Properties of Twists of Elliptic Curves

J.A. Antoniadis, M. Bungert and G. Frey

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

Federal Republic of Germany

MPI–88/68

Properties of Twists of Elliptic Curves

J.A.Antoniadis, M.Bungert and G.Frey

Nr. 68

Properties of Twists of Elliptic Curves

J.A.Antoniadis,[1] M.Bungert and G.Frey[2]

§1 Rank estimates by Galois descent

Let E/Q be an elliptic curve with absolute invariant j_E, minimal discriminant Δ_E and conductor N_E (cf. [Si]). Let d be a square free integer.

Definition 1.1. χ_d is the Dirichlet character corresponding to $Q(\sqrt{d})/Q$, and E_d is the twist of E by χ_d, i.e. E_d is an elliptic curve over Q not isomorphic to E over Q but over $Q(\sqrt{d})$.

The purpose of the following paper is to describe some methods which can be used to relate arithmetical properties of E_d to properties of $Q(\sqrt{d})$ at least for special curves E. We are especially interested in criterions for the property that $E_d(Q)$ is a finite group.

One method to find such criterions is to use Galois cohomology and to try to compute a part of the Selmer group of E_d over Q.

Let us recall the definition of this group.
For a field K we denote by G_K its absolute Galois group. Let n be a natural number. The exact sequence

$$0 \longrightarrow E_d(\bar{Q})_n \longrightarrow E_d(\bar{Q}) \xrightarrow{\cdot n} E_d(\bar{Q}) \longrightarrow 0$$

gives rise to the sequence

$$0 \longrightarrow E_d(Q)/nE_d(Q) \xrightarrow{\delta} H^1(G_Q, E_d(\bar{Q})_n) \xrightarrow{\varphi} H^1(G_Q, E_d(\bar{Q}))_n \longrightarrow 0 .$$

(As usual $E(K)$ denotes the group of K-rational points of E over a field $K \supset Q$, $E(K)_n$ is the subgroup of points of order dividing n, and $\bar{Q}$ is the algebraic closure of Q.)

Let $\mathfrak{p}$ be a (finite or infinite) place of Q, $Q_\mathfrak{p}$ the completion of Q with respect to $\mathfrak{p}$ (i.e. $Q_\mathfrak{p} = \mathbb{R}$ if $\mathfrak{p}$ corresponds to the absolute value, and $Q_\mathfrak{p} = Q_p$ if $\mathfrak{p}$ is the p-adic place for a prime p). We choose an embedding of $\bar{Q}$ to $\bar{Q}_\mathfrak{p}$ and hence we get an inclusion of $G_{Q_\mathfrak{p}}$ into G_Q.

---

[1] The first author would like to express his gratitude to Fachbereich 9 Mathematik of the University Saarbrückeh and MPI-für Mathematik Bonn, for their hospitality.

[2] This paper was partly written during a visit of the third author at the Centre de Recerca Mathematica of the Institut d'Estudis Catalans at Bellaterra. He wishes to express his gratitude for the support and the warm hospitality provided by this institution which made the visit to a very pleasant one.

The natural restriction maps yield the following commutative exact diagram for every set T of places of Q:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & E_d(Q)/nE_d(Q) & \xrightarrow{\delta} & S_T(E_d,Q)_n & \longrightarrow & Ш_T(E_d,Q)_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod\limits_{\substack{p\notin T \\ p \text{ place of } Q}} E_d(Q_p)/nE_d(Q_p) & \longrightarrow & \prod\limits_{\substack{p\notin T \\ p \text{ place of } Q}} H^1(G_{Q_p},E_d(\bar{Q})_n) & \longrightarrow & \prod\limits_{\substack{p\notin T \\ p \text{ place of } Q}} H^1(G_{Q_p},E_d(\bar{Q}_p))_n & \longrightarrow & 0
\end{array} \tag{1.2}$$

where $Ш_T(E_d,Q)_n \subset H^1(G_Q,E_d(\bar{Q}))_n$ is the intersection of the kernels of the restriction maps from $H^1(G_Q,E_d(Q))_n$ to $H^1(G_{Q_p},E_d(\bar{Q}_p))$ for all places of Q not concontained in T and $S_T(E_d,Q)_n := \varphi^{-1}(Ш_T(E_d,Q)_n)$.

<u>Definition 1.3.</u> $Ш_T(E_d,Q)_n$ is the n-part of the Tate-Shafarevic group for E_d over Q with respect to T, and $S_T(E_d,Q)_n$ is the n-part of the Selmer group of E_d over Q with respect to T. If $T = \emptyset$ we omit the index T, and get $Ш(E_d,Q)_n$ (resp. $S(E_d,Q)_n$) as the n-part of <u>the</u> Tate-Shafarevic group (resp. Selmer group) of E_d over Q.

It is important that for all n and T $S_T(E_d,Q)_n$ is finite and can, at least in principle, be computed. Hence one gets estimates for $\mathrm{rank}_{\mathbb{Z}}(E_d(Q))$ if one can estimate $\mathrm{rank}_{\mathbb{Z}/n}(S_T(E_d,Q))_n$.

It should be mentioned here that there is no algorithm known which computes $\mathrm{rank}_{\mathbb{Z}}(E_d(Q)) =: r_{E_d}$ or $\#(Ш(E_d,Q)_n)$ separately. It is conjectured that $Ш_T(E_d,Q) := \bigcup_{n\in\mathbb{N}} Ш_T(E_d,Q)_n$ is finite and that r_{E_d} and $\#(Ш(E_d,Q))$ can be computed with the help of the L-series of E. We'll come to this conjecture of Birch and Swinnerton-Dyer later on (cf. [Si], and for new results [Ru1], [Ru2], [Ko1]).

The following result is useful to compute $S_T(E_d,Q)_n$:

<u>Proposition 1.4 (Special case of the theorem of Tate-Bashmakov).</u> Let T be a set of places of Q containing all divisors of $n\cdot N_{E_d}\cdot\infty$. Let K_n be the field obtained by adjoining the coordinates of all points of order n of E_d to Q and let $K_{n,T}$ be the maximal abelian extension of K of exponent n and unramified outside of T. Then

$$\mathrm{res}_{Q/K_n}(S_T(E_d,Q)_n) \subset \mathrm{Hom}_{G(K_n/Q)}(G(K_{n,T}/K_n),E_d(\bar{Q})_n).$$

Here res_{Q/K_n} is the restriction map: $H^1(G_Q, E_d(\overline{Q})_n) \longrightarrow H^1(G_{K_n}, E_d(\overline{Q})_n)$. Its kernel is $H^1(G(K_n/Q), E_d(\overline{Q})_n)$ which is of order at most equal to n and whose intersection with $S_T(E_d, Q)_n$ is equal to $\{0\}$ in many cases.

In [Fr1] we used proposition 1.4 to get information about $S(E_d, Q)_p$ in the case that E has a Q-rational point of order p with p an odd prime. To formulate the result we need some notation.

1. For a prime q let K_q be an extension field of Q_q such that E has semi-stable reduction over K_q. Let $P \in E(\overline{K}_q)$. P is reduced to ∞ mod q if the image of P in the Néron model $\mathcal{E}$ of E over $K_q(P)$ is reduced to the neutral element of the special fibre of $\mathcal{E}$.

2. $S_{E,p} := \{q \mid N_E : q \neq 2,\ q \equiv -1 \bmod p,\ v_q(\Delta_E) \not\equiv 0 \bmod p\}$ and

$\tilde{S}_{E,p} := \{q \in S_{E,p} : v_q(j_E) < 0\}$.

Proposition 1.5 (cf. [Fr 1]. Let p be an odd prime such that E has a Q-rational point of order p. Assume that either E: $Y^2 = X^3+1$ (hence p = 3) or that P is not reduced to ∞ mod p. Let d be a square free negative integer prime to pN_E with

i) If $2 \mid N_E$ then $d \equiv 3 \bmod 4$.

ii) if $v_p(j_E) < 0$ then $\left(\frac{d}{p}\right) = -1$.

iii) for $q \mid N_E$ but $q \notin \{2, p, S_{E,p}\}$ then

$$\left(\frac{d}{q}\right) = \begin{cases} -1 & \text{if } v_q(j_E) \geq 0 \text{ or } v_q(j_E) < 0 \text{ and } E/Q_q \text{ is a Tate curve,} \\ 1 & \text{otherwise.} \end{cases}$$

Let $Cl(d)_p$ be the p-part of the class group of $Q(\sqrt{d})$. Then

$$\# Cl(d)_p \mid \# S(E_d, Q)_p \mid Cl(d)_p^2 \cdot s_E$$

with an integer s_E depending on $\tilde{S}_E$ only, with $s_E = 1$ if $\tilde{S}_E = \emptyset$.

Hence $p \mid \# Cl(d)_p$ if and only if $p \mid \# S(E_d, Q)_p$, and so especially:

$$\mathrm{rank}_{\mathbb{Z}} E_d(Q) = 0 \text{ if } p \nmid \# Cl(d)_p .$$

Due to a theorem of Mazur one knows that p can be equal to 3, 5 and 7; and for each of these numbers one has infinitely many curves for which one can apply the proposition.

We list some examples taken from the tables in [MFIV]:

1. For p = 3:

Name of the curve E	$S_E = \tilde{S}_E$	congruence conditions for d
14C		$\left(\frac{d}{7}\right) = -1$, $d \equiv 3 \bmod 4$
19B		$\left(\frac{d}{19}\right) = -1$
26B		$\left(\frac{d}{13}\right) = -1$, $d \equiv 3 \bmod 4$
35B		$\left(\frac{d}{5}\right) = -1$, $\left(\frac{d}{7}\right) = -1$
36A	$\emptyset$	$d \equiv 3 \bmod 4$
37C		$\left(\frac{d}{37}\right) = -1$
38D		$\left(\frac{d}{19}\right) = -1$, $d \equiv 3 \bmod 4$
77D		$\left(\frac{d}{7}\right) = -1$, $\left(\frac{d}{11}\right) = 1$
84C		$\left(\frac{d}{7}\right) = -1$, $d \equiv 11 \bmod 12$
91B		$\left(\frac{d}{7}\right) = -1$, $\left(\frac{d}{13}\right) = -1$
20B	5	$d \equiv 3 \bmod 4$
30A	5	$d \equiv 11 \bmod 12$
34A	17	$d \equiv 3 \bmod 4$
44A	11	$d \equiv 3 \bmod 4$
51A	17	$d \equiv 2 \bmod 3$
66A	11	$d \equiv 11 \bmod 12$
92A	23	$d \equiv 3 \bmod 4$

2. For $p = 5$:

Name of the curve E	$S_E = \tilde{S}_E$	congruence conditions for d
$11B = X_o(11)$		$\left(\frac{d}{11}\right) = -1$
$66I$		$\left(\frac{d}{11}\right) = -1$, $d \equiv 11 \bmod 12$
$110C$	$\emptyset$	$d \equiv 3 \bmod 4$, $\left(\frac{d}{5}\right) = \left(\frac{d}{11}\right) = -1$
$123A$		$d \equiv 2 \bmod 3$, $\left(\frac{d}{41}\right) \equiv -1$
$186B$		$d \equiv 11 \bmod 12$, $\left(\frac{d}{31}\right) = -1$
$38A$	19	$d \equiv 3 \bmod 4$
$57F$	19	$d \equiv 2 \bmod 3$
$58B$	29	$d \equiv 3 \bmod 4$
$118B$	59	$d \equiv 3 \bmod 4$
$158H$	79	$d \equiv 3 \bmod 4$

3. For $p = 7$:

Name of the curve E	$S_E = \tilde{S}_E$	congruence conditions for d
$174G$	$\emptyset$	$d \equiv 11 \bmod 12$, $\left(\frac{d}{29}\right) = -1$
$26D$	13	$d \equiv 3 \bmod 4$

Next we describe how to estimate the rank of $E_d(Q)$ by 2-descent. We study the $G_d \coloneqq G(Q(\sqrt{d})/Q)$-module $E(Q(\sqrt{d}))$. Since

$$\operatorname{rank}_{\mathbb{Z}}(E_d(Q)) + \operatorname{rank}_{\mathbb{Z}}(E(Q)) = \operatorname{rank}_{\mathbb{Z}}(E(Q(\sqrt{d}))$$

we can use the theorem of Tate-Chevalley about Herbrand quotients to get

$$\text{(1.8)} \quad \operatorname{rank}_{\mathbb{Z}} E_d(Q) = \operatorname{rank}_{\mathbb{Z}}(E(Q)) - h_d^0(E) + h_d^1(E) \quad \text{with}$$
$$h_d^1(E) := \log_2 \# (H^1(G_d, E(Q(\sqrt{d})))).$$

The following easy lemma can be useful if one wants to estimate $h_d^0(E)$.

Lemma 1.9. Let q be a prime dividing d but $q \nmid 2N_E$. Then

$$P \in N_{Q_q(\sqrt{d})/Q_q}(E(Q_q(\sqrt{d}))) \quad \text{if and only if } P \in 2E(Q_q).$$

Proof. E has good reduction modulo q, and the kernel E_- of the reduction is uniquely divisible by 2. Hence P is in the image of the norm map from $E(Q_q(\sqrt{d}))$ to $E(Q_q)$ if and only if its image $\overline{P}$ in $E(Q_q)/E_-(Q_q)$ is in the image of the norm. Since $q \mid d$ G_d acts trivially on this quotient, and so the lemma follows.

We give two examples which illustrate how one can use lemma 1.9:

1. E: $Y^2 = X^3+1$.
$P = (-1,0)$ is a point of order 2. The Galois closure of $Q(\frac{1}{2}P)$ is equal to $Q(\sqrt{-1}, \sqrt[4]{-3})$. Hence $P \notin N_{Q(\sqrt{d})/Q}(E(Q(\sqrt{d})))$ if there is a prime $q \mid d$, $q \nmid 6$, which is not completely split in $Q(\sqrt{-1}, \sqrt[4]{-3})/Q(\sqrt{-3})$, and in this case we have $\mathrm{rank}_{\mathbb{Z}}(E_d(Q)) = h^1_d(E)-1$.

2. E = 17C; i.e. E is the strong modular curve with conductor 17.
Let $f_E(z) = \sum_{i=1}^{\infty} a_i q^i$ be the corresponding cusp form.
If q is a prime with $q \mid d$, $q \nmid 34$ and $8 \nmid a_q-(q+1)$ then $h^0_d(E) \geq 2$ and hence $\mathrm{rank}_{\mathbb{Z}}(E_d(Q)) = h^1_d(E)-2$.

To discuss $h^1_d(E)$ we choose a suitable set T of places of Q and look at the map

$$\alpha_T(d): H^1(G_d, E(Q(\sqrt{d}))) \longrightarrow \prod_{\substack{p \notin T \\ p \text{ place of } Q}} H^1(G(Q_p(\sqrt{d})/Q_p), E(Q_p(\sqrt{d})))$$

and estimate the image of α_T by computing the order of the local groups. This computation is straight-forward, and we summarize the result in

Lemma 1.10 Assume that d is a square free integer and

$$\gcd(N_E, d) = \gcd(N_E, d^2).$$

Then

$$\# \operatorname{im}(\alpha_T(d)) \leq \mu_\infty \cdot \mu_2 \prod_1 \# E(Q_q)_2 \cdot \prod_2 c^0_q(E) \prod_3 2$$

with

$\mu_\infty = 1$ if $d > 0$ or $\Delta_E < 0$ or $\infty \in T$, and $\mu_\infty \le 2$ in all other cases,

$\mu_2 = 1$ if $d \equiv 1 \bmod 8$ or $d \equiv 1 \bmod 4$ and $2 \nmid N_E$ or $2 \| N_E$ and $v_2(j_E)$ odd or $2 \in T$, and

$\mu_2 \le 2$ in all other cases,

$\prod_1$ is to be taken over all odd primes $q \mid d$, $q \notin T$ and $q \nmid N_E$.

$\prod_2$ is to be taken over all odd primes $q \mid N_E$, $q \in T$ and $q \nmid d$ with $\left(\frac{d}{q}\right) = -1$ and $c_q^0(E)$ denotes the number of elements of order 2 in the group of connected components of the special fibre of the Néron model of E/Q_q,

$\prod_3$ runs over all odd primes $q \notin T$, $q \mid \gcd(N_E, d)$ with $\left(\frac{j_E \cdot d}{q}\right) = 1$.

It is obvious that the estimate for $\# \operatorname{im} \alpha_T(d)$ is unrealistic large if E or d is "complicated". But it can be useful in simple cases as the following example shows:

Example 1.11. Assume that E is a curve with prime conductor $N_E = p$, and assume that d is prime to 2p. Then

$$\# \operatorname{im} \alpha_T(d) \le 2^{\delta_\infty} \cdot \prod_{\substack{q \mid \Delta_{Q(\sqrt{d})/Q} \\ q \notin T}} \# E(Q_q)_2 \cdot 2^{\delta_p}$$

with $\delta_\infty \le 1$, and $\delta_\infty = 0$ if either $\infty \in T$ or $d > 0$ or $\Delta_E < 0$ and $\delta_p \le 1$, and $\delta_p = 0$ if either $\left(\frac{d}{p}\right) = 1$ or $v_p(j_E)$ odd.

We specialize even more:

1. Take $T = \{\infty\}$ and assume that $E(Q)_2 = \{0\}$. Assume moreover that for all divisors q of the discriminant of $Q(\sqrt{d})/Q$ one has: q is not split in $Q(E(\bar{Q})_2)/Q(\sqrt{\Delta_E})$. Then $\# \operatorname{im} \alpha_{\{\infty\}}(d) = 1$.
One should remark that $Q(E(\bar{Q})_2)/Q(\sqrt{\Delta_E})$ is an extension of degree 3 contained in the class field of $Q(\sqrt{\Delta_E})$ with conductor 2, and hence by a "higher reciprocity law" (cf. [A]) we get a criterion for $\alpha_{\{\infty\}}(d) = \{0\}$.

A specific elliptic curve which satisfies the conditions made above is $X_0(11)$.

2. If $E(Q)_2 = \mathbb{Z}/2$ (for instance E = 17D) then our estimate for $\# \operatorname{im} \alpha_T(d)$ is very bad if d has a lot of prime divisors. But assume that d = q is a prime

with $q \equiv 1 \bmod 4$, $\left(\frac{q}{p}\right) = 1$ if $v_p(j_E) \equiv 0 \bmod 2$ and $E(\mathbb{Q}_q)_2 = \mathbb{Z}/2$. Then $\# \operatorname{im} \alpha_{\{\infty\}}(d) \leq 2$.

After having estimated $\# \operatorname{im} \alpha_T(d)$ it remains to estimate $\# \ker \alpha_T(d)$ in order to estimate $h^1_d(E)$.
For $\varphi \in S_T(E,\mathbb{Q})_2$ let f_φ be the curve of genus 1 corresponding to the class of φ in $H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}}))$. Then

$$t(d) := \# \ker \alpha_T(d) = \frac{\#\{\varphi \in S_T(E,\mathbb{Q})_2;\ f_\varphi \text{ has a rational point in } \mathbb{Q}(\sqrt{d})\}}{\#(E(\mathbb{Q})/2E(\mathbb{Q}))} .$$

It will be difficult in general to compute $t(d)$ exactly, so one will have to be content to estimate $t(d)$ by

$$\# S_T(E,\mathbb{Q})_2 / \# (E(\mathbb{Q})/2E(\mathbb{Q}))$$

(and to hope that this number is small).

For instance we can come back to the curves discussed in example 1.11. We get

<u>Proposition</u> <u>1.12.</u> Assume that E has prime conductor $N_E = q$ and that $E(\mathbb{Q})_2 = \{0\}$. Then

$$\# S_{\{\infty\}}(E,\mathbb{Q})_2 \leq \#\{\text{conjugacy classes of fields } K/\mathbb{Q};\ \deg K/\mathbb{Q} = 4,\ G(\tilde{K}/\mathbb{Q}) = S_4 \text{ and } \Delta_{K/\mathbb{Q}} \mid 2^4 \cdot q\} .$$

Especially

$$S_{\{\infty\}}(X_0(11))_2 = \{0\} ,$$

and so

$$t(d) = 1 \quad \text{for all } d \text{ if } E = X_0(11) .$$

<u>Proof.</u> If $v_q(\Delta_E) \equiv 0 \bmod 2$ then $\mathbb{Q}(E(\bar{\mathbb{Q}})_2)$ would be an extension of degree 3 of $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{-1})$ unramified outside of 2, and since such an extension doesn't exist we conclude that $v_q(\Delta_E)$ is odd and that $\mathbb{Q}(E(\bar{\mathbb{Q}})_2)/\mathbb{Q}$ has Galois group S_3, q is decomposed in $\mathbb{Q}(E(\bar{\mathbb{Q}})_2)/\mathbb{Q}(\sqrt{\Delta_E})$ and ramified in $\mathbb{Q}(\sqrt{\Delta_E})/\mathbb{Q}$.

An element $\varphi \in S_{\{\infty\}}(E,Q)_2 \setminus \{0\}$ corresponds to an element

$$\tilde{\varphi} \in \mathrm{Hom}_{S_3}(G_{Q(E(\bar{Q})_2)}, E(\bar{Q})_2) \setminus \{0\}$$

since

$$H^1(S_3, E(\bar{Q})_2) = 0 .$$

Let K_φ be the fixed field of the kernel of $\tilde{\varphi}$. Then K_φ is a Galois extension of Q with Galois group S_4 which is unramified outside $2\cdot q$ over Q (use proposition 1.4 and the invariance of $\tilde{\varphi}$ under S_3). Moreover $\tilde{\varphi}$ (and so φ) is uniquely determined by K_φ. Hence φ is uniquely determined by the conjugacy class of an extension $K_{0,\varphi}$ of degree 4 over Q whose Galois closure over Q has Galois group S_4 and whose discriminant divides a power of 2q. Now we use the local triviality of $\mathrm{res}_q \varphi$ in $H^1(G_{Q_q}, E(\bar{Q}))$ to get that $\mathrm{res}_q \varphi$ is split in $H^1(G_{Q_q}, E(\bar{Q})_2)$ by an unramified extension. (One has to solve the equation $\frac{1}{2} Q_0 = Q$ with $Q_0 \in E_q(Q_q)$, and since $v_q(j_E) \equiv 1 \bmod 2$ this equation has a solution in an unramified extension of Q_q.) So the discriminant of $K_{0,\varphi}/Q$ is equal to $2^\alpha \cdot q$, and by analoguous considerations one can estimate α by 4.

The next special case is that E has prime conductor q but $E(Q)_2 = \mathbb{Z}/2$. After applying an isogeny of degree 2 if necessary, we can assume that $v_q(j_E) \equiv 1 \bmod 2$. We get

Proposition 1.13. Assume that E/Q has prime conductor q, that $E(Q)_2 = \mathbb{Z}/2$ and that $v_q(j_E) \equiv 1 \bmod 2$. Then $Ш_{\{\infty\}}(E,Q)_2 = \{0\}$ and so $t(d) = 1$ for all d.

Proof. Let P be a point of order 2 in E(Q). By assumption the reduction of P modulo q is in the connected component of the unity of the Néron model of E modulo q.
Since $Q(E(\bar{Q})_2) = Q(\sqrt{\gamma q})$ with $\gamma = \pm 1$ we can represent $\varphi \in S_{\{\infty\}}(E,Q)_2$ by $\tilde{\varphi} \in \mathrm{Hom}_{G(Q(\sqrt{\gamma p})/Q)}(G_{Q(\sqrt{\gamma p})}, E(\bar{Q})_2)$.
Let K_φ be the fixed field of the kernel of $\tilde{\varphi}$ with $G(K_\varphi/Q(\sqrt{\gamma p})) = \langle \varepsilon_1, \varepsilon_2 \rangle$, $\varepsilon_1^2 = \mathrm{id}$. For $\langle \tau \rangle = G(Q(\sqrt{\gamma p})/Q)$ and $Q \in E(\bar{Q}) \setminus \langle P \rangle$ one has $\tau Q = P + Q$

First case: Assume that $\langle \varepsilon_1, \varepsilon_2 \rangle = \langle \varepsilon \rangle$ with $\varepsilon \neq \mathrm{id}$.
Since $\tau \varepsilon \tau = \varepsilon$ the invariance of $\tilde{\varphi}$ under τ yields: $\varphi(\varepsilon) = P$. Using the triviality of φ in $H^1(G_{Q_q}, E(\bar{Q}_q))$ we conclude as in the proof of proposition 1.12 that $K_\varphi/Q(\sqrt{\gamma q})$ is unramified at q and so K_φ/Q cannot be cyclic, hence $K_\varphi = Q(\sqrt{\gamma p}, \sqrt{\mu})$ with $\mu \in \{-1, 2, -2\}$ (since $K_\varphi/Q(\sqrt{\gamma p})$ is unramified outside of 2).

Now E has good reduction modulo 2 and hence the triviality of φ in $H^1(G_{Q_2}, E(\bar{Q}_2))$ implies that K_φ/Q is "little" ramified (cf. [Fr1]) at 2 and so $\mu = -1$, $K_\varphi = Q(\sqrt{q}, \sqrt{-1}) = Q(\frac{1}{2}P)$, and so φ corresponds to δP.

Second case: $\# \langle \varepsilon_1, \varepsilon_2 \rangle = 4$.
We can assume that $\tau\varepsilon_1\tau = \varepsilon_2$ and so $\tau\varepsilon_1\varepsilon_2\tau = \varepsilon_1\varepsilon_2$. Hence $\varphi(\varepsilon_1\varepsilon_2) = P$, $\varphi(\varepsilon_1) = Q$ and $\varphi(\varepsilon_2) = P+Q$ for some $Q \in E_2 \backslash \langle P \rangle$.
Now Q and P+Q are not in the connected component of the unity of E modulo q, and since $\mathrm{res}_q\varphi$ has to be trivial in $H^1(G_{Q_q}, E(\bar{Q}_q))$ it follows that all divisors of q are decomposed in $K_\varphi/K_\varphi^{\langle\varepsilon_i\rangle}$ for i = 1, 2. So $K^{\langle\varepsilon_1\varepsilon_2\rangle}/Q$ is not cyclic and unramified outside of 2, and hence one sees as above that $K_\varphi^{\langle\varepsilon_1\varepsilon_2\rangle} = Q(\sqrt{q}, \sqrt{-1})$, and, since q has to be decomposed in $K_\varphi^{\langle\varepsilon_1\varepsilon_2\rangle}/Q(\sqrt{\gamma q})$, $q \equiv 1 \bmod 4$.

Now look at the behaviour of K_φ at the prime 2.
Firstly we remark that E has good ordinary reduction over Q_2 and that P is in the kernel of the reduction modulo 2 and so P+Q and Q are not in this kernel over $K_{\varphi,\mathfrak{p}_2}$ where $\mathfrak{p}_2$ is a place of K_φ dividing 2. This implies that $K_\varphi/K_\varphi^{\langle\varepsilon_i\rangle}$ is unramified at all divisors of 2, and so $Q(\sqrt{-1}, \sqrt{p})$ is unramified over $Q(\sqrt{\gamma p})$. It follows that $\gamma = -1$ and $K_\varphi = Q(\sqrt{-1}, \sqrt{p}, \sqrt{\pi_2})$ with π_2 a uniformizing element at the unique extension of 2 in $Q(\sqrt{-p})$. But this contradicts the fact that φ is split by an extension of $Q(E(\bar{Q})_2)$ which is "little ramified" at divisors of 2, and so we get the assertion of proposition 1.13.

To end this section we summarize our results we got by 2-descent in special cases to get some kind of counterpart of proposition 1.5 for p = 2:

<u>Proposition 1.14.</u> Assume that E is an elliptic curve with prime conductor q and $\mathrm{rank}_{\mathbb{Z}}(E(Q)) = 0$.

i) If $E(Q)_2 \cong \mathbb{Z}/2$ and d is a prime with $d \equiv 3 \bmod 4$ and $(\frac{\Delta_E}{d}) = -1$ then $\mathrm{rank}_{\mathbb{Z}}\, E_{-d}(Q) = 0$.

ii) If $E(Q)_2 = \{0\}$ and d is a square free integer such that for all q|d one has that q is not split in $Q(E(\bar{Q})_2)/Q(\sqrt{\Delta_E})$ then $\mathrm{rank}_{\mathbb{Z}}\, E_d(Q) = \log_2 t(d)$, and so $\mathrm{rank}_{\mathbb{Z}}\, E_d(Q) = 0$ if there is no extension K/Q of degree 4 with Galois group S_4 and discriminant dividing $2^4 q$.

<u>Examples 1.15.</u>

i) E = (17D) has conductor 17, $\Delta_E = 17$ and $E(Q)_2 = \mathbb{Z}/2$, $\mathrm{rank}_{\mathbb{Z}}\, E(Q) = 0$. Hence $E_{-p}(Q)$ has rank zero if $p \equiv 3 \bmod 4$ and $(\frac{17}{p}) = (\frac{p}{17}) = -1$, i.e. p has to satisfy linear congruence conditions.

ii) $E = X_0(11)$ has rank zero and no point of order 2 over Q, $Q(E(\bar{Q})_2) = Q(\sqrt{-11})_{(2)}$, the class field of $Q(\sqrt{-11})$ with conductor 2. Hence $\mathrm{rank}_{\mathbb{Z}}(X_0(11)_d(Q)) = 0$ if for all $q \mid d$ q is not split in $Q(\sqrt{-11})_{(2)}/Q(\sqrt{-11})$. (Of course a necessary condition for this is that $\left(\frac{-11}{q}\right) = 1$.)

§2 On the value of the L-series of E at s = 1

In this section we recall briefly the conjectured relation between the analytic behaviour of the L-series $L_E(s)$ of elliptic curves E at s = 1 and its arithmetical properties (Conjecture of Birch and Swinnerton-Dyer); this motivates the usefulnes of a method of Tunnell ([Tu]) based on a theorem of Waldspurger ([Wa]) which makes it possible to compute $L_{E_d}(1)$ for twists of many elliptic curves.

1. The conjecture of Birch and Swinnerton-Dyer

From now on we'll assume that E is a modular elliptic curve, i.e. there is a non-trivial Q-morphism

$$\varphi\colon X_0(N_E) \longrightarrow E$$

where $X_0(N_E)$ is the modular curve parametrizing elliptic curves with cyclic isogenies of degree N_E. (For details cf. [Sh 1].)
Let ω_E be the Néron differential of E. Then

$$\varphi^*(\omega_E) = c \cdot f_E \cdot \frac{dq}{q} \quad \text{with}$$

$$c \in Q^\times,\ q = e^{2\pi i z} \text{ and } f_E = 1 + \sum_{l=2}^{\infty} a_l q^l \in S_2(N_E)(\mathbb{Z}),$$

the ring of cusp forms of weight 2 and level N_E defined over $\mathbb{Z}$. Moreover f_E is an eigenfunction under the operation of the Hecke algebra, for primes $l \nmid N_E$ and the Hecke operator T_l one has:

$$a_l = 1 + l - \# E^{(l)}(\mathbb{Z}/l)$$

is the eigenvalue of T_l where $E^{(l)}$ is the reduction of E modulo l.
It follows that the L-series of E defined by

$$L_E(s) := \prod_{l \mid N_E} (1 - a_l l^{-s})^{-1} \cdot \prod_{l \nmid N_E} (1 - a_l l^{-s} + l^{1-2s})^{-1}$$

is (essentially) the Mellin transform of f_E and hence has analytic continuation to $\mathbb{C}$ satisfying a functional equation under the transformation $s \longrightarrow 2-s$.

Conjecture 2.1 (Birch and Swinnerton-Dyer).
1. The order of zero of $L_E(s)$ at $s = 1$ is equal to $r_E := \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$.
2. Let $L^{(r_E)}(s)$ be the r_E-th derivative of L_E. Then

$$L_E^{(r_E)}(1) = r_E!\ \det(h_E) \cdot \int_{E(\mathbb{R})} \omega_E \prod_{p|N} c_p \cdot \frac{\# Ш(E,\mathbb{Q})}{(\# E(\mathbb{Q})_{tor})^2}$$

where ω_E is the Néron differential of E, h_E the Néron-Tate height on $E(\mathbb{Q})$ which is a quadratic form, $\det(h_E)$ its regulator, and $c_p = [E(\mathbb{Q}_p):E_0(\mathbb{Q}_p)]$ with $E_0(\mathbb{Q}_p)$ the subgroup of $E(\mathbb{Q}_p)$ whose image in the special fibre of the Néron model of E over $\mathbb{Q}_p$ is non singular.

Remark. The conjecture of Birch and Swinnerton-Dyer contains inplicitely that $Ш(E,\mathbb{Q})$ is a finite group. A recent result of Kolyvagin (cf. [Kol], [Ru 2]) proves this for modular elliptic curves E with twist E_d for which $L_E(1)\cdot L'_{E_d}(1) \neq 0$.

We are interested in a very special case: Assume that d_0, d_1 are square free integers and that E_{d_0} resp. E_{d_1} are the twists of E by d_0 resp. d_1. Then

$$L_{E_{d_1}}(s) = L_E(s) \otimes \chi_{d_1} = 1 + \sum_{j=2}^{\infty} \chi_{d_1}(j)\, a_j q^j .$$

We assume that $L_{E_{d_0}}(1) \neq 0$. Then conjecture 2.1 implies

Conjecture 2.2. Either $L_{E_{d_1}}(s) = 0$ and so $r_{E_{d_1}} > 0$ or

$$\frac{L_{E_{d_1}}(1)}{L_{E_{d_0}}(1)} \sqrt{\frac{d_1}{d_0}} = c(d_0, d_1) \cdot \frac{\# S(E_{d_1}, \mathbb{Q})}{\# S(E_{d_0}, \mathbb{Q})}$$

with an easy computable rational number $c(d_0, d_1) \neq 0$ depending on the numbers of divisors of d_0, d_1 which is in most cases a power of 2.

2. Waldspurger's theorem

Let N be a natural number divisible by 4 and ψ a Dirichlet character modulo N. By $S_{3/2}(N,\psi)$ we denote the complex vector space of cusp forms of weight 3/2 with respect to $\Gamma_0(N)$ and with character ψ. For the precise definition we refer to [Sh 2].

$F \in S_{3/2}(N,\psi)$ has a Fourier expansion at $i\infty$:

$$F(z) = \sum_{n=1}^{\infty} a_n q^n ,$$

for primes $p \nmid N$ we have Hecke operators $T(p) = 0$ and $T(p^2)$ given by

$$T(p^2)(F) = \sum_{m=1}^{\infty} b_m q^m \quad \text{with}$$

$$b_m = a_{p^2 m} + \psi(p) \cdot \chi_{-1}(p) \cdot (\tfrac{m}{p}) \cdot a_m + \psi(p^2) \cdot p \cdot a_{\frac{m}{p^2}} \quad (a_{\frac{m}{p^2}} = 0 \text{ if } p^2 \nmid m).$$

There is a Hermitian form $\langle\ .\ \rangle$ defined on $S_{3/2}(N,\psi)$:

$$\langle F,G \rangle = \frac{1}{C(N)} \int_{\mathbb{H}/\Gamma_0(N)} F(z)\, G(\overline{z})\, y^{-\frac{1}{2}}\, dx\, dy$$

with $\mathbb{H}$ the upper half plane of $\mathbb{C}$ and $z = x+iy$.
One has for $p \nmid N$:

$$\langle T(p^2)F,G \rangle = \langle F,T(p^2)G \rangle .$$

We use $\langle\ ,\ \rangle$ to define orthogonality in $S_{3/2}(N,\psi)$. $S_0(N,\psi)$ is the subspace of $S_{3/2}(N,\psi)$ generated by forms F of the following type: There is a $t \in \mathbb{N}$ and a quadratic character χ with conductor r such that

$$N = 4r^2 t,\ \psi = \chi \cdot \chi_t \cdot \chi_{-1} \text{ and } F = \sum_{m=1}^{\infty} \chi(m)\, m q^{tm^2} .$$

The following important result is a special case of a result due to Shimura (cf. [Sh2]):

<u>Theorem</u> <u>2.3.</u> Assume that $F = \sum_{n=1}^{\infty} a_n q^n \in S_{3/2}(N,\psi) \cap S_0(N,\psi)^{\perp}$ is an eigenform under $T(p^2)$ for all primes $p \nmid N$ with eigenvalues λ_p. Assume that $\psi^2 = \mathrm{id}$. Let $S(F) := f = \sum_{m=1}^{\infty} b_m q^m$ with b_m such that

$$\sum_{m=1}^{\infty} b_m m^{-s} = \Big(\sum_{i=1}^{\infty} (\tfrac{-1}{i}) \psi(i)\, i^{-s} \Big) \Big(\sum_{j=1}^{\infty} a_{j^2} j^{-s} \Big) .$$

Then f is an element in $S_2(\tilde{N})$ with $N = 2^{\alpha} \cdot \tilde{N}$, $\alpha \geq 0$, and f is an eigenform under the Hecke operator $T(p)$ operating on $S_2(\tilde{N})$ with eigenvalue λ_p for all $p \nmid N$.

We are interested in cusp forms of weight 3/2 because of the following result of Waldspurger.

Theorem 2.4. (Waldspurger [Wa]). Assume that E/Q is a modular elliptic curve with corresponding cusp form f_E, and that

$$F \in S_{3/2}(N,\chi_t) \cap S_0(N,\chi_t)^{\perp} \quad \text{with}$$

$$S(F) = f_E, \; F = \sum_{n=1}^{\infty} a_n q^n .$$

Assume that d and d_0 are natural square free numbers with

$$d \equiv d_0 \bmod \prod_{p \mid N} Q_p^{\times 2} \text{ and } d \cdot d_0 \text{ prime to } N.$$

Then

$$L_{E_{-td}}(1)\sqrt{d}\, a_{d_0}^2 = L_{E_{-td_0}}(1)\sqrt{d_0}\, a_d^2 .$$

So especially: If

$$L_{E_{-td_0}}(1) \cdot a_{d_0}^2 \neq 0$$

then

$$L_{E_{-td}}(1) = 0. \text{ if and only if } a_d = 0 .$$

Using this theorem we can reformulate conjecture 2.2:

Conjecture 2.5. Assume that $L_{E_{-td_0}}(1) \cdot a_{d_0} \neq 0$. Then either

$$\operatorname{rank}_{\mathbb{Z}} E_{-td}(Q) > 0$$

or

$$a_d^2 = c(d,d_0)\frac{\# S(E_{-td},Q)}{\# S(E_{-td_0},Q)}\, a_{d_0}^2 .$$

So assuming that $\# S(E_{-td_0},Q) \cdot a_{d_0}^2$ is known the knowledge of a_{d^2} decides whether $\operatorname{rank}_{\mathbb{Z}}(E_{-td}(Q)) = 0$ and, if so, gives the size of the Selmer group of E_{-td} over Q. Hence it is only necessary to find finitely many test curves E_{-td_0} to discuss all twists of E.

It was Tunnell's idea to use Waldspurger's result in this way for elliptic curves with j-invariant 12^3 (cf. [Tu]); in [Fr 2] the case $j_E = 0$ was discussed. In the following sections we want to describe how one can find more examples of curves to which Tunnell's method can be applied.

§3 Construction of cusp forms of weight 3/2

Let E/Q be a modular elliptic curve with cusp form f_E. In order to use Tunnell's idea we have to find eigenfunctions $F_E \in S_{3/2}(\tilde{N},\psi)$ with ψ^2 = id. $\tilde{N} = 2^\alpha \cdot N_E$ with $S(F_E) = f_E$.
F_E doesn't exist necessarily. In [Wa] one finds a sufficient condition for the existence in terms of representation theory, another sufficient condition is due to Kohnen (cf. [Ko]):

Proposition 3.1. Assume that N_E is odd and square free. Then there is a subspace $S^-_{3/2}(4N_E,\psi_0)$ of $S_{3/2}(4N_E,\psi_0)$ which is mapped isomorphically to $S_2(N_E)$ by a linear continuation of Shimura's map S.

But even the knowledge that F_E exists may be of no great help for instance for deciding whether $L_{E_d}(1) = 0$ or not; it is essential that the Fourier coefficients of F_E are easily and exactly computable and that the way of construction reflects arithmetical properties of E_d. Hence we reverse the problem in some sense and begin by constructing elements in $S_{3/2}(N,\psi)$ for $N \in 4\mathbb{N}$ and ψ^2 = id with rather accessible arithmetical properties, and then we decide whether the Shimura map sends these forms to elliptic curves. Though this approach is rather experimental it turns out that it leads to interesting examples for small levels.

One method to construct cusp forms of weight 3/2 is related to ternary quadratic forms: Let $f(X_1,X_2,X_3)$ be an integral positive definite ternary quadratic form with associated matrix

$$A = \left(\frac{\partial^2 X}{\partial X_i \partial X_j}\right), \quad D := \det(A) .$$

Let N be the smallest natural number such that $N \cdot A^{-1}$ has integral entries and even diagonal elements. Then the theta series

$$\Theta(f) := \sum_{x \in \mathbb{Z}^3} q^{f(x)}$$

is a modular form of weight 3/2, level N and character χ_{2D}. If one takes a suitable linear combination of such theta series one gets a cusp form. For example one can use the following result due to Schulze-Pillot and Siegel (cf. [S-P]):

Proposition 3.2. Let f_1, f_2 be ternary integral positive definite quadratic forms in the same genus, i.e. $f_1 \otimes \mathbb{Z}_p \simeq f_2 \otimes \mathbb{Z}_p$ for all primes p then

$$\Theta(f_1) - \Theta(f_2) \in S_{3/2}(N, \chi_{2D}) .$$

It is not difficult to implement an algorithm which determines all reduced ternary quadratic forms which give rise to modular forms of given level and character, for instance one can use an algorithm of Brandt (cf. [B-I]), and so one can find a (in general, proper) subspace of $S_{3/2}(N,\chi_{2D})$ rather easily.

However it turns out that for levels which are small enough to be accessible to computation an even more special class of cusp forms gives interesting examples.

Let $M_{1/2}(N,\psi^{(1)})$ be the modular forms of weight 1/2 and level N, and character $\psi^{(1)}$, $S_1(N,\psi^{(2)})$ the cusp forms of weight 1, level N and character $\psi^{(2)}$. Then

$$M_{1/2}(N,\psi^{(1)}) \otimes S_1(N,\psi^{(2)}) \subset S_{3/2}(N,\psi^{(1)} \cdot \psi^{(2)} \cdot \chi_{-1})$$

and we denote by $\tilde{S}_{3/2}(N,\psi)$ the Hecke-algebra submodule of $S_{3/2}(N,\psi)$ generated by

$$\{M_{1/2}(N,\psi^{(1)}) \otimes S_1(N,\psi^{(2)})\}_{\psi^{(1)}\psi^{(2)}\chi_{-1}=\psi} .$$

$M_{1/2}(N,\psi)$ is well known:

Proposition 3.3 (Serre-Stark, cf. [S-St]). Let $\Omega(N,\psi)$ be the set of pairs (φ,t) with $t \in \mathbb{N}$, φ an even primitive Dirichlet character with conductor $r(\varphi)$ such that

i) $4 \cdot r(\varphi)^2 t \mid N$, and

ii) $\psi(n) = \varphi(n)\chi_t(n)$ for $n \in \mathbb{Z}$ prime to N.

Then

$$\{\Theta_{\varphi,t} := \sum_{-\infty}^{\infty} \varphi(n) q^{tn^2}\}_{(\varphi,t) \in \Omega(N,\psi)}$$

forms a base of $M_{1/2}(N,\psi)$.

Discussion of $S_1(N,\psi)$: Due to beautiful results of Weil, Langlands, Serre and Deligne (cf. [D-S]) one has a one-to-one correspondence between new-forms F of level N (i.e. eigenforms under Hecke operators with exact level N) in $S_1(N,\psi)$ and representations $\rho: G_{\mathbb{Q}} \longrightarrow Gl(2,\mathbb{C})$ with the following properties:

ρ is irreducible, det $\rho = \psi$ and the Artin conductor of ρ is equal to N.
If $L_\rho(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is the Artin L-series of ρ then $F = \sum_{n=1}^{\infty} a_n q^n$.
The possible images of ρ are

i) dihedral groups of order 2n, or
ii) finite subgroups in $GL(2,\mathbb{C})$ with image equal to A_4, S_4 or A_5 in $PGl(2,\mathbb{C})$.

The first case has a close connection to class field theory: Let K be an imaginary quadratic field with discriminant D_0, let χ: $G_K \longrightarrow \mathbb{C}^\times$ be a character with $\mathrm{cond}(\chi) | r \in \mathbb{N}$. $\rho := \mathrm{ind}_{K/Q}\chi$ is the 2-dimensional complex representation of G_Q induced by χ.
Let τ be a generator of G(K/Q). Then $\rho(G_Q)$ is dihedral if and only if

$$\chi(\tau\sigma\tau) = \chi^{-1}(\sigma) \quad \text{for all } \sigma \in G_K \text{ and } \chi^2 \neq \mathrm{id}.$$

Let K_r be the subfield of the ray class field $K_{(r)}$ of K with conductor r determined by the condition:

$$\tau\sigma\tau = \sigma^{-1} \quad \text{for all } \sigma \in G(K_r/K) .$$

Then

$$\{\rho\colon G_Q \longrightarrow Gl(2,\mathbb{C});\ \mathrm{im}(\rho) \text{ is dihedral, } \mathrm{cond}(\rho) | D_0 r^2\}$$

corresponds one-to-one to

$$\{\chi\colon G(K_r/K) \longrightarrow \mathbb{C}^\times \text{ with } \chi^2 \neq \mathrm{id}\} .$$

Via reciprocity $G(K_r/K)$ is canonically isomorphic to

$C(r) := I(r)/\langle(z_1),\dots,(z_l)\rangle \cdot P(r)$ with
$I(r)$ the group of ideals of K prime to r,
$P(r)$ the ray modulo r, and
$\{z_1, \dots, z_l\}$ a set of representatives of $(\mathbb{Z}/r\mathbb{Z})^\times$.

So by class field theory it is possible to determine all newforms F_ρ of weight one that correspond to representations ρ with dihedral image. The level of F_ρ is equal to $D_0 N_{K/Q}(\mathrm{cond}(\chi))$ and the character of F_ρ is equal to χ_{D_0}, if $\rho = \mathrm{ind}_{K/Q}(\chi)$ and D_0 the discriminant of K. Most convenient is the following connection with quadratic forms:
Let $H(D_0 r^2)$ be the group of classes of positive definite primitive binary quadratic forms with discriminant $D_0 r^2$. Since $H(D_0 r^2)$ is isomorphic to C(r) the

character χ of $G(K_r/K)$ can be interpreted as character of $H(D_0 r^2)$. Using this interpretation we get

Proposition 3.4 (cf. [A]).

$$F_\rho = \sum_{k \in H(D_0 r^2)} \chi(k)\, \Theta(k)$$

with $\Theta(k)$ the theta series related to a quadratic form

$$f \in k:\ \Theta(k) = \sum_{n=1}^{\infty} a_n q^n \quad \text{with}$$

$$\text{with } a_n = \tfrac{1}{2} \# \{(z_1, z_2) \in \mathbb{Z}^2;\ f(z_1, z_2) = n\}\ .$$

It is obvious that F_ρ is rather accessible to numerical computations. As an example how elements in $S_1(N,\psi)$ related to representations ρ of type ii) can be constructed we describe a method which is closely related to elliptic curves and which can be applied to representations with image $S_4 \subset PGl(2,\mathbb{C})$. For a detailed discussion we refer to [B-F].

We assume that E: $Y^2 = f(x)$ is an elliptic curve with conductor N_E and negative discriminant Δ_E without Q-rational points of order 2. Then $\alpha \in S(E,Q)\setminus\{0\}$ is given by an equation $U^2 = g(V)$ where g is a polynomial of degree 4 with cubic resolvent f, and so the splitting field of g is a Galois extension K/Q with Galois group S_4, and K/Q is unramified outside $2 \cdot N_E$.

Using a criterion of Serre ([Se]) one can find local conditions for α that are equivalent to the existence of a field $\tilde{K} \supset K$ with $G(\tilde{K}/Q) = \tilde{S}_4$ where $\tilde{S}_4$ is the double cover of S_4 in which transpositions lift to involutions. Since $\tilde{S}_4$ is isomorphic to $Gl(2,\mathbb{Z}/3)$ it has a faithful representation

$$\rho:\ \tilde{S}_4 \longrightarrow Gl(2,\mathbb{C})\ .$$

Moreover, since $\Delta_E < 0$ and since $\det \rho = \chi_{\Delta_E}$, $\det(\rho)$ is odd and ρ corresponds to a cusp form F_α of weight 1 with character χ_{Δ_E}.

Using the explicit solution of the embedding problem

$$1 \longrightarrow \mathbb{Z}/2 \longrightarrow \tilde{S}_4 \longrightarrow S_4 \longrightarrow 1$$

due to Crespo ([C]) one can choose $\tilde{K}$ in such a way that the conductor N_ρ of

ρ has support in $2 \cdot N_E$, and one has complete control over the prime-to-6 part of N_ρ and so over the prime-to-6 part of the level of F_α. Moreover it is not too difficult to implement an algorithm which computes the Fourier coefficients of α. The most simple examples for elements α are obtained by division by 2 of points in E(Q): Assume that $P \in E(Q)$ but $P \notin 2E(Q)$. Then the cocycle

$$\hat{\rho}: \; G_Q \longrightarrow E(\bar{Q})_2 \quad \text{defined by}$$

$$\hat{\rho}(\sigma): \; \sigma(\tfrac{1}{2}P) - \tfrac{1}{2}P \qquad \text{for } \sigma \in G_Q$$

defines a non-trivial class in $S(E,Q)_2$.

Tables for cusp forms constructed by using this method will be prepared by Lario and Quer, the easiest examples are constructed by using E = (48 A), $g(X) = X^4+2X+1$, and E = (121 D) with $g(X) = X^4-16X^3+30X^2+30X-74$.

After having constructed modular forms H of weight $\frac{1}{2}$ and cusp forms G of weight 1 we get by multiplying cusp forms F_0 of weight $\frac{3}{2}$. But now a technical difficulty arises: In general $F_0 = H \cdot G$ will not be an eigenform under Hecke operators.

In the following lines we describe an algorithm which enables us to find, starting with F_0, eigenforms $F \in S_{3/2}(N,\psi)$. We only have to assume that $F_0 \in S_0(N,\psi)^{\perp}$.
Let $\mathbb{T}$ denote the Hecke algebra operating on $S_{3/2}(N,\psi)$. We are looking for $F \in \langle F_0 \rangle_{\mathbb{T}}$, the cyclic $\mathbb{T}$-module generated by F_0 which are eigenforms under $\mathbb{T}$. We use that cusp forms are uniquely determined by their Fourier expansions and that it is possible to guarantee equality between two cusp forms by compairing the Fourier coefficients up to an index depending (linearly) on N only.

<u>First step of the algorithm:</u> We fix a (small) prime p_1 and consider the complex space

$$V_i = \langle F_0, T(p_1^2)F_0, \dots, T(p_1^2)^i F_0 \rangle .$$

Since $S_{3/2}(N,\psi)$ is finite dimensional we find a minimal i_0 with

$$V_i = V_{i_0} \quad \text{for all } i > i_0, \text{ i.e. } \langle F_0, \dots, T(p_1^2)^{i_0} F_0 \rangle$$

is $T(p_1^2)$-invariant.
It is not difficult to compute the characteristic polynomial $\chi_{T(p_1^2)}$ of $T(p_1^2) \mid V_{i_0}$

and to determine eigenforms $F_{1,\lambda_{p_1}} \in V_{1_0}$ with respect to $T(p_1^2)$ with eigenvalue λ_{p_1}.

<u>Second step:</u> Replace F_0 by $F_1 := F_{1,\lambda_{p_1}}$. (In concrete cases choose λ_{p_1} such that this eigenvalue appears as eigenvalue of a cusp form of weight 2 one is interested in, e.g. look for $\lambda_{p_1} \in \mathbb{Z}$ if one is interested in cusp forms related to modular elliptic curves.)
Replace p_1 by a different prime p_2 and determine

$$F_2 \in \langle F_1 \rangle_{\mathbb{T}} \quad \text{with } T(p_2^2)(F_2) = \lambda_{p_2} F_2 .$$

Then F_2 is an eigenform under $T(p_1^2)$ and under $T(p_2^2)$ with eigenvalues λ_{p_1} resp. λ_{p_2}. Here we use the fact that the Hecke operators commute.

We repeat the procedure with primes $p_3, p_4, \dots, p_n$ and so after n steps we find a cusp form F_n with $T(p_i^2) F_n = \lambda_{p_i} F_n$.
Now we use

<u>Proposition 3.5.</u> There exist a number n and primes $p_1, \dots, p_n$ such that F_n, as constructed above, is an eigenform under all Hecke operators.

to make the algorithm to a finite one.

<u>Proof of the proposition.</u> We look at cusp forms of weight 2 and level N, $S_2(N)$. Let $\{f_1, \dots, f_d\}$ be a base of $S_2(N)$ consisting of eigenfunctions under the operation of $T(p)$ for primes $p \nmid N$. We associate the vector of eigenvalues $(\lambda_p^{(i)})_{p \in \mathbb{P}}$ to f_i, and we choose $p_1, \dots, p_n$ such that

$$(\lambda_{p_j}^{(i)})_{j=1,\dots,n} \neq (\lambda_{p_j}^{(i')})_{j=1,\dots,n} \quad \text{if } (\lambda_p^{(i)})_{p \in \mathbb{P}} \neq (\lambda_p^{(i')})_{p \in \mathbb{P}} .$$

Now look at $\langle F_n \rangle_{\mathbb{T}}$ where F_n is constructed as above. Because of the commutativity of $\mathbb{T}$ and the existence of the Hermitian product on $S_{3/2}(N,\psi)$ defined in §2 we find a base of $\langle F_n \rangle_{\mathbb{T}}$ consisting of eigenforms. Let F be such an eigenform. Since $T(p_j^2) F = \lambda_{p_j} F$ for $j = 1, \dots, n$ and $S(F) \in S_2(N)$ is an eigenform under all $T(p)$ with $T(p)(S(F)) = \lambda_{p_j}(S(F))$ it follows that there exists exactly one vector of eigenvalues of cusp forms of weight 2 with p_j-component λ_{p_j}. It follows that all eigenforms in $\langle F_n \rangle_{\mathbb{T}}$ have the same eigenvalues at all primes p, and so F_n is an eigenform under $\mathbb{T}$ as claimed.

We end this section by giving some examples in which we find a cusp form F of weight 3/2 which is mapped to the cusp form of weight 2 corresponding to an elliptic curve E which is denoted as in the table of [MF IV].
For the construction of F we use $F_0 = G \cdot H$ with H a modular form of weight 1/2 and G a cusp form of weight 1 constructed by Θ-functions of binary quadratic forms as described in proposition 3.5. We use the notation of proposition 3.4 and 3.5.

Examples 3.6.

0) The cases in which the image of F corresponds to elliptic curves with $j = 12^3$ resp. $j = 0$ are discussed intensively in [Tu] and [Fr 2].

1) $N = 44$.
For H we take $\Theta_{1d,11} = \sum_{n=-\infty}^{\infty} q^{11n^2} \in M_{1/2}(44, \chi_{11})$.
For G: Take $K = \mathbb{Q}(\sqrt{-11})$, $r = 2$, K_2 the ring class field with conductor 2 over K, $C_2 \cong \mathbb{Z}/3\mathbb{Z}$.
$H(-44)$ is generated by the class of $f = (3X^2+2XY+4Y^2)$.
Take

$$\chi: G(K_2/K) \longrightarrow \mathbb{C}^\times \quad \text{given by}$$
$$\chi((f)) = e^{\frac{2\pi i}{3}}.$$

Then

$$G = F_\chi = \Theta(X^2+11Y^2) - \Theta(3X^2+2XY+4Y^2) \in S_1(44, \chi_{-11})$$

and so

$$F_0 = G \cdot H \in S_{3/2}(44).$$

F_0 is an eigenform under $\mathbb{T}$, and $S(F = F_0)$ is the cusp form corresponding to $(11B) = X_0(11)$.

2) $N = 56$.
For H we take $\Theta_{1d,14}$.
Construction of G: Take $K = \mathbb{Q}(\sqrt{-14})$, $r = 1$, K_r the Hilbert class field of K, $C_r \cong \mathbb{Z}/4\mathbb{Z}$.
$H(-56)$ is generated by the class of $f = (3X^2+2XY+5Y^2)$.

$$\chi: G(K_r/K) \longrightarrow \mathbb{C}^\times \quad \text{is given by}$$
$$\chi((f)) = i.$$

Hence

$$G = F_\chi = \Theta(X^2+14Y^2) - \Theta(2X^2+7Y^2) \in S_1(56, \chi_{-14}) .$$

$F = F_0 = G \cdot H$ is mapped to the cusp form corresponding to the curve (14C).

3) $N = 60$.

For H take $\Theta_{id,3}$.

Construction of G: Take $K = \mathbb{Q}(\sqrt{-15})$, $r = 2$, K_r is the ring class field with conductor 2 of K, $C_r \cong \mathbb{Z}/2$. Hence $G(K_r/\mathbb{Q})$ is abelian.

$H(-60) = \{X^2+15Y^2, 3X^2+5Y^2\}$.

In this case $\Theta(X^2+15Y^2) - \Theta(3X^2+5Y^2)$ is <u>no</u> cusp form but

$G := \Theta(X^2+15Y^2) - \Theta(4X^2+2XY+4Y^2)$ is an element of $S_1(60, \chi_{-5})$

$F = F_0 = G \cdot H$ is mapped to the cusp form corresponding to the curve (15C).

4) $N = 68$.

For H take $\Theta_{id,17}$ or $\Theta_{id,1}$.

Construction of G. Take $K = \mathbb{Q}(\sqrt{-17})$, $r = 1$, K_r the Hilbert class field of K, $C_r \cong \mathbb{Z}/4\mathbb{Z}$.

$H(-68)$ is generated by $(f) = (3X^2+2XY+6Y^2)$.

$\chi\colon G(K_r/K) \longrightarrow \mathbb{C}^\times$ is given by
$\chi((f)) = i$.

Then

$$G = F_\chi = \Theta(X^2+17Y^2) - \Theta(2X^2+2XY+9Y^2) \in S_1(68, \chi_{-17}) .$$

$F = F_0 = G \cdot \Theta_{id,17}$ and $F' = F_0' = G \cdot \Theta_{id,1}$ are eigenforms under $\mathbb{T}$. A little surprise is that Shimura's map sends both of them to the cusp form corresponding to $E = (34\,A)$ and <u>not</u> an elliptic curve of level 17. On the other side Kohnen's result assumes the existence of a cusp form of weight 3/2 and level 68 mapped to f_{17}, the newform corresponding to $E = (17C)$, and so we found an example for the fact that by our method one doesn't find all interesting cusp forms of weight 3/2. To repair this lack we go to a higher level:

4') $N = 272$.

For H take $\Theta_{id,17}$.

Take $K = \mathbb{Q}(\sqrt{-17})$, $r = 2$ and K_r the ring class field with conductor 2 of K,

$C_r \cong \mathbb{Z}/8$.
$H(-272)$ is generated by $(f) = (3X^2+2XY+23Y^2)$.
It we take

χ: $G(K_r/K) \longrightarrow \mathbb{C}^\times$ determined by
$\chi((f)) = i$

we get

$$G = F_\chi = \Theta(X^2+68Y^2)+2\Theta(4X^2+17Y^2)-2\Theta(8X^2+4XY+9Y^2)\ .$$

With $F_0 = G\cdot H$ we get:

$$V_2 = \langle F_0, T(3^2)F_0, T(3^2)^2 F_0\rangle$$

is invariant under $T(3^2)$, and

$$F_1 = 2F_0+2T(3^2)F_0-T(3^2)^2 F_0$$

is an eigenform under $\mathbb{T}$.
But to our disappointment F_1 is mapped to the form corresponding to (34 A) again.
So we try the character

χ: $G(K_r/K) \longrightarrow \mathbb{C}^\times$ determined by
$\chi((f)) = \zeta_8$.

Then

$F_\chi = F_\chi^{(1)}+\sqrt{2}\,F_\chi^{(2)}$ with
$F_\chi^{(1)} = \Theta(X^2+68Y^2)-\Theta(4X^2+17Y^2)$ and
$F_\chi^{(2)} = \Theta(3X^2-2XY+23Y^2)-\Theta(7X^2+6XY+11Y^2)$.

It turns out that

$$F := F_\chi^{(2)}\cdot\Theta_{\mathrm{id},17}$$

is an eigenform under $\mathbb{T}$ mapped to f_{17}.

5) $N = 76$.
For H take $\Theta_{\mathrm{id},19}$.
Construction of G: Take $K = \mathbb{Q}(\sqrt{-19})$, $r = 2$ and K_r the ring class field

with conductor 2 of K.

$C_r \cong \mathbb{Z}/3$ and $H(-76) = \langle (f) = (4X^2+2XY+5Y^2)\rangle$

χ: $G(K_r/K) \longrightarrow \mathbb{C}^\times$ is determined by

$\chi((f)) = \zeta_3$.

$G = F_\chi = \Theta(X^2+19Y^2) - \Theta(4X^2+2XY+5Y^2) \in S_1(76, \chi_{-19})$.

$F_0 = G \cdot H = F_\chi \cdot \Theta_{\mathrm{id}.19}$.

F_0 is no eigenform but $\langle F_0, T(3^2) F_0\rangle$ is $\mathbb{T}$-invariant. We get eigenforms

$F = F_0 - T(3^2) F_0$ and

$F' = 2F_0 + T(3^2) F_0$.

The image under Shimura's map of F is equal to the cusp form corresponding to E = (19 B), the image of F' corresponds to E = (38 D).

6) N = 80.

For H take $\Theta_{\mathrm{id}.20}$.

Construction of G: Take $K = Q(\sqrt{-5})$, r = 2, K_r the ring class field of K with conductor 2.

$C_r \cong \mathbb{Z}/4\mathbb{Z}$ and $H(-80) = \langle (f) = (3X^2+2XY+7Y^2)\rangle$.

χ is determined by $\chi((f)) = i$.

$G = F_\chi = \Theta(X^2+20Y^2) - \Theta(4X^2+5Y^2) \in S_1(80, \chi_{-5})$.

$F = F_0 = G \cdot H = F_\chi \cdot \Theta_{\mathrm{id}.20}$ is an eigenform under $\mathbb{T}$ which is mapped to the form corresponding to (20 B).

7) $N = 196 = 4 \cdot 49$.

For H take $\Theta_{\mathrm{id}.7}$, $K = Q(\sqrt{-1})$, r = 7 and $K_r = Q(\sqrt[4]{-7}, \sqrt{-1})$ the ring class field with conductor 7 of K.

$C_r \cong \mathbb{Z}/4\mathbb{Z}$ and $H(-196) = \langle (f) = (5X^2+2XY+10Y^2)\rangle$

χ is determined by $\chi((f)) = i$, and

$G = F_\chi = \Theta(X^2+49Y^2) - \Theta(2X^2+2XY+25Y^2)$.

$F_0 = G \cdot H = F_\chi \cdot \Theta_{\mathrm{id}.7}$ is no eigenform but $\langle F_0, T(3^2) F_0\rangle$ is invariant under $T(3^2)$, $F = 4F_0 + T(3^2) F_0$ is an eigenform under $\mathbb{T}$, and S(F) corresponds to the elliptic curve (98 B).

Of course we would have liked to get E = (49 A), the elliptic curve with complex multiplication by the ring of integers of $Q(\sqrt{-7})$.

So we enlarge N to $4\cdot N$.

7') $N = 16\cdot 49$.

Again $H = \Theta_{id.7}$.

Construction of G: Take $K = Q(\sqrt{-1})$ but $r = 14$ and K_r the ring class field of K.

$C_r \cong \mathbb{Z}/8\mathbb{Z}$ and $H(-16\cdot 49) = \langle (f) = (5X^2+4XY+40Y^2)\rangle$.

χ is determined by $\chi((f)) = \zeta_8$.

$$F_\chi = F_\chi^{(1)} + \sqrt{2}\, F_\chi^{(2)} \quad \text{with}$$

$$F_\chi^{(1)} = \Theta(X^2+196Y^2) - \Theta(4X^2+49Y^2) \quad \text{and}$$

$$F_\chi^{(2)} = \Theta(5X^2+4XY+40Y^2) - \Theta(13X^2+10XY+17Y^2).$$

Now $F_\chi^{(1)}\cdot\Theta_{id.7}, F_\chi^{(2)}\cdot\Theta_{id.7}$ and hence $F_\chi\cdot\Theta_{id.7}$ are eigenforms under $\mathbb{T}$, and their image under Shimura's map corresponds to $E = (49A)$.

Remark: This example has been found by Lehman (cf. [Le]).

In the following table we list the essential datas of our examples.

Table 3.7.

Expl.	K_r	F_0	F	Elliptic curve E
1	$Q(\sqrt{-11})_2$	$(\Theta(X^2+11Y^2)-\Theta(3X^2+2XY+4Y^2))\Theta_{id.11}$	F_0	$11B = X_0(11)$
2	$Q(\sqrt{-14})_1$	$(\Theta(X^2+14Y^2)-\Theta(2X^2+7Y^2))\Theta_{id.14}$	F_0	14C
3	$Q(\sqrt{-15})_2$	$(\Theta(X^2+15Y^2)-\Theta(4X^2+2XY+4Y^2))\Theta_{id.3}$	F_0	15C
4'	$Q(\sqrt{-17})_2$	$(\Theta(3X^2-2XY+23Y^2)-\Theta(7X^2+6XY+11Y^2))\Theta_{id.17}$	F_0	17C
4	$Q(\sqrt{-17})_1$	$(\Theta(X^2+17Y^2)-\Theta(2X^2+2XY+9Y^2))\Theta_{id.17}$	F_0	34A
5	$Q(\sqrt{-19})_2$	$(\Theta(X^2+19Y^2)-\Theta(4X^2+2XY+5Y^2))\Theta_{id.19}$	$F_0-T(3^2)F_0$	19B
			$2F_0+T(3^2)F_0$	38D
6	$Q(\sqrt{-5})_2$	$(\Theta(X^2+20Y^2)-\Theta(4X^2+5Y^2))\Theta_{id.20}$	F_0	20B
7'	$Q(\sqrt{-1})_{14}$	$(\Theta(X^2+196Y^2)-\Theta(4X^2+49Y^2))\Theta_{id.7}$	F_0	49A
7	$Q(\sqrt{-1})_7$	$(\Theta(X^2+49Y^2)-\Theta(2X^2+2XY+25Y^2))\Theta_{id.7}$	$4F_0+T(3^2)F_0$	98B

§4 Comparison of the methods

In this section we want to discuss connections between the results of §1 stating triviality of parts of the Selmer groups of twists E_d or the finiteness of $E_d(Q)$ and results concerning the values of L-series $L_{E_d}(1)$ obtained by Waldspurger's theorem. These connections confirm conjecture 2.5 at least in a weak form for some examples.

We begin with the 2-part and an easy observation:

Lemma 4.1. Assume that F_0 is a cusp form of weight 3/2 and level N given by

$$F_0 = [\Theta(X^2+\tfrac{N}{4}Y^2) - \Theta(aX^2+bXY+cY^2)]\,\Theta_{1d,t} \quad \text{with } b \neq 0 .$$

Assume that q is a prime with $q \nmid 2N$ such that $aX^2+bXY+cY^2$ represents q over $\mathbb{Z}$. Then the q-th Fourier coefficient a_q^0 of F_0 is odd.

Proof. By definition we have

$$a_q^0 = \frac{1}{2}\Big[\sum_{t=-\infty}^{\infty} (\#\{(x,y) \in \mathbb{Z}^2;\ x^2+\tfrac{N}{4}y^2+ti^2 = q\} - \#\{(x,y) \in \mathbb{Z}^2;\ ax^2+bxy+cy^2+ti^2 = q\}\Big].$$

Since all terms inside the sum except $\#\{(x,y) \in \mathbb{Z}^2;\ ax^2+bxy+cy^2 = q\}$ are divisible by 4 and since q has at most two integral representations by $aX^2+bXY+cY^2$ the assertion follows.

Lemma 4.1 can be applied to examples 1, 3, 4, 5 and 7. Examples 1 and 5 are of special interest for in these cases the field K_r used for the construction of F_0 is closely related to the elliptic curve E obtained by Shimura's map: $K_r = Q(E(\overline{Q})_2)$, and the condition that the prime q is represented by the quadratic form $aX^2+bXY+cY^2$ with $b \neq 0$ is equivalent with the condition that q is not split in $Q(E(\overline{Q})_2)/Q(\sqrt{\Delta_E})$. Hence it is easily seen that these examples are special cases of the following

Proposition 4.2. Let E be an elliptic curve with prime conductor p and $E(Q)_2 = \{0\}$. Let χ be the character of $G(Q(\sqrt{\Delta_E})_2/Q(\sqrt{\Delta_E}))$ whose kernel fixes $Q(E(\overline{Q})_2)$, and let $F_0 = G\cdot\Theta_{1d,t} \in S_{3/2}(N,\chi_1)$, $t|4p$, and hence

$$G = F_\chi = \Theta(X^2+pY^2) - \Theta(aX^2+bXY+cY^2) \quad \text{with } b \neq 0 .$$

Let q be a prime not dividing 4p. Then the q-th Fourier coefficient of F_0 is not equal to zero if q is not split in $Q(E(\overline{Q})_2)/Q(\sqrt{\Delta_E})$.

Assume now moreover that $f_E = S(F)$ with $F = \sum \lambda_{i,j} T(p_j^2)^i F_0$ such that the q-th Fourier coefficient of F is not zero if the q-th Fourier coefficient of F_0 is not zero. Then we get:

4.3. $L_{E_{-lq}}(1) \neq 0$ if q is not split in $Q(E(\bar{Q})_2)/Q(\sqrt{\Delta_E})$.

It is clear that 4.3 has a close connection to the result 1.14 ii) confirming "the 2-part of conjecture 2.5" for examples in which $S(E,Q) = \{0\}$. (If $S(E,Q)_2 \neq 0$ one should expect that the cusp forms of weight 1 constructed with the help of nontrivial elements of this group play an important role.)
For instance one can easily verify that 4.3 holds for $E = X_0(11)$ and $E = (19B)$.

It is not difficult to find conditions for the non-vanishing of Fourier coefficients of F_0 (and so for F) in the other examples too, we only mention:

Example 2: If q is a prime not dividing 14 then $a_q \neq 0$ if q is represented by $2X^2+7Y^2$.

Example 6: If q is a prime not dividing 20 then $a_q \neq 0$ if q is represented by $4X^2+5Y^2$.

Example 7': If q is a prime not dividing 14 then $a_q \neq 0$ if q is represented by exactly one of the forms X^2+196Y^2, X^2+7i^2 and $4X^2+7^2Y^2$.

The other case in which Galois descent gave information about Selmer groups was that E has a Q-rational point of order $p \in \{3,5,7\}$: Proposition 1.5 relates $S(E_{-d},Q)_p$ with the p-part of the class group of $Q(\sqrt{-d})$. Hence, if F is a cusp form of level 3/2 mapped to f_E by Shimura's map the Fourier coefficients a_d of F should be related with this class group too. One possible approach to see this is given in [A-K]:
To simplify we assume that E has prime conductor l with $l \equiv 3 \bmod 4$. (For example take $E = X_0(11)$ or $E = (19B)$.)
Define

$$\mathcal{E}_{2,l} = \frac{l-1}{24} - \sum_{n\geq 1} \sigma_1(n)_l q^n \quad \text{with}$$

$$\sigma_1(n)_l = \sum_{\substack{d|n \\ l\nmid d}} d .$$

The assumption that E has a Q-rational point of order p implies:

$$f_E \equiv \mathcal{E}_{2,l} \text{ modulo } p ,$$

and especially

$$p \mid \frac{l-1}{12} .$$

Now there is a (unique) modular form of weight 3/2 and level 4l whose Fourier coefficient are class numbers:

$$H_l(z) := \sum_{n\geq 0} H(n)_l q^n \quad \text{with}$$

$$H(n)_l = H(l^2 n) - l H(n)$$

where H(m) is the number of classes of positive definite binary quadratic forms with discriminant -m.

Define

$$G_{1,1}(z) := \tfrac{1}{2} h(-l) + \sum_{n\geq 1} \Big(\big(\sum_{d|n} (\tfrac{d}{l})\big)\Big) q^n \quad \text{with } h(-l) := \# Cl(\mathbb{Q}(\sqrt{-l})) \text{ and}$$

$$C_l(z) := \frac{l-1}{12} G_{1,1}(4z)\,\Theta(lz) - \tfrac{1}{2} h(-l) H_l(z) =: \sum_{n\geq 0} c_n q^n .$$

The following result is the main result of [A-K]:

<u>Theorem 4.4.</u> C_l is a cusp form of weight 3/2 in $S^-_{3/2}(4l,\psi_0)$ with

$$C_l \equiv -\tfrac{1}{2} h(-l) H_l \bmod p \quad \text{and}$$

$$S(C_l) \equiv -\tfrac{1}{2} h(-l)^2 \mathcal{E}_{2,l} \bmod p .$$ [1]

The $\mathbb{T}$-module generated by C_l is generated over $\mathbb{C}$ by those eigenforms $F_r \in S^-_{3/2}(4l)$ for which

$$L(S(F_r),1) \cdot L(S(F_r) \otimes \chi_{-l},1) \neq 0 .$$

Now assume that $p \nmid h(-l)$.
Then

<u>4.5.</u> $$f_E = S(F) \equiv \frac{-2}{h(-l)^2} S(C_l) \bmod p .$$

[1] cf. Propositon 3.1

Let $F(z) = \sum_{n\geq 1} a_n q^n \in S_{3/2}(N,\chi_t)$ be a form with $S(F) = f_E$, then the question arises under which conditions the equivalence

$$p \mid a_d \text{ if and only if } p \mid c_d \quad \text{(for certain d)}$$

is a consequence of 4.5.

To be more precise:

Question 4.6. Let d_0 be a square free natural number such that $p \nmid a_{d_0} \cdot c_{d_0}$ and $L_{E_{-td_0}}(1) \neq 0$.
Under which conditions implies the congruence 4.5 the equivalence

$$p \mid a_d \text{ if and only if } p \mid c_d$$

4.7. for all square free natural numbers d with $d \equiv d_0 \bmod \prod_{p \mid N} \mathbb{Q}_p^{\times 2}$ and $d \cdot d_0$ prime to N?

Using Waldspurger's result (Theorem 2.4) a sufficient condition for an affirmative answer is that p is not a congruence prime for f_E, i.e. that there is no cusp form $g \neq f$ of weight 2 and level l which is congruent to f modulo p.

Examples for which this condition is satisfied are given by the curves $X_0(11)$ ($p = 5$) and (19 B) (for $p = 3$).

Since, for square free n prime to p

$$H(n)_l = H(l^2 n) - l\,H(n) = -\tfrac{1}{2}\left(1 + \left(\tfrac{n}{l}\right)\right) H(n)$$

we get (with the notation introduced above)

Proposition 4.8. Assume that $F(z) = \sum_{n=1}^{\infty} a_n q^n \in S_{3/2}(N,\chi_t)$ is mapped to f_E. Assume that 4.7 holds with a natural number d_0, for instance assume that p is no congruence prime for f_E. Then for $d \in \mathbb{N}$ square free with $d \equiv d_0 \bmod \prod_{p \mid N} \mathbb{Q}_p^{\times 2}$ and $d \cdot d_0$ prime to N one has

$$p \mid a_d \text{ if and only if } p \mid H(l^2 d) - l\,H(d)$$

hence $L_{E_{-td}}(1) \neq 0$ if $p \nmid h(-d)$.

In view of our proposition 1.5 this result should be taken a support for conjecture 2.5.
For $X_0(11)$ we get: Assume that $\left(\frac{d}{11}\right) = 1$. Then $5 \mid \# S(E_{-d},\mathbb{Q})$ if and only if 5 di-

vides the class number of $Q(\sqrt{-d})$ (Prop. 1.5) and so $5 | a_d$ if and only if $5 | \# S(E_{-d},Q)$ (cf. [Ma]).
For E = (19 B) we get: Assume that $(\frac{d}{19}) = 1$ then $3 | \# S(E_{-d},Q)$ if and only if 3 divides the class number of $Q(\sqrt{-d})$ and so $3 | a_d$ if and only if $3 | \# S(E_{-d},Q)$.
Since the form F in example 5, table 3.7, which is mapped to the form corresponding to E = (38D) is congruent modulo 3 to the form corresponding to (19B) we get the same result for (38D)

References

[A] J.A. Antoniadis: Diedergruppe und Reziprozitätsgesetz: J. reine angew. Math. 377 (1987).

[A-K] J.A. Antoniadis and W. Kohnen: Congruences between cusp forms and Eisenstein series of half-integral weight: Abh. Math. Sem. Univ. Hamburg 57 (1987).

[B-F] P. Bayer and G. Frey: Constructions of modular forms of weight one by 2-coverings of elliptic curves: to appear.

[B-I] H. Brandt and O. Intrau: Tabellen reduzierter positiver ternärer quadratischer Formen: Abh. Sächs. Akad. Wiss. Math.-Nat. Kl. 45. Heft 4 (1958).

[C] T. Crespo: Sobre el problema de immersion de la teoria de Galois: Thesis Barcelona (1987).

[D-S] P. Deligne et J.P. Serre: Formes modulaires de poids 1: Ann. Sc. de l'ENS 7 (1974).

[Fr 1] G. Frey: On the Selmer group of twists of elliptic curves with Q-rational torsion points: Canadian Journal of Math. (1988).

[Fr 2] G. Frey: Der Rang der Lösungen von $y^2 = x^3 \pm p^3$ über Q: Manuscripta math. 48 (1984).

[Ko] W. Kohnen: Newforms of half-integral weight: J. reine angew. Math. 333 (1982).

[Kol] V.A. Kolyvagin: Finiteness of E(Q) and Ш(E,Q) for a class of Weil curves: Izv. Akad. Nauk. SSSR Ser. Math.

[Le] J.L. Lehman: Rational points on elliptic curves with complex multiplication by the ring of integers of $Q(\sqrt{-7})$: J. of Number Theory 27 (1987).

[Ma] B. Mazur: On the arithmetic of special values of L-functions. Invent. math. 55 (1979).

[MF IV] Modular functions of one variable IV: Lecture Notes in Mathematics 476 (1975).

[Ru 1] K. Rubin: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication; Invent. math. 89 (1987).

[Ru 2] The work of Kolyvagin on the arithmetic of elliptic curves; Preprint Max-Planck-Institut (1988).

[S-P] R. Schulze-Pillot: Thetareihen positiv definiter quadratischer Formen; Invent. math. 75 (1984).

[Se] J.P. Serre: L'invariant de Witt de la forme $Tr(x^2)$; Comment. Math. Helvetici 59 (1984).

[S-ST] J.P. Serre and H.M. Stark: Modular forms of weight 1/2; in: Modular functions of one variable VI, Lecture Notes in Mathematics 627 (1977).

[Sh 1] G. Shimura: Introduction to the arithmetic theory of automorphic functions; Princeton University Press (1971).

[Sh 2] G. Shimura: On modular forms of half integral weight; Ann. of Math. 97 (1973).

[Si] J.H. Silverman: The arithmetic of elliptic curves; New York (1986).

[Tu] J.B. Tunnell: A classical diophantine problem and modular forms of weight 3/2; Invent. math. 72 (1983).

[Wa] J.L. Waldspurger: Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. pures et appl. 60 (4) (1981).

Jannis A.Antoniadis
Department of Mathematics
University of Crete
Iraklio Crete, GREECE

M.Bungert, G.Frey
Fachbereich 9 Mathematik
der Universität des Saarlandes
6600 Saarbrücken, B.R.D