Which primes are sums of two cubes?

Fernando Rodriguez Villegas
Don Zagier

Department of Mathematics
Princeton University
Princeton, NJ 08544
USA

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
GERMANY

MPI/95-61

Canadian Mathematical Society Conference Proceedings
Volume 00, 0000

Which primes are sums of two cubes?

FERNANDO RODRIGUEZ VILLEGAS AND DON ZAGIER

ABSTRACT. Let S_p be the "unknown" part of the L-series of the elliptic curve $x^3 + y^3 = p$ at $s = 1$, so that conjecturally $S_p = 0$ if p is a sum of two distinct cubes and equals the order of a Tate–Shafarevich group otherwise. The question of the title is then to determine whether $S_p = 0$. For $p \not\equiv 1 \pmod 9$ the answer depends only on $p \pmod 9$ and is well known. We give three different criteria for the remaining case. Our first formula represents S_p as the trace of a certain algebraic number (the value of a specific modular function at a CM point), the second represents S_p as the square of the trace of a similar number, and the third shows that S_p vanishes if an only if $p | f_{2(p-1)/3}(0)$, where $\{f_n(t)\}_{n \geq 0}$ is a sequence of polynomials satisfying a simple recursion relation.

1. Introduction and results

A classical problem of Diophantine analysis is to recognize which numbers N are the sum of two rational cubes. For instance, 1 is not so represented (Fermat, Euler), whereas every prime of the form $9k - 1$ conjecturally is (Sylvester). If we assume the Birch–Swinnerton-Dyer conjecture, then the question is equivalent to the vanishing at $s = 1$ of the L-series of the elliptic curve $E_N : X^3 + Y^3 = N$.

We consider only the case when $N = p$ is prime. If $p \equiv 2, 3$ or $5 \pmod 9$, then $L(E_p, 1) \neq 0$, so p should not be a sum of two cubes (except for $1^3 + 1^3 = 2$). This is in fact true and follows either from a 3-descent argument (given already in the 19th century by Sylvester, Lucas and Pepin) or from the Coates-Wiles theorem. If $p \equiv 4$, 7 or 8 (mod 9) then the functional equation forces $L(E_p, 1)$ to vanish, so p should be a sum of two cubes, and for the first two of these three cases a proof of this has been announced by Noam Elkies. From now on we restrict to the remaining case $p \equiv 1 \pmod 9$. Here the L-series may or may not vanish. The question is numerically decidable for any given prime, since

$$L(E_p, 1) = \frac{\sqrt{3}\,\Gamma(\frac{1}{3})^3}{2\pi\,\sqrt[3]{p}} S_p,$$

1991 *Mathematics Subject Classification.* 11F67, 11D85, 11G40.

where S_p is known to be an integer (conjecturally equal to 0 if $E_p(\mathbb{Q}) \neq \{0\}$ and to the order of the Tate–Shafarevich group of E_p otherwise), but a table of these numbers, such as the one for $p < 2000$ given at the end of this section, suggests no simple pattern. In this paper we will give three formulas for S_p and hence three conjectural answers to the question of the title. Most of the proofs rely on ideas similar to those in [5] and [7] and have been omitted or only sketched, but, to quote from Sylvester's paper on the same subject [9], "I trust my readers will do me justice to believe that I am in possession of a strict demonstration of all that has been advanced without proof." We do include a few short proofs which use ideas different from those in the two papers cited.

First answer: We associate to the prime $p = 9k+1$ an algebraic number α_p of degree $18k$, defined as follows

$$\alpha_p = \frac{\sqrt[3]{p}}{54}\,\frac{\Theta(p\delta)}{\Theta(\delta)},$$

where $\Theta(z) = \frac{1}{2}\sum_{m,n\in\mathbb{Z}} e^{2\pi i(m^2+mn+n^2)z}$ and $\delta = -\frac{1}{2}(1+1/3\sqrt{-3})$. (The value of $\Theta(\delta)$, by the way, is $-3\Gamma(\frac{1}{3})^3/(2\pi)^2$.) Then

$$S_p = \operatorname{Tr}(\alpha_p),$$

where Tr denotes absolute trace. A more detailed statement is given in Theorem 1 below.

Second answer: This has the same form, but gives the *square root* of S_p as a trace (thus proving, in particular, that S_p is a square, as expected). Of course S_p has two square roots when nonzero. It turns out that they are canonically indexed by the two primes above p in $K = \mathbb{Q}(\sqrt{-3})$. Let $\mathcal{P}$ be one of these primes. Choosing $\mathcal{P}$ is equivalent, via $\mathcal{P} = (p, \frac{-r+\sqrt{-3}}{2})$, to choosing an integer $r \pmod{2p}$ with $r^2 \equiv -3 \pmod{4p}$. Let $z_0 = (r+\sqrt{-3})/2$ and set

$$\beta_{\mathcal{P}} = \frac{\sqrt[6]{p}}{\sqrt{\pm 12}}\,\frac{\eta(pz_0)}{\eta(z_0/p)},$$

where $\eta(z) = e^{\pi i z/12}\prod_{n=1}^{\infty}(1-e^{2\pi i n z})$ is Dedekind's eta function, the sign is $+1$ if $p \equiv 3 \pmod 4$ and -1 if $p \equiv 1 \pmod 4$, and the correct choice of the 6^{th} root of p will be explained later. Then $\beta_{\mathcal{P}}$ is algebraic of degree $6k$ over $\mathbb{Q}$ and we have

$$S_p = [\operatorname{Tr}(\beta_{\mathcal{P}})]^2, \quad \text{and} \quad \operatorname{Tr}(\beta_{\overline{\mathcal{P}}}) = -\operatorname{Tr}(\beta_{\mathcal{P}}).$$

A more detailed statement is given in Theorem 2 below.

Third answer: Define polynomials $f_n(t)$ by $f_0(t) = 1, f_1(t) = t^2$ and

$$f_{n+1}(t) = (1-t^3)\,f_n'(t) + (2n+1)\,t^2 f_n(t) - n^2 t\, f_{n-1}(t) \quad (n \geq 1),$$

and let $A_k = f_{3k}(0)$. (It is trivial that $f_n(0) = 0$ if 3 does not divide n.) Then

$$S_p \equiv (-3)^{\frac{p-10}{3}} (\frac{p-1}{3})!^2 A_{2(p-1)/9} \pmod p.$$

This determines S_p since $|S_p| < p/2$ as we shall prove in §5. In particular, we have

$$L(E_p, 1) = 0 \iff p | A_{2(p-1)/9}.$$

Third answer (variant): In fact, the A_k's of the third answer (which are normalized central values of certain Hecke L-series) are always squares, and we can get their square roots as follows. Define polynomials $g_n(t) \in \mathbf{Q}[t]$ by $g_0(t) = 1$, $g_1(t) = \frac{3}{8}t^2$ and

$$g_{n+1}(t) = (1 - t^3)\, g_n'(t) - (2n + \tfrac{3}{8})\, t^2\, g_n(t) - n(n - \tfrac{1}{2})\, t\, g_{n-1}(t) \quad (n \geq 1),$$

and let $B_k = g_{3k}(0)$. (Just as with f_n, $g_n(0) = 0$ if 3 does not divide n.) Then

$$A_{2k} = B_k^2, \quad \text{for all} \quad k \geq 0$$

and in particular

$$L(E_p, 1) = 0 \iff p | B_{(p-1)/9},$$

and

$$\sqrt{S_p} \equiv \pm(\sqrt{-3})^{\frac{p-10}{3}} (\frac{p-1}{3})!\, B_{(p-1)/9} \pmod p.$$

We conjecture that this formula is always true with the + sign if we interpret $\sqrt{S_p}$ and $\sqrt{-3} \pmod p$ as $\mathrm{Tr}(\beta_{\mathcal{P}})$ and $r \pmod p$, respectively (with r, $\mathcal{P}$, $\beta_{\mathcal{P}}$ as in the second answer), and have checked this for $p < 2000$.

We give a short table of values of the numbers B_k.

k	B_k
0	1
1	−2
2	−152
3	−6848
4	−8103296
5	22483912960
6	−8062284861440
7	1964344440706666240
8	532650564250569441280
9	2039228675045199496806400
10	−5209573728611533514689740800

This also gives the first values of the numbers $A_{2k} = B_k^2$. The odd-index values A_{2k+1}, which are not needed for our "third answer," are also the squares of the constant terms of certain polynomials $c_{3k+1}(t)$ satisfying a recursion (cf. Theorem 3 below, where a short table is given).

The numbers A_k and B_k have a different description in terms of generating functions:

$$F(\tfrac{1}{3}, \tfrac{1}{3}; \tfrac{2}{3}; x) = \sum_{k=0}^{\infty} \frac{A_k}{(3k)!} T^k$$

and

$$(1-x)^{\frac{1}{24}} F(\tfrac{1}{3}, \tfrac{1}{3}; \tfrac{2}{3}; x)^{\frac{1}{2}} = \sum_{k=0}^{\infty} \frac{B_k}{(3k)!} \left(\frac{-T}{2}\right)^k ,$$

where $F = {}_2F_1$ is Gauss's hypergeometric function and

$$T = x \frac{F(\frac{2}{3}, \frac{2}{3}; \frac{4}{3}; x)^3}{F(\frac{1}{3}, \frac{1}{3}; \frac{2}{3}; x)^3} .$$

That the coefficients in the first of these hypergeometric expansions are the squares of the coefficients in the second is a surprising and beautiful identity, quite apart from the connection with L-series.

There are similar results for the number S_{p^2} corresponding to the elliptic curve $E_{p^2} : x^3 + y^3 = p^2$, namely

$$S_{p^2} = \mathrm{Tr}(\gamma_P)^2, \qquad \gamma_P = \frac{\zeta\, p^{\frac{1}{3}}}{\sqrt{12}} \frac{\eta(pz_0)}{\eta(-\bar{z}_0/p)},$$

for a certain root of unity ζ, and

$$S_{p^2} = 0 \quad \Longleftrightarrow \quad p | A_{(p-1)/9} \quad \Longleftrightarrow \quad p | B_{2(p-1)/9}.$$

However in the rest of this note we will stay with S_p.

Using any of the "answers" given in this section, we can easily calculate S_p numerically. We give a table for $p \equiv 1 \pmod 9$, $p < 2000$. In this range, the value of S_p is always 0, 1 or 4, as follows:

$S_p = 0:$	19, 37, 127, 163, 271, 379, 397, 433, 523, 631, 829, 883, 919, 937, 1063, 1171, 1459, 1531, 1567, 1621, 1657, 1801
$S_p = 1:$	73, 109, 181, 199, 307, 487, 541, 577, 613, 757, 811, 1009, 1117, 1153, 1279, 1297, 1423, 1549, 1693, 1783
$S_p = 4:$	739, 991, 1747, 1873, 1999

A complete table of S_N for $N < 1000$ is given in [10].

2. The formulas for S_p

Let $\mathcal{O} = \mathbf{Z}[\omega] \subset K = \mathbf{Q}(\omega) = \mathbf{Q}(\sqrt{-3})$, where $\omega^2 + \omega + 1 = 0, \sqrt{-3} = 2\omega + 1$, and embed K in $\mathbf{C}$ via $\omega \mapsto e^{2\pi i/3}$. The elliptic curve $E : x^3 + y^3 = 1$ has complex multiplication by $\mathcal{O}$. Its L-series is $L(\psi, s)$, where ψ is the Hecke character of K satisfying

$$\psi((\alpha)) = \alpha, \quad \text{for all } \alpha \in \mathcal{O},\ \alpha \equiv 1 \pmod 3).$$

Let $p \equiv 1 \pmod 3$ be a prime. We consider the groups

$$\Delta = (\mathcal{O}/p\mathcal{O})^\star / (\mathbf{Z}/p\mathbf{Z})^\star \quad \text{and} \quad \Delta_0 = \Delta/\mathcal{O}^\star,$$

which are cyclic of orders $p-1$ and $(p-1)/3$ respectively. We let H_{3p} (H_p) be the ring class field modulo $3p$ (modulo p) of K and identify Δ (Δ_0) with $Gal(H_{3p}/K)$ ($Gal(H_p/K)$) via the Artin map.

Let $\chi : \Delta \longrightarrow \langle\omega\rangle$ be the cubic character defined by

$$\chi(u) \equiv \left(\frac{\overline{u}}{u}\right)^{(p-1)/3} \pmod p \qquad (u \in \mathcal{O},\ (u,p)=1).$$

Then $L(\psi\chi, s)$ and $L(\psi\chi^2, s)$ are the L-series of the curves E_p and E_{p^2}, respectively. The sign in their functional equation is $+1$ if and only if $p \equiv 1 \pmod 9$ or, equivalently, if and only if χ factors through Δ_0.

The formulas for S_p that we will obtain involve linear combinations of values of certain modular forms on CM points in the upper-half plane corresponding to Δ and Δ_0. We need to introduce the following notation in order to do this explicitly.

1) Let $\delta = (-1-1/3\sqrt{-3})/2 \in K \cap \mathcal{H}$, where $\mathcal{H}$ denotes the complex upper-half plane. As usual η will denote Dedekind's eta function. As a set of representatives for Δ we take the numbers 1 and $\delta - k$, with $k \in \mathbf{Z}/p\mathbf{Z}$ such that $\delta - k$ is prime to p (hence excluding two values and bringing the total to $p-1$).

Let $\mu_p : \Delta \longrightarrow \mathbf{C}$ be given by

$$\mu_p(1) = \frac{p\Theta(p\delta)}{\Theta(\delta)}, \qquad \mu_p(\delta - k) = \frac{\Theta(\frac{\delta-k}{p})}{\Theta(\delta)} \quad (k \in \mathbf{Z}/p\mathbf{Z},\ (\delta-k,p)=1),$$

with $\Theta(z)$ as in §1. The function μ_p is well defined and its values are conjugate algebraic integers in H_{3p}/K.

Note that $p^{\frac{1}{3}} \in H_{3p}$ and that $p^{\frac{1}{3}} \in H_p$ if and only if $p \equiv 1 \pmod 9$. We define $\kappa_p = p^{-\frac{2}{3}}\mu_p(1) = p^{\frac{1}{3}}\Theta(p\delta)/\Theta(\delta)$. It belongs to H_{3p} and its conjugates over K are $\{p^{-\frac{2}{3}}\overline{\chi}(u)\mu_p(u) : u \in \Delta\}$.

THEOREM 1. *Let $p \equiv 1 \pmod 9$ be prime. With the above notation we have*

$$Tr_{H_{3p}/K}(\kappa_p) = p^{-\frac{2}{3}} \sum_{u\in\Delta} \overline{\chi}(u)\mu_p(u) = 27\, S_p,$$

where $S_p \in \mathbf{Z}$ is the Birch-Swinnerton-Dyer number defined in the introduction.

2) We choose w a primitive cube of unity modulo p; this corresponds, via $\mathcal{P} = (w-\omega, p)$, to choosing a prime $\mathcal{P}$ of $\mathcal{O}$ above p. As a set of representatives for Δ_0 we take the numbers 1 and $\omega - k$, where k runs over $\mathbf{Z}/p\mathbf{Z}\backslash\{w, -1-w, 0, -1\})/\sim$, and where $\sim$, defined by $k \sim -1/(k+1) \sim -1-1/k$, corresponds to orbits under multiplication by ω. (The values of $\omega - k$ for $k = 0$ or -1 represent the same class as 1 in Δ_0).

Let $\lambda_{\mathcal{P}} : \Delta_0 \longrightarrow \mathbf{C}$ be given by

$$\lambda_{\mathcal{P}}(\omega - k) = \left(\frac{\omega - k}{\mathcal{P}}\right) \zeta_{24}^{kp}\, \eta(\frac{\omega - k}{p})/\eta(\omega) \qquad (k \in \mathbf{Z}/p\mathbf{Z}, \quad k \neq w, -1-w)$$

$$\lambda_{\mathcal{P}}(1) = \left(\frac{2}{p}\right) \epsilon_p \sqrt{p}\, \eta(p\omega)/\eta(\omega),$$

where $\left(\frac{\omega - k}{\mathcal{P}}\right) = \left(\frac{w-k}{p}\right)$ is the quadratic symbol at $\mathcal{P}$, $\zeta_{24} = e^{2\pi i/24}$, $\sqrt{p} > 0$, and $\epsilon_p = 1, i$ if $p \equiv 1, 3 \pmod 4$. The function $\lambda_{\mathcal{P}}$ is well defined and its values are conjugate units in an abelian extension of K, which is quadratic over H_p.

Let r be a solution of $r^2 \equiv -3 \pmod{4p}$ such that $r \equiv 2w + 1 \pmod p$, and let $z_0 = (r + \sqrt{-3})/2$. We define $\rho_{\mathcal{P}} = \left(\frac{r}{p}\right) \zeta_{24}^{-p(r+1)/2} \eta(z_0/p)/\eta(\omega)$. It is not hard to check that $\rho_{\mathcal{P}}^2 \in \mathcal{O}$ generates $\mathcal{P}$. Finally, we let $\xi_{\mathcal{P}} = \zeta\, p^{-\frac{1}{3}} \rho_{\mathcal{P}}^{-1} \lambda_{\mathcal{P}}(1)$, where $\zeta \in \mathcal{O}^\star$ is such that $\zeta\, \rho_{\mathcal{P}}^2 \equiv 1 \pmod 2$; it belongs to H_p and its conjugates over K are $\{\zeta p^{-\frac{1}{3}} \rho_{\mathcal{P}}^{-1} \chi(u) \lambda_{\mathcal{P}}(u) : u \in \Delta_0\}$.

THEOREM 2. *Let $p \equiv 1 \pmod 9$ be prime. With the above notation we have*

$$Tr_{H_p/K}(\xi_{\mathcal{P}}) = p^{-\frac{1}{3}} \rho_{\mathcal{P}}^{-1} \sum_{u \in \Delta_0} \chi(u)\, \lambda_{\mathcal{P}}(u) = \sqrt{-3}\, R_{\mathcal{P}},$$

with $R_{\mathcal{P}} \in \mathbf{Z}$. The number $R_{\mathcal{P}}$ satisfies

$$S_p = R_{\mathcal{P}}^2 \quad \textit{and} \quad R_{\overline{\mathcal{P}}} = -R_{\mathcal{P}},$$

where S_p is the Birch–Swinnerton-Dyer number defined in the introduction.

Remarks. 1. Theorem 2 holds in more generality. For any character ϕ of Δ let

$$R_{\mathcal{P}}(\phi) = \sum_{u \in \Delta} \phi(u)\, \lambda_{\mathcal{P}}(u)$$

(a Lagrange resolvent). Then for ϕ of odd order, $R_{\mathcal{P}}(\phi)^2$ is essentially the algebraic part of $L(\psi\phi^{-2}, 1)$.

2. It is possible to define, in a similar way, integers $R_{\mathcal{A}}$ associated to any cube-free ideal $\mathcal{A}$ of $\mathcal{O}$ such that $R_{\mathcal{A}}^2 = S_N$ is the Birch–Swinnerton-Dyer number of the elliptic curve $x^3 + y^3 = N$, where $N = \mathbf{N}(\mathcal{A})$. One might hope that these numbers are the Fourier coefficients of a modular form of some sort.

Theorem 1 is proved by writing the special value $L(\psi\chi, 1)$ as a linear combination of values of an Eisenstein series as in [4] and using the Shimura reciprocity law. One then deduces Theorem 2 from a variant of the factorization formula of [7] and a careful chasing of 24^{th} roots of unity. Theorems 1 and 2 are easily seen to be equivalent to the analogous statements given in the introduction.

3. Congruences

Our third answer to the question when S_p vanishes was based on a congruence between S_p (which is, up to a factor, the value of a certain L-function at $s = 1$) and another number A_k which, as we will discuss in a moment, is (again up to a factor) a special value of an L-function independent of p at some other value of s. Congruences of this sort go back to Cauchy, Kummer, and Hurwitz. For example [1], the class number $h(-p)$ of the quadratic field $\mathbf{Q}(\sqrt{-p})$ for a prime $p > 3$, $p \equiv 3 \pmod 4$ satisfies $h(-p) \equiv -2B_{(p+1)/2} \pmod p$, where (here only!) B_n denotes the n^{th} Bernoulli number. One way to interpret this is to say that the two Dirichlet series

$$\sum_{n\geq 1}\left(\frac{n}{p}\right)n^{-s} \qquad \text{and} \qquad \sum_{n\geq 1} n^{\frac{p-1}{2}}n^{-s},$$

which are congruent term by term modulo p, also have congruent values at $s = 0$. Turning this fact into a heuristic argument, we would expect that (suitable algebraic versions of) the values at $s = 0$ of the Dirichlet series

$$\sum_{\alpha\in\mathcal{O}\setminus\{0\}} \chi(\alpha)\frac{1}{\overline{\psi}(\alpha)\mathrm{N}(\alpha)^s} \qquad \text{and} \qquad \sum_{\alpha\in\mathcal{O}\setminus\{0\}} \left(\frac{\alpha}{\overline{\alpha}}\right)^{\frac{2(p-1)}{3}}\frac{1}{\overline{\psi}(\alpha)\mathrm{N}(\alpha)^s},$$

which are easily seen to equal $L(\psi\chi, 1)$ and $L(\psi^{2k-1}, k)$ respectively, with $k-1 = 2(p-1)/3$, should also be congruent modulo p (see §2 for notations). This is indeed the case, at least if $p \equiv 1 \pmod 3$, where it follows from the existence of a p-adic L-function interpolating special values of Hecke L-series due to Manin–Vishik and Katz. We now make this precise.

For $k \in \mathbf{N}$ define the algebraic part of $L(\psi^{2k-1}, k)$ to be

$$L_k = 3\nu\left(\frac{2\pi}{3\sqrt{3}\,\Omega^2}\right)^{k-1}\frac{(k-1)!}{\Omega}\,L(\psi^{2k-1}, k),$$

where $\nu = 2$ if $k \equiv 2 \pmod 6$ and $\nu = 1$ otherwise, and $\Omega = \Gamma(1/3)^3/(2\pi\sqrt{3}) = 1.766638\cdots$ is the fundamental real period of the elliptic curve $x^3 + y^3 = 1$. Then using the formulas of [2] we find that

$$S_p \equiv (-3)^{\frac{p-10}{3}}(\frac{p-1}{3})!^2 L_{(2p+1)/3} \pmod p.$$

This corresponds to the "third answer" of the introduction because $L_{3n+1} = A_n$ for all n, as we will now discuss.

4. Recursions

By the methods of [7] one can obtain formulas for $L(\psi^{2k-1}, k)$, $k \in \mathbf{N}$, in terms of derivatives of modular forms and then deduce recursive formulas giving the algebraic parts L_k, and similarly for their square roots. A typical formula for the values is the identity $L_{3n+1} = A_n$ just mentioned, but since the results for the square roots are more interesting and give more precise information, we shall state the full results only there (but see Remark 2 after Theorem 4 below).

The formulas for the square roots of L_k can be divided naturally into three branches: (a) $k \equiv 1 \pmod 6$, (b) $k \equiv 2 \pmod 6$, and (c) $k \equiv 4 \pmod 6$. (For other values of k the functional equation forces $L(\psi^{2k-1}, k)$ to be zero.) For each branch there is a formula for $\sqrt{L_k}$ in terms of a higher non-holomorphic derivative of a fixed half-integral weight modular form at a fixed CM point (e.g. for $\sqrt{L_{6n+1}}$ it is the n^{th} non-holomorphic derivative of $\eta(z)$ at the point $z = \omega$), and this in turn leads to the following description of the square roots as the constant terms of a recursively defined sequence of polynomials.

THEOREM 3. *Let $a_n(t), b_n(t), c_n(t)$ be the polynomials defined by the recursions*

$$\begin{aligned} a_{n+1}(t) &= -(1-8t^3)\, a_n'(t) - (16n+3)\, t^2\, a_n(t) - 4n(2n-1)\, t\, a_{n-1}(t), \\ b_{n+1}(t) &= (1-8t^3)\, b_n'(t) + (16n+9)\, t^2\, b_n(t) - 4n(2n+1)\, t\, b_{n-1}(t), \\ c_{n+1}(t) &= (1-8t^3)\, c_n'(t) + (16n+9)\, t^2\, c_n(t) - 4n(2n+1)\, t\, c_{n-1}(t) \end{aligned}$$

for $n \geq 1$, with initial conditions

$$a_0(t) = 1,\ a_1(t) = -3t^2,\ b_0(t) = 1,\ b_1(t) = 9t^2,\ c_0(t) = t,\ c_1(t) = 1 + t^3.$$

Then for all $n \in \mathbf{Z}_{\geq 0}$

$$L_{6n+1} = a_{3n}(0)^2, \quad L_{6n+2} = b_{3n}(0)^2, \quad L_{6n+4} = c_{3n+1}(0)^2,$$

while $a_m(0) = b_m(0) = c_{m+1}(0) = 0$ for $m \not\equiv 0 \pmod 3$.

We give a short table. Note that $a_{3n}(0)$ is the B_n of the introduction.

n	$a_{3n}(0)$	$b_{3n}(0)$	$c_{3n+1}(0)$
0	1	1	1
1	−2	6	−8
2	−152	−216	1240
3	−6848	−119232	−621440
4	−8103296	24105600	−51596800

Remark. The constant terms of the polynomials $*_n(t)$ ($* = a, b$ or c) satisfy the congruences $*_{n+(p-1)/2}(0) \equiv (\pi + \overline{\pi})\, *_n(0) \pmod p$ for all $n > 1$ and all $p \equiv 1 \pmod 3$ prime, where π denotes a generator of a prime in K above p with $\pi \equiv 1 \pmod 3$. The corresponding congruence for the squares of the $*_n(0)$ (i.e., for the numbers L_k) was known, and the possibility of choosing the signs in such a way that this congruence descends to the square roots for all p simultaneously had been conjectured by Koblitz [3]. In fact, Koblitz conjectured the existence of a p-adic L-function interpolating suitable modifications of the presumed square roots. This has been proved by Sofer [8] in other similar cases (see also [6]).

There is another way of obtaining the numbers $a_n(0)$, $b_n(0)$ and $c_n(0)$ directly in terms of generating series.

THEOREM 4. *(1) Let* $u(\tau) = F(\frac{1}{3}, \frac{1}{3}; \frac{2}{3}; \tau^3)$ *and* $v(\tau) = \tau\, F(\frac{2}{3}, \frac{2}{3}; \frac{4}{3}; \tau^3)$, *where* $F = {}_2F_1$ *is Gauss's hypergeometric function. Let*

$$h_a(\tau) = u(\tau)^{1/2}(1-\tau^3)^{1/24}, \quad h_b(\tau) = h_a(\tau)^3, \quad h_c(\tau) = \tfrac{1}{2}\tau\, h_b(\tau)$$

and define

$$H_a(x) = h_a(\tau), \quad H_b(x) = h_b(\tau), \quad H_c(x) = h_c(\tau),$$

where $x = v/2u = \frac{1}{2}(\tau + \frac{1}{6}\tau^4 + \frac{103}{1260}\tau^7 + \frac{169}{3240}\tau^{10} + \cdots)$. *Then*

$$H_a(x) = \sum_{n\geq 0}(-1)^n a_n(0)\frac{x^n}{n!}, \quad H_b(x) = \sum_{n\geq 0} b_n(0)\frac{x^n}{n!}, \quad H_c(x) = \sum_{n\geq 0} c_n(0)\frac{x^n}{n!}.$$

(2) The series $H_a(x)$ *is the expansion of* $\eta(z)$ *about* $\omega = (-1+\sqrt{-3})/2$ *in the following sense:*

$$(1-x)^{-\frac{1}{2}}\eta\left(\frac{\omega - \overline{\omega}x}{1-x}\right) = c_1 H_a(c_2 x), \qquad (|x|<1),$$

where $c_1 = \eta(\omega) = e^{\frac{2\pi i}{48}}(3^{\frac{1}{4}}\Omega/2\pi)^{\frac{1}{2}}$ *and* $c_2 = -3\sqrt{3}\,\Omega^2/4\pi$ *with* Ω *as in §2.*

Remarks. 1. As a corollary of the identity $H_b(x) = H_a(x)^3$ we obtain somewhat surprising polynomial relations between the square roots of the L-values $\{L_{6n+1}\}$ and $\{L_{6n+2}\}$. Analogous identities also hold for other CM curves, linking L-values of one curve to L-values of its twist by $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$; ultimately they boil down to classical Jacobi identity $\theta'(0) = 2\pi\eta^3$.

2. We briefly state here the power series expansions involving the L_k themselves. With the notation of Theorem 4 let $G_0(x) = u(\tau)$ and $G_1(x) = \tau\, u(\tau)$. Then $2^{-n}G_0^{(n)}(0)$ equals $a_{n/2}(0)^2$ if $n \equiv 0 \pmod 6$, $c_{(n-1)/2}(0)^2$ if $n \equiv 3 \pmod 6$, and 0 otherwise; $2^{-n}G_1^{(n)}(0)$ equals $b_{(n-1)/2}(0)^2$ if $n \equiv 1 \pmod 6$ and zero otherwise. We may even separate the two branches (a) and (b) in G_0 by considering the series $u(\tau)(1 \pm (1-\tau^3)^{\frac{1}{2}})$. It is presumably possible to prove directly that the series H_a, H_b, H_c, G_0 and G_1 have their Taylor coefficients related as indicated, but we have not done so.

Proof (sketch). Part 1) of the theorem follows from part 2) and the interpretation of the constant terms $a_n(0)$, $b_n(0)$, $c_n(0)$ as non-holomorphic derivatives of holomorphic modular forms, together with the general fact that the expansion of any modular form as a power series in a modular function satisfies a linear differential equation. (Classical examples of this latter assertion are the expansion of η^2 or $\sqrt[4]{E_4}$ as a power series in $1/j$ or of θ^2 as a power series in λ, all of which involve hypergeometric functions.) It can also be proved directly from the recursive definitions of the polynomials a_n, b_n and c_n without any a priori knowledge that modular forms are involved.

Part 2) is a consequence of the following simple result about non-holomorphic derivatives. We recall their definition. For any $k \in \mathbf{R}$ we let ϑ_k be the differential operator $\frac{\partial}{\partial z} + \frac{k}{2iy}$ acting on functions f of $z = x + iy \in \mathcal{H}$. It has the property

$$(\vartheta|_{k+2})\gamma = \vartheta(f|_k\gamma), \qquad (\gamma \in Sl_2(\mathbf{R})),$$

where $|_k$ has the usual meaning. In particular, if f is a modular form of weight k on some group $\Gamma \subset Sl_2(\mathbf{R})$, then $\vartheta_k^n f$, where $\vartheta_k^n = \vartheta_{k+2n} \circ \cdots \circ \vartheta_{k+2} \circ \vartheta_k$, is a (non-holomorphic) modular form of weight $k + 2n$ on the same group.

PROPOSITION 1. *Let $f : \mathcal{H} \longrightarrow \mathbf{C}$ be an analytic funtion and $z_0 = x_0 + iy_0$ a point in $\mathcal{H}$. Then the following expansion holds*

$$\sum_{n\geq 0} \vartheta_k^n f(z_0) \frac{(2iy_0 w)^n}{n!} = (1-w)^{-k} f\left(\frac{z_0 - \overline{z}_0 w}{1-w}\right) \qquad (|w| < 1).$$

Proof. It is easy to check by induction that

$$\frac{1}{n!}\vartheta_k^n f(z_0) = \sum_{j+l=n} \binom{j+l+k-1}{l} \left(\frac{1}{2iy_0}\right)^l \frac{f^{(j)}(z_0)}{j!}.$$

Hence,

$$\sum_{n\geq 0} \vartheta_k^n f(z_0) \frac{(2iy_0 w)^n}{n!} = \sum_{j\geq 0} \frac{f^{(j)}(z_0)}{j!}(2iy_0 w)^j \sum_{l\geq 0} \binom{j+l+k-1}{l} w^l,$$

and our claim follows from Taylor's and the binomial theorems.

Remark. Notice that the substitution $\phi(t) = (z_0 - \overline{z}_0 t)/(1-t)$ is an isomorphism from $\mathcal{H}$ to the unit disk sending z_0 to 0, with inverse $\phi^{-1}(z) = (z - z_0)/(z - \overline{z}_0)$. The proposition then says that the non-holomorphic derivatives $\vartheta_k^n f(z_0)$ are essentially the Taylor coefficients of $f|_k\phi$ at $t = 0$.

5. Estimates of S_p

The last two criteria for the vanishing of S_p described in the introduction are given in terms of the vanishing of $S_p \pmod p$. That these two statements are in fact equivalent is a consequence of the following general estimate.

PROPOSITION 2. *Let $E/\mathbf{Q}$ be a modular elliptic curve of conductor N. Then*

$$|L(E,1)| \;<\; (4N)^{1/4}\left(\log\frac{\sqrt{N}}{8\pi} + \gamma\right) \;+\; c_0\,,$$

where $\gamma = 0.577\ldots$ is Euler's constant and $c_0 = \zeta(\frac{1}{2})^2 = 2.13263\ldots$.

Proof. Because of the universal estimate $|a_n| \le \sqrt{n}\,\sigma_0(n)$ for the coefficients of $L(E,s)$ we have

$$|L(E,1)| = \left|(1+w)\sum_{n=1}^{\infty}\frac{a_n}{n}\,e^{-2\pi n/\sqrt{N}}\right| \le 2\,F\!\left(\frac{2\pi}{\sqrt{N}}\right),$$

where $w = \pm 1$ is the sign in the functional equation and $F(x) = \sum\limits_{n=1}^{\infty}\frac{\sigma_0(n)}{\sqrt{n}}\,e^{-nx}$. Using the fact that the Mellin transform of $F(x)$ is $\Gamma(s)\zeta(s+\frac{1}{2})^2$, we find the asymptotic expansion

$$F(x) = \sqrt{\frac{\pi}{x}}\,\Big(\log\frac{1}{4x}+\gamma\Big) + \sum_{n=0}^{\infty} c_n x^n \qquad (x \searrow 0)$$

with $c_0 = \zeta(\frac{1}{2})^2$ and $c_1 = -\zeta(-\frac{1}{2}) < 0$. Some numerical work shows that $\sum_{n\ge 1} c_n x^n < 0$ for all $x > 0$. (For the proposition, we need this only for $x \le 2\pi/\sqrt{11}$.)

Applying this to the curve E_p, whose conductor is $27p^2$, we find after a simple calculation the following estimate.

COROLLARY. *For* $p \equiv 1 \pmod 9$ *we have*

$$|S_p| < 0.61\,p^{5/6}\log p\,.$$

In particular, S_p *is determined by its value modulo* p *and*

$$S_p \equiv 0 \pmod p \quad \Longleftrightarrow \quad S_p = 0.$$

Remark. We can also estimate S_p using Theorems 1 or 2. For instance, from Theorem 2 and the estimate $\eta(\frac{w-k}{p}) = O(p^{1/4})$, we obtain $R_{\mathcal{P}} = O(p^{2/3})$, so that $R_{\mathcal{P}}$, and hence S_p, is determined by its value modulo p. The corresponding estimate using Theorem 1 is more difficult, because Θ is not a cusp form, but seems to lead to the estimate $S_p = O(p^{5/6+\epsilon})$, essentially the same as in the Corollary above. Note that to determine S_p from its value modulo p we need only the weaker estimate $S_p < p^2/4$, since we know that S_p is a square.

REFERENCES

1. A. Hurwitz, *Klassenzahl binärer quadratischer Formen von negativer Determinante*, Acta Math. **19** (1895), 351–384. Mathematische Werke, Bd. II, Birkhäuser-Verlag, Basel-Stuttgart, 1963, pp. 208–235.
2. N. M. Katz, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. **104** (1976), 459–571.
3. N. Koblitz, *p-adic congruences and modular forms of half-integral weight*, Math. Ann. **274** (1986), 191–220.
4. F. Rodriguez Villegas, *On the square root of special values of certain L-series*, Invent. math. **106** (1991), 549–573.
5. ———, *Square root formulas for central values of Hecke L-series* II, Duke Math. J. **72** (1993), 431–440.

6. ———, *On the Taylor coefficients of theta functions of CM elliptic curves*, Arithmetic Geometry (N. Childress and J.W. Jones, eds.), Contemporary Mathematics **174**, AMS, 1994.
7. F. Rodriguez Villegas and D. Zagier, *Square roots of central values of Hecke L-series*, Advances in Number Theory, (F. Q. Gouvêa and N. Yui, eds.), Clarendon Press, Oxford, 1993, pp. 81–99.
8. A. Sofer, *p-adic interpolation of square roots of central values of Hecke L-functions*, Ph.D. Thesis, The Ohio State University, 1993.
9. S. Sylvester, *On the equation in numbers* $Ax^3 + By^3 + Cz^3 = Dxyz$*, and its associate system of equations*, Philosophical Magazine **31** (1847), 293–296. Mathematical Papers, Vol. 1, Chelsea, New York, 1973, pp. 110–113.
10. D. Zagier and G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Ind. Math. Soc. **52** (1987), 51–69.

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NJ 08544, USA
E-mail address: villegas@math.princeton.edu

MAX-PLANCK-INSTITUT FÜR MATHEMATIK, G.-CLAREN-STR. 26, 53225 BONN, GERMANY
E-mail address: zagier@mpim-bonn.mpg.de