Honam Mathematical J. **32** (2010), No. 1, pp. 177–192

A METHOD OF COMPUTATIONS OF CONGRUENT NUMBERS AND ELLIPTIC CURVES

Park, Jong Youll† and Lee, Heon Soo

Abstract. We study the concepts of congruent number problems and elliptic curves. We research the structure of the group of elliptic curves and find out a method of the computation of $L(E_n, 1)$ and $L'(E_n, 1)$ by using SAGE program. In this paper, we obtain the first few congruent numbers for $n \leq 2500$.

1. Introduction

One of the oldest unsolved problem in mathematics is to determine the congruent numbers: Give a way to decide whether or not an integer is the area of a right triangle with rational side lengths. For example, 6 is the area of the right triangle with side lengths 3, 4 and 5. 350 years ago, Fermat proved that 1 is not a congruent number. The questions we will examine here is: Which natural numbers occur as the area of a rational right triangle?

Definition 1. *A natural number n is called a congruent number if there is a rational right triangle with the area n: there are rational numbers $a, b, c > 0$ such that $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$.*

The congruent number problem is to determine which natural numbers are congruent numbers. No one has yet found an unconditional algorithm that would decide in a finite number of steps whether a given natural number is congruent or not.

Received January 25, 2010. Revised March 12, 2010.
2000 Mathematics Subject Classification : 11M, 11N.
Key words and phrases : Congruent number problem, Elliptic curves, Modular form, Birch and Swinnerton-Dyer Conjecture, SAGE program.
† This study was financially supported by Chonnam National University in 2008.

Recently the congruent number problem has become very popular with the discovery of a deep connection between this problem and the arithmetic of elliptic curves. It is also interesting to notice that if any number n is a congruent number, then s^2n is also a congruent number by multiplying the perpendicular legs each by s. Hence, to treat the general case one need to consider only the congruent number problem for natural numbers n having no square factor larger than 1. For example, since 1 and 2 are not congruent numbers, 4, 8 and 9 cannot be congruent numbers either. From now on, we assume that natural numbers under consideration are square free.

2. Congruent Number Problems and Elliptic curves

There are two distinct problems concerning congruent numbers: How to decide whether a given integer n is a congruent number, and given a congruent number n. How to find a rational right triangle with the area n?

THEOREM 2. *For a square-free positive integer n, n is a congruent number if and only if there is a rational number x such that $x-n$, x and $x+n$ are each the squares of a rational number.*

Proof. Suppose n is a congruent number. That is, there are rational numbers a, b and c such that $a^2+b^2=c^2$ and $\frac{1}{2}ab=n$. We choose

$$x=\left(\frac{c}{2}\right)^2 \Rightarrow x \pm n=\frac{c^2 \pm 4n}{4}=\left(\frac{a \pm b}{2}\right)^2$$

Conversely, say that $x-n$, x and $x+n$ are all rational squares. We choose $a=\sqrt{x+n}-\sqrt{x-n}$, $b=\sqrt{x+n}+\sqrt{x-n}$ and $c=2\sqrt{x}$, then $a^2+b^2=c^2$ and $\frac{1}{2}ab=n$. □

The connection between congruent numbers and elliptic curves is the following fact:

THEOREM 3. *For a square-free positive integer n, n is a congruent number if and only if there exists a rational point on the elliptic curve $E_n: y^2=x^3-n^2x$.*

Proof. Suppose that there exists a rational point (x, y) such that $y \neq 0$ on the elliptic curve $E_n: y^2=x^3-n^2x$. Let $a=\left|\frac{x^2-n^2}{y}\right|$, $b=\left|\frac{2xn}{y}\right|$ and $c=\left|\frac{x^2+n^2}{y}\right|$. Then we can obtain $a^2+b^2=c^2$ and $\frac{1}{2}ab=n$.

Conversely, make the substitution: $x = (\frac{c}{2})^2$ and $y = \frac{c(a^2-b^2)}{8}$. Then (x, y) is a rational point of $y^2 = x^3 - n^2x$. □

For example, when $n = 6$ we can obtain a rational point $(x, y) = \left(\frac{25}{4}, \frac{-35}{8}\right)$.

3. The Structure of the Group of Elliptic Curves

For our purpose, we consider an elliptic curve defined by a cubic equation of the form

$$y^2 = x^3 + ax + b \quad (a, b \in Z) \tag{3.1}$$

with $4a^3 + 27b^2 \neq 0$. This means that $y^2 = x^3 + ax + b(a, b \in Z)$ has no repeated roots in the complex numbers C. It thus has either three real roots or one real root. Accordingly, the set of points on this curve with real coordinates has either one or two components.

Let $E(Q)$ denote the set of rational points on an elliptic curve E. $E(Q) = \{(x, y) \in Q^2 | y^2 = x^3 + ax + b\} \cup \{O\}$. This ideal point O is to be regarded as a point that lies at both "ends" of every vertical line. The following two facts make the study of elliptic curves interesting:

1. An elliptic curve may or may not have infinitely many rational points. Which elliptic curve has only finitely many rational points is still an open question.

2. The set $E(Q)$ has a structure of an Abelian group. We denote the group law by $+$. It is given by the chord and tangent method. The sum of two points can be explicitly computed as follows.

To add two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ of $E(Q)$ intersect the chord line L through P_1 and P_2 (the tangent to E at P if $P_1 = P_2 = P$ with E. A straight line meets a cubic in three points. Let $P_3 = (x_3, y_3)$ be the third point of intersection of E with L. Then $P_1 + P_2 = (x_3, -y_3)$. The point at infinity acts as the identity because any two points of $E(Q)$ that lie on a vertical line are collinear with O. We show that $P_1 + P_2$ belongs to $E(Q)$.

We actually compute the coordinates of $P_1 + P_2$. For a point $P = (x, y)$, let $x = x(P)$ denote the x-coordinate of P (similarly, define $y(P)$), and let the line L that arises in the definition of addition have the equation

$$y = mx + l. \tag{3.2}$$

Then

$$m = \frac{y_1 - y_2}{x_1 - x_2}$$

which is rational. Substituting from (3.2) into (3.1), we have

$$x^3 - m^2x^2 + (a - 2ml)x + b - l^2 = 0. \tag{3.3}$$

Since x_1, x_2 and x_3 are the three solutions of (3.3), this is the same as

$$(x - x_1)(x - x_2)(x - x_3) = 0$$

or in expanded form

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3 = 0. \tag{3.4}$$

Comparing the coefficients of (3.3) and (3.4), we get

$$x(P_1 + P_2) = x_3 = m^2 - (x_1 + x_2) = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - (x_1 + x_2).$$

We can then appeal to (3.2) to obtain

$$y(P_1 + P_2) = \left(\frac{y_1 - y_2}{x_1 - x_2}\right) = \left[\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - (x_1 + x_2)\right] + l.$$

Because l is plainly rational numbers, this shows that $P_1 + P_2$ has rational coordinates. Mordell-Weil proves that $E(Q)$ has the following property. Let E be an elliptic curve defined over Q. Then $E(Q)$ is a finite group. Suppose we have points $R_1, R_2, \cdots, R_n$ representing the finitely many cosets in $E(Q)/2E(Q)$. Let $c = Max_i\{h(R_i)\}$ where $h(R_i)$ is the cannonical height. Let $Q_1, Q_2, \cdots, Q_m$ be the set of points with $h(Q_i) \leq c$. Then $E(Q)$ is generated by $R_1, R_2, \cdots, R_n, Q_1, Q_2, \cdots, Q_m$.

Theorem 4 (Mordell-Weil). *Let E be an elliptic curve defined over Q defined by the form*

$$y^2 = x^3 + ax + b \quad (a, b \in Z)$$

with $4a^3 + 27b^2 \neq 0$. Then $E(Q)$ is a finitely generated abelian group.

Hence as a group

$$E(Q) \cong Z^r \bigoplus T$$

where $T = E(Q)_{tor}$ is a finite group, called the torsion subgroup of $E(Q)$. It consists of the elements of $E(Q)$ of finite order. The nonnegative integer $r = r_Q(E)$ is called the rank of E over Q. Clearly, $r_Q(E) > 0$ if and only if $E(Q)$ has infinitely many rational points. In particular, a square-free integer n is a congruent number if and only if the elliptic curve defined by (3.1) has a positive rank. While the rank of $r_Q(E)$ is harder to compute, the torsion subgroup $E(Q)_{tor}$ is fairly well understood. In fact, the following well-known theorem gives an algorithm to determine $E(Q)_{tor}$ for an arbitrary elliptic curve E.

Theorem 5 (Lutz-Nagell). *Suppose that the elliptic curve E is given by*

$$y^2 = x^3 + ax + b \quad (a, b \in Z),$$

where $4a^3 + 27b^2 \neq 0$. If $P = (x, y)$ is a point of $E(Q)_{tor}$ that is different from O, then x and y are integers.

Moreover, either $y = 0$ or y^2 divides $\triangle$ ([6, p. 205.]). We need the Lutz-Nagell theorem primarily to link the existence of a right triangle of area n with rational side-lengths to the positivity of the rank of the elliptic curves defined by (3.1).

4. Birch and Swinnerton-Dyer Conjecture

We give the definition of the L-series of an elliptic curve E defined by the form

$$y^2 = x^3 + ax + b \quad (a, b \in Z)$$

with $4a^3 + 27b^2 \neq 0$. Let $a_p = p + 1 - \sharp E(F_p)$. Then the L-function of E is the Euler product

$$L_E(s) = \prod_{badp}(1 - a_p p^{-s})^{-1} \prod_{goodp}(1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where the concept of the reduction mod p in ([6, p. 207]).

The product over all p yields an expression $L_e(S) = \sum_{n=1}^{\infty} a_n n^{-s}$. To explain the analytic properties of $L_e(S)$ we introduce a new function $f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n$ where $\tau \in H$, the upper half of the complex plane and $q = e^{2\pi i\tau}$. Let N be a positive integer and define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a\,b \\ c\,d \end{pmatrix} \in SL_2 \mid c \equiv 0(mod\ N) \right\}.$$

Theorem 6 (Breuil, Conard, Diamond, Taylor, Wiles). *Let E be an elliptic curve over Q defined by the form*

$$y^2 = x^3 + ax + b \quad (a, b \in Z)$$

with $4a^3 + 27b^2 \neq 0$. There exists an integer N such that, for all $\tau \in H$, $f_E\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau + d)^2 f_E(\tau)$ for all $\left(\begin{smallmatrix} a\,b \\ c\,d \end{smallmatrix}\right) \in \Gamma_0(N)$, $f_E(-1/N_\tau) = \pm {N_\tau}^2 f_E(\tau)$ ([6, p. 436]).

The theorem says that $f_E()$ is a modular form of weight 2 and level N. The smallest possible N is called the conductor of E. Let E_n be the elliptic curve

$$E_n : y^2 = x^3 - n^2 x,$$

where n is a positive square-free integer. If n is odd, let $N = 32n^2$, and if n is even, let $N = 16n^2$. The number N is called the conductor of E_n. For any prime $p \nmid 2n$, let $a_p = p + 1 - \sharp E_n(F_p)$ where $\sharp E_n(F_p)$ is the number of points on the elliptic curve E_n viewed modulo p. If $p|2n$, let $a_p = 0$. If m and n are coprime integers, let $a_{mr} = a_m a_r$. We can define the L series when $s = 1$.

$$L(E_n, 1) = \begin{cases} x, & \text{n = 5, 6, 7 \pmod 8} \\ 2\sum_{k=1}^{\infty} \frac{a_k}{k} e^{-2k\pi/\sqrt{N}}, & \text{otherwise} \end{cases}$$

We can explain this conjecture roughly. If $E_n(Q)$ is infinite then the number $\sharp E(F_p)$ will tend to be big, since you get lots of elements of $E(F_p)$ by reducing the elements of $E_n(Q)$ modulo p. Thus $a_p = p + 1 - \sharp E_n(F_p)$ will tend to be small. One can prove that $L(E_n, 1) = 0$, then the $E(F_p)$ are big and the points have to come from somewhere so $E_n(Q)$ is big.

Conjecture 7 (Birch and Swinnerton-Dyer). *Let E_n be the elliptic curve defined by of the form*

$$E_n = y^2 = x^3 - n^2 x,$$

where n is a positive square-free integer.

We have $L(E_n, 1) = 0$ if and only if $E_n(Q)$ is infinite ([5, p. 16]). This statement remains unproved, although there has been some progress. In 1977, Coates and Wiles showed that if E_n has complex multiplication and has a point of infinite order, then $L(E_n, 1) = 0$. In 1983, Gross and Zagier have shown that if E_n is a elliptic curve such that $L(E_n, 1) = 0$ and $L'(E_n, 1) \neq 0$, then $E_n(Q)$ contains a rational point of infinite order. In 2000, the Clay Mathematics Institute listed the Conjecture of Birch and Swinnerton-Dyer as one of its million dollar problems.

5. A computation for various n

SAGE program is an open source computer algebra package that can be downloaded for free from http://www.sagemath.org/. It is difficult to define the general function $L(E_n, s)$ for every n, but we can only evaluate $L(E_n, 1)$ by SAGE program. The Conjecture 5 says that if $L(E_n, 1) \neq 0$, then $E_n(Q)$ is finite. By Theorem 3, the finiteness of the group $E_n(Q)$ implies that n is not a congruent number. For example, we can find that $L(E_1, 1) \neq 0$ and $L(E_{41}, 1) = 0$. From the theorem of Gross and Zagier, if we can calculate $L(E_n, 1) = 0$ and $L'(E_n, 1) \neq 0$ then we can say that n is a Congruent number. By using SAGE program, we can compute $L(E_n, 1)$ and $L'(E_n, 1)$. We can get a table of the first few congruent numbers.

For example for $n = 5$, we can compute $L(E_5, 1)$ and $L'(E_5, 1)$ the following way using SAGE program;

sage: E = EllipticCurve([-5^2 ,0])
sage: E
    Elliptic Curve defined by $y^2 = x^3 - 25x$ over Rational Field
sage: E.rank()
    0
sage: L = E.lseries().dokchitser()

(* where E.lseries().dokchitser() is a Dokchitsers L-functions Calculator coded Sage interface by William Stein.)

sage: L(1)

0

sage: L.derivative(1,E.rank())

2.22737037954414

'L.derivative(1, E.rank())' returns the first derivative of the L-series at s in the case of the L-series of a rank 2 Curve and 'L.derivative(1)' returns in the case of the L-series of rank 1 Curve.

For another instance, we can compute $L(E_{269}, 1)$ and $L'(E_{269}, 1)$ in the case of a rank 1 elliptic curve when $n = 269$ as followings;

sage: E = EllipticCurve([-269^2 ,0])

sage: E

Elliptic Curve defined by $y^2 = x^3 - 72361 * x$ over Rational Field

sage: E.rank()

The rank has not been completely determined, only a lower bound of

0

and an upper bound of 1. Traceback (click to the left for traceback).

...

RuntimeError: Rank not provably correct.

sage: L = E.lseries().dokchitser()

sage: L(1)

0

sage: L.derivative(1,E.rank())

The rank has not been completely determined, only a lower bound of

0

and an upper bound of 1. Traceback (click to the left for traceback).

...

RuntimeError: Rank not provably correct.

Return the error message because the rank of Elliptic Curve defined by $y^2 = x^3 - 72361x$ over Rational Field is has not been completely determined, only a lower bound of 0 and an upper bound of 1. L.derivative(1) has to be used in this case.)

```
sage: L.derivative(1)
      8.94367097457600
```

Using the SAGE program, we evaluate values of $L(E_n, 1)$, $L'(E_n, 1)$ and rank of E_n for $n \leq 100$ in the Table 1. And, we have congruent numbers for $n \leq 2500$ in the Table 2.

Table 1. $L(E_n, 1)$ and $L'(E_n, 1)$ for $n \leq 100$

n	$L(E_n, 1)$	$L'(E_n, 1)$	rank of E_n
1	0.655514388573030	0.655514388573030	0
2	0.927037338650686	0.927037338650686	0
3	1.51384563480125	1.51384563480125	0
4	0.655514388573030	0.655514388573030	0
5	0	2.22737037954414	1
6	0	1.90246004901839	1
7	0	2.96211488325481	1
8	0.927037338650686	0.927037338650686	0
9	0.655514388573030	0.655514388573030	0
10	1.65833480552274	1.65833480552274	0
11	0.790580098754899	0.790580098754899	0
12	1.51384563480125	1.51384563480125	0
13	0	4.24156537851424	1
14	0	2.99107433715881	1
15	0	4.03863541936211	1
16	0.655514388573030	0.655514388573030	0
17	2.54376947124591	2.54376947124591	0
18	0.927037338650686	0.927037338650686	0
19	0.601541258068777	0.601541258068777	0
20	0	2.22737037954414	1
21	0	3.80260949015458	1
22	0	4.75522489696261	1
23	0	5.66850104647998	1
24	0	1.90246004901839	1
25	0.655514388573030	0.655514388573030	0
25	0.655514388573030	0.655514388573030	0

n	$L(E_n, 1)$	$L'(E_n, 1)$	rank of E_n
26	1.02845558731530	1.02845558731530	0
27	1.51384563480125	1.51384563480125	0
28	0	2.96211488325481	1
29	0	4.30603790301781	1
30	0	5.16341557986856	1
31	0	3.48514648926405	1
32	0.927037338650686	0.927037338650686	0
33	1.82576653132841	1.82576653132841	0
34	8.06022589243296e-20	12.7703039097255	2
35	1.77283447852243	1.77283447852243	0
36	0.655514388573030	0.655514388573030	0
37	0	5.84755917186704	1
38	0	6.14944286741449	1
39	0	4.85417809014757	1
40	1.65833480552274	1.65833480552274	0
41	1.56658097453827e-19	16.4310487151526	2
42	3.23673811536547	3.23673811536547	0
43	3.59874025523419	3.59874025523419	0
44	0.790580098754899	0.790580098754899	0
45	0	2.22737037954414	1
46	0	3.50308083196832	1
47	0	6.33439060047744	1
48	1.51384563480125	1.51384563480125	0
49	0.655514388573030	0.655514388573030	0
50	0.927037338650686	0.927037338650686	0
51	1.46864598898018	1.46864598898018	0
52	0	4.24156537851424	1
53	0	7.77431014997303	1
54	0	1.90246004901839	1
55	0	7.03122889532326	1
56	0	2.99107433715881	1
57	1.38920002909870	1.38920002909870	0
58	0.688586048413973	0.688586048413973	0
59	0.341362817522334	0.341362817522334	0
60	0	4.03863541936211	1
61	0	5.57653526735718	1
62	0	7.19215527552409	1
63	0	0, 2.96211488325481	1
64	0.655514388573030	0.655514388573030	0
65	6.22660450905835e-20	24.2153538528129	2

n	$L(E_n, 1)$	$L'(E_n, 1)$	rank of E_n
66	2.58202379033152	2.58202379033152	0
67	0.320335314478121	0.320335314478121	0
68	2.54376947124591	2.54376947124591	0
69	0	7.03383838349760	1
70	0	5.17645286180021	1
71	0	2.55288605041919	1
72	0.927037338650686	0.927037338650686	0
73	1.22755449667452	1.22755449667452	0
74	0.609615998673705	0.609615998673705	0
75	1.51384563480125	1.51384563480125	0
76	0.601541258068777	0.601541258068777	0
77	0	9.90734919480397	1
78	0	7.77952747985335	1
79	0	5.69024933880479	1
80	0	2.22737037954414	1
81	0.655514388573030	0.655514388573030	0
82	2.31646253741247	2.31646253741247	0
83	0.287808207097252	0.287808207097252	0
84	0	3.80260949015458	1
85	0	5.24636933737291	1
86	0	3.32848274901069	1
87	0	11.0196331919950	1
88	0	4.75522489696261	1
89	1.11175017952172	1.11175017952172	0
90	1.65833480552274	1.65833480552274	0
91	1.09946527007063	1.09946527007063	0
92	0	5.66850104647998	1
93	0	7.93765965315906	1
94	0	5.17721825236304	1
95	0	7.85471664623426	1
96	0	1.90246004901839	1
97	1.06491843300406	1.06491843300406	0
98	0.927037338650686	0.927037338650686	0
99	0.790580098754899	0.790580098754899	0
100	0.655514388573030	0.655514388573030	0

Table 2. Congruent numbers for $n \leq 2500$

	Rank 1	Rank 2
100		5,6,7,13,14,15,20,21,22,23,24,28,29,30,31,34,37,38,39, 41,45,46,47,52,53,54,55,56,60,61,62,63,65,69,70,71,77, 78,79,80,84,85,86,87,88,92,93,94,95,96 (50)
200		101,102,103,109,110,111,112,116,117,118,119,120,124, 125,126,127,133,134,135,136,137,138,141,142,143,145, 148,149,150,151,152,154,156,157,158,159,161,164,165, 166,167,173,174,175,180,181,182,183,184,188,189,190, 191,194,197,198,199 (57)
300	269,277,293 (3)	205,206,207,208,210,212,213,214,215,216,237,238,219, 220,221,222,223,224,226,229,230,231,239,240,244,245, 246,247,248,252,253,254,255,257,260,261,262,263,265, 270,271,276,278,279,280,284,285,286,287,291,293,294, 295,299 (54)
400	317,367,373, 389 (4)	301,302,303,306,308,309,310,311,312,313,316,318,319, 320,323,325,326,327,330,333,334,335,336,340,341,342, 343,344,348,349,350,351,352,353,357,358,359,365,366, 368,369,371,372,374,375,376,380,381,383,382,384,386, 390,391,395,397,398,399 (58)
500	438,445,461 (3)	404,405,406,407,408,410,412,413,414,415,421,422,423, 426,429,430,431,434,436,437,439,440,442,444,446,447, 448,453,454,455,457,462,463,464,465,468,469,470,471, 472,476,477,478,479,480,485,486,487,493,494,495,496 (52)
600	503,541,553, 557,582,599 (6)	501,502,504,505,508,509,510,511,514,517,518,519,525, 526,527,532,533,534,535,536,540,542,543,544,546,548, 549,550,551,552,558,559,561,564,565,566,567,568,572, 573,574,575,580,581,583,585,589,590,591,592,596,597, 598,600 (54)
700	607,613,646, 647,653,661, 662,677,692 (9)	602,604,605,606,608,609,614,615,616,621,622,623,624, 629,630,631,632,636,637,638,639,645,651,654,655,656, 659,660,663,664,668,669,670,671,674,678,679,685,686, 687,689,693,694,695,696,700 (46)
800	701,727,733, 743,757,758, 773,797 (8)	702,703,709,710,711,717,718,719,721,723,724,725,726, 728,731,732,734,735,736,741,742,749,750,751,752,756, 759,760,761,764,765,766,767,774,775,776,777,781,782, 783,788,789,790,791,792,793,796,798,799 (49)

	Rank 1	Rank 2
900	823,829,838, 853,863,877, 887 (7)	805,806,807,813,814,815,820,821,822,824,828,830, 831,832,837,839,845,845,847,848,852,854,855,856, 860,861,862,864,866,869,870,871,876,878,879,880, 884,885,886,888,889,890,891,892,893,894,985,896 (48)
1000	901,911,933, 941,958,959, 967,982,983, 997,998 (11)	902,903,904,905,909,910,915,916,917,918,919,920, 925,926,927,934,935,942,943,948,949,950,951,952, 956,957,960,965,966,973,974,975,976,980,981,984, 987,988,989,990,991,992,995,999 (44)
1100	1013,1061, 1063,1069, 1076,1087, 1093 (7)	1003,1005,1006,1007,1008,1012,1014,1015,1016,1020, 1021,1022,1023,1025,1028,1029,1030,1031,1037,1038, 1039,1040,1044,1045,1046,1047,1048,1052,1053,1054, 1055,1057,1060,1062,1070,1071,1073,1077,1078,1079, 1080,1081,1084,1085,1086,1094,1095 (47)
1200	1108,1109, 1117,1142, 1157,1158, 1167,1172, 1181 (9)	1101,1102,1103,1104,1105,1110,1111,1112,1113,1116, 1118,1119,1120,1122,1125,1126,1127,1131,1133,1134, 1135,1136,1140,1141,1143,1144,1145,1146,1148,1149, 1150,1151,1154,1155,1159,1164,1166,1169,1173,1174, 1175,1176,1178,1180,1182,1183,1185,1186,1189,1190, 1191,1195,1196,1197,1198,1199 (45)
1300	1213,1223, 1229,1231, 1237,1238, 1262,1268, 1277,1279, 1286 (11)	1201,1204,1205,1206,1207,1208,1212,1214,1215,1217, 1221,1222,1224,1230,1232,1233,1236,1239,1240,1241, 1242,1244,1245,1246,1247,1248,1249,1253,1254,1255, 1261,1263,1264,1270,1271,1272,1276,1278,1280,1282, 1285,1287,1292,1293,1294,1295,1300 (47)
1400	1317,1318, 1319,1327, 1366,1367, 1373,1381, 1382 (9)	1301,1302,1303,1304,1305,1308,1309,1310,1311,1320, 1321,1325,1326,1330,1332,1333,1334,1335,1336,1339, 1340,1341,1342,1343,1344,1346,1349,1350,1351,1357, 1358,1359,1360,1364,1365,1368,1372,1374,1375,1376, 1379,1383,1384,1386,1387,1389,1390,1391,1392,1393, 1396,1397,1398,1399,1400 (55)
1500	1413,1423, 1429,1439, 1446,1447, 1453,1462, 1468,1471, 1477,1478, 1487,1492 (14)	1404,1405,1406,1407,1408,1411,1412,1414,1415,1419, 1421,1422,1428,1430,1431,1432,1434,1436,1437,1438, 1443,1445,1454,1455,1460,1461,1463,1464,1469,1470, 1472,1476,1479,1482,1484,1485,1486,1488,1493,1494, 1495,1496,1500 (43)
1600	1509,1527, 1535,1543, 1549,1556, 1557,1559, 1574,1582, 1583,1597, 1598 (13)	1501,1502,1503,1504,1510,1511,1517,1518,1519,1520, 1524,1525,1526,1528,1532,1533,1534,1536,1541,1542, 1544,1550,1551,1558,1560,1561,1564,1565,1566,1567, 1573,1575,1580,1581,1588,1589,1590,1591,1592,1595, 1596,1599 (42)

	Rank 1	Rank 2
1700	1607,1613, 1621,1622, 1637,1639, 1655,1663, 1685,1693 (10)	1605,1606,1610,1614,1615,1616,1620,1623,1624,1628, 1629,1630,1631,1632,1633,1635,1638,1640,1645,1646, 1647,1648,1649,1651,1652,1653,1654,1656,1659,1660, 1661,1662,1666,1669,1670,1671,1677,1678,1679,1684, 1686,1687,1688,1692,1694,1695 (46)
1800	1718,1726, 1733,1741, 1752,1759, 1780,1781, 1783,1789 (10)	1701,1702,1703,1704,1705,1709,1710,1711,1716,1717, 1719,1720,1724,1725,1727,1731,1734,1735,1736,1742, 1743,1744,1745,1746,1748,1749,1750,1751,1756,1757, 1758,1760,1762,1765,1766,1767,1768,1770,1773,1774, 1775,1776,1782,1784,1785,1788,1790,1791,1792,1794, 1797,1798,1799 (53)
1900	1823,1837, 1844,1847, 1853,1861, 1871,1877, 1878 (9)	1805,1806,1807,1812,1813,1814,1815,1816,1820,1821, 1822,1828,1829,1830,1831,1838,1839,1845,1846,1848, 1852,1854,1855,1856,1858,1860,1862,1863,1869,1870, 1872,1876,1879,1880,1884,1885,1886,1887,1888,1892, 1893,1894,1895,1896 (44)
2000	1901,1902, 1933,1942, 1949,1951, 1958,1959, 1973,1997, 1999 (11)	1903,1904,1908,1909,1910,1911,1912,1916,1917,1918, 1919,1920,1925,1926,1927,1934,1935,1939,1940,1941, 1943,1944,1948,1950,1957,1965,1966,1967,1971,1972, 1974,1975,1976,1980,1981,1982,1983,1984,1989,1990, 1991,1995,1998,2000 (44)
2100	2005,2012, 2022,2029, 2053,2063, 2069,2077, 2078,2087 (10)	2004,2006,2007,2008,2009,2013,2014,2015,2016,2020, 2021,2023,2030,2031,2032,2034,2035,2036,2037,2038, 2039,2040,2044,2045,2046,2047,2054,2055,2056,2059, 2061,2062,2068,2070,2071,2072,2076,2079,2085,2086, 2093,2094,2095,2100 (44)
2200	2127,2134, 2141,2143, 2157,2164, 2167,2173, 2182,2183 (10)	2101,2102,2103,2104,2108,2109,2110,2111,2113,2117, 2118,2119,2125,2126,2128,2130,2132,2133,2135,2136, 2139,2140,2142,2144,2145,2149,2150,2151,2154,2158, 2159,2160,2165,2166,2168,2170,2172,2174,2175,2176, 2181,2184,2189,2190,2191,2192,2195,2196,2197,2198, 2199,2200 (52)
2300	2206,2207, 2213,2215, 2221,2222, 2228,2237, 2239,2246, 2253,2263, 2278,2287 (14)	2201,2204,2205,2208,2214,2223,2229,2230,2231,2232, 2236,2238,2244,2245,2247,2249,2254,2255,2256,2257, 2260,2261,2262,2264,2268,2269,2270,2271,2272,2277, 2279,2282,2285,2286,2288,2292,2293,2294,2295,2296, 2298,2300 (42)

	Rank 1	Rank 2
2400	2302,2309, 2311,2317, 2323,2326, 2328,2333, 2335,2342, 2357,2381, 2383,2389, 2396,2399 (16)	2301,2303,2306,2310,2313,2318,2319,2320,2324,2325, 2327,2329,2332,2334,2337,2341,2343,2349,2350,2351, 2356,2358,2359,2360,2364,2365,2366,2367,2368,2373, 2374,2375,2379,2382,2384,2385,2388,2390,2391,2392, 2397,2398,2400 (43)
2500	2413,2421, 2422,2423, 2428,2437, 2447,2452, 2453,2454, 2461,2462, 2463,2477, 2486,2487, 2493,2495 (18)	2405,2406,2407,2408,2414,2415,2416,2418,2420,2424, 2429,2430,2431,2432,2434,2436,2438,2439,2445,2446, 2455,2456,2460,2464,2465,2469,2470,2471,2478,2479, 2484,2485,2488,2492,2494,2496 (36)

References

1. J. H. Coates, *Congruent Number Problem*, Pure and Applied Mathematics Quarterly, Vol.1, No. 1 (2005).

2. A. Dujella, A. S. Janfada, S. Salami, *A Search for High Rank Congruent Number Elliptic curves*, J. of Integer Sequence, Vol.12 (2009).

3. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, (2000).

4. K. Rubin, A.Silverberg, *Ranks of Elliptic Curves*, Bulletin of AMS, Vol.39, No.4 (2002).

5. W. Stein, *The Congruent Number Problem: A Thousand Year Old Unsolved Problem (http://modular.math.washington.edu).*

6. L. C. Washington, *Elliptic curves, Number theory and Cryptography*, CRC Press, (2003).

Park, Jong Youll
Department of Mathematics Education,
Chonnam National University,
Gwangju, 501-757, Korea
Email : parkjy@chonnam.ac.kr

Lee, Heon Soo
Graduate School,
Chonnam National University,
Gwangju, 501-757, Korea
Email : mathlee@chonnam.ac.kr