The Length of an Arithmetic Progression Represented by a Binary Quadratic Form

Pallab Kanti Dey and R. Thangadurai

Abstract. In this paper we prove that if $Q(x, y) = ax^2 + bxy + cy^2$ is an integral binary quadratic form with a nonzero, nonsquare discriminant d and if Q represents an arithmetic progression $\{kn + \ell : n = 0, 1, \ldots, R - 1\}$, where k and ℓ are positive integers, then there are absolute constants $C_1 > 0$ and $L_1 > 0$ such that $R < C_1\ell(k^2|d|)^{L_1}$. Moreover, we prove that every nonzero integral binary quadratic form represents a nontrivial 3-term arithmetic progression infinitely often.

Let $Q(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form of discriminant $d = b^2 - 4ac \neq 0$. Recently, A. Alaca, Ş. Alaca, and K. S. Williams [**1**] proved that Q represents an arithmetic progression of infinite length if and only if d is a perfect square, that is, $d = m^2$ for some nonzero integer m. Suppose from now on that d is not a perfect square so that Q cannot represent an arithmetic progression of infinite length. We address the question "How long can an arithmetic progression represented by Q be?" Making use of the ideas used by Alaca, Alaca, and Williams in the proof of their theorem [**1**], we obtain an upper bound for the length of any arithmetic progression represented by Q.

We require the following result.

Proposition 1. *Let $N \equiv 0 \pmod 4$ be a nonzero integer which is not a perfect square. Then there exist absolute constants $C > 0$ and $L > 0$ for which there is a prime $p \neq 2$ satisfying*

$$p \leq C|N|^L, \quad \left(\frac{N}{p}\right) = -1.$$

Proof. As $N \equiv 0 \pmod 4$ is not a perfect square there is an integer a satisfying

$$\left(\frac{N}{a}\right) = -1, \text{ where } 1 \leq a \leq |N| - 1,$$

see for example [**2**, p. 298]. Clearly $(a, |N|) = 1$ so, by Linnik's theorem [**5**], there are absolute constants $C > 0$ and $L > 0$ such that the least prime p in the arithmetic progression

$$\{|N|k + a : \quad k = 0, 1, 2, \ldots\}$$

satisfies

$$p \leq C|N|^L.$$

http://dx.doi.org/10.4169/amer.math.monthly.121.10.932
MSC: Primary 11E25, Secondary 11E12

Since p belongs to this arithmetic progression, we have $p \equiv a \pmod{|N|}$ and, by [**2**, Lemma 2.3, p. 291] we deduce

$$\left(\frac{N}{p}\right) = \left(\frac{N}{a}\right) = -1.$$

Finally, as $N \equiv 0 \pmod 4$ and $\left(\frac{N}{p}\right) = -1$, we see that $p \neq 2$. ∎

Remark. By a deep result of Xylouris [**8**], one has $L \leq 5.2$. Xylouris's work is a refinement of that of Heath-Brown [**4**], who showed that L satisfies $L \leq 5.5$.

In this short note we prove the following result.

Theorem 1. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form with discriminant $d = b^2 - 4ac \neq 0$. Suppose that d is not a perfect square and that Q represents an arithmetic progression $\{kn + \ell : n = 0, 1, \ldots, R - 1\}$, where k and ℓ are positive integers. Then there are absolute constants $C_1 > 0$ and $L_1 > 0$ such that $R < C_1 \ell (k^2|d|)^{L_1}$.*

Proof. Set $N = 4k^2 d$ so that N is a nonzero integer with $N \equiv 0 \pmod 4$ which is not a perfect square. By the Proposition 1, there are absolute constants $C > 0$ and $L > 0$ for which there is a prime $p \neq 2$ satisfying

$$p \leq C|N|^L, \quad \left(\frac{N}{p}\right) = -1.$$

Hence $\left(\frac{4k^2 d}{p}\right) = -1$ and thus

$$(d, p) = (k, p) = 1, \quad \left(\frac{d}{p}\right) = -1.$$

If $p|ac$, then

$$-1 = \left(\frac{b^2 - 4ac}{p}\right) = \left(\frac{b^2}{p}\right) = 0 \quad \text{or} \quad 1,$$

which is impossible. Hence $(ac, p) = 1$.

As $(k, p) = 1$, there exists an integer t with $1 \leq t < p^2$ such that $kt \equiv 1 \pmod{p^2}$. Define the integer u by $u = (kt - 1)/p^2$ so that $kt = 1 + up^2$. As $kt \geq 1$, we see that $u \geq 0$. Furthermore, as $up^2 < kt < kp^2$ we have $u < k$. Hence

$$kt = 1 + up^2, \quad 1 \leq t < p^2, \quad 0 \leq u < k.$$

We now construct an integer n with $1 \leq n < C^3 \ell |N|^{3L}$ such that $p|(kn + \ell)$ and $p^2 \nmid (kn + \ell)$.

If $p > \ell$, we choose $n = t(p - \ell)$. Note that $1 \le n < p^3$. Since $p \le C|N|^L$, it is clear that $n < C^3|N|^{3L} \le C^3\ell|N|^{3L}$. Also, we see that

$$kn + \ell = kt(p - \ell) + \ell = (1 + up^2)(p - \ell) + \ell = p(1 + up^2 - up\ell),$$

so that $p|(kn + \ell)$ and $p^2 \nmid (kn + \ell)$ as required.

If $p \le \ell$ and $p \nmid \ell$, then we choose $n = \ell t(p - 1)$. Note that $1 \le n < \ell p^3 \le C^3\ell|N|^{3L}$. Moreover, we have

$$kn + \ell = k\ell t(p - 1) + \ell = \ell(1 + up^2)(p - 1) + \ell = \ell p(1 + up^2 - up)$$

so that $p|(kn + \ell)$ and $p^2 \nmid (kn + \ell)$.

If $p \le \ell$ and $p\|\ell$, then we choose $n = tsp$, where the positive integer $s = \ell/p$ is not divisible by p. Clearly $1 \le n < \ell p^3 < C^3\ell|N|^{3L}$. Here

$$kn + \ell = ktsp + \ell = (1 + up^2)sp + sp = sp(2 + up^2),$$

so that $p|(kn + \ell)$ and (as $p \ne 2$ and $p \nmid s$) $p^2 \nmid (kn + \ell)$.

Finally, if $p \le \ell$ and $p^2|\ell$, we choose $n = tp$. Note that $1 \le n < p^3 \le C^3|N|^{3L} \le C^3\ell|N|^{3L}$. In this case we have

$$kn + \ell = ktp + \ell = (1 + up^2)p + \ell = p(1 + up^2 + (\ell/p)),$$

so that $p|(kn + \ell)$ and (as $p|(\ell/p)$) $p^2 \nmid (kn + \ell)$.

This completes the construction of an integer n satisfying $1 \le n < C^3\ell|N|^{3L}$ such that $p|(kn + \ell)$ and $p^2 \nmid (kn + \ell)$.

Next we show that the integer $kn + \ell$ is not represented by Q. Suppose on the contrary that the integer $kn + \ell$ is represented by Q. Then there exist integers x and y such that $kn + \ell = ax^2 + bxy + cy^2$. Since $p|(kn + \ell)$, we have $ax^2 + bxy + cy^2 \equiv 0 \pmod{p}$. Therefore, since

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

we see that $(2ax + by)^2 \equiv dy^2 \pmod{p}$. If $p \nmid y$ then $d \equiv ((2ax + by)z)^2 \pmod{p}$ for some integer z such that $yz \equiv 1 \pmod{p}$. This contradicts that $\left(\frac{d}{p}\right) = -1$. If $p|y$ then $p|(2ax + by)$ so $p|2ax$. But $p \ne 2$ and $p \nmid a$ hence $p|x$. Therefore, p^2 divides $ax^2 + bxy + cy^2 = kn + \ell$, contradicting $p^2 \nmid (kn + \ell)$. This completes the proof that the integer $kn + \ell$ is not represented by Q.

Since all the integers $\ell, k + \ell, 2k + \ell, \ldots, (R - 1)k + \ell$ are represented by Q, we must have $n > R - 1$, that is, $R \le n$. But $n < C^3\ell|N|^{3L}$ so $R < C^3\ell|4k^2d|^{3L} = C_1\ell(k^2|d|)^{L_1}$, where L_1 and C_1 are absolute constants satisfying $L_1 = 3L > 0$ and $C_1 = C^3 2^{6L} > 0$. ∎

Remark. There is no loss of generality in assuming that Q represents an arithmetic progression of *positive* integers since if Q only represents an arithmetic progression of negative integers then $-Q$ represents an arithmetic progression of positive integers.

The least length of a nontrivial arithmetic progression is 3. Does every nonzero integral binary quadratic form represent an arithmetic progression of length 3? Two deep results of Weber [**7**] and Green [**3**] positively answer the above question in the particular case when the integral binary quadratic form is positive-definite. In 1882, Weber [**7**] proved that if Q is a primitive integral binary quadratic form which is positive-definite, then the set of primes that are represented by Q has positive relative density. In 2006 Green [**3**] proved that any subset of primes having positive relative density has a 3-term arithmetic progression. Thus, by putting these two deep results together, we see that every primitive, positive-definite, integral binary quadratic form represents a 3-term arithmetic progression. In this paper we shall prove in an elementary way that any nonzero integral, binary quadratic form represents a nontrivial arithmetic progression of length 3 infinitely often.

Theorem 2. *Every nonzero integral binary quadratic form represents a nontrivial arithmetic progression of length* 3 *infinitely often.*

Proof. Let $Q(x, y) = ax^2 + bxy + cy^2$ be a nonzero, integral binary quadratic form. Since Q is nonzero, at least one of the integers a, b, and c is nonzero. We consider the following cases.

Case 1: $a \neq 0$.

Let x be a positive integer. Then, as

$$\begin{aligned} Q(2x^2 - 1, 0) &= a(4x^4 - 4x^2 + 1), \\ Q(2x^2 + 2x + 1, 0) &= a(4x^4 + 8x^3 + 8x^2 + 4x + 1) \\ &= a(4x^4 - 4x^2 + 1) + a(8x^3 + 12x^2 + 4x), \end{aligned}$$

and

$$\begin{aligned} Q(2x^2 + 4x + 1, 0) &= a(4x^4 + 16x^3 + 20x^2 + 8x + 1) \\ &= a(4x^4 - 4x^2 + 1) + 2a(8x^3 + 12x^2 + 4x), \end{aligned}$$

Q represents a nontrivial arithmetic progression of length 3 infinitely often.

Case 2: $a = 0$

In this case, $Q(x, y) = bxy + cy^2$ and its discriminant is $d = b^2$.

Subcase (i): $b \neq 0$

Since d is a nonzero perfect square, by the result of Alaca *et al.* [**1**], the form $Q(x, y)$ represents an infinite arithmetic progression in positive integers and hence it represents a nontrivial arithmetic progression of length 3 infinitely often.

Subcase (ii): $b = 0$

In this case we have $Q(x, y) = cy^2$, where $c \neq 0$, as $a = b = 0$. Then, taking x to be any integer and proceeding similarly as in the first case, we deduce that $Q(x, y)$ represents infinitely many nontrivial arithmetic progressions of length 3. ∎

Remark. The statement of Theorem 2 is not true in general if we replace 3 by a larger integer. For example, $Q(x, y) = x^2$ does not represent an arithmetic progression of length 4 as there do not exist 4 squares in arithmetic progression (see [**6**, pp. 21–22]).

ACKNOWLEDGMENTS. We are grateful to the referees for going through the paper very carefully and modifying it to a much nicer form.

1. A. Alaca, Ş. Alaca, K. S. Williams, Arithmetic progressions and binary quadratic forms, *Amer. Math. Monthly* **115** (2008) 252–254.
2. R. Ayoub, *An Introduction to the Analytic Theory of Numbers*. Mathematical Surveys, Number 10, American Mathematical Society, Providence, Rhode Island, 1963, http://dx.doi.org/10.1090/surv/010.
3. B. Green, Roth's theorem in the primes, *Ann. Math.* **161** (2005) 1609–1636, http://dx.doi.org/10.4007/annals.2005.161.1609.
4. D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression, *Proc. London Math. Soc*. (3) **62** (1992) 265–338, http://dx.doi.org/10.1112/plms/s3-64.2.265.
5. Y. V. Linnik, On the least prime in an arithmetic progression *I*. The basic theorem, *Rec. Math. (Mat. Sbornik) N. S.* **15** no. 57 (1944) 139–178.
6. L. J. Mordell, *Diophantine Equations*. Pure and Applied Mathematics, Vol. 30, Academic Press, London, 1969.
7. H. Weber, Beweis des Satzes, daß jede eigentlich primitive quadratische Form un endliche viele Primzahlen darzustellen fähig ist, *Math. Ann.* **20** (1882) 301–329.
8. T. Xylouris, *Über die Linniksche Konstante,* Diplomarbeit, Universität Bonn, 2009. (arXiv:0906.2749v1 [math.NT] 15 Jun 2009).

Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019, India
pallabdey@hri.res.in

Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019, India
thanga@hri.res.in