ARITHMETIC PROGRESSIONS REPRESENTED BY BINARY QUADRATIC FORMS

Ajai Choudhry
13/4 A, Clay Square, Lucknow, India
ajaic203@yahoo.com

Received: 7/12/24, Revised:12/25/24 , Accepted: 2/5/25, Published: 2/21/25

Abstract

Given an arbitrary irreducible integral binary quadratic form, we show how to construct, in parametric terms, arithmetic progressions of nine terms all of which can be represented by the given binary quadratic form. For certain binary quadratic forms, we can extend the length of the arithmetic progressions to 11 terms. As an example, we construct infinitely many arithmetic progressions of length 11 which can be represented by the binary quadratic form $x^2 + y^2$.

1. Introduction

This paper is concerned with constructing arithmetic progressions consisting of integers that can all be represented by an integral binary quadratic form $ax^2 + bxy + cy^2, (a, b, c \in \mathbb{Z})$. It has been proved [1] that such a binary quadratic form can represent an arithmetic progression of infinite length if and only if its discriminant $d = b^2 - 4ac$ is a nonzero perfect square. We will therefore focus in this paper only on those binary quadratic forms whose discriminant is not a perfect square, and so the forms are irreducible.

In 1882 Weber [8] proved that the set of prime numbers represented by a primitive irreducible positive-definite integral binary quadratic form, such as $x^2 + y^2$, has positive relative density in the set of all primes. This theorem together with the well-known Green-Tao theorem [6] implies that each such binary quadratic form represents arithmetic progressions of arbitrary finite length, and therefore also infinitely many such arithmetic progressions. As the length of an arithmetic progression represented by a binary quadratic form increases, the common difference of the arithmetic progression tends to increase.

For arithmetic progressions with a given common difference, Dey and Thangadurai [4] obtained an upper bound for the length of an arithmetic progression of integers that can be represented by an irreducible integral binary quadratic form.

DOI: 10.5281/zenodo.14907299

This upper bound for the length of an arithmetic progression, with a given common difference, was improved significantly by Elsholtz and Frei [5].

There are a limited number of known examples of arithmetic progressions consisting of integers that can be represented by an irreducible integral binary quadratic form. For instance, it has been known for long that there exist infinitely many arithmetic progressions consisting of three consecutive integers that can all be expressed by the binary quadratic form $x^2 + y^2$ [3]. Dey and Thangadurai [4] gave a specific example to prove that every irreducible integral binary quadratic form represents an arithmetic progression consisting of three terms. Recently, Choudhry and Maji [2] obtained infinitely many arithmetic progressions of length five, with common difference 4, such that all the five terms of the arithmetic progressions can be represented by the quadratic form $x^2 + y^2$. A discussion on StackExchange [7] gives a one-parameter solution of an arithmetic progression of five terms all of which can be expressed as a sum of two squares. The same StackExchange website mentions two explicit numerical examples, obtained by computer programs, of arithmetic progressions of 16 and 27 terms which are all expressible as sums of two squares. We, however, do not know any method of constructing long arithmetic progressions of integers that can be represented by a given binary quadratic form.

In this paper we show how to construct, in parametric terms, arithmetic progressions of nine terms all of which can be represented by an arbitrary irreducible integral binary quadratic form. We also show that, in certain cases, the 9-term arithmetic progression can be extended to an arithmetic progression of 11 terms all of which can be represented by the given binary quadratic form. As an example, we obtain infinitely many arithmetic progressions of 11 terms that can be represented by the quadratic form $x^2 + y^2$. The paper ends with some open problems regarding the construction of arithmetic progressions that can be represented by a binary quadratic form.

2. Some Preliminary Observations

If u_1 and d are two coprime integers, and the arithmetic progression $u_i, i = 1, 2, \ldots,$ n, with common difference d, can be represented by the binary quadratic form $\phi(x, y) = ax^2 + bxy + cy^2$, then it is readily seen that for any positive integer k, the arithmetic progression $k^2u_i, i = 1, 2, \ldots, n$, can also be represented by the quadratic form $\phi(x, y) = ax^2 + bxy + cy^2$, and all such arithmetic progressions obtained from the arithmetic progression $u_i, i = 1, 2, \ldots, n$, in this manner may be considered equivalent with respect to the question of representation by binary quadratic forms.

The terms of the arithmetic progression $ku_i, i = 1, 2, \ldots, n$, where k is an integer that is not a perfect square, cannot always be expressed by the binary quadratic form $\phi(x, y) = ax^2 + bxy + cy^2$, and hence such an arithmetic progression cannot be considered equivalent to the arithmetic progression $u_i, i = 1, 2, \dots, n$.

We now prove a preliminary lemma concerning arithmetic progressions of rational numbers whose terms are all expressible by a binary quadratic form $\phi(x, y) = ax^2 + bxy + cy^2$ using rational values of x and y.

Lemma 1. *If there exists an arithmetic progression of rational numbers, $u_i, i = 1, 2, \dots, n$, such that all the terms u_i can be expressed by the integral binary quadratic form $\phi(x, y) = ax^2 + bxy + cy^2$ using rational values of the variables x and y, that is, for each i, we have $\phi(x_i, y_i) = u_i, i = 1, 2, \dots, n$, where x_i, y_i are rational numbers, then, for a suitably chosen integer value of k, all the terms of the arithmetic progression $k^2u_i, i = 1, 2, \dots, n$, are integers that can be represented by the form $\phi(x, y) = ax^2 + bxy + cy^2$ using integer values of the variables x and y.*

Proof. Since $\phi(x_i, y_i) = u_i, i = 1, 2, \dots, n$, it follows that $\phi(kx_i, ky_i) = k^2u_i, i = 1, 2, \dots, n$. Hence, taking k to be the least common multiple of the denominators of all the numbers $x_i, y_i, i = 1, 2, \dots, n$, we obtain the arithmetic progression $k^2u_i, i = 1, 2, \dots, n$, all of whose terms can be represented by the form $\phi(x, y) = ax^2 + bxy + cy^2$ using integer values of the variables x and y, and naturally all the terms of the arithmetic progression are integers. □

3. Arithmetic Progressions of Nine Terms Represented by the Binary Quadratic Form $px^2 + qy^2$

In this section we will explicitly construct a two-parameter arithmetic progression of nine terms that can all be represented by an irreducible integral binary quadratic form $px^2 + qy^2$, and then show that, in certain cases, it is possible to extend the 9-term arithmetic progression to 11 terms all of which can be represented by the aforesaid quadratic form.

3.1. An Arithmetic Progression of Nine Terms

Theorem 1. *If p and q are arbitrary integers such that the binary quadratic form $px^2 + qy^2$ is irreducible, and we define two integers u_1 and d in terms of p, q and two arbitrary integer parameters g and h by*

$$\begin{aligned} u_1 &= 4p^5g^{10} - 47p^4qg^8h^2 - 156p^3q^2g^6h^4 + 2052p^2q^3g^4h^6 \\ &\quad + 4833pq^4g^2h^8 + 324q^5h^{10}, \\ d &= 12pqg^2h^2(pg^2 - 3qh^2)(pg^2 + 6qh^2)(2pg^2 + 3qh^2), \end{aligned} \tag{3.1}$$

all the nine terms of the arithmetic progression $u_i, i = 1, 2, \dots, 9$, where $u_i = u_1 + (i - 1)d$, can be represented by the binary quadratic form $px^2 + qy^2$.

Proof. Let y_1, y_2, y_3 be integers such that y_1^2, y_2^2, y_3^2 are in arithmetic progression so that

$$y_1^2 - 2y_2^2 + y_3^2 = 0, \tag{3.2}$$

and the common difference of the arithmetic progression is $d = y_2^2 - y_1^2$.

We now construct three arithmetic progressions $(u_1, u_2, u_3), (u_4, u_5, u_6)$ and (u_7, u_8, u_9) as follows:

$$\begin{aligned}(u_1, u_2, u_3) &= (px_1^2 + qy_1^2, px_1^2 + qy_2^2, px_1^2 + qy_3^2),\\ (u_4, u_5, u_6) &= (px_2^2 + qy_1^2, px_2^2 + qy_2^2, px_2^2 + qy_3^2),\\ (u_7, u_8, u_9) &= (px_3^2 + qy_1^2, px_3^2 + qy_2^2, px_3^2 + qy_3^2),\end{aligned} \tag{3.3}$$

where x_1, x_2, x_3 are arbitrary integers. The above three arithmetic progressions have the same common difference $d = q(y_2^2 - y_1^2)$, and all the terms of the three arithmetic progressions are expressible by the quadratic form $px^2 + qy^2$. The terms $u_i, i = 1, 2, \ldots, 9$, will constitute the terms of a single arithmetic progression of nine terms if $u_4 = u_1 + 3d$ and $u_7 = u_1 + 6d$. Thus we will obtain an arithmetic progression of nine terms if we solve the following simultaneous diophantine equations:

$$px_1^2 + 3q(y_2^2 - y_1^2) = px_2^2, \tag{3.4}$$

$$px_1^2 + 6q(y_2^2 - y_1^2) = px_3^2. \tag{3.5}$$

As Equation (3.2) is an equation of degree 2 in three parameters, its solution is readily obtained and may be written as follows:

$$y_1 = h(m^2 + 2m - 1), \quad y_2 = h(m^2 + 1), \quad y_3 = h(m^2 - 2m - 1), \tag{3.6}$$

where h and m are arbitrary parameters.

Next, we eliminate y_1 and y_2 from Equations (3.4) and (3.5), and get

$$x_1^2 - 2x_2^2 + x_3^2 = 0. \tag{3.7}$$

Equation (3.7) is similar to Equation (3.2) and its solution may, accordingly, be written as follows:

$$x_1 = g(n^2 + 2n - 1), \quad x_2 = g(n^2 + 1), \quad x_3 = g(n^2 - 2n - 1), \tag{3.8}$$

where g and n are arbitrary parameters.

On substituting the values of x_i and $y_i, i = 1, 2$, given by (3.8) and (3.6), respectively, in Equation (3.4), and transposing all terms to the left-hand side, we get

$$12qm(m-1)(m+1)h^2 - 4pn(n-1)(n+1)g^2 = 0. \tag{3.9}$$

To solve Equation (3.9), we write $n = m + 1$, and now Equation (3.9) can be readily solved, and we get

$$m = (3h^2q + 2g^2p)/(3h^2q - g^2p). \tag{3.10}$$

Since $n = m + 1$, we get

$$n = (6h^2q + g^2p)/(3h^2q - g^2p). \tag{3.11}$$

Using the values of m and n given by (3.10) and (3.11), respectively, and the relations (3.6) and (3.8), we get a solution of the simultaneous diophantine equations (3.2), (3.4) and (3.5). As these three equations are homogeneous, we may write the solution already obtained, after appropriate scaling, as follows:

$$\begin{aligned}
x_1 &= -(2p^2g^4 - 12pqg^2h^2 - 63q^2h^4)g, \\
x_2 &= (2p^2g^4 + 6pqg^2h^2 + 45q^2h^4)g, \\
x_3 &= (2p^2g^4 + 24pqg^2h^2 - 9q^2h^4)g, \\
y_1 &= -(p^2g^4 - 24pqg^2h^2 - 18q^2h^4)h, \\
y_2 &= (5p^2g^4 + 6pqg^2h^2 + 18q^2h^4)h, \\
y_3 &= (7p^2g^4 + 12pqg^2h^2 - 18q^2h^4)h,
\end{aligned} \tag{3.12}$$

where g and h are arbitrary parameters.

We thus get an arithmetic progression of nine terms, whose first term u_1 and common difference d are given by the relations (3.1), such that all the nine terms of this arithmetic progression are expressible by the binary quadratic form $px^2 + qy^2$. The representations of the nine terms $u_1, u_2, \ldots, u_9$, by the form $px^2 + qy^2$ are given by the relations (3.3). This proves the theorem. □

We note that even if p and q are rational numbers such that the form $px^2 + qy^2$ is irreducible, we can find arithmetic progressions of nine terms such that all the nine terms are expressible as $px^2 + qy^2$, and by appropriate scaling, we can ensure that x and y are integers.

3.2. Extension of the Nine-term Arithmetic Progression to 11 Terms

We will now describe a method by which the arithmetic progression of nine terms obtained in Section 3.1 can sometimes be extended to an arithmetic progression of 11 terms that can all be represented by the given quadratic form.

With the arithmetic progression defined by (3.1), we first express d/q as a difference of two rational squares, $Y_2^2 - Y_1^2$, and then try to ensure that the tenth term of the arithmetic progression can be written as $pX^2 + qY_1^2$ where X is some rational number. If this condition is satisfied, the eleventh term of the arithmetic progression may be written as $pX^2 + qY_1^2 + d = pX^2 + qY_2^2$, and hence both the tenth and the eleventh terms of the arithmetic progression are expressible by the quadratic form $px^2 + qy^2$ albeit using rational numbers. On applying Lemma 1, we can now get an arithmetic progression of 11 terms that can be represented by the quadratic form $px^2 + qy^2$ using integer values of x and y.

To choose $Y_i, i = 1, 2$, suitably, we write

$$\begin{aligned} Y_2 - Y_1 &= 4h(2pg^2 + 3qh^2)(pg^2 - 3qh^2)\xi, \\ Y_2 + Y_1 &= 3pg^2h(pg^2 + 6qh^2)/\xi, \end{aligned} \tag{3.13}$$

where ξ is some nonzero rational number, so that $Y_2^2 - Y_1^2 = d/q$, and on solving Equations (3.13), we get

$$\begin{aligned} Y_1 &= (3(pg^2 + 6qh^2)pg^2h - 4(2pg^2 + 3qh^2)(pg^2 - 3qh^2)\xi^2h)/(2\xi), \\ Y_2 &= (3(pg^2 + 6qh^2)pg^2h + 4(2pg^2 + 3qh^2)(pg^2 - 3qh^2)\xi^2h)/(2\xi). \end{aligned} \tag{3.14}$$

The condition that the tenth term of the arithmetic progression may be expressible as $pX^2 + qY_1^2$ reduces, on writing $X = \eta/(2p\xi)$ and after suitable transposition of terms, to

$$\begin{aligned} &-16(2pg^2 + 3qh^2)^2(pg^2 - 3qh^2)^2pqh^2\xi^4 + 4(4p^5g^{10} + 181p^4qg^8h^2 \\ &\quad + 870p^3q^2g^6h^4 - 1026p^2q^3g^4h^6 - 1323pq^4g^2h^8 + 324q^5h^{10})p\xi^2 \\ &\qquad - 9p^5qg^8h^2 - 108p^4q^2g^6h^4 - 324p^3q^3g^4h^6 = \eta^2. \end{aligned} \tag{3.15}$$

Equation (3.15) may be considered as a quartic curve in ξ and η defined over the function field $\mathbb{Q}(g, h)$, and we have to perform trials to obtain a solution.

As a numerical example, we will apply the above method to obtain an arithmetic progression of 11 terms with all the terms being expressible as sums of two squares, that is, the arithmetic progression is representable by the quadratic form $x^2 + y^2$.

Taking $(p, q) = (1, 1)$, and proceeding as in Section 3, we first obtain an arithmetic progression of nine terms representable by the quadratic form $x^2 + y^2$, and to extend this arithmetic progression to 11 terms, we have to solve Equation (3.15).

With $(p, q) = (1, 1)$, a solution of Equation (3.15), found by trial, is as follows:

$$(g, h, \xi, \eta) = (4, 1, 30/7, 121656/7). \tag{3.16}$$

Taking $(g, h) = (4, 1)$, and using the relations (3.1), we get an arithmetic progression whose first term is 1078100, common difference is 1921920, and the first nine terms of the arithmetic progression are all expressible as sums of two squares. Further, according to the above method, the tenth and eleventh terms of our arithmetic progression namely, 18375380 and 20297300, respectively, can be expressed as sums of two squares of rational numbers as follows:

$$18375380 = (10138/5)^2 + (18884/5)^2, \quad 20297300 = (10138/5)^2 + (20116/5)^2.$$

We found by direct computation that both 18375380 and 20297300 can, in fact, be represented as sums of two squares of integers. Further, we note that $\gcd(1078100, 1921920) = 20$, and we can divide all the terms of our arithmetic progression by 4 and thus obtain a numerically smaller arithmetic progression beginning with 269525 and having common difference 480480, and such that all the 11 terms of the smaller arithmetic progression can be represented as sums of two squares of integers. We give below the representation, as sums of two squares, of all the 11 terms of the smaller arithmetic progression beginning 269525:

$$\begin{array}{lll} 269525 = 514^2 + 73^2, & 750005 = 514^2 + 697^2, & 1230485 = 514^2 + 983^2, \\ 1710965 = 1306^2 + 73^2, & 2191445 = 1306^2 + 697^2, & 2671925 = 1306^2 + 983^2, \\ 3152405 = 1774^2 + 73^2, & 3632885 = 1774^2 + 697^2, & 4113365 = 1774^2 + 983^2, \\ 4593845 = 151^2 + 2138^2, & 5074325 = 410^2 + 2215^2. & \end{array}$$

We note that when $(g, h) = (4, 1)$, Equation (3.15) represents a quartic model of an elliptic curve defined by

$$-3312400\xi^4 + 77345360\xi^2 - 1115136 = \eta^2, \tag{3.17}$$

with one rational point on the curve (3.17) being $(\xi, \eta) = (30/7, 121656/7)$. It has been verified that the elliptic curve defined by the quartic equation (3.17) is of rank 2, and there are infinitely many rational points on the curve (3.17). However, since the first term and the common difference of the arithmetic progression are determined by g and h only, the infinitely many rational solutions of the quartic equation (3.17) do not yield distinct arithmetic progressions that may be represented by the quadratic form $x^2 + y^2$.

To obtain more arithmetic progressions of length 11 that can be represented by the quadratic form x^2+y^2, we may multiply each term of the arithmetic progression of 11 terms obtained above by $\alpha^2 + \beta^2$, where α and β are arbitrary integers such that $\alpha^2 + \beta^2$ is not a perfect square, and thus obtain a new arithmetic progression of length 11 that can be represented by the quadratic form $x^2 + y^2$. Each term of the new arithmetic progression is expressible as a sum of two squares in view of the following composition of forms identity:

$$(\alpha^2 + \beta^2)(m^2 + n^2) = (\alpha m + \beta n)^2 + (\alpha n - \beta m)^2.$$

While all such arithmetic progressions are scalar multiples of the first arithmetic progression of 11 terms, since $\alpha^2 + \beta^2$ is not a perfect square, they should not be considered equivalent to the first arithmetic progression. We thus obtain infinitely many arithmetic progressions of 11 terms that can be represented by the quadratic form $x^2 + y^2$.

4. Arithmetic Progressions of Nine Terms Represented by the Binary Quadratic Form $ax^2 + bxy + cy^2$

Theorem 2. *Given an arbitrary irreducible integral binary quadratic form, it is always possible to construct arithmetic progressions of nine terms such that all the terms of these arithmetic progressions can be represented by the given binary quadratic form.*

Proof. Let $ax^2 + bxy + cy^2$ be an arbitrary irreducible integral binary quadratic form so that the discriminant $b^2 - 4ac$ is not a perfect square. Since

$$ax^2 + bxy + cy^2 = a(x + by/(2a))^2 + (4ac - b^2)y^2/(4a),$$

on writing $(p, q) = (a, (4ac - b^2)/(4a))$, and

$$x + by/(2a) = X, \quad y = Y, \tag{4.1}$$

we get $ax^2 + bxy + cy^2 = pX^2 + qY^2$. As in Section 3, we can obtain arithmetic progressions of nine terms that can be represented by the form pX^2+qY^2. Using the relations (4.1), we may express all the nine terms of these arithmetic progressions by the form $ax^2 + bxy + cy^2$ using rational values of x and y. It now follows from Lemma 1 that we can obtain arithmetic progressions of nine terms that can all be represented by the form $ax^2+bxy+cy^2$ using integer values of x and y. This proves the theorem. □

As an example, the form $\phi(x, y) = x^2 + xy + y^2$, which may be written as $X^2 + 3Y^2/4$, where $X = x + y/2, Y = y$, represents an arithmetic progression of nine terms, with the first term and the common difference of the arithmetic progression being given by

$$1024g^{10} - 9024g^8h^2 - 22464g^6h^4 + 221616g^4h^6 + 391473g^2h^8 + 19683h^{10}$$

and

$$72(2g + 3h)(2g - 3h)(8g^2 + 9h^2)(2g^2 + 9h^2)g^2h^2,$$

respectively, where g and h are arbitrary parameters.

We could not find suitable values of g and h to extend this arithmetic progression to a longer one that can be represented by the form $x^2 + xy + y^2$.

As a numerical example, taking $(g, h) = (2, 1)$, we get an arithmetic progression of nine terms beginning with 2432167 and with common difference 1405152 such that all the terms of the arithmetic progression may be represented by the form

$\phi(x, y)$ as follows:

$$2432167 = \phi(733, 1058), \qquad 3837319 = \phi(397, 1730),$$
$$5242471 = \phi(159, 2206), \qquad 6647623 = \phi(1881, 1058),$$
$$8052775 = \phi(1545, 1730), \qquad 9457927 = \phi(1307, 2206),$$
$$10863079 = \phi(2637, 1058), \qquad 12268231 = \phi(2301, 1730),$$
$$13673383 = \phi(2063, 2206).$$

5. An Open Problem

It would be of interest to devise a method that generates long sequences of arithmetic progressions that can be represented by an arbitrary irreducible integral binary quadratic form, or a specific quadratic form such as $x^2 + y^2$. It would be a more challenging problem to find binary quadratic forms that can represent arithmetic progressions whose common difference is small. For instance, it would be interesting to find binary quadratic forms that can represent long sequences of consecutive integers.

Acknowledgement. The author is grateful to the referee for his/her comments and guidance which have led to improvements in the paper.

References

[1] A. Alaca, Ş. Alaca, and K. S. Williams, Arithmetic progressions and binary quadratic forms, *Amer. Math. Monthly* **115** (2008), 252-254.

[2] A. Choudhry and B. Maji, Finite sequences of integers expressible as sums of two squares, *Int. J. Number Theory* **20** (2024), 1755-1766.

[3] T. Cochrane and R. E. Dressler, Consecutive triples of sums of two squares, *Arch. Math.* **49** (1987), 301-304.

[4] P. K. Dey and R. Thangadurai, The length of an arithmetic progression represented by a binary quadratic form, *Amer. Math. Monthly* **121** (2014), 932-936.

[5] C. Elsholtz and C. Frei, Arithmetic progressions in binary quadratic forms and norm forms, *Bull. Lond. Math. Soc.* **51** (2019), 595-602.

[6] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. of Math. (2)* **167** (2008), 481-547.

[7] Mathematics Stack Exchange website https://math.stackexchange.com/questions/4498751/arithmetic-progressions-of-sums-of-two-squares

[8] H. Weber, Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist, *Math. Ann.* **20** (1882), 301-329.