A SIMPLE PROOF OF THE MARKOFF CONJECTURE FOR PRIME POWERS

MONG LUNG LANG, AND SER PEOW TAN

Abstract. We give a simple and independent proof of the result of Jack Button and Paul Schmutz that the Markoff conjecture on the uniqueness of the Markoff triples (a, b, c) where $a \leq b \leq c$ holds whenever c is a prime power.

1. Introduction

The Markoff conjecture (first conjectured by G. Frobenius in 1913) states that the set of triples (a, b, c) of positive integer solutions of the Markoff equation

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

is uniquely determined by c, if we order the triple so that $a \leq b \leq c$. The triples (a, b, c) are called *Markoff triples* and the values *Markoff numbers.*

Theorem 1.1. (*J.Button, P. Schmutz*) *The Markoff conjecture is true when c is a prime power.*

This was proven independently by Schmutz [8] and Button [3]. We give here a very short and simple proof of their result which depends only on some elementary hyperbolic geometry and congruences. The main novelty in our method is that it combines the geometric and arithmetic information in a hitherto unexplored way.

The interest in the conjecture lies in the fact that it ties in several apparently unrelated fields including diophantine approximations, quadratic forms and hyperbolic geometry, the reader is referred to [6] for background material on the number theoretic aspects. The relation with hyperbolic geometry and the trace field of the modular torus, in particular, the relation between (1) and the Fricke trace identities appears to be first discovered by H. Cohn in [5], see [9] for an excellent survey of the subject.

Acknowledgements. We obtained our proof soon after learning of Button's result in his Warwick PhD thesis. We had not written it out then as there was no essentially new results, and it was clear that the method alone would not resolve the Markoff conjecture in full. Nonetheless, there seemed to be some interest in the proof, we thank in particular Caroline Series and Brian Bowditch for their interest and encouragement.

2. Some basic facts

We state here some basic facts which seem to be well-known to the experts in the field, and also some useful propositions.

2.1. **Markoff triples and the Markoff tree.** The Markoff triples (a, b, c) can be generated from the basic triple $(1, 1, 1)$ as values attached to the vertices of an infinite binary tree via the operations

$$(a, b, c) \mapsto (b, c, 3bc - a), \quad (a, b, c) \mapsto (a, 3ac - b, c), \quad (a, b, c) \mapsto (a, b, 3ac - b).$$

(It is perhaps visually more pleasing and systematic to think of the Markoff numbers as values attached to the complementary regions of the tree, and the triples as arising from the three regions adjacent to a vertex of the tree, see for example [2]). There is a D_6 symmetry for this tree of values and the conjecture is equivalent to saying that the values are unique up to the action of D_6.

2.2. **The modular torus and simple closed geodesics.** The modular torus is defined to be the cusped hyperbolic torus $\mathbb{T} = \mathbb{H}/G$, where $G = \langle A, B\rangle < \mathrm{SL}(2, \mathbb{Z}) = \Gamma$,

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \in \Gamma.$$

Note that $G = [\,\Gamma, \Gamma]$, see for example [4]. Also, it is common to regard A, B as matrices in $\mathrm{PSL}(2, \mathbb{Z})$, we have chosen a lift to $\mathrm{SL}(2, \mathbb{Z})$ here for which the traces of all simple closed geodesics are positive. The isometry group of $\mathbb{T}$ is also isomorphic to D_6, and there is a direct correspondence between the Markoff numbers and the traces/lengths of simple closed geodesics on $\mathbb{T}$, indeed, the traces are precisely 3 times the Markoff numbers. Similarly, there is a correspondence between the Markoff triples and the traces/lengths of triples of simple closed geodesics on $\mathbb{T}$ with pair-wise geometric intersection number one (see [5], [9] or [2]). The Markoff conjecture is equivalent to saying that the traces/lengths of the simple closed geodesics on $\mathbb{T}$ are distinct, up to the action of the isometry group D_6 on $\mathbb{T}$.

2.3. **Markoff Matrices.** A matrix $M \in G$ is *primitive* if it corresponds to a primitive curve on $\mathbb{T}$, that is, $M \neq N^n$ for some $N \in G$, $n \neq \pm 1$. A primitive matrix $M \in G$ is called a *Markoff matrix* if (i) it corresponds to a simple closed geodesic γ on $\mathbb{T}$; and (ii) its fixed axis corresponds to a lift of γ with maximum height in $\mathbb{H}^2$. Note that if M is a markoff matrix, then so is M^{-1}.

Let $T_\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, and use T for T_1. Then $[A, B^{-1}] = AB^{-1}A^{-1}B = -T_6$. We have the following which again is a reinterpretation of well-known results on the simple closed geodesics on $\mathbb{T}$.

Proposition 2.1. *If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a Markoff matrix, then $|c|$ is a Markoff number and $a + d = 3|c|$. Conversely, for any Markoff number c, there is a Markoff matrix M with $\mathrm{tr}\, M = 3c$ and the $(2, 1)$ entry of M equal to c. Furthermore, two Markoff matrices M and N correspond to the same simple closed geodesic in $\mathbb{T}$ if and only if $M^{\pm 1} = T^{3n} N T^{-3n}$ for some $n \in \mathbb{Z}$.*

Let M' be obtained from M by interchanging the diagonal entries. Taking into consideration the D_6 symmetry of $\mathbb{T}$, we define an equivalence relation $\sim$ on the set of Markoff matrices by $M \sim N$ if and only if $N^{\pm 1} = T^n M T^{-n}$, or $N^{\pm 1} = T^n M' T^{-n}$ for some $n \in \mathbb{Z}$. Since the D_6 symmetry of $\mathbb{T}$ is generated by conjugation by reflection on the hyperbolic line $(0, \infty)$ and conjugation by T, two Markoff matrices are equivalent if and only if they either correspond to the same simple closed geodesic, or to two simple closed geodesics on $\mathbb{T}$ equivalent under the

action of D_6. The Markoff conjecture is hence equivalent to the statement that the equivalence classes of Markoff matrices are uniquely determined by the traces, or alternatively, $|c|$, where c is the $(2,1)$ entry. This is the statement we will prove, in the case $|c| = p^n$, where p is prime, in the next section. We first prove some simple technical propositions on Markoff matrices.

For a Markoff matrix M, and each $k \in \mathbb{Z}$, define

$$M_k = \begin{pmatrix} 1 & k/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -k/c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+k & b+k(d-a-k)/c \\ c & d-k \end{pmatrix}.$$

It is clear that $M_k \in \mathrm{SL}(2,\mathbb{Z})$ if and only if $k(d-a-k)$ is a multiple of c.

Proposition 2.2. *Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a Markoff matrix with $c > 0$. Then c is not a multiple of 4 and all the odd prime divisors of c are of the form $4m+1$ for some $m \in \mathbb{N}$.*

Proof. Since $1 = ad - bc = 3cd - d^2 - bc$, we have $d^2 \equiv -1 \pmod{c}$. This implies that

$$X^2 \equiv -1 \,(\bmod\, c)$$

is solvable. It follows that c is not a multiple of 4 and possesses no prime divisor p such that $p \equiv 3 \pmod 4$.

□

Proposition 2.3. *Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a Markoff matrix and let $k \in \mathbb{Z}$. Then $\gcd(c, k, d-a-k) = 1$ or 2. In particular, if $M_k \in \mathrm{SL}(2,\mathbb{Z})$, then any exact divisor p^m of c (p is an odd prime) is relatively prime to either k or $d-a-k$.*

Proof. Suppose $\gcd(c, k, d-a-k) \neq 1$. Let x be a divisor of $(c, k, d-a-k)$. It follows that x is a divisor of $d-a$. Since $a+d = 3c$ and x divides c, x is a divisor of $a+d$. Consequently, x is a divisor of $2a = (a-d)+(a+d)$. Since $x|c$, $x|2a$ and $(a,c) = 1$, we conclude that $x = 2$. □

3. Proof of Theorem

Theorem 1.1 is now equivalent to the following:

Lemma 3.1. *Suppose that M and N are two Markoff matrices with $\operatorname{tr} M = \operatorname{tr} N = 3p^n$ where p is prime. Then $M \sim N$.*

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $N = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Taking inverses if necessary, we may assume that $c = c' > 0$, and so $a+d = a'+d' = 3c$. Hence $a' = a+k, d' = d-k$ for some $k \in \mathbb{Z}$. The key observation here is that since M and N have the same traces and their fixed axes have the same height, M and N are conjugate by a parabolic transformation fixing ∞. A simple computation gives

$$N = M_k = T_{k/c} \cdot M \cdot T_{k/c}^{-1} = \begin{pmatrix} a+k & b+k(d-a-k)/c \\ c & d-k \end{pmatrix}.$$

Since $N \in \mathrm{SL}(2,\mathbb{Z})$, $k(d-a-k)$ is a multiple of c. By proposition 2.2, we may assume that p is a odd prime, and by proposition 2.3, $c = p^n$ divides k or $(d-a-k)$.

In the first case, $N = T^l M T^{-l}$ for some $l \in \mathbb{Z}$, in the second case, $N = T^l M' T^{-l}$ for some $l \in \mathbb{Z}$, hence $N \sim M$.

□

4. Further remarks

4.1. **Determining Markoff matrices.** We saw that for a Markoff matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $a + d = 3|c|$. Nonetheless this is not a sufficient condition, if we denote the conjugacy class of M in $\mathrm{SL}(2, \mathbb{Z})$ by $cl(M)$, and let $M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be the elements of $cl(M)$, then it follows from some elementary hyperbolic geometry that

$$\min_{M' \in cl(M)} |c'| = |c|.$$

This extra information may allow us to obtain the Markoff conjecture for more general c using our methods, namely, even if $M_k \in \mathrm{SL}(2, \mathbb{Z})$, it may not be in G, or may not satisfy the condition above, hence, may not be a Markoff matrix.

4.2. **Representatives of the equivalence classes of Markoff matrices.** Representatives for the equivalence classes of the Markoff matrices can be enumerated starting from A and B via the Farey sequence in the following way: Associate the rational number $0/1$ to the matrix A and the number $1/1$ to the matrix B. So using W to denote the matrix corresponding to a word in A and B we can write $W_0 = A$, $W_1 = B$. Define $W_{1/2} = AB$. More generally if p/q and r/s are Farey neighbours with $0 \leq p/q \leq r/s < 1$ then we define

$$W_{\frac{p+q}{r+s}} = W_{p/q} \cdot W_{r/s}$$

In other words, the word W in A and B associated to the rational m/n is obtained by concatenating the words associated to the previous two Farey numbers, the order of the concatenation being determined by the ordering of the fractions. The representatives for the equivalence classes of Markoff matrices can be taken to be the matrices M_q where $q \in \mathbb{Q} \cap [0, 1/2]$. Details are left to the reader.

4.3. **Relation to the gaps of McShane's and his identity.** There is an interesting relation between our method and McShane's identity [7]. Each Markoff matrix (up to taking inverse and conjugation by T) gives rise to an open interval/gap in $\mathbb{R}/\mathbb{Z}$ centered at a/c, and of width $(3 - \frac{\sqrt{9c^2-4}}{c})$, (where we assume $c > 0$). These gaps are all disjoint, their complement is a Cantor set of measure 0, the fact that the sum is 1 is a special case of McShane's identity (which works for all cusped hyperbolic tori). It should be possible to exploit the disjointedness of these gaps to provide stronger evidence for the Markoff conjecture. The idea is that a shift by k/c may result in a matrix M_k in $\mathrm{SL}(2, \mathbb{Z})$ but the resulting gap may not be disjoint from the other gaps already obtained.

4.4. **Other results.** Our methods easily extend to give uniqueness for the case where $c = 2p^n$, and, using the conditions of §4.1 and some slightly tedious calculations, the case $c = 5p^n$. Baragar [1] has also proven the Markoff conjecture for certain other classes of Markoff numbers, his methods however are different from ours, and our method does not apply to the classes he considers.

References

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

[2] Bowditch, Brian. *A proof of McShane's identity via Markoff triples*, Bull. London Math. Soc. **28** (1996), no. 1, 73–78.

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

[4] Lang, Mong-Lung; Lim, Chong-Hai; Tan, Ser Peow. *Subgroups of the Hecke groups with small index,* Linear and Multilinear Algebra **35** (1993), no. 1, 75–77.

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

[6] Cusick, Thomas W.; Flahive, Mary E. *The Markoff and Lagrange spectra*, Mathematical Surveys and Monographs, 30. American Mathematical Society, Providence, RI, 1989. x+97 pp. ISBN: 0-8218-1531-8

[7] McShane, Greg. *A remarkable identity for lengths of curves*, Ph.D. Thesis, University of Warwick, 1991.

[8] Schmutz, Paul. *Systoles of arithmetic surfaces and the Markoff spectrum.*, Math. Ann. **305** (1996), no. 1, 191–203.

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

Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543

E-mail address: matlml@nus.edu.sg; mattansp@nus.edu.sg