CLASS NUMBERS OF QUADRATIC FIELDS AND SHIMURA'S CORRESPONDENCE

Jan Nekovář

Mathematical Institute of the Czechoslovak Academy of Science

I. Introduction

It is well-known (see Fueter [8] and Aigner [1]) that Fermat's equation $X^3+Y^3 = 1$ has no solutions in a quadratic field $K = \mathbf{Q}(\sqrt{D})$ (for $|D| \equiv 1 \pmod 3$), provided the class number of K is not divisible by 3. This subject was further investigated by Frey [6], who gave estimates for the 3-rank of the class group of K in terms of 3-descent on a curve $Y^2 = X^3 + D$.

In this paper we consider curves $E_D : DY^2 = 4X^3 - 27$,which are quadratic twists of the Fermat's curve $X^3+Y^3 = 1$. We give a precise formula for the rank of the Selmer group corresponding to the complex multiplication $\sqrt{-3} : E_D \longrightarrow E_{-3D}$ in terms of the 3-rank of the class group of $\mathbf{Q}(\sqrt{D})$ resp. $\mathbf{Q}(\sqrt{-3D})$. This result may be considered as a quantitative version of [1] and [8].

We discuss also Birch and Swinnerton-Dyer's conjecture for curves E_D. According to a theorem of Waldspurger [22], [23], natural rational factor of $L(E_D/\mathbf{Q}, 1)$ may be expressed in terms of coefficients of certain modular forms of weight 3/2. We identify these forms explicitely and verify (mod 3)-part of Birch and Swinnerton-Dyer's conjecture for E_D in most cases (for D of density 5/6).

II. Descent on curves E_D

1. Notation and preliminaries.

Let $D \neq 1$ be a square-free integer prime to 3.Put $D_+ = \max(D, -3D)$, $D_- = \min(D, -3D)$, $K_\pm = \mathbf{Q}(\sqrt{D_\pm})$, $K_{-3} = \mathbf{Q}(\sqrt{-3})$, $L = K_+K_-$. Let $G(L/\mathbf{Q})\hat{} = \{1, \chi_+, \chi_-, \chi_{-3}\}$ be the character group of the Galois group $G(L/\mathbf{Q})$, where Ker $(\chi_\pm) = G(L/K_\pm)$, K$er(\chi_{-3}) = G(L/K_{-3})$. Denote by $C, C_\pm$ the class groups of $L, K_\pm$ respectively and by ${}_{p^\infty}C, {}_{p^\infty}(C_\pm)$ their p-primary parts. For an odd prime p we identify ${}_{p^\infty}(C_\pm)$ with their images in C under canonical morphisms $C_\pm \longrightarrow C$.

We consider the Fermat curve $E : x^3 + y^3 = 1$, which is isomorphic (over $\mathbf{Q}$) to $Y^2 = 4X^3 - 27$, an isomorphism being given by the following formulas:

$$X = \frac{3}{x+y}, \quad Y = \frac{9(x-y)}{x+y}, \quad x = \frac{9+Y}{6X}, \quad y = \frac{9-Y}{6X}.$$

Endomorphism ring of E is $End_{K_{-3}}(E) = \mathbf{Z}[\rho]$, where $\rho = \frac{-1+\sqrt{-3}}{2}$ acts by

$$\rho(x, y) = (\rho^{-1}x, \rho^{-1}y) \qquad \text{and} \qquad \rho(X, Y) = (\rho X, Y)$$

in Fermat's and Weierstrass' coordinates respectively.

We shall also consider twisted forms

$$E_\pm : D_\pm Y^2 = 4X^3 - 27, \qquad E_{-3} : Y^2 = 4X^3 + 1$$

of E. Let $\lambda = \rho - \rho^2 = \sqrt{-3} \in End(E)$ be the unique (up to a root of unity) isogeny of degree 3. It is defined over K_{-3}, but induces isogenies $E \longleftrightarrow E_{-3}, E_+ \longleftrightarrow E_-$ defined already over $\mathbf{Q}$ (see §2).

If G is a finite abelian group, $\chi \in G\hat{}$ a character of G with values in a ring A and M an $A[G]$-module, put

$$M_\chi = \{m \in M \mid gm = \chi(g)m \qquad \text{for every} \quad g \in G\}.$$

We shall use the notation $H^i(K/k, A)$ resp. $H^i(k, A)$ for the Galois cohomology groups $H^i(G(K/k), A)$ resp. $H^i(G(\bar{k}/k), A)$.

2. Twisted isogenies.

In this section we recall some basic facts about twisted forms of abelian varieties and isogenies. We are interested only in the case of the Fermat cubic, but we prefer to give the statements first in the general context.

Let A be an abelian variety over a field K, L/K a finite Galois extension. Isomorphism classes of abelian varieties A' over K such that $A' \times_K L \simeq A \times_K L$ are in a bijective correspondence with elements of the pointed set $H^1(L/K, Aut_L(A))$: every isomorphism

$$f : A \times_K L \xrightarrow{\sim} A' \times_K L \qquad \text{defines a 1-cocycle}$$

$$a(g) = {}^g f^{-1} \circ f \in Aut_L(A) \qquad (g \in G(L/K)).$$

Cohomology class of $a(g)$ depends only on the isomorphism class of A'. Denote by $A(a)$ the abelian variety A' corresponding to the cocycle $a(g)$.

Suppose we are given a separable isogeny $\lambda : A \times_K L \longrightarrow A \times_K L$ and isomorphisms $f : A \times_K L \xrightarrow{\sim} A' \times_K L$, $f' : A \times_K L \xrightarrow{\sim} A'' \times_K L$ such that the isogeny $\lambda' = f' \circ \lambda \circ f^{-1} : A' \times_K L \longrightarrow A'' \times_K L$ is already defined over K. Then the following diagram is commutative for every $g \in G(L/K)$:

$$\begin{array}{ccccccc} A' \times_K L & \xleftarrow{f} & A \times_K L & \xrightarrow{\lambda} & A \times_K L & \xrightarrow{f'} & A'' \times_K L \\ \| & & \downarrow{\scriptstyle a(g)} & & \downarrow{\scriptstyle a'(g)} & & \| \\ A' \times_K L & \xleftarrow{{}^g f} & A \times_K L & \xrightarrow{{}^g \lambda} & A \times_K L & \xrightarrow{{}^g f'} & A'' \times_K L \end{array} \tag{2.1}$$

where $a(g), a'(g)$ are cocycles corresponding to f and f'. We say that λ is $\underline{L}/\underline{K}$ − admissible if $\mathrm{K}er(\lambda)$ is $G(L/K)-$invariant. If this is the case, it follows from the diagram (2.1) that

$$a(g) \in Aut_L(A, \lambda) := \{ a \in Aut_L(A) \mid a(\mathrm{K}er(\lambda)) = \mathrm{K}er(\lambda) \}.$$

Conversely, suppose that λ is $L/K-$admissible and $a(g)$ is a 1-cocycle with values in $Aut_L(A, \lambda)$. Such data determine uniquelly automorphisms $a'(g) \in Aut_L(A)$ making (2.1) commutative. These $a'(g)$ form a 1-cocycle, hence define a twisted form $f' : A \times_K L \xrightarrow{\sim} A'' \times_K L$ of A such that $\lambda_a := f' \circ \lambda \circ f^{-1} : A(a) \longrightarrow A(a')$ is defined over K. Cocycles cohomologous to $a(g)$ give isogenies $K-$isomorphic to λ_a. If $End_L(A)$ is commutative, then $Aut_L(A, \lambda) = Aut_L(A)$ and $a'(g) = c(g)a(g)$, where $c(g) \in Aut_L(A)$ satisfies ${}^g\lambda = c(g)\lambda$.

We summarize previous discussion in the following

Proposition 2.1. *Let $\lambda : A \times_K L \longrightarrow A \times_K L$ be an $L/K-$admissible separable isogeny. Then we have a commutative diagram, whose horizontal arrows are bijections:*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{isomorphism classes (over } K\text{)} \\ \text{of isogenies } \lambda' : A' \longrightarrow A'' \\ \text{with } \lambda' \times_K L \simeq \lambda \end{array} \right\} & \xrightarrow{1-1} & H^1(L/K, Aut_L(A,\lambda)) \\ \Big\downarrow \text{forget } \lambda', A'' & & \Big\downarrow \text{canonical} \\ \left\{ \begin{array}{c} \text{isomorphism classes (over } K\text{)} \\ \text{of } A' \text{ with } A \times_K L \simeq A' \times_K L \end{array} \right\} & \xrightarrow{1-1} & H^1(L/K, Aut_L(A)) \end{array}$$

Cocycles $a(g), a'(g)$ representing twisted forms A', A'' satisfy

$$^g\lambda \circ a(g) \;=\; a'(g) \circ \lambda.$$

If $End_L(A)$ is commutative, then $a'(g) \;=\; c(g)a(g)$, where

$$^g\lambda \;=\; c(g)\lambda. \quad \square$$

We apply Proposition 2.1 in the following situation: $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt{D}, \sqrt{-3D})$, $A = E \;:\; x^3 + y^3 = 1$, $\lambda = \rho - \rho^2 = \sqrt{-3}$. As $^g\lambda = \chi_{-3}(g)\lambda$ $(g \in G(L/\mathbf{Q}))$, λ is $L/K-$admissible. We have

$$H^1(L/\mathbf{Q}, Aut_L(E)) = H^1(L/\mathbf{Q}, \mu_6) = H^1(L/\mathbf{Q}, \mu_2) = G(L/\mathbf{Q})\widehat{\ },$$

so the $L/\mathbf{Q}-$forms of E are the following curves:

$$E_{-3} = \; E(\chi_{-3}) : \; Y^2 = 4X^3 + 1, \qquad E : Y^2 = 4X^3 - 27$$
$$E_{\pm} = E(\chi_{\pm}) : \; D_{\pm}Y^2 = 4X^3 - 27,$$

corresponding to the characters $1, \chi_{\pm}, \chi_{-3}$ respectively. According to Proposition 2.1, λ induces isogenies $\lambda_\chi : E(\chi) \longrightarrow E(\chi\chi_{-3})$ defined over $\mathbf{Q}$ for every $\chi \in G(L/\mathbf{Q})\widehat{\ }$.

Explicit formulas for λ_χ are easily obtained from a more general isogeny between curves $y^2 = 4x^3 + a$ and $y'^2 = 4x'^3 - 27a$:

$$x' = \frac{x^3 + a}{x^2}, \quad y' = \frac{y(x^3 - 2a)}{x^3}.$$

3. Descent for twisted isogenies.

Suppose K is a number field, A, A' are abelian varieties over K and $\lambda : A \longrightarrow A'$ an isogeny also defined over K. The exact sequence

$$0 \longrightarrow \mathrm{K}er(\lambda) \longrightarrow A(\bar{K}) \xrightarrow{\lambda} A'(\bar{K}) \longrightarrow 0$$

induces a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & A'(K)/\lambda A(K) & \xrightarrow{\alpha} & H^1(K, \mathrm{K}er(\lambda)) \\ & & \downarrow & & \downarrow{\scriptstyle \beta_v} \\ 0 & \longrightarrow & A'(K_v)/\lambda A(K_v) & \xrightarrow{\alpha_v} & H^1(K_v, \mathrm{K}er(\lambda)) \end{array}$$

for every prime divisor v of K and the corresponding completion K_v (including archimedean v). Selmer group of λ is defined as

$$S(\lambda, A/K) = \bigcap_v \beta_v^{-1}(\mathrm{I}m(\alpha_v)).$$

It sits in an exact sequence

$$0 \longrightarrow A'(K)/\lambda A(K) \longrightarrow S(\lambda, A/K) \longrightarrow {}_\lambda Ш(A/K) \longrightarrow 0,$$

where ${}_\lambda Ш(A/K)$ is the subgroup of $\lambda-$torsion elements of the Tate-Šafarevič group of A over K.

For $A = A' = E : x^3 + y^3 = 1, \lambda = \sqrt{-3}$ one has $\mathrm{K}er(\lambda) = \mu_3$, $H^1(K, \mathrm{K}er(\lambda)) \simeq K^*/K^{*3}$. Suppose $\mu_3 \subset K$. Then $a \in K^*/K^{*3}$ lies in $\mathrm{I}m(\alpha)$ iff the curve $D_a : a^{-1}x^3 + ay^3 = 1$ contains a K-ratinal point and $a \in S(\lambda, E/K)$ iff D_a contains a K_v-rational point for all v (see [3]).

Suppose that in the situation of Proposition 2.1, L/K is a Galois extension of number fields. We shall compare Selmer groups of λ and λ'.

Proposition 3.1. *Let L/K be a finite Galois extension, A an abelian variety over K, $\lambda : A \times_K L \longrightarrow A \times_K L$ a separable L/K-admissible isogeny of degree prime to $[L : K]$. Let $a(g), a'(g)$ be a pair of 1-cocycles corresponding to a K-isogeny $\lambda_a : A' = A(a) \longrightarrow A' = A(a')$ as in Proposition 2.1. Then we have a commutative diagram whose vertical arrows are all isomorphisms:*

$$\begin{array}{ccccc} 0 & \longrightarrow & A''(K)/\lambda_a A'(K) & \longrightarrow & H^1(K, \mathrm{K}er(\lambda_a)) \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ 0 & \longrightarrow & (A''(L)/\lambda_a A'(L))^{G(L/K)} & \longrightarrow & H^1(L, \mathrm{K}er(\lambda_a))^{G(L/K)} \\ & & \uparrow{\scriptstyle f'_*} & & \uparrow{\scriptstyle f_*} \\ 0 & \longrightarrow & (A(L)/\lambda A(L))_{a'} & \longrightarrow & H^1(L, \mathrm{K}er(\lambda))_a \end{array}$$

Here $M_a = \{m \in M \mid {}^g m = a(g)m \quad \forall g \in G(L/K)\}$.

Proof. Commutativity of the upper square is obvious. As $deg(\lambda)$ is prime to $[L:K]$, the Hochschild-Serre spectral sequence degenerates into isomorphisms

$$\mathrm{res} : H^i(K, \mathrm{K}er(\lambda_a)) \xrightarrow{\sim} H^i(L, \mathrm{K}er(\lambda_a))^{G(L/K)}.$$

From exact sequences

$$0 \longrightarrow (\mathrm{K}er(\lambda_a))(K) \longrightarrow A'(K) \longrightarrow (A'(L)/(\mathrm{K}er(\lambda_a))(L))^{G(L/K)} \longrightarrow 0$$

$$0 \to (A'(L)/(\mathrm{K}er(\lambda_a))(L))^{G(L/K)} \to A''(K) \to$$
$$\to (A''(L)/\lambda_a A'(L))^{G(L/K)} \to 0$$

it follows that the upper left vertical arrow is also an isomorphism.

From the diagram (2.1) we get exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{K}er(\lambda) & \longrightarrow & A(\bar{K}) & \xrightarrow{\lambda} & A(\bar{K}) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow f & & \downarrow f' & & \\ 0 & \longrightarrow & \mathrm{K}er(\lambda_a) & \longrightarrow & A'(\bar{K}) & \xrightarrow{\lambda_a} & A''(\bar{K}) & \longrightarrow & 0 \end{array}$$

(the vertical arrows are isomorphisms of $G(\bar{K}/L)-$modules, but not of $G(\bar{K}/K)$-modules). By taking cohomology over L, we get a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & A(L)/\lambda A(L) & \longrightarrow & H^1(L, \mathrm{K}er(\lambda)) \\ & & \downarrow f' & & \downarrow f_* \\ 0 & \longrightarrow & A''(L)/\lambda_a A'(L) & \longrightarrow & H^1(L, \mathrm{K}er(\lambda_a)) \end{array} .$$

Suppose that $F(h)(h \in G(\bar{K}/L))$ is a 1-cocycle representing a cohomology class $[F] \in H^1(L, \mathrm{K}er(\lambda))$. Then $f_*[F]$ is represented by $f_*F = f \circ F$. But

$$f_*F = ({}^g f)(a(g)F(h)) \qquad \text{and}$$
$$({}^g(f_*F))(h) = {}^g(f(F(g^{-1}hg))) = ({}^g f)(({}^g F)(h))$$

for $g \in G(L/K)$, hence

$$({}^g(f_*F) - f_*F)(h) = ({}^g f)(({}^g F)(h) - a(g)F(h))$$

and ${}^g(f_*F) - f_*F$ is a coboundary iff ${}^g F - a(g)F$ is. Similarly, for $x \in A(L)/\lambda A(L)$ and $g \in G(L/K)$,

$${}^g(f'(x)) - f'(x) = ({}^g f')({}^g x - a'(g)x).$$

This proves that both f_* and f'_* are isomorphisms. □

Proposition 3.2. *Under the hypotheses of Proposition 3.1, suppose that K is a number field. Then the map*

$$f_*^{-1} \circ \mathrm{res} : H^1(K, \mathrm{K}er(\lambda_a)) \xrightarrow{\sim} H^1(L, \mathrm{K}er(\lambda))_a$$

induces an isomorphism

$$S(\lambda_a, A/K) \xrightarrow{\sim} S(\lambda, A \times_K L/L)_a.$$

Proof. Consider the commutative diagram of Proposition 3.1

$$\begin{array}{ccc} A''(K)/\lambda_a A'(K) & \longrightarrow & H^1(K, \mathrm{K}er(\lambda_a)) \\ \downarrow f_*'^{-1} & & \downarrow f_*^{-1} \circ \mathrm{res} \\ (A(L)/\lambda A(L))_{a'} & \longrightarrow & H^1(L, \mathrm{K}er(\lambda))_a \end{array}$$

and the analogous diagrams for all completions K_v. The statement of the Proposition follows by a trivial diagram chase. □

Corollary 3.3. *For $A = E : x^3 + y^3 = 1$, $\lambda = \sqrt{-3}$, $L/K = \mathbf{Q}(\sqrt{D}, \sqrt{-3D})/\mathbf{Q}$ and $\chi \in G(L/K)\hat{}$ we have*

$$S(\lambda, E/L)_\chi = S(\lambda_\chi, E_\chi/\mathbf{Q})$$
$$S(\lambda, E/L) = \bigoplus_{\chi \in G(L/\mathbf{Q})\hat{}} S(\lambda_\chi, E_\chi/\mathbf{Q}).$$

4. Explicit calculation of Selmer groups.

In this section we show how the Selmer groups of isogenies λ_χ are related to the class groups of $K_\pm$.

Let H be the Hilbert class field of L. Artin's reciprocity law yields an isomorphism of $G(L/K)$-modules

$$\psi : C \simeq G(H/L)$$

($G(L/\mathbf{Q})$ acts on $G(H/L)$ by inner automorphisms). Let F be the subextension of H/L corresponding to the subgroup C^3. Again

$$\psi : C/C^3 \simeq G(F/L)$$

is an isomorphism of $G(L/\mathbf{Q})$-modules. By Kummer's theory we get a monomorphism

$$f : Hom(C/C^3, \mu_3) \simeq Hom(G(F/L), \mu_3) \hookrightarrow H^1(L, \mu_3) = L^*/L^{*3}.$$

In other words, $F = L(\sqrt[3]{a_1}, \cdots, \sqrt[3]{a_r})$ with $a_i \in L^*$ and $Im(f)$ is generated by the images of $a_i's$ in L^*/L^{*3}.

Proposition 4.1. *The image of*

$$f : Hom(C/C^3, \mu_3) \longrightarrow H^1(L, \mu_3) = H^1(L, \mathrm{K}er(\lambda))$$

is contained in the Selmer group $S(\lambda, E/L)$.

Proof. According to the preceding discussion, $a \in L^*/L^{*3}$ lies in $\mathrm{I}m(f)$ iff $L(\sqrt[3]{a})/L$ is unramified, i.e. iff for all (non-archimedean) prime divisors v of L the image of a under $\beta_v : H^1(L, \mathrm{K}er(\lambda)) \longrightarrow H^1(L_v, \mathrm{K}er(\lambda))$ is contained in the group of unramified cohomology classes $H^1_{ur}(L_v, \mathrm{K}er(\lambda))$. As $deg(\lambda) = 3$ and E has good reduction outside 3,

$$H^1_{ur}(L_v, \mathrm{K}er(\lambda)) = \mathrm{I}m[\alpha_v : E(L_v)/\lambda E(L_v) \longrightarrow H^1(L_v, \mathrm{K}er(\lambda))]$$

for each v of residue characteristic different from 3 (see [5]).

We are thus reduced to prove that if $L(\sqrt[3]{a})/L)$ is unramified and v is a prime divisor of L dividing 3, then the curve $D_a : a^{-1}x^3 + ay^3 = 1$ contains an L_v-rational point.

Let O_v be the ring of integers in L_v. Its prime element is $\pi = \rho - \rho^2$ and the residue field $O_v/\pi O_v$ has $q = 3$ or 9 elements. Put $U_n = 1 + \pi^n O_v$. Then $L_v^* = \pi^{\mathbf{Z}} \times \mu_{q-1} \times U_1$. We may assume, therefore, that $a \in U_1$. Let $x^3 = a, M = L_v(x)$. As M/L_v is unramified and $x^3 \equiv 1 \pmod{\pi}$, one must also have $x \equiv 1 \pmod{\pi}$, which implies that $a = x^3 \equiv 1 \pmod{\pi^3}$. Then $-\rho a - \rho^{-1}a^{-1} \equiv 1 \pmod{\pi^4}$ is a cube in L_v, as $U_4 = U_2^3$. This means that $D_{\rho a}$ contains an L_v-rational point, so $\rho a \in \mathrm{I}m(\alpha_v)$. As D_ρ contains the point (-1,-1), $a \in \mathrm{I}m(\alpha_v)$ as well. □

Corollary 4.2. *f induces monomorphisms*

$$f_\pm : Hom(C_\mp/C_\mp^3, \mu_3) \hookrightarrow S(\lambda_\pm, E_\pm/\mathbf{Q}).$$

Proof. As $\mu_3 = (\mu_3)_{\chi_{-3}}$, our claim follows from Corollary 3.3 and the following

Lemma 4.3. *If $p > 2$ is a prime, then*

$$\big({}_p\infty C\big)_{\chi_\pm} = {}_p\infty(C_\pm), \quad \big({}_p\infty C\big)_1 = \big({}_p\infty C\big)_{\chi_{-3}} = 0.$$

Proof of the Lemma. As ${}_p\infty(C_\pm) = \big({}_p\infty(C_\pm)\big)_{\chi_\pm}$, the morphism

$${}_p\infty(C_+) \oplus {}_p\infty(C_-) \xrightarrow{+} {}_p\infty C$$

is injective. On the other hand, the class number formulas together with the identity

$$\zeta^2(s)\zeta_L(s) = \zeta_{K_+}(s)\zeta_{K_-}(s)\zeta_{K_{-3}}(s)$$

imply that $\#\left({}_{p\infty}C\right) = \#\left({}_{p\infty}(C_+)\right)\#\left({}_{p\infty}(C_-)\right)$. $\square$

Before we proceed further, we need some information about bad fibres of minimal models of $E_\pm$. We recall that D is a square-free integer prime to 3 and we allow for the moment also $D = 1$. We change coordinates on $E_\pm$ as follows : let

$$E : Y^2 = X^3 - 2^4 \cdot 3^3 \cdot D^3, \quad E' : Y'^2 = X'^3 + 2^4 \cdot D^3$$

and let $\omega = \frac{dX}{2Y}, \omega' = \frac{dX'}{2Y'}$ be regular differentials on E resp. E'.

Proposition 4.4. *For a prime p, let c_p resp. c'_p denote the number of components of the fibre over p of the Néron model of E resp. E'. Let ω_{min} resp. ω'_{min} be a Néron differential of E resp. E' over $\mathbf{Z}$. Then*

(1) *The numbers of components of Néron models are*

$$c_p = c'_p = 1 \qquad \text{for } p \nmid 6D$$
$$c_p = c'_p = 1 + \#\{x \in \mathbf{F}_p \,|\, x^3 = 2\} \qquad \text{for } p|D, p \neq 2$$
$$c_3 = 1 + \#\{x \in \mathbf{F}_3 \,|\, x^2 = D\}, c'_3 = 1$$
$$c_2 = c'_2 = 1$$

The common conductor of both E, E' is

$$N = 3^3 D^2 \times \begin{cases} 1, & \text{if } D \equiv 1 \pmod 4 \\ 2^4, & \text{if } D \equiv 2, 3 \pmod 4 \end{cases}$$

(2) *The minimal equations of E, E' over $\mathbf{Z}$ are*

$$Y^2 = X^3 - 2^4 \cdot 3^3 \cdot D^3 \qquad Y'^2 = X'^3 + 2^4 \cdot D^3$$
$$Y^2 = X^3 - 2 \cdot 3^3 \cdot (D/2)^3 \qquad Y'^2 = X'^3 + 2 \cdot (D/2)^3$$
$$Y^2 + Y = X^3 - (1 + 27D^3)/4 \qquad Y'^2 + Y' = X'^3 + (D^3 - 1)/4$$

for $D \equiv 3, 2, 1 \pmod 4$ *respectively.*

$$\frac{\omega_{min}}{\omega} = \frac{\omega'_{min}}{\omega'} = \begin{cases} 1, & \text{for } D \equiv 3 \pmod 4 \\ 2, & \text{for } D \equiv 1, 2 \pmod 4 \end{cases}$$

(3)

$$\int_{E(\mathbf{R})} |\omega|_\infty = \frac{1}{2}\Omega|D|^{-1/2} \times \begin{cases} 1, & \text{for } D < 0 \\ 3^{-1/2}, & \text{for } D > 0 \end{cases}$$

$$\int_{E'(\mathbf{R})} |\omega'|_\infty = \frac{1}{2}\Omega|D|^{-1/2} \times \begin{cases} 1, & \text{for } D<0 \\ 3^{1/2}, & \text{for } D>0 \end{cases},$$

where $\Omega = \frac{1}{2\pi}\Gamma\left(\frac{1}{3}\right)^3 = 3,059908\ldots$ *is the real period of* $y^2 = 4x^3 - 1$.

(4) *The torsion subgroups over* $\mathbf{Q}$ *are*

$$\#\left(E(\mathbf{Q})_{tors}\right) = 1, \quad \#\left(E'(\mathbf{Q})_{tors}\right) = \begin{cases} 3, & \text{for } D=1 \\ 1, & \text{for } D \neq 1 \end{cases}$$

Proof. (1) and (2) follow from Tate's algorithm [21].

(3) is an elementary calculation.

(4) As the reduction map is injective in the case of good reduction, $\#\left(E(\mathbf{Q})_{tors}\right)$ divides $n := g.c.d.\{E(\mathbf{F}_p)\,|\,p \not| 6D\}$. As all $p \equiv 2 \pmod 3$ prime to $2D$ are supersingular for E, $\#E(\mathbf{F}_p) = p+1$ for such p, hence $n|3$. It follows that

$$E(\mathbf{Q})_{tors} \subseteq \mathrm{K}er(\lambda) = \{0, (0, \pm 12D\sqrt{-3D})\}$$

and similarly $E'(\mathbf{Q})_{tors} \subseteq \mathrm{K}er(\lambda') = \{0, (0, \pm 4D\sqrt{D})\}$. □

To get an upper bound for the Selmer groups in question, we note that, according to the Hilbert Theorem 90,

$$\begin{aligned} (L^*/L^{*3})_{\chi_\pm} &= \{x \in K_\pm^*/K_\pm^{*3} \mid N_{K_\pm/\mathbf{Q}}(x) \in \mathbf{Q}^{*3}\} \\ (L^*/L^{*3})_{\chi_{-3}} &= \{x \in K_{-3}^*/K_{-3}^{*3} \mid N_{K_{-3}/\mathbf{Q}}(x) \in \mathbf{Q}^{*3}\} \\ (L^*/L^{*3})_1 &= \mathbf{Q}^*/\mathbf{Q}^{*3} \end{aligned}$$

All of the groups $S(\lambda_\pm, E_\pm/\mathbf{Q})$, $C_\pm/C_\pm^3$ are vector spaces over $\mathbf{F}_3$. Denote by $s_\pm, r_\pm$ respectively their dimensions over $\mathbf{F}_3$. Then

$$\#(C_\pm/C_\pm^3) = 3^{r_\pm}, \#(C/C^3) = 3^{r_+ + r_-}, \#S(\lambda_\pm, E_\pm/\mathbf{Q}) = 3^{s_\pm}.$$

Proposition 4.5.

(1) $s_+ \leq 1 + r_+, \quad s_- \leq r_-$.

(2) $S(\lambda_1, E/\mathbf{Q}) = 0, \quad S(\lambda_{-3}, E_{-3}/\mathbf{Q}) = \mathbf{Z}/3\mathbf{Z}$.

(3) $s_+ - s_- = \begin{cases} 0, & \text{for } |D| \equiv 1 \pmod 3 \\ 1, & \text{for } |D| \equiv 2 \pmod 3 \end{cases}$

Proof. (1) $S(\lambda_+, E_+/\mathbf{Q})$ is the subgroup of all $a \in K_+^*/K_+^{*3}$ such that $N_{K_+/\mathbf{Q}}(a) \in \mathbf{Q}^{*3}$ and the curve $D_a: \ a^{-1}x^3 + ay^3 = 1$ admits a rational point in all completions $K_{+,v}$. For any such a the principal divisor $(a) = b^3$ must be a cube of some

divisor b. This defines a homomorphism $\varphi(a) = b$, $\varphi : S(\lambda_+, E_+.\mathbf{Q}) \longrightarrow {}_3C_+$ with $\mathrm{K}er(\varphi) \subseteq W_+/W_+^3 = \mathbf{Z}/3\mathbf{Z}$, where W_+ denotes the group of units of K_+. It follows that $3^{s_+} \leq 3^{1+r_+}$. One obtains similarly $S(\lambda_-, E_-/\mathbf{Q}) \hookrightarrow {}_3C_-$ and $s_- \leq r_-$.

(2) The upper bounds $\#S(\lambda_1, E/\mathbf{Q}) \leq 1$, $\#S(\lambda_{-3}, E_{-3}/\mathbf{Q})|3$ are obtained in the same way as in (1). The torsion subgroup of $E_{-3}(\mathbf{Q})$ is responsible for nontriviality of $S(\lambda_{-3}, E_{-3}/\mathbf{Q})$.

(3) According to the duality theorem of Cassels [4],

$$\frac{\#S(\lambda_+, E_+/\mathbf{Q})}{\#S(\lambda_-, E_-/\mathbf{Q})} = \left(\frac{\#E_+(\mathbf{Q})_{tors}}{\#E_-(\mathbf{Q})_{tors}}\right)^2 \prod_p \frac{c_p(E_-)}{c_p(E_+)} \frac{\int_{E_-(\mathbf{R})} |\omega^-_{min}|_\infty}{\int_{E_+(\mathbf{R})} |\omega^+_{min}|_\infty}$$

and the R.H.S. is calculated by using Proposition 4.4. □

Theorem 4.6. *Let $D \neq 1$ be a square-free integer prime to 3, $D_+ = \max(D, -3D), D_- = \min(D, -3D)$. Let r_+, r_- be the ranks of the 3-primary parts of the class groups of $\mathbf{Q}(\sqrt{D_+})$, $\mathbf{Q}(\sqrt{D_-})$ and s_+, s_- the ranks of the Selmer groups of isogenies $E_+ \xrightarrow{\lambda_+} E_-$ resp. $E_- \xrightarrow{\lambda_-} E_+$ of degree 3. Then*

(1) $r_+ \leq s_- \leq r_- \leq s_+ \leq 1 + r_+$

(2) *there exist natural exact sequences*

$$0 \to Hom(C_\mp/C_\mp^3, \mu_3) \to S(\lambda_\pm, E_\pm/\mathbf{Q}) \to A_\pm \to 0$$

with

$$A_+ = 0, \qquad \#A_- = 3^{r_- - r_+}, \qquad \text{if } |D| \equiv 1 \pmod 3$$
$$A_- = 0, \qquad \#A_+ = 3^{1+r_+-r_-}, \qquad \text{if } |D| \equiv 2 \pmod 3$$

(3) *The ranks of the Selmer groups are given by*

$$s_+ = s_- = r_-, \qquad \text{if } |D| \equiv 1 \pmod 3$$
$$s_+ = 1 + r_+, s_- = r_+, \qquad \text{if } |D| \equiv 2 \pmod 3$$

Proof. (1) By Corollary 4.2 $r_+ \leq s_-$, $r_- \leq s_+$ and by Proposition 4.5.1 $s_- \leq r_-$, $s_+ \leq 1 + r_+$.

(2),(3) Follow from (1), Corollary 4.2 and Proposition 4.5.3. □

Corollary 4.7. (Reichardt [**13**],Scholz [**15**]) $r_+ \leq r_- \leq 1 + r_+$.

Corollary 4.8. (Fueter [**8**], Aigner [**1**]) *If* $|D| \equiv 1 \pmod 3$ *and* $r_- = 0$, *then* $E(K_+) = E(K_-) = E(\mathbf{Q}) = \mathbf{Z}/3\mathbf{Z}$.

Proof. If A is a curve $A: y^2 = x^3+ax+b$, $L/K = K(\sqrt{D}/K$ a quadratic extension with Galois group $G = \{1, c\}$, define two morphisms $f, g : A(L) \to A(L)$ by $f(P) = P - {}^cP$, $g(P) = P + {}^cP$. One has an exact sequence

$$0 \to A(K) \to A(L) \xrightarrow{f} \mathrm{K}er(g) \to H^1(G, A(L)) \to 0$$

A point $P = (x, y)$ lies in K$er(g)$ iff $(x, yD^{-1/2}) \in A_D(K)$, where $A_D : Dy^2 = x^3 + ax + b$. It follows that the sequence

$$0 \to A(K) \to A(L) \to A_D(K) \to H^1(G, A(L)) \to 0$$

is exact. Take $A = E$, $L/K = K_\pm/\mathbf{Q}$, in which case $A_D = E_\pm$. If $|D| \equiv 1 \pmod 3$ and $r_- = 0$, then $E_\pm(\mathbf{Q}) = 0$ by Theorem 4.6.3 and $E(K_\pm) = E(\mathbf{Q}) = \mathbf{Z}/3\mathbf{Z}$ by Proposition 4.4.4. □

III. Modular forms

5. L-function of E_D.

L-series of the curve E is given by the well-known formula (see e.g. [10, p.313])

$$L(E/\mathbf{Q}, s) = \sum_{\alpha \equiv 1 \pmod 3} \alpha(N\alpha)^{-s},$$

where α runs through all elements of $\mathbf{Z}[\rho]$ congruent to $1 \pmod 3$. It is also classical [7, vol.II, p.388] that E is isomorphic to the (compactified) modular curve $X_0(27)$; if

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), q = e^{2\pi i z}$$

is the Dedekind function and $\eta_a(z) = \eta(az)$, then

$$X = \frac{\eta_9^4}{\eta_3 \eta_{27}^3}, \qquad Y = 2\left(\frac{\eta_3}{\eta_{27}}\right)^3 + 9$$

are functions on $X_0(27)$ satisfying $Y^2 = 4X^3 - 27$. One has

$$L(E/\mathbf{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s} = L(f, s),$$

where

$$f = \sum_{n=1}^{\infty} a_n q^n$$

is the normalized ($a_1 = 1$) generator of $S_2(\Gamma_0(27), 1)$.

Let D be a square-free integer prime to 3 and Δ the conductor of the primitive Dirichlet character $\left(\frac{D}{\cdot}\right)$. Then

$$L(E_D/\mathbf{Q}, s) = \sum_{n=1}^{\infty} a_n \left(\frac{D}{n}\right) n^{-s} = L(f \otimes \left(\frac{D}{\cdot}\right), s),$$

where

$$f \otimes \left(\frac{D}{\cdot}\right) = \sum_{n=1}^{\infty} a_n \left(\frac{D}{n}\right) q^n \quad \in S_2(\Gamma_0(27\Delta^2), 1).$$

Put $\Lambda_D(s) = (27\Delta^2)^{s/2}(2\pi)^{-s}\Gamma(s)L(E_D/\mathbf{Q}, s)$. Then $\Lambda_D(s)$ has a holomorphic continuation to $\mathbf{C}$ and satisfies the functional equation

$$\Lambda_D(s) = \left(\frac{-3}{|D|}\right) \Lambda_D(2 - s).$$

It follows that $L(E_D/\mathbf{Q}, 1) = 0$ for $|D| \equiv 2 \pmod 3$.

6. Shimura's correspondence.

To compute critical values $L_D(1) := L(E_D/\mathbf{Q}, 1)$ for $|D| \equiv 1 \pmod 3$, we shall use a theorem of Waldspurger [22],[23]. We must first find some cusp forms of weight 3/2 which are mapped to the form f under Shimura's correspondence [19]. This is a correspondence between Hecke eigenforms $F \in M_{k+1/2}(\Gamma_0(4N))$ and $f \in M_{2k}(\Gamma_0(N))$ with the same Hecke algebra eigenvalues: $T_{p^2}F = \lambda_p F$, $T_p f = \lambda_p f$ for all primes p prime to $4N$.

We start with the cubic extension $K'/K = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbf{Q}(\sqrt{-3})$ and the cubic character $\chi : G(K'/K) \to \mu_3$, which correspods via reciprocity law to the character $a \longmapsto \left(\frac{2}{a}\right)_3$, defined on ideals a in $\mathbf{Z}[\rho]$ prime to (3). According to [16, 7.2.1], $\rho = Ind_{G(\bar{\mathbf{Q}}/K)}^{G(\bar{\mathbf{Q}}/\mathbf{Q})}\chi$ is a dihedral representation of $G(\bar{\mathbf{Q}}/\mathbf{Q})$ and the Artin L-function

$$L(\rho, s) = \sum_{n=1}^{\infty} b_n n^{-s}$$

corresponds to a cusp form

$$g = \sum_{n=1}^{\infty} b_n q^n \quad \in S_1(\Gamma_0(108), \left(\tfrac{-3}{\cdot}\right)).$$

In fact,

$$g(z) = \sum_{\alpha \equiv 1 \ (3)} \left(\tfrac{2}{\alpha}\right)_3 \, q^{N\alpha} = \frac{(\theta_1 - \theta_9)(3\theta_{27} - \theta_3)}{4},$$

where $\theta_a(z) = \sum_{n \in \mathbf{Z}} q^{an^2}$.

Lemma 6.1. ([**18, 2.16**]) *Let* $0 \neq F \in M_k(\Gamma_0(N), \chi)$. *Then*

$$\mathrm{d}eg(\mathrm{d}iv(F)) = \{(2g-2) + \sum_P (1 - e_P^{-1}) + \#(cusps)\}\tfrac{k}{2},$$

where g = *genus of* $X_0(N)$ *and* P *runs through all non-equivalent elliptic points of* $\Gamma_0(N)$ *with orders* e_P.

Corollary 6.2. *For* $0 \neq F \in M_k(\Gamma_0(108), \chi)$, $\quad \mathrm{d}eg(\mathrm{d}iv(F)) = 18k$.

Proof. Indeed, $g = 10, \#(cusps) = 18$ and $\Gamma_0(108)$ has no elliptic points. □

Proposition 6.3.

(1) *The form* $g(z) = \sum_{n=1}^{\infty} b_n q^n$ *generates* $S_1(\Gamma_0(108), \left(\tfrac{-3}{\cdot}\right))$. *It has zeros of order one at all cusps and no other zeros.*

(2) $g(z) = \eta(6z)\eta(18z) = q \prod_{n=1}^{\infty}(1 - q^{6n})(1 - q^{18n})$.

Proof. (1) As $\left(\tfrac{-3}{\cdot}\right)$ is an odd character, any modular form belonging to $M_1(\Gamma_0(108), \left(\tfrac{-3}{\cdot}\right))$ has integral order at every irregular cusp. We conclude by Corollary 6.2.

(2) By (1), it is sufficient to prove that $\eta_6\eta_{18} \in S_1(\Gamma_0(108), \left(\tfrac{-3}{\cdot}\right))$. It is well-known that $\frac{\eta^3}{\eta_3} \in M_1(\Gamma_0(9), \left(\tfrac{-3}{\cdot}\right))$ and it is easy to check that $\left(\frac{\eta_{18}}{\eta_6}\right)^2$ is a function on $X_0(108)$ (cf. [12]). It follows that $\eta_6\eta_{18} = \left(\frac{\eta_{18}}{\eta_6}\right)^2 \frac{\eta_6^3}{\eta_{18}}$ transforms like a form of weight one on $\Gamma_0(108)$ with character $\left(\tfrac{-3}{\cdot}\right)$. This function is obviously holomorphic in the upper half plane and vanishes at all cusps, so it lies necessarily in $S_1(\Gamma_0(108), \left(\tfrac{-3}{\cdot}\right))$. □

Proposition 6.4. *Let* $F_- = g\theta_3$, $F_+ = g\theta_9$, $G_- = g\frac{3\theta_{27}-\theta_3}{2}$, $G_+ = g\frac{\theta_1-\theta_9}{2}$. *Then*

(1) *Both subspaces*

$$V_- = \mathbf{C}F_- \oplus \mathbf{C}G_- \quad \subseteq \quad S_{3/2}(\Gamma_0(108), 1)$$
$$V_+ = \mathbf{C}F_+ \oplus \mathbf{C}G_+ \quad \subseteq \quad S_{3/2}(\Gamma_0(108), (\tfrac{-3}{\cdot}))$$

are invariant under the action of all Hecke operators T_{p^2} $(p > 3)$.

(2) *The forms* $F_\pm$, $G_\pm$ *are eigenfunctions of all* T_{p^2} $(p > 3)$.

(3) *Under Shimura's correspondence*

$F_\pm$ *are mapped to* $f \in S_2(\Gamma_0(27), 1)$

$G_\pm$ *are mapped to* $f' = q - q^2 + q^4 + 3q^5 + \cdots \in S_2(\Gamma_0(54), 1)$ *(*f' *corresponds to the curve* $54E$ *in the tables* [**24**], p.117 *).*

Proof. (1) The key point is the following

Lemma 6.5. *Let* $0 \neq F \in M_{k/2}(\Gamma_0(108), \chi)$ *for some odd* k. *Then, for all primes* $p > 3$, $ord_c T_{p^2}(gF) \geq 1$ *at every cusp* c.

Proof of the Lemma. One has $T_{p^2}(gF) = \sum c_i(gF|\alpha_i)$ for certain matrices $\alpha_i \in M_2(\mathbf{Z})$ with $det(\alpha_i) = p^2$. Fix a cusp c of width h and $\alpha \in SL_2(\mathbf{Z})$ with $\alpha(c) = \infty$. Let $q = exp(2\pi i\alpha(z)/h)$ be the local parameter at c. As g has integral order at c, the q-expansion of $gF|\alpha_i\alpha^{-1}$ contains terms q^e with $e = \frac{i}{p^2} + \frac{j}{4}$ for some $i, j \in \mathbf{Z}$, $i \geq 1$, $j \geq 0$. The whole sum $T_{p^2}(gF)|\alpha^{-1}$ will contain only terms q^e with $e = \frac{k}{4}$, $k \in \mathbf{Z}$. The lowest term must be q^e with $e = \frac{i}{p^2} + \frac{j}{4} = \frac{k}{4}$, which can happen only for $p^2|i$, hence $i \geq p^2$ and $e \geq 1$. Lemma is proved.

We now return to the proof of Proposition 6.4. By Lemma 6.5, all T_{p^2} map V_- to $g \cdot M_{1/2}(\Gamma_0(108), (\frac{-3}{\cdot}))$ and V_+ to $g \cdot M_{1/2}(\Gamma_0(108), 1)$. According to [17],

$$M_{1/2}(\Gamma_0(108), (\tfrac{-3}{\cdot})) = \mathbf{C}\theta_3 \oplus \mathbf{C}\theta_{27}$$
$$M_{1/2}(\Gamma_0(108), 1) = \mathbf{C}\theta_1 \oplus \mathbf{C}\theta_9.$$

The claim follows.

(2) According to Corollary 6.2, for any $0 \neq F \in S_{3/2}(\Gamma_0(108), \chi)$, $ord_\infty F \leq 27 - 17/4 < 23$. By checking all coefficients up to q^{22} we coclude that $T_{5^2}F_\pm = 0$, $T_{5^2}G_\pm = 3G_\pm$. As the algebra of Hecke operators is commutative, it follows

that $\mathrm{K}er(T_{5^2}|_{V_\pm}) = \mathbf{C}F_\pm$, $\mathrm{K}er((T_{5^2} - 3\cdot 1)|_{V_\pm}) = \mathbf{C}G_\pm$ are invariant subspaces with respect to the action of all T_{p^2}.

(3) Shimura's correspondence maps any of the functions $F_\pm, G_\pm$ to some Hecke eigenform $F \in M_2(\Gamma_0(54), 1)$. As all eigenvalues λ of T_{5^2} acting on Eisenstein series satisfy $\lambda \equiv 1 \pmod 5$, F must be a cusp form. Inspection of the tables [24, p.117] shows that $S_2(\Gamma_0(54), 1)$ is spanned by the following eigenforms:

$$f = q - 2q^4 - q^7 + 5q^{13} + 4q^{16} + \dots$$
$$f' = q - q^2 + q^4 + 3q^5 - q^7 - q^8 + \dots$$
$$f'' = q + q^2 + q^4 - 3q^5 - q^7 + q^8 + \dots$$

(they correspond to the curves 27B, 54E and 54A respectively, in the notation of [24, p.117]) with $T_5 f = 0$, $T_5 f' = 3f'$, $T_5 f'' = -3f''$, which concludes the proof. □

Put

$$e(n) = \begin{cases} 1, & \text{for } n \not\equiv 5 \pmod 8 \\ \frac{1}{3}, & \text{for } n \equiv 5 \pmod 8 \end{cases}$$
$$c'(n) = c(n) \times \begin{cases} e(n), & \text{for } n < 0 \\ e(-3n), & \text{for } n > 0 \end{cases},$$

where $c(\pm n)$ are the coefficients of

$$F_\pm = \sum_{n=1}^{\infty} c(\pm n) q^n.$$

If D is prime to 3, then $c'(D) = c(D)$, unless $D_- \equiv 5 \pmod 8$.

Theorem 6.6. *Let D be a square-free integer prime to 3. Then*

$$L_D(1) = L(E_D/\mathbf{Q}, 1) = \Omega \Delta^{-1/2} c'(D)^2 \times \begin{cases} 1, & \text{for } D < 0 \\ 3^{1/2}, & \text{for } D > 0 \end{cases},$$

where $\Omega = \frac{1}{2\pi}\Gamma\left(\frac{1}{3}\right)^3$ *and Δ is the conductor of $\left(\frac{D}{\cdot}\right)$.*

Proof. According to [23, p.379], $L_D(1) = A(D)|D|^{-1/2} c(D)^2$, where $A(D)$ depends only on $D \pmod{24}$ and $\mathrm{sgn}(D)$. It is sufficient, therefore, to find the values of $A(D)$ e.g. for $|D| = 7, 10, 13, 19, 22, 73$. To do this, we make use of Stevens' tables in [20, p.199-200]. Stevens tabulates the values of

$$\Lambda(D) = \Delta^{1/2} \Omega^{-1} L_D(1) \times \begin{cases} 1, & \text{for } D < 0 \\ 3^{1/2}, & \text{for } D > 0 \end{cases},$$

as his curve $Y^2 = 4X^3 - 27$ has a real period $\Omega^+ = \Omega \cdot 3^{-1/2}$ and an imaginary period $\Omega^- = \Omega \cdot i$. Inspection of the tables shows that in almost all cases

$$\Lambda(D) = c(D)^2 \times \begin{cases} 1, & \text{for } D < 0 \\ 3, & \text{for } D > 0 \end{cases}$$

Exceptions occur for $D \equiv \begin{cases} 5 \pmod 8, & \text{for } D < 0 \\ 1 \pmod 8, & \text{for } D > 0 \end{cases}$, when $c(D)$ is to be replaced by $c(D)/3$. $\square$

7. Birch and Swinnerton-Dyer's conjecture for E_D.

In this section we examine the rational factor of $L_D(1)$. In the notation of Proposition 4.4, put

$$L_D^*(1) = L_D(1) \left(\int_{E_D(\mathbf{R})} |\omega_{min}|_\infty \right)^{-1} \prod_p c_p^{-1}.$$

Its value is conjecturaly given by

Birch and Swinnerton- Dyer's conjecture:

$$L_D^*(1) = \begin{cases} 0, & \text{for } \mathrm{rk} E_D(\mathbf{Q}) > 0 \\ \frac{\#Ш_D}{(\#E_D(\mathbf{Q})_{tors})^2}, & \text{for } \mathrm{rk} E_D(\mathbf{Q}) = 0 \end{cases},$$

where $Ш_D = Ш(E_D/\mathbf{Q})$ is the Tate-Šafarevič group of E_D.

Proposition 7.1. *Let D be a square-free integer, $|D| \equiv 1 \pmod 3$. Define $\alpha(D)$, $\beta(D)$ by*

$$2^{\alpha(D)} = \prod_{p|D} c_p = \prod_{p|D, p\neq 2} (1 + \#\{x \in \mathbf{F}_p \,|\, x^3 = 2\})$$
$$\beta(D) = \frac{\alpha(D)}{2} + \left\{ \frac{D-1}{2} \right\}$$

Then $\beta(D) = \#\{p|D,\, p = x^2 + 27y^2\} + \frac{1}{2}\#\{p|D,\, p \equiv 2 \pmod 3\}$ *is an integer and*

$$L_D^*(1) = \left(\frac{c'(D)}{2^{\beta(D)}} \right)^2$$

is a rational square.

Proof. From the definitions of $L_D^*(1), \alpha(D), \beta(D)$, Proposition 4.4 and Theorem 6.6 we get

$$\omega_{min} = 2^{2\beta(D) - \alpha(D) + 1} (|D|/\Delta)^{1/2} \omega$$

and

$$\begin{aligned} 2^{2\beta(D)}L_D(1) &= 2^{2\beta(D)}\Omega\Delta^{-1/2}c'(D)^2 \times \begin{cases} 1, & \text{for } D<0 \\ 3^{1/2}, & \text{for } D>0 \end{cases} \\ &= 2^{2\beta(D)+1}c_3(|D|/\Delta)^{1/2}c'(D)^2\int_{E_D(\mathbf{R})}|\omega|_\infty \\ &= 2^{\alpha(D)}c_3c'(D)^2\int_{E_D(\mathbf{R})}|\omega_{min}|_\infty \\ &= c'(D)^2\prod_p c_p\int_{E_D(\mathbf{R})}|\omega_{min}|_\infty \qquad \square \end{aligned}$$

Proposition 7.2. *Let $D\neq 1$ be a square-free integer with $|D|\equiv 1 \pmod 3$. Then*

$$c(D)\equiv \begin{cases} -h(D_-) \pmod 3, & \text{for } D_-\not\equiv 5 \pmod 8 \\ 0 \pmod 3, & \text{for } D_-\equiv 5 \pmod 8 \end{cases},$$

where $h(n)$ denotes the class number of $\mathbf{Q}(\sqrt{n})$ (recall that $D_-=\min(D,-3D)$).

Proof. As $g\equiv -(\theta_1-\theta_9)\theta_3 \pmod 3$,

$$c(\pm|D|)\equiv -N_\pm(|D|) \pmod 3,$$

where

$$\begin{aligned} N_+(a) &= \#\{(x,y,z)\in\mathbf{Z}^3 \mid x^2+3y^2+9z^2=a\}, \\ N_-(a) &= \#\{(x,y,z)\in\mathbf{Z}^3 \mid x^2+3y^2+3z^2=a\}. \end{aligned}$$

The statement of the Proposition is a consequence of the following

Lemma 7.3. *If $a>1$ is a square-free integer, $a\equiv 1 \pmod 3$, then*

$$N_-(a)=h(-a)\times\begin{cases} 4, & \text{for } a\equiv 1,2 \pmod 4 \\ 16, & \text{for } a\equiv 7 \pmod 8 \\ 24, & \text{for } a\equiv 3 \pmod 8 \end{cases}$$

$$N_+(a)=h(-3a)\times\begin{cases} 1, & \text{for } a\equiv 2,3 \pmod 4 \\ 4, & \text{for } a\equiv 5 \pmod 8 \\ 6, & \text{for } a\equiv 1 \pmod 8 \end{cases}$$

Sketch of the proof. We combine two facts:

(1) If $Q=x^2+3y^2+3z^2$ or $Q=x^2+3y^2+9z^2$, then the genus of Q contains only one class of forms.

(2) Siegel's formula for the average number of representstions of a number by classes in a given genus (see e.g. [11]).

Proof of (1) is a routine application of reduction theory (see e.g. [9]) and is omitted, as well as an explicit calculation of all terms in Siegel's formula. □

Corollary 7.4. *For any square-free integer $D \neq 1$, $c'(D)$ is an integer and $L_D^*(1) \in \mathbf{Z}\left[\frac{1}{2}\right]$.*

Corollary 7.5. *If $D \neq 1$ is a square-free integer, $|D| \equiv 1 \pmod 3$ and $D_- \not\equiv 5 \pmod 8$, then*

$$L_D^*(1) \not\equiv 0 \pmod 3 \iff \textit{the Selmer group } S(3, E_D/\mathbf{Q}) = 0.$$

Proof. This follows easily from Theorem 4.6, Proposition 7.1 and Proposition 7.2. □

Remark. A theorem of Rubin [14] implies that for a prime $p > 3$

$$L_D^*(1) \not\equiv 0 \pmod p \implies \text{the Selmer group } S(p, E_D/\mathbf{Q}) = 0.$$

Examination of tables of the coefficients $c(D)$ suggests that a more general congruence

$$c'(D) \equiv -h(D_-) \pmod 3 \tag{7.1}$$

holds for all squre-free $D \neq 1$, $|D| \equiv 1 \pmod 3$. Unfortunately, the above method fails for $D_- \equiv 5 \pmod 8$, because in this case one must take into account also representations of $|D|$ by forms $x^2 + 3y^2 + 27z^2$, $x^2 + 9y^2 + 27z^2$, whose genera contain several classes of forms. If (7.1) was proved, it would make the restriction $D_- \not\equiv 5 \pmod 8$ in Corollary 7.5 unnecessary.

Proposition 7.6. *If D is a square-free integer, $|D| \equiv 1 \pmod 3$, then*

$$c(D) \equiv c(-D) \pmod 2 \qquad \textit{and}$$

$$c(D) \not\equiv 0 \pmod 2 \iff \beta(D) = 0.$$

Proof. Obviously $F_+ \equiv F_- \equiv g = \sum_{n=1}^{\infty} b_n q^n \pmod 2$. If p is a prime, then

$$b_p = \begin{cases} 0, & \text{for } p \equiv 2 \pmod 3 \\ 2, & \text{for } p = x^2 + 27y^2 \\ -1, & \text{for } p \neq x^2 + 27y^2,\ p \equiv 1 \pmod 3 \end{cases},$$

or, equivalently, $b_p = \#\{x \in \mathbf{F}_p \,|\, x^3 = 2\} - 1$. Let $|D| = p_1 \dots p_k$. As g is a Hecke eigenform, b_n is a multiplicative function, so

$$c(D) \equiv c(-D) \equiv b_{|D|} = b_{p_1} \dots b_{p_k} \pmod 2$$

and $b_{|D|} \not\equiv 0 \pmod 2 \iff$ no prime $p|D$ is of the form $p \equiv 2 \pmod 3$ or $p = x^2 + 27y^2 \iff \beta(D) = 0$. $\square$

Corollary 7.7. *If D is a squre-free integer, $|D| \equiv 1 \pmod 3$ and $c(D) \not\equiv 0 \pmod 2$, then $L_D^*(1) = c'(D)^2$ is an odd square and the Selmer group $S(2, E_D/\mathbf{Q}) = 0$ vanishes.*

Proof. In [2] Aigner proves that $\beta(D) = 0 \Longrightarrow S(2, E_D/\mathbf{Q}) = 0$. $\square$

We conclude with a list of conjectural values of $\#Ш_D$ for square-free $|D| < 500$ with $L_D^*(1) \neq 0, 1$:

$$\begin{aligned}
\#Ш_D = \quad \underline{\mathbf{4}}: \quad & -58, -82, -85, -142, -166, -235 \\
& -253, -301, -346, -391, -406, -445 \\
& -454, -457, -466 \\
& 127, 166, 262, 298, 358, 403, 433 \\
& 445, 466, 478 \\
\underline{\mathbf{9}}: \quad & -61, -118, -139, -157, -199, -211 \\
& -214, -241, -247, -274, -277, -286 \\
& -331, -334, -367, -370, -379, -493 \\
& 67, 79, 103, 139, 151, 181, 199, 238 \\
& 247, 271, 322, 331, 337, 418, 427, 469 \\
\underline{\mathbf{16}}: \quad & -478 \\
& 451 \\
\underline{\mathbf{25}}: \quad & -133, -313, -349, -469, -481 \\
& 211, 259, 367 \\
\underline{\mathbf{36}}: \quad & \\
\underline{\mathbf{49}}: \quad & -373
\end{aligned}$$

References

1. A.Aigner, *Weitere Ergebnisse über $x^3 + y^3 = z^3$ in quadratischen Körpern*, Monatsh. Math. **56** (1952), 240-252.
2. ———, *Ein zweiter Fall der Unmöglichkeit von $x^3 + y^3 = z^3$ in quadratischen Körpern mit durch 3 teilbarer Klassenzahl*, Monatsh. Math. **56** (1952), 335-338.
3. J.W.S.Cassels, *Arithmetic on curves of genus 1,I*, J.Reine Angew. Math. **202** (1959), 52-99.
4. ———, *Arithmetic on curves of genus 1,VIII*, J. Reine Angew. Math. **217** (1965), 180-199.
5. ———, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193-291.
6. G.Frey, *Die Klassengruppe quadratischer und kubischer Zahlkörper und die Selmer-Gruppen gewisser elliptische Kurven*, Manuscripta Math. **16** (1975), 333-362.
7. R.Fricke, *Die elliptischen Funktionen und ihre Anwendungen*, Teubner-Verlag, Leipzig-Berlin, 1922.
8. R.Fueter, *Die diophantische Gleichung $\xi^3 + \eta^3 + \zeta^3 = 0$*, Sitz.-Ber.Akad.Wiss. Heidelberg (1913).
9. E.Grosswald, *Representations of Integers as Sums of Squares*, Springer-Verlag, New York, 1985.
10. K.Ireland, M.Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics vol.87, Springer-Verlag, New York, 1982.
11. J.Milnor, D.Hucemoller, *Symmetric bilinear forms*, Springer-Verlag, Berlin, 1983.
12. M.Newman, *Construction and application of a class of modular functions*, Proc. London Math. Soc.(3) **7** (1957), 334-350.
13. H.Reichardt, *Aritmetische Theorie der Kubischen Körper als Radikalkörper*, Monatsh. Math. Phys. **40** (1933), 323-350.
14. K.Rubin, *Tate-Šafarevič groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560.
15. A.Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201-203.
16. J.-P.Serre, *Algebraic Number Fields*, ed. by A.Fröhlich, Acad. Press, 1977, pp. 193-268.
17. J.-P.Serre, H.Stark, *Lecture Notes in Math. vol. 627*, Springer-Verlag, Berlin, 1977, pp. 29-68.
18. G.Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton Univ. Press, 1971.
19. ———, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), 440-481.
20. G.Stevens, *Arithmetic of Modular Curves*, Progress in Math. vol. 20, Birkhäuser, Boston, 1982.
21. J.Tate, *Lecture Notes in Math. vol. 476*, Springer-Verlag, Berlin, 1975, pp. 33-52.
22. J.-L.Waldspurger, *Correspondance de Shimura*, J. Math. Pures et Appl. **59** (1980), 1-132.
23. ———, *Sur les coefficiemts de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.
24. *Numerical tables on elliptic curves*, Lect. Notes in Math. vol. 476, Springer Verlag, Berlin, 1975, pp. 74-144.