ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 35, Number 3, 2005

THE MARKOFF-HURWITZ EQUATIONS OVER NUMBER FIELDS

ARTHUR BARAGAR

ABSTRACT. Let R be an order in a number field K, and let $\mathcal{M}_{a,n}(R)$ be the set of R-integral solutions to the Markoff-Hurwitz equation $x_1^2 + \cdots + x_n^2 = ax_1 \cdots x_n$, where $a \in R$, $a \neq 0$, and $n \geq 3$. This set can be expressed as the orbit of a fundamental set of solutions $\mathcal{F}_{a,n}(R)$ under the action of a group of automorphisms $\mathcal{A}_{a,n}$. Hurwitz showed that $\mathcal{F}_{a,n}(\mathbf{Z})$ is always finite. Silverman showed that $\mathcal{F}_{a,3}(R)$ is often infinite if the group of units R^* in R is infinite. In this paper, we show that if R^* is infinite and K has a real imbedding, then $\mathcal{F}_{a,n}(R)$ is either empty or infinite. We also show that if K is totally complex and $n \geq 6$, then $\mathcal{F}_{a,n}(R)$ is infinite.

Introduction. The Diophantine equation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = ax_1x_2 \cdots x_n \tag{1}$$

with a a nonzero integer and $n \geq 3$ is known as a Hurwitz or Markoff-Hurwitz equation. Such equations were first studied by Hurwitz [**7**] who thought of them as generalizations of the Markoff equation

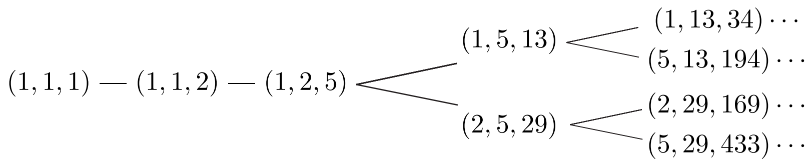
$$x^2 + y^2 + z^2 = 3xyz, \tag{2}$$

which was first studied by Markoff [**8**]. The theory surrounding the Markoff equation is rich and quite extensive, but the property we are interested in here is the following: All integer solutions (x, y, z) with $0 < x \leq y \leq z$ can be generated from the *fundamental solution* $(1, 1, 1)$ and the branching operations

$$\begin{tikzcd}[row sep=small] & (x,z,3xz-y) \\ (x,y,z) \arrow[ur, dash] \arrow[dr, dash] & \\ & (y,z,3yz-x). \end{tikzcd}$$

2000 AMS *Mathematics Subject Classification.* Primary 11D41, 11D72, 11G35.
Received by the editors on July 22, 2002, and in revised form on September 5, 2002.

This gives the tree of solutions that begins:



The set $\mathcal{M}_{3,3}(\mathbf{Z})$ of all integer solutions to the Markoff equation is the set of all triples obtained from the elements of this tree via permutations of the coordinates and sign changes in pairs. It is not too difficult to show a similar result for equation (1) when $a = n$.

Let us be a little more formal. Let $\mathcal{M}_{a,n}(\mathbf{Z})$ denote the set of nontrivial, i.e., $\neq \vec{0}$, integer solutions to equation (1). Let $\mathcal{A}_{a,n}$ be the group of automorphisms generated by the involution

$$\phi : (x_1, x_2, \dots , x_n) \longmapsto (x_1, x_2, \dots , x_{n-1}, ax_1x_2 \cdots x_{n-1} - x_n),$$

permutations of the variables, and the map

$$\psi : (x_1, x_2, \dots , x_n) \longmapsto (-x_1, -x_2, x_3, \dots , x_n),$$

which changes the sign of the first two components. Then the action of $\mathcal{A}_{a,n}$ partitions $\mathcal{M}_{a,n}(\mathbf{Z})$. For each $\mathcal{A}_{a,n}$-orbit of solutions in $\mathcal{M}_{a,n}(\mathbf{Z})$, let us choose a representative of this orbit and let $\mathcal{F}_{a,n} = \mathcal{F}_{a,n}(\mathbf{Z})$ be the set of these representatives, so

$$\mathcal{M}_{a,n}(\mathbf{Z}) = \mathcal{A}_{a,n}(\mathcal{F}_{a,n}).$$

The character of $\mathcal{F}_{a,n}$ has been studied by Hurwitz [**7**], Herzberg [**6**], and myself [**1**]. One of Hurwitz's results is the following:

Theorem 0.1 (Hurwitz). *The set of fundamental solutions $\mathcal{F}_{a,n}$ to a Hurwitz equation is finite for every pair (a, n).*

This result has an intriguing similarity to a deeper result on elliptic curves—the Mordell-Weil theorem: For any number field K, the set of K-rational points on an elliptic curve form an Abelian group of finite rank, see, for example, [**12**]. An outstanding conjecture holds that for any rank r, there are examples of elliptic curves over $\mathbf{Q}$ with rank at least r [**9**]. The analogous question for Hurwitz equations was answered in [**1**]:

Theorem 0.2. *The magnitude of $\mathcal{F}_{a,n}$ is unbounded as a and n vary. That is, for any $k > 0$, there exists a pair (a, n) such that $|\mathcal{F}_{a,n}| \geq k$.*

The simplicity of this result suggests that the above comparison is not fair. In fact, Silverman [**11**] showed a further divergence between these two results. There exist number fields K with integer rings $\mathcal{O}_K$ and pairs $(a, 3)$ such that the number of $\mathcal{A}_{a,3}$-orbits of $\mathcal{O}_K$-integer points is infinite. Precisely, he showed:

Theorem 0.3 (Silverman). *Let $K/\mathbf{Q}$ be a number field, let $R \subset K$ be a finitely generated $\mathbf{Z}$-subalgebra of K, and let $a \in R$, $a \neq 0$. Suppose that R has the following two properties*:

(1) *The group R^* of units in R is infinite.*

(2) *There exist units $u, v \in R^*$ satisfying $u^2 + v^2 + 1 \equiv 0 \pmod{aR}$.*

Then for every finite set $S \subset \mathcal{M}_{a,3}(R)$,

$$\mathcal{M}_{a,3}(R) \not\subset \mathcal{A}_{a,3}(S).$$

In this paper we improve on this result in several ways. We first note that Silverman's proof does not extend to the Hurwitz equations with $n > 3$, since it relies on a bijection between the Markoff surface and a torus, and that the proof involves a deep result due to Evertse [**5**]. In this paper our first main result is an elementary proof of the following theorem, which appears in Section 2.

Theorem 2.3. *Let $K/\mathbf{Q}$ be a number field, let R be an order in K, let $a \in R$ and $a \neq 0$. Suppose K has a real imbedding and $K \neq \mathbf{Q}$ (so R^* is infinite). Then $\mathcal{F}_{a,n}(R)$ is either empty or infinite.*

The central idea in this proof is a density argument. We show that an orbit of a point is discrete, in the topology induced by $\mathbf{R}$, and that $\mathcal{M}_{a,n}(R)$ is either empty or it includes a cluster point. Hence, if $\mathcal{M}_{a,n}(R) \neq \varnothing$, then there must be an infinite set of orbits in $\mathcal{M}_{a,n}(R)$.

In Section 3 we give an example that demonstrates that it is possible for $\mathcal{F}_{a,n}(R)$ to be empty.

In Section 4 we give the following complementary result for orders in totally complex fields.

Theorem 4.2. *Suppose R is an order in a totally complex number field K, $a \in R$, and $n \geq 6$. Then $\mathcal{F}_{a,n}(R)$ is infinite.*

In the conditions of this theorem, note that we do not require that R^* be infinite, and in the conclusion, there is no possibility that $\mathcal{F}_{a,n}(R)$ is empty. The proof exploits properties of orders in totally complex fields. We also give an example that demonstrates that it is possible for $\mathcal{F}_{a,n}(R)$ to be empty with R an order in a totally complex field and R^* infinite. When R^* is finite (so K is imaginary quadratic), Silverman [**11**] showed that it is possible for $\mathcal{F}_{a,3}(R)$ to be any one of empty, finite but not empty, or infinite.

1. Orbits in the reals are discrete.

Let us begin with a classical analysis of the Hurwitz equations over the reals. Without loss of generality, we may assume $a > 0$. To investigate an $\mathcal{A}_{a,n}$-orbit, it is enough to investigate the positive ordered solutions—those solutions $\vec{x} = (x_1, \dots, x_n)$ to equation (1) with $0 < x_1 \leq x_2 \leq \cdots \leq x_n$. All other solutions in the $\mathcal{A}_{a,n}$-orbit are derived from these via permutations and sign changes. Consider the maps $\phi_i \in \mathcal{A}_{a,n}$ for $i = 1, \dots, n$ defined by

$$\phi_i(\vec{x}) = (x_1, \dots, \hat{x}_i, \dots, x_{n-1}, (ax_1 \cdots x_n / x_i) - x_i)\,,$$

where the hat indicates that that component is omitted. If $\vec{x}$ is a positive ordered solution, then so is $\phi_i(\vec{x})$ for $i = 1, \dots, n-1$. To see this, let us look at ϕ_i, and suppose $x_n \geq x_i' = (ax_1 \cdots x_n / x_i) - x_i$. Then

$$ax_1 \cdots x_n \leq x_i^2 + x_i x_n \leq x_i^2 + x_n^2 < x_1^2 + \cdots + x_n^2 = ax_1 \cdots x_n,$$

which is a contradiction. Thus $x_i' > x_n$, so $\phi_i(\vec{x})$ is a positive ordered solution. This gives these solutions a natural tree structure. Two positive ordered solutions $\vec{x}$ and $\vec{y}$ are connected if there exists an i such that $\phi_i(\vec{x}) = \vec{y}$ or $\vec{x} = \phi_i(\vec{y})$. We call two connected solutions *neighbors*. We define a height h on solutions to equation (1) by

$$h(\vec{x}) = \max_i\{|x_i|\}.$$

Note that, for a positive ordered solution $\vec{x}$, we have $h(\vec{x}) = x_n$. From a solution $\vec{x}$ in the tree of positive ordered solutions, we can go up the tree (that is, to a solution with larger height) by applying one of the branching operations ϕ_i for $i = 1, \ldots, n-1$. If we can go down the tree, then this is achieved by applying $\phi_n = \phi$ and the permutation that suitably reorders the components. If, in a tree, there exists a solution $\vec{x}$ such that $h(\phi(\vec{x})) \geq h(\vec{x})$, then we call this solution the *fundamental solution*. Fundamental solutions are unique. In the classical case, it is clear that they exist, since we cannot descend indefinitely. This is also true over the reals, though it is not so obvious. It is a corollary of the following lemma:

Lemma 1.1. *Let $\vec{x}$ be a positive ordered solution to equation* (1) *and suppose $h(\phi_n(\vec{x})) < h(\vec{x})$. Then either $\phi_n(\vec{x})$ is a fundamental solution, or*

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

Proof. We begin by noting that

$$\begin{aligned} x_1^2 + \cdots + x_n^2 &= ax_1 \cdots x_n \\ x_1^2 + \cdots + x_{n-2}^2 + (x_{n-1} - x_n)^2 &= (ax_1 \cdots x_{n-2} - 2)x_{n-1}x_n \end{aligned}$$

so

$$ax_1 \cdots x_{n-2} \geq 2.$$

Also, by the arithmetic-geometric inequality,

$$\begin{aligned} x_1^2 + \cdots + x_{n-2}^2 &\geq (n-2)(x_1 \cdots x_{n-2})^{2/(n-2)} \\ &\geq (n-2)\left(\frac{2}{a}\right)^{2/(n-2)}. \end{aligned}$$

Since $h(\phi_n(\vec{x})) < h(\vec{x})$, we know

$$\begin{aligned} ax_1\cdots x_{n-1} - x_n &< x_n \\ ax_1\cdots x_n &< 2x_n^2 \\ x_1^2+\cdots+x_n^2 &< 2x_n^2 \\ x_1^2+\cdots+x_{n-2}^2+(x_{n-1}-x_n)^2 &< 2x_n(x_n-x_{n-1}) \\ \frac{n-2}{2x_n}\left(\frac{2}{a}\right)^{2/(n-2)} &< x_n - x_{n-1}. \end{aligned}$$

Finally, if $x_n' = ax_1\cdots x_{n-1} - x_n > x_{n-1}$, then $\phi_n(\vec{x})$ is a positive ordered solution. But then $\phi_n(\phi_n(\vec{x})) = \vec{x}$, so $h(\phi_i(\phi_n(\vec{x}))) > h(\phi_n(\vec{x}))$ for all i. That is $\phi_n(\vec{x})$ is a fundamental solution. Thus, if $\phi_n(\vec{x})$ is not a fundamental solution, then $x_n' \le x_{n-1}$, so $h(\phi_n(\vec{x})) = x_{n-1}$. Thus,

$$\frac{n-2}{2h(\vec{x})}\left(\frac{2}{a}\right)^{2/(n-2)} < x_n - x_{n-1} = h(\vec{x}) - h(\phi_n(\vec{x})). \qquad \square$$

Corollary 1.2. *Let $\vec{x}$ be a positive ordered solution to equation* (1). *Then there exists a fundamental solution $\vec{r} \in \mathcal{A}_{a,n}(\vec{x})$ and a sequence of positive ordered solutions $\vec{x} = \vec{x}_0, \dots, \vec{x}_m = \vec{r}$ such that $\vec{x}_{i-1}$ and $\vec{x}_i$ are neighbors for $i = 1, \dots, m$ and*

$$m < \frac{2(h(\vec{x})^2)}{n-2}\left(\frac{a}{2}\right)^{2/(n-2)} + 1.$$

Proof. Let $\vec{x}_0, \dots, \vec{x}_m$ be any sequence of neighbors with descending height. Then, by repeatedly applying Lemma 1.1, we get

$$h(\vec{x}) > \frac{n-2}{2}\left(\frac{2}{a}\right)^{2/(n-2)}\left(\frac{1}{h(\vec{x}_0)} + \frac{1}{h(\vec{x}_1)} + \cdots + \frac{1}{h(\vec{x}_{m-2})}\right) + h(\vec{x}_{m-1}).$$

Since $h(\vec{x}_i) < h(\vec{x})$, we get

$$h(\vec{x}) > \frac{n-2}{2}\left(\frac{2}{a}\right)^{2/(n-2)}\frac{m-1}{h(\vec{x})} + h(\vec{x}_{m-1})$$

so

$$\frac{2h(\vec{x})^2}{n-2}\left(\frac{a}{2}\right)^{2/(n-2)} + 1 > m.$$

Thus, m is bounded, so such a sequence cannot continue indefinitely. That is, there must exist a fundamental solution. □

Corollary 1.3. *Let $\vec{x}$ be a nontrivial solution to equation* (1). *Then $\mathcal{A}_{a,n}(\vec{x})$ has no cluster points.*

Proof. Suppose $\mathcal{A}_{a,n}(\vec{x})$ has a cluster point $\vec{u}$. Then there exist an infinite number of elements $\vec{y}$ in $\mathcal{A}_{a,n}(\vec{x})$ such that $h(\vec{y}) < h(\vec{u}) + 1$. But, by the previous result, there can be at most

$$\sum_{k=0}^{m}(n-1)^k$$

positive ordered solutions with height less than $h(\vec{u}) + 1$, where

$$m = \frac{2((h(\vec{u})+1)^2)}{n-2}\left(\frac{a}{2}\right)^{2/(n-2)} + 1. \qquad \square$$

2. Cluster points of solutions over R. Let us begin with a nontrivial real solution $\vec{p}$ to equation (1) and consider the equation

$$x^2 + y^2 + p_3^2 + \cdots + p_n^2 = ap_3 \cdots p_n xy. \tag{3}$$

Let us set

$$\begin{aligned} A &= ap_3 \cdots p_n \\ B &= p_3^2 + \cdots + p_n^2. \end{aligned}$$

Since $\vec{p} \in \mathbf{R}^n$ and $n \geq 3$, we know $B > 0$, and hence, since

$$(x-y)^2 + B = (A-2)xy,$$

we get $A > 2$. Consider the quadratic equation

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

which has real roots since $A > 2$. Let those roots be ω and ω^{-1}, where $\omega > 1$. With these definitions, we can rewrite equation (3) as

$$(x - \omega y)(x - \omega^{-1} y) = -B. \tag{4}$$

If $\vec{p}$ is a solution over an order R in a real number field K, and $\omega \notin K$, then we can rewrite equation (4) as a norm equation:

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

where $L = K[\omega]$. Let $S = R \oplus \omega R$. Then S is an order in L. Let S^* be its group of units, and define

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

If $u \in S_1^*$, then

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

so $u(x - \omega y) = x' - \omega y' \in S$ gives a new solution (x', y') to equation (3). This gives us a new way of finding more solutions. Our traditional method is to use the action of the subgroup of $\mathcal{A}_{a,n}$ that fixes $x_3, \dots, x_n$. This action is induced by conjugation in L/K, and multiplication by -1 and $\omega \in S_1^*$. Thus, our observation is useful only if $\operatorname{rank}(S_1^*) \geq 2$.

Theorem 2.1. *Suppose R is an order in a number field K, and K is neither $\mathbf{Z}$ nor imaginary quadratic (so R^* is infinite). Suppose also that $\omega^2 - A\omega + 1 = 0$ where $A \in R$ and $\omega \notin K$. Set $L = K(\omega)$ and $S = R \oplus \omega R$. Finally, suppose every real imbedding τ of K in $\mathbf{C}$ satisfies $|\tau(A)| > 2$. Then*

$$\operatorname{rank}(S_1^*) \geq 2.$$

Proof. Recall [**3**, Chapter II.4] that

$$\begin{aligned} \operatorname{rank}(R^*) &= r_K + s_K - 1 \\ \operatorname{rank}(S^*) &= r_L + s_L - 1 \end{aligned}$$

where r_K, $2s_K$, r_L, and $2s_L$ are the number of real and complex imbeddings of K and L in $\mathbf{C}$.

We find the rank of S_1^* by considering

$$1 \longrightarrow S_1^* \hookrightarrow S^* \xrightarrow{N_{L/K}} R^*$$

from which we get

$$\begin{aligned}\operatorname{rank}(S_1^*) &\geq \operatorname{rank}(S^*) - \operatorname{rank}(R^*) \\ &\geq r_L + s_L - r_K - s_K.\end{aligned} \tag{5}$$

Let τ be a real imbedding of K. Since $\omega^2 - A\omega + 1 = 0$, we know

$$\tau(\omega)^2 - \tau(A)\tau(\omega) + 1 = 0,$$

and since $\tau(A) > 2$, we know $\tau(\omega)$ is real, so the two extensions of τ to imbeddings of L in $\mathbf{C}$ are real. Thus $r_L = 2r_K$ and $s_L = 2s_K$. Hence,

$$\operatorname{rank}(S_1*) = r_K + s_K = \operatorname{rank}(R^*) + 1 \geq 2. \qquad \square$$

Let us now use this abundance of units to show that the solutions are dense.

Theorem 2.2. *Suppose R is an order in a number field K and that R^* is infinite. Suppose $A \in R$ and $\tau(A) > 2$ for all real imbeddings τ of K in $\mathbf{R}$. Let ω satisfy $\omega^2 - A\omega + 1 = 0$ and suppose $\omega \notin K$. Finally, suppose $(p_1, p_2) \in R^2$ is a solution to*

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

where B is in R. Then (p_1, p_2) is a cluster point of solutions to equation (6).

Proof. Let

$$\beta = p_1 - \omega p_2,$$

so $N_{L/K}(\beta) = -B$. Let u be a unit in S_1^*. Then $u\beta = x - \omega y$ where x, $y \in R$ and (x, y) satisfies equation (6). Let us solve for x and y in terms of u, $\bar{u}$, β, and $\bar{\beta}$, where the bar represents conjugation in L over K. We get:

$$\begin{aligned}u\beta &= x - \omega y \\ \bar{u}\bar{\beta} &= x - \bar{\omega} y = x - \omega^{-1} y \\ x &= \frac{\omega\bar{u}\bar{\beta} - \omega^{-1}u\beta}{\omega - \omega^{-1}} \\ y &= \frac{\bar{u}\bar{\beta} - u\beta}{\omega - \omega^{-1}}.\end{aligned}$$

We now consider the proximity of (x,y) to (p_1,p_2). Note that we can write

$$\begin{aligned} p_1 &= \frac{\omega\bar{\beta} - \omega^{-1}\beta}{\omega - \omega^{-1}} \\ p_2 &= \frac{\bar{\beta} - \beta}{\omega - \omega^{-1}}, \end{aligned}$$

so

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

Hence, if $|u-1|$ and $|\bar{u}-1|$ are small, then (x,y) is close to (p_1,p_2).

Since rank $(S_1^*) \ge 2$, there exist two linearly independent units v_1 and v_2 in S_1^*. That is, $v_1^k v_2^l = 1$ with $k,l \in \mathbf{Z}$ if and only if $k = l = 0$. Let us write $v_j = e^{2\pi i \alpha_j}$. Then we get $k\alpha_1 + l\alpha_2 + m = 0$ with $k,l,m \in \mathbf{Z}$ if and only if $k = l = m = 0$. Hence α_1, α_2 and 1 are linearly independent over $\mathbf{Q}$, and the subset of $\mathbf{C}$ spanned by α_1, α_2, and 1 is dense at 0. Consequently, 1 is a cluster point of S_1^*.

Further, if u is a unit in S_1^*, then $1 = N_{L/K}(u) = u\bar{u}$, so $\bar{u} = u^{-1}$. Hence, if u is close to 1, so $|u-1|$ is small, then so is u^{-1}. Thus, given any neighborhood U of (p_1,p_2) in R^2, we can find an infinite set of units u in S_1^* so that the (x,y) produced above is in U. Hence (p_1,p_2) is a cluster point of the solutions of equation (6) over R. □

We are now ready to prove our main result:

Theorem 2.3. *Let $K/\mathbf{Q}$ be a number field, let R be an order in K, let $a \in R$ and $a \neq 0$. Suppose K has a real imbedding and $K \neq \mathbf{Q}$ (so R^* is infinite). Then $\mathcal{F}_{a,n}(R)$ is either empty or infinite.*

Proof. Suppose equation (1) has a nontrivial solution $\vec{p}$. As before, consider equation (6) where $A = ap_3 \cdots p_n$ and $B = p_3^2 + \cdots + p_n^2$. Then (p_1, p_2) is a solution to equation (6) and $\tau(A) > 2$ for all real imbeddings τ of K. Let ω satisfy $\omega^2 - A\omega + 1 = 0$. If $\omega \notin K$, then by Theorem 2.2, $\vec{p}$ is a cluster point for solutions to equation (1) over R.

If $\omega \in K$, then the factorization

$$p_1^2 + p_2^2 - Axy = (p_1 - \omega p_2)(p_1 - \omega^{-1} p_2)$$

is over R. Let us set $\beta_1 = p_1 - \omega p_2$ and $\beta_2 = p_1 - \omega^{-1} p_2$. Then, for any $u \in R^*$,

$$(u\beta_1)(u^{-1}\beta_2) = -B.$$

Let us set $x - \omega y = u\beta_1$ and $x - \omega^{-1} y = u^{-1}\beta_2$. Then, solving for x and y, we get

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

It is clear that x and y are in K, but they may not be in R. However, setting $u = 1$, we get p_1 and p_2, which are in R, so we know x and y are in R if $u \equiv 1 \pmod{\omega - \omega^{-1}}$. So consider the group

$$R^*_{\omega - \omega^{-1}} = \{u \in R^* : u \equiv 1 \pmod{\omega - \omega^{-1}}\},$$

which has finite index in R^*, so has the same rank as R^*. Thus, $\operatorname{rank}(R^*_{\omega-\omega^{-1}}) \geq 2$ and, as in the proof of Theorem 2.2, (p_1, p_2) is a cluster point of the solutions to equation (6) over R. Hence, $\vec{p}$ is a cluster point for the solutions to equation (1) over R.

We are now left with the possibility that $\operatorname{rank}(R^*) = 1$. In this case, let us assume, without loss of generality, that R^* is already imbedded in the reals. Let $\vec{p}$ be a positive ordered solution to equation (1) over R, and consider the equation

$$\text{(7)} \qquad \begin{gathered} x^2 + y^2 + z^2 + p_4^2 + \cdots + p_n^2 = ap_4 \cdots p_n xyz \\ x^2 + y^2 + z^2 + B' = A'xyz. \end{gathered}$$

Then A', $B' \geq 0$. Let $\omega(z)$ satisfy $\omega(z)^2 - A'z\omega(z) + 1 = 0$. If $\omega(z) \notin K$ for some z, then we are done, so suppose $\omega(z) \in K$ for all z. Then $\omega(z) \in R^*$ and $\omega(z) > 0$, since $A'z \geq 0$. Since $\operatorname{rank}(R^*) = 1$, there exists a fundamental solution $u \in R^*$ such that $R^* = \{\pm u^k : k \in \mathbf{Z}\}$. Thus,

$$\omega(z) = u^{k(z)}$$

for some $k(z) \in \mathbf{Z}$. Since $A'z = \omega(z) + \omega(z)^{-1}$, we get

$$z = \frac{u^{k(z)} + u^{-k(z)}}{A'}.$$

There are similar formulas for x and y. Given $M > 0$, we can go far enough up the tree of solutions, reordered so that $p_n < x < y < z$, such that $x > (M+1)/A'$. Then

$$\begin{aligned} u^{k(x)} + u^{-k(x)} &> M + 1 \\ u^{k(x)} &> M + 1 - u^{-k(x)} > M. \end{aligned}$$

Let us go up one more step, to get $x' = A'yz - x > z$. Then

$$\begin{aligned} x' + x &= A'yz\frac{u^{k(x')} + u^{-k(x')}}{A'} + \frac{u^{k(x)} + u^{-k(x)}}{A'} \\ &= A'\frac{u^{k(y)} + u^{-k(y)}}{A'}\frac{u^{k(z)} + u^{-k(z)}}{A'}\ u^{k(x')} \\ &\quad + u^{-k(x')} + u^{k(x)} + u^{-k(x)} \\ &= u^{k(y)+k(z)} + u^{k(y)-k(z)} + u^{k(z)-k(y)} + u^{-k(y)-k(z)}. \end{aligned}$$

Let us divide through by $u^{k(y)+k(z)}$, to get

$$\begin{aligned} u^{k(x')-k(y)-k(z)} + u^{-k(x')-k(y)-k(z)} + u^{k(x)-k(y)-k(z)} + u^{-k(x)-k(y)-k(z)} \\ = 1 + u^{-2k(z)} + u^{-2k(y)} + u^{-2k(y)-2k(z)}. \end{aligned}$$

Note that $0 < u^{k(x)-k(y)-k(z)} < u^{-k(z)} < 1/M$, and that most of the other terms are similar, giving us

$$1 - \frac{3}{M} < u^{k(x')-k(y)-k(z)} < 1 + \frac{3}{M}.$$

If M is sufficiently large, then we must have

$$k(x') - k(y) - k(z) = 0.$$

Plugging this relation into the formula for x', and plugging this and the formulas for y and z into equation (7), we find that most terms cancel, and we are left with

$$4 + B'(A')^2 = 0,$$

which is a contradiction, since $B' \geq 0$. Thus, there must exist a z such that $\omega(z) \notin K$, and we are done. □

3. An example. For an order R in a number field K, it is not difficult to find a pair (a, n) so that $\mathcal{M}_{a,n}(R) \neq \varnothing$. For example, the Markoff equation ($a = n = 3$) has the solution $(1, 1, 1)$, and since $\mathbf{Z} \subset R$ for all R, we know $M_{3,3}(R) \neq \varnothing$. Thus, if K has a real imbedding and $R \neq \mathbf{Z}$, then $\mathcal{F}_{3,3}(R)$ is infinite.

In the following example, we show the other extreme is also possible. That is, there exists an order R in a real field K and a pair (a, n) such that $\mathcal{F}_{a,n}(R)$ is empty.

Theorem 3.1. *For an order R in a number field K, the equation*

$$x^2 + y^2 + z^2 = 2xyz$$

has no solutions, other than $\vec{0}$, over the ring R if there exists $\gamma \in R$ such that $|N_{K/\mathbf{Q}}(\gamma)| = 2$ and 2 is unramified in R.

Proof. Since $|N_{K/\mathbf{Q}}(\gamma)| = 2$ there are two residue classes modulo γR, and they can be represented by 0 and 1.

Assume $(x, y, z), \neq \vec{0}$, is a solution in $M_{2,3}(R)$. Then there exists a $k \geq 0$ such that γ^k divides x, y and z, but γ^{k+1} does not divide all three. Note that

$$\left(\frac{x}{\gamma^k}\right)^2 + \left(\frac{y}{\gamma^k}\right)^2 + \left(\frac{z}{\gamma^k}\right)^2 = 2\gamma^k \left(\frac{x}{\gamma^k}\right)\left(\frac{y}{\gamma^k}\right)\left(\frac{z}{\gamma^k}\right).$$

So $(x_1, y_1, z_1) = [x/(\gamma^k), y/(\gamma^k), z/(\gamma^k)]$ is a solution in $M_{2\gamma^k,3}(R)$ and $(x_1, y_1, z_1) \not\equiv (0, 0, 0) \pmod{\gamma R}$. For convenience, let us drop the subscripts. Modulo γR, $M_{2\gamma^k,3}$ becomes

$$x^2 + y^2 + z^2 \equiv 0 \pmod{\gamma R}.$$

Clearly, this is only possible if exactly one of $\{x, y, z\}$ is 0 modulo γR, since not all three are 0. But then $2xyz \equiv 0 \pmod{\gamma^2 R}$, since γ divides 2. Hence we get

$$2 \equiv 0 \pmod{\gamma^2 R}.$$

But 2 is unramified in $K/\mathbf{Q}$, so γ^2 does not divide 2. Hence $2 \not\equiv 0 \pmod{\gamma^2 R}$, (x, y, z) could not have existed, and $M_{2,3}(R) = \varnothing$. □

So we need only find an R and γ: Consider $\gamma = (3 + \sqrt{17})/2$ in $R = \mathbf{Z}[\gamma] \subset K = \mathbf{Q}(\sqrt{17})$. Note that $N_{K/\mathbf{Q}}(\gamma) = -2$, and since $\operatorname{disc}(K/\mathbf{Q}) = 17$, we know 2 is unramified in R. Hence, by Theorem 3.1, $M_{2,3}(R)$ is empty.

4. The totally complex case. The imaginary quadratic case for $n = 3$ was studied by Silverman [**11**]. The behavior is similar to the behavior over $\mathbf{Z}$, and the generalizations to $n \geq 4$ are straightforward.

If K is totally complex but not imaginary quadratic, and R is an order in K, then $\operatorname{rank}(R^*) \geq 1$. Our analysis in Section 2 is applicable to this case, though the $\operatorname{rank}(R^*) = 1$ case in the proof of Theorem 2.3 must be modified. The arguments in Section 1 depend on there being a real imbedding, and it is not clear that the analogous results are even true for orders in totally complex fields. However, such orders have unique properties that can be exploited to produce partial results.

Theorem 4.1. *Suppose R is an order in a totally complex field K and suppose $a \in R$. Suppose there exists a solution $\vec{r}$ of equation* (1) *such that $r_1 = 0$ and $\vec{r} \neq \vec{0}$. Then $\mathcal{F}_{a,n}(R)$ is infinite.*

Proof. This proof uses an idea due to Silverman [**11**]. Let $I(\vec{r})$ be the smallest ideal in R that contains all the components of $\vec{r}$. Note that $I(\sigma\vec{r}) = I(\vec{r})$ for all $\sigma \in \mathcal{A}_{a,n}$, so $I(\vec{r}) = I(\vec{x})$ for all $\vec{x} \in \mathcal{A}_{a,n}(\vec{r})$. Since $\vec{r} \neq \vec{0}$, $I(\vec{r}) \neq 0$. Hence, $I(\vec{r}) \neq I(t\vec{r})$ for any nonzero non unit $t \in R$. But since $r_1 = 0$, $t\vec{r}$ is a solution to equation (1). Since there are an infinite number of t that generate different ideals $I(t\vec{r})$, and each $t\vec{r}$ produces a different $\mathcal{A}_{a,n}$-orbit, the set $\mathcal{F}_{a,n}(R)$ must be infinite. □

Note that the above result applies to imaginary quadratic fields too, so we do not need rank$(R^*) \geq 1$. The reader might also notice that the condition that K is totally complex is not used in the proof. However, this condition is necessary if there is to exist such an $\vec{r}$. Let us also note that the theorem is not vacuous, since such an $\vec{r}$ exists if $i \in R$. In fact, if n is large enough, such an $\vec{r}$ always exists:

Theorem 4.2. *Suppose R is an order in a totally complex number field K, $a \in R$, and $n \geq 6$. Then $\mathcal{F}_{a,n}(R)$ is infinite.*

To prove this result, we will use a couple of known results:

Theorem 4.3 (The Hasse-Minkowski theorem [**10**, Chapter IV]). *A quadratic form f represents* 0 *if and only if the form f_v represents* 0 *for all valuations v. That is, a quadratic form has a global zero if and only if f has everywhere a local zero.*

Theorem 4.4 [**10**, Chapter IV]. *If f_v is a quadratic form of rank at least* 5*, and v is a finite valuation, then f_v represents zero.*

Proof of Theorem 4.2. By Theorem 4.4, the equation

$$x_1^2 + \cdots + x_5^2 = 0 \tag{8}$$

has a solution at every finite valuation. Since K is totally complex, the completion at every infinite valuation is $\mathbf{C}$, and equation (8) clearly has a solution in $\mathbf{C}$. Hence, by Theorem 4.3, there exists a solution to equation (8) over K. By multiplying through by an appropriate element of R, we obtain a solution over R. Now, append zeros to this solution to get a solution $\vec{r}$ of equation (1). Then $\mathcal{F}_{a,n}(R)$ is infinite, by Theorem 4.1. □

Note that, if two of the components of $\vec{r}$ are zero, then the orbit $\mathcal{A}_{a,n}(\vec{r})$ is finite. One might consider this to be a bit unsatisfying, but with a little work, we can derive an infinite orbit.

Lemma 4.5. *Suppose R is an order in a totally complex number field K with* rank$(R^*) \geq 1$. *Then for any nonzero $a \in R$, there exist* *non-zero x, $y \in R$ so that*

$$x^2 + y^2 = a^2.$$

Proof. We first assume $i \notin K$. Then let $L = K(i)$, and let $S = R[i]$. Since K is totally complex, $\operatorname{rank}(R^*) = s_K - 1$ and $\operatorname{rank}(S^*) = 2s_K - 1$, so $\operatorname{rank}(S_1^*) \geq s_K = \operatorname{rank}(R^*) + 1 \geq 2$. Hence there exists a unit $\omega \in S_1^*$ so that $\omega \notin R$, and we can write

$$\omega a = x + iy$$

where $x, y \in R$ are nonzero. Thus

$$\begin{aligned} x^2 + y^2 &= N_{L/K}(\omega a) \\ &= a^2, \end{aligned}$$

as desired.

If $i \in K$, then choose a unit ω in R^* such that $\omega \equiv 1 \pmod 2$ and $\omega \neq \pm 1$ or $\pm i$. Now set

$$\begin{aligned} x + iy &= \omega a \\ x - iy &= \omega^{-1} a \end{aligned}$$

so

$$x^2 + y^2 = a^2,$$

where

$$\begin{aligned} x &= \frac{(\omega + \omega^1)a}{2} \\ y &= \frac{(\omega - \omega^{-1})a}{2}. \end{aligned}$$

Since $\omega \equiv 1 \pmod 2$, both x and y are in R. Also, since $\omega \neq \pm 1$ or $\pm i$ and $a \neq 0$, neither x nor y is zero. □

Lemma 4.6. *Suppose $\vec{r}$ is a solution to equation* (1)*, $|r_1| \leq |r_2| \leq \cdots \leq |r_n|$, $r_2 \neq 0$, and $|ar_2 \cdots r_{n-1}| > 2$. Then $\mathcal{A}_{a,n}(\vec{r})$ is infinite.*

Proof. Note that

$$r_1' = ar_2 \cdots r_n - r_1$$

satisfies

$$\begin{aligned} |r_1'| &\geq |ar_2 \cdots r_{n-1}||r_n| - |r_1| \\ &> 2|r_n| - |r_n| = |r_n|. \end{aligned}$$

Thus, the solution $\vec{r}' = (r_2, \ldots , r_n, r_1')$ has height strictly larger than $h(\vec{r})$ (using the height $h(\vec{x}) = \max\{|x_i|, i = 1, \ldots , n\}$), and $\vec{r}'$ satisfies the same conditions. Thus, by repeating this process, we obtain an infinite chain of solutions to equation (1) in $\mathcal{A}_{a,n}(\vec{r})$. □

Given a solution $\vec{r} \neq \vec{0}$ to equation (1) with two or more components equal to zero, we can use Lemma 4.5 to obtain a new solution $\vec{r}'$ that has only one component equal to zero. We can then reorder the components of this solution and multiply by a suitably large element of R to arrive at a solution that satisfies the conditions of Lemma 4.6. Thus, if there exists a solution $\vec{r} \neq \vec{0}$ with at least one component equal to zero, then there exists an infinite number of infinite orbits of solutions.

Finally, let us point out that the opposite extreme can occur. That is, there exists an order R in a totally complex field K and a pair (a, n) such that $a \in R$, $\operatorname{rank}(R^*) \geq 1$, and $\mathcal{F}_{a,n}(R) = \varnothing$. Let α be a root of

$$f(x) = x^4 + x + 2.$$

Set $K = \mathbf{Q}(\alpha)$ and let $R = \mathcal{O}_K$ be the ring of integers in K. Note that $f(x)$ is irreducible over $\mathbf{Q}$, so $[K : \mathbf{Q}] = 4$. Note that $N(\alpha) = 2$, the constant term of $f(x)$. Note also that $f(x) > 0$ for all $x \in \mathbf{R}$, so K is totally complex and $\operatorname{rank}(R^*) = 1$. Lastly,

$$\operatorname{disc}(K/\mathbf{Q}) = N_{K/\mathbf{Q}}(f'(\alpha)) = N_{K/\mathbf{Q}}(4\alpha^3 + 1) \equiv 1 \pmod{\alpha},$$

so α does not divide $\operatorname{disc}(K/\mathbf{Q})$. Hence, 2 does not divide $\operatorname{disc}(K/\mathbf{Q})$, so 2 is unramified in K. Now, using Theorem 3.1 with $\gamma = \alpha$, we know $\mathcal{F}_{2,3}(R) = \varnothing$.

REFERENCES

1. A. Baragar, *Integral solutions of Markoff-Hurwitz equations*, J. Number Theory **49** (1994), 27–44.

2. ———, *The exponent of the Markoff-Hurwitz equations*, Pacific J. Math. **182** (1998), 1–21.

3. Z. Borevich and I. Shafarevich, *Number theory*, Academic Press, New York, 1996.

4. J.W.S. Cassels, *An Introduction to Diophantine approximation*, Chapter II, Cambridge Univ. Press, Cambridge, 1957.

5. J. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. **53** (1984), 225–244.

6. N.P. Herzberg, *On a problem of Hurwitz*, Pacific J. Math. **50** (1974), 485–493.

7. A. Hurwitz, *Über eine Aufgabe der unbestimmten analysis*, Arch. Math. Phys. **3** (1907), 185–196. Also in *Mathematisch Werke* Vol. 2, Chapter LXX, A. Hurwitz, 1933 and 1962, pp. 410–421.

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

9. B. Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. **14** (1986), 207–259.

10. J. Serre, *A course in arithmetic*, Springer Verlag, New York, 1973.

11. J.H. Silverman, *The Markoff equation $x^2 + y^2 + z^2 = axyz$ over quadratic imaginary fields*, J. Number Theory, **37** (1990), 72–104.

12. ———, *The arithmetic of elliptic curves*, Springer Verlag, New York, 1986.

University of Nevada Las Vegas, Las Vegas, NV 89154-4020
E-mail address: baragar@unlv.nevada.edu