Math. Ann. 273, 337–340 (1986)

Mathematische Annalen

All Congruent Numbers Less than 2000

Gerhard Kramarz

Mathematisches Institut der Universität, D-5300 Bonn 1, Federal Republic of Germany

1. Congruent Numbers

A natural number m is called congruent if it is the area of a right triangle with rational sides. An equivalent condition, as one easily checks, is that there should exist a rational square which, when increased or decreased by m, remains a square. Thus 6 is congruent because it is the area of the $(3, 4, 5)$-triangle or because $\frac{25}{4}, \frac{25}{4}+6$, and $\frac{25}{4}-6$ are all squares, and 5 is congruent because it is the area of the $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$-triangle or because $\frac{1681}{144}, \frac{1681}{144}+5$, and $\frac{1681}{144}-5$ are all squares.

The problem of congruent numbers is very old: The two examples just given can be found in an Arabian manuscript, written more than 1000 years ago, and in Fibonacci's book "liber quadratorum", published in 1225. More about its early history and the work done before 1920 can be found in Dickson's history of the theory of numbers [3].

A number m is also easily seen to be congruent if and only if there is a non-trivial rational point on the elliptic curve

$$E_m : my^2 = x^3 - x \tag{1}$$

(take the triangle with sides $x^2-1, 2x$, and x^2+1), i.e. if the rank of the Mordell-Weil group $E_m(\mathbb{Q})$ is positive. It was observed by Tunnell [7] that the conjecture of Birch and Swinnerton-Dyer and a recent result of Waldspurger [8] combine to give a complete conjectural answer to the problem. We state this in a slightly different form from that given by Tunnell. Since the condition "m congruent" is unchanged when m is multiplied by a square, we can and will assume m squarefree.

Conjecture. *For m squarefree, define*

$$c(m) = \begin{cases} \sum_{m = a^2 + 2b^2 + 8c^2} (-1)^c & (m \text{ odd}) \\ \sum_{m/2 = a^2 + b^2 + 8c^2} (-1)^c & (m \text{ even}). \end{cases}$$

Then

$$m \text{ is congruent} \Leftrightarrow c(m) = 0.$$

This implies in particular that all numbers $m \equiv 5$, 6 or 7 (mod 8) should be congruent, since the sum defining $c(m)$ is empty in this case.

The purpose of this note is to verify the conjecture for m less than 2000. Specifically, we shall show:

Theorem. *Let $m < 2000$ be a squarefree number. Then m is congruent if and only if $m \equiv 5$, 6 or 7 (mod 8) or m is one of the 106 numbers in Table 1.*

Previous numerical results can be found in a survey article by Guy [5] as well as in the aforementioned article of Tunnell.

2. The Associated L-Series

The curve E_m has complex multiplication by $\mathbb{Q}(\sqrt{-1})$ and its Hasse-Weil zeta function therefore has known analytic properties. This zeta function is given by

$$L(E_m, s) = \prod_{\substack{p \text{ prime}, \\ (p, 2m)=1}} \frac{1}{1 - \left(\frac{m}{p}\right) a_p p^{-s} + p^{1-2s}}, \quad \mathrm{Re}(s) > \tfrac{3}{2}$$

with $a_p = 0$ for $p \equiv 3 \pmod 4$ and $a_p = 2 \cdot (-1)^s \cdot r$ for $p \equiv 1 \pmod 4$ where $p = r^2 + 4s^2$ with $r \equiv 1 \pmod 4$. It extends analytically to all s and satisfies the functional equation

$$\left(\frac{N_m}{2\pi}\right)^s \Gamma(s) L(E_m, s) = \varepsilon_m \left(\frac{N_m}{2\pi}\right)^{2-s} \Gamma(2-s) L(E_m, 2-s)$$

with

$$N_m = \begin{cases} 32m^2 & \text{for } m \text{ odd} \\ 16m^2 & \text{for } m \text{ even} \end{cases}, \qquad \varepsilon_m = \begin{cases} +1 & \text{for } m \equiv 1, 2, 3 \pmod 8 \\ -1 & \text{for } m \equiv 5, 6, 7 \pmod 8 \end{cases}.$$

(For a detailed exposition of the properties of E_m and its L-series we refer to the book of Koblitz [6].)

According to the BSD-conjecture E_m should have positive rank if and only if $L(E_m, s)$ vanishes at $s = 1$, i.e.

$$m \text{ congruent} \overset{?}{\Leftrightarrow} L(E_m, 1) = 0.$$

For $m \equiv 5, 6, 7 \pmod 8$ the condition on the right is always satisfied because of the functional equation. For $m \equiv 1, 2, 3 \pmod 8$ the work of Waldspurger implies a formula for $L(E_m, 1)$ as a simple non-zero multiple of $c(m)^2$. This explains the conjecture stated in Sect. 1.

The following is known:

i) If $L(E_m, 1) \neq 0$, then $E_m(\mathbb{Q})$ is finite. This is a special case of the theorem of Coates and Wiles [2], which applies to any curve with complex multiplication.

ii) If $L(E_m, 1) = 0$ and $L'(E_m, 1) \neq 0$, then $E_m(\mathbb{Q})$ is infinite. This is a special case of the theorem of Gross and Zagier [4], which applies to any elliptic curve parametrized by modular functions, in particular to any curve with complex multiplication.

Combining this with what was said above, we get the following criteria:

(A) If $m \equiv 1, 2$ or $3 \pmod 8$ and $c(m) \neq 0$, then m is not congruent.

(B) If $m \equiv 5, 6$ or $7 \pmod 8$ and $L'(E_m, 1) \neq 0$, then m is congruent.

Thus we can proceed as follows:

If $m \equiv 1, 2, 3 \pmod 8$, then if $c(m) \neq 0$, we know by (A) that m is not congruent. If $c(m) = 0$, then the BSD-conjecture implies that $E_m(\mathbb{Q})$ should have rank at least 2 [since $L(E_m, s)$ has an even functional equation], so we expect relatively small solutions to (1) and we can simply search.

If $m \equiv 5, 6, 7 \pmod 8$, then we calculate $L'(E_m, 1)$. This can be done easily using the algorithm described in [1]. If $L'(E_m, 1)$ is not zero, we know by (B) that m is

congruent. If it is zero, then the BSD-conjecture predicts that $E_m(\mathbb{Q})$ has rank at least 3, so again we expect to find a small solution by a simple search.

In principle one could dispense with criterion (B), since we could simply exhibit a solution of (1). However, when the rank of $E_m(\mathbb{Q})$ is 1 the smallest solution of (1) can be large (for instance, for $m=157$ the simplest rational square x with $x \pm m$ also squares has 188 decimal digits in its numerator and denominator), and it is not very easy to write down such solutions.

3. Results

For numbers less than 2000 the results of the procedure described above are as follows: Of the 602 squarefree numbers $m<2000$ with $m \equiv 1, 2, 3 \pmod 8$ there are 106 for which $c(m)=0$. For each of these a non-trivial solution of (1) is given in Table 1, in the following notation:

We write (1) in the form

$$m \cdot \text{square} = A \cdot B \cdot (A-B) \cdot (A+B)$$

(A and B are the numerator and denominator of x).

Then since m is squarefree the numbers A, B, $A-B$, $A+B$ have the form sa^2, tb^2, uc^2, vd^2 for some decomposition of m as $s \cdot t \cdot u \cdot v$ and some natural numbers a, b, c, d; these 8 numbers are given in Table 1 below (blank $\hat{=}$ 1).

m	s	t	u	v	a	b	c	d
34	1	2	1	17	3	2	1	1
41	1	1	1	41	5	4	3	1
65	1	1	5	13	3	2	1	1
137	137	1	1	1	5	56	17	81
138	6	1	23	1	2	1	1	5
145	29	5	1	1	2	3	7	1
154	1	2	7	11	3	1	1	1
161	1	7	1	23	4	1	3	1
194	97	2	1	1	6	5	13	1
210	5	2	3	7	1	1	1	1
219	73	3	1	1	1	4	5	11
226	1	2	1	113	9	4	7	1
257	1	1	257	1	153	104	7	185
265	1	1	5	53	7	2	3	1
291	1	3	1	97	7	4	1	1
299	1	13	23	1	6	1	1	7
313	1	1	1	313	13	12	5	1
323	17	19	1	1	5	4	11	27
330	6	5	1	11	1	1	1	1
353	1	1	1	353	17	8	15	1
371	53	7	1	1	1	2	5	9
386	1	2	1	193	11	6	7	1
395	5	1	79	1	4	1	1	9
410	41	10	1	1	1	2	1	9
426	6	1	71	1	4	5	1	11
434	2	31	1	7	4	1	1	3
442	1	26	17	1	11	2	1	15
457	1	1	457	1	253	204	7	325
465	1	15	1	31	4	1	1	1
505	101	5	1	1	1	2	9	11
514	257	2	1	1	1	4	15	17
546	7	6	1	13	1	1	1	1
561	17	1	1	33	1	4	1	1
602	1	2	7	43	5	3	1	1
609	1	1	21	29	5	2	1	1
651	7	3	1	31	2	1	5	1
658	2	47	1	7	8	1	9	5
674	337	2	1	1	1	12	7	25
689	689	1	1	1	1	20	17	33
721	7	1	103	1	4	3	1	11
723	1	3	1	241	103	20	97	7
731	1	43	17	1	39	4	7	47
761	761	1	1	1	29	40	799	801
777	37	3	1	7	2	3	11	5
793	793	1	1	1	5	132	49	193
866	1	2	1	433	19	6	17	1
889	1	7	1	127	8	3	1	1
890	1	10	1	89	7	2	3	1
905	181	5	1	1	1	6	1	19
915	61	15	1	1	1	2	1	11
985	1	1	5	197	163	82	63	13
987	21	1	47	1	4	17	1	25
995	5	1	199	1	8	11	1	21

m	s	t	u	v	a	b	c	d
1003	1	59	1	17	63	4	55	17
1057	151	1	7	1	44	333	161	635
1073	1	1	37	29	23	14	3	5
1081	1	1	1081	1	35	12	1	37
1105	1	1	13	85	7	6	1	1
1113	7	1	3	53	2	5	1	1
1122	1	2	17	33	5	2	1	1
1131	1	13	3	29	4	1	1	1
1145	1145	1	1	1	5	52	161	177
1146	2	191	3	1	13	1	7	23
1154	1	2	1	577	17	12	1	1
1155	11	1	7	15	1	2	1	1
1169	7	1	167	1	12	29	1	43
1178	2	31	19	1	5	1	1	9
1185	1	15	1	79	8	1	7	1
1186	593	2	1	1	193	1972	3783	5465
1195	1	5	239	1	22	7	1	27
1201	1	1	1	1201	25	24	7	1
1217	1217	1	1	1	65	1504	1697	2721
1241	1	1	1	1241	29	20	21	1
1249	1	1	1	1249	481	360	319	17
1282	641	2	1	1	1	10	21	29
1321	1321	1	1	1	85	2952	911	4273
1330	14	5	1	19	1	1	3	1
1339	1	13	103	1	34	9	1	47
1346	673	2	1	1	17	42	437	445
1379	197	7	1	1	1	2	13	15
1387	73	19	1	1	25	48	43	299
1393	7	1	199	1	260	531	31	869
1411	17	83	1	1	37	16	45	211
1419	3	1	11	43	3	4	1	1
1434	6	1	239	1	10	19	1	31
1443	1	3	13	37	5	2	1	1
1482	19	6	13	1	1	1	1	5
1513	89	1	1	17	1	8	5	3
1561	1	223	1	7	116	3	107	47
1595	5	1	11	29	2	3	1	1
1610	14	1	5	23	1	3	1	1
1633	71	1	23	1	36	203	47	365
1635	109	15	1	1	1	2	7	13
1649	1649	1	1	1	1	40	7	57
1651	13	1	127	1	4	9	1	17
1659	1	21	79	1	10	1	1	11
1705	5	11	1	31	2	1	3	1
1731	577	3	1	1	1	4	23	25
1745	349	5	1	1	1	6	13	23
1762	881	2	1	1	1	20	9	41
1770	2	3	5	59	4	3	1	1
1785	3	5	7	17	2	1	1	1
1794	26	23	3	1	1	1	1	7
1858	1	2	1	929	27	10	23	1
1939	277	7	1	1	1	6	5	23
1995	3	7	5	19	2	1	1	1

For the 613 squarefree numbers $m<2000$ with $m\equiv 5, 6, 7 \pmod 8$ the calculation of $L'(E_m, 1)$ was carried out to about 6 decimal places. A small excerpt from the result is given in Table 2.

In all cases except $m=1254$ the value of $L'(E_m, 1)$ lay between 0.86 ($m=1669$) and 30.09 ($m=1743$), while for $m=1254$ the value was zero within the accuracy of the computation. Using the results of [4], one could now check that $L'(E_m, 1)$ is in fact zero, but we do not really care about this since the converse of criterion (B) is not true.

Table 2

m	$L'(E_m, 1)$	m	$L'(E_m, 1)$
5	2.227370	1245	16.833922
6	1.902460	1246	4.296937
7	2.962115	1247	11.999654
13	4.241565	1253	8.635734
14	2.991074	1254	0.000000
15	4.038635	1255	11.548777
21	3.802609	1261	7.363428
22	4.755225	1262	21.009608
23	5.668501	1263	12.558427

For $m=1254$ we write the equation of E_m in the equivalent form

$$y^2=x^3-m^2x=x\cdot(x-m)\cdot(x+m)$$

($x\to mx$, $y\to m^2y$). The three smallest integer solutions

$$(x, y)=(-198,17424),\ (-171,16245),\ (-98,12376)$$

are linearly independent over $\mathbb{Z}$, so $\operatorname{rank} E_m(\mathbb{Q})\geqq 3$. In fact the rank is exactly 3, as can be seen by a descent argument. A numerical calculation shows $L''(E_m, 1)\approx 322.546347\neq 0$, so the order of vanishing of the L-function at $s=1$ is also 3, in accordance with the BSD-conjecture.

Acknowledgement. I would like to thank Prof. Don Zagier for his help and encouragement.

References

1. Buhler, J.P., Gross, B.H., Zagier, D.B.: On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. Math. Comput. **44**, 473–481 (1985)
2. Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **39**, 223–251 (1977)
3. Dickson, L.E.: History of the theory of numbers. Vol. 2. New York: Stechert 1934
4. Gross, B.H., Zagier, D.B.: Points de Heegner et derivées de fonctions L. C.R. Acad. Sci. Paris **297**, 85–87 (1983)
5. Guy, R.K.: Unsolved problems in number theory. Berlin, Heidelberg, New York: Springer 1981
6. Koblitz, N.: Introduction to elliptic curves and modular forms. Graduate Texts in Mathematics 97. Berlin, Heidelberg, New York, Tokyo: Springer 1984
7. Tunnell, J.: A classical Diophantine problem and modular forms of weight 3/2. Invent. Math. **72**, 323–334 (1983)
8. Waldspurger, J.L.: Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. Pures Appl. **60**, 375–484 (1981)

Received August 15, 1985