ON MARKOFF TYPE SURFACES OVER NUMBER FIELDS AND THE ARITHMETIC OF MARKOFF NUMBERS

SEOYOUNG KIM, DAMARIS SCHINDLER, AND JYOTHSNAA SIVARAMAN

ABSTRACT. In this note we study arithmetic properties of solutions to inhomogeneous Markoff-Hurwitz equations, in particular we study counterexamples to the Hasse principle as well as the question of finite generation of the solution set under Vieta involutions, sign changes and permutations of coordinates.

CONTENTS

1. Introduction 1
Acknowledgements 4
2. Inhomogenous Markoff equations over number fields with a real embedding 4
3. Inhomogenous Markoff equations over arbitrary number fields 8
4. Fundamental domain 12
4.1. Case $k < 0$ and $a > 1$ 12
4.2. Case $k \geqslant 0$ and $a > 1$ 13
5. Finding local solutions 14
5.1. Primes above 3 15
5.2. Primes above 2 15
6. Exhibiting failure of the Hasse Principle 15
7. Prime factors in Homogenous Markoff equations of Degree 3 18
References 20

1. INTRODUCTION

The main goal of this article is to study the arithmetic of Markoff equations and generalized Markoff equations. The classical Markoff equation [18] is the affine cubic equation over the rational integers

$$x^2 + y^2 + z^2 - 3xyz = 0.$$

There are infinitely many integer solutions to this equation and by ordering them into a Markoff tree, Zagier [21] has given an asymptotic for the number of integer solutions of bounded naive height, refining previous results of Gurwood [14]. More recently, Mirzakhani [19] has given

a yet different proof as special case of her much more general work, using a dynamical point of view. For generalizations of Zagier's work see work of Baragar [2] and Gamburd, Magee and Ronan [12]. It is a natural question to deform this equation and say for $k \in \mathbb{Z}$ study the solubility of

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

over the rational integers. If there is a solution with coordinates in $\mathbb{Z}$, then there is also a solution in $\mathbb{R}$ and solutions in $\mathbb{Z}_p$ for every prime p. If the existence of these local solutions is already sufficient to deduce the existence of a solution over $\mathbb{Z}$, then we say that the affine Hasse principle holds. The question, for which k the affine Hasse principle holds, has been taken up amongst other questions in work of Ghosh and Sarnak [13]. First they find congruence conditions for $k \in \mathbb{Z}$ such that equation (1) has solutions in all of $\mathbb{Z}_p$ for every prime p. Those values of k are called admissible. Moreover, an admissible k is called generic if there is no solution to (1) with one coordinate in the set $\{0, \pm 1, \pm 2\}$. For generic admissible k they then describe fundamental domains for the integer solutions to (1) modulo the action of Vieta involutions, permutations of coordinates and sign changes of two of the coordinates. These fundamental domains, which are in this case compact, are then used to find infinite families of counterexamples to the affine Hasse principle. Note that not all of the counterexamples to the affine Hasse principle for the equation (1) can be explained by a Brauer-Manin obstruction, see [17] and [10] for a study of the associated Brauer groups and Brauer-Manin sets. Once the Hasse principle holds for a certain member in the family, it is an interesting question when strong approximation holds. For the original Markoff equation this has been studied in work of Bourgain, Gamburd and Sarnak [5] and has recently seen a breakthrough by Chen [9], who showed that the classical Markoff equation satisfies a strong approximation property at all but finitely many primes.

One goal of this article is to study the arithmetic of homogeneous and inhomogeneous Markoff equations over number fields. Let K be a number field and $\mathcal{O}_K$ its ring of integers. For $a, k \in K$ consider the equation

$$\mathcal{M}_{a,k} : \; x^2 + y^2 + z^2 - axyz = k,$$

and more generally for $n \in \mathbb{N}_{\geqslant 3}$ the affine hypersurface

$$\mathcal{M}_{a,k,n} : \; x_1^2 + \ldots + x_n^2 - ax_1x_2 \ldots x_n = k.$$

For $k = 0$ these have already been studied in 1907 by Hurwitz [16] and are now also known as Markoff-Hurwitz equations. Here again we can ask if a local to global principle holds for solutions in the ring of integers $\mathcal{O}_K$. First one notices that one has again n Vieta involutions mapping solutions over $\mathcal{O}_K$ to solutions over $\mathcal{O}_K$ assuming that a and k are integral. It is then a natural question to ask if there are finitely many orbits under the group Γ generated

by all n Vieta involutions, permutations of variables and sign changes of two of the variables. Hurwitz [16] showed that over the rational integers the set of integer solutions falls into finitely many orbits under Γ. The question of existence of solutions has for example been studied by Herzberg in [15] for the homogeneous case and in work of Fine et al. [11] for more general cases.

Over other rings of integers of number fields one may not at all expect that the set of solutions is a union of only finitely many orbits under Γ. Silverman in [20] showed in the case of the homogeneous Markoff equation in 3 variables and $a \neq 0$, that one has infinitely many orbits as soon as the group of units in the ring of integers is infinite and the equation $u^2 + v^2 + 1 \equiv 0 \bmod a\mathcal{O}_K$ is soluble in units. The question of finite generation of all integral solutions under the group Γ has been taken up for the homogeneous Markoff-Hurwitz equation by Baragar [3]. He showed that for $k = 0$, $a \neq 0$ and a number field $K \neq \mathbb{Q}$ which has a real embedding, the set of solutions is either empty or the set of orbits under the group Γ is infinite. The strategy of proof is to show that every orbit of Γ is discrete after embedding the solutions into $\mathbb{R}$, and that the solution set over $\mathcal{O}_K$ is either empty or has a cluster point. We study the question on finiteness of fundamental solutions in the case of the inhomogeneous Markoff-Hurwitz equation. In section 2, we show that for $k < 0$ and $a > 0$ every orbit under Γ is discrete. Our first main goal of this article is then to generalize work of Silverman and Baragar to inhomogeneous Markoff equations, where in the case of three variables, we obtain the following result.

Theorem 1.1. *Let $K/\mathbb{Q}$ be a number field and $a \in \mathcal{O}_K$ with $a \neq 0$. Suppose that K has a real embedding and that $K \neq \mathbb{Q}$. Then consider the equation*

$$x^2 + y^2 + z^2 = axyz + k \tag{2}$$

with $a, k \in \mathcal{O}_K$. We assume that $\tau(a) > 0$ and $\tau(k) < 0$ for a fixed real embedding τ of K. Then the number of orbits is either 0 or infinite.

Next we focus on the situation of real quadratic fields and explicitly work out domains for minimal solutions in orbits under Γ inspired by the fundamental domains that appear in work of Ghosh and Sarnak [13]. For this we consider the case of three variables and allow k to be positive or negative.

We already know that the family of inhomogeneous Markoff equations (1) with $a = 3$ in general does not satisfy the integral Hasse principle over the rational integers. What happens over number fields? Our second main goal of this article is the study of local solubility (see section 5) as well as global solubility (see section 6) and the construction of counterexamples to the Hasse principle over number fields. For the violation to the integral Hasse principle over

number fields we obtain the following example with elementary methods. To produce further examples and work over more general number fields, one could study the Brauer-Manin obstruction and evaluation of Brauer classes as in [17] and [10].

Theorem 1.2. *Let K be the subfield of degree 3 of the field $\mathbb{Q}(\zeta_{31})$. Consider the equation*

$$x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3 = 118. \tag{3}$$

This has no global solutions but has local solutions modulo each power of a prime ideal of K.

In another direction one can study the arithmetic of Markoff equations in fixing one member of the families described above, and try to learn more about the arithmetic properties of the solutions. Considering $\mathcal{M}_{3,0}$ we find all Markoff numbers as coordinates of positive solutions. It is not much known about arithmetic properties of Markoff numbers. By a deep result of Bourgain, Gamburd and Sarnak [5] we know that almost all Markoff numbers are composite. For more background on Markoff numbers we refer the reader to the book of Aigner [1] (see also work of Bombieri [4]).

What is the typical size of the largest prime factor of Markoff numbers? In section 7 we study the linear recurrence sequences ocurring as branches of the Markoff tree. Combining this with work of Bugeaud [6] we give a lower bound on the largest prime factor of Markoff numbers which appear in certain branches of the Markoff tree.

ACKNOWLEDGEMENTS

We thank the organizers of WIN5, Renate Scheidler, Alina Bucur and Wei Ho, and express our deep gratitude to Elisa Bellah, Elena Fuchs and Lynnelle Ye, and in particular Elena for initiating this WIN group. Moreover, we express our gratitude to the two anonymous referees for their very careful reading of an earlier draft of this article and numerous helpful suggestions.

2. INHOMOGENOUS MARKOFF EQUATIONS OVER NUMBER FIELDS WITH A REAL EMBEDDING

Let K be a number field with ring of integers $\mathcal{O}_K$ and at least one real embedding. For the rest of this section fix a real embedding $K \subset \mathbb{R}$ and let

$$\mathcal{M}_{a,k} : x_1^2 + x_2^2 + x_3^2 = ax_1x_2x_3 + k,$$

where $a, k \in \mathcal{O}_K$ and $a > 0, k < 0$. Further $\mathcal{M}_{a,k}(\mathcal{O}_K)$ shall be used to denote the set of all solutions of $\mathcal{M}_{a,k}$ with co-ordinates in $\mathcal{O}_K$. Let ϕ_i for $i \in \{1, 2, 3\}$ be used to denote the following involutions:

$$\begin{aligned} \phi_1(x_1, x_2, x_3) &= (x_2, x_3, ax_2x_3 - x_1), \\ \phi_2(x_1, x_2, x_3) &= (x_1, x_3, ax_1x_3 - x_2) \\ \text{and } \phi_3(x_1, x_2, x_3) &= (x_1, x_2, ax_1x_2 - x_3). \end{aligned}$$

These involutions are called the Vieta involutions. We denote by Γ the group generated by the involutions ϕ_i, the automorphisms of the $\mathcal{M}_{a,k}(\mathcal{O}_K)$ given by permuting the co-ordinates of each solution and the automorphisms given by sign change of the first two entries in a solution tuple.

We define more generally, the following form of equations

$$\mathcal{M}_{a,k,n} : x_1^2 + x_2^2 + \cdots + x_n^2 = ax_1x_2\cdots x_n + k, \quad \text{for } a > 0, k < 0,$$

which was introduced and studied in [3]. That is to say, $\mathcal{M}_{a,k,3} = \mathcal{M}_{a,k}$. Similarly, the idea of n Vieta involutions

$$\phi_i(x_1, x_2, \ldots, x_n) = (x_1, \ldots, \hat{x}_i, \ldots, x_n, \left(\frac{ax_1\cdots x_n}{x_i}\right) - x_i), \quad i = 1, \ldots, n, \tag{4}$$

where the hat denotes that the component is omitted, and possible permutations along with sign changes can be perused to study the set $\mathcal{M}_{a,k,n}(\mathcal{O}_K)$ of integral solutions of $\mathcal{M}_{a,k,n}$. In case that $x_i = 0$ we read the expression above as $\frac{ax_1\ldots x_n}{x_i} = ax_1 \ldots x_{i-1}x_{i+1}\ldots x_n$.

In this section, we assume that **the set $\mathcal{M}_{a,k,n}(\mathcal{O}_K)$ is non-empty**.

Definition 1. *For a point P in $\mathcal{M}_{a,k,n}(\mathcal{O}_K)$, we define $h(P) = \max_i |x_i|$.*

Definition 2. *If $h(\phi(P)) \geqslant h(P)$ for every Vieta involution ϕ then $P \in \mathcal{M}_{a,k}(\mathcal{O}_K)$ will be called a fundamental solution.*

We say that a solution $(x_1, x_2, \ldots, x_n)$ is a positive ordered solution in $\mathcal{M}_{a,k,n}$ if $0 < x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$. We say that two positive ordered solutions are connected if there exists a Vieta involution which maps one to the other. In this case, we say that the two positive ordered solutions are neighbors. The following lemma illustrates the relation between neighbors when the height of the image of ϕ_n is strictly less than its preimage.

Lemma 2.1. *Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be a positive ordered solution in $\mathcal{O}_K$ to the equation*

$$\mathcal{M}_{a,k,n} : x_1^2 + x_2^2 + \cdots + x_n^2 = ax_1x_2\cdots x_n + k, \quad \textit{for } a > 0, k < 0,$$

such that $h(\phi_n(\mathbf{x})) < h(\mathbf{x})$. Then either $\phi_n(\mathbf{x})$ is a fundamental solution, or we have

$$h(\mathbf{x}) > h(\phi_n(\mathbf{x})) - \frac{k}{h(\mathbf{x})} + \frac{n-2}{2h(\mathbf{x})}\left(\frac{2}{a}\right)^{2/(n-2)}.$$

Proof. Since the proof is similar to the proof of Lemma 1.1 in [3], we will give a rough sketch of the proof. As we assume $k < 0$, we have the $ax_1x_2\cdots x_{n-2} > 2$. This implies that for $i \leqslant n-1$ we have

$$ax_1\cdots\hat{x_i}\cdots x_{n-1} > 2.$$

Therefore

$$ax_1\cdots\hat{x_i}\cdots x_n - x_i > 2x_n - x_i > x_n.$$

Therefore if $\mathbf{x} = (x_1, x_2, \dots, x_n)$ is a positive ordered solution, then $\phi_i(\mathbf{x})$ is also a positive ordered solution for $i = 1, \dots, n-1$. In other words, ϕ_n is the only involution which can (potentially) decrease the height of a given solution in $\mathcal{M}_{a,k,n}(\mathcal{O}_K)$. Now the arithmetic-geometric inequality gives

$$x_1^2 + \cdots + x_{n-2}^2 \geqslant (n-2)\left(\frac{2}{a}\right)^{2/(n-2)}.$$

Under the assumption $h(\phi_n(\mathbf{x})) < h(\mathbf{x})$, the above inequality implies

$$\frac{n-2}{2x_n}\left(\frac{2}{a}\right)^{2/(n-2)} - \frac{k}{x_n} < x_n - x_{n-1}.$$

If $x_n' = ax_1 \cdots x_{n-1} - x_n > x_{n-1}$, then $\phi_n(\mathbf{x})$ is a positive ordered solution. This implies that $\phi_n(\mathbf{x})$ is a fundamental solution. Otherwise, we have $x_n' \leqslant x_{n-1}$ and $h(\phi_n(\mathbf{x})) = x_{n-1}$. Thus, we obtain the result. □

Lemma 2.2. *Any orbit in the set of ordered solutions in $\mathcal{M}_{a,k,n}(\mathcal{O}_K)$ is discrete in $\mathbb{R}^n$.*

Proof. The proof is similar to that of Baragar [3] section 1. For simplicity, we consider the case $n = 3$. A similar argument can easily be reproduced for the case $n \geqslant 3$ using Lemma 2.1. We assume the following ordering on the solution $P = (x, y, z) \in \mathcal{M}_{a,k}(\mathcal{O}_K)$

$$0 \leqslant |x| \leqslant |y| \leqslant |z|.$$

Given a solution to the Markoff equation either all the entries are non-negative or exactly two are negative. We first work with the non-negative solutions in the orbit. That is to say, the solutions (x, y, z) with $0 \leqslant x \leqslant y \leqslant z$ to the equation $\mathcal{M}_{a,k} : x^2 + y^2 + z^2 = axyz + k$ satisfy

$$x^2 + (y - z)^2 = (ax - 2)yz + k.$$

It follows that since $k < 0$, $ax > 2$. If for a point P, $|axy - z| > z$ then, consider the Vieta involution ϕ given by

$$(x, y, z) \to (x, y, axy - z).$$

We have $\phi \cdot \phi(P) = P$ and therefore

$$h(\phi \cdot \phi(P)) < h(\phi(P)).$$

Since this is the only involution for which we may obtain a Markoff triple with lower height, it follows that P is a fundamental solution. If for a positive ordered solution P, $|axy - z| \leqslant z$, it is still true that $axy - z > 0$ since two entries of this triple are already positive. Therefore, we have $axyz \leqslant 2z^2$ and it now follows that

$$x^2 + y^2 + z^2 - k \leqslant 2z^2$$

by the Markoff equation. This further implies that

$$x^2 + (z - y)^2 - k \leqslant 2z(z - y).$$

Since $ax > 2$, we get

$$(z - y) > \frac{\left(\frac{2}{a}\right)^2 - k}{2z}.$$

In this case if $|axy - z| > |y|$, we use the same argument as before. We get

$$\begin{aligned} \phi \cdot \phi(P) &= P \\ \text{but} \quad h(\phi \cdot \phi(P)) &\geqslant h(\phi(P)). \end{aligned}$$

This implies that $\phi(P)$ is a fundamental solution. Further if we consider a sequence of n consecutive non-negative solutions in this orbit from P_1, culminating in P, we get

$$2h(P) > \left(\left(\frac{2}{a}\right)^2 - k\right) \cdot \left(\frac{1}{h(P_1)} + \frac{1}{h(P_2)} + \ldots + \frac{1}{h(P_{n-1})}\right).$$

This gives the following upper bound on n

$$\frac{2h(P)^2}{\left(\frac{2}{a}\right)^2 - k} + 1 > n.$$

Finally, if Q is a cluster point for the non-negative solutions in this orbit, then there are infinitely many non-negative solutions R in the orbit with $h(R) < h(Q) + 1$. But from the above bound on n the number of non-negative solutions in the orbit with $h(R) < h(Q) + 1$ is finite. This implies that the set of non-negative solutions in the orbit is discrete in $\mathbb{R}$.

If we consider the negative solutions in the orbit, they can be obtained by changing the signs of two of the entries in each triple of the positive solutions. It follows that the orbit is discrete. □

Remark 2.1. *In due course of the above proof, we have shown that since $k < 0$, we have $ax > 2$ for any ordered positive solution $(x, y, z) \in \mathcal{O}_K^3$. This implies that if we consider the involutions*

$$(x, y, z) \to (x, axz - y, z) \qquad \textit{and} \qquad (x, y, z) \to (ayz - x, y, z)$$

we have

$$axz - y > 2z - y > z \qquad \textit{and} \qquad ayz - x > axz - x > 2z - x > z.$$

Therefore by rearranging the new solutions in ascending order and applying the above Vieta involutions, we observe that there are infinitely many solutions in each orbit. If the set of z co-ordinates of the solutions in an orbit is bounded above then the set of all solutions in the orbit must lie in a compact set and therefore have a limit point. This contradicts Lemma 2.2. However if the set of x coordinates is bounded then the above implies that the set of z coordinates is also bounded.

3. Inhomogenous Markoff equations over arbitrary number fields

Let K be an arbitrary number field. We now consider the Markoff- Hurwitz equation

$$x^2 + y^2 + z^2 = axyz + k$$

for some $a, k \in \mathcal{O}_K$. Suppose we have a solution (p_1, p_2, p_3) in $\mathcal{O}_K$. We now consider the equation

$$x^2 + y^2 + p_3^2 = ap_3xy + k. \tag{5}$$

Let $A = ap_3$ and $B = p_3^2 - k$. This brings us to the equation

$$x^2 - Ax + 1 = 0.$$

Let the roots be ω and ω'. We can now re-write the equation (5) as

$$(x - \omega y)(x - \omega' y) = -B.$$

Suppose further that $\omega \notin K$. Then the left hand side is simply

$$N_{L/K}(x - \omega y) = -B$$

where $L = K(\omega)$. However, we now note that if we multiply any solution with $z = p_3$ by a unit u of norm one, we get another solution. Let $S^* = \mathcal{O}_L^*$, the group of units of $\mathcal{O}_L^*$, and

$$S_1^* = \{u \in S^* : N_{L/K}(u) = 1\}.$$

We now recall two theorems of [3].

Theorem 3.1. *([3, Theorem 2.1]) Suppose that R is an order in a number field K, and K is neither $\mathbb{Q}$ nor imaginary quadratic. Suppose also that*

$$\omega^2 - A\omega + 1 = 0$$

for $A \in R$ and $\omega \notin K$. Set $L = K(\omega)$ and $S = R \bigoplus \omega R$. Finally suppose that every real embedding τ of K in $\mathbb{C}$ satisfies $|\tau(A)| > 2$. Then

$$rank(S_1^*) \geqslant 2.$$

The second theorem talks about the existence of a cluster point in $\mathcal{O}_K^2$ for the set of solutions of the equation

$$x^2 + y^2 - Axy = -B$$

where A, B are in $\mathcal{O}_K$.

Theorem 3.2. *([3, Theorem 2.2]) Suppose that R is an order in a number field K and R^* is infinite. Further suppose that $A \in R$ and $\tau(A) > 2$ for all real embeddings τ of K. Let ω satisfy*

$$\omega^2 - A\omega + 1 = 0$$

and suppose that $\omega \notin K$. Finally if $(p_1, p_2) \in R^2$ is a solution to

$$x^2 - Axy + y^2 = -B \tag{6}$$

where $B \in R$. Then (p_1, p_2) is a cluster point for the solutions of (6) in $\mathbb{C}^2$.

For convenience of the reader we now state a version of Kronecker's approximation theorem, which we need in the next lemma.

Theorem 3.3. *For any $\alpha, \beta, \epsilon \in \mathbb{R}$ with $\alpha \notin \mathbb{Q}$, and $\epsilon > 0$ there exist integers p and q such that*

$$|p\alpha - q - \beta| < \epsilon.$$

Two intermediate lemmas we will require are the following.

Lemma 3.4. *Let $K \subset \mathbb{R}$ and $S \subseteq \mathcal{O}_K^*$ be a subgroup. If the rank of S is at least 2, then S is dense at 1 in $\mathbb{C}$. That is to say, 1 is a cluster point of S.*

Proof. Let v_1 and v_2 be two positive multiplicatively independent units in S. It follows that $\log v_1$ and $\log v_2$ are $\mathbb{Q}$ linearly independent. Therefore $\log_{v_1} v_2$ is irrational. By Theorem 3.3 the $\mathbb{Z}-$ span of 1 and $\log_{v_2} v_1$ is dense in $\mathbb{R}$. Therefore the subgroup S is dense at 1. □

Before we proceed to the next lemma, we make the following observation. Going back to the Markoff-Hurwitz equation

$$x^2 + y^2 + z^2 = axyz + k,$$

suppose we have a solution (p_1, p_2, p_3) in $\mathcal{O}_K^3$. Now set $A = ap_3$ and $B = p_3^2 - k$ and consider the equation

$$x^2 + y^2 - Axy = -B$$

with $A, B \in \mathcal{O}_K$. For any real embedding τ of K into $\mathbb{C}$, we have

$$\tau(p_1)^2 + \tau(p_2)^2 - \tau(A)\tau(p_1p_2) = -\tau(B).$$

We may assume that $\tau(p_1p_2) > 0$. Suppose this were false, we may choose another solution by multiplying p_1 and p_3 by -1. This equation can be rewritten as

$$(\tau(p_1) - \tau(p_2))^2 = (\tau(A) - 2)\tau(p_1p_2) - \tau(B).$$

If $\tau(B) \geqslant 0$ and if the solution (p_1, p_2, p_3) is non-trivial, then it follows that $\tau(A) > 2$.

Lemma 3.5. *If the number field $K \subset \mathbb{R}$ is such that the rank of $\mathcal{O}_K^*$ is 1, and $(p_1, p_2, p_3) \in \mathcal{O}_K^3$ is a positive solution to the equation*

$$x^2 + y^2 + z^2 = axyz + k, \tag{7}$$

with $k < 0$ and $a > 0$, then the quadratic equation

$$x^2 - ap_3x + 1 = 0$$

has no solution in K.

Proof. The proof of this lemma is already contained in the second half of the proof of [3, Theorem 2.3], we repeat the arguments here for convenience of the reader.

Consider the equations $x^2 - ap_ix + 1 = 0$, for $i \in \{1, 2, 3\}$. If any of these equations have a solution $\omega \in K$, then it follows that $\omega \in \mathcal{O}_K^*$. Since the rank of $\mathcal{O}_K^*$ is 1, we have the existence of a positive fundamental unit u, and therefore $\omega = \pm u^{k_z}$ for some $k_z \in \mathbb{Z}$. Since $k < 0$ and $a > 0$, without loss of generality, we may assume that the $p_i \geqslant 0$. Therefore, we have the following expressions for the p_i,

$$p_1 = \frac{u^{k_x} + u^{-k_x}}{a},\ p_2 = \frac{u^{k_y} + u^{-k_y}}{a},\ p_3 = \frac{u^{k_z} + u^{-k_z}}{a}$$

for integers k_x, k_y and k_z. Without loss of generality we assume that u^{k_x}, u^{k_y} and u^{k_z} are greater than 1. Further we may assume that $u^{k_x} < u^{k_y} < u^{k_z}$. By remark 2.1, we may assume that, given a positive constant M, if we traverse far enough along an orbit, $\frac{M+1}{a} < p_1 < p_2 < p_3$. Therefore $u^{k_x} > M + 1 - u^{-k_x} \geqslant M$. We also have from the usual Vieta involutions that (p_1', p_2, p_3) is also a solution, where $p_1' = ap_2p_3 - p_1$. Further, by the same argument as above we have an expression for p_1',

$$p_1' = \frac{u^{k_x'} + u^{-k_x'}}{a}.$$

From the two expressions for p_1', we get

$$\frac{u^{k_x'} + u^{-k_x'}}{a} + \frac{u^{k_x} + u^{-k_x}}{a} \quad = \quad a \cdot \frac{u^{k_y} + u^{-k_y}}{a} \cdot \frac{u^{k_z} + u^{-k_z}}{a}.$$

This implies

$$u^{k_x'-k_y-k_z} + u^{-k_x'-k_y-k_z} + u^{k_x-k_y-k_z} + u^{-k_x-k_y-k_z} \quad = \quad 1 + u^{-2k_z} + u^{-2k_y} + u^{-2k_y-2k_z}.$$

Since $u^{k_x-k_y} < 1$, we have $u^{k_x-k_y-k_z} < u^{-k_z} < \frac{1}{M}$. Therefore

$$1 - \frac{3}{M} < u^{k_x'-k_y-k_z} < 1 + \frac{3}{M} \implies k_x' - k_y - k_z = 0$$

for M sufficiently large. Since $p_1' = ap_2p_3 - p_1$, we get

$$u^{k_x} + u^{-k_x} = u^{k_y-k_z} + u^{k_z-k_y}.$$

Substituting in (7), we get $4 - k(a)^2 = 0$, which is a contradiction since $k < 0$. □

Proof of Theorem 1.1. We have already proved in Lemma 2.2 that each orbit in the set of solutions is discrete. Therefore to show infinitude of the number of orbits it suffices to show that the set of solutions has a cluster point. If (p_1, p_2, p_3) is a solution to (2), then setting $A = ap_3$ and $B = p_3^2 - k$, we consider the equation

$$x^2 - Axy + y^2 = -B. \tag{8}$$

Let ω be a solution to $\omega^2 - A\omega + 1 = 0$.

Case 1 : If $\omega \notin K$ applying Theorem 3.2, we get that (p_1, p_2) is a cluster point in $\mathbb{C}^2$ of the solutions in $\mathcal{O}_K$ to the equation

$$x^2 - Axy + y^2 = -B, \tag{9}$$

if a solution ω to $\omega^2 - A\omega + 1 = 0$ is not in K. Therefore if $\omega \notin K$, (p_1, p_2, p_3) is a cluster point in $\mathbb{C}^3$ in the set of all solutions to equation (2) by Theorem 3.2.

Case 2: If $\omega \in K$, we first identify $\omega, K, p_1, p_2, p_3, A$ and B with their images under a fixed real embedding. Then in K we have

$$p_1^2 + p_2^2 - Ap_1p_2 = (p_1 - \omega p_2)(p_1 - \omega^{-1}p_2) = -B.$$

Let $\beta_1 = p_1 - \omega p_2$ and $\beta_2 = p_1 - \omega^{-1}p_2$. For any $u \in \mathcal{O}_K^*$, if we set $x - \omega y = u\beta_1$ and $x - \omega^{-1}y = u^{-1}\beta_2$, then solving for x and y, we get

$$x = \frac{\omega u^{-1}\beta_2 - \omega^{-1}u\beta_1}{\omega - \omega^{-1}} \text{ and } y = \frac{u^{-1}\beta_2 - u\beta_1}{\omega - \omega^{-1}}.$$

It follows immediately that $x, y \in \mathcal{O}_K$ whenever $u \equiv 1 \bmod (\omega - \omega^{-1})$.

Subcase 1 : Suppose that the rank of $\mathcal{O}_K^*$ is greater than or equal to 2. Since the subgroup of units given by

$$S^* = \{u \in \mathcal{O}_K^* : u \equiv 1 \bmod (\omega - \omega^{-1})\}.$$

is of finite index in $\mathcal{O}_K^*$, by Lemma 3.4, 1 is a cluster point for S^*. Now consider for $u \in S^*$,

$$\begin{aligned} |x - p_1| &= \left|\frac{\omega\beta_2}{\omega - \omega^{-1}}(u^{-1} - 1) + \frac{\omega^{-1}\beta_1}{\omega - \omega^{-1}}(1 - u)\right| \\ &\leqslant \left|\frac{\omega\beta_2}{\omega - \omega^{-1}}(u^{-1} - 1)\right| + \left|\frac{\omega^{-1}\beta_1}{\omega - \omega^{-1}}(1 - u)\right|. \\ |y - p_2| &= \left|\frac{\beta_2}{\omega - \omega^{-1}}(u^{-1} - 1) + \frac{\beta_1}{\omega - \omega^{-1}}(1 - u)\right| \\ &\leqslant \left|\frac{\beta_2}{\omega - \omega^{-1}}(u^{-1} - 1)\right| + \left|\frac{\beta_1}{\omega - \omega^{-1}}(1 - u)\right|. \end{aligned}$$

Since β_1, β_2, ω and ω^{-1} are fixed by p_1 and p_2 it follows by Lemma 3.4 that (p_1, p_2) is a cluster point for the solutions of (8) in $\mathcal{O}_K$. Therefore, once again we have that (p_1, p_2, p_3) is a cluster point in $\mathbb{C}^3$ for the set of all solutions to equation (2).

Subcase 2 : As for the case when the rank of $\mathcal{O}_K^*$ is 1, upto an isomorphism we may assume that it is imbedded in the reals. It now follows from Lemma 3.5, the comment before Lemma 3.5 and Theorem 3.2 that if there is a solution (p_1, p_2, p_3) then it is a cluster point to the set of solutions to (2).

□

4. Fundamental domain

Throughout this section, we assume that the field K is a real quadratic field.

4.1. **Case $k < 0$ and $a > 1$.** In this section (following [13]), we consider the equation for $k < 0$ and $a > 1$

$$x_1^2 + x_2^2 + x_3^2 = ax_1x_2x_3 + k. \tag{10}$$

We would like to construct the fundamental domain for the set of solutions under the action of the group Γ generated by the Vieta involutions, permutations and double sign change in the ring of integers of a real quadratic field. Treating the above equation as a quadratic in x_3, we get

$$2x_3 = ax_1x_2 \pm \sigma \text{ where } \sigma = \sqrt{(ax_1x_2)^2 - 4(x_1^2 + x_2^2 - k)}. \tag{11}$$

Since for an ordered solution $x_1 \leqslant x_2 \leqslant x_3$, $ax_1x_2 - 2x_3 \leqslant x_2(ax_1 - 2)$ we have

$$|\sigma|^2 \leqslant (x_2(ax_1 - 2))^2.$$

Simplifying we get

$$x_2^2(ax_1 - 2) \leqslant x_1^2 - k. \tag{12}$$

Considering the points for which $x_3 \leqslant ax_1x_2 - x_3$ we get $x_1 \leqslant x_2 \leqslant x_3 \leqslant \frac{a}{2}x_1x_2$.

If $x_1 \leqslant \frac{2}{a}$, then from equation (10) we get

$$x_1^2 + (x_2 - x_3)^2 \leqslant k.$$

This implies that for a solution with $x_1 \geqslant 0$, $\frac{2}{a} < x_1$. Further there is no solution for which only one $x_i \leqslant 0$ and no solution with $x_i \leqslant 0$ for all i. This leaves the case where $x_1 \leqslant x_2 < 0 < x_3$. However this solution is equivalent by double sign change to the one given by $|x_1|, |x_2|$ and x_3.

Lemma 4.1. *Every solution to the equation given by* (10) *in the real quadratic field K is Γ equivalent to a point in*

$$G_a^-(k) = \left\{(x_1, x_2, x_3) \ : \ \frac{2}{a} < x_1 \leqslant x_2 \leqslant x_3 \leqslant \frac{a}{2}x_1x_2\right\}.$$

Let us assume $\frac{2}{a} < x_1 \leqslant x_2 \leqslant x_3 \leqslant \frac{a}{2}x_1x_2$. If $x_1 \geqslant \frac{4}{a}$, then we obtain from equation (12) that

$$2x_2^2 \leqslant x_1^2 + |k| \implies x_2 \leqslant \sqrt{|k|} \implies x_3 \leqslant \frac{a|k|}{2}.$$

For $\frac{2}{a} < x_1 < \frac{4}{a}$, then from equation (12) we get

$$x_2^2 \leqslant \frac{x_1^2 + |k|}{ax_1 - 2}.$$

Therefore we have the following lemma.

Lemma 4.2. *Every solution to the equation given by* (10) *in the real quadratic field* K *is* Γ *equivalent to a point in*

$$G_1 = I_1 \bigcup I_2$$

where

$$I_1 = \left\{(x_1, x_2, x_3) \ : \ \frac{4}{a} \leqslant x_1 \leqslant x_2 \leqslant \sqrt{|k|}, \frac{4}{a} \leqslant x_3 \leqslant \frac{a|k|}{2}\right\}$$

and

$$I_2 = \left\{(x_1, x_2, x_3) \ : \ \frac{2}{a} < x_1 < \frac{4}{a}, \ x_1 \leqslant x_2 \leqslant \sqrt{\frac{x_1^2 + |k|}{ax_1 - 2}}, \ x_2 \leqslant x_3 \leqslant \frac{ax_1}{2}\sqrt{\frac{x_1^2 + |k|}{ax_1 - 2}}\right\}.$$

4.2. **Case** $k \geqslant 0$ **and** $a > 1$**.** We now describe the fundamental domain of the equation (10)

$$x_1^2 + x_2^2 + x_3^2 = ax_1x_2x_3 + k$$

for $k \geqslant 0$ and $a > 1$. In particular, we obtain the following Lemma.

Lemma 4.3. *For* $k > \frac{4}{a^2}$*, every solution to the equation given by* (10) *in the real quadratic field* K *is* Γ *equivalent to a point in the compact set* $G^+(k) \cup \mathfrak{T}(k)$ *where* $\mathfrak{T}(k) \subset \mathbb{Z}^3$ *is the finite set of solutions having coordinates either* 0 *or* 1 *and*

$$G^+(k) = \left\{(-x_1, x_2, x_3) \in O_K^3 : \frac{2}{a} < x_1 \leqslant x_2 \leqslant x_3, \ x_1^2 + x_2^2 + x_3^2 - ax_1x_2x_3 = k\right\}, \tag{13}$$

or if not, then it is equivalent to a triple $(x_1, ax_1x_2 - x_3, x_2)$ *with* $\frac{2}{a} < ax_1x_2 - x_3 < x_2 \leqslant x_3$ *and* $x_1 > \frac{2}{a}$.

Proof. When $k \geqslant 0$, there are only finitely many triples $(x_1, x_2, x_3) \in \{0, 1\}^3$ satisfying the equation (10). We denote the finite set by $\mathfrak{T}(k)$. Now we consider the Vieta involution on (10)

$$(x_1, x_2, x_3) \to (x_1, x_2, ax_1x_2 - x_3).$$

If $ax_1x_2 - x_3 < 0$, then (x_1, x_2, x_3) is equivalent to a solution of $G_a^+(k)$. Hence, we consider the case $ax_1x_2 - x_3 \geqslant 0$. Now, we assume that $ax_1x_2 - x_3 \geqslant x_3$. In this case, we have $2x_3 \leqslant ax_1x_2$. Similar to the description (11), solving for x_3 of the equation (10) gives

$$2x_3 = ax_1x_2 \pm \sigma \text{ where } \sigma = \sqrt{(ax_1x_2)^2 - 4(x_1^2 + x_2^2 - k)}$$

and this further implies $\sigma = |ax_1x_2 - 2x_3| = ax_1x_2 - 2x_3$ and (12) for an ordered solution. If $x_1 < \frac{2}{a}$, we conclude $k \leqslant \frac{4}{a^2}$. Thus for all $k > \frac{4}{a^2}$, we have a contradiction to the assumption $ax_1x_2 - x_3 \geqslant x_3$. So, when $k > \frac{4}{a^2}$, we have

$$0 \leqslant ax_1x_2 - x_3 < x_3.$$

Moreover, we can prove $\frac{2}{a} < ax_1x_2 - x_3 < x_2 \leqslant x_3$: if $x_2 \leqslant ax_1x_2 - x_3 < x_3$, then we have $ax_1x_2 < 2x_3 \leqslant 2x_2(ax_1 - 1)$. This gives

$$\sigma = 2x_3 - ax_1x_2 \leqslant 2x_2(ax_1 - 1) - ax_1x_2 = ax_1x_2 - 2x_2 = (ax_1 - 2)x_2,$$

and the same argument gives a contradiction. Hence, we proved the desired result. □

5. Finding local solutions

Let K be a number field and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above a prime $p \in \mathbb{Z}$. We denote by $\mathbb{F} = \mathcal{O}_K/\mathfrak{p}$ the residue field of size $|\mathbb{F}| = \mathfrak{N}(\mathfrak{p})$. In order to show the existence of local solutions of the Markoff-Hurwitz equation, we need the following result of Carlitz [7, 8].

Theorem 5.1. *Given a number field K and a prime ideal $\mathfrak{p}$ which does not lie above 2, the number of solutions $N_\mathfrak{p}$ modulo $\mathfrak{p}$ to the equation, with an arbitrary e and $abcd \neq 0$,*

$$ax^2 + by^2 + cz^2 = 2dxyz + e$$

is determined by

$$N_\mathfrak{p} = \mathfrak{N}(\mathfrak{p})^2 + 1 + \mathfrak{N}(\mathfrak{p})\{\psi(a) + \psi(b) + \psi(c) + \psi(e)\}\psi(d^2 - abc),$$

where ψ is the quadratic symbol taking value 1 for squares, -1 for non-squares, and 0 at 0.

Proof. The proof can be found in [7]. □

Theorem 5.1 implies the following local property of the Markoff-Hurwitz equation, that is to say, when the parameters are $a = b = c = 1$ and suitable d.

Corollary 5.2. *Given a number field K and a prime ideal $\mathfrak{p}$ which does not lie above 2, the number of solutions $N_\mathfrak{p}$ modulo $\mathfrak{p}$ to the equation*

$$x_1^2 + x_2^2 + x_3^2 = \alpha x_1x_2x_3 + \gamma \ \text{ with } \ \alpha, \gamma \in \mathbb{Z}$$

is strictly greater than 0. In fact

$$N_\mathfrak{p} \geqslant \mathfrak{N}(\mathfrak{p})^2 - 4\mathfrak{N}(\mathfrak{p}).$$

We now prove a lemma on finding solutions modulo $\mathfrak{p}^n$.

Lemma 5.3. *Let K be a number field. Further let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{N}(\mathfrak{p}) > 4$ and such that $\mathfrak{p}$ does not lie above 2. We consider the equation*

$$x_1^2 + x_2^2 + x_3^2 = \alpha x_1x_2x_3 + \gamma \ \text{ with } \ \alpha, \gamma \in \mathbb{Z}. \tag{14}$$

It has a solution modulo $\mathfrak{p}^n$ for all $n \geqslant 1$.

Proof. By Corollary 5.2, we know that the equation has solutions modulo $\mathfrak{p}$. We now break the proof into three cases. Let

$$f = x_1^2 + x_2^2 + x_3^2 - \alpha x_1x_2x_3$$

then f' takes one of the following three forms $2x_i - \alpha x_jx_k$ for $\{i, j, k\} = \{1, 2, 3\}$. If all three forms are $0 \bmod \mathfrak{p}$ for (a, b, c) with entries in $\mathcal{O}_K$ where (a, b, c) is a solution mod $\mathfrak{p}$ then we call the solution singular.

Case 1: If we have a non-singular solution then by Hensel's lemma we have solutions modulo $\mathfrak{p}^n$ for all $n \geqslant 1$.

Case 2: If a given solution is singular, we further suppose that $\mathfrak{p} \nmid (\gamma)$ and $\mathfrak{p} \nmid (abc)$. Since the solution is singular we have

$$2x_i \equiv \alpha x_j x_k \bmod \mathfrak{p} \ ,$$

where x_i, x_j, x_k is a permutation of a, b, c. Since $\mathfrak{p}$ does not lie above 2, we have

$$\alpha abc \equiv 2a^2 \bmod \mathfrak{p}$$

and therefore

$$a^2 \equiv b^2 \equiv c^2 \bmod \mathfrak{p}.$$

Substituting in (14), we get

$$0 \not\equiv a^2 \equiv \gamma \bmod \mathfrak{p}.$$

It follows that $(a, 0, 0)$ is a solution modulo $\mathfrak{p}$ to (14). Further, since $2a - \alpha bc = 2a$ and $\mathfrak{p}$ does not lie above 2, it follows that this solution is non-singular, thereby leading back to case 1.

Case 3: If a given solution is singular and $\mathfrak{p} \mid x_1x_2x_3$ we have that $\gamma \in \mathfrak{p}^2$. However , again using the fact that the solution is singular and that $\mathfrak{p}$ does not lie above 2, we get that the solution is $(0, 0, 0) \bmod \mathfrak{p}$. On the other hand from Corollary 5.2 we observe that there is at least one other solution which reduces the problem to one of the above two cases. □

5.1. **Primes above** 3. If $\alpha \in \mathfrak{p}$ and $\gamma - 1 \in \mathfrak{p}$, where $\mathfrak{p}$ lies above 3, then $(1, 0, 0)$ is a non singular solution modulo $\mathfrak{p}$. If $\alpha \in \mathfrak{p}$ and $\gamma \in \mathfrak{p}^2$ where $\mathfrak{p}$ lies above 3, then $(3, 0, 0)$ is a non-singular solution modulo $\mathfrak{p}^2$ and $(0, 0, 0)$ is a solution modulo $\mathfrak{p}$.

5.2. **Primes above** 2. If $\alpha - 1, \gamma \in \mathfrak{p}$ where $\mathfrak{p}$ where $\mathfrak{p}$ lies above 2, then $(1, 1, 1)$ is a non-singular solution modulo $\mathfrak{p}$.

In all the above two cases, we have by Hensel's lemma solutions modulo $\mathfrak{p}^n$ for $n \geqslant 1$.

6. Exhibiting failure of the Hasse Principle

The following lemma is a formulation of the well-known supplement to the law of quadratic reciprocity in number fields.

Lemma 6.1. *Given a number field K and a prime ideal $\mathfrak{p}$ not lying above 2, we have*

$$\left(\frac{2}{\mathfrak{p}}\right) = (-1)^{\frac{\mathfrak{N}(\mathfrak{p})^2-1}{8}}.$$

Here $(\cdot)$ is used to indicate the 2-power residue symbol modulo $\mathfrak{p}$ and the norm is with respect to $K/\mathbb{Q}$.

Proof. By definition, we have

$$\left(\frac{2}{\mathfrak{p}}\right) \equiv 2^{\frac{\mathfrak{N}(\mathfrak{p})-1}{2}} \bmod \mathfrak{p}\mathcal{O}_K.$$

Consider the field given by $K(i)$, denoted L. We now have

$$(2i)^{\frac{\mathfrak{N}(\mathfrak{p})-1}{2}} \cdot (1+i) \equiv (1+i)^{\mathfrak{N}(\mathfrak{p})} \equiv 1 + i^{\mathfrak{N}(\mathfrak{p})} \equiv 1 + i \cdot (-1)^{\frac{\mathfrak{N}(\mathfrak{p})-1}{2}} \bmod \mathfrak{p}\mathcal{O}_L.$$

This implies that

$$\left(\frac{2}{\mathfrak{p}}\right) \equiv \frac{1 + i \cdot (-1)^{\frac{\mathfrak{N}(\mathfrak{p})-1}{2}}}{i^{\frac{\mathfrak{N}(\mathfrak{p})-1}{2}}(1+i)} \equiv \frac{(1 + i \cdot (-1)^{\frac{\mathfrak{N}(\mathfrak{p})-1}{2}})(1-i)}{2i^{\frac{\mathfrak{N}(\mathfrak{p})-1}{2}}} \bmod \mathfrak{p}\mathcal{O}_L$$

Therefore,

$$\left(\frac{2}{\mathfrak{p}}\right) \equiv \begin{cases} (-1)^{\frac{\mathfrak{N}(\mathfrak{p})-1}{4}} \bmod \mathfrak{p}\mathcal{O}_L, & \frac{\mathfrak{N}(\mathfrak{p})-1}{2} \text{ is even} \\ (-1)^{\frac{\mathfrak{N}(\mathfrak{p})+1}{4}} \bmod \mathfrak{p}\mathcal{O}_L, & \frac{\mathfrak{N}(\mathfrak{p})-1}{2} \text{ is odd.} \end{cases}$$

Combining both

$$\left(\frac{2}{\mathfrak{p}}\right) \equiv (-1)^{\frac{\mathfrak{N}(\mathfrak{p})^2-1}{8}} \bmod \mathfrak{p}\mathcal{O}_L \implies \left(\frac{2}{\mathfrak{p}}\right) \equiv (-1)^{\frac{\mathfrak{N}(\mathfrak{p})^2-1}{8}} \bmod \mathfrak{p}\mathcal{O}_K.$$

Hence the lemma. □

Lemma 6.2. *Let K be a Galois number field of degree 3 such that 2 splits in K. Further let $v \neq 0$ be a rational integer such that all its prime divisors in $\mathbb{Z}$ are in $\{\pm 1 \bmod 8\}$. Then the set of solutions in $\mathcal{O}_K$ to the equation*

$$x_1^2 + x_2^2 + x_3^2 - a x_1 x_2 x_3 = a^{-2}(4 + 2v^2), \text{ with } a \in \mathcal{O}_K$$

is empty.

Proof. It suffices to show that the equation

$$x_1^2 + x_2^2 + x_3^2 - x_1 x_2 x_3 = 4 + 2v^2 \tag{15}$$

has no solutions in $\mathcal{O}_K$. Suppose otherwise and let $(x_1, x_2, x_3) \in \mathcal{O}_K^3$ be a solution. Let $w = 2x_3 - x_1 x_2$, we can now rewrite the equation as

$$w^2 - 8v^2 = (x_1^2 - 4)(x_2^2 - 4). \tag{16}$$

Since all the prime divisors of v are in $\{\pm 1 \bmod 8\}$ they must all be odd. Therefore $4 + 2v^2$ is not divisible by 4. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ above $2\mathbb{Z}$. We now have $4 + 2v^2 \notin \mathfrak{p}^2 \cap \mathbb{Z}$, since $v_{\mathfrak{p}}(2) = 1$. So for each $\mathfrak{p}$ above $2\mathbb{Z}$ at least one $x_i \notin \mathfrak{p}$. If $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are the primes above $2\mathbb{Z}$ in K, we claim that there exists a solution (x_1, x_2, x_3) such that at least one $x_i \notin \mathfrak{p}_j$ for all $j \in \{1, 2, 3\}$. It is easy to see from (15) that if $x_1, x_2 \in \mathfrak{p}_1$ then so is x_3. So let us assume this does not happen and assume that $x_1 \in \mathfrak{p}_1$, $x_2 \in \mathfrak{p}_2$ and $x_3 \in \mathfrak{p}_3$. We now look at the solution given by

$$(x_1, x_2, x_1 x_2 - x_3).$$

Since $x_1 \in \mathfrak{p}_1$ and $x_2 \in \mathfrak{p}_2$, we have that $x_1x_2 - x_3 \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$. But the fact that $x_3 \in \mathfrak{p}_3$ implies that $x_1x_2 - x_3 \notin \mathfrak{p}_i$ for all i. This proves our claim. Now let (x_1, x_2, x_3) be a solution such that $x_1 \notin \mathfrak{p}$ for all primes $\mathfrak{p} \mid 2\mathcal{O}_K$. We now look at the ring homomorphism

$$\begin{aligned} \phi \quad &: \quad \mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}^3 \\ &\quad\quad a \to a \bmod \mathfrak{p}^3. \end{aligned}$$

The kernel is $\mathfrak{p}^3 \cap \mathbb{Z} \supseteq 8\mathbb{Z}$ and since $v_{\mathfrak{p}}(4) = 2$, we have $Ker(\phi) = 8\mathbb{Z}$. We now have the injective map

$$\begin{aligned} \psi \quad &: \quad \mathbb{Z}/8\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}^3 \\ &\quad\quad a \to a \bmod \mathfrak{p}^3. \end{aligned}$$

Finally since the norm of $\mathfrak{p}^3$ is 8 the map is surjective. This implies that since invertible classes must go to invertible classes through ψ,

$$x_1^2 \equiv 1 \bmod \mathfrak{p}^3.$$

If $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are the primes above $2\mathbb{Z}$ in K and $x_1 \notin \mathfrak{p}_i$ for all i, we have

$$x_1^2 \equiv 1 \bmod \mathfrak{p}_i^3$$

for all i. By the Chinese remainder theorem

$$x_1^2 \equiv 1 \bmod 8\mathcal{O}_K \implies x_1^2 - 4 \equiv 5 \bmod 8\mathcal{O}_K.$$

Therefore if the degree of K over $\mathbb{Q}$ is 3

$$\mathfrak{N}(x_1^2 - 4) \equiv 5^3 \bmod 8\mathcal{O}_K \implies \mathfrak{N}(x_1^2 - 4) \equiv 5^3 \bmod 8\mathbb{Z} \implies \mathfrak{N}(x_1^2 - 4) \equiv 5 \bmod 8\mathbb{Z}.$$

Therefore there exists a rational prime p such that

$$p \equiv \pm 5 \bmod 8\mathbb{Z} \text{ such that } p \mid \mathfrak{N}(x_1^2 - 4).$$

By our hypothesis $p \nmid v$. Let $\mathfrak{q}_1$ be a prime in $\mathcal{O}_K$ that lies above p with $\mathfrak{N}(\mathfrak{q}_1) = p^f$ for some natural number f and $\mathfrak{q}_1 \mid (x_1^2 - 4)\mathcal{O}_K$. By (16), 2 is a quadratic residue modulo $\mathfrak{q}_1$. Since the number field is Galois and of degree 3, the exponent f is odd. We now have $p = \pm 5 + 8k$ and therefore

$$p^{2f} = (25 \pm 80k + 64k^2)^f \implies p^{2f} - 1 \equiv 25^f - 1 \bmod 16 \implies \frac{p^{2f} - 1}{8} \equiv \frac{25^f - 1}{8} \bmod 2.$$

However

$$\frac{p^{2f} - 1}{8} \equiv \frac{25^f - 1}{8} \bmod 2 \implies \frac{p^{2f} - 1}{8} \equiv 3 \cdot (25^{f-1} + \cdots + 1) \bmod 2 \equiv 1 \bmod 2.$$

Therefore by Lemma 6.1 we get that 2 is a quadratic non-residue modulo $\mathfrak{q}_1$. This gives us a contradiction. □

Proof of Theorem 1.2. By Lemma 5.3, the above equation has solutions mod $\mathfrak{p}^n$ for all $n \geqslant 1$ and primes not lying above 2, with $\mathfrak{N}(\mathfrak{p}) > 4$ in K. The only other primes are those above 2 and 3. By the remarks after Lemma 5.3 the above equation has solution mod $\mathfrak{p}^n$ for all $n \geqslant 1$ and $\mathfrak{p}$ above 2 and 3. Since the Artin symbol for 2 with respect to $\mathbb{Q}(\zeta_{31})/\mathbb{Q}$ has order 5, the prime 2 splits in K. By Lemma 6.2, we have for $a = 3$ and $v = 23$, the equation in (3) has no global solutions. □

7. Prime factors in Homogenous Markoff equations of Degree 3

Markoff numbers are positive integers which appear in the integral solutions of the Diophantine equation $\mathcal{M} = \mathcal{M}_{3,0} : x^2 + y^2 + z^2 = 3xyz$. They form a sequence starting with $1, 2, 5, 13, 29, 34 \ldots$. A triple of integers (x, y, z) which satisfies $\mathcal{M}$ is called a Markoff triple. We say a triple (x, y, z) is normalized if its coordinates satisfy $0 \leqslant x \leqslant y \leqslant z$. We note that all Markoff triples can be easily retrieved from the set of normalized Markoff triples using permutations and sign changes. The Markoff tree $\mathfrak{M}$ with normalized Markoff triples is constructed by the initial triple $(1, 1, 1)$ and subsequent group action of Γ, the group of affine morphisms of $\mathbb{A}^3$ generated by the permutations and the two Vieta involutions ϕ_1 and ϕ_2 from (4). A nice description of the tree can be found as Figure 2 in [21]. There are two (maximal) branches of the tree which have $m \in \mathfrak{M}\backslash\{1, 2\}$. In fact, the unicity conjecture implies that the tree has exactly two (maximal) branches with a fixed smallest coordinate m: when $m \in \mathfrak{M}\backslash\{1, 2\}$ appears as a triple (a, m, b) in the tree. One branch can be obtained by applying ϕ_1 twice, and ϕ_2 infinitely many times, and the other branch can be obtained by first using ϕ_1, and then ϕ_2 infinitely many times. Hence, for a fixed Markoff number m, we have two branches of the Markoff tree which have m as the lowest term for the triples. When $m = 5$, we have two branches which have 5 as the lowest term of each triple which are

$$(5, 13, 194) - (5, 194, 2897) - (5, 2897, 43261) - (5, 43261, 646018) - \cdots$$

and

$$(5, 29, 433) - (5, 433, 6466) - (5, 6466, 96557) - (5, 96557, 1441889) - \cdots .$$

We summarize the properties of branches of the Markoff tree with fixed smallest coordinates in the following lemma.

Lemma 7.1. *For a fixed Markoff number $m \geqslant 5$, the unicity conjecture implies that there are exactly two maximal branches of the Markoff tree which have m as the lowest term for their triples*

$$\mathfrak{L}^{(j)} : (m, \ell_1^{(j)}, \ell_2^{(j)}) - (m, \ell_2^{(j)}, \ell_3^{(j)}) - \cdots - (m, \ell_n^{(j)}, \ell_{n+1}^{(j)}) - \cdots ,$$

for $j = 1, 2$, then the following are true:

(1) For $i = 1, 2$, it is possible to extend the sequence $\{\ell_n^{(i)}\}_{n\geqslant 0}$ to sequences $\{L_n^{(i)}\}_{n\geqslant 0}$ which satisfy the linear recurrence

$$L_{n+1}^{(i)} = 3mL_n^{(i)} - L_{n-1}^{(i)}, \quad \text{for } n \geqslant 1,$$

such that $L_0^{(1)} = L_0^{(2)} = 1$. Without loss of generality, we assume $L_1^{(1)} \geqslant L_1^{(2)}$.

(2) The terms of the sequences $\{L_n^{(1)}\}_{n\geqslant 0}$ and $\{L_n^{(2)}\}_{n\geqslant 0}$ can be represented as linear combinations of terms of the Lucas sequence $\{\mathcal{L}_n\}_{n\geqslant 0}$ which is defined by

$$\mathcal{L}_0 = 0,\ \mathcal{L}_1 = 1,\ \mathcal{L}_{n+1} = 3m\mathcal{L}_n - \mathcal{L}_{n-1} \quad \text{for } n \geqslant 0. \tag{17}$$

More precisely, for $n \geqslant 0$ and $j = 1, 2$, we can write

$$L_n^{(j)} = L_1^{(j)}\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) - L_0^{(j)}\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) = L_1^{(j)}\mathcal{L}_n - L_0^{(j)}\mathcal{L}_{n-1}, \tag{18}$$

where α and β are numbers which generate the sequence $\{\mathcal{L}_n\}_{n\geqslant 0}$.

(3) We have

$$L_n^{(1)} - L_n^{(2)} = (L_1^{(1)} - L_1^{(2)})\mathcal{L}_n, \quad n \geqslant 0$$
$$L_n^{(1)} + L_n^{(2)} = L_0^{(1)}(\mathcal{L}_{n+1} - \mathcal{L}_{n-1}) = L_0^{(2)}(\mathcal{L}_{n+1} - \mathcal{L}_{n-1}), \quad n \geqslant 1.$$

-

Proof. The first claim naturally follows by backtracking Vieta involutions. To prove (2), we use properties of the Lucas sequences, and we have

$$L_n^{(j)} = (L_1^{(j)} - 3mL_0^{(j)})\mathcal{L}_n + L_0^{(j)}\mathcal{L}_{n+1} = L_1^{(j)}\mathcal{L}_n + (-3m\mathcal{L}_n + \mathcal{L}_{n+1})L_0^{(j)} = L_1^{(j)}\mathcal{L}_n - L_0^{(j)}\mathcal{L}_{n-1},$$

for $j = 1, 2$. The first equality in (3) naturally follows from (2). The second equality can be proved by induction. □

The Lemma 7.1, along with Theorem 3.9 in [6], implies the following.

Theorem 7.2. *Following the notation in Lemma 7.1, let $\{L_n^{(1)}\}_{n\geqslant 0}$ and $\{L_n^{(2)}\}_{n\geqslant 0}$ be two linear recurrence sequences in the Markoff tree following the recurrence relation*

$$L_{n+1}^{(i)} = 3mL_n^{(i)} - L_{n-1}^{(i)}, \quad \text{for } n \geqslant 1 \text{ and } i = 1, 2.$$

Then for sufficiently large integers n, the greatest prime factor of the terms $L_n^{(1)}$ and $L_n^{(2)}$ satisfies

$$P(L_n^{(i)}) \gg \log n \frac{\log\log n}{\log\log\log n}, \quad \text{for } i = 1, 2,$$

where the implied constant depends on the choice of m, the smallest coordinate of triples which contain the terms in $\{L_n^{(1)}\}_{n\geqslant 0}$ and $\{L_n^{(2)}\}_{n\geqslant 0}$.

REFERENCES

[1] M. Aigner. *Markov's theorem and 100 years of the uniqueness conjecture*. Springer, Cham, 2013.

[2] A. Baragar. Asymptotic growth of Markoff-Hurwitz numbers. *Compositio Math.*, 94(1):1–18, 1994.

[3] A. Baragar. The Markoff-Hurwitz equations over number fields. *Rocky Mountain J. Math.*, 35(3):695–712, 2005.

[4] E. Bombieri. Continued fractions and the Markoff tree. *Expo. Math.*, 25(3):187–213, 2007.

[5] J. Bourgain, A. Gamburd, and P. Sarnak. Markoff triples and strong approximation. *C. R. Math. Acad. Sci. Paris*, 354(2):131–135, 2016.

[6] Yann Bugeaud. *Linear forms in logarithms and applications*, volume 28 of *IRMA Lectures in Mathematics and Theoretical Physics*. European Mathematical Society (EMS), Zürich, 2018.

[7] L. Carlitz. Certain special equations in a finite field. *Monatsh. Math.*, 58:5–12, 1954.

[8] Leonard Carlitz. The number of points on certain cubic surfaces over a finite field. *Boll. Un. Mat. Ital. (3)*, 12:19–21, 1957.

[9] W. Chen. Nonabelian level structures, Nielsen equivalence, and Markoff triples. *Accepted for publication in Annals of Mathematics, arXiv:2011.12940*.

[10] J.-L. Colliot-Thélène, D. Wei, and F. Xu. Brauer-Manin obstruction for Markoff surfaces. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 21:1257–1313, 2020.

[11] B. Fine, G. Kern-Isberner, A. I. S. Moldenhauer, and G. Rosenberger. On the generalized Hurwitz equation and the Baragar-Umeda equation. *Results Math.*, 69(1-2):69–92, 2016.

[12] A. Gamburd, M. Magee, and R. Ronan. An asymptotic formula for integer points on Markoff-Hurwitz varieties. *Ann. of Math. (2)*, 190(3):751–809, 2019.

[13] A. Ghosh and P. Sarnak. Integral points on Markoff type cubic surfaces. *Invent. Math.*, 229(2):689–749, 2022.

[14] C. Gurwood. Diophantine approximation and the markoff chain. *PhD thesis, New York University*, 1976.

[15] N. P. Herzberg. On a problem of Hurwitz. *Pacific J. Math.*, 50:485–493, 1974.

[16] A. Hurwitz. Ueber eine Aufgabe der unbestimmten Analysis. *Arch. Math. Phys.*, 3:185–196, 1907.

[17] D. Loughran and V. Mitankin. Integral Hasse principle and strong approximation for Markoff surfaces. *Int. Math. Res. Not. IMRN*, (18):14086–14122, 2021.

[18] A. Markoff. Sur les formes quadratiques binaires indéfinies. *Math. Ann.*, 17(3):379–399, 1880.

[19] M. Mirzakhani. Counting mapping class group orbits on hyperbolic surfaces. *https://doi.org/10.48550/arXiv.1601.03342*, 2016.

[20] J. H. Silverman. The Markoff equation $X^2 + Y^2 + Z^2 = aXYZ$ over quadratic imaginary fields. *J. Number Theory*, 35(1):72–104, 1990.

[21] D. Zagier. On the number of Markoff numbers below a given bound. *Math. Comp.*, 39(160):709–723, 1982.

DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEEN'S UNIVERSITY, KINGSTON, CANADA, ON K7L 3N6.
Email address: sk206@queensu.ca

MATHEMATISCHES INSTITUT, GEORG-AUGUST UNIVERSITÄT GÖTTINGEN, BUNSENSTRASSE 3-5, 37073 GÖTTINGEN, GERMANY
Email address: damaris.schindler@mathematik.uni-goettingen.de

CHENNAI MATHEMATICAL INSTITUTE, H1, SIPCOT IT PARK, SIRUSERI KELAMBAKKAM, CHENNAI, TAMIL NADU, INDIA 603103.
Email address: jyothsnaas@cmi.ac.in