ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 41, Number 6, 2011

ARITHMETIC PROGRESSIONS ON CONGRUENT NUMBER ELLIPTIC CURVES

BLAIR K. SPEARMAN

ABSTRACT. We give an infinite family of congruent number elliptic curves each possessing a nontrivial rational arithmetic progression. These elliptic curves yield a new infinite family of congruent number curves having rank at least three.

1. Introduction. The congruent number elliptic curves are defined by

$$E_n : y^2 = x(x^2 - n^2),$$

where n is a positive integer. If P_i, $i = 1, 2, 3$, are rational points on E_n, then they form an arithmetic progression if their $x-$coordinates $x_i = x(P_i)$ form an arithmetic progression. Such an arithmetic progression is called trivial if at least one of the points P_i is a torsion point, that is, $P_i \in \{(0,0), (n,0), (-n,0)\}$ for some $i = 1, 2, 3$. Otherwise the arithmetic progression is nontrivial. In [**2**], Bremner, Silverman and Tzanakis showed that the curves E_n do not possess a nontrivial arithmetic progression of integral points if the rank of E_n is equal to 1. They do give one congruent number curve with a nontrivial arithmetic progression of integral points, namely,

$$y^2 = x(x^2 - 1254^2),$$

with integral points

$$(-528, 26136), \qquad (-363, 22869), \qquad (-198, 17424).$$

In [**1**] Bremner noted that rational points in arithmetic progression tend to be independent in the group of rational points. This suggests a possible rank of at least 3 for E_{1254}. In fact the rank of E_{1254} is

2010 AMS *Mathematics subject classification.* Primary 11G05.
Keywords and phrases. Arithmetic progression, congruent number, elliptic curve, rank.
Research supported by the Natural Sciences and Engineering Research Council of Canada.
Received by the editors on April 20, 2009, and in revised form on May 5, 2009.
DOI:10.1216/RMJ-2011-41-6-2033