36. Computations of the Rank of Elliptic Curve $y^2 = x^3 - n^2x$*)

By Hideo WADA and Mayako TAIRA

Department of Mathematics, Sophia University

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1994)

§1. Notations and results. Let n be a square free positive integer, E_n be the elliptic curve $y^2 = x^3 - n^2x$ and $L_n(s)$ be the Hasse-Weil L-function of E_n. About the behavior of $L_n(s)$ at $s = 1$, Birch and Swinnerton-Dyer [1] conjectured that the order s_n of zero at $s = 1$ is equal to the rank r_n of E_n over $\mathbf{Q}$. Formulas to calculate $L_n^{(r)}(1)$, $r = 0,1,2, \ldots$, are given in Cremona[4]. We have calculated by them the value of s_n for $n < 30000$. On the other hand, Chahal [2] gives a method, as explained in §2, to obtain r_n. We have calculated r_n for $n < 10000$ by this method and could obtain its value except for 77 cases:

Table I

s_n	r_n	number of n
0	0	2580
1	1	3035
2	$?(1 \leqq r_n \leqq 2)$	57(Table II)
2	2	376(Table II in [7])
2	$?(2 \leqq r_n \leqq 4)$	20(Table III)
3	3	15(Table IV)

For those n with $s_n \geqq 1$, $10000 < n < 20201$, we could verify that $r_n \geqq 1$. As $r_n \geqq 1$ implies $s_n \geqq 1$ as was shown by Coates and Wiles [3], we have obtained:

Result. $r_n > 0$ if and only if $s_n > 0$ for $n < 20201$.

Moreover we could get all congruent numbers < 20201 as shown in Table V (cf. [7]).

Our calculation was made by programs written in UBASIC.

§2. Method. If $x/y = u^2$ for some rational number u, we write $x \sim y$. Consider the next diophantine equations:

(1) $dX^4 - (n^2/d)Y^4 = Z^2$, $d \mid n^2$, $d \neq \pm 1$, $d \neq \pm n$

(2) $dX^4 + (4n^2/d)Y^4 = Z^2$, $n =$ odd, $d \mid 4n^2$, $d \neq 1$

(3) $dX^4 + (n^2/4d)Y^4 = Z^2$, $n =$ even, $4d \mid n^2$, $d \neq 1$.

Let $\{d_1, \ldots, d_\mu\}$ be the set of d's, for which (1) is solvable in X, Y, Z with $(X, Z) = (Y, Z) = 1$, and $\{d_{\mu+1}, \ldots, d_{\mu+\nu}\}$ be the set of d's, for which (2) or (3) is solvable in X, Y, Z with $(X, Z) = (Y, Z) = 1$ (we assume $d_i \neq d_j$ for $1 \leqq i, j \leqq \mu$, and for $\mu + 1 \leqq i, j \leqq \mu + \nu$ possibly $\mu = 0$, $\nu = 0$). Then $2^{r_n+2} = (4 + \mu)(1 + \nu)$, which gives us r_n. When $s_n > 1$, the values of r_n in Table I were obtained by this method.

*) Dedicated to professor S. Iyanaga on his 88th birthday.

Case 1. If $n \equiv 5,6,7 \pmod 8$ then s_n is odd (cf. [6]). Gross and Zagier [5] and Rubin [8] proved that $s_n = 1$ implies $r_n = 1$. There are 3035 values of n with $s_n = 1$ in the range $n < 10000$.

There are 15 numbers n such that $L_n'(1) \fallingdotseq 0$ which are listed in Table IV. For all these numbers n, we got $L_n^{(3)}(1) \neq 0$ and $r_n = 3$. If $L_n'(1) \neq 0$ then $s_n = r_n = 1$. Therefore we got $s_n = 3$ (cf. [4]).

Case 2. When $n \equiv 1,2,3 \pmod 8$ then s_n is even. For $n < 10000$, we get 2580 numbers n such that $L_n(1) \neq 0$. For these n, we have $r_n = 0$[3]. We got 453 numbers n such that $L_n(1) = 0$ which are listed in [7]. For all these n we got $L_n''(1) \neq 0$. Therefore maybe $r_n = 2$. For 376 numbers n, we got $r_n = 2$. But for 57 numbers n in Table II, we only got $1 \leqq r_n \leqq 2$ because of lack of time and for 20 numbers n in Table III, we only got $2 \leqq r_n \leqq 4$.

Example 1. We solved the equations (1)–(3) and we got next solutions.

	n	d	X	Y		n	d	X	Y
(1)	2434	1217	33	8	(3)	14114	7057	713118	384763
(3)	2434	1217	324641	121064	(1)	15721	1241959	92399	193673
(1)	4258	2129	240641	148120	(2)	16043	61	104065	447
(3)	4258	2129	5	28	(1)	17795	88975	236852	472781

From this table we get $r_{2434} = r_{4258} = 2$, $r_{14114} \geqq 1$, $r_{15721} \geqq 1$, $r_{16043} \geqq 1$, $r_{17795} \geqq 1$.

Example 2. When $n = 1513$, we have $L_{1513}(1) = 0$. We have a solution of (1): $25721 \cdot 3^4 - 89 \cdot 5^4 = 1424^2$ and a solution of (2): $3026 \cdot 7^4 + 3026 \cdot 5^4 = 3026^2$. Therefore $r_n \geqq 2$. When $d = 1513$, if the equation $1513X^4 + 6052Y^4 = Z^2$ is solvable then $Z = 1513W$ for some integer W and we get $X^4 + 4Y^4 = 1513W^2$. Maybe this equation is not solvable. But

$$X^4 + 4Y^4 \equiv 1513W^2 \pmod m$$

has non-trivial solution for $m = 17, 89, 16$ so that we can not easily decide the non-solvability. There are 6 d's for which the same situation occurs. Therefore we only get $2 \leqq r_{1513} \leqq 4$.

Table II. $s_n = 2$, $1 \leqq r_n \leqq 2$

1282	1762	1858	2273	3017	3433	3443	3593	3603	3713
3778	4411	4481	4681	4793	4834	4843	4889	4898	5273
5314	5362	5449	5587	5602	5657	5666	5747	5849	6073
6529	6658	6769	6995	7321	7394	7498	7609	7747	8122
8258	8354	8498	8521	8609	8801	9122	9257	9281	9377
9395	9442	9451	9497	9601	9634	9841			

Table III. $s_n = 2$, $2 \leqq r_n \leqq 4$

1513	2329	2379	3026	4633	4810	5986	6001	6355	6402
6953	7361	7585	7769	8106	8547	8555	9554	9595	9809

Table IV. $s_n = 3$, $r_n = 3$

1254	2605	2774	3502	4199	4669	4895	6286	6671	7230
7766	8005	9015	9430	9654					

Table V. $r_n > 0$, $10000 < n < 20201$, $n \equiv 1,2,3 \pmod 8$

10001	10010	10011	10033	10059	10074	10145	10146	10195	10329
10337	10346	10355	10370	10371	10385	10434	10489	10491	10505
10545	10553	10562	10601	10619	10626	10635	10649	10699	10730
10777	10785	10810	10945	10961	11010	11065	11082	11186	11193
11195	11201	11211	11226	11234	11265	11297	11330	11369	11377
11401	11458	11513	11523	11539	11571	11577	11635	11641	11659
11713	11715	11753	11778	11811	11819	11914	11978	12035	12121
12155	12161	12185	12209	12241	12257	12259	12306	12331	12361
12369	12378	12426	12435	12505	12513	12545	12570	12595	12603
12673	12682	12706	12747	12761	12785	12809	12833	12859	12889
12898	12929	12930	12937	12962	12986	12994	13019	13065	13114
13154	13169	13179	13195	13202	13210	13242	13251	13258	13299
13323	13345	13346	13362	13363	13369	13395	13441	13442	13513
13515	13531	13539	13546	13561	13585	13593	13601	13610	13634
13706	13715	13746	13785	13795	13801	13826	13841	13890	13921
13930	14003	14035	14089	14091	14114	14154	14170	14186	14209
14273	14281	14289	14321	14322	14385	14393	14394	14442	14449
14529	14531	14539	14554	14593	14603	14610	14649	14658	14705
14722	14763	14794	14818	14835	14890	14915	14929	14938	14946
14978	15035	15067	15073	15074	15105	15106	15169	15170	15185
15249	15258	15266	15281	15347	15361	15371	15378	15395	15449
15465	15481	15499	15515	15546	15569	15585	15617	15626	15635
15665	15699	15721	15737	15738	15753	15761	15763	15770	15771
15785	15811	15833	15834	15841	15857	15946	15977	16034	16043
16057	16089	16107	16147	16153	16154	16162	16185	16195	16226
16241	16259	16346	16347	16378	16385	16409	16417	16419	16426
16465	16482	16505	16530	16531	16539	16610	16666	16673	16674
16705	16714	16761	16771	16786	16795	16827	16835	16882	16898
16907	16913	16985	17009	17017	17059	17067	17113	17114	17121
17202	17227	17259	17266	17283	17290	17355	17401	17402	17418
17435	17458	17459	17473	17474	17490	17498	17506	17521	17561
17570	17641	17731	17753	17754	17777	17794	17795	17803	17810
17841	17843	17906	17953	17963	17985	18010	18034	18042	18051
18154	18161	18219	18265	18290	18299	18330	18354	18363	18377
18403	18410	18465	18497	18506	18507	18530	18546	18561	18562
18595	18618	18705	18715	18722	18746	18753	18761	18833	18849
18907	18921	18938	18970	18995	19065	19106	19146	19147	19194
19195	19273	19298	19329	19401	19402	19537	19561	19569	19610

19619	19642	19714	19721	19762	19778	19810	19866	19873	19939
19947	19995	20001	20002	20009	20026	20033	20066	20105	20113
20130	20131	20137	20155	20162					

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer: Notes on elliptic curves. I. II. J. Reine Angew. Math., **212**, 7–25 (1963); **218**, 79–108 (1965).
[2] J. S. Chahal: Topics in Number Theory. Plenum (1988).
[3] J. Coates and A. Wiles: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math., **39**, 223–251 (1977).
[4] J. E. Cremona: Algorithms for Modular Elliptic Curves. Cambridge (1992).
[5] H. Gross and D. Zagier: Points de Heegner et dérivées de fonctions L. C. R. Acad. Sc. Paris, **297**, 85–87 (1983).
[6] N. Koblitz: Introduction to Elliptic Curves and Modular Forms. Springer-Verlag (1984).
[7] K. Noda and H. Wada: All congruent numbers less than 10000. Proc. Japan Acad., **69**A, 175–178 (1993).
[8] K. Rubin: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. Invent. Math., **89**, 527–559 (1987).
[9] M. Taira: On the structure of the Model-Weil group $E(\mathbf{Q})$. Master's Thesis (1994) (in Japanese).