**Amer. Math. Monthly 115 (2008), 252-254.**

# Arithmetic Progressions and Binary Quadratic Forms

**Ayşe Alaca, Şaban Alaca, and Kenneth S. Williams**

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$, and $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. For $k \in \mathbb{N}$ and $l \in \mathbb{N}$

$$k\mathbb{N}_0 + l = \{l, k+l, 2k+l, \ldots\}$$

is a (nonconstant) arithmetic progression of positive integers. We consider a general binary quadratic form $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ and ask the question "Can the form $ax^2 + bxy + cy^2$ represent every integer in the arithmetic progression $k\mathbb{N}_0 + l$ for any natural numbers $k$ and $l$?" In a sampling of books containing a discussion of binary quadratic forms [**2**]–[**9**], we did not find this question treated. In answering our question we shall see that the discriminant $d = b^2 - 4ac \in \mathbb{Z}$ of the form $ax^2 + bxy + cy^2$ plays a key role. We prove:

**Theorem.** *A binary quadratic form $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ can represent all the integers in some arithmetic progression $k\mathbb{N}_0 + l$ $(k, l \in \mathbb{N})$ if and only if its discriminant is a nonzero perfect square.*

Before beginning the proof we note that if $r(\neq 0) \in \mathbb{Z}$ and $s \in \mathbb{Z}$ then $k\mathbb{N}_0 + l \subset r\mathbb{Z} + s$ with $k = |r| \in \mathbb{N}$ and $l$ any positive integer in $r\mathbb{Z} + s$.

*Proof.* Clearly the zero form $(a = b = c = 0)$ has discriminant equal to 0 and it only represents 0. Thus we need only consider nonzero forms.

We begin by observing that if $A$ is a fixed nonzero integer then the set of values of $Ax^2$ $(x \in \mathbb{N})$ cannot contain an infinite arithmetic progression of integers as it contains unbounded gaps of integers. Since a nonzero binary quadratic form $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ of discriminant equal to 0 is of the form $A(Bx + Cy)^2$ for some integers $A(\neq 0)$, $B$, and $C$ with $\gcd(B, C) = 1$, it cannot represent all the integers in $k\mathbb{N}_0 + l$ for any $k, l \in \mathbb{N}$.

If the form $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ has a discriminant which is a nonzero perfect square and $a \neq 0$ then

$$a(ax^2 + bxy + cy^2) = (ax + gy)(ax + hy)$$

for some integers $g$ and $h$ with $g \neq h$ and at least one of $g$ and $h$ nonzero, say $g \neq 0$. Set $m = \gcd(a, g) \in \mathbb{N}$. Let $x_0, y_0 \in \mathbb{Z}$ be such that $ax_0 + gy_0 = am$. Choose $x = x_0 + gt/m$ and $y = y_0 - at/m$, where $t \in \mathbb{Z}$, so that $x, y \in \mathbb{Z}$ and $ax + gy = am$. Then $ax^2 + bxy + cy^2 = m(ax + hy) = a(g - h)t + m(ax_0 + hy_0)$ takes on all the values in the arithmetic progression $r\mathbb{Z} + s$, where $r = a(g - h) \in \mathbb{Z}\backslash\{0\}$ and $s = m(ax_0 + hy_0) \in \mathbb{Z}$. Thus, by the remark preceding the proof, $ax^2 + bxy + cy^2$ takes on all the values in the arithmetic progression $k\mathbb{N}_0 + l$, where $k = |r| \in \mathbb{N}$ and $l$ is any positive integer in $r\mathbb{Z} + s$.

If the form $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ has a discriminant which is a nonzero perfect square and $a = 0$ then $b \neq 0$ and we see that $ax^2 + bxy + cy^2 = y(bx + cy)$ represents every integer in the arithmetic progression $b\mathbb{Z} + c$ by taking $y = 1$. Thus, by the remark preceding the proof, $ax^2 + bxy + cy^2$ takes on all the values in the arithmetic progression $k\mathbb{N}_0 + l$, where $k = |b| \in \mathbb{N}$ and $l$ is any positive integer in $b\mathbb{Z} + c$.

Finally we show that a binary quadratic form $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ having a discriminant which is not a perfect square cannot represent all the integers in $k\mathbb{N}_0 + l$ for any $k, l \in \mathbb{N}$. Suppose on the contrary that the binary quadratic form $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ of nonsquare discriminant $d = b^2 - 4ac$ represents all the integers in $k\mathbb{N}_0 + l$ for some $k, l \in \mathbb{N}$. Let $\left(\frac{d}{*}\right)$ denote the Kronecker symbol for discriminant $d$ [**1**, p. 290]. It is a well-known result that as $d$ is not a perfect square there exists an integer $m$ such that $\left(\frac{d}{m}\right) = -1$; see for example [**1**, p. 292]. As $\gcd(|d|, m) = 1$, by Dirichlet's theorem on primes in arithmetic progression [**1**, p. 23] there exist infinitely many primes congruent to $m \pmod{|d|}$. We can therefore choose a prime $p > \max(4|a|, m, k, l)$ such that $p \equiv m \pmod{|d|}$. Next we recall that if $m_1, m_2 \in \mathbb{N}$ and $m_1 \equiv m_2 \pmod{|d|}$ then $\left(\frac{d}{m_1}\right) = \left(\frac{d}{m_2}\right)$; see for example [**1**, p. 291]. Hence

$$\left(\frac{d}{p}\right) = \left(\frac{d}{m}\right) = -1.$$

As $p$ is a prime and $p > k$, we have $p \nmid k$, so there are integers $t$ and $u$ such that

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

Set $n = t(p^2 + p - l) \in \mathbb{N}$. A short calculation shows that

$$kn + l = p(1 + (1 - lu)p + up^2 + up^3)$$

so that $p \mid kn + l$ and $p^2 \nmid kn + l$. By assumption there exist integers $x$ and $y$ such that $kn + l = ax^2 + bxy + cy^2$. Hence

$$(2ax + by)^2 = 4a(kn + l) + dy^2 \equiv dy^2 \pmod{p}.$$

Suppose $p \nmid y$. Then there exists an integer $z$ such that $yz \equiv 1 \pmod{p}$ and

$$((2ax + by)z)^2 \equiv dy^2z^2 \equiv d \pmod{p}$$

so that $\left(\frac{d}{p}\right) = 0$ or $1$, contradicting $\left(\frac{d}{p}\right) = -1$. Hence $p \mid y$. Thus $p \mid 2ax + by$ and so $p^2 \mid 4a(kn + l)$. But $p > 4|a|$ so $p \nmid 4a$. Thus $p^2 \mid kn + l$. This is the required contradiction.

The proof is now complete. ■

We leave the reader with a problem: If $ax^2 + bxy + cy^2$ $(a, b, c \in \mathbb{Z})$ has a discriminant which is a nonzero perfect square, classify all the arithmetic progressions $k\mathbb{N}_0 + l$ $(k, l \in \mathbb{N})$ which it represents.

## REFERENCES


1. R. Ayoub, *An Introduction to the Analytic Theory of Numbers,* American Mathematical Society, Providence, RI, 1963.
2. D. A. Buell, *Binary Quadratic Forms,* Springer-Verlag, New York, 1989.
3. H. Cohn, *Advanced Number Theory,* Dover, New York, 1980.
4. L. E. Dickson, *Modern Elementary Theory of Numbers,* University of Chicago Press, 1939.
5. L. E. Dickson, *Introduction to the Theory of Numbers,* Dover, New York, 1957.
6. L.-K. Hua, *Introduction to Number Theory,* Springer-Verlag, Berlin, 1982.
7. W. Narkiewicz, *Classical Problems in Number Theory,* Polish Scientific Publishers, Warsaw, 1986.
8. I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers,* 5th ed., John Wiley, New York, 1991.
9. J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory,* McGraw-Hill, 1939.



*Centre for Research in Algebra and Number Theory, School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6*
*aalaca@math.carleton.ca,*
*salaca@math.carleton.ca,*
*williams@math.carleton.ca*