All congruent numbers less than 40000

By Fidel Ronquillo NEMENZO

Department of Mathematics, Sophia University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1998)

§1. Results. A square-free positive integer n is called a *congruent number* if it is the area of a right triangle with rational sides. The relevant family of elliptic curves defined over the rational field $\boldsymbol{Q}$ is

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

This is because a necessary and sufficient condition for n to be congruent is that E_n is of positive rank r_n. The Hasse-Weil L-function $L(E_n, s)$ has analytic continuation to all of $\boldsymbol{C}$, so we can consider its order s_n of vanishing at $s = 1$. Birch and Swinnerton-Dyer (BSD) conjectured that $s_n = r_n$. Using algorithms in Cremona [4], we computed $L^{(r)}(E_n, 1)$ for $r = 0, 1, 2, \ldots$ using 300000 series terms, thus producing estimates of s_n for all square-free $n < 100000$. Together with rank computations for this range, we have obtained the following results.

a) 56949 curves have $s_n \leq 1$. Among these, 26729 curves have $s_n = 0$ and the remaining 30220 curves have $s_n = 1$. The work of Coates-Wiles [1] and Gross-Zagier [2] proves $r_n = s_n$ for these curves.

b) 3656 curves have $s_n = 2$. We found that among such curves, all the 1665 curves with $n < 42553$ have $r_n \geq 1$.

c) There are 185 curves with $s_n \fallingdotseq 3$. Among these, 177 curves have $r_n = 3$, while for the remaining 8 curves, we have $3 \leq r_n \leq 5$. In either case, it follows that $s_n = 3$ because otherwise s_n should be 1, and $s_n = 1$ would imply $r_n = 1$, a contradiction. For the 8 curves, it is difficult to determine r_n because of the existence of certain quartic equations which are solvable locally everywhere but not globally. This suggests a non-trivial Tate-Shafarevich group for E_n or its 2-isogenous curve,

$$E'_n : y^2 = x^3 + 4n^2 x.$$

d) For $n < 100000$, four curves have $s_n \fallingdotseq 4$. These are E_{29274}, E_{46274}, E_{46754} and E_{57715}. All four curves have rank equal to 4.

These results, together with those of Coates and Wiles [1], show that if $n < 42553$, the weak form of BSD holds: $r_n > 0$ if and only if $L(E_n, 1) = 0$. As a consequence, we obtain all congruent numbers less than 42553.

§2. Rank computation algorithm. Using 2-descent, the computation of the rank r_n can be transformed into the problem of determining the solvability or non-solvability of certain Diophantine equations. Write $x \sim y$ whenever x and y belong to the same coset of $\boldsymbol{Q}^\times/(\boldsymbol{Q}^\times)^2$. Consider two types of equations:

$$dX^4 + \frac{4n^2}{d}Y^4 = Z^2 ;\ d \mid 4n^2, \tag{1}$$

$$dX^4 - \frac{n^2}{d}Y^4 = Z^2 ;\ d \mid n^2. \tag{2}$$

Now let $D_1 = d_1, d_2, \ldots, d_\mu$ be the set of distinct (i.e. pairwise inequivalent) square-free integers d_i such that $d_i \sim d$ $(i = 1, 2, \ldots, \mu)$ for some d dividing $4n^2$ and (1) is globally solvable in integers X, Y, and Z with $(X, \frac{4n^2}{d}YZ) = (Y, dXZ) = 1$. Similarly, let $D_2 = d_{\mu+1}, d_{\mu+2}, \ldots, d_{\mu+\nu}$ be the set of distinct square-free integers d_j such that $d_j \sim d$ $(j = \mu+1, \mu+2, \ldots, \mu+\nu)$ for some divisor d of n^2 and (2) is solvable in integers X, Y and Z with $(X, \frac{n^2}{d}YZ) = (Y, dXZ) = 1$. Then D_1 and D_2 are finite subgroups of $\boldsymbol{Q}^\times/(\boldsymbol{Q}^\times)^2$ and $r_n = \log_2 \mu\nu - 2$ (cf. Silverman and Tate [6]).

By determining the integers d such that (1) or (2) are locally solvable everywhere, we can bound r_n from above. We then search for global solutions of (1) and (2) to bound r_n below. While the assumption of the BSD conjecture would guarantee the eventual termination of solution search algorithms, several equations have very large solutions. The following method involving successive parameter changes was used for a more efficient search of solutions of the equation

$$aX^4 + bY^4 = Z^2. \tag{3}$$

First we search for (x_0, y_0, Z_0) satisfying the equation $ax^2 + by^2 = Z^2$, which has quadratic form parametric solutions

$$x = a_1 i^2 + a_2 ij + a_3 j^2 = f(i, j),$$
$$y = b_1 i^2 + b_2 ij + b_3 j^2 = g(i, j).$$

Next we search for (i_0, j_0, X_0) satisfying the equation $a_1 i^2 + a_2 ij + a_3 j^2 = X^2$, which has parametric solutions

$$i = c_1 k^2 + c_2 kl + c_3 l^2 = F(k, l),$$
$$j = d_1 k^2 + d_2 kl + d_3 l^2 = G(k, l).$$

We then search for k and l such that $y = g(F(k, l), G(k, l))$ is a square . If unsuccessful over a certain range, we employ another change of parameters and solution search. This method has allowed us to produce large solutions for equations (3). For example, we found the solution $X = 23134031$, $Y = 81124821$ and $Z = 1327\,211620355592802$ to the equation $2nX^4 + 2nY^4 = Z^2$ for $n = 20201$, proving that 20201 is a congruent number. For $n = 35842$, we found the solution $X = 19482547427$, $Y = 8090\,1619850$ to the equation $X^4 + Y^4 = 17921Z^2$, to prove likewise that 35842 is congruent.

§3. Local-global. Equations (2) and (1) which have solutions everywhere locally but none globally determine non-trivial elements of the Tate-Shafarevich groups Ш $(E_n(\boldsymbol{Q}))$ and Ш $(E'_n(\boldsymbol{Q}))$, which we shall describe in part.

Consider the 2-isogeny $\phi : E_n \to E'_n$ given by

$$(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 + n^2)}{x^2} \right)$$
$$(0, 0) \mapsto \infty'$$
$$\infty \mapsto \infty'$$

and its dual $\psi : E'_n \to E_n$ given by

$$(x, y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(x^2 - 4n^2)}{8x^2} \right)$$
$$(0, 0) \mapsto \infty$$
$$\infty' \mapsto \infty.$$

One can show that $E_n(\boldsymbol{Q})/\psi(E'_n(\boldsymbol{Q}))$ and $E'_n(\boldsymbol{Q})/\phi(E_n(\boldsymbol{Q}))$ are isomorphic to D_2 and D_1, respectively. The finite subgroup $S^{\psi}(E'_n) \subset \boldsymbol{Q}^{\times}/(\boldsymbol{Q}^{\times})^2$ consisting of d's for which (2) is locally solvable everywhere is the ψ-part of the Selmer group of E'_n. Similarly, the finite subgroup $S^{\phi}(E_n) \subset \boldsymbol{Q}^{\times}/(\boldsymbol{Q}^{\times})^2$ consisting of d's for which (1) is locally solvable everywhere is the ϕ-part of the Selmer group of E_n. The quotient of $S^{\psi}(E'_n)$ by D_2 is isomorphic to Ш $(E'_n)[\psi] \subset$ Ш (E'_n), while that of $S^{\phi}(E_n)$ by D_1 is isomorphic to Ш $(E_n)[\phi] \subset$ Ш (E_n). We have the following exact sequences:

$$0 \to E_n(\boldsymbol{Q})/\psi(E'_n(\boldsymbol{Q})) \to S^{\psi}(E'_n) \to \text{Ш}(E'_n)[\psi] \to 0,$$
$$0 \to E'_n(\boldsymbol{Q})/\phi(E_n(\boldsymbol{Q})) \to S^{\phi}(E_n) \to \text{Ш}(E_n)[\phi] \to 0.$$

For 0-rank curves E_n, we computed the order $|\text{Ш}(E_n)|$ using the conjectural (BSD) equation,

$$L(E_n, 1) = \Omega\, |\text{Ш}(E_n)|\, \|E_n(\boldsymbol{Q})_{tors}|^{-2} \prod c_p,$$

where Ω is a real period of E_n, $c_p = (E_n(\boldsymbol{Q}_p) : E_n^o(\boldsymbol{Q}_p))$ is the index of the subgroup $E_n^o(\boldsymbol{Q}_p)$ of p-adic points with good reduction mod p in $E_n(\boldsymbol{Q}_p)$; and the product is taken over all primes of bad reduction. For all 0-rank curves E_n with $n < 100000$, computations show that $|\text{Ш}(E_n)| = t^2$ for $t \le 40$. In particular, $|\text{Ш}(E_{72073})| = 40^2$.

Let E_n have rank 0. Using Tate's algorithm (cf. [4]) to compute c_p, we can obtain the ratio of the orders of the Tate-Shafarevich groups of the isogenous curves E_n and E'_n.

Proposition. *Let k be the number of prime divisors p of n such that $p \equiv 3 \pmod 4$. For 0-rank curves E_n, the ratio $|\text{Ш}(E'_n)|/|\text{Ш}(E_n)|$ of the orders of the Tate-Shafarevich groups of the isogenous curves E_n and E'_n is*

$$2^{k-2} \text{ if } n \equiv 1 \pmod 8,$$
$$2^{k-1} \text{ if } n \equiv 3 \pmod 8,$$
$$2^{k} \text{ if } n \text{ is even}.$$

For example, consider the 0-rank curve E_{42}. Assuming the BSD conjecture, we compute $|\text{Ш}(E_{42})|$ to be trivial. The proposition shows that $|\text{Ш}(E'_{42})| = 4$, suggesting the existence of an associated equation (2) which has local solutions everywhere but none globally. One such equation is $-7 \cdot 3^2 \cdot X^4 + 7 \cdot 2^2 \cdot Y^4 = Z^2$.

§4. Tables. (E_n is represented by the number n in Tables II -IV.)

Table I

s_n	r_n	No. of curves E_n with $n < 100000$
4	4	4
3	3	177
3	$3 \le r_n \le 5$	8
2	$1 \le r_n \le 2$	1558($n < 42553$)
2	$1 \le r_n \le 4$	107 ($n < 42553$)
2	$0 \le r_n \le 2$	1767($n \ge 42553$)
2	$0 \le r_n \le 4$	224 ($n \ge 42553$)
1	1	30220
0	0	26729

Table Ⅱ. All curves E_n ; $n < 100000$; $s_n \doteqdot 4$, $r_n = 4$

29274	46274	46754	57715

Table Ⅲ. All curves E_n ; $n < 100000$; $s_n = 3$; $3 \leq r_n \leq 5$

26245	42486	68839	80189	82205	83845	88502	92045

Table Ⅳ. All curves E_n ; $n < 100000$; $s_n = r_n = 3$

1254	2605	2774	3502	4199	4669	4895	6286	6671	7230
7766	8005	9015	9430	9654	10199	10549	11005	12166	12270
12534	12935	13317	14965	15655	16206	16887	17958	18221	19046
19726	20005	20366	20774	20909	21414	22134	23359	23405	23446
23709	24190	24414	26013	26565	27613	28007	28221	28806	29055
29294	29614	30270	32039	32318	32599	32893	33117	33286	35269
35286	35719	36366	36519	37862	38982	39630	40397	40406	40710
40885	40894	41151	41181	41230	41309	41582	41943	42029	43405
43870	45037	45118	46246	47094	47957	48622	50061	50583	50629
51302	51359	51590	51933	53605	55279	55510	55549	56406	56630
56990	57310	58326	58695	59415	60006	60119	60229	60415	60574
60847	61815	63005	65198	65310	65535	65639	67438	67542	67606
68295	68605	69015	69085	69326	69509	69870	70013	70189	70774
70941	70959	71654	72151	72854	73055	73151	74102	74166	75174
75454	76245	76479	76958	77046	77486	78422	78526	80015	81469
81669	81959	82309	83159	84134	84390	85470	85702	86086	86790
88206	88422	89238	89286	90174	90597	91749	91910	92157	93126
94655	95095	97422	98798	99231	99309	99645			

References

[1] J. Coates and A. Wiles: On the conjecture of Birth and Swinnerton-Dyer. Invent. Math., **39**, 223–251 (1977).

[2] B. Gross and D. Zagier: Heegner points and derivatives of L-series. Invent. Math., **84**, 225–320 (1986).

[3] H. Wada and M. Taira: Computations of the rank of the elliptic curve $y^2 = x^3 - n^2x$. Proc. Japan Acad., **70A**, 154–157 (1994).

[4] J. E. Cremona: Algorithms for Modular Elliptic Curves. Cambridge University Press (1992).

[5] J. H. Silverman: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, 106, Springer-Verlag, New York (1986).

[6] J. H. Silverman and J. Tate: Rational Points on Elliptic Curves. Springer-Verlag, New York (1992).