A search for high rank congruent number elliptic curves

Andrej Dujella
Department of Mathematics, University of Zagreb,
Bijenička cesta 30, 10000 Zagreb, Croatia
duje@math.hr

Ali S. Janfada [1]
Department of Mathematics, University of Urmia,
P.O. Box 165, Urmia, Iran
a.sjanfada@urmia.ac.ir

Sajad Salami
salami.sajad@gmail.com

Abstract

In this article, we describe a method for finding congruent number elliptic curves with high ranks. The method involves an algorithm based on the Monsky's formula for computing 2-Selmer rank of congruent number elliptic curves, and Mestre-Nagao's sum which is used in sieving curves with potentially large ranks. We apply this method for positive squarefree integers in two families of congruent numbers and find some new congruent number elliptic curves with rank 6.

2000 Mathematical Subject Classification: Primary 11G05, Secondary 14H52.
Keywords: Congruent number elliptic curve, Mordell-Weil rank, Selmer rank, Mestre-Nagao sum

1 Introduction

One of the major topics connected with elliptic curves is construction of elliptic curves with high ranks. Several authors considered this problem for elliptic curves with prescribed properties and relatively high ranks. For instance, we cite [6, 17] for the curves with given torsion groups, [2, 9] for the curves $y^2 = x^3 + dx$, [10, 22] for the curves $x^3 + y^3 = k$ related to the so-called taxicab problem, [8] for the curves $y^2 = (ax+1)(bx+1)(cx+1)(dx+1)$

[1] The second author was partially financed by a grant from Urmia University

induced by Diophantine quadruples $\{a, b, c, d\}$, etc. Dujella [6] collected a list of known high rank elliptic curves with prescribed torsion groups. The largest known rank of elliptic curves, found by N. D. Elkies in 2006, is 28.

In this work we deal with a family of elliptic curves which are closely related to the classical Congruent Number problem. A positive squarefree integer n is called a *congruent number* if it is the area of a right triangle with rational sides. The problem of determining congruent numbers is closely related to the curves $E_n : y^2 = x^3 - n^2x$, which are called *congruent number elliptic curves* or *CN-elliptic curves*. In fact, the positive squarefree integer n is a congruent number if and only if the Mordell-Weil rank $r(n)$ of E_n is a positive integer [16]. In this case, we refer to n itself as a CN-elliptic curve, which corresponds to E_n. In 1972, Alter, Curtz, and Kubota [1] conjectured that $n \equiv 5, 6, 7 \pmod 8$ are congruent numbers. In 1975, appealing Birch and Swinnerton-Dyer conjecture and Shafarevich-Tate conjecture, Lagrange [26] deduced a conjecture on the parity of the $r(n)$ as follows:

$$r(n) \equiv \begin{cases} 0 \pmod 2, & \text{if } n \equiv 1, 2, 3 \pmod 8; \\ 1 \pmod 2, & \text{if } n \equiv 5, 6, 7 \pmod 8. \end{cases}$$

The problem of constructing high rank CN-elliptic curves was considered by several authors. In 1640, Fermat proved that $r(1) = 0$, so $n = 1$ is not a congruent number. Billing [3] proved that $r(5) = 1$. Wiman [30] proved that $r(34) = 2$, $r(1254) = 3$ and $r(29274) = 4$. In 2000, Rogers [21], based on an idea of Rubin and Silverberg [25], found the first integers $n = 4132814070$, 61471349610 such that $r(n) = 5, 6$, respectively. Later, in his PhD thesis [22], Rogers gave another integers with $r(n) = 5, 6$ smaller than those presented in [21]. Also he could find the first integer n such that $r(n) = 7$. During the preparation of this paper, Rogers informed us that the smallest n with $r(n) = 5$ which he was aware is 48272239, while the smallest n with $r(n) = 6$ is 6611719866. The only known n with $r(n) = 7$ remains $n = 797507543735$, found in [22]. Here we give the complete list on n's with $r(n) = 6$ communicated to us by Rogers [23], other than those curves which are noted above: 66637403074, 94823967361, 129448648329, 179483163699, 208645752554, 213691672290, 226713842409, 248767798521, 344731563386, 670495125874, 797804045274, 898811499201.

In Section 2, we shortly describe the Selmer groups of CN-elliptic curves. In Section 3, we describe Monsky's formula for computing $s(n)$, 2-Selmer rank of CN-elliptic curves. In section 4, we study Mestre-Nagao's sum method for finding high rank elliptic curves, which is a part of our algorithm. In section 5, we design an algorithm to find high rank CN-elliptic curves. Our algorithm is based on the Monsky's formula for 2-Selmer rank CN-elliptic curves $s(n)$, and Mestre-Nagao's sum $S(N, n)$. We applied our algorithm for positive squarefree integers arisen from two specific families of congruent numbers. We have found a large number of curves with rank 5 and twenty four new curves with rank 6. We have not found any new curve with $r(n) \geq 7$, although with some variants of our method we have rediscovered the Rogers' example with $r(n) = 7$ (and some of his examples with $r(n) = 5$ and 6). We have also found several curves with $5 \leq r(n) \leq 7$, where the upper bound is obtained by MWRANK program (option `-s`). It might be a challenging problem to decide whether these curves have ranks equal to 5 or 7.

In our computations we used the PARI/GP software (version 2.4.0) [20] and Cremona's MWRANK program [5] for computing the Mordell-Weil rank of the CN-elliptic curves.

2 Selmer groups and 2-Selmer rank of E_n

In this section, we shortly describe the Selmer groups and 2-Selmer rank of CN-elliptic curves. We cite [27, 29] for more details. Consider the CN-elliptic curve $E_n : y^2 = x^3 - n^2 x$ over $\mathbb{Q}$ for an arbitrary positive squarefree integer n with odd prime factors $p_1, p_2, \ldots, p_t$. Define the set $S = \{\infty, 2, p_1, p_2, \ldots, p_t\}$ and the subgroup $M =< -1, 2, p_1, p_2, \ldots, p_t >$ of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. For each $d \in M$ define the curves

$$C_d : dw^2 = d^2t^4 + 4n^2z^4,$$

$$C_d' : dw^2 = d^2t^4 - n^2z^4,$$

in variables (w, t, z), which are called the *homogeneous spaces* of E_n. For more details see [27]. The *Selmer group* Sel_n (resp. Sel'_n) corresponds to the curve C_d (resp. C'_d) having non-trivial solutions in the local field $\mathbb{Q}_p$ for all $p \in S$, when d runs over all divisors of $2n$. In fact, there are the isomorphisms

$$Sel_n \cong \{d \in M : C_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in S\},$$

$$Sel_n' \cong \{d \in M : C_d'(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \in S\}.$$

One can see easily that the orders of the Selmer groups Sel_n and Sel_n' are powers of 2. Let $|Sel_n| = 2^s$ and $|Sel_n'| = 2^{s'}$. Then the 2-*Selmer rank* of E_n is defined to be the value $s + s' - 2$, which we denote by $s(n)$. It is an upper bound for the Mordell-Weil rank $r(n)$ of E_n. Faulkner and James [11] gave a method for computing Sel_n and Sel'_n which is based on the graph theory. Heath-Brown [14] and [15] studied extensively the size of Selmer groups of CN-elliptic curves and proved some theorems on average value of $s(n)$ for $n < X$, as X tends to infinity.

3 Monsky's formula for $s(n)$

In 1994, P. Monsky [15] proved a theorem on the parity of the 2-Selmer rank of CN-elliptic curves. He gave a formula for computation of the $s(n)$ through his proof of this theorem.

Theorem 1 *Let n be a positive squarefree integer. Then*

$$s(n) \equiv \begin{cases} 0 \pmod 2, & \text{if } n \equiv 1,2,3 \pmod 8; \\ 1 \pmod 2, & \text{if } n \equiv 5,6,7 \pmod 8. \end{cases}$$

For a proof of this theorem see Appendix of [15].

Let n be a positive squarefree integer with odd prime factors $p_1, \ldots, p_t$. Define the diagonal $t \times t$ matrix $D_j = (d_i)$, for $j \in \{-1,-2,2\}$, and the square $t \times t$ matrix $A = (a_{ij})$ as follows:

$$d_i = \begin{cases} 0, & \text{if } (\frac{j}{p_i}) = 1; \\ 1, & \text{if } (\frac{j}{p_i}) = -1, \end{cases} \quad \text{and} \quad a_{ij} = \begin{cases} 0, & \text{if } (\frac{p_j}{p_i}) = 1; \\ 1, & \text{if } (\frac{p_j}{p_i}) = -1. \end{cases}$$

Monsky showed that $s(n)$ can be computed as

$$s(n) = \begin{cases} 2t - \operatorname{rank}_{\mathbb{F}_2}(M_o), & \text{if } n = p_1 p_2 \cdots p_t; \\ 2t - \operatorname{rank}_{\mathbb{F}_2}(M_e), & \text{if } n = 2p_1 p_2 \cdots p_t, \end{cases}$$

where M_o and M_e are the following $2t \times 2t$ matrices:

$$M_o = \left[\begin{array}{c|c} A + D_2 & D_2 \\ \hline D_2 & A + D_{-2} \end{array}\right], \quad M_e = \left[\begin{array}{c|c} D_2 & A + D_2 \\ \hline A^T + D_2 & D_{-1} \end{array}\right].$$

4 Mestre-Nagao's sum

Now we describe a sieving method for finding the best candidates for high rank CN-elliptic curves. For any elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Q}$, and every prime number p not dividing the discriminant $\Delta = -16(4a^3+27b^2)$ of E, we can reduce a and b modulo p and view E as an elliptic curve over the finite field $\mathbb{F}_p$. Let $\#E(\mathbb{F}_p)$ be the number of points on such reduced curve:

$$\#E(\mathbb{F}_p) = 1 + \#\{0 \leq x, y \leq p-1 : y^2 \equiv x^3 + ax + b \pmod{p}\}.$$

There is both theoretical and experimental evidence which suggests that elliptic curves of high ranks have the property that $\#E(\mathbb{F}_p)$ is large for many primes p.

Definition 2 Let N be a positive integer and $\mathbf{P}_N$ be the set of all primes less than N. Mestre-Nagao's sum is defined by

$$S(N,E) = \sum_{p \in \mathbf{P}_N} \left(1 - \frac{p-1}{\#E(\mathbb{F}_p)}\right) \log p = \sum_{p \in \mathbf{P}_N} \frac{-a_p + 2}{\#E(\mathbb{F}_p)} \log p.$$

Note that $S(N,E)$ can be computed efficiently provided N is not too large with PARI/GP software [20]. It is experimentally known [7, 18, 19] that we may expect that high rank curves have large $S(N,E)$. See [4] for a heuristic argument which connects this assertion with the famous Birch and Swinnerton-Dyer conjecture. For a positive squarefree integer n, we denote $S(N, E_n)$ by $S(N, n)$.

5 An algorithm for high rank CN-elliptic curves

Now we are ready to exhibit our algorithm for finding high rank CN-elliptic curves, based on the Monsky's formula for $s(n)$ and Mestre-Nagao's sum $S(N, n)$.

Step 1. Let s be a positive integer. Choose a non-empty set T of some squarefree congruent numbers. For any $n \in T$ compute $s(n)$ by the Monsky's formula. Define the subset T_s of T containing all $n \in T$ with $s(n) = s$. If T_s is empty choose another set T.

Step 2. Let k be a positive integer. Choose the set $\mathcal{M}_s$ as follows:

$$\mathcal{M}_s = \{(N_i, M_i) : \ 0 < N_1 < \cdots < N_k, \ 0 < M_i, \ 1 \leq i \leq k\}.$$

Put $T_s^0 = T_s$, and for any i with $1 \leq i \leq k$, define the recursive sets

$$T_s^i = \left\{n \in T_s^{i-1} : \ S(N_i, n) \geq M_i\right\}.$$

Step 3. Take j, $1 \le j \le k$, such that for any i with $j < i \le k$, the sets T_s^i are empty. Now for any $n \in T_s^j$, compute $r(n)$ using Cremona's MWRANK.

Remark 3 For a given positive integer s in Step 1, choice of the starting set T is very important. To save the time, we should avoid any repeated elements in T. By applying Theorem 1 and Lagrange's conjecture about the parity of $r(n)$, one can expect to find an integer n in the set T_s such that $r(n)$ is less than s and has the same parity as s.

Remark 4 The most sensitive part of our algorithm is choosing the sets $\mathcal{M}_s$ in Step 2. For a prescribed value of s, we must choose the elements of $\mathcal{M}_s$ and its cardinality in such a way that the total time of available computations is as small as possible. Note that the elements of the sets T_s^j, in Step 3, are the best candidates for high rank CN-elliptic curves.

Remark 5 In Step 3, we try to compute $r(n)$ for any $n \in T_s^j$. This is done by the Cremona's program MWRANK efficiently for small values of n. However, for large n's the computation can be much slower, and MWRANK often gives only lower and upper bounds for $r(n)$.

Given any positive integer s, our algorithm can be implemented in different ways depending on the choice of the starting set T in Step 1. In this paper, we focused on the integers $s \ge 5$ and considered T in two different ways. To explain the first way, we need the next result which gives two specific families of congruent numbers. For a proof of the case (I) see [24] and for the case (II) see [26].

Theorem 6 *Let u and v be arbitrary positive integers such that $u < v$, $\gcd(u, v) = 1$ and $u + v$ is odd. Then the squarefree parts of the following families of integers are congruent numbers:*

$$\text{(I) } uv(v-u)(v+u), \quad \text{(II) } uv(u^2+v^2)/2.$$

In the first way, as the starting set T, we considered positive squarefree integers n of the forms (I) and (II) with $u < v \le 10^5$ and $\omega(n) \ge 5$, where $\omega(n)$ denotes the number of distinct prime factors of n.

In the second way, as the starting set T, we considered squarefree integers with prescribed number of prime factors and $s(n) \ne 0$ as follows. For a positive squarefree integer n, Keqin Feng [12, 13] defined a directed graph $G(n)$ whose vertices are all prime factors of n and its edges are related to

(p_i/p_j), the Kronecker symbol for any two primes p_i and p_j dividing n. Also, he defined a certain oddness terminology for each graph $G(n)$ under prescribed conditions. Then he classified some families of non-congruent numbers n by showing that $s(n) = 0$ if and only if $G(n)$ is an odd graph. We considered the integers n with $5 \leq \omega(n) \leq 12$, which does not satisfy the conditions described in [12, 13], and limit the prime factors of n by a certain upper bound.

For an integer $s \geq 5$, after choosing different sets T by the ways described above, we got different sets T_s which have some common elements. To save the time, we took the union of the different sets T_s as starting set of Step 2 in algorithm. Then for each $s \geq 5$, we considered the related sets $\mathcal{M}_s$ as follows:

$$\{N_i\}_{i=1}^{7} = \{500, 1000, 5000, 10000, 15000, 20000, 50000\}\,,$$

$$\begin{aligned}
\mathcal{M}_5 &= \{(N_1, 10), (N_2, 12), (N_3, 15), (N_4, 20), (N_5, 25), (N_6, 28), (N_7, 30)\}\,,\\
\mathcal{M}_6 &= \{(N_1, 10), (N_2, 14), (N_3, 18), (N_4, 22), (N_5, 25), (N_6, 30), (N_7, 35)\}\,,\\
\mathcal{M}_7 &= \{(N_1, 10), (N_2, 15), (N_3, 20), (N_4, 25), (N_5, 30), (N_6, 35), (N_7, 40)\}\,,\\
\mathcal{M}_8 &= \{(N_1, 10), (N_2, 14), (N_3, 16), (N_4, 20), (N_5, 25), (N_6, 30), (N_7, 35)\}\,,\\
\mathcal{M}_9 &= \{(N_1, 10), (N_2, 15), (N_3, 20), (N_4, 25), (N_5, 28), (N_6, 30), (N_7, 35)\}\,,\\
\mathcal{M}_{\geq 10} &= \{(N_1, 10), (N_2, 12), (N_3, 15), (N_4, 18), (N_5, 22), (N_6, 25), (N_7, 30)\}\,.
\end{aligned}$$

For each $s \geq 5$ and each i, $1 \leq i \leq 7$, by choosing $(N, M) = (N_i, M_i) \in \mathcal{M}_s$ and computing $S(N_i, n)$ for all $n \in T_s^{i-1}$, gets the sets T_s^i of n's that satisfy $S(N_i, n) \geq M_i$. The elements of the sets T_s^j are best candidates to give high rank CN-elliptic curves. Finally, we used MWRANK to compute Mordell-Weil rank $r(n)$, for n's in each of the sets T_s^j. This stage of our algorithm was very time consuming. By the implementation of our algorithm, we have rediscovered some of the Rogers' examples with $r(n) = 5, 6$, and 7. Also, we were able to find some new CN-elliptic curves with $r(n) = 6$ and some curves with $5 \leq r(n) \leq 7$. We give these curves in the Tables 1 and 2, respectively.

n	factorization	n mod 8	$s(n)$
531670544130	2·3·5·11·17·107·463·1913	2	6
602730488666	2·29·41·97·137·19073	2	6
1079812755065	5·11·23·41·89·449·521	1	6
1351528542210	2·3·5·7·11·29·31·47·61·227	2	6
1440993982946	2·7·17·23·41·73·281·313	2	8
1544991154746	2·3·13·19·83·163·251·307	2	6
1663586838899	17·103·137·756·9161	3	8
2280190889130	2·3·5·7·11·23·41·257·4073	2	6
4611082954146	2·3·19·41·113·953·9161	2	8
8231905771386	2·3·11·17·19·23·41·43·89·107	2	6
9033322597530	2·3·5·7·11·43·53·59·127·229	2	6
17434310103210	2·3·5·7·11·13·17·19·67·139·193	2	6
46485304142530	2·5·11·19·23·43·67·107·3137	2	6
90181020280890	2·3·5·7·11·251·397·401·977	2	6
165130972136130	2·3·5·7·11·13·29·103·233·7901	2	6
179009302343970	2·3·5·7·17·19·23·47·53·73·631	2	6
181025271456226	2·17·103·127·151·1259·2141	2	6
243339180933145	5·11·401·1049·3169·3319	1	8
339507119347242	2·3·7·17·19·23·37·59·113·401	2	6
444724421083665	3·5·17·31·71·103·137·233·241	1	8
846249312638730	2·3·5·7·11·13·31·37·41·101·349	2	6
1056710141801930	2·5·7·11·41·43·53·71·269·769	2	6
4601440550332626	2·3·7·11·13·17·19·37·41·101·113·137	2	6
13897395819317010	2·3·5·7·11·13·23·29·31·61·113·191	2	6

Table 1: Some new CN-elliptic curves with $r(n) = 6$

n	factorization	n mod 8	$s(n)$
1024801887174	2·3·13·37·409·769·1129	6	7
1025774078934	2·3·11·17·41·43·641·809	6	7
1649085975174	2·3·11·47·73·97·193·389	6	7
2093383150230	2·3·5·29·73·97·419·811	6	7
2392760979654	2·3·17·41·43·83·160313	6	7
2473595024934	2·3·11·17·41·83·347·1867	6	7
5080701332454	2·3·11·17·41·59·521·3593	6	7
5449406258406	2·3·11·17·41·251·683·691	6	7
7322494848870	2·3·5·17·19·137·151·36529	6	7
7391341307526	2·3·11·19·59·67·523·2851	6	7
7697325362694	2·3·11·137·401·547·3881	6	7
7836495180886	2·17·281·353·971·2393	6	9
7889458857566	2·11·19·881·1049·1571	6	7
8549294440966	2·17·19·37·137·353·5857	6	7
10571147972390	2·5·17·89·277·587·4297	6	7
11050024116846	2·3·11·13·17·29·31·569·1481	6	7
12651761296614	2·3·11·17·19·43·59·449·521	6	7
14020765617254	2·11·17·23·71·241·95257	6	7
19843964725254	2·3·17·19·937·2683·4073	6	7
25161173711039	19·23·29·103·1657·11633	7	7
25837148295902	2·31·97·593·1217·5953	6	9
26755379766174	2·3·23·59·233·353·39953	6	7
29130582949206	2·3·19·113·283·1913·4177	6	7
32334652741974	2·3·11·43·89·113·883·1283	6	7
34243576397574	2·3·73·89·457·953·2017	6	7
35876712238310	2·5·31·41·1289·1361·1609	6	7
44066140293846	2·3·11·17·41·43·59·491·769	6	9
56858065281654	2·3·7·13·19·73·89·769·1097	6	7
57705905931141	3·13·17·131·521·937·1361	5	7
57939619068870	2·3·5·7·11·37·53·89·137·1049	6	7
61639096639029	3·7·13·29·241·2113·15289	5	7
109995988504269	3·17·41·65809·114193	5	7
114490690064454	2·3·11·19·577·1873·84481	6	9
117205364344206	2·3·7·17·73·97·233·293·2377	6	7
119231629856526	2·3·11·17·29·41·59·83·18251	6	7
121466637600990	2·3·5·11·17·31·89·107·1033	6	7
130629627999390	2·3·5·13·17·37·41·97·257·521	6	7
146421396607926	2·3·11·17·19·449·2417·6329	6	7
175656508365734	2·11·97·113·10169·71633	6	9
180196195115046	2·3·11·17·43·83·179·251393	6	7
191519081464326	2·3·7·11·31·41·59·89·89·179·347	6	7
242515586992326	2·3·19·41·73·587·641·1889	6	9
433182183087126	2·3·11·17·41·251·2707·13859	6	7
459848288031405	3·5·7·13·17·41·61·389·20369	5	7
1687029282320910	2·3·5·11·1049·1729·2027	6	7
2053424339679966	2·3·11·17·19·31·43·179·499·809	6	7
2059195525185430	2·5·89·641·823·929·4721	6	9
3167344617712806	2·3·19·73·89·283·3137·4817	6	9
8797235243700486	2·3·11·19·313·577·5147·7547	6	9
342916139097905191	3·13·17·37·53·61·157·1753·6733	7	7

Table 2: Some CN-elliptic curves with $5 \leq r(n) \leq 7$

6 Acknowledgements

The authors would like to express their gratitude to N. Rogers for giving the list of his unpublished results. The third author would like to thank J. Cremona for his helpful guides for using MWRANK and his suggestions to resolve certain computational issues in computing ranks of CN-elliptic curves for large positive integers.

References

[1] R. Alter, T. B. Curtz, and K. K. Kubota, Remarks and Results on Congruent numbers, *Proc. Third Southestern Conf. on Combinatorics, Graph Theory and Computing*, 1972 pp. 27–35.

[2] J. Aguirre, F. Castaneda, and J. C. Peral, High rank Elliptic Curves of the forms $y^2 = x^3 + Bx$, *Rev. Math. complut.*, **XIII**, num. 1 (2000), 1–15.

[3] G. Billing, Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven Geschlechteeins, *Nova Acta Reg. Soc. Sc. Upsaliensis* (4) **11** (1938), Nr. 1. Diss. 165 S.

[4] G. Campbell, Finding Elliptic Curves and Families of Elliptic Curves over $\mathbb{Q}$ of Large Rank , PhD Thesis, Rutgers University (1999).

[5] J. Cremona, `MWRANK` program, available from `http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/`.

[6] A. Dujella, High rank elliptic curves with prescribed torsion, `http://www.maths.hr/~duje/tors.html`, 2009.

[7] A. Dujella, On the Mordell-Weil groups of elliptic curves induced by Diophantine triples, *Glas. Mat.* **42** (2007), 3–18.

[8] A. Dujella, Irregular Diophantine m-tuples and elliptic curves of high rank, *Proc. Japan Acad. Ser. A Math. Sci.* **74** (2000), 66–67.

[9] N. D. Elkies, Algorithmic Number Theory: Tables and Links, `http://www.math.harvard.edu/~elkies/compnt.html`, (2002-2006).

[10] N. D. Elkies and N. F. Rogers, Elliptic Curves $x^3 + y^3 = k$ with High Rank, *Proc. ANTS-6 (ed. D. Buell), Lecture Notes in Comput. Sci.* **3076** (2004), 184–193.

[11] B. Faulkner and K. James, A graphical approach to computing Selmer groups of congruent number curves, *Ramanujan J*, **14** (2007), 107–129.

[12] K. Feng, Non-congruent numbers, odd graphs and the Birth-Swinnerton-Dyer conjecture, *Acta Arith.* **65** (1996), 71–83.

[13] K. Feng and M. Xiong, On the elliptic curves $y^2 = x^3 - n^2x$ with rank zero, *J. Number Theory* **109** (2004), 1–26.

[14] D. R. Heath-Brown, The size of Selmer groups for congruent number problem, *Invent. math.* **111** (1993), 171–195.

[15] D. R. Heath-Brown, The size of Selmer groups for congruent number problem, II. *Invent. math.* **118** (1994), 331–370.

[16] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms,* Springer-Verlag, GTM 97, 2nd ed, Berlin (1993).

[17] L. Kulesz and C. Stahlke, Elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$, *Experiment Math.* **10** (2001), 475–480.

[18] K. Nagao, An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20, *Proc. Japan Acad. Ser. A Math. Sci.* **69** (1993), 291–293.

[19] K. Nagao, An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 21, *Proc. Japan Acad. Ser. A Math. Sci.* **70** (1994), 104–105.

[20] PARI/GP, version 2.4.0, Bordeaux, 2008, `http://pari.math.u-bordeaux.fr`.

[21] N. Rogers, Rank computations for the congruent number elliptic curves, *Experiment. Math.* **9** (2000), no. 4, 591–594.

[22] N. Rogers, Elliptic curves $x^3 + y^3 = k$ with high rank, PhD Thesis in Mathematics, Harvard University (2004).

[23] N. Rogers, Personal communication, 2009.

[24] S. Roberts, Note on a Problem of Fibonacci's, *Proc. London Math. Soc.* **11** (1879), 35–44.

[25] K. Rubin and A. Silverberg, Ranks of elliptic curves in the families of quadratic twists, *Experiment Math.* **9** (2000), no. 4, 583–590.

[26] P. Serf, Congruent numbers and elliptic curves. *In Computational Number Theory. Debrecen: de Gruyter* (1991), 227–238.

[27] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Springer-Verlag, GTM **106**, New york (1986).

[28] N. J. A. Sloane, The on-line encyclopedia of integer sequences, `http://www.research.att.com/~njas/sequences/`.

[29] J. T. Tate and J. H. Silverman, *Rational Point on Elliptic Curves*, second edition, Springer-Verlag, UTM, New york (1994).

[30] A. Wiman, Über rationale Punkte auf Kurven $y^2 = x(x^2 - c^2)$, *Acta Math.* **77** (1945), 281–320.