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 quadra-