ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 9, Number 2, Spring 1979

ARITHMETIC PROGRESSIONS IN THE VALUES OF A QUADRATIC POLYNOMIAL

BENNETT SETZER

ABSTRACT. The following theorem is proved:

THEOREM. *Let A, B, C, $A \neq 0$ be rational numbers. There do not exist four unequal rational numbers x_1, x_2, x_3, x_4 such that $f(x_1)$, $f(x_2)$, $f(x_3)$, $f(x_4)$ are in arithmetic progression, where $f(x) = Ax^2 + Bx + C$.*

The proof depends on determining the rational points on a certain elliptic curve.

This paper is concerned with the proof of the following theorem.

THEOREM. *Let A, B, C, $A \neq 0$ be rational numbers. There do not exist four unequal rational numbers x_1, x_2, x_3, x_4 such that $f(x_1)$, $f(x_2)$, $f(x_3)$, $f(x_4)$ are in arithmetic progression, where $f(x) = Ax^2 + Bx + C$.*

PROOF. Assuming the contrary, we may normalize the x_i and f so that $x_i = 0, 1, a, b$ while $f(0) = 0$, $f(1) = 1$, $f(a) = 2$, $f(b) = 3$. For a quadratic polynomial to satisfy these relations, it is necessary that

$$\det \begin{pmatrix} 1 & 1 & 1 \\ a^2 & a & 2 \\ b^2 & b & 3 \end{pmatrix} = 0$$

so

$$a^2b - b^2a - 3a^2 + 2b^2 + 3a - 2b = 0 \tag{1}$$

which in projective form is

$$a^2b - b^2a - 3a^2c + 2b^2c + 3ac^2 - 2bc^2 = 0. \tag{2}$$

The following five points satisfying (1) are seen not to be solutions to the original problem:

$$(2, 3), \quad (0, 0), \quad (1, 0), \quad (0, 1), \quad (1, 1).$$

Neither, of course, can these points at infinity be solutions to the original problem:

$$(0, 1, 0), \quad (1, 0, 0), \quad (1, 1, 0).$$

Received by the editors on December 27, 1976.
AMS-MOS Subject Classification: 10B10.

The theorem will be proved if we show that the curve (2) has no other rational points. This curve is a non-singular cubic, so defines an elliptic curve. We bring the curve into Weierstrass form by the transformation

$$X = 6\left(\frac{a+b-c}{3a+b-3c}\right), \qquad Y = 6\left(\frac{a-b+c}{3a+b-3c}\right).$$

Note here, the line $3a+b-3c=0$ is triply tangent to the curve at $(1, 0, 1)$; the line $a+b-c=0$ is doubly tangent at $(0, 1, 1)$ and passes through $(1, 0, 1)$; the line $a-b+c=0$ contains the points $(0, 1, 1)$, $(2, 3, 1)$, $(1, 1, 0)$. So X has a double pole and Y a triple pole at $(1, 0, 1)$ and Y is 0 at the three points of order two in the group structure of the curve while X is 0 at the point of order two $(0, 1, 1)$. From this, the transformed equation must be of the general form $Y^2 = X(X-D)(X-E)\,F$ for some constants D, E, F. Using the transformation, the points previously given have the images

$$(2, -2),\ (0, 0),\ (6, 6),\quad (4, 0),\quad (6, -6),\quad (2, 2),\quad (3, 0),$$

and the point at infinity. The transformed equation is easily seen to be:

$$Y^2 = X(X-3)\,(X-4). \tag{3}$$

Denote by $E(\mathrm{Q})$ the set of rational points on (3). We will follow the proof of the Mordell-Weil theorem found in [2] to determine this group. Unless otherwise indicated, proofs of assertions made in the following are to be found in this reference.

The following functions are group homomorphisms

$$g_i : E(\mathrm{Q}) \to \mathrm{Q}^*/\mathrm{Q}^{*2}.$$

$$g_1(P) = \begin{cases} X & \text{if } P = (X, Y),\ X \neq 0 \\ 3 & \text{if } P = (0, 0) \\ 1 & \text{if } P = \mathcal{O}, \text{ the point at infinity,} \end{cases}$$

$$g_2(P) = \begin{cases} X-4 & \text{if } P = (X, Y),\ X \neq 4 \\ 1 & \text{if } P = (4, 0) \\ 1 & \text{if } P = \mathcal{O}. \end{cases}$$

Here, we denote a class in $\mathrm{Q}^*\mathrm{Q}^{*2}$ by a member of that class. A class in the image of g_1 must contain some divisor of 12. X evidently cannot be negative. An inspection of the known points on the curve shows that $\mathrm{Im}(g_1) = \{1, 2, 3, 6\}$. Similarly, a class in the image of g_2 must contain a divisor of 4 and $\mathrm{Im}(g_2) = \{1, -1, 2, -2\}$.

Define a homomorphism $g = (g_1, q_2) : E(\mathbf{Q}) \rightarrow \mathbf{Q}^*/\mathbf{Q}^{*2} \times \mathbf{Q}^*/\mathbf{Q}^{*2}$. Then, $\ker(g) = 2E(\mathbf{Q})$. So, $E(\mathbf{Q})/2E(\mathbf{Q}) \xrightarrow{\sim} \operatorname{Im}(g)$. We will show that $\operatorname{Im}(g)$ is precisely $\{(2, -2), (3, -1), (6, 2), (1, 1)\}$. These are the images of the known points, thus it is sufficient to show that $(3, 1)$, $(3, -2)$ and $(1, -2)$ are not in $\operatorname{Im}(g)$. Let $P = (X, Y)$ be a finite point with $X \neq 0, 4$ and suppose $g(P) = (d_1, d_2)$ where d_i are square-free integers. Then, it is easily seen that there are integers U_1, U_2, V so that

$$X = d_1 U_1^2/V^2, \quad X - 4 = d_2 U_2^2/V^2, \tag{4}$$

and $\gcd(d_1 U_1, V) = \gcd(d_2 U_2, V) = 1$. We obtain then

$$d_1 U_1^2 - 4V^2 = d_2 U_2^2. \tag{5}$$

Now, for $(d_1, d_2) = (3, 1)$ or $(3, -2)$, this equation is impossible modulo 3, so these points are not in $\operatorname{Im}(g)$. For $(d_1, d_2) = (1, -2)$, we have, by standard arguments,

$$U_1 = 2A^2 - 4B^2, \quad U_2 = 4AB, \qquad V = A^2 + 2B^2, \tag{6}$$

where A and B are relatively prime integers and A is odd. From (6), (4) and (3) we then obtain

$$A^4 - 28A^2B^2 + 4B^4 = -2Z^2 \tag{7}$$

for some integer Z. But, this implies that A is even, which contradiction establishes $\operatorname{Im}(g)$ as claimed. Thus $E(\mathbf{Q})/2E(\mathbf{Q})$ is order 4. Now, the eight known points form a group isomorphic to $\mathbf{Z}/2 \times \mathbf{Z}/4$. Since $E(\mathbf{Q})$ is finitely generated, there can thus be no points of infinite order. It remains only to determine the points of finite order.

The curve (3) when reduced either modulo 5 or modulo 7 is a nonsingular cubic with just eight rational points. Thus, there can be no further points of finite order than the ones already known. (see [1], p. 112).

The group $E(\mathbf{Q})$ has only the eight given points, which establishes the theorem.

References

1. S. Lang, *Elliptic Functions*, Addison-Wesley Publishing Co. Inc., Reading, Mass., 1973.

2. L. J. Mordell, *Diophantine Equations*, Academic Press, New York, N.Y., 1969.

MATHEMATICS DEPARTMENT, UNIVERSITY OF ILLINOIS, CHICAGO CIRCLE, BOX 4348, CHICAGO, ILLINOIS 60680.