Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 25, 2019, No. 3, 21–35
DOI: 10.7546/nntdm.2019.25.3.21-35

Direct parametrization of Pythagorean triples

Sungkon Chang

Department of Mathematics, Georgia Southern University, Armstrong Campus
11935 Abercorn St, Savannah GA, U.S.A.
e-mail: schang@georgiasouthern.edu

Received: 9 September 2018 **Revised:** 18 April 2019 **Accepted:** 22 July 2019

Abstract: If the two axes of symmetry of a quadratic form in two variables have integer coefficients, the reflection across the axes defines a group action on the primitive solutions of the Diophantine equation defined by the quadratic form. In this paper, we introduce quadratic forms with rational axes of symmetry that admit a single set of polynomials which parametrize their primitive solutions up to the reflections.
Keywords: Parametrization of primitive solutions
2010 Mathematics Subject Classification: 11D09.

1 Introduction

A solution $(a_1, \ldots, a_n)$ to a Diophantine equation given by a homogeneous polynomial in n variables is called a *primitive solution* if $\gcd(a_1, \ldots, a_n)$ is 1. The equation $x^2 + y^2 = z^2$ asserted by the Pythagorean theorem has infinitely many primitive solutions such as $(3, 4, 5)$. From a geometric point of view, the task is to find all triangles that have integer side lengths and have an inner angle $\theta = 90°$. Having an equilateral triangle in mind, we may ask ourselves a similar question. How can we find all triangles that have integer side lengths and have an inner angle $\theta = 60°$? Our work is motivated from this consideration, and in general, it is a problem of finding integer solutions to $x^2 - 2xy\cos\theta + y^2 = z^2$. The method of finding the integer solutions to this equation is well-known, and uses the idea of Riemann stereographic projection [15, Chp 1], [13, Chp 1], which will be reviewed in Section 4. For example, if θ is the larger acute angle of the right triangle with lengths $(3, 4, 5)$, then $\cos\theta = 3/5$, and the Diophantine equation is $5x^2 - 6xy + 5y^2 = 5z^2$, and the projection method yields three polynomials

$$x = 5(n^2 - m^2), \quad y = 2n(3n - 5m), \quad z = 5m^2 - 6mn + 5n^2, \tag{1}$$

where $\gcd(m,n) = 1$. If $(m,n) = (-1,3)$, then the values of the polynomials are $(x,y,z) = (40,84,68)$, and by cancelling out their common factor of 4, we obtain a primitive solution $(10,21,17)$ of the Diophantine equation. The method claims that all primitive solutions for the Diophantine equation are obtained in this fashion.

Nevertheless, there are no values of (m,n) for which the values of the polynomials in (1) match any of the six permutations of $(10,21,17)$, and there are many more primitive solutions that cannot be the values of the polynomials in (1), up to permutation. However when $\theta = 90^\circ$, the situation is different. The projection method yields three polynomials with integer coefficients as described in (2) below:

$$x = n^2 - m^2,\ y = 2mn,\ z = m^2 + n^2. \tag{2}$$

This is also known as Euclid's parametrization, and different proofs are available in [9, 14]. First of all, the projection method claims that all primitive solutions are obtained by cancelling out their common factors of the triples (2). For example, when $(m,n) = (1,3)$, the values of the polynomials in (2) are $(x,y,z) = (8,6,10)$ where $\gcd(x,y,z) = 2$, and after cancelling the factors of 2 across the solution, we obtain a primitive solution $(4,3,5)$. On the other hand, for parameters $(m,n) = (1,2)$, the values of the polynomials are $(3,4,5)$. In general, the polynomials in (2) reach all primitive Pythagorean triples, up to transpose of the first two entries, precisely with parameters (m,n) such that $\gcd(m,n) = 1$ and $m \not\equiv n \pmod 2$. We call this property of Euclid's polynomials *the restricted parametrization of symmetry classes of primitive solutions* as they parametrize $(3,4,5)$ instead of $(4,3,5)$, and certain input values such as $m \equiv n \pmod 2$ are not allowed. In Theorem 1.1, we shall introduce Diophantine equations $Ax^2 + Bxy + Cy^2 = qz^2$ whose primitive solutions enjoy a similar parametrization property.

Let us begin with a few definitions, assumptions, and notations, which will be used throughout the paper. Let $k(x,y)$ be a nonsingular binary quadratic form $Ax^2 + Bxy + Cy^2$ with integer coefficients, and let d be the absolute value of its discriminant $-B^2 + 4AC$. Notice that $d \neq 1$, and hence, $d > 1$. Our work concerns the primitive solutions (x,y,z) of Diophantine equations $k(x,y) = qz^2$ where $q \neq 0$. By definition, the trivial solution $(0,0,0)$ is not a primitive solution, and we assume that it has a particular primitive solution $(x_0, y_0, 1)$. Let k_x and k_y be the values of the partial derivatives at (x_0, y_0) with respect to x and y, respectively, and define three polynomials (f,g,k) as follows:

$$\begin{aligned} f(m,n) &= x_0 k(m,n) - m(k_x m + k_y n), \\ g(m,n) &= y_0 k(m,n) - n(k_x m + k_y n),\ z = k(m,n). \end{aligned} \tag{3}$$

If (u,v) is a pair of rational variables, the equation $k(u,v) = 1$ defines a conic section in the uv plane, and we assume that the axes of symmetry of the conic section are defined over integer coefficients. Then, the reflection across the axes of symmetry defines a group action on the rational solutions of the conic section, and the action can be lifted to all primitive solutions of $k(x,y) = qz^2$. Let us call the map $(x,y,z) \mapsto (-x,-y,-z)$ on the primitive solutions the *antipedal map*. Then, the two reflections and the antipedal map define an action of the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ on the primitive solutions. We call the orbits of this action *symmetry classes* of

primitive solutions. Our main result is formulated as follows, and examples are introduced in Section 2.

Theorem 1.1. *Let $k(x, y)$ be a binary quadratic form $Ax^2 + Bxy + Cy^2$ with integer coefficients such that the absolute value of its discriminant is an odd prime number d. Suppose that the associated conic section $k(u, v) = 1$ has rational axes of symmetry, and let (α, β) and $(-\beta, \alpha)$ in $\mathbb{Z}^2$ be direction vectors of the axes where $\gcd(\alpha, \beta) = 1$.*

Let q be 1 or an odd prime different from d, and suppose that the Diophantine equation $k(x, y) = qz^2$ in (x, y, z) has a solution $(x_0, y_0, 1)$. If $q \neq 1$ and $\alpha^2 + \beta^2 \not\equiv 0 \pmod{q}$, then the polynomials of two variables in (3) make a parametrization of the symmetry classes of primitive solutions of the Diophantine equation with restriction $k_x m + k_y n \not\equiv 0$ mod d, and mod q if $q \neq 1$, and so do they if $q = 1$.

Introduced in [17] are results on (unrestricted) polynomial parametrizations of the solutions of various Diophantine equations related to the determinant equation $xy - zw = 1$, and if we use Theorem 13 of [17], we can prove that the symmetry classes of primitive solutions considered in Theorem 1.1 are parametrized without restriction.

Corollary 1.2. *Let $k(x, y) = qz^2$ be the Diophantine equation considered in Theorem 1.1. Then, the symmetry classes of primitive solutions of the Diophantine equation are parametrized by polynomials in 98 variables.*

Introduced in [6] is a general result on parametrizations of the solutions of Diophantine equations of genus 0 with integer-valued polynomials defined over $\mathbb{Q}$ such as $\frac{1}{2}\, x(x+1)$. The main theorem of [6] implies that the (primitive and non-primitive) solutions of our equation $k(x, y) = qz^2$ are parametrized by a single set of integer-valued polynomials. Introduced in [5, 17] are examples of Diophantine equations for which the solution sets are not parametrized by a single set of polynomials defined over $\mathbb{Z}$. Especially, in [5], it is proved that the set of (primitive and non-primitive) Pythagorean triples does not admit an (unrestricted) polynomial parametrization with integer coefficients, and their proof is immediately adapted for the statement that the set of primitive Pythagorean triples does not admit a polynomial parametrization with integer coefficients. We would like to note, though, that by our Corollary 1.2, its symmetry classes are parametrized.

In our opinion, if q or d in Theorem 1.1 is not prime, it is very unlikely that the polynomials in (3) parametrize the primitive solutions. This is due to the fact that if (m, n) generates a non-primitive solution, there are only three options for different pairs (m_1, n_1) that may generate its primitive solution, as illustrated in Figure 2 in Section 5, and it is unlikely that the congruence conditions required for having a primitive solution are satisfied for one of these three options. Recall the equation $5x^2 - 6xy + 5y^2 = 5z^2$, and the polynomials given in (1). Its discriminant is -2^6, and no primitive solutions in the symmetry class of the solution $(10, 21, 17)$ are the values of the polynomials. Nevertheless, it is still reasonable to ask if there is a different set of polynomials that parametrizes the primitive solutions.

In Section 2, we introduce more examples of integer-sided triangles, and examples for which the axes of symmetry are not given by $x \pm y = 0$. We discovered the very first six equations using the unique factorization of the ring of integers associated with a Diophantine equation, which is

different from the method on which Theorem 1.1 is based, and they are introduced in Section 3. In Section 4, we introduce the idea of Riemann stereographic projection, which is the method used in Theorem 1.1, and in Section 5 we prove the property of restricted parametrization of symmetry classes of primitive solutions, and prove Corollary 1.2.

2 Examples

To demonstrate Theorem 1.1, let us consider the Diophantine equation $x^2 - xy + y^2 = z^2$, which is the law of cosines for integer-sided triangles with angle 60°. The discriminant of the quadratic form is 3, and it has a solution $(x_0, y_0, 1) = (1, 0, 1)$. The direction vectors for the axes of symmetry are $(\alpha, \beta) = (1, 1)$ and $(-\beta, \alpha) = (-1, 1)$, and the polynomials in (3) simplify to

$$x = (n^2 - m^2),\ y = n(n - 2m),\ z = m^2 - mn + n^2, \tag{4}$$

where the restrictions are $\gcd(m, n) = 1$ and $2m \not\equiv n \pmod 3$. Listed below are some examples of primitive solutions and their corresponding parameters:

$$\begin{array}{c|ccccc} (x, y, z) & (8, 3, 7) & (-5, -8, 7) & (21, 5, 19) & (40, 7, 37) \\ \hline (m, n) & (1, 3) & (3, 2) & (2, 5) & (3, 7) \end{array}.$$

More importantly, the primitive solutions that are not the values of these polynomials are obtained by transposing the first two entries of, and changing the signs of (f, g, k) that are allowed by the action of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. For example, a primitive solution $(3, -5, 7)$ is obtained with $(m, n) = (4, 5)$ where $2m \equiv n \pmod 3$ after cancelling out the common factors of 3 across the values of the polynomials $(9, -15, 21)$, but $(3, -5, 7)$ are not the values of the polynomials in (4). On the other hand, if $(m, n) = (2, 3)$, then the values of the polynomials are $(5, -3, 7)$, which belong to the same symmetry class of $(3, -5, 7)$. This case of integer-sided triangles and the case of $\theta = 120^\circ$ are known in the literature as *Eisenstein triples*, and the name seems to be coined in [2]. The methods of finding primitive Eisenstein triples are also found in [2, 7, 11, 12, 16].

Let us consider cases for which the direction vectors of axes of symmetry are not $(1, 1)$ and $(-1, 1)$. The quadratic form $k(u, v)$ is given by the matrix form

$$\tfrac{1}{2}\begin{bmatrix} u & v \end{bmatrix}\begin{bmatrix} 2A & B \\ B & 2C \end{bmatrix}\begin{bmatrix} u \\ v \end{bmatrix}. \tag{5}$$

We denote the 2×2 matrix in (5) by W. The characteristic polynomial of the matrix W is

$$\lambda^2 - (2A + 2C)\lambda + (4AC - B^2). \tag{6}$$

Notice that the nonsingular matrix W has rational eigenvectors if and only if the characteristic polynomial (6) has rational zeros. Recall that $d = \epsilon(4AC - B^2)$ is assumed to be prime where $\epsilon = 1$ if $-B^2 + 4AC > 0$ and $\epsilon = -1$ if $-B^2 + 4AC < 0$. The following is a necessary and sufficient condition for our requirements, and we leave the proof to the reader.

Lemma 2.1. *The nonsingular symmetric matrix W has rational eigenvectors if and only if there is $\delta = \pm 1$ such that the following two conditions are satisfied*

1. $(2A-\delta)(2C-\delta) = B^2$

2. $\delta(2A+2C) - \epsilon = d$.

For example, choose $C = 1$ and $\delta = 1$. Then, $2A = B^2 + 1$, and $d = B^2 + 2$ needs to be prime. If $B = 3$, then $d = 11$ is prime, and $A = 5$. The quadratic form $k(x, y)$ is $5x^2 - 3xy + y^2$, and the axes of symmetry are given by direction vectors $(\alpha, \beta) = (1, 3)$ and $(-3, 1)$, which are eigenvectors of $W = \left[\begin{smallmatrix} 10 & -3 \\ -3 & 2 \end{smallmatrix}\right]$. Throughout the paper, we denote by (α, β) and $(-\beta, \alpha)$ two eigenvectors in $\mathbb{Z}^2$ with $\gcd(\alpha, \beta) = 1$, which are linearly independent over $\mathbb{Q}$, and they are direction vectors of the two axes of symmetry of the conic section defined by $k(u, v) = 1$.

Now, let us consider the Diophantine equation $5x^2 - 3xy + y^2 = 23z^2$. Then, $q = 23$ is an odd prime, and the equation has a particular solution $(x_0, y_0, z) = (-1, 3, 1)$. Since $\alpha^2 + \beta^2 = 10 \not\equiv 0 \pmod{q}$, by Theorem 1.1 the symmetry classes of its primitive solutions are parametrized by

$$f = 14m^2 - 6mn - n^2, \quad g = 15m^2 + 10mn - 6n^2, \quad k = 5m^2 - 3mn + n^2 \tag{7}$$

with restrictions $\gcd(m, n) = 1$, $8m \not\equiv 9n \pmod{1}1$, and $19m \not\equiv 9n \pmod{2}3$.

Let us consider the possibilities of odd primes q described in Theorem 1.1, namely, the set of odd primes q that are represented by a nonsingular quadratic form $k(x, y)$ since $(x_0, y_0, 1)$ is a particular solution, and that do not divide $\alpha^2 + \beta^2$. The following lemma lists odd primes q that are not allowed, and we leave the proof to the reader.

Lemma 2.2. *If $q \neq 1$, and $-d$ is not a quadratic residue mod q, then $k(x, y) = q$ is not solvable for integers (x, y).*

The converse of this lemma does not have an easy answer. For example, for the case of $(A, B, C) = (1, 0, C)$ and $C > 0$, though $\epsilon(-B^2 + 4AC)$ cannot be an odd prime for us, the answers for the representability of odd primes by $x^2 + Cy^2$ involve the theory of complex multiplication of elliptic curves; see [1]. Nevertheless, if the ring of integers associated with $k(x, y)$ is a unique factorization domain, the converse of Lemma 2.2 may be true. For example, if the Diophantine equation is $x^2 - xy + y^2 = qz^2$, then the ring of integers associated with the binary quadratic form is the Eisenstein integers $\mathbb{Z}[\omega]$ where $\omega = (-1 + \sqrt{-3})/2$, and it is a unique factorization domain. If -3 is a quadratic residue mod q, then the Diophantine equation has a solution, and via the law of quadratic reciprocity, the residue condition is equivalent to $q \equiv 1 \pmod{3}$. We shall discuss more about the case of unique factorization domains in Section 3.

Let us discuss the reflection across the axes of symmetry. Given a direction vector (α, β) of an axis of symmetry, the matrix of the reflection across the vector (α, β) for the conic section $k(u, v) = 1$ is given by $\bar{M}$ where

$$M = \begin{bmatrix} \alpha^2 - \beta^2 & 2\alpha\beta \\ 2\alpha\beta & \beta^2 - \alpha^2 \end{bmatrix}, \quad \bar{M} = \tfrac{1}{\alpha^2+\beta^2} M. \tag{8}$$

We define the induced reflection γ on the primitive solutions across the direction (α, β) as follows.

$$\gamma(x, y, z) = (\gamma_x/h, \gamma_y/h, (\alpha^2 + \beta^2)z/h), \tag{9}$$

where $\left[\begin{smallmatrix}\gamma_x\\ \gamma_y\end{smallmatrix}\right] = M\left[\begin{smallmatrix}x\\ y\end{smallmatrix}\right]$ and $h = \gcd(\gamma_x, \gamma_y, (\alpha^2+\beta^2)z)$. For the equation $5x^2 - 3xy + y^2 = 23z^2$, the matrix M is $\left[\begin{smallmatrix}-8 & 6\\ 6 & 8\end{smallmatrix}\right]$. The reflection across $(-3, 1)$ is given by $\left[\begin{smallmatrix}8 & -6\\ -6 & 8\end{smallmatrix}\right]$. For example, consider a primitive solution $(29, 97, 15)$. Its reflections across the two axes are $(7, 19, 3)$ and $(-7, -19, 3)$, and with further reflections across the two axes, we obtain $(-29, -97, 15)$. Finally, applying the antipedal map $(x, y, z) \mapsto (-x, -y, -z)$ we obtain all eight primitive solutions that make one symmetry class. It turns out that the values of the polynomials (f, g, k) in (7) are never equal to any solutions $(a, b, \pm 15)$ in the symmetry class for all $(m, n) \in \mathbb{Z}^2$, but when $(m, n) = (1, 1)$, we have $(f, g, k) = (7, 19, 3)$.

Let us use the equation $5x^2 - 3xy + y^2 = 5z^2$ to demonstrate that the condition $\alpha^2 + \beta^2 \not\equiv 0 \pmod{q}$ in Theorem 1.1 is necessary for our result. Notice that the direction vectors are the same as before, but we have a different particular solution $(x_0, y_0, 1) = (1, 3, 1)$. The polynomials in (3) simplify to

$$x = 4m^2 - 6mn + n^2,\ y = 15m^2 - 10mn,\ z = 5m^2 - 3mn + n^2.$$

For example, the symmetry class of the primitive solution $(4, 7, 3)$ contains $(1, 8, 3)$ obtained by reflecting $(4, 7, 3)$ across $(\alpha, \beta) = (1, 3)$, and other solutions in the symmetry class are obtained by changing the signs of these two solutions allowed by the action of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. However, it turns out that none of the eight solutions are the values of the above polynomials. Nevertheless, if $(m, n) = (-1, 2)$, the values of the polynomials are $(20, 35, 15)$, whose primitive version is $(4, 7, 3)$, and if $(m, n) = (2, 1)$, the values of the polynomials are $(5, 40, 15)$, whose primitive version is $(1, 8, 3)$.

3 Gaussian triples

Recall that $x^2 - 2xy\cos\theta + y^2 = z^2$ is the law of cosines for integer-sided triangles with angle θ. In [2], it was pointed out that parametrization polynomials for $x^2 - xy + y^2 = z^2$ where $\theta = 60^\circ$ can be discovered easily if we use the unique factorization property of *the Eisenstein integers* $\mathbb{Z}[\omega]$ where $\omega = (-1 + \sqrt{-3})/2$, and our very first approach to the problem was to use the property of unique factorization as well. The ring of integers associated with the law of cosines for an angle θ are quadratic imaginary field extensions of $\mathbb{Q}$, and Gauss conjectured that there are only finitely many quadratic imaginary field extensions whose ring of integers is a unique factorization domain. It was proved by a combined result of Hecke and Heilbronn [3, Chp 21]. Moreover we have the complete list of such fields $\mathbb{Q}(\sqrt{-d})$ where $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ from the works of various independent contributors Heilbronn, Linfoot, Heegner, Baker, Stark, and Deuring [3, Chp 21]. In our very first approach, we used six values of $d \in \{7, \ldots, 163\}$ to find six more examples of θ for which the symmetry classes are parametrized by a set of three polynomials, and in honor of Gauss' work, we call the solutions of the following Diophantine equations *Gaussian triples:*

$$qx^2 \pm (2q-1)xy + qy^2 = qz^2,$$

where $\cos\theta = \pm(2q-1)/q$, $q = (d+1)/4$, and $d \in \{3, 7, \ldots, 163\}$. For these values of d and $\cos\theta > 0$, the parametrization polynomials are given by

$$x = m^2 + 2(q-1)mn - (2q-1)n^2,\ y = q(2mn - n^2),\ z = m^2 - mn + qn^2.$$

We shall use the example of $d = 163$ to demonstrate the method, in the proof of Theorem 3.1. Let $\cos\theta = 81/82$. Then, $q = 41$ and $d = 163$, and the law of cosines for integer-sided triangles with angle θ yields

$$41x^2 - 81xy + 41y^2 = 41z^2. \tag{10}$$

It has direction vectors $(1, 1)$ and $(-1, 1)$ for the axes of symmetry, and a particular solution $(x_0, y_0, 1) = (1, 0, 1)$.

Theorem 3.1. *The symmetry classes of the primitive solutions of (10) are parametrized by*

$$x = m^2 + 80mn - 81n^2,\ y = 41(2mn - n^2),\ z = m^2 - mn + 41n^2, \tag{11}$$

with restriction $\gcd(m, n) = 1$, $2m \not\equiv n \pmod{163}$, *and* $m \not\equiv n \pmod{41}$.

Proof. To use the ring of integers $\mathbb{Z}[\omega]$, we reduce the equation as follows. Since 41 is prime, without loss of generality, the Diophantine equation is equivalent to $x^2 - 81x\tilde{y} + 41^2\tilde{y}^2 = z^2$, where $y = 41\tilde{y}$, and this corresponds to the reflection across $(1, 1)$ that makes y divisible by 41. We shall focus on the Diophantine equation

$$x^2 - 81x\tilde{y} + 41^2\tilde{y}^2 = z^2. \tag{12}$$

Let $d = 163$ and $\omega = (-1 + \sqrt{-d})/2$. Notice that the Diophantine equation (12) is factored as follows:

$$(x - 40\tilde{y} + \tilde{y}\omega)(x - 40\tilde{y} + \tilde{y}\bar{\omega}) = z^2, \tag{13}$$

and the ring of integers is $\mathbb{Z}[\omega]$ is a unique factorization domain.

Suppose that $(x, \tilde{y}, z)$ is a primitive solution of (12). Recall the factorization in (13), and we consider the factorization of $x - 40\tilde{y} + \tilde{y}\omega$ into irreducibles in $\mathbb{Z}[\omega]$. The irreducibles ρ in $\mathbb{Z}[\omega]$ are classified into three kinds, depending on its $\mathbb{Q}$-norm value $N(\rho) = p$, which must be prime in $\mathbb{Z}$ since $\mathbb{Z}[\omega]$ is a unique factorization domain.

1. *Split primes:* If $p \neq d$, and $-d$ is a quadratic residue mod p, then p factors into two irreducibles π and $\bar{\pi}$ in $\mathbb{Z}[\omega]$ such that π is not an associate of $\bar{\pi}$, i.e., $\bar{\pi} \neq \pm\pi$. Hence, ρ is either $\pm\pi$ or $\pm\bar{\pi}$.

2. *Inert primes:* If $p \neq d$, and $-d$ is a quadratic nonresidue mod p, then p is an irreducible in $\mathbb{Z}[\omega]$. Hence, $\rho = \pm p$.

3. *Ramified primes:* If $p = 163$, then $\rho = \pm(1 + 2\omega)$, and $-d = (1 + 2\omega)^2$.

Let $x - 40\tilde{y} + \tilde{y}\omega = u\beta\prod_{k=1}^{s}\pi_k^{v_k}$ be a factorization into irreducibles, where β is the product of inert primes in the above classification, and π_k are irreducibles over split and ramified primes. Let us write $\prod_{k=1}^{s}\pi_k^{v_k} = a + b\omega$, where $a, b \in \mathbb{Z}$. Since $\beta \in \mathbb{Z}$, $x - 40\tilde{y} + \tilde{y}\omega = \beta(a + b\omega)$ implies

that β must divide $\tilde{y}$, and hence, each of $x, \tilde{y}, z$. This contradicts $\gcd(x, \tilde{y}, z) = 1$. Therefore, we conclude $\beta = 1$.

Let us use a similar argument to show that $N(\pi_k) \neq N(\pi_j)$ for $k \neq j$. Suppose that $N(\pi_k) = N(\pi_j) = p$ for $k \neq j$, i.e., $\pi_k \bar{\pi}_k = \pi_j \bar{\pi}_j = p$. Then the unique factorization property implies that $\bar{\pi}_k = \pm\pi_j$; otherwise, $\bar{\pi}_k = \pm\bar{\pi}_j$, and hence, $k = j$. Thus, $\pi_k \pi_j = \pm p$, and this implies that $x - 40\tilde{y} + \tilde{y}\omega$ is divisible by p. As in the case for β above, this implies that p divides $\gcd(x, \tilde{y}, z)$, but it is a contradiction to $\gcd(x, \tilde{y}, z) = 1$.

Thus, we conclude for each $k = 1, \ldots, s$ that if $p_k := N(\pi_k) = \pi_k \bar{\pi}_k$, then $p_k \neq p_j$ for all $k \neq j$. Since $z^2 = u \prod_{j=1}^{s} \pi_j^{v_j} \cdot u \prod_{j=1}^{s} \bar{\pi}_j^{v_j} = \prod_{j=1}^{s} p_j^{v_j}$ where $u = \pm 1$ and p_j are distinct primes, since the factorization $z^2 = \prod_{j=1}^{s} p_j^{v_j}$ is taking place in $\mathbb{Z}$, we have $v_j = 2\ell_j$. Thus $x - 40y + y\omega = u \left(\prod_{j=1}^{s} \pi_j^{\ell_j} \right)^2$, and if $m + n\omega = \prod_{j=1}^{s} \pi_j^{\ell_j}$, then

$$x - 40\tilde{y} + \tilde{y}\omega = u'(m + n\omega)^2, \quad u' = \pm 1. \tag{14}$$

Notice that $(m + n\omega)^2 = (m^2 - 41n^2) + (2mn - n^2)\omega$, and (14) implies that $\tilde{y} = u'(2mn - n^2)$, and hence, $x = u'(m^2 + 80mn - 81n^2)$. On the other hand, $z^2 = N(x - 40\tilde{y} + \tilde{y}\omega)$ implies $z^2 = N(m + n\omega)^2 = (m^2 - mn + 41n^2)^2$, and hence, $z = \pm(m^2 - mn + 41n^2)$. Since $y = 41\tilde{y}$, it proves that the polynomials reach all primitive solutions up to $u' = \pm 1$ and the sign of z.

It is straightforward to prove that the values of polynomials will have common factors of 41 or 163 if the modular congruence relations in Theorem 3.1 are not satisfied, and to prove the part of the converse that the polynomials satisfy the Diophantine equation. We leave that part of the proof to the reader, but prove here that if a prime p divides the values of the polynomial, then it must be 41 or 163. Suppose that p divides the values of the polynomials, but different from 41 and 163. It follows from $y \equiv 0 \pmod{p}$ that $2m \equiv n$ or $n \equiv 0 \pmod{p}$. If $n \equiv 0$, then $x \equiv 0$ implies $m \equiv 0 \pmod{p}$, which is a contradiction to $\gcd(m, n) = 1$. If $2m \equiv n$, then $x \equiv 0$ implies $0 \equiv m^2 + 80m(2m) - 81(2m)^2 = -163m^2$, and hence, $m \equiv 0 \pmod{p}$. Again $0 \equiv 2m \equiv 0 \pmod{p}$ implies $\gcd(m, n) \neq 1$. □

Our second approach was to exploit the idea of Riemann stereographic projection, by which Theorem 1.1 is established. In that approach, we discovered far more angles θ, and the list includes the ones obtained with the property of unique factorization. However, the infinitude of the larger list of θ seems to remain conjectural. The law of cosines reduces to $qx^2 + Bxy + qy^2 = qz^2$, and, as required in Theorem 1.1, if $d = -B^2 + 4q^2$ and q are distinct odd primes, then $d = 4q - 1$, and the existence of infinitely many prime pairs $(q, 4q - 1)$ will imply that there are infinitely many angles θ for which the symmetry classes will admit a restricted parametrization. The following are the first twenty prime numbers d for which $(d + 1)/4$ is also prime:

$$3, 7, 11, 19, 43, 67, 163, 211, 283, 331, 523, 547, 691, 787, 907, 1051, 1123, 1171, 1531, 1723.$$

In [4] a general problem of computing the asymptotic formulas for the number of prime tuples such as ours $(n, 4n - 1)$ is introduced, and in the celebrated result [8] the authors point out that the cases such as the twin primes $(n, n + 2)$, the Sophie Germain primes $(n, 2n + 1)$, and ours $(n, 4n - 1)$ remain as the most difficult cases.

4 Riemann stereographic projection

The method of using Riemann stereographic projection is a well-known ancient idea in number theory, but to these days it stands as one of the most inspiring ideas in the area of solving Diophantine equations. Let us explain the idea below. If a quadratic polynomial in two variables has rational coefficients, and it has one pair of rational solutions (x_0, y_0), then a line L with slope ℓ passing through (x_0, y_0) with rational coefficients must intersect the graph of the quadratic polynomial at rational coordinates (u, v). Let the y-intercept of the line L to be the projection of a rational solution (u, v), and this is called a *Riemann stereographic projection*; see Figure 1.

Let $\tilde{u} = u - x_0$ and $\tilde{v} = v - y_0$, and recall that k_x and k_y are the values of the partial derivatives of $k(x, y)$ at (x_0, y_0). Then, by the Taylor series of $k(x, y)$ at (x_0, y_0) we have

$$k(u, v) - q = k_x\tilde{u} + k_y\tilde{v} + A\tilde{u}^2 + B\tilde{u}\tilde{v} + C\tilde{v}^2.$$

For the intersection point with L, let $\tilde{v} = \ell\tilde{u}$. If $\tilde{u} \neq 0$, the above expansion implies that

$$0 = k_x + k_y\ell + \tilde{u}(A + B\ell + C\ell^2).$$

Let $\ell = n/m$ where $\gcd(m, n) = 1$, dehomogenize the equation for m and n, and solve for $\tilde{u} = u - x_0$. Then we have

$$u - x_0 = -\frac{m(k_x m + k_y n)}{k(m, n)} \Rightarrow u = \frac{x_0 k(m, n) - m(k_x m + k_y n)}{k(m, n)},$$
$$v - y_0 = \ell(u - x_0) \Rightarrow v = \frac{y_0 k(m, n) - n(k_x m + k_y n)}{k(m, n)}.$$

If (a, b, c) is a primitive solution of $k(x, y) = qz^2$ such that $(a/c, b/c) = (u, v)$, then there must be h such that $(ah, bh, ch) = (x, y, z)$ where (x, y, z) is given in (3).

Lemma 4.1 below is useful throughout our work.

Lemma 4.1. *If* $\gcd(m, n) = 1$*, and*

$$k_x m + k_y n \equiv 0 \pmod{p}^e \tag{15}$$

for $e \geq 1$*, then* $k(m, n) \equiv (-B^2 + 4AC)q \pmod{p}^e$.

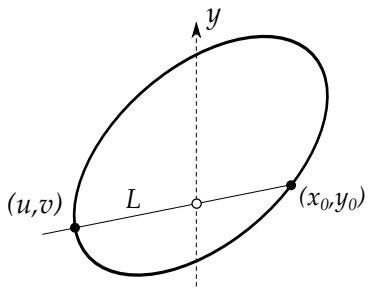

Figure 1. Riemann stereographic projection

Proof. For $e = 1$ we have $m \equiv t_1 k_y$ and $n \equiv -t_1 k_x \pmod p$ for some integer $t_1 \not\equiv 0 \pmod p$. Applying the method of lifting solutions to mod p^{e+1} inductively, we obtain that (15) implies $m \equiv t_e k_y$ and $n \equiv -t_e k_x \pmod p^e$ for some integer $t_e \not\equiv 0 \pmod p$. Thus,

- $k(m,n) \equiv t_e^2\big(Ak_y^2 - Bk_yk_x + Ck_x^2\big) \pmod p^e$
- $k_y = Bx_0 + 2Cy_0,\ k_x = 2Ax_0 + By_0 \Rightarrow$

$$Ak_y^2 - Bk_yk_x + Ck_x^2 = (-B^2+4AC)(Ax_0^2 + Bx_0y_0 + Cy_0^2) = (-B^2+4AC)q. \qquad \square$$

The following theorem is an immediate consequence of Lemma 4.1 and the formulas in (3).

Theorem 4.2. *Let $(x_0, y_0, 1)$ be a solution to $Ax^2 + Bxy + Cy^2 = qz^2$, let (f, g, k) be the polynomials defined in (3), and let $h = \gcd(f(m,n), g(m,n), k(m,n))$ for some $(m,n) \in \mathbb{Z}^2$ with $\gcd(m,n) = 1$. Then, $h \equiv 0 \pmod p^e$ if and only if*

$$k_x m + k_y n \equiv 0 \pmod p^e, \text{ and } q(4AC - B^2) \equiv 0 \pmod p^e.$$

In particular, h divides $q(4AC - B^2)$.

5 Parametrization

We prove Theorem 1.1 in this section. Recall that $d := \epsilon(-B^2 + 4AC)$ and q are distinct odd primes or 1 where $\epsilon = \pm 1$. Let $(a,b,c) = (f(m,n), g(m,n), k(m,n))$ for some $(m,n) \in \mathbb{Z}^2$ with $\gcd(m,n) = 1$, and $(a_0, b_0, c_0) = (a/h, b/h, c/h)$ where $h = \gcd(a,b,c)$.

Let us say that (x,y) is *orthogonal* to $(s,t) \bmod p$ if p is prime, $xs + yt \equiv 0 \pmod p$, and (x,y) and $(s,t) \not\equiv (0,0) \pmod p$. Then, (x_1, y_1) and (x_2, y_2) are orthogonal to $(s,t) \bmod p$ if and only if (x_1, y_1) and (x_2, y_2) are scalar multiples to each other mod p.

Proposition 5.1. *Under $\bmod q$ and d, the column vectors $\left[\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} k_x \\ k_y \end{smallmatrix}\right]$ are $\not\equiv \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$.*

There is $u \not\equiv 0 \pmod d$ such that $k(x,y) \equiv u(k_x x + k_y y)^2$. There are integers δ_x and δ_y such that $k(x,y) \equiv (k_x x + k_y y)(\delta_x x + \delta_y y)$ and $\det \left[\begin{smallmatrix} k_x & k_y \\ \delta_x & \delta_y \end{smallmatrix}\right] \not\equiv 0 \pmod q$.

Proof. If $x_0 \equiv y_0 \equiv 0 \pmod q$, then $k(x_0, y_0) \equiv 0 \pmod q^2$ while $k(x_0, y_0) = q$. Notice that $\left[\begin{smallmatrix} k_x \\ k_y \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right]\left[\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right] \not\equiv \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right] \pmod q$. Since $\det \left[\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right] \not\equiv 0$, $\left[\begin{smallmatrix} k_x \\ k_y \end{smallmatrix}\right] \not\equiv \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right] \pmod q$. Notice that $k(x_0, y_0) \not\equiv 0 \pmod d$, and this implies that $\left[\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right] \not\equiv \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right] \pmod d$. Also

$$k(x_0, y_0) = \tfrac{1}{2}\left[\begin{smallmatrix} x_0 & y_0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right]\left[\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right] = \tfrac{1}{2}\left[\begin{smallmatrix} x_0 & y_0 \end{smallmatrix}\right]\left[\begin{smallmatrix} k_x \\ k_y \end{smallmatrix}\right] \not\equiv 0 \pmod d,$$

and this implies that $(k_x, k_y) \not\equiv (0,0) \pmod d$.

Since the discriminant of $k(x,y)$ is d, we have $k(x,y) \equiv u'(sx + ty)^2$ for some $u', s, t \in \mathbb{Z}$. If $(m,n) = (-k_y, k_x)$, then $k_x m + k_y n = 0$ and $(m,n) \not\equiv 0 \pmod d$. Thus, by Lemma 4.1, $k(m,n) \equiv 0$, and it follows that (m,n) is orthogonal to (k_x, k_y) and $(s,t) \bmod d$. Therefore, (k_x, k_y) is a scalar multiple of $(s,t) \bmod d$, and hence, $u'(sx + ty)^2 \equiv u(k_x x + k_y y)^2 \pmod d$.

Notice that, by Lemma 4.1, $k(m,n) \equiv 0 \pmod q$ if $(m,n) = (-k_y, k_x) \pmod q$. Since the discriminant of $k(x,y)$ is not divisible by q, the polynomial factors into two distinct linear polynomials, up to constant multiplication, and one of them must be $(k_x x + k_y y)$.

Since $(k_x, k_y) \not\equiv (0,0) \pmod q$, this proves the assertion about the determinant as well. □

Lemma 5.2. $c_0 \not\equiv 0 \pmod d$.

Proof. Suppose that $k_x m + k_y n \not\equiv 0 \pmod d$. Then, by Proposition 5.1, $c = k(m,n) \not\equiv 0 \pmod d$, and hence, $c_0 \not\equiv 0 \pmod d$.

Suppose that $k_x m + k_y n \equiv 0 \pmod d$, i.e., $h \equiv 0 \pmod d$. Notice that $d = \epsilon(-B^2 + 4AC)$ implies that $A \not\equiv 0$ or $C \not\equiv 0 \pmod d$; otherwise, $-B^2 + 4AC$ is divisible by d^2. Notice that c can be written in two ways depending on the case $A \not\equiv 0$ or $C \not\equiv 0 \pmod d$:

$$c = \frac{1}{4A}(2Am + Bn)^2 + \frac{\epsilon d}{4A} n^2 = \frac{\epsilon d}{4C} m^2 + \frac{1}{4C}(Bm + 2Cn)^2. \tag{16}$$

Since $c = k(m,n) = Am^2 + Bmn + Cn^2 \equiv 0 \pmod d$ and $\gcd(m,n) = 1$, it follows that if $A \not\equiv 0$, then $n \not\equiv 0 \pmod d$, and that if $C \not\equiv 0$, then $m \not\equiv 0 \pmod d$.

For the case of $A \not\equiv 0$, we have $2Am + Bn \equiv 0 \pmod d$, and the first version in (16) and $n \not\equiv 0$ imply that $c_0 = c/h \not\equiv 0 \pmod d$. For the case of $B \not\equiv 0$, the argument is similar, and we conclude $c_0 \not\equiv 0 \pmod d$ as well. □

Lemma 5.3. $a_0 \not\equiv 0$ *or* $b_0 \not\equiv 0 \pmod q$.

Proof. Suppose that $a_0 \equiv 0$ and $b_0 \equiv 0 \pmod q$. Then, $Aa_0^2 + Ba_0b_0 + Cb_0^2 = qc_0^2$ implies that $qc_0^2 \equiv 0 \pmod q^2$, and hence, $c_0 \equiv 0 \pmod q$. □

Recall that (α, β) is a direction vector of an axis of symmetry of the conic section $k(u,v) = 1$, and that it is an eigenvector of the matrix W, whose characteristic equation is given in (6).

Lemma 5.4. $\alpha^2 + \beta^2 \equiv 0 \pmod q$ *if and only if* $k(\alpha, \beta) \equiv 0 \pmod q$.

Proof. Recall the matrix $W = \left[\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right]$. Then, $k(\alpha,\beta) = \frac{1}{2}\left[\begin{smallmatrix} \alpha & \beta \end{smallmatrix}\right] W \left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right] = \frac{1}{2}\left[\begin{smallmatrix} \alpha & \beta \end{smallmatrix}\right] \left[\begin{smallmatrix} \lambda\alpha \\ \lambda\beta \end{smallmatrix}\right] = \frac{\lambda}{2}(\alpha^2 + \beta^2)$ where $\lambda = \pm 1$ or $\pm d$. □

In Theorem 1.1 we assumed that $\alpha^2 + \beta^2 \not\equiv 0 \pmod q$, so by Lemma 5.4, $k(\alpha,\beta) \not\equiv 0 \pmod q$.

Lemma 5.5. $\alpha^2 + \beta^2 \not\equiv 0 \pmod d$.

Proof. Suppose that $\alpha^2 + \beta^2 \equiv 0 \pmod d$. Since d is prime, the equation (6) implies that the eigenvalue must be ± 1 or $\pm d$, we let $(\tilde\alpha, \tilde\beta)$ be either of (α, β) and $(-\beta, \alpha)$, whose eigenvalue is ± 1. Since $\gcd(\alpha,\beta) = 1$, both $\tilde\alpha$ and $\tilde\beta$ are $\not\equiv 0 \pmod d$. Then, $\tilde\alpha^2 + \tilde\beta^2 \equiv 0 \pmod d$, and there must be an integer i such that $i^2 \equiv -1$ and $\tilde\beta \equiv i\tilde\alpha$. Notice that if $d = -B^2 + 4AC$, then $d \equiv 3 \pmod 4$, and there is no such i in $\mathbb{Z}$. If $d = B^2 - 4AC$, there will be such an i in $\mathbb{Z}$. Since $(\tilde\alpha, \tilde\beta)$ is an eigenvector of $\left[\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right]$ with eigenvalue ± 1, $k(\tilde\alpha, \tilde\beta) = \frac{\pm 1}{2}(\tilde\alpha^2 + \tilde\beta^2) \equiv 0 \pmod d$. On the other hand, $0 \equiv k(\tilde\alpha, \tilde\beta) = A\tilde\alpha^2 + B\tilde\alpha\tilde\beta + C\tilde\beta^2 \equiv \tilde\alpha^2(A + Bi - C)$. Since $\tilde\alpha \not\equiv 0$, we have $Bi \equiv C - A$. Then, $-B^2 \equiv A^2 + C^2 - 2AC$, and $-B^2 \equiv -4AC$ implies that $(A + C)^2 \equiv 0$. By Lemma 2.1, $d = \pm 2(A + C) \pm 1$, and hence, $A + C \not\equiv 0 \pmod d$. □

Since $k(x_0, y_0) \equiv 0 \pmod{q}$, by Proposition 5.1, (x_0, y_0) is orthogonal to either (k_x, k_y) or $(\delta_x, \delta_y) \bmod q$, but not both. In Lemma 5.6 below we show that the reflection γ reduces to a nontrivial action on the set of the two orthogonal complements $\bmod q$, and would like to note that the hypothesis $\alpha^2 + \beta^2 \not\equiv 0 \pmod{q}$ is necessary for this action to be nontrivial.

Lemma 5.6. *Let (a_0, b_0, c_0) be a primitive solution, and $(a_1, b_1, c_1) = \gamma(a_0, b_0, c_0)$. If (a_0, b_0) is orthogonal to (k_x, k_y) mod q, then (a_1, b_1) is orthogonal to $(\delta_x, \delta_y) \bmod q$. If (a_0, b_0) is orthogonal to $(\delta_x, \delta_y) \bmod q$, then (a_1, b_1) is orhtogonal to $(k_x, k_y) \bmod q$.*

Proof. Notice that $\det(M) \equiv -(\alpha^2 + \beta^2)^2 \not\equiv 0 \pmod{q}$. Then, M is nonsingular mod q, and $(a_1, b_1) \not\equiv (0, 0) \pmod{q}$ by Lemma 5.3.

Suppose that (a_0, b_0) is orthogonal to (k_x, k_y) mod q. If (a_1, b_1) is orthogonal to (k_x, k_y) mod q, then (a_1, b_1) is a scalar multiple of (a_0, b_0) mod q, and hence, (a_0, b_0) is an eigenvector of M mod q. Since $\alpha^2 + \beta^2 \not\equiv 0 \pmod{q}$, the two vectors (α, β) and $(-\beta, \alpha)$ remain as two linearly independent eigenvectors of M mod q, and (a_0, b_0) must be a scalar multiple of (α, β) or $(-\beta, \alpha)$ mod q. However, by Lemma 5.4 and Proposition 5.1, the eigenvectors (α, β) and $(-\beta, \alpha)$ are not orthogonal to any of (k_x, k_y) and (δ_x, δ_y) mod q. Therefore, (a_1, b_1) must be orthogonal to (δ_x, δ_y) mod q. The proof of the case that (a_0, b_0) is orthogonal to (δ_x, δ_y) is similar, and we leave it to the reader. □

Our goal is to find a primitive solution in a symmetry class that is the values of the polynomials defined in (3), and in Definition 5.7 below, depending on which orthogonal complement mod q the solution (x_0, y_0) belongs to, we shall consider the reflection of the primitive solution (a_0, b_0, c_0) by M defined in (8) and (9); see Figure 2.

Definition 5.7. *We define the following under $\bmod q$. Suppose that (x_0, y_0) is orthogonal to (k_x, k_y) and $c_0 \not\equiv 0$. If (a_0, b_0) is orthogonal to (k_x, k_y), then define $(a_1, b_1, c_1) = \gamma(a_0, b_0, c_0)$, and if (a_0, b_0) is orthogonal to (δ_x, δ_y), then define $(a_1, b_1, c_1) = (a_0, b_0, c_0)$.*

Suppose that (x_0, y_0) is orthogonal to (δ_x, δ_y) and $c_0 \not\equiv 0 \pmod{q}$. If (a_0, b_0) is orthogonal to (δ_x, δ_y), then define $(a_1, b_1, c_1) = \gamma(a_0, b_0, c_0)$, and if (a_0, b_0) is orthogonal to (k_x, k_y), then define $(a_1, b_1, c_1) = (a_0, b_0, c_0)$.

Suppose that $c_0 \equiv 0 \pmod{q}$. If (a_0, b_0) is orthogonal to (k_x, k_y), then define $(a_1, b_1, c_1) = \gamma(a_0, b_0, c_0)$, and if (a_0, b_0) is orthogonal to (δ_x, δ_y), then define $(a_1, b_1, c_1) = (a_0, b_0, c_0)$.

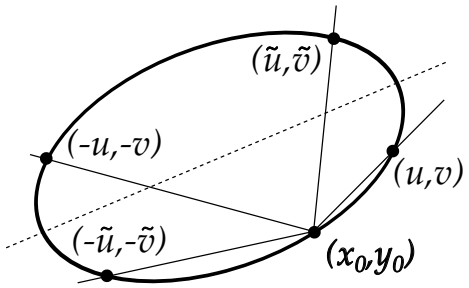

Figure 2. A symmetry class

Lemma 5.8. *Let (a_1, b_1, c_1) be as defined in Definition 5.7. Let $t = \pm 1$, and let n/m be the slope of $(ta_1/c_1, tb_1/c_1)$ and (x_0, y_0) where $\gcd(m, n) = 1$. Then, the gcd of $(f(m, n), g(m, n), k(m, n))$ is $\not\equiv 0 \pmod{q}$ for both $t = \pm 1$.*

Proof. Notice that

$$\frac{n}{m} = \frac{tb_1 - y_0c_1}{ta_1 - x_0c_1} \Rightarrow ns = tb_1 - y_0c_1, \quad ms = ta_1 - x_0c_1$$
$$\Rightarrow s(k_xm + k_yn) = t(k_xa_1 + k_yb_1) - (k_xx_0 + k_yy_0)c_1.$$

Notice that $c_1 = (\alpha^2 + \beta^2)c_0$ and $\alpha^2 + \beta^2 \not\equiv 0 \pmod{q}$. If $c_0 \equiv 0 \pmod{q}$, then $c_1 \equiv 0$, and by Definition 5.7 and Lemma 5.6, $s(k_xm + k_yn) \not\equiv 0 \pmod{q}$. If $c_0 \not\equiv 0 \pmod{q}$, then $c_1 \not\equiv 0$, and again Definition 5.7 and Lemma 5.6 guarantee that $s(k_xm + k_yn) \not\equiv 0 \pmod{q}$ for both cases of $k_xx_0 + k_yy_0 \equiv$ or $\not\equiv 0$ mod q. Hence, $k_xm + k_yn \not\equiv 0 \pmod{q}$, and by Theorem 4.2, the gcd is $\not\equiv 0 \pmod{q}$ for both slopes. □

The following proposition concludes the proof of Theorem 1.1.

Proposition 5.9. *Let (a_1, b_1, c_1) be as defined in Definition 5.7. For at least one value of $t = \pm 1$, (ta_1, tb_1, c_1) is the value of (uf, ug, uk) where $u = \pm 1$.*

Proof. Write the slopes of $(ta_1/c_1, tb_1/c_1)$ and (x_0, y_0) for both $t = \pm 1$ in lowest terms;

$$\frac{n_t}{m_t} = \frac{y_0c_1 - tb_1}{x_0c_1 - ta_1} \Rightarrow \begin{cases} m_ts_t = x_0c_1 - ta_1 \\ n_ts_t = y_0c_1 - tb_1, \end{cases} \qquad \gcd(m_t, n_t) = 1$$

Suppose that $k_xm_t + k_yn_t \equiv 0 \pmod{d}$ for both $t = \pm 1$, and let $t_1 = 1$ and $t_2 = -1$. Then,

$$0 \equiv (k_xm_{t_1} + k_yn_{t_1})s_{t_1} = (k_xx_0 + k_yy_0)c_1 - t_1(k_xa_1 + k_yb_1)$$
$$0 \equiv (k_xm_{t_2} + k_yn_{t_2})s_{t_2} = (k_xx_0 + k_yy_0)c_1 - t_2(k_xa_1 + k_yb_1).$$

By adding the two equations, we obtain $2(k_xx_0 + k_yy_0)c_1 \equiv 0 \pmod{d}$.

Since $c_1 = (\alpha^2 + \beta^2)^w c_0 \not\equiv 0 \pmod{d}$ by Lemma 5.2 and 5.5 where $w = 0, 1$, we conclude that $k_xx_0 + k_yy_0 \equiv 0 \pmod{d}$, and by Lemma 4.1, $k(x_0, y_0) \equiv 0$. However, $k(x_0, y_0) = q \not\equiv 0 \pmod{d}$.

Therefore, $k_xm_{t_*} + k_yn_{t_*} \not\equiv 0 \pmod{d}$ for some $t_* = \pm 1$. Then, by Lemma 5.8 and Theorem 4.2, we conclude that the only common divisors of the value of (f, g, k) at (m_{t_*}, n_{t_*}) are ± 1. □

Recall the restrictions on the parameters (m, n) in Theorem 1.1, and that the symmetry classes can be parametrized without restrictions, according to Corollary 1.2, if more parameters are used. We use Lemma 5.10 below to accomplish this, and it is a corollary of Theorem 13 of [17]. Lemma 5.10 does not appear in [17], and we introduce Professor Vaserstein's proof, which was communicated to us. First of all, notice that $\gcd(m, n) = 1$ if and only if $mx - ny = 1$ for

$(x, y) \in \mathbb{Z}^2$, which is equivalent to $\left[\begin{smallmatrix} m & n \\ y & x \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. The congruence conditions on m and n will be parametrized in the context of the following standard short exact sequence:

$$1 \to \mathrm{SL}_2(N\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to 1 \tag{17}$$

where $\mathrm{SL}_2(N\mathbb{Z}) := \{\left[\begin{smallmatrix} m & n \\ -x & y \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}) : m \equiv y \equiv 1,\ n \equiv x \equiv 0 \pmod{N}\}$. Lemma 5.10 below is in fact valid for an arbitrary positive m rather than dq, but we prove the case of m being the product of two distinct primes.

Lemma 5.10 (Vaserstein)**.** *Let X be a finite subset of $\mathrm{SL}_2(\mathbb{Z})$. The following subset is parametrized by polynomials with 98 variables:*

$$X\,\mathrm{SL}_2(dq\mathbb{Z}) := \{\delta\tau : \delta \in X,\ \tau \in \mathrm{SL}_2(dq\mathbb{Z})\}. \tag{18}$$

Proof. Suppose that X has r matrices $\delta_1, \ldots, \delta_r$, and let p be d or q. Let us denote by $X \bmod p$ the image of X in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ as defined in (17). Then, by the method of Lagrange Interpolation we can construct four polynomials (P, Q, R, S) with integer coefficients in four variables (v_1, v_2, v_3, v_4) such that $\left[\begin{smallmatrix} P & Q \\ R & S \end{smallmatrix}\right]$ parametrizes X mod p as the four variables v_k vary from 0 to $p-1$. This is possible since r is smaller than the number of elements in the domain $(\mathbb{Z}/p\mathbb{Z})^4$. For example, there are integers μ_w for each $w \in (\mathbb{Z}/p\mathbb{Z})^4$ such that the polynomial P is given by

$$\sum_{w \in (\mathbb{Z}/p\mathbb{Z})^4} \mu_w \frac{\prod_{j=1}^{4} \prod_{e=0}^{p-1} (v_j - e)}{\prod_{j=1}^{4} (v_j - w_j)}$$

where w_j are the entries of w, i.e., $w = (w_1, w_2, w_3, w_4)$. Thus, we have constructed a surjective map from $(\mathbb{Z}/p\mathbb{Z})^4$ to $X \pmod{p}$, and Chinese Remainder Theorem applied to two distinct prime modulus d and q implies that there are four polynomials (P, Q, R, S) with integer coefficients that induce a surjective map from $(\mathbb{Z}/dq\mathbb{Z})^4$ to $X \pmod{d}q$.

By the short exact sequence (17) with $N = dq$, we have $\left[\begin{smallmatrix} P & Q \\ R & S \end{smallmatrix}\right] = \delta_j\gamma$ for $1 \le j \le r$ and $\gamma \in \mathrm{SL}_2(dq\mathbb{Z})$, and hence, the set of matrices $\left[\begin{smallmatrix} P & Q \\ R & S \end{smallmatrix}\right]\gamma'$ where $\gamma' \in \mathrm{SL}_2(dq\mathbb{Z})$ is equal to the one in (18). By Theorem 13 of [17], $\mathrm{SL}_2(dq\mathbb{Z})$ is parametrized by 94 variables, and hence, the subset in (18) is parametrized by 98 variables. □

For the proof of Corollary 1.2, we choose X to be the subset of $\left[\begin{smallmatrix} m & n \\ -x & y \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ such that $0 \le m, n, x, y < dq$, $k_x m + k_y n \not\equiv 0 \pmod{d}$, and $k_x m + k_y n \not\equiv 0 \pmod{q}$. Then, by the sequence (17), the set of all pairs $(m, n) \in \mathbb{Z}^2$ considered in Theorem 1.1 is equal to the projection of $X\,\mathrm{SL}_2(pq\mathbb{Z})$ onto the first row. Therefore, this proves Corollary 1.2.

6 Future work

Recall the example $5x^2 - 6xy + 5y^2 = 5z^2$ in Section 1, and that our polynomials in (3) were proved to not parametrize the symmetry classes of the primitive solutions. However, we do not know if there is a different set of polynomials that may parametrize the symmetry classes. We hope to be able to develop a method by which we can determine whether there cannot be a restricted polynomial parametrization of symmetry classes, and also hope to find examples for which the polynomials in (3) do not make a parametrization, but there is a different set of polynomials that does parametrize the symmetry classes.

Acknowledgement

I would like to thank Professor Vaserstein for his kind assistance.

References

[1] Cox, D. A. (2013). *Primes of the form* $x^2 + ny^2$, Wiley.

[2] Cuoco, A. (2000). Meta Problems in Mathematics, *College Math. J.*, 31, 373–378.

[3] Davenport, H. (2000). *Multiplicative Number Theory*, Springer-Verlag, New York.

[4] Dickson, L. E. (1904). A new extension of Dirichlet's theorem on prime numbers, *Messenger of Math.*, 33, 155–161.

[5] Frisch, S., & Vaserstein, L.(2008) Parametrization of Pythagorean triples by a single triple of polynomials, *J. Pure Appl. Algebra*, 212 (1), 271–274.

[6] Frisch, S.,& Lettl, G. (2008). Polynomial parametrization of the solutions of Diophantine equations of genus 0, *Funct. Approx. Comment. Math.*, 39 (2) (Narkiewicz Volume), 205–209.

[7] Gilder, J. (1982). Integer-sided triangles with a 60° angle, *Math Gazette*, 66, 261–266.

[8] Green, B. & Tao, T. (2010). Linear equations in primes, *Ann. Math.*, 171, 1753–1850.

[9] Jones, G. & Jones, J. M. (1998). *Elementary Number Theory*, Springer.

[10] Petulante, N., & Kaja, I. (2000). How to generate all integral triangles containing a given angle, *Internat. J. Math. & Math. Sci.*, 24, 569–572.

[11] Read, E. (2006). On integer-sided triangles containing angles of 120° or 60°, *Math. Gazette*, 90, 299–305.

[12] Selkirk, K. (1983). Integer-sided triangles with angle of 120°, *Math. Gazette*, 67, 251–255.

[13] Shafarevich, I. R. (1994). *Basic Algebraic Geometry 1: Varieties in Projective Space*, Springer-Verlag.

[14] Sierpiński, W. (2011) *Pythagorean Triangles*, Dover Publications.

[15] Silverman, J. H. & Tate, J., (1992). *Rational Points on Elliptic Curves*, Springer.

[16] Stewart, B. M. (1964). *The Theory of Numbers*, MacMillan, New York, NY.

[17] Vaserstein, L. (2010). Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups, *Ann. of Math.*, 171, 979–1009.