{4}$ and $\frac{3c+2}{8}$ are odd integers.*

Proof. Rewriting (1.1) as $c(3ab - c) = a^2 + b^2$, we see that c divides a sum of two coprime squares and hence part 1 of the lemma follows.

As c is a Markoff number, the form $e = (1, -3c, 1)$ represents $-c^2$ (as $e(a, b) = -c^2$). Moreover it also represents 1. Therefore by Lemma 3.4, for every odd prime $r|d$ we have $(\frac{-c^2}{r}) = (\frac{1}{r})$, that is $(\frac{-1}{r}) = 1$. Hence $r \equiv 1 \mod 4$ and part 2 of the lemma follows.

Let c be even. It is clear from part 1 of the lemma that $\frac{3c-2}{4}$ is odd.

As $e(a, b) = -c^2$ and equivalent forms represent the same integers, the identity form $(1, 0, -\frac{9c^2-4}{4})$ represents $-c^2$. Hence there exist coprime integers x, y such that $x^2 - \frac{9c^2-4}{4}y^2 = -c^2$. As c is even, x is even and thus y is odd. Looking at the above equation modulo 4 and by part 1, we deduce that $\frac{9c^2-4}{32}$ is an odd integer and this concludes the proof of the lemma. □

The following theorem is proved in [1] and [3] in the case when c is odd.

Theorem 4.3. *A positive integer c is a Markoff number if and only if there exists a pair of primitive principal ideals $\{(\beta), (\overline{\beta})\}$ in R, where the norm of β is $-c^2$. Furthermore c is unique if and only if there exists exactly one pair of such ideals.*

Proof. Firstly recall that ψ is a bijection from binary quadratic forms to invertible integral ideals, where all forms considered are primitive. If (a, b, c) is a Markoff triple, it follows from (1.1) that $e(a, b) = -c^2$. As $\gcd(a, b) = 1$ there exists $A = \begin{pmatrix} a & \beta \\ b & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ and we have $e(ax + \beta y, bx + \delta y) = (-c^2, B, l) = f$. It follows that $\psi(f)$ is a primitive principal ideal generated by an element of norm $-c^2$. Conversely if I is a primitive principal ideal generated by an element of norm $-c^2$ then $\psi^{-1}(I) = (-c^2, B, l)$ is a form that is equivalent to e. Hence there exists $A = \begin{pmatrix} a & \beta \\ b & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $e(ax + \beta y, bx + \delta y) = (-c^2, B, l)$. It follows that $e(a, b) = -c^2$ and hence we obtain a Markoff triple (a, b, c). Now let (a_1, b_1, c) and (a_2, b_2, c) be two Markoff triples that correspond as above to forms $f_1 = (-c^2, b_1, l_1)$ and $f_2 = (-c^2, b_2, l_2)$. It can be shown using automorphisms of the form e that if the two triples satisfy $a_i \leq b_i \leq c$, then $b_1 \not\equiv \pm b_2 \mod 2c^2$. Therefore $\psi(f_1) \neq \psi(f_2)$ or $\psi(f_2^{-1})$ and hence to each Markoff triple (a, b, c) with $a \leq b \leq c$ there corresponds a pair of primitive principal ideals as stated in the theorem and the result follows. □

The following is also [1, Lemma 2.5] where the result is expressed in terms of ideals.

Lemma 4.4. *Let c be an odd Markoff number and $d = 9c^2 - 4$. Let f be an ambiguous form corresponding to a divisor r of $3c - 2$. If f represents an integer n with $|n| < \frac{\sqrt{d}}{2}$, then $|n| = r$ or $\frac{3c-2}{r}$.*

Proof. Let $3c - 2 = rr'$ and $f = (r, 3c - 2, r')$. If f represents n, then there is a form $g = (n, l, k)$ that is equivalent to f. If $\psi(f) = J$ and $\psi(|n|, l, k\frac{n}{|n|}) = I$ then $I \sim J$. The lemma follows on applying [1, Lemma 2.5], which states that if $I \sim J$ with $N(I) < \frac{\sqrt{d}}{2}$ and such that $N(J) = r$ divides $3c - 2$, then $N(I) = r$ or $\frac{3c-2}{r}$. □

5. The uniqueness criterion

Let $d = 9c^2 - 4$. All the forms considered in this section are of discriminant d and all ideals are in R, the unique quadratic order of discriminant d in $\mathbb{Q}(\sqrt{d})$. Note that for $c \neq 1$ the fundamental unit of the order R has positive norm and hence an ideal generated by an element of negative norm is not strictly equivalent to an ideal generated by an element of positive norm.

Theorem 5.1. *Let c be a Markoff number that is not unique. Then there exist coprime integers p, q greater than 1 with $c = pq$ such that the following equivalent statements hold.*

(1) *There exist primitive ideals I and J of norm p^2 and q^2 respectively, such that $J \approx \overline{J} \approx I\sqrt{d}$.*
(2) *There exists a form f with $f \sim f^{-1}$ such that f represents both $-p^2$ and q^2.*

Proof. We will prove the statement for ideals first and then translate it via the map ψ to statement 2 for forms.

If c is not unique then by Theorem 4.3 there exist two distinct pairs of primitive principal ideals generated by elements of norm $-c^2$. Let us denote these ideals as

$$P_1 = c^2\mathbb{Z} + \frac{-b_1 + \sqrt{d}}{2}\mathbb{Z}, \quad P_2 = c^2\mathbb{Z} + \frac{-b_2 + \sqrt{d}}{2}\mathbb{Z}.$$

Note that $R \approx P_1\sqrt{d} \approx P_2\sqrt{d}$. By the ideal condition $4c^2 | d - b_i^2$ and therefore $b_1^2 \equiv b_2^2 \mod 2c^2$. Moreover $b_1 \not\equiv \pm b_2 \mod 2c^2$. Therefore as $\gcd(c, b_i) = 1$, there exist coprime integers p, q greater than 1 with $c = pq$ such that

$$b_1 + b_2 \equiv 0 \mod 2p^2, b_1 - b_2 \equiv 0 \mod 2q^2. \tag{5.1}$$

Let $I = p^2\mathbb{Z} + \frac{-b_1+\sqrt{d}}{2}\mathbb{Z}$ and $J = q^2\mathbb{Z} + \frac{-b_1+\sqrt{d}}{2}\mathbb{Z}$. By Definition 3.2 and (5.1), as p, q are coprime, we have $IJ \approx P_1$ and $\overline{I}J = P_2$ and hence

$$R \approx P_1\sqrt{d} \approx IJ\sqrt{d} \approx P_2\sqrt{d} \approx \overline{I}J\sqrt{d}.$$

It follows that

$$J \approx \overline{J} \approx I\sqrt{d}$$

and statement 1 follows.

To prove statement 2, let $c_i = \frac{b_i^2 - d}{4c^2}$ and let $f = (-p^2, b_1, q^2c_1)$ and $g = (q^2, b_1, p^2c_1)$. Then $\psi(f) = I\sqrt{d}$ and $\psi(g) = J$. It follows from the ideal equivalences in part 1 that $f \sim f^{-1} \sim g$ and statement 2 follows.

To show that the second statement implies the first one, we simply observe that if c is not unique, then there exist two inequivalent forms $(-c^2, b_1, w_1)$ and $(-c^2, b_2, w_2)$ that are equivalent to the identity form and that correspond via the map ψ mentioned in Section 3.2 to the ideals P_1 and P_2. □

Let c be an odd integer that is not a prime power. It follows from Theorem 4.3 that c is a Markoff number if and only if there is a pair of primitive principal ideals generated by elements of norm $-c^2$. Using the notation in the proof above, we have that c is a Markoff number if and only if there are ideals P_1, I and J such that $IJ \approx P_1$ and $J \approx I\sqrt{d}$. It follows

on using the equivalence given by ψ, as in the last paragraph of the proof, that c is a Markoff number if and only if there is a form f that represents $-p^2$ and q^2, where p, q are coprime integers greater than 1 such that $c = pq$.

The above theorem leads us to make the following conjecture about quadratic fields.

Conjecture 5.2. Let p, q be coprime integers greater than 1 with $c = pq$. Then the following equivalent statements hold.

(1) There does not exist a binary quadratic form f that represents both $-p^2$ and q^2 and such that $f \sim f^{-1}$.
(2) There do not exist primitive ideals I and J of norms p^2 and q^2 respectively such that $J \approx \overline{J} \approx I\sqrt{d}$.

Theorem 5.3. *The Markoff conjecture for a Markoff number c that is not a prime power is equivalent to Conjecture 5.2 for the quadratic field $\mathbb{Q}(\sqrt{9c^2-4})$.*

Proof. As in Theorem 5.1, we will prove the result for ideals and the result for forms will follow on using the correspondence given by the map ψ.

From Theorem 5.1, if the conjecture for the quadratic field is true then the Markoff conjecture is true. To prove the converse let $I = p^2\mathbb{Z} + \frac{-b_1+\sqrt{d}}{2}\mathbb{Z}$ and $J = q^2\mathbb{Z} + \frac{-b_1+\sqrt{d}}{2}\mathbb{Z}$ be ideals as given in statement 2 of Conjecture 5.2. Then

$$R \approx J^2 \approx \sqrt{d}I \cdot J \approx \sqrt{d}I \cdot \overline{J}.$$

Let $P_1 = I \cdot J$ and $P_2 = I \cdot \overline{J}$. Then from Definition 3.2 for the product of ideals we obtain

$$P_i = \left(c^2\mathbb{Z} + \frac{-m_i + \sqrt{d}}{2}\mathbb{Z}\right), \quad i = 1, 2,$$

for some integers m_i where it can be verified that $m_1 \not\equiv \pm m_2 \mod 2c^2$. It follows from Theorem 4.3 that c is a Markoff number that is not unique. □

In the following theorem we present a criterion for uniqueness that follows immediately from Theorem 5.1 and Lemma 4.4.

Theorem 5.4. (**Uniqueness Criterion**) Let c be an odd Markoff number. Assume that every ambiguous form that belongs to a class in the principal genus corresponds to a divisor of $3c - 2$. Then c is unique.

Proof. If c is not unique, then by Theorem 5.1 there is a form f that represents both $-p^2$ and q^2 such that $f \sim f^{-1}$. We assume without loss of generality that $p < q$. By Lemma 3.3, f is equivalent to an ambiguous form g. It follows that g represents $-p^2$. Morever g is in the principal genus as it represents a square q^2. By assumption g corresponds to a divisor of $3c - 2$

and hence by Lemma 4.4 does not represent $-p^2$ as $p^2 < \frac{\sqrt{d}}{2}$. Therefore c is unique. □

6. Applications of the uniqueness criterion

The criterion given in Theorem 5.4 is made explicit in the following theorem.

Theorem 6.1. *Let c be an odd Markoff number. Assume that for every $0 < d_1 < \sqrt{d}$ with $d = d_1 d_2$, $d_1 \nmid 3c-2$ and $\gcd(d_1, d_2) = 1$, one of the following is true.*

(1) *There exists a prime $r|d_1$ such that $(\frac{d_2}{r}) = -1$.*
(2) *There exists a prime $r|d_2$ such that $(\frac{d_1}{r}) = -1$.*

Then c is unique.

Proof. Let $f = (d_1, d_1 r_1, -c_1)$ be the ambiguous form corresponding to the divisor d_1 of d. Let $m = f(1, d_2)$. Then $\gcd(m, 2d) = 1$. If r is a prime dividing d_1, then $(\frac{m}{r}) = (\frac{c_1}{r}) = (\frac{d_2}{r})$. The last equality follows from the discriminant equation $d_1 r_1^2 + 4c_1 = d_2$. If $r|d_2$, then $(\frac{m}{r}) = (\frac{d_1}{r})$. It follows that if any one of the above Legendre symbols is equal to -1, then f belongs to a class that is not in the principal genus and hence c is unique by Theorem 5.4. □

Example. Using Theorem 6.1 it can be shown that the Markoff conjecture is true for $c = 7561$ as follows. There are 12 divisors of d that are less than $\sqrt{d}$ and that do not divide $3c-2$. We give below a list of these divisors d_1 and the corresponding r in each case that satisfies one of the conditions in the theorem.

d_1	5	13	349	$5 \cdot 13$	$5 \cdot 349$	$13 \cdot 349$	$5 \cdot 37$	$5 \cdot 613$	$13 \cdot 37$
r	5	5	349	13	349	13	37	613	37

d_1	$13 \cdot 613$	$37 \cdot 349$	$5 \cdot 13 \cdot 37$
r	613	349	5

.

In the following we consider the case when $3c-2$ and $3c+2$ are both products of two odd primes.

Lemma 6.2. *Let c be an odd Markoff number. Let $3c-2 = r_1 r_2$ and $3c+2 = r_3 r_4$. Assume that the integers r_i are pairwise coprime. Then the Jacobi symbols $(\frac{r_i}{r_j})$ are as given in the following table, where $r, s, t \in \{-1, 1\}$.*

$(\frac{r_i}{r_j})$	r_1	r_2	r_3	r_4
r_1	0	r	s	s
r_2	r	0	s	s
r_3	s	s	0	t
r_4	s	s	t	0

Proof. Observe that by Lemma 4.2 all prime divisors of d are congruent to 1 mod 4 and hence $(\frac{r_i}{r_j}) = (\frac{r_j}{r_i})$. Also $(\frac{-1}{r}) = 1$ for any $r|d$. Let $f = (r_1, r_1r_2, -r_2)$. Let $m = f(1, r_3r_4)$ and $m' = f(r_3r_4, 1)$. Then $\gcd(2d, mm') = 1$. By Lemma 3.4 we have $(\frac{m}{r_3}) = (\frac{m'}{r_3})$. Note that $(\frac{m}{r_3}) = (\frac{r_1}{r_3})$ and $(\frac{m'}{r_3}) = (\frac{r_2}{r_3})$. Therefore $(\frac{r_1}{r_3}) = (\frac{r_2}{r_3})$. Also since $(\frac{3c-2}{3c+2}) = 1$, we have $(\frac{r_1}{r_3}) = (\frac{r_2}{r_4})$ and $(\frac{r_2}{r_3}) = (\frac{r_1}{r_4})$. Hence $(\frac{r_1}{r_3}) = (\frac{r_1}{r_4}) = (\frac{r_2}{r_3}) = (\frac{r_2}{r_4})$. □

Lemma 6.3. *Let c be an odd Markoff number. Let $3c - 2 = r_1r_2$ and $3c + 2 = r_3r_4$ where the r_i are distinct primes. Then the generic values of the ambiguous forms corresponding to the divisors r_1, r_3 and r_1r_3 are respectively, $(r, r, s, s), (s, s, t, t)$ and (rs, rs, st, st).*

Proof. Let $f = (r_1, r_1r_2, -r_2)$. If $m = f(1, r_3r_4)$ then $\gcd(2d, m) = 1$. For the generic values of f we have $(\frac{m}{r_1}) = r, (\frac{m}{r_2}) = r, (\frac{m}{r_3}) = s$ and $(\frac{m}{r_4}) = s$. Hence $\theta(f) = (r, r, s, s)$.

Let $g = (r_3, r_3\phi, -\psi)$. As above if $m = g(1, r_1r_2r_4)$ then $\gcd(2d, m) = 1$ and using the discriminant equation $r_3\phi^2 + 4\psi = r_1r_2r_4$, we have $(\frac{m}{r_1}) = s, (\frac{m}{r_2}) = s, (\frac{m}{r_3}) = t$ and $(\frac{m}{r_4}) = t$. Thus $\theta(g) = (s, s, t, t)$.

For the generic values of the form $h = (r_1r_3, r_1r_3\phi, -\psi)$, we consider $m = h(1, r_2r_4)$ and using the discriminant equation $r_1r_3\phi^2 + 4\psi = r_2r_4$, we obtain $\theta(h) = (rs, rs, st, st)$. □

Theorem 6.4. *Let c be an odd Markoff number. Let $3c - 2 = r_1r_2$ and $3c + 2 = r_3r_4$ where the r_i are distinct primes. Then c is unique if one of the following conditions is satisfied,*

(1) $(\frac{r_1}{r_3}) \cdot (\frac{r_3}{r_4}) = -1$.
(2) $(\frac{r_1}{r_3}) = (\frac{r_3}{r_4}) = -1$ *and* $(\frac{r_1}{r_2}) = 1$.

Proof. Firstly we observe that there are 8 ambiguous classes (Lemma 3.3), namely, the classes containing ambiguous forms that correspond to the divisors $1, r_1, r_3$, and r_1r_3 and their negatives. If c is not unique, then by Theorem 5.1 there is an ambiguous form g that represents $-p^2$ and is in the principal genus. It is easily verified using Lemma 6.3 that if any one of the conditions given in the theorem is satisfied, then the ambiguous forms corresponding to r_3 and r_1r_3 belong to classes that are not in the principal genus. Therefore g corresponds to the divisor 1 or r_1. However by Lemma

4.4 as $p^2 < \frac{\sqrt{d}}{2}$, an ambiguous form that corresponds to a divisor of $3c-2$ does not represent $-p^2$. Therefore we conclude that c is unique. □

In the following example we apply Theorem 6.4 to a Markoff number and demonstrate that some existing uniqueness criteria do not apply to this number.

Example. Consider the Markoff number $c = 9077$. We have $r_1 = 73, r_2 = 373, r_3 = 113, r_4 = 241$. Also $(\frac{r_1}{r_3}) = -1$ and $(\frac{r_3}{r_4}) = 1$. Hence condition 1 of Theorem 6.4 is satisfied and so the Markoff conjecture is true for 9077. To take an instance of an existing criterion, we consider one of the criteria presented by Button [4], which is that if all ambiguous cycles are of length 2 or 4, then c is unique. Note that in this example, for the divisor $73 \cdot 241$ of d, the length of the associated ambiguous cycle is 12 and hence this condition does not apply. It is reasonable to assume that there are arbitrarily large Markoff numbers of the kind in Theorem 6.4 and hence we have enlargened the set of Markoff numbers for which the Markoff conjecture can be shown to be true.

Acknowledgements

Many thanks to Jorge Jiménez for numerous vivacious discussions on the topic. I would also like to thank R. Balasubramanian, director of Institute of Mathematical Sciences, where this work was completed, for his invitation to the institute and for his enthusiasm for the topic. Thanks also to Pablo Arés for a greatly improved presentation of the paper.

References

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

[2] E. Bombieri, *Continued fractions and the Markoff tree*. Expo. Math. **25** (2007), no. 3, 187–213

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

[4] J. O. Button, *Markoff numbers, principal ideals and continued fraction expansions*. Journal of Number Theory, **87** (2001), 77–95.

[5] J. W. S. Cassels, *An introduction to Diophantine approximation*. Cambridge University Press, 1957.

[6] H. Cohen, *A course in computational algebraic number theory*. Springer-Verlag, 1993.

[7] H. Cohn, *Advanced Number Theory*. Dover Publications, 1980.

[8] M. L. Lang, S. P. Tan, *A simple proof of the Markoff conjecture for prime powers*. Geom. Dedicata **129** (2007), 15–22.

[9] A. A. Markoff, *Sur les formes quadratiques binaires indéfinies I*. Math. Ann. **15** (1879), 381–409.

[10] R. A. Mollin, *Quadratics*. CRC press, Boca Raton, 1996.

[11] S. Perrine, *Sur une généralisation de la théorie de Markoff*. Journal of Number Theory **37** (1991), 211–230.

[12] S. Perrine, *Un arbre de constantes d'approximation analogue à celui de l'équation diophantienne de Markoff*. Journal de Théorie des Nombres de Bordeaux, **10**, no. 2, (1998), 321–353.

[13] P. Ribenboim, *My Numbers, My Friends, Popular Lectures on Number Theory*. Springer-Verlag, 2000.
[14] P. Schmutz, *Systoles of arithmetic surfaces and the Markoff spectrum*. Math. Ann. **305** (1996), no. 1, 191–203.
[15] A. Srinivasan, *A note on the Markoff conjecture*. Biblioteca de la Revista Matemática Iberoamericana, Proceedings of the "Segundas Jornadas de Teoría de Números" (Madrid, 2007), pp. 253–260.
[16] D. Zagier, *On the number of Markoff numbers below a given bound*. Math. Comp. **39** (1982), 709–723
[17] Y. Zhang, *Conguence and uniqueness of certain Markoff numbers*. Acta Arith. **128** (2007), no. 3, 295–301.
[18] Y. Zhang, *An elementary proof of uniqueness of Markoff numbers which are prime powers*. Preprint, arXiv:math.NT/0606283 (version 2).

Anitha Srinivasan
Siddhartha College (Mumbai University)
Mumbai, INDIA
E-mail: rsrinivasan.anitha@gmail.com