A FAMILY OF CONGRUENT NUMBER ELLIPTIC CURVES OF RANK THREE

LORENZ HALBEISEN, NORBERT HUNGERBÜHLER, AND ARMAN SHAMSI ZARGAR

Abstract. Recent progress in the theory of Heron triangles and their elliptic curves led to new families of congruent number elliptic curves with rank at least two. Based on these results, we derive an infinite family of congruent number elliptic curves with rank at least three. It turns out that this family is isomorphic to a family which was recently discovered by the third author, however the new approach is simpler, more flexible and gives new insight. In particular, it provides in addition three formulae for congruent numbers.

1. Introduction

In [3] it was shown that for any positive integers l, m, n with

$$m = n^2 + nl + l^2,$$

the integer

$$A = mnl(n^2 - l^2)(n + 2l)(2n + l)$$

is a congruent number and the corresponding elliptic curve

$$y^2 = x^3 - A^2 x$$

has rank at least 2. It is natural to ask whether the condition on m is necessary in order to obtain a congruent number elliptic curve with high rank. We shall see that this is not the case. In fact, below we show that for $m = 3$, $l = \mu^2$, and $n = \nu^2$, where $\mu^2 + \nu^2$ is a square, the elliptic curve which corresponds to

$$A = -3(\mu^2 - \nu^2)(\mu^2 + 2\nu^2)(2\mu^2 + \nu^2) \tag{1.1}$$

has rank at least 3. For $\mu = 2uv$, $\nu = u^2 - v^2$, and by clearing squares, this leads to

$$A = 6(u^4 + v^4)(u^4 - 6u^2v^2 + v^4)(u^4 + 6u^2v^2 + v^4).$$

Finally, for $w := \frac{u}{v}$ we obtain

$$A = 6(w^4 + 1)(w^4 - 6w^2 + 1)(w^4 + 6w^2 + 1),$$

or equivalently

$$\begin{aligned} A &= 6(w^4 + 1)(w^8 - 34w^4 + 1) \\ &= 6(w^{12} + 33w^8 + 33w^4 + 1). \end{aligned} \tag{1.2}$$

For some fractions w, the corresponding elliptic curve has rank 4 (or even rank 5) over $\mathbb{Q}$, but over $\mathbb{Q}(w)$, the rank is exactly 3. A different family of congruent number elliptic curves with rank at least 3 is given in [4].

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 14H52.
Key words and phrases. congruent number, elliptic curve, rank.

In [2], it is shown that for any positive integers l, m, n with

$$m^2 = n^2 + nl + l^2,$$

the congruent number elliptic curve which corresponds to

$$A = nl(n+l)m$$

has rank at least 2. By omitting the requirement on m, we obtain some formulae for congruent numbers (see Section 4).

2. A Family of Congruent Number Elliptic Curves of Rank at Least 3

Theorem 2.1. *For rational numbers w, let*

$$A_w = 6(w^4+1)(w^4-6w^2+1)(w^4+6w^2+1).$$

If the discriminant of $x^3 - A_w^2 x$ is nonzero, then the congruent number elliptic curve

$$E_w: \ y^2 = x^3 - A_w^2 x$$

has rank at least 3.

Proof. Let

$$\delta := w^4+1, \quad \bar\gamma := w^4-6w^2+1, \quad \gamma := w^4+6w^2+1.$$

Then $A_w = 6\delta\bar\gamma\gamma$. By an easy calculation one can verify that the following rational points belong to the curve E_w:

$$\begin{aligned} P_1(w) &= \left(-3\bar\gamma\gamma^2, 9(w^2+1)\bar\gamma^2\gamma^2\right), \\ P_2(w) &= \left(12\delta^2\gamma, 36(w^2-1)\delta^2\gamma^2\right), \\ P_3(w) &= \left(-36w^2\bar\gamma\gamma, 36w\bar\gamma^2\gamma^2\right). \end{aligned}$$

By the specialization theorem [8, Theorem 11.4], in order to prove that this family has rank at least three over $\mathbb{Q}(w)$, it suffices to find a specialization $w = w_0$ such that the points $P_1(w)$, $P_2(w)$, and $P_3(w)$ are linearly independent on the specialized curve over $\mathbb{Q}$. We take $w = 4$, then

$$\begin{aligned} P_1(4) &= (-60186147, 494188453017), \\ P_2(4) &= (279783564, 4444361914140), \\ P_3(4) &= (-32735808, 465118544016) \end{aligned}$$

are linearly independent points of infinite order on the curve

$$E: \ y^2 = x^3 - 87636486^2 x.$$

Indeed, the determinant of the Néron-Tate height pairing matrix of the three points is the nonzero value 228.131887800624 according to sage [6]. Now, noting that the specialization map is an injective group homomorphism, the points $P_1(w)$, $P_2(w)$, $P_3(w)$ being linearly independent for all but finitely many values of w. Hence, the family of elliptic curves E_w has rank at least three over $\mathbb{Q}(w)$ with linearly independent points $P_1(w)$, $P_2(w)$, and $P_3(w)$. □

Among the curves $y^2 = x^3 - A^2 x$ with A as in (1.2) which turn out to have rank at least 3, we find curves of higher rank as well: If we let `magma` [5] compute the rank for all values of w in the Farey sequence F_{13} we find rank 4 for

$$w = \frac{1}{9}, \frac{1}{7}, \frac{1}{5}, \frac{3}{13}, \frac{1}{3}, \frac{1}{2}, \frac{5}{8}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{7}{8}$$

and the corresponding reciprocals, and rank 5 for

$$w = \frac{1}{6},\ \frac{5}{7}$$

and the corresponding reciprocals.

Apart from the points $P_1(w), P_2(w), P_3(w)$ which were used above, for integral w we find the following integral points on the curve:

$$\left(18(w^2-1)^2\delta\bar{\gamma}, 72(w^2-1)\delta^2\bar{\gamma}^2\right), \quad \left(12\delta^2\bar{\gamma}, 36(w^2+1)\delta^2\bar{\gamma}^2\right), \quad \left(-6\delta\bar{\gamma}^2, 72w\delta^2\bar{\gamma}^2\right),$$
$$\left(18(w^2+1)^2\delta\gamma, 72(w^2+1)\delta^2\gamma^2\right), \quad \left(-3\bar{\gamma}^2\gamma, 9(w^2-1)\gamma^2\bar{\gamma}^2\right), \quad \left(6\delta\gamma^2, 72w\delta^2\gamma^2\right).$$

3. Rank of E_w Over $\mathbb{Q}(w)$ is Three

Our curve E_w has full 2-torsion. We can therefore get more precise information on E_w by applying the Gusić and Tadić algorithm, see [1, Theorem 3.1 and Corollary 3.2]. Using the algorithm we can show that rank $E_w(\mathbb{Q}(w)) = 3$ and that the three points $P_1(w)$, $P_2(w)$, and $P_3(w)$ are free generators of $E_w(\mathbb{Q}(w))$.

We first sketch the application of the algorithm and then use it for our curve. To apply the algorithm, we rewrite E_w in the form

$$y^2 = (x-e_1)(x-e_2)(x-e_3),$$

with $e_1, e_2, e_3 \in \mathbb{Z}[w]$, and consider the factorization

$$(e_1-e_2)(e_1-e_3)(e_2-e_3) = a \cdot f_1(w)^{a_1} \cdots f_k(w)^{a_k},$$

where $a \in \mathbb{Z}$ and $f_i \in \mathbb{Z}[w]$ are irreducible (of positive degree) and $a_i \geq 1$, $1 \leq i \leq k$. Consider $w_0 \in \mathbb{Q}$. Assume that for each $1 \leq i \leq k$ the square-free part of each of $f_i(w_0)$ has at least one prime factor that does not appear in the square-free part of any of $f_j(w_0)$ for $j \neq i$ and does not appear in the factorization of a. Then the specialization homomorphism $E_w(\mathbb{Q}(w)) \to E_{w_0}(\mathbb{Q})$ is injective. Furthermore, if $|E_w(\mathbb{Q}(w))_{\text{tors}}| = |E_{w_0}(\mathbb{Q})_{\text{tors}}|$ and there exist points $P_1, \ldots, P_r \in E_w(\mathbb{Q}(w))$ such that $P_1(w_0), \ldots, P_r(w_0)$ are the free generators of $E_w(w_0)(\mathbb{Q})$, then the specialization homomorphism $E_w(\mathbb{Q}(w)) \to E_{w_0}(\mathbb{Q})$ is an isomorphism. Thus $E_w(\mathbb{Q}(w))$ and $E_{w_0}(\mathbb{Q})$ have the same rank r, and $P_1, \ldots, P_r$ are the free generators of $E_w(\mathbb{Q}(w))$.

Keeping the notations above, we have

$$e_1 = 0, \quad e_2 = -6w^{12} + 198w^8 + 198w^4 - 6, \quad e_3 = -e_2$$

so that

$$\prod_{1 \leq i < j \leq 3} (e_i - e_j) = 432(w^2-2w-1)^3(w^2+2w-1)^3(w^4+1)^3(w^4+6w^2+1)^3.$$

The curve E_w satisfies the aforementioned conditions when specializing at for example $w_0 = 4$, which shows the specialization homomorphism $E_w(\mathbb{Q}(w)) \to E_4(\mathbb{Q})$ is injective. On the other hand, this value of w leads to the rank-three curve

$$E_{24}: \ y^2 = x^3 - 87636486^2 x,$$

being generated by

$$G_1 = (-27450339, 436048635015),$$
$$G_2 = \left(-\frac{250330850}{81}, \frac{112242399817240}{729}\right),$$
$$G_3 = (106658598, 627853339728),$$

with the linearly independent points $P_i(4)$, $i = 1, 2, 3$ and the 2-torsion points

$$T_1 = (0, 0), \quad T_2 = (-87636486, 0), \quad T_3 = (87636486, 0).$$

We have the following relations between the generators and linearly independent points:

$$P_1(4) = G_1 - G_3 + T_3, \quad P_2(4) = G_1 + T_1, \quad P_3(4) = -G_1 + G_2 + G_3 + T_1.$$

Since the determinant of the change of basis matrix, i.e.,

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 0 & 0 \\ -1 & 1 & 1 \end{pmatrix}$$

is 1 in absolute value, then $\{P_1(4), P_2(4), P_3(4)\}$ is the set of free generators, that means it generates the whole group $E_4(\mathbb{Q})/E_4(\mathbb{Q})_{\text{tors}}$.

4. Three Formulae for Congruent Numbers

In [2], it is shown that for any positive integers l, m, n with

$$m^2 = n^2 + nl + l^2,$$

the congruent number elliptic curve which corresponds to

$$A = nl(n + l)m$$

has rank at least 2. If we drop the condition on m, and set $m := n+2l$ or $m := n-l$, we still obtain congruent numbers:

(1) If we set $m := n+2l$, then for nonzero integers n, l with $(n+l)(n+2l) \neq 0$, the integer

$$A = nl(n + l)(n + 2l)$$

is a congruent number, which is witnessed by the point

$$\left(n(n + l)^2(n + 2l), n^2(l + n)^2(2l + n)^2\right).$$

In particular, for any positive integer n, $A = n(n+1)(n+2)$ is a congruent number.

We can make sure that the the rank of the elliptic curve is at least 2 by requiring that

$$x_2 = n(n + l)(n + 2l)^2$$

is the x-coordinate of a rational point on the curve. This implies that $n(n + 3l)$ is a square and for $n = \frac{p}{q}$, this is the case for $p = \nu^2$ and $q = \frac{\mu^2-\nu^2}{3l}$. By clearing squares, we obtain

$$A_2 = 3(\mu^2 - \nu^2)(\mu^2 + 2\nu^2)(2\mu^2 + \nu^2),$$

which leads to the same curve as with A in equation (1.1).

(2) If we set $m := n - l$, then for nonzero integers n, l with $(n + l)(n - l) \neq 0$, the integer

$$A = nl(n + l)(n - l)$$

is a congruent number, which is witnessed by the point

$$\left(-nl(n - l)^2, 2n^2l^2(l - n)^2\right).$$

In particular, for any positive integer n, $A = n(n+1)(n-1)$ is a congruent number.

Also in this case we can make sure that the rank of the elliptic curve is at least 2 by requiring that

$$x_2 = nl(n-l)^2$$

is the x-coordinate of a rational point on the curve. This implies that $(l-2n)(l+n)$ is a square, which is the case for $n = \frac{\mu^2-\nu^2}{3}$ and $l = \frac{2\mu^2-nu^2}{3}$. By clearing squares, we obtain

$$A_2 = 3(\mu^2-\nu^2)(\mu^2+2\nu^2)(2\mu^2+\nu^2),$$

which leads again to the same curve as with A in equation (1.1).

Finally, let us consider again the equation $m = n^2+nl+l^2$. As mentioned above, in [3] it was shown that for any positive integers l, m, n with $m = n^2 + nl + l^2$, the integer $A = mnl(n^2-l^2)(n+2l)(2n+l)$ is a congruent number, where the corresponding elliptic curve has rank at least 2. If we drop the condition on m, we may still find congruent numbers:

(3) If we set $m := 3nl$, then for any nonzero integers n and l with the property that $(n+l)(n-l)(n+2l)(2n+l) \neq 0$, the integer

$$A = 3n^2l^2\,(n+l)\,(n-l)\,(n+2l)\,(2n+l)$$

is a congruent number, which is witnessed by the point

$$\left(-3n^2l^2\,(n^2-l^2)\,(n+2l)^2, 9n^3l^3\,(n^2-l^2)^2\,(n+2l)^2\right).$$

Thus, by clearing squares, for any relatively prime integers n, l,

$$A = 3\,(n+l)\,(n-l)\,(n+2l)\,(2n+l)$$

is a congruent number.

To summarize, for suitably chosen integers n and l, the following three integers are congruent numbers:

$$nl(n+l)(n+2l), \quad nl(n+l)(n-l), \quad 3(n+l)(n-l)(n+2l)(2n+l).$$

Acknowledgement

We would like to thank the referee for the careful reading and the valuable comments which helped to improve the article.

References

1. I. Gusić, P. Tadić, A remark on the injectivity of the specialization homomorphism, Glas. Mat. Ser. III 74 (67) (2012) 265–275.
2. L. Halbeisen, N. Hungerbühler, Congruent number elliptic curves related to integral solutions of $m^2 = n^2 + nl + n^2$, J. Integer Sequences 22 (2019) Article 19.3.1.
3. L. Halbeisen, N. Hungerbühler, Heron triangles and their elliptic curves, J. Number Theory 213 (2020) 232–253.
4. J. A. Johnstone, B. K. Spearman, Congruent number elliptic curves with rank at least three, Canad. Math. Bull. 53 (2010) 661–666.
5. Magma Computational Algebra System: http://magma.maths.usyd.edu.au/calc/.
6. sage software, Available at http://sagemath.org.
7. A. Shamsi Zargar, On the rank of elliptic curves arising from Pythagorean quadruplets, Kodai Math. J. 43 (2020) 129–142.
8. J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer, New York, 1994.

ETH Zentrum, Department of Mathematics, Rämistrasse 101,
8092 Zürich, Switzerland
Email address: lorenz.halbeisen@math.ethz.ch

ETH Zentrum, Department of Mathematics, Rämistrasse 101,
8092 Zürich, Switzerland
Email address: norbert.hungerbuehler@math.ethz.ch

Department of Mathematics and Applications, University of Mohaghegh Ardabili,
Ardabil, Iran
Email address: zargar@uma.ac.ir