NUMERICAL INVESTIGATIONS RELATED TO THE L-SERIES OF CERTAIN ELLIPTIC CURVES

by

D. Zagier and G. Kramarz

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

Germany

MPI/87-18

Numerical investigations related to the L-series of certain elliptic curves

by D. Zagier and G. Kramarz

According to the theorem of Mordell, the set of rational solutions $E(\mathbb{Q})$ of an elliptic curve E over the rational numbers is a finitely generated abelian group. The rank of this group is called the rank of the elliptic curve and is the basic invariant of E; it is positive if and only if the equation defining E has infinitely many rational solutions.

The common opinion among specialists, based on both numerical experience and heuristic considerations, seems to be that half of all elliptic curves have rank 0 and half rank 1, with higher ranks occurring asymptotically for only 0% of all curves (with respect to any natural ordering). More precisely, the Birch - Swinnerton-Dyer (BSD) conjecture says that the rank of an elliptic curve should equal the order of vanishing of the associated L-series at $s = 1$ and hence should be even or odd according to the sign of the functional equation of this L-series; this sign is + or - with equal frequencies, and the expectation is that almost all curves have the smallest rank compatible with the predicted parity.

The purpose of this note is to present numerical evidence suggesting that, at least for one family of elliptic curves, this expectation may be wrong. The family in question is the famous one

$$x^3 + y^3 = m \qquad (m \in \mathbb{N},\ m \text{ cubefree}), \tag{1}$$

and the numerical data suggests that of the values of m for which the functional equation has a plus sign almost one-quarter (more precisely: about 23.3%) have rank 2 or greater. In fact, it seems that odd ranks ≥ 3 also occur with a positive density (about 2.2% of the curves with odd rank), giving the distribution shown in the "pie-chart" of Figure 1.

To obtain this conclusion we computed the value of the L-series of the elliptic curve (1) for all $m \leq 70000$ (thus we are tacitly assuming the BSD

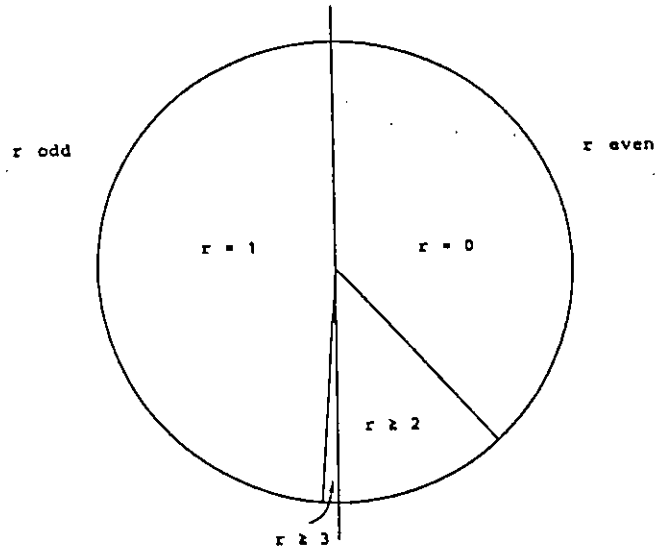

Fig. 1: Empirical distribution of r, the rank of the elliptic curve $x^3+y^3=m$

conjecture, or at least its consequence $L(1) = 0 \Rightarrow \text{rank} > 0$; the reverse implication follows from a theorem of Coates and Wiles). This value is the product of a known real number with a certain integer S which is conjecturally always a square (namely 0 if the rank of E is positive and the order of the Tate-Shafarevich group of E if the rank is 0). This was always true in the range studied, and we will also give tables and graphs on the distribution of S and compare these with heuristic expectations.

§1. The elliptic curves $x^3+y^3=m$ and their L-series

We first make some general remarks about the curves (1). The problem of representing a number as a sum of two rational cubes is a very classical one: Dickson lists 50 papers on the subject before 1918 in his History of the Theory of Numbers, and there has been a comparable amount of work since. We mention in particular the work of Cassels [2] and Selmer [9,10] in which the method of descent is pushed far enough to prove the insolubility of (1) or exhibit a solution (sometimes very large) for all $m < 500$, and the very recent paper of Satgé [8] showing that (1) is always soluble for $m = 2p$, $p \equiv 2 \pmod 9$ or $m = 2p^2$, $p \equiv 5 \pmod 9$, p prime. We have the following equivalent statements about a number m:

(i) m is a sum of two cubes;

(ii) m is a product of three rational numbers with sum 0;

(iii) $-432\,m^2$ can be expressed as a square minus a cube;

(iv) $16m^2$ can be so expressed.

(Here "square" and "cube" mean square or cube of a rational number.) Indeed, if $m = x^3+y^3$ then m is the product of $\frac{m}{xy}$, $\frac{-x^2}{y}$, and $\frac{-y^2}{x}$ which have sum 0; if m is the product of three numbers a, b, c with sum 0 then the formula for the discriminant of the cubic polynomial $x^3 + (ab+ac+bc)x - m$ with roots a, b, c expresses $-432m^2$ as a square minus a cube; if $-432m^2$ equals y^2-x^3 then m is the sum of the cubes of $(36m+y)/6x$ and $(36m-y)/6x$; and finally (ii) and (iv) are equivalent because $m = ab(-a-b)$ can be rewritten $(-4m/a)^3 = (4m(1+2b/a))^2 - 16m^2$. In a more mathematical language, the equivalence of (i) and (ii) says that the elliptic curve E defined by (1) has a solution if any of the curves

$$(2) \qquad m_1x^3 + m_2y^3 + m_3z^3 = 0 \qquad (m_1, m_2, m_3 \in \mathbb{N},\ m_1m_2m_3 = m)$$

do, and comes from the fact that E is the Jacobian of each of the genus 1 curves (2); the equivalence of (ii) and (iii) says that the Weierstrass form of E is

$$(3) \qquad y^2 = x^3 - 432m^2$$

(or $y^2 = 4x^3 - 27m^2$, according to taste); and the equivalence of (iii) and (iv) comes from the fact that E is 3-isogenous to the curve

$$(4) \qquad y^2 = x^3 + 16m^2 .$$

The curve E has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$ and hence is modular, i.e. its L-series is the L-function of a modular form of weight 2 and in particular is entire and satisfies the functional equation

$$(5) \qquad (2\pi)^{-s} N^s \Gamma(s) L(s) = \varepsilon (2\pi)^{-2+s} N^{2-s} \Gamma(2-s) L(2-s)$$

for some integers $N > 0$ (conductor) and $\varepsilon = \pm 1$ (root number). We will give formulas for N and ε below.

The BSD conjecture gives the criterion

(6) Eq. (1) has a solution $\overset{?}{\Leftrightarrow}$ $L(1) = 0$.

The implication "$\Rightarrow$" is a consequence of the famous theorem of Coates and Wiles [3]. The reverse implication is conjectural. Since our concerns are heuristic anyway, we will simply assume it in this paper. Actually, it would not be hard to check this implication for $m \leq 20000$, using the numerical results of this paper, since if the sign of the functional equation is -1 and $L'(1)$ (which we have computed in this range) does not vanish, the main theorem of [6] implies that (1) has a non-trivial solution, and in all other cases the rank of E (unless the BSD conjecture is wrong!) is at least 2 and we would presumably quickly find a small integral solution of one of the equations (2) by direct search. (A similar method was used in [7] to check the validity of the analogue of (6) for the problem of "congruent numbers.")

The BSD conjecture gives more than (6), e.g., that the parity of r (the rank of E) is given by $(-1)^r = \varepsilon$ and that $r = 1$ if and only if $\varepsilon = -1$ and $L'(1) \neq 0$. Moreover, for $L(1)$ it gives the formula

$$L(1) = c \cdot \Omega \cdot \frac{S}{T} \tag{7}$$

where c is a certain positive integer coming from the primes of bad reduction of E, Ω is the basic real period, T is the square of the order of the torsion subgroup of $E(\mathbb{Q})$, and S is an integer given by

$$S = \begin{cases} 0 & \text{if } r > 0, \\ |Ш| & \text{if } r = 0, \end{cases} \tag{8}$$

where $Ш$ denotes the Tate-Shafarevich group. All of these invariants except S are computable. Specifically, the invariants N, ε, c and Δ (the discriminant of a minimal model for E over $\mathbb{Z}$) are given by

$$N = \prod_p N_p, \quad \varepsilon = \prod_p \varepsilon_p, \quad c = \prod_p c_p, \quad \Delta = \prod_p \Delta_p,$$

where the products are taken over all primes p and the factors are given by

	$p \equiv \pm 1 \pmod 3$			$p = 3$				
	$p \nmid m$	$p \| m$	$p^2 \| m$	$m \underset{9}{\equiv} \pm 1$	$m \underset{9}{\equiv} \pm 2$	$m \underset{9}{\equiv} \pm 4$	$3 \| m$	$3^2 \| m$
N_p	1	p^2		3^3	3^2	3^3	3^5	
ε_p	1	± 1		1	-1	-1	1	-1
c_p	1	2 ± 1		3	2	1	1	
Δ_p	1	p^4	p^8	3^9			3^{13}	3^5
type	I	IV	IV*	IV*	III*	IV*	II*	II

Table 1. Multiplicative invariants of the elliptic curve E

Table 1 (all of whose entries, except the value of ε_p, are taken from Tate [11]; the "type" is the Kodaira symbol of the local fiber as given in [11]), while Ω and T are given by

$$(9) \qquad \Omega = \frac{\Gamma(\frac{1}{3})^3}{2\pi\sqrt{3}} \cdot \begin{cases} m^{-\frac{1}{3}} & \text{if } 9 \nmid m \\ 3m^{-\frac{1}{3}} & \text{if } 9 \mid m \end{cases} = \frac{\text{const.}}{|\Delta|^{1/12}}, \qquad T = \begin{cases} 9 & \text{if } m = 1, \\ 4 & \text{if } m = 2, \\ 1 & \text{if } m > 2. \end{cases}$$

The formula (8) for S is not computable. Instead, we will *define* S by equation (7). This is a rational number with bounded denominator by Damerell's theorem [5]. One could doubtless prove that it is in fact always an integer (indeed, this is probably in the literature), but since, again, our aims are only heuristic, we do not do this. Numerically, the value we find always turns out to be an integer, and indeed--as required if (8) is to hold--a perfect square.

To compute S exactly (assuming it is integral), we need to compute the value of $L(1)$ sufficiently accurately to determine S in (7) with an error less than 1. We will also want to calculate the derivative $L'(1)$. The relevant formulas are

$$(10) \qquad L(1) = 2 \sum_{n=1}^{\infty} \frac{a(n)}{n} e^{-2\pi n/\sqrt{N}}$$

and (if $\varepsilon = -1$)

$$(11) \qquad L'(1) = 2 \sum_{n=1}^{\infty} \frac{a(n)}{n} G(2\pi n/\sqrt{N}),$$

where $a(n)$ are the coefficients of $L(s)$ and $G(x)$ the exponential integral

function (cf. [1]). Thus we need about $O(\sqrt{N})$ coefficients $a(n)$ to achieve a reasonable accuracy for $L(1)$ or $L'(1)$. Since, by Table 1, N can be as large as $27m^2$, and our m will run up to 70000, we need $\sim 10^5$ terms for each of $\sim 10^5$ L-series. Hence it is imperative to have a fast algorithm to calculate the $a(n)$. Luckily, the complex multiplication on $E = E_m$ and the fact that all the E_m are (cubic) "twists" of a fixed curve E_1 gives such a method. Namely, we have (putting a subscript on $L(s)$ and $a(n)$ to indicate the dependence on m)

$$L_m(s) = \prod_{\substack{p \text{ prime} \\ p \nmid 3m}} \frac{1}{1 - a_m(p)\, p^{-s} + p^{1-2s}}$$

where, for all m, $a_m(p)$ (if $p \equiv 1 \pmod 3$ and $p \nmid m$; otherwise $a_m(p) = 0$) is one of the three elements of the set

$$A_p = \{ a \mid a \equiv 2 \pmod 3,\ a^2 + 3b^2 = 4p \text{ for some } b \in \mathbb{Z} \}, \tag{12}$$

which one depending only on the cube root of unity $m^{\frac{p-1}{3}} \pmod p$. Specifically,

$$p \equiv 1 \pmod 3,\ p \nmid m \ \Rightarrow\ a_m(p) \equiv m^{\frac{p-1}{3}}\, a_1(p) \pmod p,\ |a_m(p)| < 2\sqrt{p}, \tag{13}$$

where $a_1(p)$ is the unique element $a \in A_p$ satisfying $a^2+3b^2=4p$ with $3 \mid b$. This determines $a_m(p)$ completely (unless $p = 7$, in which case one must choose $a_m(7)$ to lie in $A_7 = \{-1,-4,5\}$). Thus our algorithm proceeds in two stages: in a preliminary computation we compute and store, for each $n \equiv 1 \pmod 6$ up to some limit, the smallest prime factor p of n if n is composite and the (unique) solution $a = a_1(p)$ of $a^2 + 27\square = 4p$, $a \equiv 2 \pmod 3$, if $n = p \equiv 1 \pmod 3$ is prime; then for each curve E_m we compute $a(n) = a_m(n)$ by (13) if $n = p \equiv 1 \pmod 3$ and by

$$a(n) = a(p)a(n/p) + \begin{cases} p\, a(n/p^2) & \text{if } p^2 \mid n,\ p \nmid 3m, \\ 0 & \text{otherwise.} \end{cases}$$

if n is composite. In this way $a(n)$ is calculated in $O(1)$ steps if n is not prime and $O(\log n)$ steps if n is prime, i.e. an average of $O(1)$ steps for each n. (The value of $m^{(p-1)/3} \pmod p$ can be determined in $O(\log p)$ steps by the standard binary algorithm. If $p \equiv 2 \pmod 3$, then $a_m(p) = 0$ for all p.)

§2. The numerical data

We calculated the value of $S = S_m$, and hence of $L(1)$, for all cubefree $m \leq 70000$ with sign of the functional equation $\varepsilon_m = 1$, by the method explained in §1. In the preliminary computation, the values of $a_1(p)$ were calculated and stored for all $p < 960000$; then $L(1)$ was computed by summing the series in (10) to various limits of the order of $\sqrt{N}$ until three successive sums led to a value of S in (7) satisfying either $|S| < 0.023$ or $|\sqrt{S} - s| < 0.08$ for some positive integer s. The beginning of the table (up to $m = 1000$) is reproduced in Table 2; here m has been tabulated as $m_1 + m_2$ with $25 | m_1$ and $1 \leq m_2 \leq 25$, and the entry for m is "K" if m has a cubic factor >1, "-" if the sign of the functional equation of E_m is -1, and $\sqrt{S_m}$ otherwise.

The full table is too long to be given here; instead, we give statistical data

m_1 \ m_2	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	N_+	N_0
0	1	1	1	1	1	-	-	K	-	1	1	-	-	1	-	K	-	1	0	-	1	-	1	K	1	13	1
25	-	K	-	1	0	-	K	-	-	-	1	0	1	1	K	2	-	-	1	1	1	1	K	-	-	24	3
50	-	1	-	K	1	K	1	-	2	3	-	-	-	K	0	3	-	-	-	-	-	K	1	1	-	33	4
75	1	1	-	-	K	K	1	1	-	-	0	-	K	-	-	0	-	1	-	1	K	-	-	1	1	43	6
100	2	3	-	K	-	-	-	K	1	0	1	K	1	-	-	2	-	1	1	K	1	2	-	0	K	55	8
125	0	0	K	2	-	2	0	-	-	K	K	2	3	-	-	-	-	-	K	1	1	1	1	1	3	68	11
150	-	K	0	1	1	-	-	2	-	K	-	K	0	-	3	-	1	K	-	-	-	-	1	3	1	78	13
175	K	-	-	-	-	1	0	0	K	2	-	-	1	K	1	1	K	-	1	-	1	-	-	1	K	88	15
200	0	-	0	3	-	-	2	K	0	0	-	-	-	-	-	K	0	0	0	3	1	-	-	K	1	100	22
225	2	1	-	-	3	-	K	-	1	2	-	1	-	1	K	-	2	K	-	1	0	-	K	-	K	110	23
250	-	1	1	0	3	K	1	-	-	1	1	2	2	K	-	1	-	1	-	K	0	K	0	-	-	123	26
275	3	-	-	-	K	1	0	-	-	-	-	-	K	-	3	1	1	1	-	-	K	K	2	1	3	133	27
300	-	2	-	K	-	-	1	-	0	-	2	K	-	-	1	-	1	3	-	K	-	-	-	K	-	140	28
325	2	1	K	1	-	-	2	-	1	0	K	-	1	-	3	-	0	K	K	0	-	2	0	-	1	153	32
350	K	K	2	3	-	-	-	-	-	K	1	1	-	1	1	-	-	K	1	0	1	-	-	3	K	163	33
375	K	-	K	0	-	2	-	2	K	-	-	-	-	2	0	-	K	-	-	-	-	0	1	0	K	171	37
400	2	-	-	1	K	1	0	K	-	3	-	1	-	-	1	K	2	-	1	0	-	-	2	K	-	182	39
425	3	-	-	-	-	-	K	0	1	0	0	2	-	-	K	-	1	2	-	-	0	-	K	-	-	191	43
450	1	-	0	-	1	K	-	-	K	-	1	0	-	K	-	-	-	0	0	3	1	K	3	-	1	202	47
475	1	0	1	1	K	-	1	-	-	-	K	1	K	2	-	4	3	-	-	-	K	0	0	-	K	213	50
500	-	-	-	K	1	0	2	3	2	-	-	K	K	1	2	-	-	1	-	K	-	-	0	-	-	222	52
525	-	1	K	2	-	1	-	1	3	-	K	-	-	-	K	1	1	2	K	2	-	-	2	-	-	232	52
550	1	K	-	0	-	2	-	1	0	K	3	-	2	3	-	-	K	K	2	3	-	-	-	-	1	243	54
575	K	1	-	0	3	0	-	-	K	1	2	1	-	-	0	-	K	-	K	1	-	1	-	5	K	254	57
600	-	-	-	-	-	-	6	-	K	-	-	-	-	1	0	0	K	2	-	-	1	K	1	1	K	K	262	59
625	1	-	0	-	-	0	K	1	-	0	3	-	-	0	K	2	3	-	-	-	-	-	-	K	1	-	272	63
650	0	1	1	-	-	K	-	0	1	-	-	4	-	K	-	1	1	-	1	-	0	K	-	-	K	282	66
675	-	2	3	-	K	-	-	-	1	1	K	1	K	3	-	-	2	1	2	1	K	-	1	-	-	293	66
700	-	K	1	K	3	-	1	3	-	-	-	K	0	0	-	-	-	-	-	-	K	0	1	1	2	-	303	69
725	3	-	K	K	0	1	-	-	1	-	K	-	-	2	-	1	-	1	K	-	-	1	-	1	K	312	70
750	-	K	-	-	-	K	1	1	3	K	1	-	-	1	-	4	1	K	-	3	-	1	-	1	-	322	70
775	K	1	-	1	3	-	-	K	K	1	0	-	-	-	-	-	K	0	0	6	2	1	-	-	K	332	73
800	3	1	1	-	-	1	-	K	-	K	1	-	0	-	3	K	-	-	-	-	-	1	3	-	K	0	342	75
825	-	-	-	0	3	1	K	2	-	-	1	K	1	2	K	2	2	-	2	-	-	-	K	1	6	354	76
850	0	3	-	-	0	K	4	3	-	-	-	-	-	K	1	0	-	1	1	-	-	K	-	0	K	364	80
875	-	-	3	-	K	-	1	0	-	0	-	1	K	-	-	K	-	1	3	-	K	-	-	-	-	371	82
900	0	3	0	K	0	-	-	1	2	1	1	K	-	3	-	0	-	K	0	K	3	-	1	0	1	386	88
925	-	-	K	1	0	-	-	-	-	-	-	K	0	1	2	0	2	-	-	K	K	0	1	-	-	-	395	92
950	-	K	-	-	2	-	0	-	1	K	-	-	3	-	1	0	-	K	-	-	-	K	0	2	-	403	95
975	K	2	-	-	1	-	1	4	K	-	3	-	0	-	3	2	K	1	-	0	3	-	-	K	K	414	97

Table 2. Values of $S_m^{\frac{1}{2}}$ for cubefree $m \leq 1000$ with $\varepsilon_m = 1$

x	N_+	N_0	N_1	N_4	N_9	N_{16}	N_{25}	N_{36}	N_{49}	N_{64}	N_{81}	N_{100}	N_{144}	other
50	24	3	20	1										
100	43	6	33	2	2									
150	68	11	44	8	5									
200	88	15	56	10	7									
250	110	23	63	14	10									
300	133	27	75	17	14									
350	153	32	83	22	16									
400	171	37	90	26	18									
450	191	43	97	31	20									
500	213	50	107	32	23	1								
600	254	57	123	43	29	1	1							
700	293	66	142	48	33	2	1	1						
800	332	73	163	51	39	3	1	2						
900	371	82	178	56	47	4	1	3						
1000	414	97	191	63	54	5	1	3						
1500	622	142	278	99	84	10	2	7						
2000	835	193	354	137	119	19	2	10			1			
2500	1044	243	429	181	144	23	3	18	1		2			
3000	1251	289	503	216	175	30	8	25	2		3			
3500	1453	336	576	257	200	33	10	33	3	1	4			
4000	1668	389	650	292	238	37	14	39	3	1	5			
4500	1872	430	718	325	281	46	19	42	3	1	7			
5000	2084	481	792	354	318	56	23	48	3	1	8			
6000	2499	586	921	416	391	73	32	64	4	2	9		1	
7000	2910	687	1043	485	473	91	38	70	5	2	13		3	
8000	3324	786	1161	556	549	112	48	84	6	2	13		7	
9000	3741	886	1283	647	608	130	52	97	7	4	19		8	
10000	4161	1001	1401	714	678	147	58	114	11	5	23	1	8	
15000	6243	1498	1999	1050	1049	233	114	195	24	12	47	3	17	2
20000	8319	1972	2564	1419	1407	329	162	286	33	25	79	7	29	7
30000	12478	2953	3661	2111	2126	539	262	491	65	47	130	11	57	25
40000	16620	3896	4730	2770	2852	746	371	729	101	74	201	17	85	48
50000	20793	4880	5698	3471	3596	952	478	996	144	112	264	25	110	67
60000	24935	5842	6684	4127	4302	1186	598	1253	195	143	336	37	136	96
70000	29105	6778	7657	4802	5027	1411	711	1523	240	180	414	52	175	135

x	N_{121}	N_{169}	N_{196}	N_{225}	N_{256}	N_{289}	N_{324}	N_{361}	N_{400}	N_{441}
15000				2						
20000	2			5						
30000	4	3	2	12			4			
40000	8	5	3	20	2	1	9			
50000	15	5	4	26	2	1	11	1		2
60000	19	6	6	34	2	1	24	1		3
70000	26	11	8	48	3	1	32	2	0	4

Table 3. Values of $N_+(x)$ and $N_S(x)$ for $x \leq 70000$

in terms of the functions

$$N_+(x) = \#\{1 \leq m \leq x \mid m \text{ cubefree}, \varepsilon_m = +1\},$$

$$N_S(x) = \#\{1 \leq m \leq x \mid m \text{ cubefree}, \varepsilon_m = +1, S_m = S\} \quad (S \in \mathbb{Z}).$$

The values of these functions for selected $x \leq 70000$ and all S are given in Table 3. Obviously, $N_+ = \sum N_S$, where S a priori ranges over the integers but actually (on BSD or in the range of our computations) only over perfect squares; in fact, S takes on only the values $0, 1^2, \ldots, 10^2, 12^2$ for $m \leq 10000$ and $0, 1^2, \ldots, 19^2, 21^2$ for $m \leq 70000$. Graphical representations of $N_S(x)$ as a

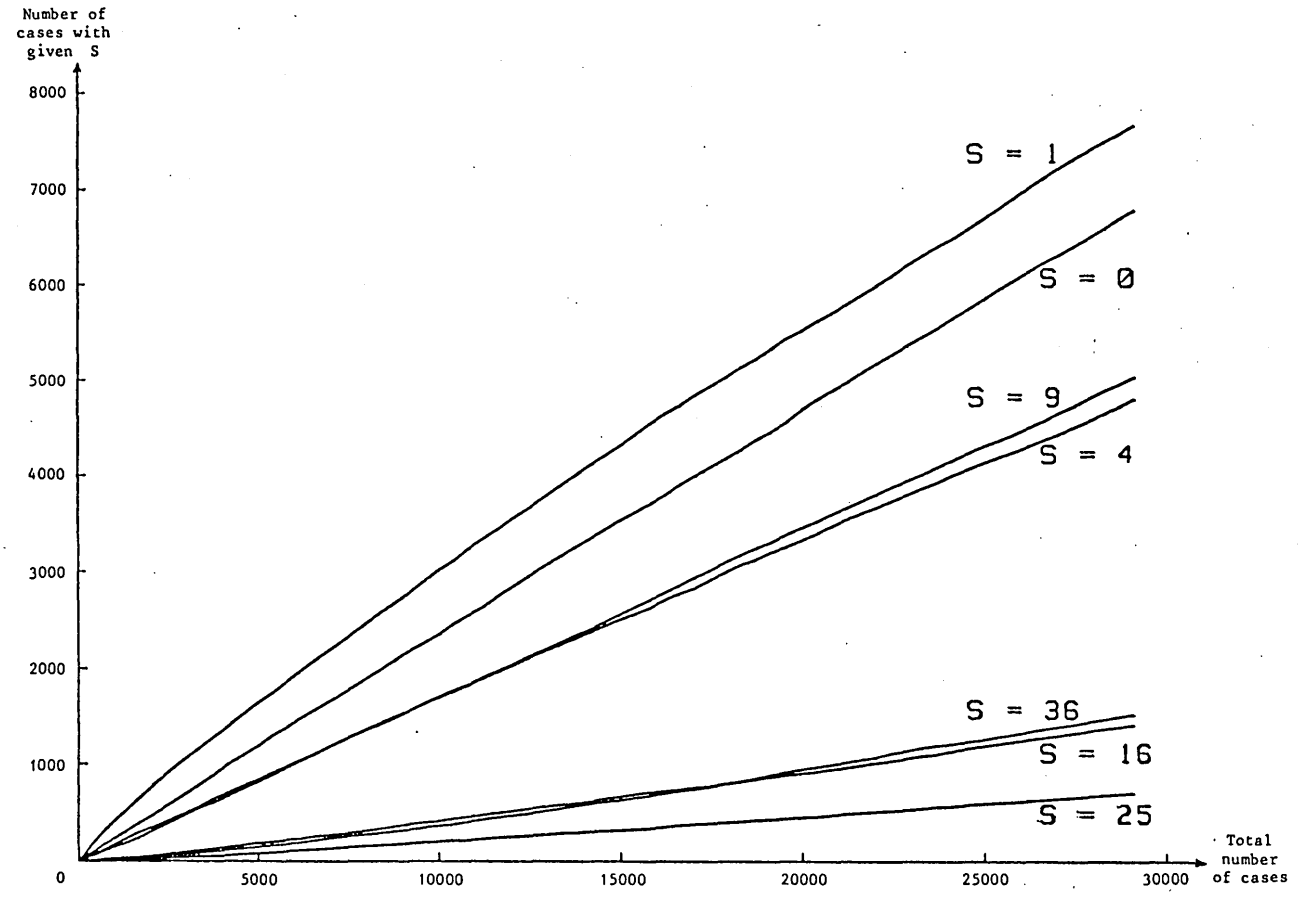

Figure 2. Number of curves with $S_m = 0, 1^2, \ldots, 6^2$ for $m \leq 70000$

function of $N_+(x)$ for $x \leq 70000$ and $\sqrt{S} \leq 6$ are given in Figure 2. The most interesting numbers for us are the quotients $N_S(x)/N_+(x)$. Since their sum is 1, they can be conveniently represented on a single graph as in Figure 3. The most

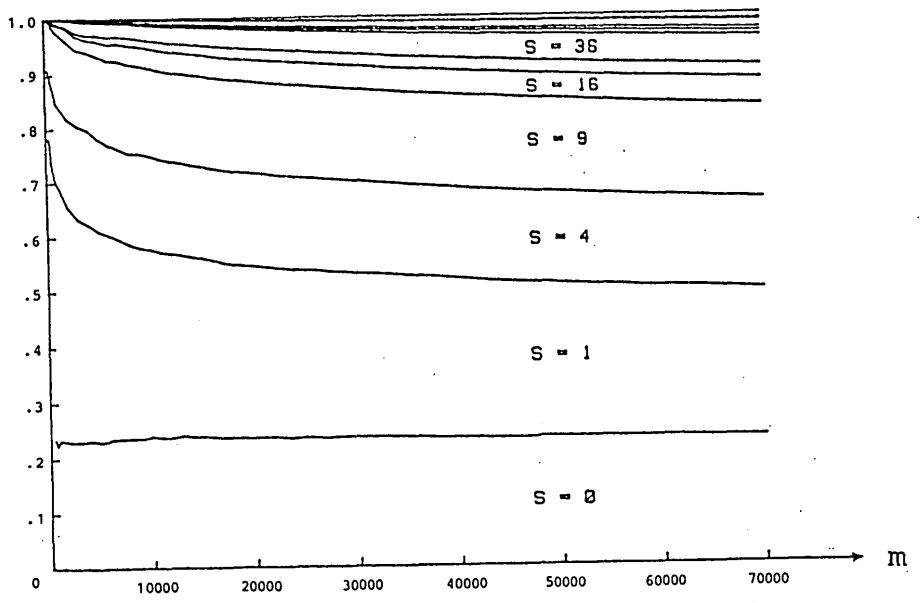

Figure 3. Frequencies of various values of S_m for $m \leq 70000$

striking feature of Figures 2 and 3 is the near constancy of $N_0(x)/N_+(x)$, which can be seen numerically in the following mini-table:

x	500	1000	2000	5000	10000	20000	30000	50000	70000
$N_0(x)/N_+(x)$	0.235	0.234	0.231	0.231	0.241	0.237	0.237	0.235	0.233

This is the phenomenon which was mentioned in the introduction and which is the main empirical result of the paper.

Figure 2 also suggests at first glance that the other $N_S(x)$ are roughly proportional to $N_+(x)$, but from Figure 3 it is clear that, for instance, $N_1(x)/N_+(x)$ is decreasing as x grows. To decide whether $N_1(x)/N_+(x)$ has a positive limit or tends to zero as $x \to \infty$ is difficult on the basis of these two graphs, since we have to visually extrapolate slowly falling curves out to infinity. In Figure 4 we have graphed the function $x \mapsto y = N_1(x)/N_+(x)$ with a change of coordinates $x \to x^{-1/3}$, $y \to y^2$ which pulls infinity to the origin and exaggerates the variation of y. This picture seems to suggest that in fact $N_1(x)/N_+(x)$, unlike $N_0(x)/N_+(x)$, tends to zero as $x \to \infty$. (We discuss this more in §3.)

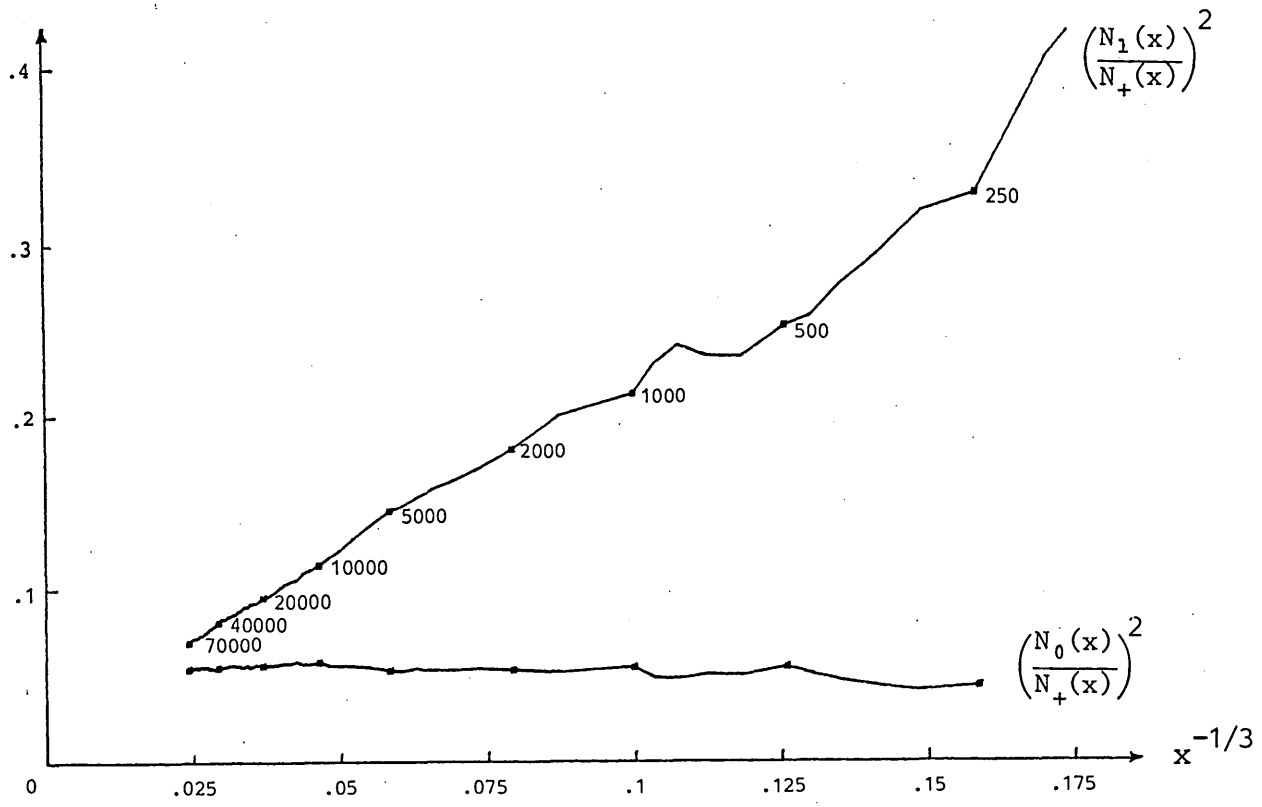

Figure 4. Rescaled graph of the frequencies of $S = 0$ and $S = 1$

Finally, we also calculated $L'(1)$ for all elliptic curves (1) with $m \leqq 20000$ and $\varepsilon_m = -1$. Here there is no closed formula like (7). However, $L'(1)$ is given not only by (11) but by the formula

$$(14) \qquad L'(1) = \sum_{n=1}^{\infty} \frac{a(n)}{n} \left[G(2\pi A/\sqrt{N}) + G(2\pi/A\sqrt{N}) \right]$$

for any $A > 0$, so to estimate the speed of convergence we computed $L'(1)$ using both (11) and (14) with $A = 2$; the results agreed to about 5 digits after the decimal, providing a check on the computation. The values obtained were either quite far from zero (usually in the range from about 1 to 30) or else equal to zero to 5 or 6 decimals, so that we could identify the curves with $L'(1) = 0$ (and hence conjecturally $r \geqq 3$) with confidence. Table 4 gives the first few values of $L'(1)$ and a few in the neighborhood of $m = 657$, the

$m = 6$	$L'(1) = 2.376185$	$m = 647$	$L'(1) = 11.840825$
$m = 7$	$L'(1) = 1.651771$	$m = 650$	$L'(1) = 6.073495$
$m = 9$	$L'(1) = 1.290191$	$m = 654$	$L'(1) = 7.193217$
$m = 12$	$L'(1) = 2.314463$	$m = 655$	$L'(1) = 13.692513$
$m = 13$	$L'(1) = 2.953426$	$m = 657$	$L'(1) = 0.000001$
$m = 15$	$L'(1) = 3.160715$	$m = 660$	$L'(1) = 10.313723$
$m = 17$	$L'(1) = 3.972532$	$m = 661$	$L'(1) = 14.565052$
$m = 20$	$L'(1) = 2.317275$	$m = 663$	$L'(1) = 5.183534$
$m = 22$	$L'(1) = 4.318084$	$m = 665$	$L'(1) = 8.093288$

Table 4. Some values of $L'(1)$

first zero.

The first values of m with $L'(1) = 0$ were $m = 657, 854, 1020, 1122, 1241, 1267, 1330, 1339, 1426, 1482, 1554, 1798, 1853, 1892$. (Selmer [9] already mentions $m = 657$ as being the first case where E_m has rank 3.) Altogether we found 179 curves with $L'(1) = 0$ among the 8320 curves with odd functional equation in the range $m \leqq 20000$. Figure 5 gives a graph of

$$N_-^0(x) = \#\{ 1 \leqq m \leqq x \mid m \text{ cubefree}, \ \varepsilon_m = -1, \ L_m'(1) = 0 \}$$

as a function of $N_-(x)$ (defined like N_+ but with $\varepsilon = -1$) in this range, suggesting that the ratio $N_-^0(x)/N_-(x)$ is in fact fairly constant near

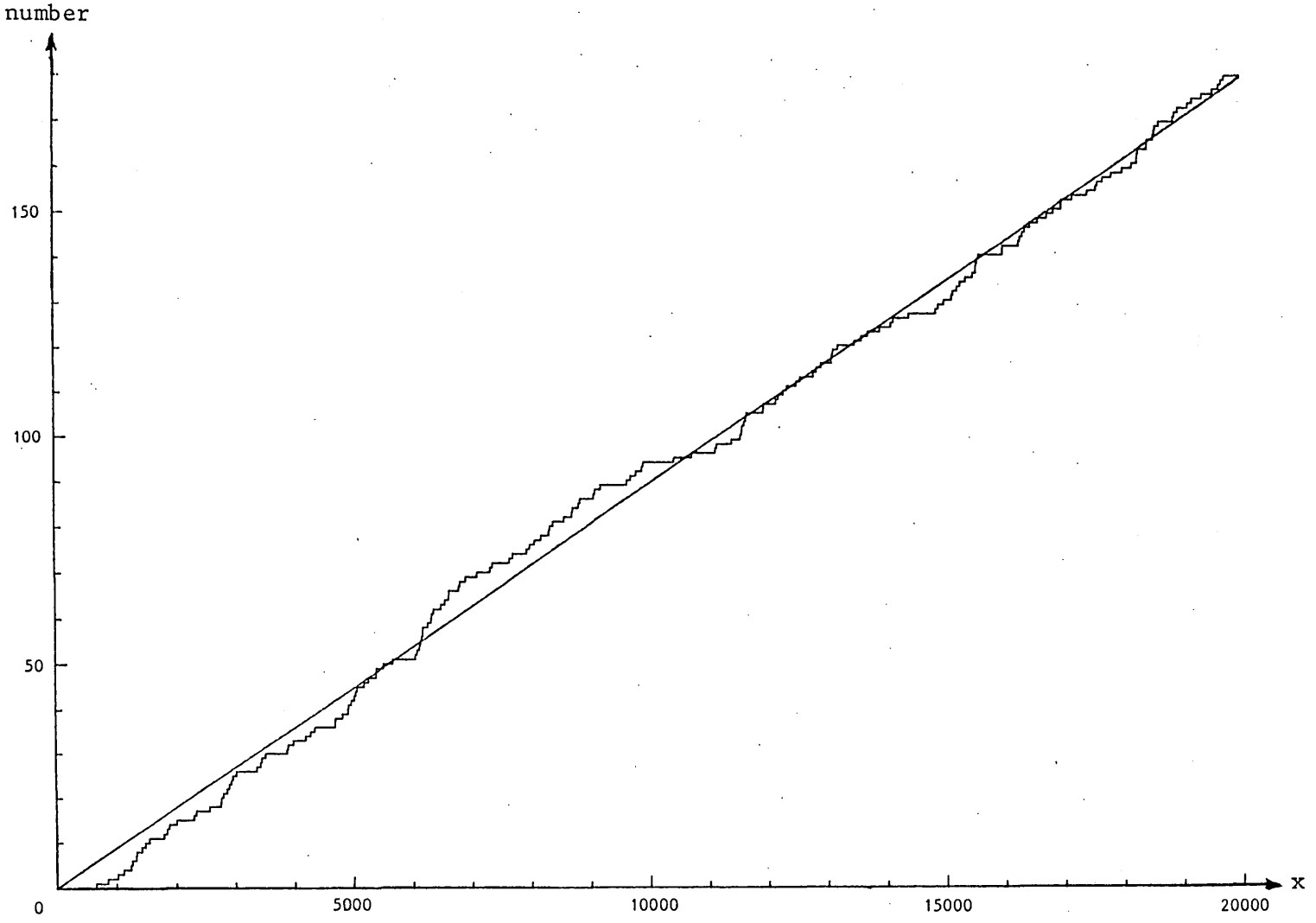

Figure 5. Number of $m \leqq x$ with $\operatorname{ord}_{s=1} L_m(s)$ odd and $\geqq 3$

$\frac{179}{8320} = 2.15\,\%$, as already indicated in Figure 1.

§3. Discussion

To conclude this paper we discuss some questions concerning the curves (1) which are suggested by our numerical investigations.

1. Can one give a closed form for S_m?

This is certainly the most interesting question one can ask about the curves E_m; answering it would require a deep understanding of the L-series and would give an at least conjectural answer to the question, which numbers are sums of two cubes.

As already mentioned, the curves E_m are all cubic twists of a fixed curve E_1 (i.e., E_m becomes isomorphic to E_1 over $\mathbb{Q}(\sqrt[3]{m})$). For the similar situation of quadratic twists, Waldspurger's theorem [13] gives an answer: it says that the

numbers S_m defined by the analogue of (7) for a quadratic twist of a fixed elliptic curve by $\mathbb{Q}(\sqrt{m})$ is the square of the m^{th} coefficient of a certain modular form of weight 3/2 (at least if the elliptic curve being twisted is a modular one). For instance, for the classical problem of congruent numbers ($y^2 = x^3 - m^2x$, m squarefree) it gives the formula

$$(15) \qquad S_m = \left(\sum_{a,b,c} (-1)^{c/4} \right)^2 \quad (m \text{ even}) \quad \text{or} \quad \left(\sum_{a,b,c} (-1)^{(b-c)/4} \right)^2 \quad (m \text{ odd}),$$

where the sum is over $(a,b,c) \in \mathbb{Z}^3$ with $a^2 + b^2 + c^2 = m$ and $c \equiv 0 \pmod 4$ or $b \equiv c \pmod 4$, respectively (cf. [12]). One may speculate that in our case, too, S_m is the square of a Fourier coefficient of some type of modular form, perhaps on a 3-fold covering group of GL(2).

2. How convincing is the evidence that $S = 0$ for a positive proportion of the curves (1) with even functional equation?

This is obviously a matter of personal opinion. Formulas (7) and (9) imply (since L(1) is presumably $O(m^{\varepsilon})$ for any $\varepsilon > 0$) that $\sqrt{S_m}$ is roughly $O(m^{1/6})$ (rather than $O(m^{1/4})$ as would be the case for quadratic twists by $\mathbb{Q}(\sqrt{m})$), so the naive expectation is that $\sqrt{S_m}$ would be 0 with a probability of $m^{-1/6}$, giving a frequency $N_0(x)/N_+(x)$ which tends to 0 like $x^{-1/6}$. But Figures 2, 3, and 4 do not seem to be compatible with a rate of decrease anything like as fast as this, and once one has rejected the obvious rate of growth, there seems little reason not to believe the evidence of the tables that $N_0(x)/N_+(x)$ is in fact roughly constant.

3. Does a similar phenomenon (i.e., positive density of curves with rank ≥ 2) occur for other families of curves? If not, what special properties do the curves $x^3 + y^3 = m$ have which can explain their high ranks?

The answer to the first question, at least for the family of quadratic twists of a fixed elliptic curve, seems to be no: we calculated S_m for the family of curves $y^2 = x^3 - m^2x$ associated to the congruent number problem (using (15)) for all $m \equiv 1 \pmod{16}$ up to 500000 and obtained the values

x	1000	2000	5000	10000	20000	50000	100000	200000	500000
$N_0(x)/N_+(x)$	0.227	0.216	0.193	0.172	0.160	0.152	0.139	0.130	0.106

which are clearly decreasing, in contrast with the corresponding values for the curves (1) ("mini-table" in §2). We have no data for other families.

As to the second question, we can offer two tentative suggestions.

(i) As mentioned in §1, E_m is the Jacobian of each of the curves (2). If m is highly composite, then there are many such curves, and if any of them has a rational point, then so does E_m; this tends to make the rank of E_m large. In a related vein, even if none of the curves (2) is known to have a rational point, when there are many of them this will make the 3-Selmer group of E_m big and hence (on BSD) force S_m to be divisible by a large power of 3; for small m this will tend to make S_m (which is trying to be no larger than $O(m^{1/3})$) to vanish. However, although this argument might explain the large frequency of curves with $S = 0$, it does not at all explain why this frequency is so nearly constant.

(ii) A different argument, not too convincing, is the following naive one. Let us guess at the number of solutions of $a^3 + b^3 = mc^3$ in (say, positive) coprime integers a, b, c less than some very large number L for a "random integer" m (whatever that means). For m fixed, the number of positive coprime pairs of integers a, b with $\frac{1}{2}L < \max(a,b) < L$ and $a^3+b^3 \equiv 0 \pmod m$ is $O(L^2)$, and the probability for a given quotient $\frac{a^3+b^3}{m}$ to be a perfect cube is $O(L^{-2})$, so we expect about $O(\log L)$ solutions in the range $\max(a,b) < L$. On the other hand, from height theory it follows that the number of solutions for a *given* m grows like $(\log L)^{r/2}$, where r is the rank of E_m, so this suggests that $r \geq 2$ may occur with a positive density. However, apart from the general vagueness of this argument, it suggests that $r = 2$ is the highest value occurring with positive density, whereas our data seem to suggest that $r \geq 3$ occurs more than 1% of the time.

4. *Are the asymptotic frequencies of other values of* S *also positive, or*

do they tend to zero?

Here the same a priori argument as for $S = 0$ predicts that $N_S(x)/N_+(x)$ for a fixed value of S should tend to zero roughly like $x^{-1/6}$, and now Figure 4 (for $S = 1$) is eminently compatible with this prediction. Since there is no reason to suppose that $S = 1$ behaves differently from other positive values of S, the same presumably holds for them, too. The fact that $N_S(x)/N_+(x)$ for $S = 4$ and $S = 9$ is nearly constant in our range can be explained by observing that the mean value of $\sqrt{S_m}$ is of the order of $m^{1/6}$, which is growing very slowly, so that for m of the order of 50000 the values $\sqrt{S} = 2$ or 3 are at the height of their popularity, while for m around 5000, say, they are still rare because S is usually 0 or 1. Thus we have tendencies to increase and to decrease which in this range roughly compensate; and indeed, for the larger values $\sqrt{S} = 4, 5, 6$ we actually see an increase of $N_S(x)/N_+(x)$ in Figure 3 which will surely eventually be reversed, so that these ratios, too, will be roughly constant over some very long range later on.

It is amusing to note that we can make the statement about $L(1)$ (or, equivalently, $m^{-1/3}S_m$) being of the order of 1 on the average much more precise. Using the exact formulas for $a_m(n)$ given in §1, we find that for fixed n the Fourier coefficient $a_m(n)$ has a well-defined average value $a_{av}(n)$ as m runs over cube-free integers prime to n; these average values are multiplicative and are the coefficients of a Dirichlet series $L_{av}(s) = \sum a_{av}(n)\, n^{-s}$ whose p-Euler factor is 1 for $p = 3$, $(1 + p^{1-2s})^{-1}$ for $p \equiv 2 \pmod 3$, and equal to

$$\frac{1}{3} \sum_{a \in A_p} \frac{1}{1 - ap^{-s} + p^{1-2s}} = \frac{1 - p^{3-6s}}{1 - p^{1-2s}} \cdot \frac{1}{1 - c(p)p^{-3s} + p^{3-6s}}, \quad c(p) = \prod_{a \in A_p} a$$

(A_p as in (12)) for $p \equiv 1 \pmod 3$. The number $c(p)$ is the p^{th} Fourier coefficient of the unique normalized cusp form f of weight 4 on $\Gamma_0(9)$, and we find

$$L_{av}(s) = \frac{L(2s-1,\chi)}{L(6s-3,\chi)} L(f, 3s),$$

where $\chi = (\frac{\cdot}{3})$ is the non-trivial Dirichlet character of conductor 3. In

particular, $L_{av}(s)$ is regular at $s = 1$ with

$$L_{av}(1) = \frac{L(1,\chi)}{L(3,\chi)} L(f,3) = \frac{\pi/3\sqrt{3}}{4\pi^3/81\sqrt{3}} \cdot 2 \sum_{n=1}^{\infty} \frac{c(n)}{n^3} e^{-2\pi n/3} \cong 0.16840248;$$

this presumably gives the average value of $L_m(1)$, taken over all m having no small prime factors.

5. What can one say about the relative frequency of occurrences of $S = 1$, $S = 4$, $S = 9$, *etc.?*

So far, nothing. The only line of attack which seemed promising was to imitate the Cohen-Lenstra heuristics [4] on the behavior of (the odd parts of) class numbers or class groups of imaginary quadratic fields (this is a natural analogy because imaginary quadratic fields have unit rank 0, corresponding to $r = 0$ here), but this led to an answer in complete disagreement with the empirical results. Recall that the idea in [4] was to observe that the non-2-part of the class group of an imaginary quadratic field belongs to the class $\mathcal{G}$ of finite abelian groups of odd order, and to postulate that its probability of being equal to a given group $G \in \mathcal{G}$ is proportional to $|\mathrm{Aut}\, G|^{-1}$. This led to the correct prediction that any given group occurs with density zero (since $\sum_{G \in \mathcal{G}} |\mathrm{Aut}\, G|^{-1}$ diverges) and gave specific, and experimentally confirmed, predictions for the frequencies of various properties of G (e.g., being cyclic, having order divisible by 3, etc.). In our case the analogue of the class group is the Tate-Shafarevich group Ш and it belongs to the class $\mathcal{S}$ of finite abelian groups together with a skew symmetric pairing $Ш \times Ш \to \mathbb{Q}/\mathbb{Z}$. The problem is that such objects are rare and have many automorphisms (for instance, there is only one isomorphism class of order p^2, and its automorphism group has order p^3-p), so that the sum $\sum_{Ш \in \mathcal{S}} |\mathrm{Aut}\, Ш|^{-1}$ *converges*, and indeed converges to a number c not much bigger than 1. (More precisely, $c = \zeta(3)\zeta(5)\zeta(7)\ldots \cong 1.2602057106$.) Thus the analogue of the Cohen-Lenstra heuristics would suggest:

i) that each order $S = |Ш|$ occurs with a positive frequency;

ii) that this frequency for $S = 1$ is $1/c$, or about 79%; and

iii) that the ratios of the frequencies of $S = 1$, $S = 4$, and $S = 9$ are $1 : 1/6 : 1/24$.

The first prediction, though it disagrees with the arguments given in connection with Question 4, is conceivable, but the second two do not agree at all with the data on $S = 1, 4$, and 9 in Figures 2 and 3, so that, at least in its original form, the Cohen-Lenstra recipe seems not to work its magic in our situation.

Bibliography

[1] J. Buhler, B. Gross, D. Zagier: On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. Math. Comp. 44 (1985), 473-481.

[2] J.W.S. Cassels: The rational solutions of the diophantine equation $Y^2 = X^3 - D$. Acta Math. 82 (1950), 243-273.

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

[4] H. Cohen, H.W. Lenstra, jr.: Heuristics on class groups of number fields. In: Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. 1068, pp. 33-62. Springer-Verlag, Berlin and New York, 1984.

[5] R. Damerell: L-functions of elliptic curves with complex multiplication, I, II. Acta Arithm. 17 (1970), 287-301 and 19 (1971), 311-317.

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

[7] G. Kramarz: All congruent numbers less than 2000. Math. Ann. 273 (1986), 337-340.

[8] Ph. Satgé: Un analogue du calcul de Heegner. Invent. Math. 87 (1987), 425-439.

[9] E. Selmer: The diophantine equation $ax^3+by^3+cz^3 = 0$. Acta Math. 85 (1951), 203-362.

[10] E. Selmer: The diophantine equation $ax^3+by^3+cz^3 = 0$. Completion of the tables. Acta Math. 92 (1954), 191-197.

[11] J. Tate: Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular Functions of One Variable IV, Lecture Notes in Math. 476, pp. 33-52. Springer-Verlag, Berline-Heidelberg-New York, 1975.

[12] J. Tunnell: A classical Diophantine problem and modular forms of weight 3/2. Invent. Math. 72 (1983), 323-334.

[13] J.L. Waldspurger: Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. Pures Appl. 60 (1981), 375-484.